Request for Proposal for

Security Analytics Platform

September 27, 2021

Center for Internet Security

31 Tech Valley Drive
East Greenbush, NY 12061

Table of Contents

1.0 Project Background

1.1 Introduction

The Center for Internet Security, Inc. (CIS)® is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities. Membership in the MS-ISAC is open to employees or representatives from all 50 states, the District of Columbia, U.S. Territories, local and tribal governments, public K-12 education entities, public institutions of higher education, public utilities, councils of governments, associations of governments or government officials, authorities, and any other non-federal public entity in the United States of America. Alongside the MS-ISAC, CIS also operates the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) which is a critical resource for cyber threat prevention, protection, response and recovery for the nation's election offices.

The MS/EI-ISACs provide multiple security services to SLTT organizations, at the center of which is a 24x7 Security Operations Center (SOC). In the SOC, a joint security operations and analytics team monitors, analyzes, and responds to cyber threat events and incidents targeting U.S. SLTT government entities. The core services of the MS/EI-ISAC include:

- **Real-time network and endpoint monitoring.** Through tools such as the Albert Intrusion Detection Systems (IDS), Endpoint Security Services (ESS), Domain Name System (DNS) security through the Malicious Domain Blocking and Reporting (MDBR) offering, as well as other managed security products and services
- **Vulnerability research, scanning, and tracking.** Vulnerability analysts closely monitor the publicly known vulnerability landscape to identify, categorize, prioritize, and inform SLTTs of potential weaknesses in their environments, as well as performing assistance such as scanning and reporting, and providing resources for mitigation and remediation
- **Cyber Threat Intelligence (CTI) analysis and intelligence sharing.** CTI Analysts monitor federal government, third party, and open sources to collect, correlate, analyze, and enrich threat information in a rigorous and focused effort to make informed assessments about cyber threats, actors, and associated tactics, techniques, and procedures (TTPs). In addition to producing and disseminating traditional finished reporting, the MS-ISAC maintains a Threat Intelligence Platform (TIP) and intelligence sharing capability to provide the SLTT community with malicious indicators in a standard format
- **Monitoring of member websites for compromises and defacements.** MS-ISAC SOC analysts notify members of potential compromises identified based on the MS-ISAC's unique awareness of the threat landscape
- **Exercise support.** The MS-ISAC participates in federally sponsored cybersecurity exercises and acts as a voice for SLTT governments in planning meetings
- **Cyber forensics.** The Cyber Incident Response Team (CIRT) provides SLTT governments with digital forensics and incident response (DFIR) functions that include malware analysis, host and network forensics, and mitigation, remediation, and recovery support
- **Threat analysis and situational awareness.** The Liaison Officers and Analysts Team is assigned to the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Operations Communications Center (CIOCC) in Arlington, VA and

Pensacola, FL. The CIOCC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement

CIS is seeking to upgrade the core capabilities of the SOC through procurement of a Security Analytics Platform ("Platform") (sometimes referred to as a security event and information management (SIEM) capability). The selected Platform must support the SOC analysts in their primary role of managing, investigating, and reporting on events generated from the various monitoring services, member reported incidents, Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and other federal government reported incidents, CIRT incidents, and CTI.

1.2 Current Environment

Today, CIS utilizes an in-house and on premise developed platform called the SOC Control Panel (SCP) to notify analysts of events and incidents. SCP is built upon an Oracle database which stores incident and event notification information, metadata from events, and integrates with other CIS tools to allow for escalation workflows for MS/EI-ISAC member notifications. The current SCP is resource intensive and requires specialized Oracle database knowledge in addition to regular maintenance. The front-end to the SCP is written in PHP. In addition, the SCP is only available to CIS staff and no customer portal or access exists.

CIS has identified the need to replace the SCP and Oracle backend with a cloud-native commercial solution that will better allow for scalability, compatibility, disaster recovery, resiliency, searching, reporting, alerting, event correlation, and data aggregation.

1.3 Description of Deployment Objectives

SOC analysts need to analyze security event data in near real time in order to prevent or minimize the impact of attacks and breaches. The required Security Analytics Platform capabilities include the ability to collect, store, normalize, and aggregate log data and other critical data elements to support the timely investigation and response to cyber events. This includes providing critical information to directly support digital forensics and incident response (DFIR), event mitigation, recovery, and regulatory compliance, as well as event reporting for situational awareness and decision making. This document details the requirements and the process that will be used to evaluate the vendors' product offerings against the MS/EI-ISAC required capabilities.

The selected Security Analytics Platform will ingest and aggregate event data and logs produced by Albert sensors, endpoint security agents, next generation anti-virus (NGAV) software, syslog data from customer infrastructure devices, DNS records from MDBR, as well as NetFlow and passive DNS data stored in the MS-ISAC data lake. Figure 1 below visually depicts the MS/EI-ISAC environment that includes sensors transferring, in near real-time, threat data to the SOC for analysis. The platform will integrate with threat feeds via the TIP ('Analyst 1' in the figure), signature sources, and internal systems such as Salesforce for customer relationship management (CRM) and JIRA for ticketing. TIP integration will allow for automated enrichment of indicators in the platform facilitated by the knowledgebase stored within the TIP, speeding up the research and analysis process for SOC analysts, providing context for case management and triage, and ultimately allowing for faster decisions and action.

The MS/EI-ISAC has over 11,000 SLTT members and those organizations vary in the amount of MS/EI-ISAC products and services they consume. Thousands of member organizations rely on the MS/EI-ISAC as their Managed Security Services Provider (MSSP). More mature SLTT organizations have expressed a desire to have access to their security event data within the MS/EI-ISAC to conduct their own queries and analysis. The new security analytics platform solution will primarily be for the consumption and use of

MS/EI-ISAC staff, however it will need to have the capability to connect to a member portal, giving credentialed and authorized members the ability to do pre-defined queries of their data. This will require integration with an Identity and Access Management (IAM) solution for access control and data segmentation to ensure members are only able to access their own organization's data, while allowing MS/EI-ISAC staff visibility across all data sources.

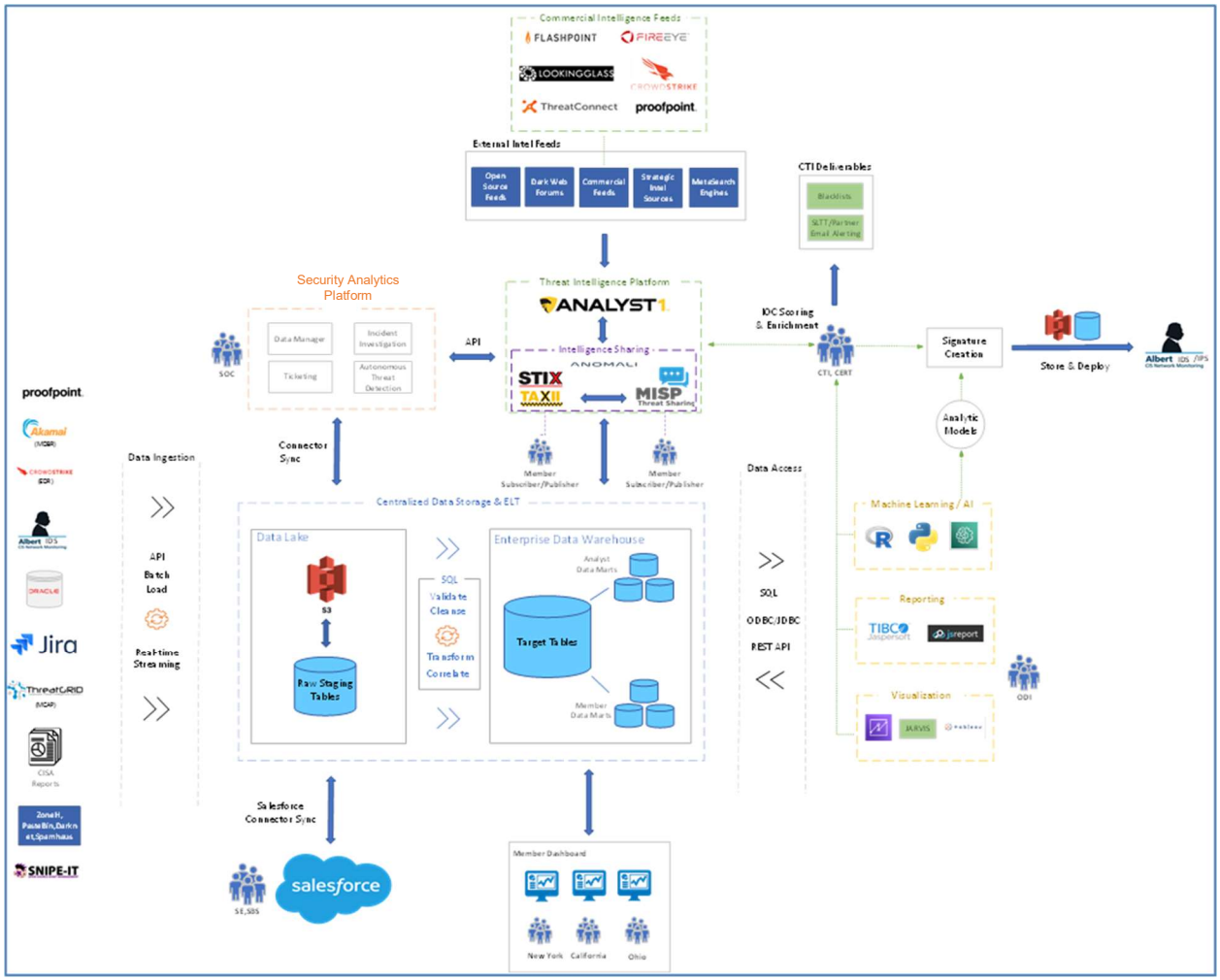

Figure 1: Concept of Operations Diagram

1.4 Clarifying CIS Definitions

For the purposes of this document, CIS uses the following definitions:

- **Albert**: CIS' proprietary Intrusion Detection System (IDS)
- **API**: Application Programming Interface
- **CIRT**: Cyber Incident Response Team
- **CISA**: Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security
- **CTI**: Cyber Threat Intelligence
- **Data Warehouse**: a large store of data accumulated from a wide range of sources within CIS
- **DHS**: Department of Homeland Security

- **DLApp**: CIS custom-built CRM and distribution list management application
- **EDR**: Endpoint Detection and Response
- **EI-ISAC®**: Elections Infrastructure Information Sharing and Analysis Center
- **ESS**: Endpoint Security Services
- **Integrate**: Integration between the proposed Platform and other systems requires that the Platform be able to recognize the syntax and semantics of the information being exchanged
- **Interface**: An interface between the proposed Platform and other systems can be accomplished via an API or other data exchange protocol to allow systems to exchange data
- **JHU APL**: John Hopkins University, Applied Physics Laboratory
- **MDBR**: Malicious Domain Blocking & Reporting
- **MS-ISAC®**: Multi-State Information Sharing and Analysis Center
- **MSS**: Managed Security Services – Leveraging a third-party relationship with Accenture, CIS offers the service of device management and log collection/correlation for infrastructure devices (firewalls, routers, switches, IDPS, etc.)
- **Netflow Data**: IP traffic flows for each connection in or out of a network interface is captured by our Albert devices. The Netflow Data contains information about the IP addresses, ports, duration of connection, volume of traffic and data transferred for each connection
- **PIQ data**: Product Installation Questionnaire
- **Salesforce**: Application used by CIS for Customer Relationship Management (CRM)
- **SCP**: SOC Control Panel – a custom developed system currently performing security analytics for the MS and EI-ISAC customers
- **SLTT**: State, Local, Tribal and Territorial
- **SOC**: Security Operations Center – the collection of tools and personnel that provide security operations, analysis, and support to SLTT organizations
- **UEBA**: User and Entity Behavior Analytics

1.5 Project Implementation Timeline

Event	Target Dates
Customer Onboarding on Platform	Beginning 01/03/2022
Training for CIS staff on Platform	01/03/2022 – 02/07/2022
Initial Go-Live	02/14/2022
Integration with CIS Systems	02/14/2022 – 07/31/2022

2.0 Instructions to Vendors

2.1 Schedule of Events

Event	Target Dates
RFP Release	09/27/2021
Offeror Questions (Accepted 09/27/21 – 10/07/21)	10/07/2021
CIS Response to Offeror Questions	10/15/2021
Proposals Due to CIS by **3:00 PM EDT**	10/27/2021
Notify Offeror of Demonstration Date/Time	11/03/2021
Demonstration / Presentations (Virtual)	11/10/2021 – 11/22/2021

3.0 Mandatory Technical Requirements

The MS/EI-ISAC requires an enterprise Security Analytics Platform that can meet the dynamic demands required of operating a SOC for a wide and varied membership in a modern environment. The list below outlines the requirements of the MS/EI-ISAC Security Analytics Platform. The requirements are focused on the software or code-enforced capabilities inherent in the Platform to include the ability to seamlessly link with existing as well as future tools and capabilities.

3.1 Mandatory Requirements

Ease of deployment, administration, and maintenance

- Platform shall be architected as a cloud-native application, not an on premise software package used on Infrastructure-as-a-Service (IaaS)
- Platform shall be capable of handling access to long term storage within the Amazon Web Services (AWS) cloud environment as well as with the Snowflake data warehouse architecture used by CIS
- Platform must have the ability to use single sign-on (SSO) and integrate with CIS's Active Directory (AD) environment for internal employee authentication and for the creation of security groups
- Platform must allow for granular, on-demand elasticity for data ingestion, computer, and storage requirements. CIS expects the Security Analytics Platform to be able to scale resource and compute needs automatically if necessary without human interaction to ensure events are not dropped or unnecessarily queued in the event of a surge. The software used by the Platform must also be architected to scale as CIS event numbers and data ingestion needs continue to increase
- Vendor must provide data that demonstrates an availability of the Security Analytics Platform that exceeds 99.5% *measured monthly* with no outages lasting longer than 30 minutes in duration. This includes all of the underlying infrastructure necessary for the Platform to operate, including the network, cloud infrastructure, and software
- Vendor shall have a documented disaster recovery plan that will be available to CIS upon request. Vendor shall demonstrate a minimum of biannual testing of their disaster recovery plan and agree to provide evidence of testing upon request of CIS
- Vendor shall agree to provide CIS with at least 72-hours' notice of any scheduled maintenance, upgrade, or other planned downtime and that CIS and the vendor shall mutually agree to when scheduled downtime may occur to minimize operational disruption
- Vendor shall provide CIS with the following as part of the onboarding activities: Technology health check to ensure cloud instantiation is functioning properly and that CIS has the necessary access, log source review to ensure data is flowing into the Platform as expected, implementation of default analytics (rules, signatures, behaviors, etc.), handover of fully functional production environment to CIS staff, and training in the administration and use of the Platform
- Vendor shall provide CIS with 24x7x365 phone support for the Platform and all related infrastructure, whether provided by the vendor or a third-party to the vendor (e.g., service provider) which have the ability to impact the confidentiality, integrity, or availability of the Platform

Information capture

- Platform shall have the ability to ingest data from on-premise collector appliances, agents, API access, batch ingestion, and on-demand acquisition from on premise and cloud-based sources
- Ability to have at least two separate indexes for the Platform to segment data and report on indexes separately
- Ability to consume native logs (i.e. syslog, auditd, and flat text files)
- Platform shall have the ability to correlate events to MITRE ATT&CK tactics and techniques
- Platform shall have the ability to aggregate data from a variety of disparate sources, source types, and indexes, normalize the data, and allow for searching across all sources while correlating events
- Ability to customize sources and source types at ingestion so that CIS can create rules to customize feeds and "train" the Platform at the point of ingestion
- Platform shall allow for data encryption at rest and in transit

Integration with other systems

- This Platform will be an analytics tool within the CIS data architecture and must be able to connect with our data warehouse (Snowflake) to receive logs and events as well as via other systems via direct connection and API. The platform shall include the ability to receive data inputs from Snowflake while also receiving data from external sources such as Albert IDS sensors. CIS currently ingests 40 GB of log data daily and that number will continue to grow. The Platform must be able to receive this amount of logs with capacity to expand and have a delay that does not exceed 5 minutes
- Vendor shall provide an API allowing the secure integration of the Platform to Jira
- Vendor shall provide an API allowing the secure integration of the Platform to Salesforce CRM

Log management and data archiving

- Platform shall support the creation of custom rules and signatures to allow for the correlation of events across any source, source type, index, or system
- Platform shall support indexing and advanced search function
- Platform shall support archiving or data warehousing of data on a pre-determined basis
- Vendor shall provide a capability that ensures that all CIS data will be removed/returned at contract termination and vendor shall provide sufficient time to move data off of vendor's systems if the vendor is not continuing to provide the Platform

Security event management (near real-time monitoring)

- Platform shall support the ability for users to create, modify, share, and delete customizable dashboards using data from any available source, source type, or index
- Platform shall allow users to schedule the frequency of queries to create notifications. For example, SOC management should be able to determine that events from EDR agents are sent to analysts every five minutes, where dashboard views showing Albert trends are updated every 2 hours

- The MS-ISAC SOC currently receives an average of 38 events every hour, or 912 events each day from a variety of sources. These volumes will continue to increase. The average response time between event detection and response is 6 minutes. The Platform shall have the ability to ingest, aggregate, correlate, and alert on (when appropriate) at this scale and beyond as the MS-ISAC continues to grow rapidly.

Business context

- Vendor shall provide an API to allow integration with our TIP (Analyst1) to allow for event enrichment

Advanced analytics

- Platform shall provide the ability to display raw ingested data as well as allow analysts to create custom searches with the Platform's language to create different views, filter data, tag data, create reports, and share information
- Vendor shall offer a Security Orchestration, Automation, and Response (SOAR) capability for the Platform, whether made by the Vendor or a trusted third-party that is certified as compatible with the Platform. The SOAR capability must be generally available (GA) and deployed to other customers using the Platform

Incident response and management

- Platform shall provide the ability to configure predefined escalation workflows
- Platform shall provide role-based control within workflows to support segregation of incidents and cases

User and resource access monitoring

- Platform shall provide the ability to audit all analyst activities
- Platform shall provide the ability to monitor the platform itself to alert analysts on conditions such as data feeds being down, more or less traffic than normally seen, configuration errors, system unavailability, resource contention, and licensing / consumption metrics
- Platform shall integrate with Okta for single sign-on and multifactor authentication

Reporting

- Platform shall support the ability to build in workflows for escalation (e.g., if one event is seen within 10 minutes it is less critical than if 5 are seen within one minute) and the ability to tailor alerts based upon escalation workflows. For example, alerts may be sent to analysts by the Platform in a number of ways (dashboard, via API, via email, etc.) and those alerts can be customized based upon the criticality of the alert and predefined escalation workflows that CIS will develop in the Platform
- Platform shall allow for the creation and sharing of customizable reports. Reports shall be available in editable formats (e.g., Word, Excel) as well as in PDF and the user must be able to make that selection
- Platform shall allow generation of standard and ad-hoc reports to meet specific business requirements such as data ingestion metrics, volume of events, events via different sources, source types, and indexes, licensing compliance, system health, and escalated events
- Platform shall provide the ability to schedule and distribute reports via email natively at a minimum

Cloud Security

- The Platform shall be resident in a GovCloud cloud environment with all systems and data residing within the United States
- Vendor shall demonstrate certification/compliance with formal third-party security evaluation, preferably ISO/IEC 27001 or AICPA SOC 2 Type 2

U.S. Citizen Requirement

Due to the sensitive nature of the MS/EI-ISAC and the relationship with DHS/CISA, any employee, contractor, or consultant that will be part of the implementation engagement or follow on support of this platform must be a United States citizen. Additionally, support personnel that will have access to CIS facilities or sensitive data must have a national agency background check within the last twelve months and may need to undergo a DHS Fitness Suitability determination. This requirement must be acknowledged within the final contract.

4.0 Desired Technical Features

The list below details the desired technical features of the MS/EI-ISAC security analytics platform. The desired technical features are focused on operational procedures, methodology, and work instructions that the platform should meet to be an effective capability for the MS/EI-ISAC SOC.

Ease of deployment, administration, and maintenance

- Platform shall support a multitenant environment to allow customers to see only their data and perform pre-configured queries against their own data

Log management and data archiving

- Platform shall support sigma formatted rules

Advanced analytics

- Platform shall use statistical models and machine learning to identify relationships between data and behavioral elements
- Platform shall support user entity behavior analytics (UEBA). Describe included UEBA capabilities (e.g., profiling, anomaly detection, prebuilt analytics, prebuilt use cases, risk rating, etc.) if available with the Platform

Reporting

- Platform has other report distribution methods such as direct upload to the cloud or integration with API

Cloud Security

- Platform shall provide a FedRAMP authorized offering, with an Impact Level of at least Moderate

5.0 Platform Demonstration in Response to RFP

Vendors must show how their proposed solution meets all of the required and applicable desired requirements outlined within this RFP in a Platform demonstration. Additionally, CIS will ask each vendor to perform a demonstration of the following CIS cybersecurity scenarios (based on real-world experiences

and situations) on a live Platform using the exact software being proposed to CIS. For each of the eight scenarios, the demonstration should enable CIS to understand the following:

- How your product will detect the activity identified in the scenario
- How the CIS SOC will be notified of this activity
- What would CIS expect to see and how
- What information will be available and how will it be made available
- How CIS could add value to assist the affected entity

5.1 Scenarios

I. **Scenario 1 – Detection of Brute Force Attack.** With the evolution of faster and more efficient password cracking tools, brute force attacks are increasing against the services of an organization. When configured, the security analytics platform should count the frequency of login attempts (failed or successful), multiple logins from the same IP address or geo-location, etc., so that a possible attack underway will get noticed and can generate an alert before the attack succeeds. Given the correlation of login attempts across the network, the platform should uniquely identify patterns that would be missed on an individual device.

II. **Scenario 2 – Detection of Malware Activity.** Organizations believe in protecting their network end to end; from their network perimeter, with devices like firewalls and Intrusion Prevention Systems (IPS), to the endpoint devices with security features like antivirus and multi-factor authentication. Most organizations collect reports of security incidents from these security products in a standalone mode, which brings problems like false positives and an overwhelming number of raw events.

    Correlation logic is the backbone of a modern security analytics solution, and correlation is more effective when built over the output from disparate log sources. For example, an organization can correlate various security events like unusual port activities in firewalls, suspicious DNS requests, warnings from Web Application firewalls and Intrusion Prevention System (IPS), threats recognized from antivirus, Host IPS, etc. to detect a potential threat. Malware activity should be detected by the Platform in the following ways:

    - Traffic/queries to malware domains/IPs
    - Unusual network traffic spikes to and from sources
    - Endpoints with maximum number of malware threats
    - Top trends of malware observed; detected, prevented, mitigated
    - Brute force pattern checks on Bastion hosts

III. **Scenario 3 – Detection of Suspicious User Behavior.** Reportedly, more than 30 percent of attacks initiate from malicious insiders within an organization. Insider behavior may be more challenging to detect given they already have access to the network. It is imperative that platform rules can be written to discover activity patterns of insiders that can alert on suspicious behavior.

    To counter such insider threats, a well-configured security analytics platform should collect and correlate the following to determine if there is a possible threat:

    - Account creation, deletion, and login patterns

- Multiple system logins
- System changes by user
- Data exfiltration
- Anomalous traffic patterns

IV. **Scenario 4 – Detection of Suspicious Network Behavior.** IT networks are growing ever more distributed, complex and difficult to manage. This makes it harder to visualize traffic and exploitation attempts across the network and its many ingress and egress points. The platform can be a valuable link to discovering the suspicious inbound and outbound connectivity and enrich that traffic information with details such as geo-location to make the traffic more meaningful. This suspicious traffic can indicate possible attacks underway including account compromises, data exfiltration, malware activity, DDoS events, and connectivity to known bad sites.

To discover the true nature of the network traffic, a well-configured security analytics platform should collect and correlate the following information to identify the suspicious behavior:

- Suspicious connections, connection patterns, and geo-locations
- Suspicious data transfers
- Excessive connections
- Account access attempts
- Connectivity to blocked and deny-listed sites
- Backdoor connections
- IDS/IPS exploits
- Spyware activity
- Man-in-the-middle activity

V. **Scenario 5 – Suspicious Device Behavior.** Log sources are the feeds for any security analytics solution. For platform services, logging levels are set in the system registry and sent to an on-premise collector or the platform manager for analysis.

An attacker, after gaining control over a compromised machine/account, tends to stop or reduce logging services so that their unauthorized and illegitimate behavior goes unnoticed. To counter such malicious actions, platform is configured to raise an alert if a host stops or dramatically reduces forwarding logs after a threshold limit.

Another common pattern found among compromised log sources is that attackers tend to change the configuration files of endpoint agents installed and forward a large amount of irrelevant files to the platform, causing a bandwidth choke between the endpoint agent and manager. This affects the performance of near real-time searches, storage capacity, dashboards and reporting. Rules and analytics can be implemented to handle this suspicious behavior of log sources. This scenario asks that the Platform demonstrate the detection capabilities for the described behavior.

VI. **Scenario 6 – Track System Changes and Authentication.** Attackers will install files, modify systems, use existing accounts or create new accounts to execute their attack. The attacker will leave a bread crumb trail of user authentication, source locations and system and file changes. All of these factors can be evidence that an attack is underway.

Platform rules are developed to track changes and administrative actions across internal systems and matching them to allowed policy. Detection of policy violations or behavior that is not normal is well within the scope of the platform detection capabilities. Here is a classic case that an analytics platform should easily detect: “root access from an unknown IP in a foreign country that you do not do business with at 3AM, leading to system changes”. This will raise alarms in the platform and provide specific actions such as adding IPs to a deny list or logging communications from various geographies, as well as provide a forensic trail to undo the specific changes. Furthermore, user login information is captured so accounts can be suspended, deleted or watched closely for additional activity. This scenario asks that the Platform demonstrate the detection capabilities for the described behavior.

VII. **Scenario 7 – Continuous Compliance Management.** Almost every business is bound by some sort of regulation, such as PCI-DSS, HIPAA, FFIEC/GLBA, and Sarbanes-Oxley (SOX). Attaining and maintaining compliance with these regulations can be a daunting time and resource intensive task. Platform technologies can address compliance requirements, both directly and indirectly.

Virtually every regulatory guideline requires some form of log management to maintain an audit trail of activity. Security analytics platforms provide a mechanism to rapidly and easily deploy a log collection infrastructure that directly supports this requirement, and allows instant access to recent log data, as well as archival and retrieval of older log data. Alerting and correlation capabilities also satisfy routine log data review requirements, an otherwise tedious and daunting task when done manually.

In addition, security analytics platform reporting capabilities provide audit support to verify certain requirements are being met. Most platforms provide reports that directly map to specific compliance regulations. Demonstrate these can be run with minimal configuration and will aggregate and generate reports from across the enterprise to meet audit requirements.

VIII. **Scenario 8 – Detection of Unknown Threats.** Many threats may elude perimeter or end point security. Advanced persistent threats (APT) which target a specific piece of data or infrastructure utilizing a sophisticated combination of attack vectors and methods to elude detection. For example, with Zero Day Threats the specific Malware is often not yet discoverable by the perimeter or endpoint protection.

Given the sophistication of APTs, enterprises must have an in-depth defense strategy to block activity beyond the perimeter (perimeter FW, IDS/IPS, internal FW, AV, multi- factor, etc.). All of these devices generate a huge amount of data that is difficult to monitor. A security team cannot realistically have several dashboards open and correlate events among multiple components fast enough to keep up with the packets traversing the network. Security analytic platform technologies bring all of these controls together into a single engine capable of continuous, real-time monitoring and correlation across the breadth and depth of the enterprise.

But what if an attack is not detected before entering the network or system? After a host is compromised, the attacker must still locate the target data and extract it. Advanced security analytics platforms use correlation engines are able to monitor for a threshold of unique values. For example, a rule that looks for a certain number of unsuccessful access attempts on TCP port 445 (or ports 137, 138 and 139 if NetBIOS is used) from the same host within a short time frame would identify a scan for shared folders. A similar rule looking for standard database ports would indicate a scan for databases listening on the network.

New attack vectors and vulnerabilities are discovered every day. Signature based detection solutions (FW, IDS, AV, etc.) are not equipped to detect zero-day attacks. An advanced security analytics platform can detect activity associated with an attack rather than the attack itself. For instance, a well-crafted spear-phishing attack using a zero-day exploit has a high likelihood of

making it through spam filters, firewalls and antivirus software, and being opened by a target user. An advanced security analytics platform can be configured to detect activity surrounding such an attack. For example, a PDF exploit generally causes the Adobe Reader process to crash. Shortly thereafter, a new process will launch that either listens for an incoming network connection, or initiates an outbound connection to the attacker. Many platforms offer enhanced endpoint monitoring capabilities that keep track of processes starting and stopping as well as network connections opening and closing. By correlating process activity and network connections from host machines, a security analytics platform can detect attacks without ever having to inspect packets or payloads. While IDS/IPS and AV do what they do well, demonstrate that the platform provides a safety net to catch malicious activities that slip through traditional defenses such as those described in this scenario.

6.0 Proposal Preparation Instructions

Deliver proposal materials (via email only) to Christina Hilts, Director of Procurement: christina.hilts@cisecurity.org.

6.1 Volume 1 – Technical (30-page limit)

For the written proposal, address each of the paragraphs below. No cost or price information may be included in Volume 1.

a. Technical Materials (20-page limit)

I. Provide a description of the proposed security analytics solution, including how CIS's requirements in Section 3 above will be met. Describe the major strengths of your solution that significantly exceed the stated requirement and how each strength will be beneficial to CIS

II. Identify any mandatory requirement specified in Section 3 or desired feature in Section 4 that is not fully met, and explain how that requirement can be satisfied using alternative means if appropriate or reflected in a commitment for the capability to be provided in a future release with the release timeframe identified. Any alternative means must be addressed during the demonstration

III. Describe two customer operational implementations of your solution that are of comparable size, scope, and complexity as described herein. The implementations must be in the cloud. Provide the contact information for each reference

b. Technology roadmap (10-page limit, included in the 30-page limit mentioned above). Describe major improvements, innovations, or substantive changes planned for your product during the next 24 months. This must also address Section 4, Desired Technical Features that are not currently available in the proposed products. CIS is willing to sign a non-disclosure agreement (NDA) to ensure appropriate protection of proprietary information if requested in advance of proposal submission.

c. Documentation (no page limit; not included in page limits)

I. Provide the complete API developer's documentation (or a URL reference) for your platform. This will be used to evaluate the specific functions you provide via API for monitoring and managing the platform

II. Provide a listing and details for the cloud services that the Platform can natively connect to via API or other means. Examples include AWS, Microsoft Azure/365, Jira, Okta,

Analyst1

d. Demonstration / Presentation Materials (12-page limit; not included in page limits)

I. Provide the presentation slides that will be used as further described in Section 6.2 below

6.2 Instructions for Demonstration

As part of the proposal, CIS requires a demonstration of capabilities offered in the proposal. The instructions below apply to that demonstration. The intent of the demonstration is to allow CIS to fully understand how your solution meets the technical requirements and how well your solution will enable CIS to detect, mitigate, and provide insight into various cybersecurity threats affecting CIS customers.

a. Where: The WebEx video teleconference will be setup by CIS for an up-to-180-minute demonstration with no CIS questions or interruptions, followed by a 60-minute break, and then a 60-minute CIS question and answer session. The teleconference may be recorded by CIS

b. When: 10-22 November 2021; CIS will provide a date and time

c. Who will attend from CIS: CIS senior executives, engineers, operations, sales, business services, program management, and procurement personnel

d. Presentation: Start with no more than 12 presentation slides to discuss the following features of your solutionto meet the technical requirements and features:

- The product name and any additional products and/or purchases required to demonstrate the CIS requirements stated in this CIS RFP and the demonstration tasks that are provided in Section 6 above
- Show the architecture of the solution. For example:
    - What is the relationship between the management consoles, agents, databases, correlated threat identification, and intelligence?
    - Describe where the elements of the proposed architecture can be hosted.

e. Demonstration: At the beginning of the demonstration, the offeror should explicitly identify any platform demonstration requirements in Sections 3 that will not be demonstrated and provide the rationale. Offerors are expected to demonstrate how their product will meet each requirement; this demonstration can be incorporated in the scenarios listed in Section 6, or if they cannot be incorporated into a scenario, then independently shown or discussed as appropriate

f. Mapping to Requirements: During the demonstration, the offeror should orient the CIS evaluators to the mandatory and desired requirements from Sections 3 and 4 that are being demonstrated. As noted, the offeror may choose to demonstrate mandatory or desired requirements as a part of the demonstrations of the provided scenarios.

- If the offeror chooses to do this, the offeror should provide the cross-reference information in Table 1 below to ensure the CIS evaluators know which requirements are being demonstrated as part of one or more scenario demonstrations or the appropriate slide number if outside of a demonstration
- This table below will not be counted as part of the page count limitation
- This table should be provided via email to christina.hilts@cisecurity.org at least one business day before the demonstration

g. Information offered in the demonstration will be incorporated into the contract

6.3 Table 1. Demonstration Cross Reference

	Identify Requirements from Section 3 Being Demonstrated
Scenario 1	
Scenario 2	
Scenario 3	
Scenario 4	
Scenario 5	
Scenario 6	
Scenario 7	
Scenario 8	

Note: There is no limitation on the number of rows for this table

6.4 Volume 2 – Vendor Profile, Support, Terms and Conditions, and Contract (10-page limit)

a. Vendor Profile. Provide a statement giving a brief history of your company, how it is organized, and how its resources will be used to meet the requirements of CIS. The vendor shall submit the following information:

- Location of your company headquarters
- Indicate the number of years your company has been in business
- The total revenue generated by your security analytics platform product
- The number of employees your company has, and how many of them are aligned to the platform business unit/product
- Indicate the number of deployments in production

- The average size of deployment for your security analytics platform solution in terms of volume (events per second or messages per day)
- Indicate the number of partners your company has that supports, provides integrations, and/or develops products for your proposed solution
- Whether you maintain an App Store or other marketplace where users can acquire integration bindles/content for your platform. If so, indicate the number of available apps

b. Vendor Support Services. Provide details on the below vendor support services for the Platform

I. Product Release Details

- Describe the product upgrade schedule and the overall lifecycle management of the Platform
- Describe your quality assurance process for software updates and the automated software assurance standards used to provide the software manifest and code signing (e.g., SWID, Co-SWID, SBOM)
- Indicate which third-party software packages are required for your application to function correctly (for example, operating systems, web servers, databases, agents or clients for backup). In addition, indicate who is responsible (the customer or the vendor) for purchasing and maintaining licenses for this software

II. Skill Set Requirements of Personnel

- Describe the skills needed by CIS to implement and support your product as outlined in this proposal
- Describe any management and/or monitoring service offerings provided directly by your company for your platform

III. Services and Support

- Attach a sample support SLA to your proposal. The SLA should cover topics such as availability, incident response time, incident resolution time, root cause analysis timelines, support levels, and on-site versus remote work. The SLA should also detail the exclusions, including third-party failures when calculating uptime
- Provide information on service credits available to CIS when the vendor does not meet the SLA and how they are applied to fees
- Provide details on the costs associated with vendor support for the Platform and the different tiers of support available to CIS. Provide details of the responsiveness and escalation options in the different support tiers
- Provide details on your disaster recovery and continuity of operations plans. Include what recovery options are available to CIS in the event of a critical outage with your platform
- Describe your cyber insurance coverage. Specifically, what indemnity clauses exist in the event a flaw or vulnerability is discovered in your platform that places CIS at risk. Additionally, discuss your company's risk management plan to continuously monitor and mitigate risks within the platform

IV. Professional Services

- Describe your approach for onboarding a new customer, integrating with existing systems, ingesting data, and your project management tools and methodologies for the proposed solution
- Identify the staff members who would be involved in onboarding CIS as a new customer to the Platform. Are they employees of your company? If not, provide a representative example of third-parties you may use that are all based in the United States
- Provide a detailed explanation of the roles and responsibilities between you as the vendor and CIS as the customer of your cloud-based platform. Specifically indicate responsibilities for outages and security events and incidents within the platform itself as well as vulnerability management processes for the Platform as a service offering

V. Training

- Describe what training for CIS staff is required or recommended to support the implementation of the proposed Platform
- Describe the training that accompanies the implementation of the system
- Is there a published schedule of classes? What is the fee schedule?

VI. Maintenance

- Describe your product support including facilities, staffing, and response times, etc.
- Do you have a 24/7 help desk? Where is it located? Is it staffed by your own employees, or is it a third-party facility?
- Discuss the maintenance programs available. Do you offer on-site support if needed? Highlight a program recommended for CIS. What are the price differences between the programs?
- What is the frequency of application/System updates and or point releases? How are they communicated to the customer? Are there critical releases, Bug fixes and or security release schedules?
- Do you provide maintenance or support on customization implemented during the initial installation?
- Does the maintenance program cover all future software upgrades? Explain
- What are the recommended staffing requirements for ongoing support of the proposed solution? Discuss in terms of full-time equivalents (FTEs)

6.5 Volume 3– Pricing

a. Price Model and Explanation.

Cost is an important factor to CIS. The Volume 3 shall include the following information:

I. Business model and pricing model description.

Describe your business model and explain your pricing. If licensing is part of your business model, please describe how this is done (e.g., consumption based, number of events, etc.) and provide tiered pricing options. This explanation should also explain the methodology for any pricing changes over the five-year contract period (e.g., no price

increases, no change in percentage discount from commercial price, etc.), including the pricing approach for new product versions or new product releases. This explanation should include the planned product changes described in the Technology Roadmap. The methodology will be incorporated into the final contract

II. Configuration Components and Pricing

- Provide a detailed price quote for the software proposed for this solution, with pricing for each component. Include list prices and discounted prices. Provide statements of work and project plans for each major phase (if applicable)
- Provide details on costs, if any, associated with bandwidth and data charges moving into and out of the platform. If costs are consumption based, provide the costs or tiers associated with data
- Provide details on any Platform usage charges, if any, including data movement (ingress/egress), bandwidth, consumption, resources, etc. If pricing is based on consumption, provide the costs and tiers associated with the amount of data consumed
- Provide pricing for a Five (5) Year Period of Performance Agreement: a two-year base contract with three additional one-year options

III. Service Pricing

- Provide hourly or daily professional services rates for technical services as well as training for CIS personnel

IV. Maintenance Pricing

- Provide prices for any maintenance contracts that you offer for your products

V. Terms and Conditions

- This should include the company's proposed terms and conditions for your products and services

7.0 Basis for Award and Evaluation Factors

7.1 Basis for Contract Award

- Contract award(s) will be based on an evaluation of best value to CIS
- All offerors will be evaluated for compliance with the RFP requirements. Offeror's written submission shall adequately detail technical capability to meet each of the mandatory product and technical services requirements. Note that any mandatory requirement(s) that are not met must be mitigated either by an alternative means of meeting the requirement or a commitment for the capability to be provided in a future release of the product.
- The two evaluation factors described below, Technical and Price, are of equal importance. The CIS goal is to provide the best solution at the best price. Within the Technical Factor, Sub-factors 1, 2, and 3 are the most important and listed in decreasing order of importance. Sub-factors 4 and 5 are of equal importance and combined are less important than Sub-factors 1, 2, or 3 individually.

7.2 Evaluation Factors

a. Evaluation Factor 1: Technical

I. **Sub-Factor 1: Demonstration.** Platform functionality (both mandatory requirements as defined in Section 3 and the desired functionality as defined in Section 4) as demonstrated in the scenarios described in Section 5

II. **Sub-Factor 2: Written proposal.** For requirements that could not be demonstrated, the vendor written proposal responses for each of the following will be evaluated (from Section 3): Ease of deployment, administration, and maintenance; Information capture; Integration with other systems; Log management and data archiving; Security event management (near real-time monitoring); Business context; Advanced analytics; Incident response and management; User and resource access monitoring; Reporting; and Cloud security

III. **Sub-Factor 3: Support.** CIS will use the vendor responses to Section 6.4(b) to evaluate the offeror's approach to support CIS's implementation from customer onboarding through ongoing support and maintenance of the Platform throughout the lifecycle of the contract

IV. **Sub-Factor 4: Product evolution.** This will include an evaluation of the expected evolution of the offeror's products and services as described in the Technology Roadmap.

V. **Sub-Factor 5: Past performance.** An evaluation will be made of customer operational implementations of the proposed solution that are of comparable size, scope, and complexity as CIS

b. Evaluation Factor 2: Pricing

I. **Sub-Factor 1: Pricing.** CIS will use the proposed vendor pricing in its evaluation, which includes, at a minimum, the software licensing price, licensing model (e.g., consumption based, event based, resource based, etc.) and the projected costs based upon CIS's volume of data and events. Other costs will also be evaluated including hosting costs, storage costs, bandwidth consumption costs, and other recurring and non-recurring fees as outlined in the proposal

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community- driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguardagainst emerging threats.

Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

To learn more, visit www.CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity