Exhibit D, F, G

Digital Security Solutions

RFP No. 24-43230000-RFP

Attachment L1 – Service Category 1: Endpoint-Based Asset Discovery

Respondent Name: R2 Unified Technologies

Solution Name: SentinelOne Singularity Vulnerability Management

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 10. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 10 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 10 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-10 / 9) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1.

Prompt 1: An Endpoint-Based Asset Discovery Solution must continuously scan, detect, and inventory all endpoint devices, including, but not limited to, laptops, desktops, servers, and any other connected devices across the enterprise. The Solution must utilize lightweight agents that are deployed via endpoints, consuming minimal CPU and memory resources to avoid degrading performance or user experience.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Vulnerability Management (formerly known as Network Discovery) is designed to leverage the Singularity Complete agent to do a lightweight scanning of a customer's network scanning for other devices, inventory the devices, OS, applications, type, version, and more. This information can be used to identify risky devices like those without an agent or IoT devices with an easy to use interface.

The core functionality of Singularity Vulnerability Management includes continuous and real-time visibility into application and operating system vulnerabilities across Windows, macOS, and Linux environments. This solution leverages both passive and active scanning techniques to identify and fingerprint devices, including IoT devices, with unmatched accuracy. This dual approach ensures that security teams can capture crucial information and maintain a high level of network visibility without the need for traditional, bandwidth-intensive network scanners.

One of the standout features of Vulnerability Management is its ability to prioritize vulnerabilities based on the likelihood of exploitation and business criticality. This prioritization helps organizations focus their remediation efforts on the most critical vulnerabilities, thereby maximizing risk reduction with minimal effort. The solution also automates controls to isolate unmanaged endpoints and deploy agents, closing visibility gaps and enhancing overall security posture.

Singularity Vulnerability Management simplifies the vulnerability management process by eliminating the need for tedious scheduled scans and reducing dependency on network connectivity. This is particularly beneficial in a remote-first world where traditional network vulnerability scanners may fall short. The solution deploys in minutes as an add-on to existing EDR deployments, providing immediate value without the need for additional siloed security tools.

The platform also offers a high degree of customization, allowing security teams to control the depth and breadth of their vulnerability scans through customizable scan policies. This ensures that the scanning process aligns with the specific needs and priorities of the organization.

In addition to its core capabilities, Singularity Vulnerability Management includes a graphic dashboard that provides a comprehensive overview of vulnerability data. This dashboard aggregates risks by applications and allows users to drill down into additional data based on endpoints or CVEs. The solution also scores each vulnerability based on temporal values, reflecting the current state of exploit techniques or code availability, which helps in making informed decisions about vulnerability management.

Vulnerability Management is included in the offering laid out in Category 3 - Endpoint Detection and Response because it cannot be used without Singularity Complete licenses.

Network Discovery is no longer available for sale company-wide at SentinelOne.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Real-Time Asset Discovery –Solution should run continuously, detecting new devices as they connect to the network. This should include remote devices.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Scans run automatically at a set interval of one week, once enabled. Scans can also be configured to run only on certain devices, exclude/include certain devices from scanning, and exclude/include specific networks from being scanned. This includes remote networks that can be configured to scan only when a set number of devices with an agent are on the same network as to avoid populating the data with inventories of public networks when a single device connects to a public wifi network.

Prompt 3: Detailed Hardware and Software Inventories – Solution should include inventory of processor types, memory, storage, installed software, patch levels, operating system versions, and device configurations.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Vulnerability Management includes data like chassis type, internal and public IP address, OS type/version, secured state, host name, MAC, manufacturer, discovery method, open ports and more. It also includes application scanning.

Also it provides CVEs ranked by temporal value, exploit method, OS level vulnerabilities, missing patches, and ranks them. Also includes data like attack vector, complexity, and more. This creates an inventory of applications and respective versions on each device.

Prompt 4: Customizable Asset Classifications – Solution should allow administrators to tag devices by type, location, or business unit for easier management.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Vulnerability Management can tag devices by type, IP, or add custom tags. This is in addition to the device fingerprinting to reduce duplication. It also has the ability to see vulnerabilities grouped by application or other metrics to help prioritize the riskiest vulnerabilities for more effective vulnerability remediation.

Devices can always be grouped by the site/group hierarchy used to manage machines in the console.

Prompt 5: Agent Health Monitoring – Solution should ensure that agents are functioning correctly and can be managed or repaired from a central console, if necessary. The Solution should provide alerts if an agent becomes inactive or fails to report.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The new Singularity Health Center (included in Complete EDR) is a central management interface for operational observability. It monitors endpoint protection and asset operational health status, and provides immediate visibility into unprotected and partially-protected assets. This allows console users to identify any issues from agent resource usage, operation and protection state, connectivity, or configuration.

Prompt 6: Centralized Management Console – Solution should provide a centralized management console that displays an up-to-date view of all discovered endpoints, including non-standard devices such as personal mobile devices or tablets.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Vulnerability Management is contained within the same centralized console as the Complete EDR functionality. This makes it easy to see and act on this data as you are managing endpoints, removing the requirement to switch consoles or manage another account login to manage asset discovery and vulnerabilities.

This includes the management of workstations, servers, mobile, IoT, printer, medical devices and more.

Prompt 7: Compliance Enforcement – Solution should provide alerts to where endpoints that fail to meet security requirements (e.g., outdated patches or unauthorized software) can be flagged for remediation.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The solution has the ability to identify vulnerable applications and apply attributes based on context, which allows the ability to create custom filters and alerts to prioritize vulnerabilities by criticality, likelihood of exploitation, and if a patch/mitigation has been applied. Custom alerts can also be created using STAR rules to alert on unauthorized applications and notify users of the affected endpoints. Rules can be configured to alert and configured to take action on the event.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time insights into endpoint vulnerabilities, ensuring that newly discovered devices are checked against the latest IoCs (Indicators of Compromise) and CVEs (Common Vulnerabilities and Exposures) behaviors targeting specific operating systems or device types.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Vulnerability Management constantly updates with the latest intelligence brought in from a variety of sources. The base CVE score of a vulnerability doesn't change, but the temporal score can be updated based on newly available information like how it is exploited or a change in its confidentiality.

Prompt 9: Patching and Deployment Capability – Solutions should provide endpoint patch and deploy services which allows managing patch and deployment of operating system and application updates on systems utilizing the agent.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Patch management is not currently a function of the Vulnerability Management modules, but it is expected to be added in the future. Once available, SentinelOne will look to add the product to the contract.

Prompt 10: Metrics – Solution should provide the ability to roll-up patch and deployment level metrics across the domain.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Patch management is not currently a function of the Vulnerability Management modules, but it is expected to be added in the future. Once available, SentinelOne will look to add the product to the contract.

Metrics can be gathered from the console on a number of different metrics for review.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SentinelOne provides a 99.5% uptime for the Management Server and Console.

SentinelOne Agents are autonomous and continue to provide protection and detection, even when the Management is undergoing maintenance.

The maintenance window below is not included in this SLA.

Maintenance Window:

SentinelOne reserves the right to perform maintenance operations on Sundays:

Maintenance Start: 10:00 UTC+3

Maintenance End: 18:00 UTC+3

Maintenance Stages:

SentinelOne does our best to limit actual customer downtime to two hours every other week.

Global and Regional Infrastructure Maintenance - Customers have access to their Management Console but specific cloud services might be unavailable intermittently. This can affect all customers, starting at 9:00.

Global and Regional infrastructure maintenance typically runs for two hours, but it can continue until 18:00.

Specific Customer Maintenance - Only specific customers are affected while their management is undergoing maintenance. During a customer's maintenance slot, they might not be able to access their Management Console. SentinelOne Agents continue to provide protection and detection.

Customer maintenance slots begin as soon as the Global and Regional infrastructure maintenance is completed, and end by 18:00. Slots are scheduled by region, so that downtime is as convenient as possible. The euce1-100 and euce1-102 are updated from 17:00 until 19:00.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L2 – Service Category 2: Network-Based Asset Discovery

Respondent Name: R2 Unified Technologies

Solution Name: Cisco Identity Services Engine

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: A Network-Based Asset Discovery Solutions identifies devices and systems communicating within the network infrastructure without the need for software agents to be deployed to most endpoints or servers. By analyzing network traffic, the Solution should detect all connected assets, including those that do not run traditional operating systems, such as IoT devices, switches, routers, and printers.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cisco utilizes network-based asset discovery solutions to identify devices and systems within the network infrastructure without requiring software agents on endpoints or servers. By analyzing network traffic, these solutions detect all connected assets, including those without traditional operating systems, such as IoT devices, switches, routers, and printers. Here's how Cisco achieves this:

Key Solutions and Methods:

1. Cisco Secure Network Analytics

Cisco Secure Network Analytics leverages agentless technology to deliver comprehensive, enterprise-wide visibility across on-premises and cloud environments. It continuously monitors network activities, using protocols like SNMP and NetFlow to analyze traffic patterns and behaviors. This enables the solution to detect and classify connected devices, including those without traditional operating systems.

•Traffic Analysis: Continuously analyzes network flows to detect and monitor devices based on their behavior and communication patterns.

•Baseline Behavior: Creates baselines for normal network activity and identifies anomalies that could indicate unauthorized or unknown devices.

•IoT and Non-Traditional Devices: Detects and monitors IoT devices, switches, routers, and other non-traditional devices without the need for endpoint agents.

2. Cisco Identity Services Engine (ISE)

Cisco ISE enhances visibility by profiling devices as they connect to the network. Using passive network monitoring and active probing, ISE collects detailed information about connected assets and categorizes them.

•Device Profiling: Profiles devices such as printers, IoT endpoints, and unmanaged assets by analyzing network behavior and using metadata.

•Access Control: Enables organizations to enforce network access policies based on device type and security requirements, ensuring secure segmentation and management.

3. Network Traffic-Based Discovery

Cisco solutions rely on traffic data to identify and classify connected devices. By analyzing communication patterns, protocols, and device fingerprints, the platform provides visibility into all devices communicating on the network, including:

•IoT devices

•Operational Technology (OT) systems

•Network equipment (e.g., switches, routers)

•Printers and other non-standard endpoints

Benefits of Cisco's Network-Based Asset Discovery

•Provides a holistic view of all connected devices, including unmanaged and non-traditional systems, ensuring no asset is overlooked.

•Identifying devices enables organizations to enforce appropriate security controls, monitor behaviors, and mitigate risks from unauthorized or rogue devices.

•Eliminates the need for software agents on endpoints, reducing deployment overhead and streamlining device inventory management.

•Detects anomalies and suspicious activities based on device behavior, enabling early threat detection and response.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Agentless Discovery – Solution should be capable of using passive network scanning techniques that observe traffic and communications, including deep packet inspection (DPI) and flow-based analysis.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco ISE supports agentless discovery using passive network scanning techniques, including deep packet inspection (DPI) and flow-based analysis. By observing network traffic and communications, it identifies and profiles devices without the need for agents. DPI helps analyze the payload of packets for detailed device identification, while flow-based analysis provides insights into traffic patterns, enabling comprehensive asset discovery and classification across the network.

Prompt 3: Continuous Network Monitoring – Solution should automatically detect new devices as they are added to the network, whether they are traditional endpoints, virtual machines, or IoT devices.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco ISE provides continuous network monitoring, automatically detecting new devices as they are added to the network. Whether traditional endpoints, virtual machines, or IoT devices, Cisco ISE profiles and classifies these devices based on network behavior. This continuous monitoring ensures that all devices are promptly detected and securely integrated into the network, enhancing visibility and security in real-time.

Prompt 4: Granular Device Identification – Solution should collect metadata such as MAC address, IP address, operating system, software versions, device make and model and open ports.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco ISE provides granular device identification by collecting detailed metadata, including MAC address, IP address, operating system, software versions, device make and model, and open ports. It uses profiling techniques to gather this information through network traffic analysis, enabling accurate classification and detailed visibility of all devices on the network. This metadata helps administrators enforce security policies based on device characteristics and behavior.

Prompt 5: Network Topology Visualization – Solution should map discovered devices and displays how they connect and communicate within the network. The visualization should dynamically update as devices are added, removed, or reconfigured.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco ISE provides network topology visualization by mapping discovered devices and illustrating how they connect and communicate within the network. It dynamically updates this visualization as devices are added, removed, or reconfigured, giving administrators real-time insight into network changes. This helps maintain accurate network maps and enhances visibility into device interactions, enabling effective security monitoring and management.

Prompt 6: Customizable Device Grouping and Tagging – Solution should allow administrators to categorize assets based on network segment, physical location, or function (e.g., servers, IoT, printers).

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco ISE allows administrators to categorize assets using customizable device grouping and tagging. Devices can be grouped based on network segment, physical location, or function (e.g., servers, IoT devices, printers). This flexibility enables tailored security policies and access control for different asset types, enhancing network segmentation and simplifying management of diverse devices within the infrastructure.

Prompt 7: Vulnerable Detection – Solution should identify outdated software versions, unpatched firmware, or insecure configurations that could expose the network to threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco ISE identifies vulnerable devices by profiling and analyzing their configurations, software versions, and firmware. It detects outdated software versions, unpatched firmware, or insecure configurations that could expose the network to threats. By continuously monitoring devices, ISE helps administrators spot vulnerabilities and enforce security policies to mitigate risks, ensuring devices comply with up-to-date security standards and reducing the likelihood of exploitation.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time insights into suspicious network activity, such as communication with known malicious IP addresses or domains. Solution should flag devices that may be compromised or communicating with threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco ISE integrates with various threat intelligence solutions to provide real-time insights into suspicious network activity. This integration helps identify devices communicating with known malicious IP addresses or domains. When such activity is detected, ISE can flag affected devices, enabling security teams to take appropriate action, enhancing network security and helping to mitigate potential risks.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L3 – Service Category 3: Endpoint Detection and Response

Respondent Name: R2 Unified Technologies

Solution Name: Cisco Secure Endpoint

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 9. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 9 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 9 are worth a maximum of 4 points total. An individual Evaluator's technical score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-9 / 8) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: An Endpoint Detection and Response (EDR) Solution is designed to provide continuous and comprehensive monitoring of endpoint activities to detect, investigate, and respond to threats in real-time. The Solution collects and analyzes detailed telemetry data, such as file access patterns, process execution, network connections, and registry changes, to identify malicious behavior that traditional antivirus software might miss.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Endpoint provides a robust Endpoint Detection and Response (EDR) solution designed to deliver comprehensive, real-time protection across all endpoint activities. Leveraging advanced telemetry collection, Secure Endpoint continuously monitors and analyzes data points like file access, process execution, network interactions, and registry modifications. This proactive analysis goes beyond traditional antivirus capabilities, detecting sophisticated, emerging threats that might evade basic defenses.

Our solution employs behavioral analysis and machine learning to identify and categorize suspicious actions based on typical threat behavior patterns. By using these insights, Cisco Secure Endpoint can pinpoint malware, ransomware, and other threats early, triggering immediate alerts and automated responses to mitigate risks before they escalate. Threat intelligence is continually updated from Cisco Talos, one of the largest commercial threat intelligence teams globally, ensuring Secure Endpoint stays ahead of the latest tactics and threat variants.

Cisco Secure Endpoint's real-time response capabilities empower teams with the tools needed to swiftly investigate incidents, offering a clear picture of the attack's progression. The platform includes endpoint isolation, file and process blocking, and retrospective alerting, which enables remediation even after initial execution. The cloud-managed solution simplifies deployment and offers scalable monitoring and response across large, distributed environments without extensive infrastructure overhead.

Secure Endpoint's unified interface enhances visibility into endpoint security status, allowing IT teams to focus on prioritized, actionable insights. Integration with Cisco XDR extends this visibility across the broader security environment, correlating endpoint data with network, email, and cloud telemetry to provide holistic threat insights. Together, these features offer a solution that not only detects and investigates threats but also provides the means to quickly and effectively neutralize them, aligning with the real-time response requirements outlined in the prompt.

This robust EDR functionality makes Cisco Secure Endpoint a strong choice for organizations seeking comprehensive, real-time threat detection and response capabilities.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Real-Time Monitoring and Logging – Solution should provide real-time monitoring and logging of all endpoint activities, including, but not limited to, file changes, process creation and termination, registry edits, network connections, and USB device insertion.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Endpoint offers real-time monitoring and logging of endpoint activities, including file changes, process creation/termination, registry edits, network connections, and USB device insertions. This continuous telemetry enables rapid threat detection, providing security teams with detailed insights into endpoint behavior. The solution's cloud-based architecture ensures real-time data visibility and analysis, supporting proactive threat monitoring across all endpoints.

Prompt 3: Behavioral Analytics – Solution should use an extended portfolio of security tools, like endpoint firewalls, device and application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Endpoint uses behavioral analytics, combining signature matching, process monitoring, and file analysis to detect threats beyond traditional methods. While it integrates endpoint controls like application whitelisting and process blocking, it does not include built-in firewall, patch management, or email security features. However, it delivers robust endpoint-focused analytics to detect and respond to malicious behaviors effectively.

Prompt 4: Automated Response Mechanisms – Solution should take predefined actions when threats are detected, such as isolating the affected device from the network, terminating malicious processes, or blocking IP addresses.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Endpoint includes automated response mechanisms that take predefined actions when threats are detected, such as isolating compromised devices, terminating malicious processes, and quarantining suspicious files. These automated responses help contain threats immediately, reducing the risk of lateral spread and mitigating impact. By enabling customizable response actions, Secure Endpoint supports rapid, consistent threat containment across all monitored endpoints.

Prompt 5: Threat Hunting Tools – Solution should allow analysts to query across the entire organization's endpoints, searching for specific indications or compromise (IoCs) or patterns that may indicate the presence of advanced threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Endpoint provides threat-hunting capabilities, allowing analysts to query across all endpoints for specific IoCs or suspicious activity patterns. Security teams can search by file hash, process name, IP, and other indicators to detect advanced threats. This capability enables proactive identification of potential compromises and supports in-depth investigation, helping analysts quickly uncover threats across the entire endpoint environment.

Prompt 6: Support for Remote Endpoints – Solution should ensure that devices outside of the network, such as remote or mobile works, are protected and monitored regardless of location.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Endpoint provides comprehensive protection and monitoring for remote devices, ensuring continuous security regardless of location. Its cloud-based management enables real-time visibility, threat detection, and automated responses for endpoints outside the corporate network. As long as the remote device is internet-connected, it remains protected, receiving updates and allowing security teams to monitor and manage it effectively.

Prompt 7: Remediation Playbooks – Solution should provide detailed guidance for resolving detected incidents, including step-by-step instructions for isolating infected devices, rolling back malicious changes, and restoring systems to a known good state.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Endpoint provides essential remediation tools like device isolation, malicious process termination, and file quarantine. Security teams can leverage its capabilities to develop customized workflows for incident response, allowing them to isolate threats, remove malicious elements, and restore devices to a secure state based on organizational policies and needs.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time updates on emerging malware strains, threat actor campaigns, and new attack vectors targeting endpoints. The EDR Solution can use CTI feeds to compare endpoint behavior when known IoCs, enhancing detection and automated response capabilities.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Endpoint integrates with Cisco Talos for real-time CTI data, providing updates on emerging malware, threat actor campaigns, and attack vectors. This CTI integration allows Secure Endpoint to compare endpoint behavior with known IoCs, enhancing its detection and response capabilities. By leveraging Talos intelligence, Secure Endpoint dynamically adapts to new threats, enabling proactive identification and automated responses to evolving endpoint risks.

Prompt 9: Forensic Capabilities – Solution should allow security analysts to investigate historical endpoint activities, enabling root cause analysis and providing a detailed timeline of events leading up to a security incident.

Cisco Secure Endpoint offers robust forensic capabilities, allowing security analysts to investigate historical endpoint activities for root cause analysis. It provides detailed timelines of events, capturing file actions, process executions, network connections, and registry changes. This data

enables analysts to reconstruct the sequence leading to an incident, understand attack origins, and assess impact, supporting thorough investigations and informed responses.

Digital Security Solutions

RFP No. 24-43230000-RFP

Attachment L3 – Service Category 3: Endpoint Detection and Response

Respondent Name: R2 Unified Technologies

Solution Name: Singularity Complete, Vulnerability Management, and Vigilance MDR + DFIR

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 9. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 9 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 9 are worth a maximum of 4 points total. An individual Evaluator's technical score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-9 / 8) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: An Endpoint Detection and Response (EDR) Solution is designed to provide continuous and comprehensive monitoring of endpoint activities to detect, investigate, and respond to threats in real-time. The Solution collects and analyzes detailed telemetry data, such as file access patterns, process execution, network connections, and registry changes, to identify malicious behavior that traditional antivirus software might miss.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

SentinelOne's platform suite proposed for Category 3 includes these products;

●Singularity Complete Endpoint Detection and Response (EDR) covering workstations, servers, pods, and containers

●Vigilance Managed Detection and Response (MDR) + DFIR

●Singularity Vulnerability Management

●Singularity Platform access

With this suite of tools the solution is a comprehensive EDR solution that is supported by a 24/7/365 MDR service, and can identify malicious and suspicious behaviors, respond to those behaviors with automated and human resources, discover vulnerabilities, risks, and unprotected or unknown assets, all in one easy to use console.

Complete EDR is an agent based behavioral process inspection tool that protects against threats and malicious activities in real time. This leverages local machine learning engines (no internet access required) that is backed up by the collection, analysis, and contextualization of telemetry like file access, process execution, and more that enable threat hunting and improve remediation efforts.

SentinelOne's Complete EDR is ranked by MITRE ATT&CK as a top performer and had the least amount of noisy alerts passing the detection and protection phases with only 7 consolidated alerts that create an easy to use experience, while still maintaining the same level of detail as those with tens of thousands of alerts.

SentinelOne is not only top rated for efficacy but also leverages a defense-in-depth strategy with features like patented One-Click Ransomware Rollback, and deception tactics allowing attackers to think that they're successful, distracting them from their mission and giving you precious time to respond.

The included Vigilance MDR +DFIR Managed Detection and Response service brings 24/7 hands-on-keyboard analysts that are responding to detections as they happen with a mean-time-to-response under 22 min. This service is also specifically staffed with 100% US based individuals that are all US citizens to comply with the FedRAMP policy. It also includes a bank of hours for Digital Forensics and Incident Response that can be used any time.

The entire offering is the only EDR that is FedRAMP High certified.

More about what's included with our Vulnerability Management can be found in our response to Service Category 1, and by purchasing this category these will be included in the purchase for no additional cost. Previously only Network Discovery was presented, but that has been replaced company-wide with Vulnerability Management to improve the amount of useful information in the console driving decision making.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Real-Time Monitoring and Logging – Solution should provide real-time monitoring and logging of all endpoint activities, including, but not limited to, file changes, process creation and termination, registry edits, network connections, and USB device insertion.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The SentinelOne Complete agent monitors all activities named and logs all data considered standard EDR data for 14 days. If an alert is created then the related data is kept for 1 year. This activity is the first layer of how the EDR tool then uses its machine learning and artificial intelligence to know what to block, flag, or ignore, to stop threats but allow normal activity to continue.

Prompt 3: Behavioral Analytics – Solution should use an extended portfolio of security tools, like endpoint firewalls, device and application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Behavioral analysis is the core function of SentinelOne's EDR functionality. Leveraging machine learning and artificial intelligence that doesn't require a cloud connection to work is critical to the successful protection of the machines. There are currently 13 different detection engines on each agent inspecting different behaviors and processes. The Vulnerability Management tool improves that functionality to show missed patches, known vulnerabilities, and consequences of not resolving.

Prompt 4: Automated Response Mechanisms – Solution should take predefined actions when threats are detected, such as isolating the affected device from the network, terminating malicious processes, or blocking IP addresses.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The most simple responses are built in the policy to "kill, quarantine, remediate, or roll back" an affected machine automatically as prescribed in the policy manually or automatically.

Additionally, leveraging STAR rules and the provided library of rule templates, actions can be defined for certain scenarios based on the policies, hashes, etc.
Beyond EDR, the MDR service can build playbooks with a customer on how they should respond to a threat or alert of observed malicious behavior.

Prompt 5: Threat Hunting Tools – Solution should allow analysts to query across the entire organization's endpoints, searching for specific indications or compromise (IoCs) or patterns that may indicate the presence of advanced threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The SentinelOne management console provides an easy-to-use user interface with a built-in feature called Deep Visibility. Deep Visibility allows security analysts to easily run queries against all endpoints at once, or with targeted queries against specific endpoints. This feature comes standard with example queries, syntax guides, and autocomplete-predictive assist to aid analysts in writing their queries. All common IoC types can be entered into queries, either individually or in combinations.

Prompt 6: Support for Remote Endpoints – Solution should ensure that devices outside of the network, such as remote or mobile works, are protected and monitored regardless of location.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Endpoints are always protected whether they are on network or off, at work, at home, anywhere. They're even protected by the agent if the device is disconnected from the internet entirely. That's because the cloud console is used only for management and monitoring by users and Vigilance, but the machine-speed protection is always working locally with very limited resource utilization.

Prompt 7: Remediation Playbooks – Solution should provide detailed guidance for resolving detected incidents, including step-by-step instructions for isolating infected devices, rolling back malicious changes, and restoring systems to a known good state.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The solution has the ability to both automatically or manually respond and resolve incidents, using the mitigation actions (Kill, Quarantine, Remediate, Rollback). Using the combination of these actions will restore a device to the last known good state. SentinelOne provides customers with a library of detailed instructions and documentation on how to execute all of the possible response actions. Policies can be customized based on the user's needs, to respond using minimal or full action.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time updates on emerging malware strains, threat actor campaigns, and new attack vectors targeting endpoints. The EDR Solution can use CTI feeds to compare endpoint behavior when known IoCs, enhancing detection and automated response capabilities.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

SentinelOne continuously receives threat intel from multiple sources on a regular basis, and uses that to create block rules at the Cloud level (SentinelOne controlled) which is then available for the customer. These blocks are designed to block major adversaries and threats that are active and identified in the wild. It also has the ability to connect threat intel sources to a customer's console to enrich threat data, both from major threat intel companies and custom repositories (add on).

Prompt 9: Forensic Capabilities – Solution should allow security analysts to investigate historical endpoint activities, enabling root cause analysis and providing a detailed timeline of events leading up to a security incident.

Leveraging the available EDR and event data, threat hunting is made easy with visual timelines of an event, process graphs to visualize the event and related events, and searching the EDR logs is intuitive and easily filtered to find relevant information.

PurpleAI makes this even simpler by allowing analysts to use natural language to ask questions of the EDR data, provide summaries of alerts, and suggest additional actions. (add on)

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Management Console SLA

SentinelOne provides a 99.5% uptime for the Management Server and Console.

SentinelOne Agents are autonomous and continue to provide protection and detection, even when the Management is undergoing maintenance.

The maintenance window below is not included in this SLA.

Maintenance Window:

SentinelOne reserves the right to perform maintenance operations on Sundays:

Maintenance Start: 10:00 UTC+3

Maintenance End: 18:00 UTC+3

Maintenance Stages:

SentinelOne does our best to limit actual customer downtime to two hours every other week.

Global and Regional Infrastructure Maintenance - Customers have access to their Management Console but specific cloud services might be unavailable intermittently. This can affect all customers, starting at 9:00.

Global and Regional infrastructure maintenance typically runs for two hours, but it can continue until 18:00.

Specific Customer Maintenance - Only specific customers are affected while their management is undergoing maintenance. During a customer's maintenance slot, they might not be able to access their Management Console. SentinelOne Agents continue to provide protection and detection.

Customer maintenance slots begin as soon as the Global and Regional infrastructure maintenance is completed, and end by 18:00. Slots are scheduled by region, so that downtime is as convenient as possible. The euce1-100 and euce1-102 are updated from 17:00 until 19:00.

MDR Service:

Vigilance Managed Detection and Response leverages KPIs for target response times. This is the second line of defense after the agent sends an in-scope alert.

Critical - 45 mins - Imminent or ongoing threat with potential for catastrophic impact.

High - 2 hours - Significant potential impact

Medium - 3 hours - Moderate potential impact

Low/Informational - 5 hours - Minor potential/ not indicative of a threat.

The target is to respond to 90% of alerts in a calendar month within the target response time.

Any applicable Additional Terms and Conditions Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L5 – Service Category 5: Email Security

Respondent Name: R2 Unified Technologies

Solution Name: Abnormal

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Email Security Solutions must protect against email-based threats such as phishing, malware, ransomware, and email compromises. The Solution should analyze both inbound and outbound email communications in real-time, using advanced detection techniques to filter malicious content without disrupting legitimate business correspondence.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal Security provides comprehensive email protection against attacks that exploit human behavior, including malware, phishing, social engineering, ransomware, and account takeovers, with an email security platform that deeply understands human behavior.

Abnormal analyzes incoming email messages and detects potential threats in real-time. Abnormal is designed to be highly effective at identifying and blocking malicious emails, while minimizing false positives. Abnormal Security is classified as an Integrated Cloud Email Security (ICES) solution which supplements cloud email providers' (Microsoft and Google) built-in email security hygiene capabilities. Abnormal's ICES capabilities supplement these native features and utilize API access to the cloud email provider to analyze email content without the need to change the MX record.

Abnormal deeply understands human behavior to detect anomalies, protect against account takeovers, and prevent breaches. Abnormal uses a suite of neural networks and large language models to compare profiles to raw data and detect fraudulent topics, tone, and sentiment, including urgency and formality, within email content. The solution builds a relationship graph between entities both within and outside of your organization.

Abnormal, compared to other email security solutions, utilizes a modern API architecture to seamlessly integrate with M365 / GWS, using advanced AI and machine learning models to provide email security. While SEGs typically rely on rule-based filtering and known threat signatures, Abnormal employs behavioral analytics to detect subtle anomalies and identify sophisticated business email compromise attacks.

The API architecture eliminates the need for changes in MX records, ensuring it can work in parallel with email flow without disruptions. The API architecture gives Abnormal visibility on inbound email and also lateral email within an organization. Unlike SEGs which require constant updates, tuning, and rely on threat intelligence reports, Abnormal learns the different facets of emerging attacks automatically, and it autonomously adapts to how the customer interacts with email. Abnormal analyzes inbound emails against 40,000+ unique signals to detect malicious messages not only from what constitutes the attack but also from what aligns or deviates from the customer's normal email environment

Abnormal leverages multiple types of AI and machine learning models for the best security outcomes. These include a suite of neural networks, tree models, NLP, NLU, generative large language models LLMs) like GPT and discriminative LLMs like BERT. The models are used to create deep behavioral understanding for each customer, and used to detect fraudulent topics, tone, and sentiment, including urgency and formality, within email content for email protection.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Content Filtering – The Solution should break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, a nationally recognized standard, or company policy.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal utilizes a behavioral platform to judge the communication as a whole. This is the most effective method of protecting from attacks, where ones that utilize content disarm and reconstruction techniques fail. URLs contained within attachments are analyzed and Abnormal scans and extracts text from within images and other attachments. Attachments are also scanned for malware and malicious signals associated with the files are detected.

Prompt 3: Phishing Detection – Solution should analyze the email's context, structure, and metadata (e.g., header information) to detect phishing attempts, which may include spear-phishing and targeted attacks.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal provides techniques and technologies that prevent and counteract phishing attempts, unauthorized access, and theft. This includes Metadata Analysis, Uniform Resource Locator (URL) and Domain Analysis, Content Analysis, Behavioral Analysis, Real-Time Threat Intelligence. AI-Native approach to stop both credential and lateral phishing. ingests thousands of behavioral signals from multiple sources via the API architecture to detect unusual email-sending patterns.

Prompt 4: Sandboxing Technology – Solution should have the capability to safely execute email attachments and embedded links in an isolated environment to determine if they are malicious before delivery to the recipient.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Payload detection capabilities supplement behavioral analysis detection. This is the most effective method of detecting the spectrum of attacks. Sandboxing controls are bypassed by attackers through legitimate sites like SharePoint by embedding links from that site.. AI models detect and remediate malicious emails using signals including the behavior of links and attachments. There are pre-built integrations with AnyRun to provide sandboxing for threat hunting and investigation purposes.

Prompt 5: Advanced Anti Spoofing Protections – Solution should include enforcement of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols to prevent sender impersonation.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal Inbound Cloud Email Security is capable of spotting all types of spoofed emails, including uncommon signs other security solutions miss. Using hundreds of thousands of signals, including DMARC and SPF, Abnormal can stop email spoofing attacks before they reach inboxes, alongside dozens of other attack types. Abnormal leverages email authentication results (SPF, DKIM, DMARC, and ARC) as inputs into the detection platform to prevent sender impersonation.

Prompt 6: Email Encryption – Solution should include encryption for sensitive communications, ensuring enforcement that messages are encrypted both in transit and at rest.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal, partnered with Microsoft/Google, delivers multiple encryption options for data in transit and data at rest. M365/GWS rules can be configured to encrypt outgoing email messages and remove encryption from messages. This includes both emails originating within your organization and replies to encrypted messages sent from your organization. Using M365/GWS + Abnormal, you can replace your traditional SEG and remain confident in how you encrypt and protect your organization's data.

Prompt 7: End-User Awareness Features – Solution should include automatic banners or warnings added to suspicious emails, helping users recognize potential threats.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal enables an organization to add banners to emails to indicate caution or draw attention to possible email risks. Customers can also choose to use the Microsoft-native and Google-native email bannering capabilities. The use of bannering and being dependent on security awareness training as primary email security controls are no longer necessary for customers that deploy Abnormal. The organization can still choose to utilize banners on the messages deemed safe by Abnormal if desired.

Prompt 8: Quarantine and Remediation Tools – Solution should provide quarantine and remediation tools for administrators, allowing them to review flagged messages, release legitimate emails mistakenly identified as threats, and block harmful content.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal customers can report False Positives through the Detection 360 page in the Portal. Abnormal has a Detection team that uses Detection 360 data to improve their AI models and provide customers with transparency into the frequency of FPs. Abnormal also locates all messages related to a misclassified case and returns FP messages to user inboxes. Flagged messages are reviewed by administrative users in the threat log, and harmful content can be blocked and removed via Search and Respond.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

ABNORMAL SECURITY CORPORATION SUPPORT AND SERVICE LEVEL AVAILABILITY POLICY

This Support and Service Level Availability Policy ("Policy") describes Abnormal Security Corporation's ("Abnormal") support offering ("Support") in connection with Customer-reported bugs, defects, or errors in the Service ("Error(s)"). Support shall be provided in accordance with the written subscription agreement under which Abnormal provides its Service as entered into by and between you ("Customer") and Abnormal ("Agreement"). Customer shall receive the level of Support set forth in this Policy or as designated in the applicable Order ("Support Level"). Abnormal may update this Policy from time to time, provided that any such update does not modify any provision of the Agreement except for this Policy. Any such updates will be posted to https://legal.abnormalsecurity.com/ or otherwise made available as set forth in the Agreement. Capitalized terms not defined in this Policy shall have the meanings given to them in the Agreement.

I. Support

1. General Support Offering. Abnormal shall provide English-speaking remote assistance to Customer Contacts (as defined below) for questions or issues arising from any Error, as further described in this Policy, including troubleshooting, diagnosis, and recommendations for potential workarounds for the duration of Customer's subscription to the applicable Service.

2. Customer Contacts. Customer shall inform Abnormal as to its approved contacts for Support, one of which must be designated as an account administrator (each, a "Customer Contact"). Customer is solely responsible for maintaining an accurate list of Customer Contacts with Abnormal, including names and contact information. Abnormal assumes no responsibility for Support Cases that cannot be addressed due to a lack of updated Customer Contact information.

3. Submitting Support Cases. Customer Contacts must use reasonable diligence to ensure a perceived Error is not an issue with Customer's own equipment, software, or internet connectivity prior to requesting Support. Customer Contacts may contact Support by submitting a Support request (each, a "Support Case") to: (a) the support portal located at https://support.abnormalsecurity.com (or such successor URL as may be designated by Abnormal) (such website, the "Support Portal") or (b) the web interface as described in the Documentation. If Customer Contacts cannot access the Support Portal they may open a Support Case by emailing support@abnormalsecurity.com or, in the event Customer Contacts cannot access the Support Portal or email, they may contact Abnormal Support by phone solely for purposes of having the Support Case submitted on their behalf. All Customer Contacts must be familiar with the Documentation and be reasonably trained in the use and functionality of the

Service. Customer Contacts will assist Abnormal to resolve Support Cases by complying with the Customer obligations set forth in Table 1.

4. Support Cases. Each Support Case shall: (a) designate the Severity Level of the Error in accordance with the definitions in Table 1; (b) identify the Customer account that experienced the error; (c) include information sufficiently detailed to allow Abnormal to attempt to duplicate the Error (including any relevant error messages, but not export-controlled data, personal data (other than as required herein), sensitive data, other regulated data, or Customer Data); and (d) identify the Customer Contact most familiar with the issue. The Customer Contact shall also give Abnormal any other important Support Case information requested by Abnormal in a timely manner. Unless Customer expressly designates the Severity Level, the Support Case will default to Severity Level 4. If Customer Contacts submit Support Cases related to enhancement or feature requests, Abnormal shall treat those tickets as closed once the request has been forwarded internally.

Table 1: Error Severity Level Definitions and Initial Response Times

Error Severity Level	Description	Initial Response Time Target	Customer Responsibility
Severity Level 1 (Urgent)	An Error that causes a (a) service disruption or (b) degraded condition that renders the Service inoperable.	One (1) Hour	Commit appropriate resources to provide additional information as needed. Make reasonable efforts to apply solutions quickly.
Severity Level 2 (High)	An Error that (a) causes the Service to operate in a degraded condition with a high impact to key portions of the Service or (b) seriously impairs Customer's use of material function(s) of the Service and Customer cannot reasonably circumvent or avoid the Error without the expenditure of significant time or effort.	Two (2) Business Hours	Commit appropriate resources to be available to provide additional information as needed. Make reasonable efforts to apply solutions upon receipt.
Severity Level 3 (Normal)	An Error that has a medium-to-low impact on the Service. The Service is (a) running with limited functionality in one or more areas or (b) experiencing intermittent issues. Customer can		

access and use the material functionality of the Service. Eight (8) Business Hours Monitor and respond as necessary.

Severity Level 4

(Low)

How-to questions and Service issues with no Service degradation. One (1) Business Day Monitor and respond as necessary.

RFE Requests for enhancements to the Service. Two (2) Business Days N/A

5. Other Support and Training. Abnormal also offers various support and training resources such as documentation, FAQs and user guides available on the Abnormal Community.

6. Error Response. Abnormal Support will investigate Errors and assign the applicable Severity Level listed in Table 1. If Abnormal's Severity Level designation is different from that assigned by Customer, Abnormal will promptly notify Customer of such designation. If Customer notifies Abnormal of a reasonable basis for disagreeing with Abnormal's designated Severity Level, the parties each will make a good faith effort to discuss, escalate internally, and mutually agree on the appropriate Severity Level. Abnormal shall use commercially reasonable efforts to meet the Initial Response Time Target for the applicable Severity Level, as measured during the Support hours set forth in Table 2 below (with the total Business Hours in an in-region support day each a "Business Day").

Table 2: Support Hours

RegionAmericas EMEA Asia Pacific

Severity 1 24 x 7 x 365 24 x 7 x 365 24 x 7 x 365

Severity 2-4 6AM-6PM PT Mon-Fri8AM-5PM GMT Mon-Fri 8AM-5PM AEDT Mon-Fri

Exclusions U.S. Federal HolidaysUnited Kingdom Public and Bank Holidays Australian National and Public Holidays

II. Service Level Agreement

The Monthly Availability Percentage for the Service is ninety-nine and nine-tenths percent (99.9%) ("Service Level"). If the Service does not meet the Service Level in a given month ("Service Level Failure"), then as Customer's sole and exclusive remedy, Customer shall be eligible to receive the applicable number of Service level credits set forth in Table 3 below ("Service Level Credits"), credited towards extending Customer's Subscription Term at no charge, provided that Customer requests Service Level Credits within thirty (30) days from the time Customer becomes eligible to receive Service Level Credits under this Policy by filing a Support Case. Failure to comply with this notification requirement will forfeit Customer's right to receive Service Level Credits. The aggregate maximum amount of Service Level Credits for a Service Level Failure will not exceed

15 days per month. Service Level Credits may not be exchanged for, or converted to, monetary amounts. Customer may request the Service Level attainment for the previous month by filing a Support Case.

Table 3: Service Level Credits

Monthly Availability Percentage

Service Level Credit

< 99.9% - ≥ 98.0% 3 Days

< 98.0% - ≥ 95.0% 7 Days

< 95.0% 15 Days

Policy Exclusions

Abnormal will have no liability for any failure to meet the Service Level to the extent arising from: (a) Planned Maintenance or Emergency Maintenance; (b) third-party platforms and networks, Customer or User application, equipment, software or other third-party technology; (c) Customer or its User's use of the Service in violation of the Agreement or not in accordance with the Documentation; (d) force majeure events — i.e., any cause beyond such party's reasonable control, including but not limited to acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, public health emergencies (including pandemics and epidemics), acts or orders of government, acts of terrorism, or war; or (e) any access to the Service (or Service features) on a free, trial, beta or early access basis, or due to suspension, limitation, and/or termination of Customer's access or use of the Service in accordance with its Agreement.

Definitions:

"Calendar Minutes" is defined as the total number of minutes in a given calendar month.

"Emergency Maintenance" means circumstances where maintenance is necessary to prevent imminent harm to the Service, including critical security patching.

"Monthly Availability Percentage" is defined as the difference between Calendar Minutes and the Unavailable Minutes, divided by Calendar Minutes, and multiplied by one hundred (100).

"Planned Maintenance" means routine maintenance periods that continue for no more than four hours in any one instance, so long as Abnormal provides at least 48 hours prior notice (including by email) to Customer.

"Unavailable" means if Customer is unable to access the Service by means of a web browser and/or API as a result of failure(s) in the Service, as confirmed by Abnormal.

"Unavailable Minutes" is defined as the total accumulated minutes when the Service is Unavailable.

Any applicable Addtional Terms and Conditons Goes Here

ABNORMAL SECURITY CORPORATION INFORMATION SECURITY POLICY

This Information Security Policy ("Policy") is incorporated into the subscription agreement under which Abnormal Security Corporation ("Abnormal", "we", or "us") provides its Service ("Agreement") to the Party listed as Customer on the Agreement ("Customer") and describes Abnormal's Information Security Program ("Security Program") which Abnormal has implemented and will maintain in accordance with this Policy.

Abnormal may update this Policy from time to time, provided that any such update does not: (i) modify any provision of the Agreement except for this Policy; or (ii) materially diminish the overall security protections described herein during the Subscription Term. Any such updates will be posted to https://legal.abnormalsecurity.com/. Capitalized terms not otherwise defined in this Policy shall have the meanings given to them in the Agreement. Any ambiguity, conflict or inconsistency between this Policy, the Agreement, the DPA, or other document comprising this Agreement shall be resolved according to the following order of precedence: (1) DPA; (2) this Policy; (3) the Agreement; and (4) other supplementary documents incorporated into the Agreement.

Minimum Security Standards. The Security Program will use industry-standard controls designed to protect the confidentiality, integrity, and availability of Customer Data against anticipated or actual threats or hazards; accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or damage. The Security Program will use administrative, technical, and physical safeguards appropriate to: (a) the size, scope, and type of Abnormal's business; (b) the type of information that Abnormal processes on behalf of Customer (where such information is provided to Abnormal in accordance with the Agreement); and (c) the corresponding need for security and confidentiality of such information.

For more details on Abnormal's Security Program, please see the Security Hub at security.abnormalsecurity.com ("Security Hub").

Service Infrastructure. The Service and Customer Data are hosted on infrastructure using industry-leading cloud hosting providers. No Customer Data is stored or processed in Abnormal office facilities.

Elements of the Security Program.

1. Policies and Procedures. Abnormal has implemented and will maintain security, privacy, confidentiality, availability, and code of conduct policies and procedures designed to ensure that the Service and Abnormal's employees and contractors ("Personnel") process Customer Data in accordance with this Policy and the Agreement. Abnormal has implemented and will enforce disciplinary measures against Personnel for failure to abide by the aforementioned policies and procedures.

2. Logical Access Controls. Abnormal will take reasonable measures that are designed to ensure appropriate user authentication for Personnel with access to Customer Data, including without limitation, by assigning each Personnel unique authentication credentials for accessing any system on which Customer Data is processed and prohibiting Personnel from sharing their authentication credentials. Abnormal will restrict access to Customer Data solely to those Personnel who need access to Customer Data to perform Abnormal's obligations under the Agreement.

Further, Abnormal will take reasonable measures to implement and maintain logging and monitoring technologies designed to help detect and prevent unauthorized access to its networks, servers, and applications, including but not limited to those that process Customer Data. Abnormal will conduct periodic reviews of systems that process Customer Data to verify the identities of individuals who access and have privileged access to systems to help detect and prevent unauthorized access to its network, servers, and applications and verify that all changes to its authentication systems were authorized and correct. Abnormal has implemented and will maintain procedures and policies that are designed to ensure that, upon termination of any Personnel the terminated user access to any Customer Data on Abnormal systems will be promptly revoked, and in all cases, revocation will occur no later than twenty-four (24) hours following such termination.

3. Intrusion Prevention. Abnormal utilizes reasonable measures designed to ensure that its infrastructure protections are consistent with industry standards in preventing unauthorized access to Abnormal networks, servers, and applications. Such measures include but are not limited to the implementation of intrusion prevention technologies, anti-malware services, and firewall rules.

4. Physical Access. Abnormal limits physical access to its office facilities using physical controls (e.g., coded badge access). Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that access to their data centers and other areas where Customer Data is stored is limited to authorized individuals. Cloud hosting provider data centers and Abnormal office facilities leverage camera or video surveillance systems at critical internal and external entry points and are monitored by security Personnel.

5. Environmental Protection. Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that cloud hosting provider data centers implement and maintain appropriate and reasonable environmental controls for its data centers and other areas where Customer Data is stored, such as air temperature and humidity controls, and protections against power failures.

6. Backup, Disaster Recovery, and Business Continuity. Abnormal will: (a) back up its production file systems and databases according to a defined schedule and conduct regular testing of

backups; and (b) maintain a disaster recovery plan for the production data center and maintain business continuity plans designed to manage and minimize the effects of disaster events or unplanned operational disruptions with a stated goal of resuming routine service within forty-eight (48) hours; and (c) conduct regular testing of the effectiveness of such plans.

7. Security Incident Response. For purposes of this Policy, any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data is a "Security Incident". Abnormal will: (a) take reasonable measures to implement and maintain logging and monitoring technologies designed to identify, alert, and analyze security events; and (b) maintain plans and procedures to be followed in the event of an actual or suspected Security Incident ("Incident Response Plans"). The Incident Response Plans require Abnormal to undertake a root cause analysis of any actual or suspected Security Incident and to document remediation measures.

8. Security Incident Notification. Abnormal will implement and follow procedures that are designed to detect and respond to Security Incidents and will notify Customer of any Security Incident affecting its Customer Data within forty-eight (48) hours of Abnormal becoming aware of the Security Incident, regardless of whether the Security Incident triggers any applicable breach notification law. Such notification will be executed using the contact information provided by Customer under the Records and Validation section of the Agreement.

Notice to a Customer will include: (a) a description of the nature of the Security Incident, including the categories and approximate number of Customer's data subjects and personal data records concerned; (b) the name of Abnormal's contact where more information can be obtained; (c) a description of the likely consequences of the Security Incident; (d) a description of the measures taken or proposed to address or mitigate the adverse effects of the Security Incident, to the extent within Abnormal's reasonable control.

9. Storage and Transmission Security. Abnormal will logically segregate Customer Data from all other Abnormal or third-party data. Abnormal will: (a) securely store Customer Data; (b) encrypt Customer Data during transmission using, at a minimum, Transport Layer Security (TLS) protocol version 1.2 or above; and (c) encrypt Customer Data at rest using, at a minimum, the Advanced Encryption Standard (AES) 256-bit encryption protocol. Abnormal will establish encryption key management processes that are designed to ensure the secure generation, storage, distribution, and destruction of encryption keys. Abnormal will not store Customer Data on any removable storage devices or other similar portable electronic media.

10. Data Retention and Secure Disposal. Abnormal will retain and securely dispose of Customer Data in accordance with the Agreement. During the Subscription Term, Customer may through the features of the Service access, return to itself or delete Customer Data. Following termination or expiration of the Agreement, Abnormal will delete all Customer Data from Abnormal's systems.

Deletion will be in accordance with industry-standard secure deletion practices. Abnormal will issue a certificate of deletion upon Customer's written request. Notwithstanding the foregoing, Abnormal may retain Customer Data: (a) as required by applicable laws, or (b) in accordance with its standard backup or record retention policies, as governed by the Agreement.

11. Risk Identification and Assessment. Abnormal will implement and maintain a risk assessment program to help identify foreseeable internal and external risks to Abnormal's information resources and to Customer Data, and determine if existing controls, policies, and procedures are adequate.

12. Subprocessors. Abnormal will authorize third-party service providers to access or process Customer Data ("Subprocessors") only in accordance with the requirements and procedures specified in the Agreement, and specifically in the DPA. Prior to authorizing Subprocessors, Abnormal security Personnel will conduct a risk assessment of each Subprocessor to seek assurances of its data security practices (e.g., in the form of an independent third-party audit report such as the SOC 2 Type 2, ISO 27001, or a vendor security and risk evaluation). Abnormal enters into written agreements with its Subprocessors with security and data processing obligations substantially the same as those contained in this Policy.

13. Change and Configuration Management. Abnormal has implemented and will maintain processes for managing changes and updates to production systems, applications, and databases, including without limitation, processes for documenting, testing, and approval of changes into production, security patching, and authentication.

14. Release Management. Abnormal follows a continuous release process versus a standard release schedule and does not require a maintenance downtime window for the Service when pushing a new release. No Customer interaction is required to upgrade to the new version; the release is automatically applied to all Customers. Releases follow Abnormal's change management procedures that are designed to ensure that releases are tested and approved prior to push to production. Abnormal communicates release information using the notification functionality within the Service.

15. Training. Abnormal will undertake the following measures that are designed to ensure that Personnel who will have access to Customer Data are appropriately qualified and trained to handle Customer Data:

15.1. Information Security and Privacy Awareness Training. Upon hire and at minimum annually thereafter, Abnormal will require security and privacy awareness training to all Personnel who will process or have access to Customer Data. Abnormal security and privacy awareness training is designed to meet industry standards and will include, at a minimum, education on safeguarding

against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, and social engineering mechanisms.

15.2. Secure Code Training. Abnormal will require annual training on secure coding principles and their application at minimum annually to all Personnel who develop or handle any Abnormal source code. Abnormal secure code training will cover topics such as: (a) the Open Web Application Security Project list of the 10 most critical security risks to web-based applications (OWASP Top 10); and (b) appropriate techniques for the remediation of the listed security vulnerabilities.

16. Background Checks. Abnormal Personnel will undergo a civil and criminal background check, to the extent permitted by applicable law.

17. Audit and Assessments. Abnormal has implemented and will maintain a Compliance Audit Program including assessments performed by an independent third-party ("Auditor") and defined Customer audit rights in accordance with the Agreement.

17.1 Independent Security Audit. Abnormal will engage an Auditor to certify compliance with the ISO 27001 standard, and conduct a SOC 2 Type 2 audit with a scoped audit period of a maximum 12 months to demonstrate its compliance with the security requirements of the Security Program. Abnormal's SOC 2 Type 2 audit covers the Trust Services Criteria of Security, Availability, Confidentiality, and Privacy. Abnormal will make available to Customer publicly available certificates and summary copies of its SOC 2 Type 2 audit report (each, an "Audit Report") on the Security Hub.

17.2 Customer Audits. Abnormal will make available the information necessary to demonstrate its compliance with the Security Program to support Customer in obtaining the information necessary to complete Customer's audits, reviews, risk assessments, and security-related questions of Abnormal as Customer's vendor. Please see the Security Hub for this information. For further details on Customer audit rights, please see your Data Processing Addendum (DPA).

17.3 Penetration Tests. At least once per twelve (12) month period, Abnormal will undertake a network penetration test by an independent third-party. Abnormal will make available to Customer an executive summary section of the penetration test report that pertains to the systems and operations that process, store, or transmit Customer Data. Abnormal will remediate all vulnerabilities that the penetration test identifies in accordance with the following remediation timelines:

Level	Timeline
Critical	15 days

High	30 days
Medium	60 days
Low	Reasonable timeframe based on nature and probability of exploitation

All information exchanged between the Parties in the course of the activities described in all Sections above are deemed to be Abnormal Confidential Information.

Abnormal Security Acceptable Use Policy

This Acceptable Use Policy (“AUP”) describes the prohibited uses of the Software as a Service offering (the "Service") provided by Abnormal Security Corporation (“Abnormal"). This AUP is in addition to any other terms and conditions under which Abnormal provides the Service to you. In addition to any other remedies available to Abnormal, if Abnormal determines in its sole discretion that you violate the AUP, we may suspend, limit, or terminate your use of the Service without prior notice or liability. This right applies, even if the breach is unintentional or unauthorized, if we believe that any such suspension, limitation, or termination is necessary to ensure compliance with laws, or to protect the rights, safety, privacy, security, or property (including the Service) of Abnormal or others.

Abnormal may modify this AUP at any time by posting an updated version of this document. Such updates will be effective upon posting. We therefore recommend that you visit the Abnormal website regularly to ensure that your activities conform to the most recent version. Your continued access to and use of the Service constitutes your agreement to be bound by such updates.

The prohibited uses listed below are not exhaustive. Prohibited uses and activities by you, the customer, your users or any third party include, without limitation:

- Violating any applicable laws or regulations (including without limitation data, privacy, and export control laws) or use the Service in a manner that gives rise to civil or criminal liability;

- Intentionally distributing malicious code, viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive manner;

- Infringing or misappropriating Abnormal’s or any third party’s intellectual property, proprietary or privacy rights;

- Reverse engineering, decompiling, or disassembling the Service or any software used in the provision of the Service;

- Interrupting, or attempting to interrupt, violate, obtain unauthorized access to, disrupt, damage, overburden, breach, or compromise the operation or security of the Service or any networks or systems;

- Using the Service for any reason other than as intended by the parties.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L5 – Service Category 5: Email Security

Respondent Name: R2 Unified Technologies

Solution Name: Cisco Secure Email

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Email Security Solutions must protect against email-based threats such as phishing, malware, ransomware, and email compromises. The Solution should analyze both inbound and outbound email communications in real-time, using advanced detection techniques to filter malicious content without disrupting legitimate business correspondence.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email provides advanced protection against email-based threats such as phishing, malware, ransomware, and business email compromise (BEC) while ensuring legitimate business communication flows smoothly. Its multi-layered defenses and real-time analysis secure both inbound and outbound emails, preventing threats and safeguarding sensitive data.

Inbound and Outbound Protection: Cisco Secure Email scans inbound traffic to block malicious content and outgoing messages to prevent data exposure. This approach ensures compliance with security policies and regulatory standards.

Advanced Detection Techniques: Leveraging machine learning, sandboxing, and reputation filtering, it identifies phishing and spear-phishing attempts, detects unusual patterns, and analyzes potentially harmful attachments or URLs in secure environments.

Phishing and Impersonation Defense: Sender authentication (DMARC, DKIM, SPF) and domain reputation checks protect against phishing and impersonation. Display name spoofing and domain similarity attacks are detected, shielding users from social engineering.

URL and Attachment Protection: Links are rewritten and scanned in real time, blocking delayed malicious URLs. Attachments are analyzed using sandboxing, detecting malware before reaching users.

Ransomware and Advanced Malware Defense: Powered by Cisco Talos threat intelligence, Secure Email blocks ransomware and evolving malware variants with continuous updates and robust defenses.

BEC and Data Loss Prevention (DLP): Secure Email detects BEC patterns, such as financial fraud attempts, and DLP scans outgoing emails to prevent unauthorized sharing of sensitive data, maintaining compliance.

Real-Time Threat Intelligence: Cisco Talos provides ongoing updates on phishing campaigns, malware, and attack vectors, enhancing detection and keeping defenses current against emerging threats.

Quarantine and Remediation: Malicious content is quarantined, with options for automated or manual remediation. Administrators can review quarantined items, ensuring threats are contained and legitimate emails are released.

User Awareness: Features like warning banners on suspicious emails educate users about potential threats, promoting secure email practices and reducing risks.

In summary, Cisco Secure Email combines real-time threat analysis, advanced detection, and Talos threat intelligence to defend against diverse email-based threats. By protecting inbound and

outbound traffic and integrating with Cisco's security ecosystem, it delivers robust protection with minimal disruption to business communications.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Content Filtering – The Solution should break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, a nationally recognized standard, or company policy.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email performs content filtering by breaking down files into discrete components, analyzing them in real-time, and reconstructing a clean version of the email. It removes non-compliant elements, such as malicious macros or scripts, ensuring conformity with file type standards and company policies. This approach protects users by delivering only safe, policy-compliant content, preventing harmful elements from reaching inboxes.

Prompt 3: Phishing Detection – Solution should analyze the email's context, structure, and metadata (e.g., header information) to detect phishing attempts, which may include spear-phishing and targeted attacks.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email analyzes email context, structure, and metadata, including header information, to detect phishing attempts. It identifies indicators of spear-phishing and targeted attacks by examining patterns, sender reputation, and anomalies in email composition. Advanced algorithms and Talos threat intelligence enhance its ability to detect and block phishing, protecting users from deceptive and targeted threats.

Prompt 4: Sandboxing Technology – Solution should have the capability to safely execute email attachments and embedded links in an isolated environment to determine if they are malicious before delivery to the recipient.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email includes sandboxing technology to safely execute email attachments and analyze embedded links in an isolated environment. This process identifies malicious behavior before email delivery, ensuring that harmful content is blocked from reaching recipients. By using real-time analysis, Secure Email protects users from advanced threats embedded in attachments and links, enhancing security against sophisticated email attacks.

Prompt 5: Advanced Anti Spoofing Protections – Solution should include enforcement of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols to prevent sender impersonation.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email enforces SPF, DKIM, and DMARC protocols to provide advanced anti-spoofing protections. By validating these authentication mechanisms, Secure Email identifies and blocks impersonation attempts, ensuring that only legitimate senders are allowed. This enforcement prevents common spoofing attacks and enhances security by verifying sender authenticity, protecting users from phishing and email-based impersonation threats.

Prompt 6: Email Encryption – Solution should include encryption for sensitive communications, ensuring enforcement that messages are encrypted both in transit and at rest.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email includes encryption capabilities to protect sensitive communications, enforcing encryption both in transit and at rest. This ensures that sensitive data remains secure from unauthorized access during transmission and while stored. Cisco Secure Email offers flexible encryption policies, enabling automatic encryption based on content, recipient, or policy requirements, thereby safeguarding sensitive information.

Prompt 7: End-User Awareness Features – Solution should include automatic banners or warnings added to suspicious emails, helping users recognize potential threats.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email includes end-user awareness features, such as automatic banners or warnings on suspicious emails. These alerts help users recognize potential threats by flagging emails from unknown or potentially risky sources. This feature educates users to be cautious with suspicious emails, adding an extra layer of defense against phishing and other social engineering attacks.

Prompt 8: Quarantine and Remediation Tools – Solution should provide quarantine and remediation tools for administrators, allowing them to review flagged messages, release legitimate emails mistakenly identified as threats, and block harmful content.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Email offers robust quarantine and remediation tools for administrators. These tools allow admins to review flagged messages, release legitimate emails mistakenly marked as threats, and block malicious content. This capability ensures accurate threat management, giving administrators control to prevent harmful emails from reaching users while minimizing disruption to legitimate communications.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: R2 Unified Technologies

Solution Name: Arctic Wolf Managed Detection and Response

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: The Security Operations Platform (SOP) must integrate multiple security tools and technologies into a single unified platform, providing comprehensive visibility into an organization's IT environment. The Solution should allow security teams to detect, investigate, and respond to threats in real-time, correlating data from across the infrastructure to provide a holistic view of security incidents.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Arctic Wolf is a SaaS based solution. The Arctic Wolf Security Operations Cloud platform is hosted entirely in AWS and as such does not require any design, implementation, or ongoing maintenance by the customer or a SIEM to host. The performance, availability and capacity management of the Arctic Wolf Cloud platform is solely the responsibility of Arctic Wolf and is included as part of solution costs. The platform and associated detection logic is continuously being updated (as new threats and indications of compromise are discovered).

The Arctic Wolf Security Operations Cloud is built on an open XDR architecture, solving the biggest challenge organizations face in cybersecurity: collecting and storing security data across attack surfaces in real time; enriching, analyzing, and investigating this data; and using both machine automation and humans to respond decisively to threats and attacks.

The platform processes over 700 billion security observations per day. The cloud native scaling of our platform ensures all events are processed in near real time regardless of ingestion rate. This means your security observations are analyzed without delay.

The service is security tooling vendor agnostic, it can accept any security telemetry into our platform but have integration with many leading security tools across endpoints, network, cloud, and identity.

Arctic Wolf can ingest any security syslog from your environment via Arctic Wolf network sensor(s). The sensors will securely transport these to our Security Operations Cloud platform.

Arctic Wolf deploys an architecture supporting broad visibility across many different elements of the State of Florida's network. Since licensing is not on an ingest or volume basis, customers are able to provide abundant telemetry to monitor their environment.

Through real-time pipeline of ingest, parse, and analyze Arctic Wolf currently ingests over 700 billion observations daily, and after parsing, enriching, analyzing (including AI/ML) to get to around 90,000 high alerts/investigations humans review every day. Out of that around 6000 security incidents are escalated each day within the entire Arctic Wolf customer base (typically one or a few ticketed incidents per day per customer, with full guided remediation). This is a large part of removing alert fatigue within customers, by providing high fidelity detections that are timely and add value.

The customers will also have access to the Arctic Wolf customer portal to:

•Review and interact with incident tickets and associated Security Analysts

•Manage and review telemetry sources

•Explore analyzed data and search raw logs, review login events, and network flow data.

•Download scheduled standard and customized reports

•Contact their Concierge Security Team to discuss security questions, request customization, and reports.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Log Event Aggregation and Correlation – Solution should log event aggregation and correlation from various security devices (firewalls, IDS/IPS, endpoint detection tools, network devices, and cloud services) to identify patterns and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Broad visibility: We leverage customers existing security tools and infrastructure. We have integrations with many popular security tools and also integrate with productivity tools like O365. This gives us maximum visibility and ensures the fastest time to detection and remediation. Log source categories include Endpoint (EDR & Arctic Wolf Agent), Network (i.e. FW logs, AW network sensor), Cloud (i.e. AWS, Azure, O365), and Identity (I.e. OKTA, EntraID).

Prompt 3: Automated Incident Response Workflows – Solution should allow security operations teams to optionally automate common tasks such as blocking IP addresses, isolating infected devices, or generating alerts for further investigation

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Arctic Wolf Active Response has a number of SOAR capabilities that can be executed by Arctic Wolf Triage personnel as part of the proposed MDR service. Endpoint Active Response includes host containment (through supported EDR vendors or the Arctic Wolf Agent). Identity Active Response includes Disable and Enable users, close user connections. Network block can block internet bound traffic if a network sensor is deployed at the internet egress point.

Prompt 4: Real-Time Threat Detection – Solution should be powered by machine learning models and behavioral analytics, capable of identifying zero-day attacks, insider threats, and anomalous activities that deviate from the organization's baseline.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Ingested data is parsed, enriched with metadata and attribution, and analyzed using multiple techniques including AI/ML, UEBA, custom and static rulesets. Any security event of interest elevated from the platform is always reviewed by a Triage Security Analyst/Engineer prior to customer escalation. Threat intelligence consists of a combination of Arctic Wolf Labs, intelligence from Arctic Wolf Incident Response, plus commercial threat intelligence feeds.

Prompt 5: Customizable Dashboards – Solution should have dashboards displaying real-time security metrics, providing visualizations of key performance indicators (KPIs) such as the number of incidents, time-to-respond, or threat severity.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The Arctic Wolf customer portal allows for the creation of custom Dashboards where customers can build widgets with queries to display the desired parameters in the dashboard(s).

Prompt 6: Incident Management Capabilities – Solution should provide detailed incident tracking, ticketing integration, and root cause analysis, ensuring that all security events are fully documented and addressed.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

If through the forensics process it is deemed a security incident needs to be raised to the customer, the CSE will create a ticket based on the agreed upon escalation chain. Ticketing integration is supported for ServiceNow and ConnectWise. Arctic Wolf tickets include remediation steps and evidence navigator. RCA reports are available upon request. All tickets including attachments and documentation remain available to the customer throughout the contract lifetime.

Prompt 7: Integration with Threat Intelligence Platforms (TIPs)– Solution should enrich security alerts with contextual information about current threat actors, malware campaigns, and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Customers are informed about current security exploits via Security Bulletins. An additional benefit of becoming an Arctic Wolf customer is that the customer would inherit 10 years' worth of real-customer threat intelligence as well as all live and historical Tactics, Techniques and Procedures (TTPs) observed from threat actors & groups as soon as you go live into production. The Arctic Wolf platform is continuously updated with new detection rules.

Prompt 8: Integration of CTI Data Feeds – Solution should Allow for real-time enrichment of alerts, correlating incidents with known global threat actor campaigns, IoCs, and TTPs (Tactics, Techniques, and Procedures), improving situational awareness and response times

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

As described, Arctic Wolf provides a service that delivers security outcomes. The Arctic Wolf platform is continually updated with the latest detection logic based on the various sources of threat intelligence we ingest (both in-house and from commercial threat feeds). Every Arctic Wolf customer automatically benefits from this threat intelligence and any new detection will be immidiately available to all Arctic Wolf customers.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Arctic Wolf Managed Detection and Response Solution Terms (these terms can also be found at https://arcticwolf.com/terms/solutions-terms/managed-detection-and-response/

(password: "mdr2024")

Last Updated Date: June 2024

This Managed Detection and Response – Solution Terms ("Solutions Terms") describes the Managed Detection and Response Solution (the "Solution"). The Solution, if purchased by Customer as evidenced by Customer's election on an Order Form, will be provided in accordance with the terms set forth herein and the Solutions Agreement (the "Solutions Agreement") made by and between Customer and Arctic Wolf Networks, Inc. ("Arctic Wolf"). Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Solutions Agreement.

Solution. The Solution may be licensed separately or as part of a Security Operations Bundle as more fully described at https://arcticwolf.com/terms/bundles-tiers/ (each a "Bundle") and includes the following Components:

Component

Software The object form of any software, including any operating system software included in the Equipment, and add-ons offering enhanced features and functionality made generally available to Arctic Wolf customers from time-to-time

Equipment Virtual appliances or physical sensors

Services Support, onboarding services, and services provided by Security Services, all as described herein, and Cyber Resilience Assessment ("CRA")

Platform One (1) vSensor 100 series

Unlimited data ingestion

Access to the Customer Portal

Use of the Arctic Wolf Agent

ITSM Ticketing Integrations (if elected by Customer)

90-day Log Retention (unless another retention period is purchased by Customer and set forth on an Order Form)

The Solution is delivered by the Security Services team which is comprised of two (2) teams: (1) the Concierge SecurityTM Team ("CST"), and (2) the Security Operations Center ("SOC").

Specific features and functionality provided as part of the Solution include:

• collection of Solutions Data and Points of Contact Information, including Customer's system logs, from Customer's systems using Equipment,

• analysis by Arctic Wolf Security Services of both Equipment and log data through the correlation of Solutions Data with threat and vulnerability information,

• scanning of Customer's internal and external systems,

• escalation of Security Incidents (as defined below) in need of attention by Customer as set forth herein,

• advisory recommendations intended to improve Customer's security robustness,

• calculation of Customer's Security Score, as more fully described below,

• Access to additional modules, if licensed by Customer as reflected on an Order Form (as more fully described below)1,

• Response Actions2 (as more fully described below),

• Cyber Resilience Assessment ("CRA") subject to the terms set forth at https://arcticwolf.com/terms/cyber-jumpstart-portal-subscription-agreement/, and

• regular summary Executive Dashboard reports, as described herein and the Documentation.

NOTE: The performance of the Solution, including specifically, notification of Emergencies or Security Incidents, as defined below, will not commence until after initial deployment is complete. The performance of (i) remediation services for Security Incidents (as defined below), (ii) the re-imaging of Customer's systems, or (iii) change of policy settings is outside the scope of the Solution.

Data Transfer. Any Equipment provided by Arctic Wolf to Customer is physically or virtually deployed to monitor Customer's system traffic. Such system traffic is augmented with additional sources of log data, as required, to deliver the Solution. Except as otherwise set forth in the Solutions Agreement, all such system traffic information is deemed Solutions Data. Essential log sources will be determined by Customer and Arctic Wolf during the onboarding process following the Order Form Effective Date.

Any Solutions Data and Points of Contact Information will be securely transmitted to Arctic Wolf in accordance with the Agreement. The Solution operates redundantly with Customer's High Availability (HA) specifications to minimize potential service interruptions. Hosting providers used by Arctic Wolf to deliver the Solution may experience service interruptions and service outages outside the control of Arctic Wolf. If such a hosting provider issues an outage notice that could materially impact delivery of the Solutions, Arctic Wolf will use commercially reasonable efforts to promptly notify Customer about the outage and communicate the planned recovery time provided by the hosting provider.

Solutions Data and Points of Contact Information may include personal or confidential information. Customer will provide any such personal or confidential information in accordance with the terms of the Solutions Agreement.

Data Retention. Arctic Wolf will store Solutions Data and Points of Contact Information for the Data Retention period specified in Customer's then-current Order Form. Solutions Data and Points of Contact Information may be returned to Customer in accordance with the terms of the Solutions Agreement.

Data Storage. Arctic Wolf will store raw Solutions Data and Points of Contact Information in the platform location set forth on an Order Form.

Updates & Upgrades. Automated maintenance and update cycles to the Equipment will be performed remotely by Arctic Wolf Security Services. Arctic Wolf will provide any services related to the replacement or upgrades of the Equipment. Any costs related to such Equipment replacement or upgrades will be in accordance with the Solutions Agreement.

Security Incidents. The CST supporting Customer is available 8:00 am to 5:00 pm (based on the time zone within which the CST is located), Monday through Friday (excluding holidays) and will provide Concierge Security™ Tier support in accordance with the Concierge Security™ Tier selected by Customer, as applicable. The SOC is available 24 hours a day, 7 days a week, including holidays. Customer may schedule specific activities with their CST, in accordance with Customer's Concierge Security™ Tier, as applicable, by contacting the Arctic Wolf SOC at security@arcticwolf.com. Arctic Wolf Security Services will acknowledge any schedule request submitted by Customer to security@arcticwolf.com within one (1) hour of receipt of such request. Arctic Wolf Security Services will provide an estimate of response time determined by scope, size, and urgency.

Arctic Wolf Security Services will notify and escalate to Customer any Security Incidents, the definition of which will be agreed upon by Customer and its CST during the Subscription Term after transition from the deployment team, discovered by Arctic Wolf within two (2) hours of Arctic Wolf's discovery of such Security Incident. Arctic Wolf standard Security Incident notification process is through a ticket to the Customer; however, Arctic Wolf and Customer may agree to alternate notification processes. Security Incident notifications will include a description of the Security Incident, the level of exposure, and a suggested remediation strategy. Customer is responsible for implementing, in its sole discretion, any remediation strategies identified by Arctic Wolf. Customer may request validation by Arctic Wolf that any such implemented remediation strategies are working as expected.

Emergencies. Following transition from the deployment team to the CST, Customer and the CST will agree on and document which Security Incidents will be defined as an "Emergency". Emergencies will typically include the discovery of ransomware and other alerts that could cause degradation/outage to Customer's infrastructure security. Arctic Wolf will escalate Emergencies to Customer within thirty (30) minutes of Arctic Wolf's discovery of the Emergency.

Any Emergency identified by Customer can be escalated to Arctic Wolf's Security Services by calling: 1-888-272-8429, option 2 or by calling the toll-free number based on the location from which you are calling found at https://arcticwolf.com/toll-free/. Customer must describe the Emergency in the initial call and Arctic Wolf will respond within 5 minutes. In addition, with respect to any urgent inquiries, Customer may contact Arctic Wolf's Security Services by calling: 1-888-

272-8429, option 2 or using the applicable toll-free number for the location from which Customer is located as set forth at https://arcticwolf.com/toll-free/.

Ticketing Integration (included in the Platform component of the Solutions). At Customer's election and based on configurations and permissions collected from Customer, Arctic Wolf may employ an integration to transfer data into and out of Customer's third-party ticketing system, provided Arctic Wolf supports integrations to such systems.

Scans. On a monthly basis, Arctic Wolf will use the Solution to conduct external vulnerability assessment scans of Customer's environment. As part of these scans, vulnerability and exploit information will be normalized and correlated with other data sources to determine Customer's Security Score and prioritization of any identified remediation strategies. Arctic Wolf will deliver to Customer a summary security report that includes Security Incident and Emergency notification activities on a monthly and quarterly basis.

Coverage Score (fka Configuration Score or Security Score). Customer's Coverage Score is provided as part of the Solution for illustrative and informational purposes only and may be used by Customer for internal benchmarking. The Coverage Score is based on certain information related to the results of the Solution within Customer's environment and is compiled using the Solutions Data made available to Arctic Wolf in conjunction with its delivery of the Solution. Customer's Coverage Score will be communicated in Customer's summary reports in addition to being available on Customer's online Executive Dashboard. Customers may elect to compare their Coverage Score against industry averages from organizations in the same industry vertical to assess how Customer is performing against industry norms.

Response Actions. Arctic Wolf may, if agreed with Customer, using commercially reasonable efforts, perform response actions, including application/removal of host containment, enable/disable user accounts, block URLs, modify deny lists and iprules, retrieve files, kill processes, and run files or scripts, as described below (collectively, "Response Actions"), provided that Customer has deployed the Arctic Wolf Agent, such other agreed upon third party agents, and/or configured the appropriate integrations. In the event Customer has deployed multiple agents, including the Arctic Wolf Agent, within its environment, Arctic Wolf will attempt to contain first using the Arctic Wolf Agent. Based on (i) information provided by Customer to its CST following initial deployment, (ii) a mutually agreed upon response and escalation process set forth in Customer's onboarding document, as updated upon agreement by Customer and its CST during the Subscription Term, and (iii) Arctic Wolf is provided appropriate access to applicable third party security applications, if any, within Customer's environment, the Security Services team may remotely isolate a Customer endpoint device(s), network appliance, or user account that shows evidence of compromise or other suspicious activity. When the Security Services team identifies certain indicators of attack on an endpoint, network device, or user account, the Response Action will be initiated systematically, in accordance with the agreed upon response and escalation process, and subject to the requirements set forth herein, to rapidly quarantine the suspected compromised system or account.

The indicators of attack that may drive Response Actions include those relating to ransomware (and other types of advanced malware), malicious command-and-control (C2) activity, or active data exfiltration attempts.

The endpoints, network, or user accounts participating in the Response Actions will receive a notification and the Response Actions will be detailed in an incident ticket. If using the Arctic Wolf

Agent, the Customer Portal will display the Customer endpoints that are currently in a contained state. Security Services team is available to Customer to answer questions or provide detailed information on any endpoints, network, and/or user accounts participating in the Response Action.

Pre-requisites for Response Actions –

Customer must:

• Complete a checklist in partnership with its CST, which will include further definition, including but not limited to the scenarios where Arctic Wolf will and will not perform Response Actions including specific information regarding which endpoints/servers, network appliances, and/or user accounts where Response Actions will and will not be performed, the times of day for Response Actions to occur, notification and escalation preferences related to Response Actions (If parties have not defined the Response Actions pertaining to Customer endpoints, network, and/or user accounts, Arctic Wolf will take Response Actions in accordance with Arctic Wolf's standard response and containment policy);

• Provide Arctic Wolf with technical permissions to allow Arctic Wolf to perform Response Actions within Customer's environment (Customer understands that should Arctic Wolf have invalid access or is blocked from initiating Response Actions, Arctic Wolf will be unable to provide the agreed upon Response Actions);

• Implement appropriate internal procedures and oversight to the extent Customer utilizes the configuration of workflows and processes, including but not limited to Response Actions and other similar functionalities; and

• Enable software or services, in Customer's discretion, to permit necessary visibility into Customer's environment to perform Response Actions.

Active Directory Deception. If licensed and implemented by Customer either as a standalone or bundled feature within the Solution, Customer may deploy Active Directory Deception ("AD Deception"). With AD Deception, Customer creates, configures, and maintains Active Directory decoy account(s) intended to act as a deception trap within Customer's network.

The Active Directory decoy account is not intended to participate in normal business activities and should not log-in to Customer's system. The Active Directory decoy account is intended to provide a high-fidelity mechanism for detecting abnormal activity yielding no false positives. If a decoy account is deployed by Customer, Customer is responsible for creating, configuring, and maintaining the decoy account. The naming of the decoy account should follow Customer's account naming conventions. Arctic Wolf will provide reasonable guidance and assistance to Customer in the configuration of such decoy accounts. Customer will provide Arctic Wolf details of the decoy account to Arctic Wolf for monitoring. Customer understands that any changes to the decoy account configurations may impact the security of Customer's environment.

Microsoft US Government Community and High US Government Community Environment Monitoring. In the event Arctic Wolf monitors applications for Customer within the Microsoft US

Government Community environment or US Government Community High environment (each a "GCC environment") as part of the delivery of the Solutions, Customer understands and agrees as follows:

1. Arctic Wolf is not FedRAMP compliant.

2. Only Arctic Wolf supported and integrated applications will be monitored in the GCC environment.

3. Solutions Data (i) may be accessed by Arctic Wolf, its Affiliates, and any third-party providers, from locations outside the United States, and (ii) may be accessed by persons who are not United States citizens;

4. Arctic Wolf does not require access to or delivery of Customer's Controlled Unclassified Information ("CUI") and in the event information classified as CUI is provided, Arctic Wolf may immediately cease ingestion of Customer Solutions Data without further liability to Customer;

5. Arctic Wolf will provide reasonable cooperation to Customer in the event of a data breach involving Solutions Data including, but not limited to assistance in responding to any government or regulatory inquiries;

6. Certain Microsoft log sources may be in beta and, consequently, Arctic Wolf makes no representations as to the delivery of the Solutions related to any such beta Microsoft log sources; and

7. Customer will immediately notify Arctic Wolf of non-consent or any change in consent and any monitoring of Customer's GCC environment will immediately cease without further liability to Arctic Wolf.

Additional Modules.

• Cloud Detection and Response ("CDR"). Customers may license CDR for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud IaaS and SaaS environments that Arctic Wolf may agree to monitor. Customer's election to license such CDR feature will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will provide detection and response for the respective IaaS and SaaS environments as described herein. Arctic Wolf is not responsible for any software and/or application changes made by the cloud IaaS and SaaS providers which affect or impair the CDR feature.

• Data Explorer. Customer may elect to license the Data Explorer feature. Should Customer subscribe to such feature, Data Explorer will be included on an Order Form. Data Explorer allows Customer to access historical data for quick, ad-hoc investigations and self-service reporting.

Customer may identify and remediate risk in Customer's environment and may take appropriate actions when needed depending on results. Data Explorer includes (i) access to the prior ten (10) days of event and analyzed data, and (ii) Log Search 3 which permits Customer to query its retained Solutions Data in 30-day increments.

• Data Explorer – Lite. Customers licensing MDR as part of a Bundle will receive Data Explorer – Lite which includes access to the prior three (3) days of event data.

For purposes of Data Explorer and Data Explorer-Lite, analyzed data includes parsed, normalized, and enriched data processed by the Arctic Wolf platform, however, not all logs ingested by Arctic Wolf will be parsed, normalized, or enriched. Event data is a collection of analyzed observations Arctic Wolf finds to be interesting from a security standpoint.

• Application and SaaS Integrations. Customers may license application and SaaS integrations as may be offered by Arctic Wolf. Customer's election to license such integration will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will provide detection and response for the respective integrated environments as described herein. Arctic Wolf is not responsible for any software and/or application changes made by the third-party application provider which affect or impair the integration with such third-party application.

1 Existing Arctic Wolf MDR Customers may be, subject to authorization by Arctic Wolf, eligible to license Log Search capabilities only. In such event, Log Search will be included on an Order Form.

2 Response Actions were formerly referred to as Host Containment Actions.

3 Legacy customers licensing Log Search are entitled to Log Search only.

Any applicable Addtional Terms and Conditons Goes Here

Arctic Wolf's terms and conditions for the provision of its solutions to its customers can be located at https://arcticwolf.com/terms/msa/. If down selected, we are confident we would be able to reach agreement with The State of Florida, Department of Management Services on acceptable terms to govern our relationship.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: R2 Unified Technologies

Solution Name: Cisco XDR

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: The Security Operations Platform (SOP) must integrate multiple security tools and technologies into a single unified platform, providing comprehensive visibility into an organization's IT environment. The Solution should allow security teams to detect, investigate, and respond to threats in real-time, correlating data from across the infrastructure to provide a holistic view of security incidents.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cisco XDR (Extended Detection and Response) is a unified Security Operations Platform (SOP) that integrates endpoint, network, email, cloud, and application data to provide complete visibility across the IT environment. It enables real-time threat detection, investigation, and response, streamlining security operations.

Unified Visibility Across Security Domains: Cisco XDR aggregates data from various security tools into a single interface, offering comprehensive visibility for tracking and monitoring incidents across the infrastructure.

Real-Time Threat Detection: Leveraging machine learning and behavioral analysis, Cisco XDR detects anomalies and correlates data from multiple sources, identifying sophisticated multi-vector attacks while reducing false positives.

Automated Incident Response: Cisco XDR automates workflows, gathering data and creating incident timelines. It prioritizes threats based on risk and impact, enabling faster and more efficient resolution.

Integrated Threat Intelligence: Powered by Cisco Talos, Cisco XDR incorporates global threat intelligence, ensuring the platform stays updated on emerging attack vectors and vulnerabilities.

Flexible Response Options: Automated actions include endpoint isolation, malicious IP blocking, and email quarantining. Teams can also execute manual responses for tailored threat mitigation.

Comprehensive Incident Analysis: With a holistic view of security events, Cisco XDR supports root cause analysis, helping teams trace attack origins and vulnerabilities to improve remediation efforts.

Scalable and Customizable: Designed for organizations of all sizes, Cisco XDR supports open APIs for third-party tool integration and workflow customization, ensuring adaptability to specific security needs.

Reduced Alert Fatigue: By correlating alerts and consolidating duplicates, Cisco XDR minimizes noise, enabling security teams to focus on high-priority threats.

In summary, Cisco XDR delivers centralized security visibility, real-time threat detection, integrated intelligence, and automated response capabilities, enhancing security posture and operational efficiency.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Log Event Aggregation and Correlation – Solution should log event aggregation and correlation from various security devices (firewalls, IDS/IPS, endpoint detection tools, network devices, and cloud services) to identify patterns and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco XDR aggregates and correlates log events from various security devices, including firewalls, IDS/IPS, endpoint detection tools, network devices, and cloud services. By unifying this data, it identifies patterns and Indicators of Compromise (IoCs), enabling faster detection of threats across the IT environment. This centralized approach provides comprehensive insight, allowing security teams to detect and respond to complex attacks with enhanced accuracy.

Prompt 3: Automated Incident Response Workflows – Solution should allow security operations teams to optionally automate common tasks such as blocking IP addresses, isolating infected devices, or generating alerts for further investigation

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco XDR enables automated incident response workflows, allowing security teams to streamline common tasks like blocking IP addresses, isolating infected devices, and generating alerts for further investigation. These automation options reduce response times and enhance efficiency, enabling rapid threat containment while allowing teams to focus on more complex security tasks.

Prompt 4: Real-Time Threat Detection – Solution should be powered by machine learning models and behavioral analytics, capable of identifying zero-day attacks, insider threats, and anomalous activities that deviate from the organization's baseline.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco XDR uses machine learning models and behavioral analytics for real-time threat detection, enabling it to identify zero-day attacks, insider threats, and anomalous activities that deviate from the organization's baseline. By analyzing behavior patterns and leveraging advanced algorithms, Cisco XDR detects and alerts on suspicious activities, enhancing the ability to identify and respond to sophisticated, previously unknown threats.

Prompt 5: Customizable Dashboards – Solution should have dashboards displaying real-time security metrics, providing visualizations of key performance indicators (KPIs) such as the number of incidents, time-to-respond, or threat severity.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco XDR offers customizable dashboards that display real-time security metrics, including visualizations of key performance indicators (KPIs) such as incident count, time-to-respond, and threat severity. These dashboards enable security teams to monitor and assess performance efficiently, providing actionable insights and improving incident response through clear, at-a-glance data visualization of critical security metrics.

Prompt 6: Incident Management Capabilities – Solution should provide detailed incident tracking, ticketing integration, and root cause analysis, ensuring that all security events are fully documented and addressed.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco XDR includes incident management capabilities with detailed incident tracking, ticketing integration, and root cause analysis. It documents and organizes security events, enabling comprehensive tracking from detection through resolution. Ticketing system integration streamlines workflows, while root cause analysis tools help identify attack origins, ensuring that all incidents are fully documented, addressed, and resolved effectively.

Prompt 7: Integration with Threat Intelligence Platforms (TIPs)– Solution should enrich security alerts with contextual information about current threat actors, malware campaigns, and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco XDR integrates with Threat Intelligence Platforms (TIPs), enriching security alerts with contextual information about threat actors, malware campaigns, and indicators of compromise (IoCs). This integration provides real-time, actionable insights, allowing security teams to understand the threat landscape, prioritize alerts, and make informed response decisions, enhancing overall threat detection and response capabilities.

Prompt 8: Integration of CTI Data Feeds – Solution should Allow for real-time enrichment of alerts, correlating incidents with known global threat actor campaigns, IoCs, and TTPs (Tactics, Techniques, and Procedures), improving situational awareness and response times

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco XDR integrates Cyber Threat Intelligence (CTI) data feeds for real-time alert enrichment, correlating incidents with global threat actor campaigns, IoCs, and TTPs (Tactics, Techniques, and Procedures). This enrichment enhances situational awareness and enables faster, more informed responses, as security teams gain immediate insights into threat context, helping to prioritize incidents and streamline response efforts.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L8 – Service Category 8: Identity and Access Management (IAM)

Respondent Name: R2 Unified Technologies

Solution Name: Cisco Identity Services Engine

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: IAM Solutions must provide centralized management for digital identities and control access to systems and data based on organizational policies. The Solution should manage the full lifecycle of user identities, from onboarding to de-provisioning, and enforce access control through role-based (RBAC) and attribute-based (ABAC) mechanisms.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Identity Services Engine (ISE) offers centralized management of digital identities and enforces access to systems and data by leveraging Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). This approach allows organizations to implement flexible, policy-based access management that aligns with security and operational requirements.

Role-Based Access Control (RBAC):

RBAC in Cisco ISE assigns users specific roles that define their access permissions, streamlining identity and access management across the network. For example, roles can be assigned by job functions, such as granting "Network Admin" roles more extensive permissions than "Helpdesk Technician" roles. This simplifies administration and minimizes risks by limiting each user to only the resources necessary for their role, ensuring consistent application of permissions aligned with organizational requirements.

Attribute-Based Access Control (ABAC):

ABAC enables Cisco ISE to evaluate access requests based on multiple attributes of users, devices, and environmental context. These attributes might include user identity, device type, location, or the time of day. For example, ABAC allows policies that grant access to sensitive applications only during business hours or from company-owned devices. ABAC provides more granular control over access, adjusting permissions dynamically based on changing contexts, which makes it ideal for environments requiring adaptive security postures.

Centralized Management and Policy Enforcement:

Cisco ISE acts as a single platform for defining, managing, and enforcing access policies organization-wide. It integrates with identity sources like Active Directory and LDAP for unified authentication and authorization processes. This centralization simplifies management by allowing administrators to set consistent access rules and ensures compliance with corporate policies and regulatory requirements. Additionally, Cisco ISE provides visibility into access patterns and anomalies across the network, improving both security insights and troubleshooting.

By combining RBAC for structured role assignments and ABAC for context-sensitive access decisions, Cisco ISE offers a comprehensive, flexible framework for access management. This approach helps organizations enforce security policies more precisely, reduce the risk of unauthorized access, and enhance overall cybersecurity resilience in alignment with operational needs.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Single Sign-On (SSO) – Solution should be compatible across on-premise and cloud based applications, reducing password fatigue and ensuring a seamless login experience for users.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

ISE enhances user access across on-premises and cloud applications via SSO, reducing password fatigue and streamlining login. By integrating with SAML-compliant identity providers like Azure AD and Duo SSO, Cisco ISE supports seamless access to diverse applications. Acting as a SAML Service Provider, it offers a unified login experience and enforces consistent security policies, ensuring both ease of access and compliance across organizational resources.

Prompt 3: Multi-Factor Authentication (MFA) – Solution should provide enforcement, supporting various authentication methods (e.g., Time-based one-time Password (TOTP), Short Message Service (SMS), biometrics) to add an extra layer of security.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Identity Services Engine (ISE) enhances security by supporting MFA through integrations with providers like Duo Security. This enables various methods, including TOTP via authenticator apps and SMS-based codes. ISE enforces MFA by defining policies that prompt for a second authentication factor after primary credentials are verified. This setup strengthens access control by adding an extra security layer, reducing the risk of unauthorized access.

Prompt 4: Role-Based Access Control (RBAC) and Attribute-Based Control (ABAC) – Solution should include mechanisms, enabling fine-grained access permissions based on user roles or attributes such as location, department, or security clearance.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

ISE enables fine-grained access control using RBAC and ABAC. RBAC assigns permissions based on predefined roles, ensuring users have access suited to their job functions. ABAC adds flexibility by evaluating attributes like location, department, and security clearance, allowing dynamic access decisions. Together, RBAC and ABAC enable Cisco ISE to adaptively enforce security policies, providing consistent, context-aware access control.

Prompt 5: Federated Identity Management – Solution should allow cross-domain authentication using standard protocols like SAML, OAuth, and OpenID Connect.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

ISE enables cross-domain authentication with federated identity management using protocols like SAML, OAuth, and OpenID Connect. Acting as a Service Provider (SP) in SAML, ISE redirects authentication to external Identity Providers (IdPs) for seamless Single Sign-On (SSO) across domains. With OAuth and OpenID Connect, ISE integrates with third-party IdPs to authenticate and authorize users, enhancing secure, flexible access control across varied network environments.

Prompt 6: Privileged Access Management (PAM) – Solution should provide capabilities to control and monitor the use of administrative or high-privilege accounts, ensuring that elevated access is limited and auditable.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

ISE offers Privileged Access Management using TACACS+ to control and audit high-privilege access to network devices. Through RBAC, Cisco ISE limits elevated access by assigning roles with specific permissions. Additionally, command authorization and accounting ensure that only authorized actions are performed and logged, creating an auditable trail of administrative activities. This approach enhances security by restricting and monitoring privileged access effectively.

Prompt 7: Self-Service Functionality – Solution should allow users to manage their own passwords, request access to systems, and track the status of access requests through an approval workflow.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

ISE offers Privileged Access Management using TACACS+ to control and audit high-privilege access to network devices. Through RBAC, Cisco ISE limits elevated access by assigning roles with specific permissions. Additionally, command authorization and accounting ensure that only authorized actions are performed and logged, creating an auditable trail of administrative activities. This approach enhances security by restricting and monitoring privileged access effectively.

Prompt 8: Integration of CTI Data Feeds – Solution should allow the IAM system to detect compromised credentials, suspicious login attempts, or help identify identity-related threat actor activities in real-time.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

ISE integrates with CTI data feeds via its Platform Exchange Grid (pxGrid), enabling real-time detection of identity threats like compromised credentials or suspicious logins. Using threat data, ISE can flag breached accounts and apply Adaptive Network Control (ANC) policies, such as access restriction or multi-factor authentication enforcement. This integration provides proactive threat detection and response, helping secure user identities across the network.

Digital Security Solutions

RFP No. 24-43230000-RFP

Attachment L9 – Service Category 9: Mobile Security and Threat Detection

Respondent Name: R2 Unified Technologies

Solution Name: SentinelOne Mobile Threat Defense

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 10. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 10 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 10 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-10 / 9) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor any additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Mobile Security Solutions must protect mobile devices (smartphones, tablets, and laptops) from unauthorized access, data leakage, and malware while maintaining compliance with security policies. The Solution should work across iOS, Android, and other mobile operating systems, integrating with Mobile Device Management (MDM) platforms to enforce security policies and track compliance.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

SentinelOne's Mobile Threat Defense (MTD) protects devices from a variety of threats, including both known and zero-day mobile malware attacks. It leverages advanced techniques such as machine learning, behavioral analysis, and threat intelligence to proactively detect and block malicious activities before they can cause harm. The solution provides protection against mobile malware, phishing, smishing, and man-in-the-middle (MITM) attacks, including rogue wireless and secure communications tampering. Additionally, it can detect and protect against zero-day mobile malware and phishing attacks, eliminate risks from jailbroken and rooted devices, and provide protection from data-stealing apps and ransomware.

SentinelOne's MTD integrates with Mobile Device Management (MDM) solutions such as Intune (Microsoft Endpoint Manager) and VMware Workspace ONE. The integration allows organizations to enhance their mobile security by combining the device management capabilities of MDM with the advanced threat detection and protection features of MTD. This integration ensures comprehensive security for mobile devices, including those in Bring Your Own Device (BYOD) environments, without compromising user privacy.

SentinelOne's Mobile Threat Defense supports iOS, Android, and ChromeOS.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and the Solution meets the identified technical capabilities and features.

Prompt 2: Mobile Threat Detection – Solution should include capabilities that monitor device behavior, app activity, and network connections for suspicious activities such as unauthorized data access, unapproved app installations, or malware downloads.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

SentinelOne's MTD can monitor device and app activity to detect a variety of threats in real-time including mobile malware, phishing and smishing, Man-in-the-Middle (MITM) attacks, jailbroken and rooted devices, and data-stealing application installations. The solution leverages advanced techniques such as machine learning, behavioral analysis, and threat intelligence to proactively detect and block malicious activities before they can cause harm.

Prompt 3: Mobile Application Management (IAM) – Solution should manage and secure the use of both enterprise and personal apps on mobile devices, including the ability to blacklist unsafe apps or restrict certain app permissions.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Singularity Mobile Threat Defense is able to blacklist applications but not restrict permissions. Many mobile device management tools can achieve this while Mobile Threat Defense is designed to augment that management with security toolsets.

Prompt 4: Device Encryption Enforcement – Solution should ensure that all data stored on the device is encrypted using industry-standard encryption algorithms (AES-256).

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

When integrated with an MDM that can encrypt devices Mobile Threat Defense can place a device into a "remediation" state until the issue is resolved. This state is designed to "contain" a device and restrict a user's ability to access certain information or functions, such as corporate apps. This helps keep a mobile device active and connect for critical functions, but protects information or tools that could be at risk.

Prompt 5: Remote Wipe and Lock Capabilities – Solution should enable administrators to remotely erase data from lost or stolen devices to prevent unauthorized access.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

When paired with an MDM with these capabilities, Mobile Threat Defense can place the device into a remediation state until the issue is resolved

Prompt 6: VPN Enforcement – Solution should ensure that all mobile data traffic is securely transmitted through encrypted channels, even when using public Wi-Fi networks.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

SentinelOne's MTD works with or without a Mobile Device Management (MDM) system and can integrate with various MDM products, including those that support VPN configurations. This integration allows for the enforcement of VPN policies to ensure secure mobile device connections.

Prompt 7: Behavioral Analytics – Solution should identify anomalous activities on mobile devices, such as attempts to bypass security controls or connect to unauthorized networks.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Mobile Threat Defense uses behavioral AI-driven protection, anomaly protection, real-time monitoring, integrations with zero-trust controls (like MDMs), and PII/privacy protection.

Prompt 8: Integration of MDM Solutions – Solution should enforce policies for password strength, screen lock timers, device encryption, and software updates.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

When integrated with an MDM capable of these functions, Mobile Threat Defense can place the device in a remediation mode until the device is brought into compliance with the related policies.

Prompt 9: Geo-Fencing Capabilities – Solution should allow administrators to restrict device functionality or access based on geographic location.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Mobile Threat Defense is able to geo-fence data from going to restricted countries and locations. It is not an MDM and cannot restrict a device based on its location.

Prompt 10: Integration of CTI Data Feeds – Solution should detect mobile-specific malware, phishing campaigns, or command-and-control traffic targeting mobile devices, providing real-time intelligence to block such threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The solution integrates with threat intelligence platforms (TIPs) to enrich security alerts with contextual information about current threat actors, malware campaigns, and indicators of compromise (IOCs)

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Any applicable Addtional Terms and Conditons Goes Here

SLA and Support Services

This Schedule B describes the maintenance service and support services that Zimperium will provide to Licensee for the applicable Products. All capitalized terms not otherwise defined in this schedule will have the meanings ascribed to them in the Agreement.

1. Definitions.

(a) "Initial Response Time" means the length of time after Zimperium's receipt of notice of a

Problem during which Zimperium will initiate a technical assessment of the Problem and acknowledge to Licensee its receipt of notice of the Problem

(b) "Problem" means a defect in a Product that causes the Product not to conform to its Documentation in one or more material respects. Problems are classified in four (4) categories:

(i) Level 1 Problem. Problems that arise when hardware, software, or network causes a complete disruption to Company's normal business activity. An error that renders the Products inoperative or where the production system is down or does not function at all, and there is no workaround for the problem. When a reasonable workaround is the resolution, the problem will be reclassified to Level 4 for software resolution.

(ii) Level 2 Problem. A Problem that significantly affects operation of the Products, and materially disrupts Licensee's use thereof. When a reasonable workaround is the resolution, the problem will be reclassified to Level 4 for software resolution.

(iii) Level 3 Problem. A Problem that affects the operation of the Products or impedes production in one or more non-core areas. Includes minor issues with core areas where there is no reasonable work around. Includes when a component of the Purchased Services is not performing as documented; there are unexpected results; problems are avoidable; there is moderate or minor operational impact. When a reasonable workaround is the resolution, the problem will be reclassified to Level 4 for software resolution.

(iv) Level 4 Problem. A Problem that has a minor impact on the operation of the Products, but does not materially degrade Licensee's use thereof. Level 4 problems include higher classification Problems for which reasonable workarounds exist.

(c) "Problem Resolution" means the implementation and release of a correction, patch, fix, alteration, or temporary workaround that eliminates or mitigates the impact of a Problem.

(d) "Support Ticket" means the mechanism defined by Zimperium to record Problems and track their resolution.

(e) "Target Resolution Time" means the time objective for Zimperium to either provide a Problem Resolution or define a mutually acceptable resolution plan.

2. Support. *Zimperium will provide support as described in this Schedule B for Problems that Licensee reports to Zimperium. Zimperium will only accept Problems reported by Licensee using the mechanism defined herein. For a Problem to be accepted for resolution, Licensee must provide a reproducible case using one of the specified release versions previously provided to Licensee, using tools available or made available to Licensee by Zimperium. If requested by Zimperium, Licensee will provide Zimperium a copy of the relevant source code so that Zimperium can reproduce and evaluate the Problem. If a specific device is necessary to reproduce the Problem, the device as well as the necessary tools and instructions to debug, build, and test the device image must be made available to Zimperium. If access to a server is necessary to observe the Problem or collect logs, access to that server must be provided.*

3. Issuance of Releases*. During the Term, Zimperium will provide Licensee all Functional Releases, Maintenance Releases and One-off Bug Fixes, as they are issued by Zimperium in its discretion. It is currently anticipated that Maintenance Releases will occur generally at three (3) month intervals unless no bugs have been fixed in the previous three (3) months. Additional information regarding releases is provided in Appendix 1.*

4. Problem Reporting and Resolution

4.1 Reporting Procedures. Problems must be reported as an email to a Zimperium-provided dedicated email address. All Problems reported as described above are documented in a Support Ticket.

4.2 Problem Resolution

(a) Licensee will make an initial assessment of the priority level of a Problem when it reports the Problem to Zimperium. Zimperium's initial response time will be based on the initial priority level proposed by Licensee, but Zimperium may reclassify Problems that were initially misclassified. For each reported Problem, Zimperium will use commercially reasonable efforts to meet the applicable Initial Response Time and Target Resolution Time set forth in the following table (presuming that Zimperium is provided access to the relevant Product during a period in which the system on which it resides is not undergoing maintenance or otherwise unavailable):

Problem Priority	***MAPS Suite***		***MTD Application***	
	Initial Response	*Target Resolution*	*Initial Response*	*Target Resolution*
Level 1	*1 Business Day*	*3 Business Days*	*I Hour*	*4 Hours*
Level 2	*2 Business Days*	*5 Business Days*	*4 hours*	*5 Days*
Level 3	*10 Business Days*	*40 Business Days*	*8 Hours*	*10 Days*
Level 4	*20 Business Days*	*Not Specified*	*2 Days*	*Next Regular Update Cycle*

5. Exclusions*. Zimperium will have no obligation to respond to or resolve any incidents, problems or issues that are not caused by defects in the Products. Without limitation of the generality of the foregoing, Zimperium will have no obligation with respect to any incident, problem or issue that is caused in whole or in part by (i) the acts or omissions of Licensee or its employees or contractors, including any negligence, willful misconduct, or use of any Product in a manner not authorized by this Agreement or inconsistent with the applicable Documentation; (ii) modification of any Product by anyone other than Zimperium; or (iii) any combination or integration of any Product with hardware, software and/or technology not provided by Zimperium.*

6. Escalation*. If there is any dispute or disagreement regarding the Services that cannot be resolved by the Parties' respective technical representatives, including a disagreement with respect to the severity level of any Problem, either Party may escalate the dispute or disagreement to the Parties' respective primary business contacts as identified in the table below:*

Zimperium: Zimperium Support: Support@zimperium.com

Licensee: Designated Contact: designated contact email

7. New Feature Requests or Suggestions*. Requests for new features or for functionalities beyond those described in the current Documentation are not subject to this Exhibit and will be treated by Zimperium in its sole discretion. Licensee may communicate to Zimperium any suggestions, recommendations or feedback regarding the Products, including modifications, design changes, or improvements ("Suggestions"). Licensee agrees that Zimperium may freely use all Suggestions in connection with the Products or any other products or services. Licensee acknowledges and agrees that such consideration is reasonable and fair.*

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L10 – Service Category 10: Secure Access Service Edge (SASE)

Respondent Name: R2 Unified Technologies

Solution Name: Cisco Secure Access

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8 Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for the proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-9 / 8) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: SASE Solutions combine networking and security services, delivering both through a cloud-based framework that supports remote users, branch offices, and cloud applications. The Solution integrates Software-Defined Wide Area Networking (SD-WAN) with advanced security features like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS).

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cisco Secure Access, part of Cisco's SASE (Secure Access Service Edge) framework, integrates networking and security in a cloud-based solution that supports remote users, branch offices, and cloud applications. Combining SD-WAN with advanced security features, it delivers scalable protection and optimized connectivity for distributed environments.

SD-WAN Integration for Connectivity: Cisco Secure Access includes SD-WAN, dynamically routing traffic based on network conditions and policies. It ensures optimal performance for remote users and branches by prioritizing critical applications and managing bandwidth efficiently, simplifying centralized management and security across sites.

Secure Web Gateway (SWG): The SWG inspects all web traffic for malware, phishing, and other threats, enforcing real-time policies to protect users and block malicious content. Administrators gain granular control to align web access with organizational policies, ensuring safe internet usage.

Cloud Access Security Broker (CASB): CASB safeguards data between users and cloud services, identifying risky behaviors, shadow IT, and unsanctioned apps. It enforces policies for cloud access, securing sensitive data and maintaining regulatory compliance, including SaaS applications.

Zero Trust Network Access (ZTNA): ZTNA enforces identity-based access, granting application and resource access based on user identity, device health, and security posture. Continuous authentication minimizes risks of unauthorized access, enhancing protection against internal and external threats.

Firewall as a Service (FWaaS): FWaaS delivers advanced firewall capabilities through the cloud, inspecting and controlling traffic flows while enabling centralized policy management. It ensures consistent enforcement across distributed networks, protecting users and applications everywhere.

Unified Management Console: Cisco Secure Access offers a unified console to configure, monitor, and enforce policies across all locations. This centralized management simplifies operations, providing real-time insights and ensuring consistent security within the SASE framework.

Real-Time Threat Intelligence: Powered by Cisco Talos, Cisco Secure Access integrates real-time intelligence on new threats and attack vectors, automatically updating policies to counter evolving risks.

Scalability for Remote Work and Branch Offices: Its cloud-based architecture supports distributed environments, eliminating hardware complexity and adapting easily to changing network needs and emerging threats.

In summary, Cisco Secure Access integrates SD-WAN, SWG, CASB, ZTNA, and FWaaS in a cloud-based SASE framework. This approach enhances network performance, strengthens security, and ensures scalability for remote and branch deployments.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: SD-WAN with Policy-Based Routing– Solution should enable dynamic, intelligent path selection to ensure optimal network performance for applications, even across distributed cloud environments.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Access integrates seamlessly with Cisco SD-WAN, allowing organizations to leverage SD-WAN's policy-based routing capabilities. This integration enables dynamic, intelligent path selection for optimal application performance across distributed cloud environments. Cisco SD-WAN prioritizes traffic based on policies, ensuring efficient bandwidth use and reduced latency, while Secure Access provides complementary security enforcement across these connections.

Prompt 3: Zero Trust Network Access (ZTNA) Principles – Solution should enforce least-privilege access to applications based on identity and context (e.g., user role, device health, location) rather than assuming trust based on network location.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Access enforces Zero Trust Network Access (ZTNA) principles by applying least-privilege access based on identity and contextual factors like user role, device health, and location. It continuously verifies user and device trust before granting application access, ensuring that access decisions are dynamic and aligned with security policies, rather than relying on network location. This approach minimizes risk by restricting access strictly to authorized users and resources.

Prompt 4: Secure Web Gateway (SWG)– Solution should include features that protect users from web-based threats, such as malware, malicious URLs, and phishing attempts, by inspecting traffic at the cloud edge and enforcing acceptable use policies.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Access includes a Secure Web Gateway (SWG) that protects users from web-based threats like malware, malicious URLs, and phishing. It inspects web traffic at the cloud edge, blocking harmful content and enforcing acceptable use policies. This filtering ensures that users access only safe, policy-compliant websites, enhancing security by preventing exposure to online threats regardless of user location.

Prompt 5: Firewall as a Service (FwaaS) – Solution should deliver consistent firewall policies across multiple locations and devices, centralizing management of security controls such as network segmentation, access control, and intrusion detection.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Access provides Firewall as a Service (FWaaS), delivering consistent firewall policies across locations and devices. It centralizes management of security controls like network segmentation, access control, and intrusion detection, ensuring uniform enforcement of security policies. This centralized approach simplifies policy management, allowing organizations to maintain a strong security posture across distributed environments.

Prompt 6: Real-Time Analytics and Reporting – Solution should provide insights into network performance, traffic patterns, security threats, and user behavior across distributed environments.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Access offers real-time analytics and reporting, providing insights into network performance, traffic patterns, security threats, and user behavior across distributed environments. These analytics help organizations monitor and assess network health, identify security risks, and understand user activity, supporting proactive management and informed decision-making to strengthen security and optimize performance.

Prompt 7: Integration of CTI Data Feeds – Solution should detect and block malicious network traffic or unauthorized access attempts based on real-time threat intelligence, correlating user activity and network behavior with known threat actors or compromised infrastructure.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Access leverages threat intelligence feeds from Cisco Talos to enhance security by identifying potential threats. While it does not directly block malicious traffic based on real-time CTI data, Talos intelligence helps inform Secure Access's threat detection capabilities, supporting proactive monitoring and alerting against known threat indicators and risky behaviors across the network.

Prompt 8: Cloud Access Security Broker (CASB) – Solution should integrate to provide visibility and control over cloud applications and services, monitoring and securing data stored in third-party SaaS platforms.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cisco Secure Access integrates Cloud Access Security Broker (CASB) functionality to provide visibility and control over cloud applications and services. It monitors and secures data in third-party SaaS platforms, enabling organizations to detect shadow IT, enforce data protection policies, and ensure compliance. This integration helps safeguard sensitive information in the cloud by identifying risky behavior and applying security controls to cloud-based interactions.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L11 – Service Category 11: Governance, Risk, and Compliance (GRC)

Respondent Name: R2 Unified Technologies

Solution Name: Drata MSSP

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: GRC Solutions should provide a structured approach to managing governance frameworks, assessing enterprise risks, and ensuring compliance with industry regulations. The Solution must facilitate the development of policies, automate compliance checks, and enable risk management and assessment workflows that align with business objectives.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Drata's Governance, Risk, and Compliance (GRC) solutions provide a structured approach for managing governance frameworks, assessing risks, and ensuring regulatory compliance. Through policy management, automated compliance checks, and risk assessment workflows, Drata enables organizations to streamline GRC processes aligned with business goals. Here's an overview:

1. Policy Development and Management

Drata offers customizable, auditor-approved policy templates, enabling organizations to create and manage compliance policies effectively. Policy acknowledgment tracking ensures compliance across teams, with clear records. This simplifies policy development, keeping them aligned with governance standards.

2. Automated Compliance Checks

Drata's automated monitoring continuously checks security controls, assessing audit readiness daily and identifying compliance gaps. This real-time monitoring offers visibility into compliance status, enabling proactive issue resolution. Automation reduces manual tasks, saving time and minimizing error in compliance management.

3. Risk Management and Assessment Workflows

Drata's risk management tools facilitate structured assessment and treatment, allowing organizations to classify risks by severity. Drata supports various responses (accept, mitigate, avoid) to align risk management with business objectives. This workflow organization ensures consistent risk assessments and mitigations across the organization.

4. Real-Time Dashboard and Reporting

A centralized, real-time dashboard provides metrics on compliance status, policy adoption, and outstanding risks. This simplifies reporting to executives and audit committees. Detailed reports also support audits, enabling effective communication with auditors and stakeholders.

5. Integration and Scalability

Drata scales to meet organizational needs, supporting frameworks like SOC 2, ISO 27001, HIPAA, and GDPR. It integrates with existing tools, automating compliance checks across environments, enabling organizations to stay compliant as they grow.

By combining these capabilities, Drata's GRC solutions deliver a proactive approach to governance and compliance. Automation reduces manual workloads and allows continuous monitoring, while risk assessment aligns management efforts with business goals. This integrated suite helps organizations uphold compliance standards, manage risk effectively, and streamline GRC processes.

In summary, Drata empowers organizations to establish a resilient compliance program, aligning policies and risk management with business goals. It automates compliance checks, ensures continuous regulatory adherence, supports streamlined audits, and offers scalable solutions for complex regulatory environments. This approach enables real-time visibility, minimizes compliance risk, and provides a robust framework for managing governance, risk, and compliance.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Centralized Policy Management – Solution should allow the creation, distribution, and tracking of governance frameworks, compliance guidelines, and operational policies. The Solution should support version control and electronic signatures for policy acceptance.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Policy Center simplifies management with tools for creating, distributing, and tracking governance frameworks, compliance guidelines, and operational policies. It offers version control, integration with platforms like BambooHR, and templates for customization. Policies can be assigned owners, mapped to controls, and tracked with a full version history. Approval workflows and electronic signatures ensure personnel acknowledgment, providing a transparent solution for compliance and acceptance.

Prompt 3: Risk Assessment Tools – Solution should enable organizations to identify, assess, and prioritize risks across departments or business units based on likelihood and impact.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Drata's Risk Assessment tools help organizations identify, assess, and prioritize risks using a structured approach. A library of over 200 risk scenarios supports comprehensive identification, while a 5x5 scale evaluates likelihood and impact to quantify severity. Risks are then prioritized,

and treatment plans—such as mitigation, acceptance, or avoidance—are developed. This framework enables effective risk management tailored to business objectives across departments.

Prompt 4: Risk Mitigation and Treatment Workflows – Solution should allow teams to define and track risk response plans, assign responsibilities, and monitor progress toward mitigation goals.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Workflows enable teams to define risk response plans, assign responsibilities, and track mitigation progress. Organizations can tailor treatment plans—such as mitigating, accepting, transferring, or avoiding risks—based on impact and likelihood. Assigned risk owners ensure accountability, while a centralized dashboard provides real-time visibility into progress and alerts for emerging threats. This process ensures effective risk mitigation aligned with busisness goals.

Prompt 5: Audit Management Capabilities – Solution should support the planning, scheduling, and execution of internal and external audits. The platform should automatically generate audit reports, track findings, and ensure follow-up actions are completed.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Drata's Audit Hub streamlines internal and external audits with tools for planning, scheduling, and execution. It automates evidence collection, reducing manual effort, and centralizes communication for real-time collaboration. Auditors can request, approve, and track evidence within the platform, ensuring efficient task management. The system archives past audits for context and ensures findings are tracked and follow-up actions completed, enhancing audit efficiency and compliance.

Prompt 6: Compliance Tracking – Solution should include industry-specific regulations (e.g., NIST CSF, GDPR, HIPAA, PCI-DSS), with automated controls and real-time monitoring to detect non-compliance or control failures.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Drata supports compliance with industry-specific regulations like NIST CSF, GDPR, HIPAA, and PCI DSS using automated controls and real-time monitoring. Its pre-mapped controls simplify implementation, while continuous monitoring detects non-compliance or control failures for swift remediation. Cross-mapping of controls across frameworks reduces duplication, streamlining efforts for organizations adhering to multiple standards, ensuring proactive, efficient, and scalable compliance management.

Prompt 7: Customizable Risk Dashboards – Solution should provide executives with an overview of key risks, compliance metrics, and the overall health of the governance program. Dashboards should display real-time data and support drill-down views for detailed analysis.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Drata's customizable risk dashboards provide executives with real-time overviews of key risks, compliance metrics, and governance program health. Dashboards display up-to-date data, support tailored views for specific frameworks or business units, and enable drill-down analysis for detailed insights. This functionality helps executives monitor compliance, perform root cause analysis, and align governance efforts with strategic objectives effectively.

Prompt 8: Third-Party Risk Management – Solution should facilitate the assessment of third-party vendor risks and perform due diligence on vendors' compliance and risk management practices.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Drata's customizable risk dashboards provide executives with real-time overviews of key risks, compliance metrics, and governance program health. Dashboards display up-to-date data, support tailored views for specific frameworks or business units, and enable drill-down analysis for detailed insights. This functionality helps executives monitor compliance, perform root cause analysis, and align governance efforts with strategic objectives effectively.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Any applicable Addtional Terms and Conditons Goes Here

Terms of Service - Subscription Agreement

We have updated Drata's Terms of Service - Subscription Services Agreement ("Agreement") effective as of March 4, 2024. If you want to view the previous version of this, click here. If you want a PDF version of this, click here. THIS AGREEMENT IS A BINDING CONTRACT AND GOVERNS THE USE OF AND ACCESS TO THE SERVICES BY YOU AND YOUR AUTHORIZED USERS WHETHER IN CONNECTION WITH A PAID SUBSCRIPTION OR FREE TRIAL FOR THE SERVICES. By accepting this Agreement, either by accessing or using a Service, or authorizing or permitting any User to access or use a Service, Customer agrees to be bound by this Agreement as of the date of such access or use of the Service (the "Effective Date"). If You are entering into this Agreement on behalf of a company, organization or another legal entity (an "Entity"), You are agreeing to this Agreement for that Entity and representing to Drata that You have the authority to bind such Entity and its Affiliates to this Agreement, in which case the terms "Customer," "You," or "Your" herein refers to such Entity and its Affiliates. If You do not have such authority, or if You do not agree with this Agreement, You must not use or authorize any use of the Services. Customer and Drata shall each be referred to as a "Party" and collectively referred to as the "Parties" for purposes of this Agreement. The purpose of this Agreement is to establish the terms and conditions under which Customer may purchase Drata's Services and Professional Services as described in an Order Form, Statement of Work or other document signed or agreed to by the Customer. The terms of the Order Form or Statement of Work shall control in the event of any inconsistency or conflict with the terms of this Agreement. Non-English translations of this Agreement are provided for convenience only. In the event of any ambiguity or conflict between translations, the English version shall control. Table of Contents: General Terms and Conditions:

1. Access to the Services
2. Use of the Services
3. Term, Cancellation and Termination
4. Fees, Billing, Plan Modification and Payments
5. Confidential Information
6. Subprocessors and Security of Customer Data
7. Temporary Suspension
8. Non-Drata Services

General Terms and Conditions

SECTION 1. ACCESS TO THE SERVICES

1.1 Service. Drata will make the Services and Customer Data available pursuant to this Agreement and the applicable Order Form(s) and Documentation. Drata will use commercially reasonable efforts to make the Services available twenty-four (24) hours a day, seven (7) days a week maintaining 99.9% Service availability, except during (i) Planned Downtime (of which Drata will give advance notice via the Site or to the Account admin); and (ii) Force Majeure Events.

1.2 Support. Drata will, at no additional charge, provide support via chat and ticket on Mondays through Fridays (24 hours per day), excluding federal public holidays in the United States and other Drata announced support holidays. If purchased by Customer, Drata will provide upgraded support or support that includes service level agreements.

1.3 Professional Services. Upon Customer's request, Drata may provide Professional Services subject to the terms and conditions stated at: https://drata.com/proserv.

1.4 Modifications. Customer acknowledges that Drata may modify the features and functionality of the Services during the Subscription Term. Drata shall provide Customer with thirty (30) days' advance notice of any deprecation of any material feature or functionality. Drata will not materially decrease the overall functionality of the Services purchased by Customer or of the security measures detailed in this Agreement during the Subscription Term.

1.5 Additional Features. Drata will notify Customer of applicable Supplemental Terms or alternate terms and conditions prior to Customer's activation of any additional features. Customer's activation of any additional features in Customer's Account will be considered acceptance of the applicable Supplemental Terms or alternate terms and conditions where applicable.

1.6 Extension of Rights to Affiliates. Customer may extend its rights, benefits and protections provided herein to its Affiliates and to contractors or service providers acting on Customer's or Customer's Affiliates' behalf, provided that Customer remains responsible for their compliance hereunder. An Affiliate may also directly purchase Services or Professional Services pursuant to the terms of this Agreement provided that such Affiliate (i) executes an Order Form or Statement of Work for such Services or Professional Services; and (ii) agrees to be bound by the terms of this Agreement as if it were an original party hereto. Customer hereby authorizes Drata to share the content of this Agreement with Customer's Affiliates.

SECTION 2. USE OF THE SERVICES

2.1 Login Management. Access to and use of certain Services is restricted, such as to the specified number of individual Users permitted under Customer's subscription to the applicable Service, as detailed in the Documentation. For Services that are User-based, Customer agrees and acknowledges that a User login cannot be shared or used by more than one (1) individual per Account. However, User logins may be reassigned to new individuals replacing former individuals who no longer require ongoing use of the Services. Customer and Users are responsible for maintaining the confidentiality of all User login information for an Account. Customer shall not use the API or any Software in such a way to circumvent applicable Service feature or functionality restrictions or User licensing restrictions that are enforced in the Service user interface. Drata reserves the right to charge Customer, and Customer hereby agrees to pay, for any overuse of a Service in violation of this Agreement or the features and limitations on the Site or Documentation, in addition to other remedies available to Drata.

2.2 Compliance. As between Customer and Drata, Customer is responsible for compliance with the provisions of this Agreement by Users and for any and all activities that occur under an Account, which Drata may verify from time to time. Without limiting the foregoing, Customer will ensure that its use of the Services is compliant with all applicable laws and regulations as well as any and all privacy notices, agreements or other obligations Customer may maintain or enter into with Users.

2.3 Use Restrictions. Customer will not, and will ensure its Users will not: (i) make the Services available to anyone other than Customer or its Users, or use the Services for the benefit of anyone other than Customer or Customer's Affiliates, except as expressly allowed in an Order Form; (ii) modify, adapt, alter or translate the Services; (iii) sublicense, lease, sell, resell, rent, loan, or distribute the Services, or any part thereof, or include the Services in a service bureau or outsourcing offering; (iv) reverse engineer, decompile, disassemble, or otherwise derive or determine or attempt to derive or determine the source code (or the underlying ideas, algorithms, structure or organization) of the Services or any part thereof, except as permitted by law; (v)

interfere in any manner with the operation of the the Services or the hardware and network used to operate the same, or attempt to probe, scan or test vulnerability of the Services without prior authorization of Drata; (vi) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights; (vii) modify, copy, disclose (except as expressly authorized in this Agreement) or make derivative works based on any part of the Services; (viii) access or use the Services, or any feature, information or functionality thereof, to build a similar or competitive product or service or otherwise engage in competitive analysis or benchmarking; (ix) attempt to access the Services through any unapproved interface; (x) remove, alter, or obscure any proprietary notices (including copyright and trademark notices) of Drata or its licensors on the Services or any copies thereof; (xi) upload to the Services any Customer Data that contains any sensitive personal information (such as financial, medical or other sensitive personal information such as government IDs, passport numbers, protected health information, credit card data, or social security numbers); or (xii) otherwise use the Services in any manner that exceeds the scope of use permitted under applicable Order Forms.

2.4 System Requirements. A high-speed Internet connection is required for proper transmission of the Services. Customer is responsible for procuring and maintaining the network connections that connect Customer's network to the Services including, but not limited to, browser software that supports protocols used by Drata, including the Transport Layer Security (TLS) protocol or other protocols accepted by Drata and following procedures for accessing services that support such protocols. Drata is not responsible for notifying Customer or Users of any upgrades, fixes or enhancements to any such software or for any compromise of data, including Customer Data, transmitted across computer networks or telecommunications facilities (including but not limited to the Internet) which are not owned, operated or controlled by Drata. Drata assumes no responsibility for the reliability or performance of any connections as described in this section.

SECTION 3. TERM, CANCELLATION AND TERMINATION

3.1 Term. The term of this Agreement begins on the Effective Date and will remain in effect as long as the Customer has an active subscription to the Services, Statement of Work or until this Agreement is otherwise terminated in accordance with the terms hereof, whichever occurs first. The Subscription Term will be defined in each individual Order Form. Unless an Account and subscription to a Service are terminated in accordance with this Agreement or the applicable Order Form, or unless otherwise stated in the applicable Order Form, (i) Customer's subscription to a Service will automatically renew for a Subscription Term equivalent in length to the then-expiring Subscription Term; and (ii) the Subscription Charges applicable to any subsequent Subscription Term shall be Drata's Standard Subscription Charges for the applicable Service plan types at the time of such renewal.

3.2 Cancellation. Either Party may elect to terminate an Account and subscription to a Service at the end of the then-current Subscription Term by providing notice in accordance with Section 18 of this Agreement to support@drata.com no less than thirty (30) days prior to the end of the then-existing Subscription Term.

3.3 Termination for Cause. A Party may terminate this Agreement for cause (i) upon written notice to the other Party of a material breach by the other Party, provided that the breaching Party shall have thirty (30) days to cure such material breach from the date of receipt of such written notice; or (ii) if the other Party becomes the subject of a petition in bankruptcy or any other proceeding

relating to insolvency, receivership, liquidation, or assignment for the benefit of creditors. Additionally, Drata may immediately terminate this Agreement for cause without notice if Customer violates Drata's User Conduct and Content Policy or if provision of the Service violates applicable law, regulation or court order.

Drata will refund any prepaid fees covering the remainder of the Subscription Term as of the effective date of termination if this Agreement is terminated by Customer in accordance with this section for Drata's uncured material breach.

Customer agrees to pay any unpaid fees covering the remainder of the Subscription Term pursuant to all applicable Order Forms if Drata terminates this Agreement for Customer's material breach in accordance with this section. In no event will Drata's termination for cause relieve Customer of Customer's obligation to pay any fees payable to Drata for the period prior to termination.

3.4 Payment Upon Termination. Except for Customer's termination under Section 3.3, in addition to any other amounts Customer may owe Drata, Customer must immediately pay any and all unpaid Subscription Charges associated with the remainder of such Subscription Term.

3.5 No Refunds/Credits. Except for Customer's termination rights under Section 3.3, Drata does not provide refunds or credits for Subscription Charges or other fees or payments.

3.6 Export of Customer Data. Upon Customer's written request and in accordance with Drata's Customer Data Deletion and Retention Policy found in Drata's Trust Center, Drata will make Customer Data available to Customer for export or download as provided in the Documentation for thirty (30) days after the effective date of termination, expiration or migration of the Account, except for Customer Data which (i) has been deleted in accordance with the Documentation; (ii) was created and/or used in violation of this Agreement; or (iii) which, if made available, would violate applicable law. Thereafter, Drata will have no obligation to maintain or provide any Customer Data and Drata will delete Customer Data in accordance with Drata's Data Deletion and Retention Policy available in Drata's Trust Center unless prohibited by law or legal order.

SECTION 4. FEES, BILLING, PLAN MODIFICATIONS AND PAYMENTS

4.1 Payment and Billing. Unless otherwise expressly set forth in this Agreement, an Order Form, a Statement of Work, or as otherwise agreed for Usage Charges, all Subscription Charges are due in full upon commencement of the Subscription Term. Customer is responsible for providing valid and current account information which shall include (i) physical billing address; (ii) ship-to address; and (iii) billing contact email address. Customer agrees to promptly update the account information, including billing information, with any changes that may occur (for example, a change in Customer's billing address or credit card expiration date). If Customer fails to pay Subscription Charges or any other charges indicated on any Order Form or Statement of Work, or in any Supplemental Terms, within five (5) days of Drata's notice to Customer that payment is delinquent, or if Customer does not update payment information upon Drata's request, in addition to other remedies, Drata may suspend access to and use of the Services by Customer and Users. As permitted by applicable law, Drata reserves the right to charge the Customer late payment penalties and interest charges on any past-due invoices that are not subject to a previously-noticed good faith dispute as to amount owed.

4.2 Fees. Customer will pay all Fees to Drata in accordance with the Order Form and this Agreement. Payment obligations are non-cancelable, and Fees paid are non-refundable. Except as otherwise set forth in an Order Form, Drata may increase Subscription Charges upon renewal of each Order Form Subscription Term by providing written notice to Customer at least forty-five (45) days prior to the commencement of the applicable renewal Subscription Term.

4.3 Upgrades. If Customer chooses to upgrade its plan type or add products (such as additional frameworks) during the Subscription Term, any incremental Subscription Charges associated with such upgrade will be charged in accordance with the remaining Subscription Term. In any subsequent Subscription Term, the Subscription Charges will reflect any such upgrades.

4.4 Downgrades. Customer may not downgrade its plan type or reduce the number of frameworks during any Subscription Term. Customer may only downgrade its plan type or reduce the number of frameworks for a subsequent Subscription Term at the end of the then-current Subscription Term by providing Drata with thirty (30) days prior written notice indicating which instances will be affected and the details of the downgrade requested. If a new Order Form is not signed by the Customer before the end of the then-current Subscription Term, the Services will renew as described in Section 3.1.

4.5 If applicable, Usage Charges, limits and pricing are set forth on the Order Form associated with each purchase. Drata will not prevent Customer from increasing product volume usage beyond the licensed usage volume. Such increases shall trigger an adjustment to the contract terms and result in a supplemental Order Form, or at prevailing and customary rates if not otherwise indicated. Adjustments will be applied to the remainder of the Subscription Term. In the event Customer objects to the volume increases, the Parties will work together in good faith to reduce the volume below the original Order Form volume limits or separately adjust contract terms.

4.6 Taxes. Unless otherwise stated, Drata's Subscription Charges do not include any Taxes. Customer is responsible for paying Taxes assessed in connection with the subscription to the Services except those assessable against Drata measured by its net income. If Drata has a legal obligation to pay or collect any Taxes for which Customer is responsible, Drata will invoice Customer and Customer will pay that amount. Drata agrees to exempt Customer from any taxes for which Customer provides to Drata a tax exemption certificate prior to the issuance of an invoice; provided, however, that no such exemption shall be extended to Customer following written notice to Drata from a taxing authority of appropriate jurisdiction that Customer does not qualify for the claimed exemption.

4.6.1 If the Customer is required to withhold Taxes from payments to Drata, Customer shall pay Drata the amount owing on the invoice, less a deduction for such Taxes withheld to be remitted directly by the Customer to the relevant tax authority. Customer will provide Drata with a valid receipt for such Taxes remitted to the relevant tax authority within ninety (90) days of Customer's payment to Drata from which the withholding was made. If Customer does not provide the valid receipt for such Taxes remitted within ninety (90) days, Customer agrees and acknowledges that it will be charged and will have to pay for the full amount of the invoice.

4.6.2 If the Customer is legally required to withhold Taxes from payments to Drata but fails to do so and pays an invoice in full, Customer may be entitled to reimbursement by Drata of the Taxes which should have been withheld. Drata shall only make such reimbursement during the first year

following payment of the relevant invoice to Drata, once the Customer provides Drata with a valid receipt for the Taxes remitted to the relevant tax authority in respect of that invoice.

4.7 Payment Portals. If Customer mandates Drata to use a vendor payment portal or compliance portal that charges Drata a subscription fee or a percentage of any uploaded invoice as a required cost of doing business, Customer shall be invoiced by Drata for, and Customer shall pay, the cost of this fee.

SECTION 5. CONFIDENTIAL INFORMATION

In connection with the Services, each Party will protect the other's Confidential Information from unauthorized use, access or disclosure in substantially the same manner as each Party protects its own Confidential Information, but with no less than reasonable care. Except as otherwise expressly permitted pursuant to this Agreement, each Party may use the other Party's Confidential Information solely to exercise its respective rights and perform its respective obligations under this Agreement and shall disclose such Confidential Information (i) solely to the employees and/or non-employee service providers and contractors who have a need to know such Confidential Information and who are bound by terms of confidentiality intended to prevent the misuse of such Confidential Information; (ii) as necessary to comply with an order or subpoena of any administrative agency or court of competent jurisdiction; or (iii) as reasonably necessary to comply with any applicable law or regulation. The provisions of this Section 5 shall control over any non-disclosure agreement by and between the Parties and any such non-disclosure agreement shall have no further force or effect with respect to the exchange of Confidential Information after the execution of this Agreement. This section shall not apply to any information which (a) was publicly known prior to the time of disclosure by the disclosing Party; or (b) becomes publicly known after such disclosure through no action or inaction of the receiving Party in violation of this Agreement. For clarity, any exchange of Confidential Information prior to the execution of this Agreement shall continue to be governed by any such non-disclosure agreement. Given the unique nature of Confidential Information, the Parties agree that any violation or threatened violation by a Party to this Agreement with respect to Confidential Information may cause irreparable injury to the other Party. Therefore, the Parties agree such violation or threatened violation shall entitle the other Party to seek injunctive or other equitable relief in addition to all legal remedies.

SECTION 6. SUBPROCESSORS AND SECURITY OF CUSTOMER DATA

6.1 Subprocessors. Drata will utilize Subprocessors who will have access to or process Customer Data to assist in providing the Services to the Customer as detailed on the Authorized Subprocessors Page. Customer hereby confirms and provides general authorization for Drata's use of the Subprocessors listed on the Authorized Subprocessors Page. Drata shall be responsible for the acts and omissions of members of Drata Personnel and Subprocessors to the same extent that Drata would be responsible if Drata was performing the services of each Drata Personnel or Subprocessor directly under the terms of this Agreement. Drata will notify a Customer's admin when a new Subprocessor is added (including the name and location of the relevant Subprocessor and the activities it will perform) and by updating the Authorized Subprocessors Page.

6.2 Third-Party Service Providers. Drata may use third-party service providers that are utilized by Drata to assist in providing the Services to Customer, but do not have access to Customer Data. Any third-party service providers utilized by Drata will be subject to confidentiality obligations which are substantially similar to the confidentiality terms herein. Drata shall be responsible for

the acts and omissions of members of Drata's third-party service providers to the same extent that Drata would be responsible if Drata was performing the services of each third-party service provider directly under the terms of this Agreement.

6.3 Safeguards. Drata will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data. If either Party becomes aware of a Security Incident, that Party must promptly notify the other Party, unless legally prohibited from doing so, within forty-eight (48) hours or any shorter period required by law except that Customer is not required to notify Drata unless Customer reasonably determines there is a threat to the Service. Additionally, each Party shall reasonably assist the other Party in mitigating any potential damage. As soon as reasonably practicable after any Security Incident, Drata shall conduct a root cause analysis and, upon request, shall share the results of its analysis and its remediation plan with Customer. Unless prohibited by law, each Party shall provide the other Party with reasonable notice of and the opportunity to review and comment on the content of all public notices, filings, or press releases about a Security Incident that identify the other party by name prior to any such publication.

6.4 Customer Data. Drata will, and Customer hereby instructs Drata to, access Customer Data to provide, secure and improve the Services. Customer is solely responsible for the accuracy, content, and legality of all Customer Data. When Customer Data is used to improve Drata's machine learning models, Drata will ensure that such Customer Data, including Personal Data, is not reproduced by the model to another customer, and will take necessary steps to prevent this, such as applying data sanitation algorithms to training data.

6.5 Customer Information. Drata shall be the Data Controller of personal information of Customer's Users and admins; and, shall process such personal information in accordance with Drata's Privacy Notice. Customer is responsible for informing its Users and admins of their rights set forth in Drata's Privacy Notice. Customer represents and warrants that it has obtained all relevant consents, permissions and rights and provided all relevant notices necessary under applicable data protection laws for Drata to lawfully process such personal information for the purposes set forth in Drata's Privacy Notice. 6.6 Data Processing Addendum. The Data Processing Addendum can be signed here and thereafter shall be incorporated by reference herein into this Agreement once signed by the Parties.

SECTION 7. TEMPORARY SUSPENSION

Drata reserves the right to restrict functionalities or suspend the Services (or any part thereof), Customer's Account or Customer's and/or Users' rights to access and use the Services and remove, disable or quarantine any Customer Data or other content if (i) Drata reasonably believes that Customer or Users have violated this Agreement; or (ii) Drata suspects or detects any Malicious Software connected to a Customer's Account or use of a Service by Customer or Users. This right includes the removal or disablement of Customer Data or other content in accordance with Drata's policies. Drata also reserves the right to immediately suspend Customer's Account for Customer's violation of Drata's User Conduct and Content Policy. Drata will use commercially reasonable efforts to notify Customer via email when taking any of the foregoing actions unless legally prohibited. Drata shall not be liable to Customer, Users or any other third party for any modification, suspension or discontinuation of Customer's rights to access and use the Services. Drata may refer any suspected fraudulent, abusive, or illegal activity by Customer or Users to law enforcement authorities at Drata's sole discretion.

SECTION 8. NON-DRATA SERVICES

If Customer decides to enable, access or use Non-Drata Services, Customer's access and use of such Non-Drata Services shall be governed solely by the terms and conditions of such Non-Drata Services. Drata does not endorse, is not responsible or liable for, and makes no representations as to any aspect of such Non-Drata Services, including, without limitation, their content or the manner in which they handle, protect, manage or process data (including Customer Data), or any interaction between Customer and the provider of such Non-Drata Services. Drata cannot guarantee the continued availability of such Non-Drata Service features, and may cease enabling access to them without entitling Customer to any refund, credit or other compensation if, for example and without limitation, the provider of a Non-Drata Service ceases to make the Non-Drata Service available for interoperation with the corresponding Service in a manner acceptable to Drata. Customer irrevocably waives any claim against Drata with respect to such Non-Drata Services. Drata shall not be liable for any damage or loss caused or alleged to be caused by or in connection with Customer's enablement, access or use of any such Non-Drata Services, or Customer's reliance on the privacy practices, data security processes or other policies of such Non-Drata Services. Customer may be required to register for or log into such Non-Drata Services on their respective websites. By enabling any Non-Drata Services, Customer is expressly permitting Drata to disclose Customer's login and Customer Data to the provider of the Non-Drata Service as necessary to facilitate the use or enablement of such Non-Drata Services.

SECTION 9. FREE TRIALS

If Customer is approved by Drata for Free Trial Services, Drata will make the applicable Free Trial Services available to Customer free of charge until the earlier of: (i) the end of the free trial period communicated by Drata to Customer; (ii) the start date of any Purchased Services subscriptions ordered by Customer for such Service(s); or (iii) termination of the Free Trial Services period by Drata in its sole discretion. For the purposes of trials, Section 10.5 herein shall not apply. ANY CUSTOMER DATA CUSTOMER ENTERS INTO THE FREE TRIAL SERVICES WILL BE PERMANENTLY LOST UNLESS CUSTOMER PURCHASES A SUBSCRIPTION TO THE SAME SERVICES AS THOSE COVERED BY THE FREE TRIAL SERVICES OR EXPORTS SUCH CUSTOMER DATA BEFORE THE END OF THE TRIAL PERIOD. NOTWITHSTANDING THE "REPRESENTATIONS, WARRANTIES AND DISCLAIMERS" SECTION AND "INDEMNIFICATION BY DRATA" SECTIONS BELOW, FREE TRIAL SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY AND DRATA SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO THE FREE TRIAL SERVICES UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW IN WHICH CASE DRATA'S LIABILITY WITH RESPECT TO THE FREE TRIAL SERVICES SHALL NOT EXCEED $1,000.00. WITHOUT LIMITING THE FOREGOING, DRATA AND ITS AFFILIATES AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO CUSTOMER THAT: (i) CUSTOMER'S USE OF THE FREE TRIAL SERVICES WILL MEET CUSTOMER'S REQUIREMENTS; (ii) CUSTOMER'S USE OF THE FREE TRIAL SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR; AND (iii) USAGE DATA RELATED TO FREE TRIAL SERVICES WILL BE ACCURATE. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE "LIMITATION OF LIABILITY" SECTION BELOW, CUSTOMER SHALL BE FULLY LIABLE UNDER THIS AGREEMENT TO

DRATA AND ITS AFFILIATES FOR ANY DAMAGES ARISING OUT OF CUSTOMER'S USE OF THE FREE TRIAL SERVICES.

SECTION 10. INTELLECTUAL PROPERTY RIGHTS 10.1 Intellectual Property Rights. Each Party shall retain all rights, title and interest in any and all of such Party's respective Intellectual Property Rights. The rights granted to Customer and Users to use the Service(s) under this Agreement do not convey any additional rights in the Service(s) or in any Intellectual Property Rights of Drata associated therewith. Subject only to limited rights to access and use the Service(s) as expressly stated herein, all rights, title and interest in and to the Services and all hardware, Software and other components of or used to provide the Services and Drata's machine learning algorithms, including all related Intellectual Property Rights, will remain with Drata and belong exclusively to Drata. 10.2 Feedback. Drata shall have a fully paid-up, royalty-free, worldwide, transferable, sub-licensable (through multiple layers), assignable, irrevocable and perpetual license to implement, use, modify, commercially exploit, incorporate into the Services or otherwise use any suggestions, enhancement requests, recommendations or other feedback regarding the Services that Drata receives from Customer, Users, or other third parties acting on Customer's behalf. Drata also reserves the right to seek intellectual property protection for any features, functionality or components that may be based on or that were initiated by suggestions, enhancement requests, recommendations or other feedback regarding the Services that Drata receives from Customer, Users, or other third parties acting on Customer's behalf.

10.3 Aggregated Information. Drata may aggregate, collect and analyze information relating to the provision, use and performance of the Services and may use (during and after the Term) such information to develop and improve the Services and other Drata offerings, including disclosure of such information to third parties in an aggregated and anonymized format such that no Customer nor any individual or household can be identified.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L16 – Service Category 16: Enterprise Security Log Management, Analytics, and Response

Respondent Name: R2 Unified Technologies

Solution Name: Arctic Wolf Managed Detection and Response

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Enterprise Security Log Management, Analytics, and Response consists of multiple components that support and provide enterprise security operations, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and backend capabilities for log collection, storage, aggregation and analytics. This service category enables organizations to monitor, detect, and respond to security threats and provide operational visibility across their technology infrastructure.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

The Arctic Wolf Managed Detection and Response service includes the above mentioned components and implements them as follows:

Arctic Wolf is a SaaS based solution. The Security Operations Cloud platform is hosted entirely in AWS and as such does not require any design, implementation, or ongoing maintenance by the State of Florida or a SIEM to host. The performance, availability and capacity management of the Arctic Wolf Cloud platform is solely the responsibility of Arctic Wolf and is included as part of solution costs. The platform and associated detection logic is continuously being updated (as new threats and indications of compromise are discovered).

The Arctic Wolf Security Operations Cloud is built on an open XDR architecture, solving the biggest challenge organizations face in cybersecurity: collecting and storing security data across attack surfaces in real time; enriching, analyzing, and investigating this data; and using both machine automation and humans to respond decisively to threats and attacks.

The platform processes over 700 billion security observations per day. The cloud native scaling of our platform ensures all events are processed in near real time regardless of ingestion rate. This means you security observations are analyzed without delay. Security logs can be retained for up to 10 years in the Arctic Wolf platform and all retained logs are user searchable at any time.

The Arctic Wolf service is security tooling vendor agnostic, we can accept any security telemetry into our platform but have integration with many leading security tools across endpoints, network, cloud, and identity. We can ingest any security syslog from your environment via our network sensor(s). The sensors will securely transport these to our Security Operations Cloud platform.

Arctic Wolf Active Response has a number of SOAR capabilities that can be executed by Arctic Wolf Triage personnel as part of the proposed MDR service. Endpoint Active Response includes host containment (through supported EDR vendors or the Arctic Wolf Agent). Identity Active Response includes Disable and Enable users, close user connections. Network block can block internet bound traffic if a network sensor is deployed at the internet egress point.

Ingested data is parsed, enriched with metadata and attribution, and analyzed using multiple techniques including AI/ML, UEBA, custom and static rulesets. Any security event of interest elevated from the platform is always reviewed by a Triage Security Analyst/Engineer prior to customer escalation. Threat intelligence consists of a combination of Arctic Wolf Labs, intelligence from Arctic Wolf Incident Response, plus commercial threat intelligence feeds.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Data Collection and Aggregation – Solution should gather log data from multiple sources, including endpoints, servers, and applications, centralizing them for analysis. It supports structured and unstructured log formats like Syslog and JSON and provides or integrates with cybersecurity analysis solutions (such as SIEM).

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Broad visibility: We have integrations with many popular security tools and also integrate with productivity tools like O365. This gives us maximum visibility and ensures the fastest time to detection and remediation. Log source categories include Endpoint (EDR & Arctic Wolf Agent), Network (i.e. FW logs, AW network sensor), Cloud (i.e. AWS, Azure, O365), and Identity (I.e. OKTA, EntraID). Log ingestion happens via API integration with supported tools or via Syslog.

Prompt 3: Long-Term Data Storage – Solution should provide scalable storage solutions like data and security lakes and archiving to ensure long-term retention of logs for compliance purposes. This includes cloud and on-premises storage with secure, tamper-proof archiving. Options including long-term/cold storage should be available.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

The Arctic Wolf platform is fully hosted in AWS. All raw logs ingested into the platform are being retained for the duration of the contracted retention period (90 days - 10 years). All ingested logs are searchable across the entire retention period at any time (no storage tiers).

Prompt 4: Security Event Correlation - Solution should provide real-time event correlation, detecting complex attacks and anomalies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Ingested data is parsed, enriched with metadata and attribution, and analyzed using multiple techniques including AI/ML, UEBA, custom and static rulesets. Any security event of interest elevated from the platform is always reviewed by an Arctic Wolf Triage Security Analyst/Engineer prior to customer escalation. Threat intelligence consists of a combination of Arctic Wolf Labs, intelligence from Arctic Wolf Incident Response, plus commercial threat intelligence feeds.

Prompt 5: Big Data Engine – Solution should process and analyze large volumes of security data in real time. By leveraging distributed computing frameworks this component enables complex

threat detection, pattern recognition, and predictive analytics across large data sets. Provide training data sets to reduce false alerts and optimize efficiency of the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Through our real-time pipeline of ingest, parse, and analyze we currently ingest over 700 billion observations daily, and after parsing, enriching, analyzing (including AI/ML) we get to around 90,000 high alerts/investigations humans review every day. Out of that we escalate around 6000 security incidents each day within our entire customer base. The sheer size of our customer base and dataset positions us uniquely to train our AI/ML models and reduce false alerts.

Prompt 6: Microservices Architecture – Solution should provide a modular approach to security operations, allowing individual services (e.g., log collection, incident response, threat detection) to operate independently. This architecture ensures scalability and flexibility, allowing organizations to adapt to evolving security needs without overhauling the entire system.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Our Security Operations platform is hosted entirely in AWS and as such does not require any design, implementation, or ongoing maintenance by the State of Florida. Arctic Wolf has approximately 500 engineers in R&D responsible for running the platform and continual enhancement through additional integrations and threat detection rules. State of Florida will benefit from inherited characteristics of our SaaS platform i.e. availability, resilience, and enhancements.

Prompt 7: Monitoring and Threat Detection – Solution should provide continuous real-time monitoring with customizable alerts and advanced analytics that identify threats using machine learning, AI, and behavioral analysis. Integration with threat intelligence ensures proactive threat detection and enriched security alerts with additional threat intelligence.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Ingested data is parsed, enriched with metadata and attribution, and analyzed using multiple techniques including AI/ML, UEBA, custom and static rulesets. Any security event of interest elevated from the platform is always reviewed by a Triage Security Analyst/Engineer prior to customer escalation. Threat intelligence consists of a combination of Arctic Wolf Labs, intelligence from Arctic Wolf Incident Response, plus commercial threat intelligence feeds.

Prompt 8: Log Management. Solution should provide centralized or federated management of logs, enabling real-time indexing and analysis of security events. It ensures that logs are stored and managed according to compliance standards, with flexible retention policies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

All customer logs ingested into the Arctic Wolf platform are stored and retained for the contracted retention period and fully searchable by customer.

Prompt 9: Incident Response and Automation - Solution should automate responses, isolating compromised systems or blocking malicious activity based on predefined playbooks. Incident management tools provide a centralized view of security events from detection to resolution.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Arctic Wolf Active Response has a number of SOAR capabilities that can be executed by Arctic Wolf Triage personnel as part of the proposed MDR service. Endpoint Active Response includes host containment (through supported EDR vendors or the Arctic Wolf Agent). Identity Active Response includes Disable and Enable users, close user connections. Network block can block internet bound traffic if a network sensor is deployed at the internet egress point.

Prompt 10: Case Management and Collaboration – Solution should track incidents through case management, documenting all actions taken for compliance. Collaboration tools ensure effective communication among security team members.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

If through the forensics process it is deemed a security incident needs to be raised to the customer, the CSE will create a ticket based on the agreed upon escalation chain. Arctic Wolf tickets include remediation steps and evidence navigator and also document SOAR actions taken by the Arctic Wolf triage engineer. All tickets including attachments and documentation remain available to the customer throughout the contract lifetime.

Prompt 11: Analytics and Reporting – Solution should provide powerful tools for transforming raw security data into meaningful insights. Customizable dashboards and reports help security teams and decision-makers visualize security metrics, alerts, and trends in real time. End User integration allows the platform to connect with business intelligence (BI) tools for further analysis and reporting.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

The Arctic Wolf customer portal allows for the creation of custom Dashboards where customers can build widgets with queries to display the desired parameters in the dashboard(s). Dozens of standard reports are available and custom reports can be generated upon request by the assigned Concierge Security Team.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Arctic Wolf Managed Detection and Response Solution Terms (these terms can also be found at https://arcticwolf.com/terms/solutions-terms/managed-detection-and-response/

(password: "mdr2024")

Last Updated Date: June 2024

This Managed Detection and Response – Solution Terms ("Solutions Terms") describes the Managed Detection and Response Solution (the "Solution"). The Solution, if purchased by Customer as evidenced by Customer's election on an Order Form, will be provided in accordance with the terms set forth herein and the Solutions Agreement (the "Solutions Agreement") made by and between Customer and Arctic Wolf Networks, Inc. ("Arctic Wolf"). Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Solutions Agreement.

Solution. The Solution may be licensed separately or as part of a Security Operations Bundle as more fully described at https://arcticwolf.com/terms/bundles-tiers/ (each a "Bundle") and includes the following Components:

Component

Software The object form of any software, including any operating system software included in the Equipment, and add-ons offering enhanced features and functionality made generally available to Arctic Wolf customers from time-to-time

Equipment Virtual appliances or physical sensors

Services Support, onboarding services, and services provided by Security Services, all as described herein, and Cyber Resilience Assessment ("CRA")

Platform One (1) vSensor 100 series

Unlimited data ingestion

Access to the Customer Portal

Use of the Arctic Wolf Agent

ITSM Ticketing Integrations (if elected by Customer)

90-day Log Retention (unless another retention period is purchased by Customer and set forth on an Order Form)

The Solution is delivered by the Security Services team which is comprised of two (2) teams: (1) the Concierge SecurityTM Team ("CST"), and (2) the Security Operations Center ("SOC").

Specific features and functionality provided as part of the Solution include:

• collection of Solutions Data and Points of Contact Information, including Customer's system logs, from Customer's systems using Equipment,

• analysis by Arctic Wolf Security Services of both Equipment and log data through the correlation of Solutions Data with threat and vulnerability information,

• scanning of Customer's internal and external systems,

• escalation of Security Incidents (as defined below) in need of attention by Customer as set forth herein,

• advisory recommendations intended to improve Customer's security robustness,

• calculation of Customer's Security Score, as more fully described below,

• Access to additional modules, if licensed by Customer as reflected on an Order Form (as more fully described below)1,

• Response Actions2 (as more fully described below),

• Cyber Resilience Assessment ("CRA") subject to the terms set forth at https://arcticwolf.com/terms/cyber-jumpstart-portal-subscription-agreement/, and

• regular summary Executive Dashboard reports, as described herein and the Documentation.

NOTE: The performance of the Solution, including specifically, notification of Emergencies or Security Incidents, as defined below, will not commence until after initial deployment is complete. The performance of (i) remediation services for Security Incidents (as defined below), (ii) the re-imaging of Customer's systems, or (iii) change of policy settings is outside the scope of the Solution.

Data Transfer. Any Equipment provided by Arctic Wolf to Customer is physically or virtually deployed to monitor Customer's system traffic. Such system traffic is augmented with additional sources of log data, as required, to deliver the Solution. Except as otherwise set forth in the Solutions Agreement, all such system traffic information is deemed Solutions Data. Essential log sources will be determined by Customer and Arctic Wolf during the onboarding process following the Order Form Effective Date.

Any Solutions Data and Points of Contact Information will be securely transmitted to Arctic Wolf in accordance with the Agreement. The Solution operates redundantly with Customer's High Availability (HA) specifications to minimize potential service interruptions. Hosting providers used by Arctic Wolf to deliver the Solution may experience service interruptions and service outages outside the control of Arctic Wolf. If such a hosting provider issues an outage notice that could materially impact delivery of the Solutions, Arctic Wolf will use commercially reasonable efforts to promptly notify Customer about the outage and communicate the planned recovery time provided by the hosting provider.

Solutions Data and Points of Contact Information may include personal or confidential information. Customer will provide any such personal or confidential information in accordance with the terms of the Solutions Agreement.

Data Retention. Arctic Wolf will store Solutions Data and Points of Contact Information for the Data Retention period specified in Customer's then-current Order Form. Solutions Data and Points of Contact Information may be returned to Customer in accordance with the terms of the Solutions Agreement.

Data Storage. Arctic Wolf will store raw Solutions Data and Points of Contact Information in the platform location set forth on an Order Form.

Updates & Upgrades. Automated maintenance and update cycles to the Equipment will be performed remotely by Arctic Wolf Security Services. Arctic Wolf will provide any services related to the replacement or upgrades of the Equipment. Any costs related to such Equipment replacement or upgrades will be in accordance with the Solutions Agreement.

Security Incidents. The CST supporting Customer is available 8:00 am to 5:00 pm (based on the time zone within which the CST is located), Monday through Friday (excluding holidays) and will provide Concierge Security™ Tier support in accordance with the Concierge Security™ Tier selected by Customer, as applicable. The SOC is available 24 hours a day, 7 days a week, including holidays. Customer may schedule specific activities with their CST, in accordance with Customer's Concierge Security™ Tier, as applicable, by contacting the Arctic Wolf SOC at security@arcticwolf.com. Arctic Wolf Security Services will acknowledge any schedule request submitted by Customer to security@arcticwolf.com within one (1) hour of receipt of such request. Arctic Wolf Security Services will provide an estimate of response time determined by scope, size, and urgency.

Arctic Wolf Security Services will notify and escalate to Customer any Security Incidents, the definition of which will be agreed upon by Customer and its CST during the Subscription Term after transition from the deployment team, discovered by Arctic Wolf within two (2) hours of Arctic Wolf's discovery of such Security Incident. Arctic Wolf standard Security Incident notification process is through a ticket to the Customer; however, Arctic Wolf and Customer may agree to alternate notification processes. Security Incident notifications will include a description of the Security Incident, the level of exposure, and a suggested remediation strategy. Customer is responsible for implementing, in its sole discretion, any remediation strategies identified by Arctic Wolf. Customer may request validation by Arctic Wolf that any such implemented remediation strategies are working as expected.

Emergencies. Following transition from the deployment team to the CST, Customer and the CST will agree on and document which Security Incidents will be defined as an "Emergency". Emergencies will typically include the discovery of ransomware and other alerts that could cause degradation/outage to Customer's infrastructure security. Arctic Wolf will escalate Emergencies to Customer within thirty (30) minutes of Arctic Wolf's discovery of the Emergency.

Any Emergency identified by Customer can be escalated to Arctic Wolf's Security Services by calling: 1-888-272-8429, option 2 or by calling the toll-free number based on the location from which you are calling found at https://arcticwolf.com/toll-free/. Customer must describe the Emergency in the initial call and Arctic Wolf will respond within 5 minutes. In addition, with respect to any urgent inquiries, Customer may contact Arctic Wolf's Security Services by calling: 1-888-

272-8429, option 2 or using the applicable toll-free number for the location from which Customer is located as set forth at https://arcticwolf.com/toll-free/.

Ticketing Integration (included in the Platform component of the Solutions). At Customer's election and based on configurations and permissions collected from Customer, Arctic Wolf may employ an integration to transfer data into and out of Customer's third-party ticketing system, provided Arctic Wolf supports integrations to such systems.

Scans. On a monthly basis, Arctic Wolf will use the Solution to conduct external vulnerability assessment scans of Customer's environment. As part of these scans, vulnerability and exploit information will be normalized and correlated with other data sources to determine Customer's Security Score and prioritization of any identified remediation strategies. Arctic Wolf will deliver to Customer a summary security report that includes Security Incident and Emergency notification activities on a monthly and quarterly basis.

Coverage Score (fka Configuration Score or Security Score). Customer's Coverage Score is provided as part of the Solution for illustrative and informational purposes only and may be used by Customer for internal benchmarking. The Coverage Score is based on certain information related to the results of the Solution within Customer's environment and is compiled using the Solutions Data made available to Arctic Wolf in conjunction with its delivery of the Solution. Customer's Coverage Score will be communicated in Customer's summary reports in addition to being available on Customer's online Executive Dashboard. Customers may elect to compare their Coverage Score against industry averages from organizations in the same industry vertical to assess how Customer is performing against industry norms.

Response Actions. Arctic Wolf may, if agreed with Customer, using commercially reasonable efforts, perform response actions, including application/removal of host containment, enable/disable user accounts, block URLs, modify deny lists and iprules, retrieve files, kill processes, and run files or scripts, as described below (collectively, "Response Actions"), provided that Customer has deployed the Arctic Wolf Agent, such other agreed upon third party agents, and/or configured the appropriate integrations. In the event Customer has deployed multiple agents, including the Arctic Wolf Agent, within its environment, Arctic Wolf will attempt to contain first using the Arctic Wolf Agent. Based on (i) information provided by Customer to its CST following initial deployment, (ii) a mutually agreed upon response and escalation process set forth in Customer's onboarding document, as updated upon agreement by Customer and its CST during the Subscription Term, and (iii) Arctic Wolf is provided appropriate access to applicable third party security applications, if any, within Customer's environment, the Security Services team may remotely isolate a Customer endpoint device(s), network appliance, or user account that shows evidence of compromise or other suspicious activity. When the Security Services team identifies certain indicators of attack on an endpoint, network device, or user account, the Response Action will be initiated systematically, in accordance with the agreed upon response and escalation process, and subject to the requirements set forth herein, to rapidly quarantine the suspected compromised system or account.

The indicators of attack that may drive Response Actions include those relating to ransomware (and other types of advanced malware), malicious command-and-control (C2) activity, or active data exfiltration attempts.

The endpoints, network, or user accounts participating in the Response Actions will receive a notification and the Response Actions will be detailed in an incident ticket. If using the Arctic Wolf

Agent, the Customer Portal will display the Customer endpoints that are currently in a contained state. Security Services team is available to Customer to answer questions or provide detailed information on any endpoints, network, and/or user accounts participating in the Response Action.

Pre-requisites for Response Actions –

Customer must:

• Complete a checklist in partnership with its CST, which will include further definition, including but not limited to the scenarios where Arctic Wolf will and will not perform Response Actions including specific information regarding which endpoints/servers, network appliances, and/or user accounts where Response Actions will and will not be performed, the times of day for Response Actions to occur, notification and escalation preferences related to Response Actions (If parties have not defined the Response Actions pertaining to Customer endpoints, network, and/or user accounts, Arctic Wolf will take Response Actions in accordance with Arctic Wolf's standard response and containment policy);

• Provide Arctic Wolf with technical permissions to allow Arctic Wolf to perform Response Actions within Customer's environment (Customer understands that should Arctic Wolf have invalid access or is blocked from initiating Response Actions, Arctic Wolf will be unable to provide the agreed upon Response Actions);

• Implement appropriate internal procedures and oversight to the extent Customer utilizes the configuration of workflows and processes, including but not limited to Response Actions and other similar functionalities; and

• Enable software or services, in Customer's discretion, to permit necessary visibility into Customer's environment to perform Response Actions.

Active Directory Deception. If licensed and implemented by Customer either as a standalone or bundled feature within the Solution, Customer may deploy Active Directory Deception ("AD Deception"). With AD Deception, Customer creates, configures, and maintains Active Directory decoy account(s) intended to act as a deception trap within Customer's network.

The Active Directory decoy account is not intended to participate in normal business activities and should not log-in to Customer's system. The Active Directory decoy account is intended to provide a high-fidelity mechanism for detecting abnormal activity yielding no false positives. If a decoy account is deployed by Customer, Customer is responsible for creating, configuring, and maintaining the decoy account. The naming of the decoy account should follow Customer's account naming conventions. Arctic Wolf will provide reasonable guidance and assistance to Customer in the configuration of such decoy accounts. Customer will provide Arctic Wolf details of the decoy account to Arctic Wolf for monitoring. Customer understands that any changes to the decoy account configurations may impact the security of Customer's environment.

Microsoft US Government Community and High US Government Community Environment Monitoring. In the event Arctic Wolf monitors applications for Customer within the Microsoft US

Government Community environment or US Government Community High environment (each a "GCC environment") as part of the delivery of the Solutions, Customer understands and agrees as follows:

1. Arctic Wolf is not FedRAMP compliant.

2. Only Arctic Wolf supported and integrated applications will be monitored in the GCC environment.

3. Solutions Data (i) may be accessed by Arctic Wolf, its Affiliates, and any third-party providers, from locations outside the United States, and (ii) may be accessed by persons who are not United States citizens;

4. Arctic Wolf does not require access to or delivery of Customer's Controlled Unclassified Information ("CUI") and in the event information classified as CUI is provided, Arctic Wolf may immediately cease ingestion of Customer Solutions Data without further liability to Customer;

5. Arctic Wolf will provide reasonable cooperation to Customer in the event of a data breach involving Solutions Data including, but not limited to assistance in responding to any government or regulatory inquiries;

6. Certain Microsoft log sources may be in beta and, consequently, Arctic Wolf makes no representations as to the delivery of the Solutions related to any such beta Microsoft log sources; and

7. Customer will immediately notify Arctic Wolf of non-consent or any change in consent and any monitoring of Customer's GCC environment will immediately cease without further liability to Arctic Wolf.

Additional Modules.

• Cloud Detection and Response ("CDR"). Customers may license CDR for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud IaaS and SaaS environments that Arctic Wolf may agree to monitor. Customer's election to license such CDR feature will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will provide detection and response for the respective IaaS and SaaS environments as described herein. Arctic Wolf is not responsible for any software and/or application changes made by the cloud IaaS and SaaS providers which affect or impair the CDR feature.

• Data Explorer. Customer may elect to license the Data Explorer feature. Should Customer subscribe to such feature, Data Explorer will be included on an Order Form. Data Explorer allows Customer to access historical data for quick, ad-hoc investigations and self-service reporting.

Customer may identify and remediate risk in Customer's environment and may take appropriate actions when needed depending on results. Data Explorer includes (i) access to the prior ten (10) days of event and analyzed data, and (ii) Log Search 3 which permits Customer to query its retained Solutions Data in 30-day increments.

• Data Explorer – Lite. Customers licensing MDR as part of a Bundle will receive Data Explorer – Lite which includes access to the prior three (3) days of event data.

For purposes of Data Explorer and Data Explorer-Lite, analyzed data includes parsed, normalized, and enriched data processed by the Arctic Wolf platform, however, not all logs ingested by Arctic Wolf will be parsed, normalized, or enriched. Event data is a collection of analyzed observations Arctic Wolf finds to be interesting from a security standpoint.

• Application and SaaS Integrations. Customers may license application and SaaS integrations as may be offered by Arctic Wolf. Customer's election to license such integration will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will provide detection and response for the respective integrated environments as described herein. Arctic Wolf is not responsible for any software and/or application changes made by the third-party application provider which affect or impair the integration with such third-party application.

1 Existing Arctic Wolf MDR Customers may be, subject to authorization by Arctic Wolf, eligible to license Log Search capabilities only. In such event, Log Search will be included on an Order Form.

2 Response Actions were formerly referred to as Host Containment Actions.

3 Legacy customers licensing Log Search are entitled to Log Search only.

Any applicable Addtional Terms and Conditons Goes Here

Arctic Wolf's terms and conditions for the provision of its solutions to its customers can be located at https://arcticwolf.com/terms/msa/. If down selected, we are confident we would be able to reach agreement with The State of Florida, Department of Management Services on acceptable terms to govern our relationship.

Digital Security Solutions

RFP No. 24-43230000-RFP

Attachment L16 – Service Category 16: Enterprise Security Log Management, Analytics, and Response

Respondent Name: R2 Unified Technologies

Solution Name: Singularity Data Lake (SDL)

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Enterprise Security Log Management, Analytics, and Response consists of multiple components that support and provide enterprise security operations, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and backend capabilities for log collection, storage, aggregation and analytics. This service category enables organizations to monitor, detect, and respond to security threats and provide operational visibility across their technology infrastructure.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Singularity Data Lake (SDL) is a next generation AI SIEM that leverages the power and scale of the Singulairy XDR platform to add data from 3rd party sources right into the same data lake as the EDR data. Functionality is then built around the ingested data and API connectors to add context to existing EDR logs, take response actions directly from the S1 console, and build no-code/low-code automation (SOAR) from these same integrations.

SentinelOne's back end was rebuilt to support the OCSF framework as many other vendors have also standardized on. This makes integration simple with a large library of prebuilt integrations, but also supports ingestion via SysLog. What that means is that as an analyst is investigating an alert from the S1 console, whether it's from an S1 agent or a 3rd party, the relevant data is brought into a single place to begin an investigation.

From there an analyst can do all of the same investigating they would do on an endpoint but use the additional context from other data sources, like EntreID suspicious logins, to understand where the threat originated and understand the scope. Next, an analyst would be able to see the threat is related to 1 or a subset of users based on a variety of data (group, location, device type, etc) and take a response action. With EntraID that could include forcing a user to log out, force reset their password, and end their session. From one alert on a device now a breach from a compromised credential can be stopped and resolved.

Threat hunting and incident response is now done in one place across platforms from any source that has a built in integration, can leverage SysLog, or can be built upon request.

Not only that, but for organizations that are already invested Splunk, SDL can substitute Splunks storage at a fraction of the cost, eliminating the need to learn a new platform, reducing cost, and improving speed of the platform by an average of

PurpleAI can leverage its generative AI to do incident investigation, threat hunting, response actions, and summaries with natural language prompts. (add on) This levels up analysts to investigate with confidence, ask questions, and even help with support cases. Purple can also summarize events and make recommendations on next steps.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Data Collection and Aggregation – Solution should gather log data from multiple sources, including endpoints, servers, and applications, centralizing them for analysis. It supports structured and unstructured log formats like Syslog and JSON and provides or integrates with cybersecurity analysis solutions (such as SIEM).

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

SDL uses the Open-Source Cybersecurity Framework to ingest log data from a wide variety of sources. This can include APIs, SysLog and others. Data can be ingested via an integration in the marketplace or via syslog ingestor.

The GUI of SDL then makes that data easy to search, filter, sort, and understand for faster investigations, and the ability to take cross-platform response actions. This all reduces the Mean-Time-To-Response (MTTR) for an incident.

Prompt 3: Long-Term Data Storage – Solution should provide scalable storage solutions like data and security lakes and archiving to ensure long-term retention of logs for compliance purposes. This includes cloud and on-premises storage with secure, tamper-proof archiving. Options including long-term/cold storage should be available.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Retention is standard at 30 days but is available for up to 5 years for purchase. Inside of 1 year this includes unlimited queries. At 1 year the ingestion cost drops as the data is flagged for archival. The data doesn't actually move, but is only tagged. This means queries never slow down. Storage is only available in our FedRAMP High certified cloud storage. RBAC is also a part of the native multi-tenancy architecture.

Prompt 4: Security Event Correlation - Solution should provide real-time event correlation, detecting complex attacks and anomalies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Data can be ingested into SDL with a number of available functionalities that vary based on method, level of integration, and the sources own limitations. This ranges from pure ingestion to contextualization, response actions, and automation. These are clearly noted on each integration and the level of functionality with more details about them are all included in the Singularity Marketplace.

Prompt 5: Big Data Engine – Solution should process and analyze large volumes of security data in real time. By leveraging distributed computing frameworks this component enables complex

threat detection, pattern recognition, and predictive analytics across large data sets. Provide training data sets to reduce false alerts and optimize efficiency of the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

As a cloud based service, the computing is distributed across multiple availability zones and clusters, but all in the US to meet FedRAMP compliance requirements. The data doesn't need to be indexed making the services extremely fast and agile. Threat detection and analytics can therefore be done at machine speed as well. PurpleAI (add on) can also be used to comb through and identify risks using natural language.

Prompt 6: Microservices Architecture – Solution should provide a modular approach to security operations, allowing individual services (e.g., log collection, incident response, threat detection) to operate independently. This architecture ensures scalability and flexibility, allowing organizations to adapt to evolving security needs without overhauling the entire system.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Like the above, the cloud based service is built across multiple AZs and clusters allowing for unlimited scalability and is designed with a microservices architecture to achieve that scalability and flexibility.

Prompt 7: Monitoring and Threat Detection – Solution should provide continuous real-time monitoring with customizable alerts and advanced analytics that identify threats using machine learning, AI, and behavioral analysis. Integration with threat intelligence ensures proactive threat detection and enriched security alerts with additional threat intelligence.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

SDL unifies and extends detection and response capability across multiple security layers with centralized end-to-end visibility, powerful stream analytics, and automated response across the technology stack in real-time.

SDL offers a dashboard view, which is customizable per user. Users can also create multiple custom dashboards with widgets to quickly see the information that is most relevant to various stakeholders. Then STAR rules can automate responses. PurpleAI (add-on) supports this also.

Prompt 8: Log Management. Solution should provide centralized or federated management of logs, enabling real-time indexing and analysis of security events. It ensures that logs are stored and managed according to compliance standards, with flexible retention policies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Leveraging the OCSF architecture on a cloud based platform makes federated management simple with no need to do any indexing. This improves the responsiveness of the ingestion, queries, and usability immensely. Queries in other platforms that take hours can now be done in seconds. Role-Based Access Control is also a part of our native multi-tenancy architecture.

All of this is compliant with FedRAMP.

Prompt 9: Incident Response and Automation - Solution should automate responses, isolating compromised systems or blocking malicious activity based on predefined playbooks. Incident management tools provide a centralized view of security events from detection to resolution.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

SDL offers custom configurable policies to automatically terminate malicious processes and automatic incident response tools that can isolate infected endpoints to prevent lateral movement. SentinelOne does offer IR playbooks that are part of a comprehensive incident response process that includes various steps such as incident reporting, response, and post-incident follow-up.

Incident Reports generated by the MDR team contain details about the actions taken during IR, including escalation steps, network isolation, remediation actions and recommended actions to reduce the likelihood of similar incidents in the future.

Prompt 10: Case Management and Collaboration – Solution should track incidents through case management, documenting all actions taken for compliance. Collaboration tools ensure effective communication among security team members.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

A full integration with JIRA is made available for the full automation of ticketing and case management. There are also ServiceNow integrations.

Integrations with other collaboration tools like Teams and Slack are also available to alert analysts or relevant stakeholders to an alert or incident.

Prompt 11: Analytics and Reporting – Solution should provide powerful tools for transforming raw security data into meaningful insights. Customizable dashboards and reports help security teams and decision-makers visualize security metrics, alerts, and trends in real time. End User integration allows the platform to connect with business intelligence (BI) tools for further analysis and reporting.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Custom dashboard and detailed reports, including threat, application, and executive reports, are available out of the box. Additionally, a variety of business value and estate health reports are available to customers through the digital Customer Community. Users can create custom dashboards or use dashboards provided in the Library or SentinelOne github repo.

SDL as a point of ingest and analytics is capable of doing the analysis natively and PurpleAI (add-on) can simplify that with LLM tools.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Management Console:

SentinelOne provides a 99.5% uptime for the Management Server and Console.

SentinelOne Agents are autonomous and continue to provide protection and detection, even when the Management is undergoing maintenance.

The maintenance window below is not included in this SLA.

Maintenance Window:

SentinelOne reserves the right to perform maintenance operations on Sundays:

Maintenance Start: 10:00 UTC+3

Maintenance End: 18:00 UTC+3

Maintenance Stages:

SentinelOne does our best to limit actual customer downtime to two hours every other week.

Global and Regional Infrastructure Maintenance - Customers have access to their Management Console but specific cloud services might be unavailable intermittently. This can affect all customers, starting at 9:00.

Global and Regional infrastructure maintenance typically runs for two hours, but it can continue until 18:00.

Specific Customer Maintenance - Only specific customers are affected while their management is undergoing maintenance. During a customer's maintenance slot, they might not be able to access their Management Console. SentinelOne Agents continue to provide protection and detection.

Customer maintenance slots begin as soon as the Global and Regional infrastructure maintenance is completed, and end by 18:00. Slots are scheduled by region, so that downtime is as convenient as possible. The euce1-100 and euce1-102 are updated from 17:00 until 19:00.

Any applicable Addtional Terms and Conditons Goes Here