Exhibit D, F

Digital Security Solutions

RFP No. 24-43230000-RFP

Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Rapid7

Solution Name: InsightVM

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

Rapid7 InsightVM is a vulnerability management offering that helps its customers find IT vulnerabilities and prioritize risk, allowing customers to be proactive and minimize the impact of risk elements. Customers can use InsightVM to continuously scan their IT assets for security vulnerabilities, evaluate the risks associated with these vulnerabilities, and prioritize remediation efforts.

InsightVM includes dashboards that provide visibility into assets, vulnerabilities, remediations, scans, and software found by InsightVM. Dashboards are powered by the Rapid7 Insight platform and allow you to explore all of your vulnerability management data in one place. They also include pre-packaged analytics that answer security questions for you without exploration. Dashboards are made up of data cards that explain your security data in simple ways.

Remediation information is available for all vulnerabilities and presented in reports as either high-level or detailed step-by-step instructions. Remediation workflow in InsightVM lets you take a more strategic approach to remediation by creating remediation projects focused on the risk that actually matters to you, in the context of your unique environment. You can then send the right information to the right teams using their existing ticketing systems.

InsightVM Remediation Analytics offers a remediation workflow that is operationalized and manageable in one unified view. The Projects feature allows administrators to group like assets and solutions together using flexible filtering options, creating

focused action plans for remediation teams. Project creators can set an end date for a project and measure overall and individual solution progress throughout its duration. Projects are updated as scans are completed: once the vulnerability has been fixed, the remediation step is updated.

Other Key benefits include:

- **Real Risk Prioritization -** InsightVM lets you prioritize risk based on the likeliness of an attacker exploiting the vulnerability in a real attack.
- **Vulnerability Assessment -** With InsightVM, you can accurately assess your changing environment.
- **Full Attack Surface Visibility -** InsightVM provides full visibility of your entire attack surface, providing asset inventory for on-premises, remote, and virtual assets.
- **Real-Time Remediation -** InsightVM uses Remediation Projects to identify individual steps that can reduce the most risk, such as the implementation of a single patch that fixes dozens of vulnerabilities.
- **Measuring & Reporting -** With InsightVM's Live Dashboards, you can easily create custom and full dashboards for every stakeholder and query each card with simple language to track progress of your security program.

Rapid7 offers a range of security solutions and services to help organizations become more secure. InsightVM is at the core of the security equation by providing visibility into vulnerabilities and the associated risks.

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 this above prompt in the field below.

Yes. InsightVM includes automated and continuous scanning of network devices, servers, endpoints, and applications. Scans can be performed ad hoc or scheduled to run at predetermined times. Duration, date and time (including time zone), as well as the length of time between scans are all configurable settings. InsightVM scans are able to identify known vulnerabilities, misconfigurations, and missing patches.

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 this above prompt in the field below.

Yes. The risk scoring in InsightVM allows for prioritization of vulnerabilities based on criticality, exploitability, business impact, and provides an accurate look at the system's most critical issues first. InsightVM presents vulnerabilities with associated malware kits and exploit modules, illustrating the known impact these vulnerabilities could have on an organization. Exploit availability allows teams to focus on vulnerabilities that have the highest likelihood of being leveraged.

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 this above prompt in the field below.

Yes. Remediation workflows in InsightVM lets you take a strategic approach to remediation by creating remediation projects focused on the risk that actually matters to you, in the context of your unique environment. You can then send the right information to the right teams using their existing ITSM systems. Assets can be automatically grouped based on specific criteria. Pre-built reports can be run at the conclusion of each scan and automatically sent to specified asset owners.

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.

Yes, InsightVM can do this. InsightVM includes the ability to provide reports including information such as affected assets, severity ratings, vulnerability descriptions, and recommended fixes. InsightVM contains pre-packaged report templates such as, remediation plan, executive summary, compliance, & trend data about the environment, baseline comparisons to analyze change, and more. **Here is a list of built-in report templates: https://docs.rapid7.com/insightvm/report-templates-and-sections/**

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 this above prompt in the field below.

Yes. InsightVM includes real-time insights and trend analysis that provide visibility into assets, vulnerabilities, remediations, scans, & software. Dashboards in InsightVM allow you to explore all of your vulnerability management data in one place, including pre-packaged analytics that answer security questions for you. Dashboards are made up of data cards that explain your security data in simple ways, such as the number of open vulnerabilities, time-to-remediation, & patch compliance rates.

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 this above prompt in the field below.

Yes. InsightVM integrates with patch management solutions such as Microsoft SCCM and IBM BigFix via in-product automation workflows to support automated patching. After an assessment, patches will be staged and a human decision point will be created in InsightVM. Users will deploy the patches to their assets and then use the decision point to confirm that the work is complete. At this point, InsightVM will kick off a rescan of the assets to validate remediation efforts.

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.

Yes. InsightVM uses risk data from the Rapid7 Threat Feed, which is a live, curated feed of vulnerabilities being actively exploited by attackers in the wild. The feed combines data collected by our honeypots and incident response activity with

information from trusted 3rd parties. Rapid7's TI team adds context such as threat vector and actor information so you can see how relevant a threat is to your organization. **https://www.rapid7.com/products/insightvm/features/integrated-threat-feeds/**

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: https://www.rapid7.com/legal/tos/

Digital Security Solutions

RFP No. 24-43230000-RFP

Attachment L14 – Service Category 14: Cybersecurity Threat Intelligence (CTI)

Respondent Name: Rapid7

Solution Name: Threat Command

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 a response 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 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: Cybersecurity Threat Intelligence (CTI) Solutions must aggregate threat data from multiple sources, analyze it to uncover emerging threats, and provide actionable intelligence to enhance security defenses. The Solution should integrate with an organization's existing security operations workflows, ensuring that threat intelligence is used to improve detection, prevention, and response efforts.

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

Rapid7 Threat Command is a threat intelligence and digital risk protection solution that delivers instant value while reducing your risk exposure from external threats. Threat Command pairs AI and machine learning models with expert human intelligence to help you prioritize what's relevant for immediate action. We act as an extension of your team, providing expertise on demand so you can quickly remove threats impacting your organization, while simplifying your security workflows and freeing up resources.

Threat Command Solution Benefits

- **Reduce noise; prioritize relevant threats** - Threat Command prioritizes and alerts on the most relevant threats to your organization. By consistently monitoring customers' digital properties and assets, we match those IOCs and vulnerabilities to the customer's actual environment, delivering them relevant, contextualized intelligence.
- **Speed response across your environment** - By integrating our solution with a vast ecosystem of integration partners across the entire security ecosystem of SIEM, SOAR, XDR, VM, endpoint, firewall, and network technology partners, we enable customers to speed responses across their environment - by sending those threats immediately to their blocklists, or automating their responses on particular types of threats within the platform.
- **Threat expertise on demand** - We understand that most security teams are understaffed and under-resourced. We act as an extension of your security team by offering unlimited direct access within the platform to ask our security

analysts questions about alerts, and single-click remediation so our analysts can do the work for you in taking down threats while reducing the amount of time your brand is exposed.

- **Simplified Workflow** - With our intuitive all-in-one cloud-based platform, easy onboarding, unlimited seats, and multi-tenancy capabilities, we are custom-built to support and simplify your workflows, easing the burden on overwhelmed security teams.

Threat Command offers an all-in-one solution for all of your threat intelligence workflows by aggregating threat data from multiple sources, analyzing it to uncover emerging threats, and providing actionable intelligence to enhance security defenses. Threat Command also provides digital risk protection & remediation which helps protect your organization from external threats across the clear, deep, and dark web with AI/ML detections paired with human intelligence scenarios for highly-contextualized alerts on the most pressing threats to your organization, as well as an in-house expert threat remediation team to take down threats from phishing campaigns, impersonations, and fraudulent activities and sites.

https://docs.rapid7.com/threat-command/architecture-overview

For the portions that are prompts (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: Threat Data Aggregation – Solution should include open-source threat feeds, paid subscriptions, and proprietary sources. The platform should support integration with standards-based threat intelligence feeds such as STIX, TAXII, and others.

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

Yes. Rapid7 is designed to manage multiple intelligence feeds of data, from open source, proprietary and 3rd party sources. TIP ingests intelligence feeds, extracts indicators, aggregates them from multiple sources & then enriches the indicators into a single data set. Threat Information can be correlated and easily shared with existing security tools utilizing the platform's 3rd party integrations. TIP supports multiple formats;. STIX/TAXII, MISP, CSV, PDF, IOCs lists, email, API and JSON.

Prompt 3: Threat Intelligence Platform (TIP) – Solution should consolidate and normalizes threat data, making it easy to share actionable intelligence with internal teams or external partners on a platform that has the capability to integrate with the CTI Solution. The platform should provide support for enrichment, scoring, and threat actor profiling.

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

Yes. Rapid7 TIP provides real-time threat intelligence, monitoring thousands of sources across the clear, deep and dark web to identify threats targeting your environment. TIP leverages automated and manual collection of threat data, combined with in-house threat research expertise to deliver relevant, actionable, contextual and automated alerts and further orchestrate proactive response with built-in playbooks. Threat alerts are automatically classified, scored and prioritized in the platform.

Prompt 4: Real-Time Threat Alerts – Solution should notify Customer designated security teams of emerging threats relevant to their environment, such as new vulnerabilities, malware campaigns, or attack techniques in real-time. Alerts should include contextual information such as indicators of compromise (IoCs), threat actor motivations, and recommended mitigations.

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

Yes. Rapid7 classifies all threats across various threat categories and automatically assigns a risk score to help analysts prioritize their efforts. This is determined by many factors, supported by the platform's detection policy algorithms that can be further configured and tuned if required. For technical IOC management, Rapid7 automatically ingests, collates and aggregates intelligence from multiple sources/feeds. Alerts include IOCs, threat actor motivations, and recommended mitigations.

Prompt 5: Custom Intel – Solution should include the ability to incorporate threat intelligence feeds and manual intelligence to include custom work/intel.

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

Yes. Rapid7 includes the ability to incorporate threat intelligence feeds and manual intelligence to include custom work/intel. Rapid7 enables you to aggregate IOCs from public and private feeds and enrich your threat workflows all in one place, alongside contextualized threat intelligence alerts, a threat library, a dark web search tool, a browser extension, and threat mapping to speed investigations.

Prompt 6: Customer Feeds – Solution should include the ability to potentially change feeds if needed to include, remove, or modify research, analysis, and intelligence feeds.

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

Yes. Rapid7 TIP enables the customer to determine which threat data feeds to ingest and provides the ability to change feeds if needed to include, remove, or modify research, analysis, and intelligence feeds. You can enable or disable all the feeds that are available in your account.

Here's additional information on changing threat feeds: https://docs.rapid7.com/threat-command/tip-sources

Prompt 7: Integration with SIEM, SOAR, and SOC Tools – Solution should provide contextual threat intelligence directly within the security operations workflow. This integration should enable automated response actions such as blocking malicious IP addresses or adjusting firewall rules based on threat intelligence.

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

Rapid7 provides an out of the box API integration with many SIEM/SOAR solution providers such as Azure Sentinel, Splunk, Qradar, and Palo Alto, as well as firewalls (i.e. Palo Alto, Cisco, Checkpoint, Fortinet) and endpoint solutions including Crowdstrike, Microsoft, and SentinelOne to send Alerts/IOCs for automated blocking for example. A public RestAPI can also be leveraged to query, upload and enrich threat data as well as integrating into many other workflows.

Prompt 8: Feed Control – Solution should include Capabilities for incorporating premium feeds and manual intelligence.

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

Yes. Customers can use Threat Command to automatically pull threat data from feeds they are subscribed to, to use in addition to those feeds that Threat Command provides. To use these feeds, the user must subscribe directly with the provider, and then enter their user credentials into Threat Command.

Here's additional information on incorporating threat feeds: https://docs.rapid7.com/threat-command/tip-sources

Prompt 9: Dynamic Threat Detection – Solution should include the ability to provide tailored threat intelligence focusing on specific threats relevant to an organization's unique environment, including industry-specific and organization specific risks and potential adversaries, ensuring that security measures are aligned with real-world scenarios.

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

Yes. Rapid7 analyzes, categorizes, and prioritizes cyberthreats in real-time, leveraging proprietary, data mining algorithms and machine learning capabilities, delivering highly tailored intelligence. Before an alert is triggered, automated processes validate the existence of a cyber threat and its relevance. If and only when these conditions are met, the information goes through a classification process and an alert is triggered directly within Threat Command's dedicated alerts and dashboards.

Prompt 10: Threat Context – Solution should include the ability to provide contextual awareness threat intelligence, to include custom intelligence, that provides insights that consider the broader context of an organization's operations, including user behavior, network architecture, and business priorities, allowing for more informed risk management.

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

Yes. Rapid7 includes the ability to provide contextual awareness threat intelligence. Ex: Threat Command identifies mentions of company name, brand names, VIP names and other company-related assets across various cybercrime sources including dark web forums and black markets, and analyzes the identified mentions for context and sentiment. This allows the solution to generate alerts around intents to attack or harm the organization, allowing for more informed risk management.

Prompt 11: Threat Insights – Solution should include capability to provide actionable insights from custom intelligence offering clear recommendations for mitigation, response strategies, and risk prioritization, empowering an organization to make informed decisions and improve their security posture effectively.

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

Yes. Rapid7 provides actionable insights from custom threat intelligence offering clear recommendations for mitigation, response strategies, and risk prioritization. Such alerts will include details on the source and the threat actor, along with recommendations for mitigation steps to mitigate the risk of the threat. This can be shared using the sharing capabilities in Threat Command, empowering an organization to make informed decisions and improve their security posture effectively.

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

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

Any Applicable SLA Goes Here: https://www.rapid7.com/legal/tos/

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Rapid7

Solution Name: InsightIDR

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.

Rapid7's InsightIDR is a single, complete solution for incident detection and response that combines compliance reporting, log aggregation, user behavior analytics, endpoint interrogation, real-time search, and Security Orchestration, Automation, and Response (SOAR). It covers an organization's entire network, including endpoints and cloud apps. InsightIDR is powered by our Insight Platform to simplify and combine data collection, analytics, and search technology. This combination enables effective detection and efficient investigation, so that organizations can rapidly go from compromise to containment.

InsightIDR leverages attacker analytics to detect intruder activity, cutting down false positives and days' worth of work for your security professionals. It hunts for actions indicative of compromised credentials, spots lateral movement across assets, detects malware, and sets traps for intruders. InsightIDR is the only fully integrated detection and investigation solution that lets you identify a compromise as it occurs and complete an investigation before things get out of control. InsightIDR leverages machine learning, allowing the solution to continuously evolve as attacker behaviors do; monitors and tracks endpoints to detect local account abuses, malicious processes, and log manipulations; and makes it easy to use deception and set intruder traps such as honey pots, honey users, and honey credentials to detect intruders when they are initially exploring the network before they've had a chance to do damage.

Log data from various event sources is aggregated at one or more on-premise InsightIDR Collectors. The Collector is a piece of software installed on a dedicated server host (64-bit Windows or Linux OS). The Collector aggregates logs in real time, compresses the log data, encrypts the log data, and securely transmits it to the Insight cloud platform for parsing and analysis. The raw log data is deposited in an AWS S3 bucket managed by Rapid7 and dedicated to the customer. InsightIDR's backend services then parse the raw data, and we run analytics on this data, correlating events, users, accounts, authentications, alerts, privileges, etc. to understand the regular behavior of each user in the environment, while looking for known IOCs and patterns commonly indicative of user or asset compromise. Interaction with InsightIDR is done via a web-based console and, through a robust multi-tenant cloud architecture, can scale to an unlimited number of users accessing a single solution host without performance degradation.

InsightIDR does not require agent software to be installed on end devices to detect or monitor cloud services, but we do recommend the use of our endpoint agent as it offers enhanced EDR capabilities. InsightIDR can monitor endpoints to provide visibility into endpoint process activity, authentications, services, registry keys, and more forensic artifacts. The agent can also be used for endpoint quarantine and process containment.

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.

Yes. InsightIDR gathers logs from many sources, such as endpoints, servers, & applications. InsightIDR allows the ingestion of logs through agents, listening on a network port (syslog), tailing a file, watching a directory, using an existing log aggregator, or through an S3 or SQS messages on AWS. Using a combination of these methods, all of these are capable of being ingested. InsightIDR allows full data search of the raw log files in addition to the log event as parsed and normalized as JSON.

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.

Yes. Log data is retained for 13 months. Ingested logs over that time window are retained and available for search, visualization, and investigations. Rapid7 can either use an S3 bucket to retain the data for longer at a minimal cost, or we can charge to store the logs for additional time for you. Typically, we see our customers take advantage of the 13-month retention we provide and use the S3 bucket to store for longer as it is more cost-advantageous than having us store it for you.

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.

Yes. Rapid7 can ingest and correlate logs from proprietary applications. InsightIDR's native User Behavior Analytics (UBA) engine automatically correlates IP addresses in raw log data with associated hostnames and associates hostnames with primary users. Additional decoration of log data, including geoip lookup & behavioral anomaly flags (ex: first-time login), are automatically added based on the log type. Alerts in InsightIDR rely on a combination of correlation alerts & behavioral patterns.

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.

Yes. InsightIDR leverages a Big Data architecture and tooling to process data, perform analytics on that data, & retain it. **An architectural diagram is available here: https://insightidr.help.rapid7.com/docs.** There are 3 types of databases used in the Insight Cloud for InsightIDR retention and analysis of large volumes of data… Relational databases, NoSQL Ring (tracks associations between customers, users, assets, & last access dates), & Shared databases for data that is not customer-specific.

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.

Yes. InsightIDR provides a modular approach to security operations, allowing individual services (e.g., log collection, incident response, threat detection) to operate independently. **Please refer to the InsightIDR architecture diagram below:**

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.

Yes. InsightIDR provides continuous real-time monitoring with customizable alerts and advanced analytics that identify threats using machine learning, AI, and behavioral analysis. Threat analysis can be used to track IOCs. Any and all Threat Intelligence is further contextualized by InsightIDR with the user, asset, account, and behaviors associated with the time frame the IOC was seen. Endpoints are automatically monitored for malware, lateral movement, and privilege exploits.

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.

Yes. InsightIDR provides centralized management of logs, enabling real-time indexing and analysis of security events. With InsightIDR's SIEM capabilities, any syslog can be ingested for use in log search and data visualizations, such as dashboards to measure and report on compliance. Log data is retained for 13 months according to compliance standards, with flexible retention policies. Ingested logs over that time window are retained and available for search, visualization, & investigations.

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.

Yes. InsightIDR provides automated workflows: **https://docs.rapid7.com/insightidr/automate-workflows/.** All alerts triggered in InsightIDR are presented to customers as open investigations. Each investigation is presented as a visual timeline and automatically surfaces notable user and asset behavior in a 48-hour window surrounding the alert. With InsightIDR you can automatically isolate compromised systems, block malicious activity, or kick off case management with a ServiceNow or JIRA ticket.

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.

Yes. InsightIDR tracks all open & closed cases through our "Investigations" section; allows you to see the status of any incident and the applicable data from the analyst(s) working it. Insight Platform products monitor event collection infrastructure to display CPU, memory, OS, hostname, and events per minute (EPM). As alerts are created, InsightIDR automatically develops a case/investigation for each. InsightIDR can also integrate with a SIEM or Ticketing system to track/ manage the cases.

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.

Yes. InsightIDR allows you to create reports out of your custom dashboards, built from pre-configured cards that you can mix/match to capture & display the data you care about most. You can generate reports a single time or on a unique or pre-configured schedule. These reports will download as a PDF. After you create a report, you can see all the reports you've generated in the Reporting Archive section. **More information here: https://insightidr.help.rapid7.com/docs/generate-and-manage-reports.**

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: https://www.rapid7.com/legal/tos/