Exhibit D

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: TelaForce, LLC

Solution Name: ServiceNow Discovery, SecOps, ITAM, and ITOM

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.

Utilizing ServiceNow Discovery, we can identify endpoints on a network, and proceed to collect and aggregate endpoint information from all devices on the network such as Laptops, Desktops, Servers, and other network connected devices. The Agent runs on devices while using the least amount of system resources necessary, avoiding any noticible impact to network or system performance.

Using ServiceNow, we deploy a Management, Instrumentation, and Discovery (MID) Server(s) in any network and support Windows, OSX, and Linux devices. The MID server uses agent-based and agentless tools to identify devices on a network and retrieve information about the asset. Discovery begins by scanning the internal IP ranges of the network to identify assets and then scan standard ports to see what protocols can be queried to determine what operating system (OS) is used on the device and what applications may be running. After the classification phase, the MID server connects using Windows Management Instrumentation (WMI) and Secure Shell (SSH) for Windows and Linux devices to determine if each asset has the necessary credentials to run commands on the device.

We have expensive experience deploying and managing agent-based and agentless solutions using both ServiceNow Discovery to discover and catalog devices in a network. Our solutions operate as efficiently as possible to transmit only newly discovered information from assets, minimizing the impact that data transmission has on networks. We also utilize scheduling to ensure that agents run after hours or during low bandwidth usage periods for systems that are online consistently to further reduce the impact to available bandwidth on a network.

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.

ServiceNow Discovery runs on set schedules and there is no limit to the number of schedules that can be defined. Using these schedules we can configure ServiceNow Discovery to continuously poll network assets to identify devices that are added to the network in as close to real time as possible, ensuring that your network map is complete and up-to-date at all times. Once new assets are identified, a new record is created and detailed asset information is added.

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.

After discovering assets on a network, agentless, and agent-based probes can be used to gather configuration data and log information for each asset on the network and provide insight into the health of each device, gather data on installed software, patch data, and provide usage metrics. To reduce the amount of bandwidth that is utilized when transmitting data, only new data collected since the collector was last run on a device is transmitted.

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.

ServiceNow allows customers to create custom classifications for each asset and set up rules that allow assets to be categorized or tagged so tags can be based on data retrieved from or about the system, or based on rules created by the user based on the system data. Once the data is parsed or assigned using rules, it can be added to the record of the asset in the system to allow administrators to track it more easily and use the data elements in reports if they want.

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 ServiceNow Agent can collect event information from devices and transmit that information back to ServiceNow for processing and analysis. based on that data servicenow can determine if an asset may be experiencing issues and displays that information on a centralized dashboard for analysis and remediation. Alerts can also be sent out to users, and automated remediation actions can be defined for common health issues.

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.

ServiceNow offers several Out of the Box dashboards for viewing assets in the network, and their statuses. ServiceNow also gives you the ability to define your own custom dashboards with pre-

made metrics, or using your own custom defined metrics. Using these dashboards you can monitor all discovered endpoints as well as any related information you wish to see such as system health, patching information, or open tickets related to an asset.

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 ServiceNow Security Operations (SecOps) suite provides a comprehensive view of a client's asset security posture and consolidate security data from across the entire IT infrastructure including out of date software and OS's. This enables security teams to quickly detect, investigate, and respond to security threats, with the goal of minimizing the impact of security incidents and reducing overall risk.

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.

Using ServiceNow Security Operations (SecOps) suite along with integrations to supported EDR tools, we can provide a streamlined System that can collect event information, detect issues on endpoints, and provide automated and manual threat response capabilities. The SecOps suite integrates with EDR tools to collect endpoint data, behavioral analysis, Machine Learning (ML) analysis, Indicators of Compromise and checks against published CVE's.

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.

ServiceNow ITOM allows an organization to deploy patches for both OSs and installed applications to devices using integrations with existing patch management platforms such as SCCM, Intune, and Qualys using the Orchestration module. Servicenow offers Out-of-the-Box integrations with several patch management tools and allows admins to define new patch releases in the patch platform using orchestration, and displays deployment progress on dashboards in ServiceNow.

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.

ServiceNow's Orchestration platform allows users to display Patch, Vulnerability, and Deployment metrics across the entire network using dashboards hosted on the ServiceNow Platform. Using dashboards in ServiceNow administrators can track the status of deployments, patch compliance and system health. ServiceNow comes with pre-built dashboards to help track deployment information but administrators can also create their own dashboards and metrics if they wish.

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 L2 – Service Category 2: Network-Based Asset Discovery

Respondent Name: TelaForce, LLC

Solution Name: ServiceNow Discovery and SecOps

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.

ServiceNow Discovery supports agentless identification of Windows, OSX, Linux, Android, and iOS devices on the network. Using agentless discovery methods, we can simplify network asset discovery and minimize the impact that our discovery process has on the devices it identifies and retrieves data from. Using this data and traffic driven approach to network discovery we can detect the existence of any IP devices on a network. Discovery allows us to deploy a Management, Instrumentation, and Deployment (MID) Server that can authenticate with the network switches to retrieve a full map of a clients network topology, connecting to each device as they are identified in the routing table and then querying the device using standard protocols such as RCP or SSH to determine if the port is open and accepts queries to identify all devices in each network segment and begin classifying them.

During the classification phase, the MID server can connect using WMI for Windows Devices and SSH for OSX and Linux devices to gain additional information about each asset if it has the necessary credentials to run commands on the device. After discovering assets on a network, agentless probes can be used to gather configuration data and log information for each asset on the network and provide insight into the health of each device, what applications are installed, the make and model of the device,and whether it is a virtual device or not. We also use these tools to identify devices that are communicating with each other and on what ports so that we can automatically begin to build out a service map of their internal infrastructure and applications traffic. This data is transmitted back to ServiceNow via the MID server and only data collected since the collector was last run is transmitted, reducing the bandwidth use on the network.

Devices that do not match a current classification model can be reviewed and new classification models can be created to help continue to capture and track new types of equipment as it is added to the network. This can help administrators track device types that do not have classifiers already defined for them such as IOT devices and mobile devices if there are no Out of the Box classifiers defined for them.

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.

ServiceNow Discovery supports agentless identification of devices on the network. Using agentless discovery we can monitor network traffic to detect the existence of any IP devices on a network. These tools identify devices that are communicating with each other and on what ports. Using that information we can automatically begin to build out a service map of their internal infrastructure and what applications are in use based on what ports the traffic moving over.

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.

Discovery allows us to authenticate with the network switches to retrieve a full map of a clients network, connecting to each device as they are identified in the routing table and then querying the device using standard management protocols such as RCP or SSH to determine if the port is open and accepts queries to identify all devices in each network segment and begin classifying them and fill in device information for the newly created CMDB record.

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.

Discovery allows us to retrieve data from network switches to create a full map of a clients network, connecting to each device as they are identified in the routing table. We retrieve MAC and IP information and then query the device using standard management protocols, determining if the port is open and accepts queries and then run OS specific queries to get detailed asset information and installed applications.

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.

Data retrieved by Discovery is stored in the ServiceNow CMDB.Using the CMDB provides out of the box visualizations of network health so network administrators can monitor the entire network and Identify issues efficiently. The CMDB provides feature-rich analysis of collected network data and asset health and provides outage detection, impact analysis, automated alerting, and service mapping. Clients can also define custom dashboards to create custom metrics and alerts.

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.

ServiceNow discovery allows users to add custom logic based on the data gathered by Discovery to add additional data to CMDB records. Transform Maps can populate Out of the Box fields on a record, or custom fields. Using this tool you can parse out data from any collected information such as naming conventions from asset tags having department information, or network information relating back to a specific physical location.

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.

The ServiceNow Security Operations (SecOps) suite provides a comprehensive view of your asset security posture and consolidate security data from across the entire IT infrastructure including misconfigured devices, out of date software, and Operating Systems. This enables security teams to quickly detect, investigate, and respond to security threats, with the goal of minimizing the impact of security incidents and reducing overall risk.

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.

Using ServiceNow Security Operations (SecOps) suite along with integrations to supported EDR tools, we can provide a streamlined System that can collect event information, detect issues on endpoints, and provide automated and manual threat response capabilities for flagged devices. The SecOps suite integrates with EDR tools to collect endpoint data, behavioral analysis, Machine Learning (ML) analysis, Indicators of Compromise and checks against published CVE's.

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 L3 – Service Category 3: Endpoint Detection and Response

Respondent Name: TelaForce, LLC.

Solution Name: SecOps, TISC, Orchestration, 3rd-party EDR tool

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.

Using ServiceNow Security Operations (SecOps) suite along with integrations to supported EDR tools, we can provide a streamlined System that can collect event information from a device, such as telemetry data, file access patters, process execution, network traffic and changes to the registry. With this data SecOps can detect issues on endpoints, and provide automated and manual threat response capabilities. The SecOps suite integrates with popular EDR tools such as MS Endpoint for Defender and Symantec Endpoint Protection to collect endpoint level data, behavioral analysis, Machine Learning (ML) analysis, and threat intelligence capabilities.

The SecOps Suite leverages integrations with these EDR tools to track configuration and event data from all integrated security tools in the network such as endpoint firewalls, EDR, and IDP tools to monitor for intrusion attempts, suspicious behaviour, changes to device configurations, and network level threats. SecOps can also ingest a machines application inventory to monitor what software is installed on a device and prevent unauthorized software from being installed. SecOps Integrations collect threat data from these tools to match threats using signature-based detection methods and collect data around software vulnerabilities and missing patches.

Once data is collected from EDR Tools, the SecOps suite automatically logs a security incident in the SecOps console and looks for automated and manual responses to the identified threats. Automated responses can include containing malicious runtimes, isolating devices on a network, and removing malware. If the respons is allowed to run automatically without approval from a security engineer it will do so and the outcome of the remediation attempt will be added to the incident. If automated remdiation fails or there is no automated remdiation defined for a threat, custom responses can be defined using playbooks in ServiceNow, allowing the security team to continually improve its automated and manual response capabilities.

When automated responses are not defined or not suitable for an identified threat, the console provides all relevant collected information to the security team along with remediation suggestions, allowing them to determine the best path forward and potentially create an automated response for similar threats in the future.

If automated responses are not feasible for any reason, manual responses can be created for identified threats to aid security personnel in responding and resolving threats as quickly as possible. Manual response runbooks can list the steps needed for a security engineer to resolve a threat and multiple response playbooks can be suggested to security engineers inside the automatically generated security incident if they are applicable to the threat remediation.

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 ServiceNow SecOps Suite allows customers to integrate with their existing EDR Tools to collect data that may indicate suspicious or malicious activity. The SecOps suite uses machine learning, behavioural analysis, published threat data, and indicators of compromise to analyze event, log,application, and network logs that could indicate security issues or that a device is compromised. Any potential issues automatically generate an incident in the SecOps console.

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.

The ServiceNow SecOps Suite allows customers to integrate with their existing security infrastructure to consolidate security data across the enterprise for analysis, visibility, and response. SecOps can integrate with firewalls, IDS/IPS, EDR, vulnerability scanning tools, network devices, and cloud hosted infrastructure. Ingested event information from all of those sources are analyzed and incidents are generated automatically if potential issues are detected.

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.

Once data is collected from integrated security tools, the SecOps suite enables the security team to define both automated and manual responses to identified threats from the SecOps Console. Automated responses include containing malicious runtimes, isolating devices on a network, and removing malware. Custom responses can be defined using playbooks in ServiceNow, allowing the security team to continually improve its automated and manual response capabilities.

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 SecOps Suite ingests event information from Security sources across the network and analyzes data using Machine Learning for Threat Pattern Recognition, Behavioral Analysis, Indicators of Compromise and other supicious activity. Once data is analyzed and potential threats are identified, security incidents are generated automatically and the security team can use automated and manual responses to identified threats from the SecOps Console.

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.

Devices outside the network can still be monitored if managed scanning tools are deployed to the device. EDR tools can still collect data for devices outside of the network and flow that information into SecOps for analysis. If remote machines also use VPNs to connect into the network traffic information and any collected security data from the VPN can also be integrated for threat analysis and detection in the same way as devices inside the network.

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.

Once data is collected from integrated security tools, the SecOps suite can provide the security team with manual remediation actions to identified threats when no automated responses have been defined or were successful. Manual responses can be generated from published threat remdiation information or created by the security team to address threats where the published remdiation steps are not effective or cannot be used.

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.

ServiceNow Threat Intelligence Security Center (TSIC) can integrate with multiple external threat intelligence feeds and correlate vulnerability and threat data in real time to improve threat detection and response for an organization. These CTI data feeds are correlated, de-duplicated and applied to security incidents to ensure that emerging threats, exploits, and malware campaigns are included in ongoing threat detection activities.

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.

The SecOps Suite provides comprehensive incident tracking. SecOps ingests data from security tools and automatically create incidents. Incidents can be created including the root cause analysis that generated the incdent and related event information that informed the analysis. Data can be correlated with other incidents of the same type to create a timeline of events and identify the scope of the threat to your organization.

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 L5 – Service Category 5: Email Security

Respondent Name: TelaForce, LLC.

Solution Name: SecOps,M365 Defender, M365 Purview, Orchestration

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.

Using ServiceNow SecOps suite along with integrations to external detection tools, we can provide a streamlined System that can collect threat data, provide reporting around email threat activity, and provide automated and manual threat response capabilities. The SecOps suite can integrate with popular EDR tools such as MS Defender for Endpoint in the MS Defender XDR Suite to collect endpoint level data and uses Machine Learning (ML) to perform threat scans using behavioral analysis and threat intelligence.

To secure email communications and protect against a wide range of email threats we utilize existing email security detection tools such as MS O365 Defender. For example, protecting clients against display name spoofing, suspicious links and domains in messages, scan attachments and links to phishing sites, and utilize AI/ML tools to constantly analyze sender and user behaviors for suspicious activities.

We can ingest existing email security data and automatically create security incidents when potential threats are identified. This allows Security teams to monitor email threats along with other types of security incidents. We can create parsing rules to classify alerts and populate extracted data into the security incidents in the SecOps console and automate responses such as alerting relevant stakeholders and executing remediation steps using integrations to EDR tools. This allows the security team to manage investigations, remediations, and reporting across all security incident types from a centralized platform.

Leveraging the many integrated features in MS O365 and Exchange Online to safeguard against business email compromise and other email-based threats we utilize the many integrated features in M365 and Exchange Online that fulfils the role of standalone third-party Secure Email Gateway (SEG) products. Features such as content filtering, perform malware scans, and utilize Automated Investigation and Response (AIR) tools in Defender for Endpoint Advanced Threat Protection (ATP) to identify a wide array of attacks. ATP automatically detects emails coming from the same sender to multiple recipients in the organization, and with a high confidence level automatically blocks them if they are determined to be spam. It also lets us view messages that were not flagged automatically for quarantine and review so that any and remove them from inboxes if the security team determines that they are malicious.

ATP also contains several tools to enable us to block spoofed messages using a variety of methods. Anti phishing policies in M365 Defender prevent and counteract phishing attempts, unauthorized access, and theft to catch messages sent from threat actors that are trying to either spoof the client's domain, or by spoofing a user's display name in the sender field of an email.

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.

Using ServiceNow and Defender XDR we can enable content filtering for inbound and outbound correspondence and actively scan for malicious links, attachments, and threat patterns and behaviors that require action to protect an organization. ServiceNow SecOps ingests that data to alert stakeholders of potential threats to the organization from email as well as other attack vectors such as attached storage, network intrusion and suspicious behavior analysis.

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.

Using MS Defender XDR and SecOps we leverage AI and ML based detection tools and awareness of active and previous malicious email campaigns to actively scan for and prevent phishing campaigns and improve threat awareness. The content of message data is analyzed for common indicators of attacks and new indicators gathered from recent or active threat actor activity. Identified threats generate incidents automatically into the SecOps console are quarantined for review.

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.

XDR protects users from malicious links and attachments by scanning all messages for potentially dangerous code. Anything found to have potentially harmful content is automatically Quarantined.Links in emails are protected using SafeLinks to scan pages opened from an email before it is loaded to identify if the site is malicious.Integrating with the SecOps platform,incidents are generated automatically for the security team to investigate and remediation actions can

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.

MS 365 and XDR utilizes tools to secure communications and prevent attacks such as business email compromise, phishing, and credential farming and integrate with SecOps to generate incidents for review. DMARC, DKIM, and SPF configurations can be used to intercept messages if they appear fraudulent or contain malicious attachments or links. XDR uses threat analytics and information on threat actors' active campaigns to maintain scanning definitions and anticipate new 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.

M365 Purview allow organizations to define Sensitivity Label policies that enforce encryption, watermarking, access, and transmission restrictions for emails that contain sensitive information. Users can manually apply a sensitivity label to a message, or automated labeling policies can be defined to apply labels to policies if the email contains types of data the policy is set to look for. When encryption is applied the message encryption is enforced at rest as well as in transit.

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.

Using the SecOps Platform, M365 and XDR allow organizations to define alert policies that automatically add warnings to emails received from outside the organization, or when an email may be suspicious.These warnings can be banners applied to messages, or actions taken automatically like removing content from an email or quarantining messages. Using the SecOps console we can aggregate these alerts along with other threat data to improve security awareness.

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.

Combining MS Defender and the SecOps Platform allows us to actively search for and analyze communications across an organization for potential threats. Defender XDR and Purview integrate with SecOps to create notifications and incidents when messages are quarantined or flagged for supcious content along with incidents generated by other security tools integrated to SecOps. Security Personnel can use the console to review and take action to remediate issues as necessary.

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 L7 – Service Category 7: Security Operations Platform

Respondent Name: TelaForce, LLC

Solution Name: SecOps,Threat Intelligence Orchestration

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.

The ServiceNow Security Operations (SecOps) suite provides a comprehensive view of a client's security posture and consolidates security data from across the entire IT infrastructure. This enables security teams to quickly detect, investigate, and respond to security threats, with the goal of minimizing the impact of security incidents and reducing overall risk. TelaForce will utilize and combine multiple security data sources and tools such as MS Defender for Endpoint, MS Defender for Cloud, MS O365 Compliance/Security Center tools integrated with the ServiceNow SecOps Suite, to provide insight into every level of your organizations security posture and give you rapid alerts for active threats.

Using the SecOps suite along with integrations to supported EDR tools, we can provide a streamlined platform that can collect event information, detect issues on endpoints, and provide automated and manual threat response capabilities. The SecOps suite can integrate with popular EDR tools such as MS Endpoint for Defender and Symantec Endpoint Protection to collect endpoint level data, behavioral analysis, Machine Learning (ML) analysis, and threat intelligence capabilities.

The SecOps Suite leverages integrations with these EDR tools to track configuration and event data from endpoint firewalls to monitor for intrusion attempts, and network level threats. It can leverage the existing malware, phishing, zero-day vulnerability, and insider threat detection capabilities of an industry standard EDR and provide a consolidated reporting and automation interface and automated security incident generation.

Once data is collected from EDR Tools, the SecOps suite enables the security team to define both automated and manual responses to identified threats from the SecOps Console. Automated responses can include containing malicious runtimes, isolating devices on a network, and removing malware. Custom automated responses can be defined using playbooks in ServiceNow, allowing the security team to continually improve its automated response capabilities and react to issues in real time.

When automated responses are not defined or not suitable for an identified threat, the console provides all relevant collected information to the security team along with remediation suggestions, allowing them to determine the best path forward and create an automated response for similar threats in the future.

Industry standard EDR tools such as MS Defender for Cloud will support multi-cloud deployments and enable threat analysis data to propagate back into the SecOps module for further action.

We can also automate remediation actions and create standard Security Incident Playbooks to coordinate and automate actions across relevant teams. ServiceNow can also be integrated with other ITSM instances so that security incidents are automatically reported to the state Cybersecurity Operations Center (CSOC).

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.

The ServiceNow SecOps Suite allows customers to integrate with their existing security infrastructure to consolidate security data across the enterprise for analysis, visibility, and response. SecOps can integrate with firewalls, IDS/IPS, EDR, network devices, and cloud hosted infrastructure. Ingested event information from all of those sources are analyzed using SecOps Machine Learning tools for Pattern Recognition, behavioral analysis, Indicators of compromise and other supicious activity.

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.

Once data is collected from integrated security tools, the SecOps suite enables the security team to define both automated and manual responses to identified threats from the SecOps Console. Automated responses can include containing malicious runtimes, isolating devices on a network, and removing malware. Custom automated responses can be defined using playbooks in ServiceNow, allowing the security team to continually improve automated response capabilities.

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.

The SecOps Suite ingests event information from Security sources and analyzes data using Machine Learning tools for Pattern Recognition, Behavioral Analysis, Indicators of Compromise and other supicious activity. Once data is analyzed the security team can use automated and manual responses to identified threats from the SecOps Console. Automated responses can include containing malicious runtimes, isolating devices on a network,and removing malware.

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 SecOps suite provides a comprehensive view of a client's security posture and allows an organization to consolidate security data from across the entire IT infrastructure into a single location for visibility and response. This enables security teams to quickly detect, investigate, and respond to security threats. The console includes dashboards for tracking standard incident KPIs and users can define custom KPIs for metrics not covered by OOTB 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.

The SecOps Suite provides comprehensive incident tracking. SecOps ingests data from security tools and automatically create incidents. Incidents can be created with root cause analysis, related event information that created the incident, and suggest or execute automated responses that can be performed to mitigate or resolve the issue.Security Incidents can also generate alerts for further investigation if proposed automated responses do not resolve the incident.

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.

ServiceNow Threat Intelligence Security Center (TSIC) integrates external threat data with your internal information, offering a holistic view of the threat landscape including current threat actors, active threat campaigns and new indicators of compromise for new expoloits. It uses a custom threat score calculator so clients can weight threat scores from third party sources to reflect the risk profile of an organization and enhance their real world threat awareness.

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.

ServiceNow Threat Intelligence Security Center (TSIC) can integrate with multiple external threat intelligence feeds and correlate vulnerability and threat data in real time to improve threat detection and response for an organization. These CTI data feeds are correlated and de-duplicated and applied to security incidents to ensure that emerging threats, exploits and malware campaigns are included in ongoing threat detection activities and response times for threats are as efficient as possible.

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

Respondent Name: TelaForce, LLC.

Solution Name: ServiceNow Governance, Risk and Compliance

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.

The ServiceNow Governance, Risk, and Compliance (GRC) module provides a comprehensive platform to manage governance frameworks, assess enterprise risks, and ensure compliance with industry regulations. Its robust capabilities enable organizations to streamline policy development, automate compliance processes, and align risk management workflows with business objectives.

Governance Frameworks: ServiceNow GRC centralizes governance by providing a structured approach to defining and managing policies, standards, and frameworks. Organizations can map policies to regulations and frameworks like ISO, NIST, and GDPR, ensuring alignment with compliance requirements. Policy lifecycle management tools support drafting, approval, dissemination, and periodic review of governance documents.

Risk Management and Assessment: The platform facilitates enterprise-wide risk assessments with tools for identifying, assessing, and mitigating risks. It enables users to document risks, evaluate their impact and likelihood, and prioritize mitigation efforts based on risk appetite. ServiceNow's risk register centralizes all risk data, providing a single source of truth for tracking and reporting. Risk scoring models and real-time dashboards help organizations visualize risk exposure and support data-driven decision-making.

Compliance Automation: ServiceNow GRC automates compliance checks by integrating with IT systems to monitor controls and enforce policies. The platform supports continuous control monitoring (CCM), automatically testing compliance requirements and flagging violations. Automated workflows enable quick responses to compliance gaps, ensuring ongoing adherence to regulatory standards.

Policy Development and Enforcement: Organizations can develop policies using intuitive templates, ensuring consistency and ease of collaboration. The GRC module links policies to controls, risks, and audit findings, ensuring that policies remain relevant and actionable. Integration with task management workflows enforces policy adherence and tracks implementation progress.

Audit Management: ServiceNow simplifies audit processes by centralizing audit plans, evidence collection, and findings. Automated workflows streamline the audit lifecycle, from planning to reporting. This integration ensures audit readiness and facilitates swift remediation of findings, reducing regulatory risks.

Real-Time Insights: The platform provides real-time dashboards and analytics to track governance, risk, and compliance performance. Prebuilt reports and customizable metrics offer visibility into control effectiveness, risk exposure, and compliance trends, enabling proactive management and strategic alignment.

Integration and Scalability: ServiceNow GRC integrates seamlessly with other modules and external systems, ensuring a holistic view of governance and risk. Its scalable architecture allows organizations to adapt to evolving business needs, regulatory changes, and risk landscapes.

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.

ServiceNow GRC centralizes policy management, enabling the creation, distribution, and tracking of governance frameworks, compliance guidelines, and operational policies. It supports version control to manage updates and ensures auditability. Electronic signature functionality facilitates policy acceptance, while automated workflows streamline dissemination and compliance tracking. Real-time dashboards provide visibility into policy adherence and organizational and regulatory compliance.

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.

ServiceNow GRC provides risk assessment tools that enable organizations to identify, assess, and prioritize risks across departments. The platform uses customizable risk scoring models to evaluate likelihood and impact, centralizing risks in a unified risk register. Automated workflows streamline assessments, while real-time dashboards and analytics provide visibility into risk exposure. This ensures proactive risk management and alignment with business objectives.

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.

ServiceNow GRC enables teams to define and track risk response plans with structured workflows. Responsibilities are easily assigned, and automated notifications keep stakeholders informed. Real-time dashboards and task management tools monitor progress toward mitigation goals, ensuring accountability and timely resolution. This streamlined approach enhances collaboration and ensures alignment with organizational risk management objectives.

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.

ServiceNow GRC streamlines audit management by supporting the planning, scheduling, and execution of internal and external audits. The platform automates evidence collection, tracks findings, and links them to corrective action plans. Real-time dashboards monitor audit progress, while automated workflows ensure follow-up actions are completed. Audit reports are generated automatically, providing clear insights and ensuring compliance with regulatory requirements.

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.

ServiceNow GRC simplifies compliance tracking by integrating industry-specific regulations like NIST CSF, GDPR, HIPAA, and PCI-DSS. Automated controls and real-time monitoring detect non-compliance or control failures, triggering alerts for timely action. The platform maps regulations to policies and controls, enabling centralized management and continuous compliance. Dashboards and reports provide insights into compliance status and trends, ensuring proactive risk mitigation.

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.

ServiceNow GRC offers customizable risk dashboards that provide executives with a real-time overview of key risks, compliance metrics, and governance health. These dashboards display aggregated data with drill-down capabilities for detailed analysis. Visualizations, including charts and heatmaps, enhance clarity and decision-making. Automated updates ensure data accuracy, enabling proactive management of risks and compliance efforts across the organization.

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.

ServiceNow GRC streamlines third-party risk management by enabling assessments of vendor risks and due diligence on compliance practices. It centralizes vendor data, automates risk questionnaires, and evaluates vendors against predefined criteria. Integrated workflows manage remediation actions, while dashboards provide real-time visibility into vendor risk profiles. This ensures informed decision-making and alignment with organizational risk management strategies.

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 L12 – Service Category 12: IT Service Management (ITSM)

Respondent Name: TelaForce, LLC.

Solution Name: ServiceNow IT Service 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 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: ITSM Solutions are designed to streamline the delivery and management of IT services by providing a structured approach to incident management, problem resolution, change control, and service request fulfillment. The Solution should support automation, self-service capabilities, and detailed reporting on service levels.

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

The ServiceNow ITSM module is designed to meet the described needs by providing a robust, scalable platform that streamlines IT service delivery and management. It supports a structured approach to incident management, problem resolution, change control, and service request fulfillment, leveraging automation, self-service capabilities, and comprehensive reporting.

Incident Management: ServiceNow ensures efficient incident resolution by automating ticketing, prioritization, and escalation. Using AI-driven workflows and predictive intelligence, the platform routes incidents to the appropriate teams and suggests solutions based on historical data, reducing resolution times and improving service quality.

Problem Management: The module helps identify root causes of recurring issues through advanced analytics and knowledge base integration. ServiceNow automates problem documentation and links related incidents, allowing teams to proactively address underlying problems and minimize disruptions.

Change Management: ServiceNow's change management module streamlines the planning, approval, and implementation of changes. Automated workflows ensure consistent processes, while risk assessments and Change Advisory Board (CAB) tools help minimize potential disruptions. Real-time tracking of change activities provides visibility into progress and outcomes.

Service Request Management: The platform delivers a consumer-grade self-service experience through the Service Portal, allowing users to submit, track, and manage requests easily. Automation of routine tasks, such as provisioning access or resetting passwords, reduces IT workload and improves user satisfaction.

Automation: The ITSM module integrates with the Now Platform to automate repetitive tasks and workflows, such as ticket creation, incident routing, and notification management. This reduces manual effort, enhances efficiency, and ensures consistency across IT processes.

Self-Service Capabilities: ServiceNow empowers end-users with a centralized, user-friendly portal that integrates with a robust knowledge base. Virtual agents provide 24/7 assistance, offering solutions to common issues and reducing reliance on IT staff.

Detailed Reporting: ServiceNow provides advanced analytics and real-time dashboards to monitor service levels and performance metrics. Built-in reporting tools allow stakeholders to track key performance indicators (KPIs), identify trends, and make data-driven decisions to enhance service delivery.

Integration and Scalability: The platform seamlessly integrates with third-party tools and supports a wide range of IT operations, enabling organizations to scale as their needs evolve. This flexibility ensures that ServiceNow adapts to changing business requirements while maintaining operational excellence.

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: Automated Incident Management Workflows – Solution should detect, categorize, and prioritize IT incidents based on predefined rules. The system should support automatic escalation and notification of incidents to the appropriate teams.

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

ServiceNow automates incident management with predefined rules to detect, categorize, and prioritize incidents. AI-driven workflows route incidents to the right teams and provide resolution suggestions. Automatic escalations ensure urgent issues are addressed promptly, while real-time notifications keep stakeholders informed. The platform's flexibility allows custom rules to align with business needs, ensuring streamlined processes, reduced response times, and improved resolution outcomes.

Prompt 3: Self-Service Portal – Solution should enable end-users to submit service requests, track the status of requests, and access knowledge base articles for self-help. The portal should integrate with automated fulfillment workflows, reducing the need for manual intervention.

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

ServiceNow ITSM delivers a user-friendly self-service portal where end-users can submit and track service requests and access a robust knowledge base for self-help. The portal integrates with automated workflows to fulfill requests, such as password resets or access provisioning, with minimal manual intervention. AI-powered virtual agents provide 24/7 support, enhancing the user experience while reducing IT workload, ensuring faster resolution and improved service efficiency.

Prompt 4: Change Management Tools – Solution should include request and approval workflows, risk assessment for changes, and automated enforcement of change windows and rollback plans.

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

ServiceNow ITSM provides robust change management tools with request and approval workflows, ensuring structured handling of changes. Built-in risk assessment evaluates potential impacts, while automated enforcement of change windows ensures changes occur at appropriate times. The platform supports rollback plans through detailed change records and pre-configured contingency workflows, minimizing disruption and enhancing control over the change process.

Prompt 5: Configuration Management Database (CMDB) – Solution should track all configuration items (CIs) within the IT infrastructure, including hardware, software, networks, and cloud assets.

The CMDB should map dependencies between CIs and provide insights into potential impact during incident resolution or change requests.

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

ServiceNow CMDB tracks all configuration items (CIs) across hardware, software, networks, and cloud assets, maintaining a comprehensive IT asset inventory. It maps dependencies between CIs, enabling impact analysis for incident resolution and change requests. Integrated with ITSM workflows, the CMDB provides real-time visibility into the IT environment, supports root cause analysis, and ensures informed decision-making, enhancing operational efficiency and minimizing risks during changes.

Prompt 6: Service Level Management – Solution should define, monitor, and report on Service Level Agreements (SLAs). The system should automatically calculate performance metrics such as response time, resolution time, and service availability, and provide real-time dashboards.

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

ServiceNow ITSM enables Service Level Management by defining and monitoring SLAs with automated tracking of performance metrics like response time, resolution time, and service availability. Real-time dashboards and reports provide visibility into SLA compliance and trends. The platform ensures proactive management with automated alerts for potential breaches, empowering teams to maintain high service standards and continuously improve performance.

Prompt 7: Pre-Buit Integrations – Solution should include monitoring tools, security platforms, and asset management systems to provide full visibility into the health and performance of IT services.

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

ServiceNow ITSM offers pre-built integrations with monitoring tools, security platforms, and asset management systems, ensuring full visibility into IT service health and performance. These integrations enable real-time data flow, centralized management, and automated workflows across systems. By consolidating insights into a single platform, ServiceNow enhances proactive issue resolution, improves operational efficiency, and ensures seamless IT service delivery.

Prompt 8: Integration of CTI Data Feeds – provide insights into security incidents or vulnerabilities that could affect IT service delivery, allowing ITSM platforms to correlate service disruptions with known global security threats.

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

ServiceNow ITSM integrates CTI data feeds to provide real-time insights into security incidents and vulnerabilities. This allows the platform to correlate service disruptions with global security threats, enabling proactive responses. Automated workflows link threat intelligence to incident management, prioritizing actions based on risk. This integration ensures enhanced visibility, faster remediation, and improved resilience of IT services.

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. 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 L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: TelaForce, LLC.

Solution Name: ServiceNow

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: Vulnerability Assessment and Management Solutions must enable organizations to continuously scan their IT assets for security vulnerabilities, evaluate the risks associated with these vulnerabilities, and prioritize remediation efforts. The Solution should automate both scanning and remediation workflows, providing real-time visibility into the organization's security posture.

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

The ServiceNow platform enables comprehensive vulnerability assessment and management by integrating with security tools to continuously scan IT assets, evaluate risks, and prioritize remediation efforts. Its robust automation capabilities streamline workflows, ensuring a proactive approach to maintaining a strong security posture.

Continuous Vulnerability Scanning: ServiceNow integrates with leading vulnerability scanners, such as Qualys, Tenable, and Rapid7, to automatically identify vulnerabilities across hardware, software, and network assets. These integrations provide real-time updates, ensuring an up-to-date inventory of vulnerabilities in the organization's IT environment.

Risk Evaluation and Prioritization: The platform evaluates vulnerabilities using advanced risk-scoring models that consider factors such as CVSS scores, exploitability, asset criticality, and business impact. This prioritization allows teams to focus remediation efforts on vulnerabilities that pose the highest risk to business operations, ensuring efficient use of resources.

Automated Remediation Workflows: ServiceNow automates remediation workflows by linking identified vulnerabilities to ITSM processes, such as incident and change management. For example:

• Incident Creation: High-risk vulnerabilities automatically trigger incident tickets, routing them to the appropriate teams for immediate action.

• Change Management Integration: Remediation efforts that involve patches or system updates are automatically aligned with change management workflows to ensure safe implementation.

Real-Time Visibility and Reporting: Dashboards and reports provide a centralized view of the organization's security posture, showing metrics such as the number of vulnerabilities, their severity, and remediation progress. These dashboards offer drill-down capabilities for detailed analysis, enabling security teams and executives to make informed decisions quickly.

Proactive Threat Mitigation: By integrating with threat intelligence feeds, the platform correlates vulnerabilities with known exploits and global security threats. This proactive approach helps identify and address vulnerabilities that are actively being exploited in the wild, further reducing the risk of compromise.

Continuous Improvement: ServiceNow's reporting and analytics tools provide insights into remediation trends, bottlenecks, and areas for improvement. By analyzing this data, organizations can optimize their vulnerability management processes, ensuring continuous enhancement of their security practices.

Scalability and Integration: The platform's scalability allows organizations to manage vulnerabilities across on-premises, cloud, and hybrid environments. Its integrations with other

ServiceNow modules, such as ITSM and GRC, ensure a unified approach to IT security and risk management.

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: Automated and Continuous Vulnerability Scanning – Solution should include automated and continuous scanning of network devices, servers, endpoints, and applications. The scans should identify known vulnerabilities (e.g., CVEs), misconfigurations, and missing patches.

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

ServiceNow Vulnerability Response integrates with vulnerability scanners like Qualys and Tenable to automate continuous scanning of network devices, servers, endpoints, and applications. The platform identifies known vulnerabilities (e.g.,CVEs), misconfigurations, and missing patches, consolidating findings into a centralized dashboard. Automated workflows prioritize risks, trigger remediation actions, and track progress, ensuring efficient vulnerability management and enhanced security posture.

Prompt 3: Risk-Based Vulnerability Prioritization – Solution should allow vulnerabilities to be sorted and ranked based on the criticality of the affected asset, the exploitability of the vulnerability, and the business impact. This helps organizations focus on high-priority issues that pose the most risk.

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

ServiceNow Vulnerability Response and GRC prioritizes vulnerabilities by combining asset criticality, exploitability, and business impact into a risk-based scoring model. It integrates data from vulnerability scanners and asset inventories to rank issues, ensuring focus on high-priority risks. Real-time dashboards highlight the most critical vulnerabilities, while automated workflows enable swift remediation, aligning security efforts with organizational risk priorities.

Prompt 4: Remediation Workflows – Solution should integrate with IT service management (ITSM) systems, automatically creating tickets or work orders for IT teams to address vulnerabilities, track progress, and close issues once remediated.

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

ServiceNow integrates vulnerability management with ITSM, automatically creating incident tickets or change requests for remediation tasks. The platform tracks progress, assigns responsibilities, and provides automated notifications to ensure timely resolution. Real-time

dashboards monitor remediation efforts, and issues are closed once resolved and verified, ensuring streamlined vulnerability management aligned with IT operations.

Prompt 5: Detailed Vulnerability Reports – Solution should include the ability to provide reports including information such as affected assets, severity ratings (e.g., CVSS scores), vulnerability descriptions, and recommended fixes.

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

ServiceNow generates detailed vulnerability reports with information on affected assets, severity ratings (e.g., CVSS scores), vulnerability descriptions, and recommended fixes. These reports are customizable and provide real-time insights through dashboards and analytics using the Performance Analytics module. Automated updates ensure accuracy, enabling security teams to prioritize actions and effectively communicate risk and remediation strategies to stakeholders.

Prompt 6: Real-Time Insights and Trend Analysis – Solution should provide insights into the overall security posture, such as the number of open vulnerabilities, time-to-remediation, and patch compliance rates.

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

ServiceNow provides real-time insights into security posture with dashboards tracking open vulnerabilities, time-to-remediation, and patch compliance rates. Trend analysis tools in the Performance Analytics module highlight remediation progress, bottlenecks, and recurring issues. Automated data updates ensure accuracy, enabling proactive risk management and informed decision-making to enhance security and operational efficiency.

Prompt 7: Integration with Patch Management Solutions – Solution should allow organizations to deploy patches to vulnerable systems directly from the platform.

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

ServiceNow integrates with patch management solutions, enabling seamless deployment of patches to vulnerable systems directly from the platform. Automated workflows link identified vulnerabilities to patching tasks, ensuring efficient remediation. Real-time tracking monitors patch deployment progress, while integration with ITSM ensures changes are implemented safely and effectively, reducing security risks and operational disruptions.

Prompt 8: Integration of CTI Data Feeds – Solution should enhance vulnerability prioritization by providing real-time threat intelligence on active exploitation campaigns, emerging threats, or vulnerabilities that are being specifically targeted by threat actors.

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

ServiceNow integrates CTI data feeds to enhance vulnerability prioritization by correlating real-time threat intelligence with known vulnerabilities. Using the Security Incident Response and GRC modules, it identifies active exploitation campaigns, emerging threats, and targeted vulnerabilities, updating risk scores dynamically. This enables security teams to prioritize remediation of the most critical threats, ensuring a proactive and intelligence-driven approach to vulnerability management.

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

Respondent Name: TelaForce, LLC.

Solution Name: ServiceNow

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 ServiceNow platform provides robust capabilities to support Enterprise Security Log Management, Analytics, and Response by integrating SIEM, SOAR, and backend solutions for log collection, storage, aggregation, and analytics. These functionalities empower organizations to monitor, detect, and respond to security threats while gaining comprehensive visibility into their IT infrastructure.

Integration with SIEM Solutions: ServiceNow seamlessly integrates with leading SIEM tools, such as Splunk, QRadar, and ArcSight, to ingest security event logs and provide centralized management of security incidents. This integration enables real-time analysis of security events, correlating data across systems to identify patterns, anomalies, and potential threats efficiently.

SOAR: ServiceNow's SOAR capabilities, provided through the Security Incident Response module, automate threat detection, analysis, and response. Key features include:

• Playbooks and Workflows: Automate incident response steps, from triaging alerts to executing mitigation actions.

• Threat Intelligence Integration: Enriches security events with contextual data from CTI feeds, enabling smarter decision-making.

• Automated Responses: Executes predefined actions, such as isolating compromised systems or blocking malicious IPs, directly from the platform.

Log Management and Aggregation: ServiceNow provides integration capabilities to collect, aggregate, and analyze logs from diverse sources, including network devices, servers, applications, and cloud environments. Its centralized repository simplifies data correlation and provides a unified view of the organization's security posture.

Advanced Analytics and Machine Learning: The platform leverages advanced analytics and AI-powered tools to analyze security data in real-time, identifying anomalies and predicting potential threats. Machine learning models enhance threat detection accuracy by learning from historical data and adapting to evolving attack patterns.

Incident Management and Response: Integrated with ITSM, ServiceNow ensures streamlined incident handling by automating ticket creation, prioritization, and assignment. The platform's escalation and notification capabilities keep stakeholders informed throughout the incident lifecycle.

Dashboards and Reporting: ServiceNow provides real-time dashboards and customizable reports that offer insights into security trends, incident metrics, and operational performance. Drill-down capabilities allow teams to investigate issues in detail, supporting proactive threat management.

Compliance and Audit Support: ServiceNow facilitates compliance with industry standards (e.g., GDPR, HIPAA, NIST) by linking security logs and incident data to governance frameworks. Automated documentation of response activities ensures audit readiness.

Integration and Scalability: The platform's flexibility allows it to integrate with existing security tools and scale alongside the organization's infrastructure.

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.

ServiceNow integrates with SIEM tools like Splunk and QRadar to gather and centralize log data from endpoints, servers, and applications, supporting structured and unstructured formats like Syslog and JSON. Logs are aggregated in a centralized repository for real-time analysis and correlation with cybersecurity events. This integration enables seamless threat detection, streamlined workflows, and improved visibility across the IT environment.

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.

ServiceNow integrates with scalable storage solutions, including cloud and on-premises data lakes, to support long-term log retention for compliance. It ensures secure, tamper-proof archiving through encryption and audit trails, with options for cold storage to optimize costs. ServiceNow's flexibility enables seamless integration with third-party storage providers for scalable and compliant data retention, meeting regulatory and operational needs effectively.

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.

ServiceNow integrates with SIEM tools to perform real-time event correlation, detecting complex attacks and anomalies by analyzing patterns across diverse data sources. Enriched with threat intelligence, the platform identifies suspicious activity and prioritizes incidents for response. Automated workflows streamline investigation and remediation, ensuring rapid detection and mitigation of security threats.

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.

ServiceNow integrates with big data engines and distributed computing frameworks via its Security Operations module, enabling real-time analysis of large security data sets. It supports complex threat detection, pattern recognition, and predictive analytics by leveraging machine learning models trained on historical data. This reduces false alerts and optimizes efficiency, ensuring accurate threat identification and streamlined security operations.

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.

ServiceNow's modular architecture supports independent operation of services like log collection, incident response, and threat detection through its Security Operations and integration capabilities. This microservices approach ensures scalability and flexibility, allowing organizations to enhance or replace components without overhauling the entire system. APIs and integrations enable seamless adaptation to evolving security needs while maintaining operational efficiency.

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.

ServiceNow provides continuous real-time monitoring with customizable alerts powered by advanced analytics, AI, and behavioral analysis. Integration with threat intelligence enriches security alerts, enabling proactive detection of threats. Machine learning models identify

anomalies and evolving attack patterns, while automated workflows streamline investigation and response, ensuring comprehensive and efficient threat management.

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.

ServiceNow integrates with log management solutions to provide centralized or federated log management, enabling real-time indexing and analysis of security events. It supports compliance standards with secure storage, audit trails, and flexible retention policies. Integration with SIEM tools ensures comprehensive visibility and streamlined workflows for managing and analyzing logs, enhancing security and regulatory adherence.

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.

ServiceNow automates incident response with predefined playbooks that isolate compromised systems or block malicious activity. Its Security Incident Response (SIR) module provides a centralized view of security events, integrating detection, investigation, and resolution workflows. Automated actions, enriched with threat intelligence, streamline remediation, reduce response times, and enhance overall security operations.

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.

ServiceNow's Security Incident Response (SIR) module provides robust case management to track incidents, document actions for compliance, and maintain audit trails. Integrated collaboration tools, such as task assignments, real-time updates, and chat features, ensure seamless communication among security team members. This enables coordinated responses, enhances transparency, and supports compliance with regulatory requirements.

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.

ServiceNow offers advanced analytics and customizable dashboards to transform raw security data into actionable insights. Real-time visualizations display metrics, alerts, and trends, aiding security teams in decision-making. Integration with business intelligence (BI) tools enables deeper analysis and reporting, ensuring comprehensive visibility and enhanced strategic planning across the organization.

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