31 TECH VALLEY DRIVE, EAST GREENBUSH, NY, 12061
Request for Information (RFI) for

SLTT Endpoint Protection Platform (EPP) Program
22 February 2021

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 organizations 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. Additionally, CIS operates the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) to support the cybersecurity needs of election offices, Boards of Elections, Secretaries of State, Registrars of Voters and similar entities.

Clarifying Definitions. For the purposes of this document, CIS uses the following definitions for Next Generation Antivirus (NGAV), Endpoint Detection and Response (EDR) and Endpoint Protection Platform (EPP).

Next Generation Antivirus (NGAV). Next Generation Antivirus is a solution deployed on endpoint devices to prevent cyber-attacks. The capabilities for endpoint devices include:

1. Detect malicious activity using signature-based and behavior-based threat detection methods with the capability to automate prevention (block attacks).
2. Deny/allow indicators list management to include anomalous behavior-based indicators.
3. Endpoint and file quarantine functionality and threat notification and alerts.
4. A web-based management interface with a cloud-based data administration component for enterprise deployment.

Endpoint Detection and Response (EDR). Endpoint Detection and Response (EDR) is a solution deployed on endpoint devices to prevent cyber-attacks. The EDR services may include next generation antivirus, behavioral-based threat detection, threat hunting, root cause analysis, and remediation. The EDR capabilities may include:

1. All NGAV capabilities fully integrated with the EDR solution.
2. Behavior-based anomalous malicious activity detection with the ability to automate prevention (block attacks).
3. Out of the box integrations and application programming interfaces (API) to integrate with other security and operations tools (e.g., threat telemetry API; security information and event management (SIEM), and security orchestration, automation,

and response (SOAR) tools) and functions available in the EDR console that can also be performed through an EDR API. This would be used to extract threat and indicator details from each agent.

4. Integrated web-based service portal with an EDR services dashboard with role-based access control (RBAC).
5. Investigation and remediation capabilities needed for an analyst to manage the EDR services.
6. A cloud based EDR data administration component for enterprise deployment and capabilities that allow an analyst to:
    a. investigate and respond to dynamic security incidents and alerts;
    b. perform vulnerability assessments and virtual patching;
    c. perform asset discovery and baseline assets;
    d. perform remote threat hunt engagements with the ability to remotely collect endpoint data and logs.

Endpoint Protection Platform (EPP). An Endpoint Protection Platform is a solution deployed on endpoint devices to prevent, detect, respond to, and remediate security incidents and alerts. The standard EPP services include EDR and/or NGAV, asset discovery, virtual patching, remediation automation, vulnerability assessment, web filtering, data loss prevention, and a host firewall. The capabilities for endpoint devices include:

1. Integrated EDR and/or NGAV capabilities.
2. Web-based portal that allows investigation and remediation capabilities needed for an analyst to manage the EPP services. The integrated EDR and/or NGAV features should be fully integrated into the web interface along with the additional EPP features to include but not limited to the following:
    a. Monitor and control endpoint USB devices
    b. Asset discovery
    c. Vulnerability assessment
    d. Remediation automation
    e. Virtual patching
    f. Data loss prevention
    g. Host firewall
    h. Web filtering
3. A cloud based EPP data administration component for enterprise deployment and modules/views for all EPP offerings to include all EDR and/or NGAV functionality specified above fully integrated.

CIS SLTT Endpoint Protection Concept of Operations (CONOPS) (Elections Infrastructure Pilot)

The EI-ISAC is currently conducting an EDR pilot and has deployed agents on election infrastructure systems. Pilot activities started in February 2020 and will end in July 2021. During the pilot, EDR agents from a single vendor (CrowdStrike) were deployed to thousands of endpoints, which span across several hundred election entities. The EI-ISAC's primary role during the pilot is to act as a Managed Security Service Provider (MSSP). The CIS Security Operations Center (SOC) receives threat telemetry data from all of the EDR agents from the commercial service provider's virtual private cloud using a well-formed API. Figure 1 below details this concept of operations between the SLTT entities' IT environment, the EDR vendor, and CIS SOC analysts who access our existing EDR provider's web portal to view additional context about EDR agent generated alerts.

In addition to analyzing threat data, the CIS SOC is responsible for 'deny/allow' list management and 'indicators of actions rule' tuning. The EDR pilot vendor's portal also enables the CIS Device Engineering team to onboard new pilot participants and to manage all deployed EDR agents.

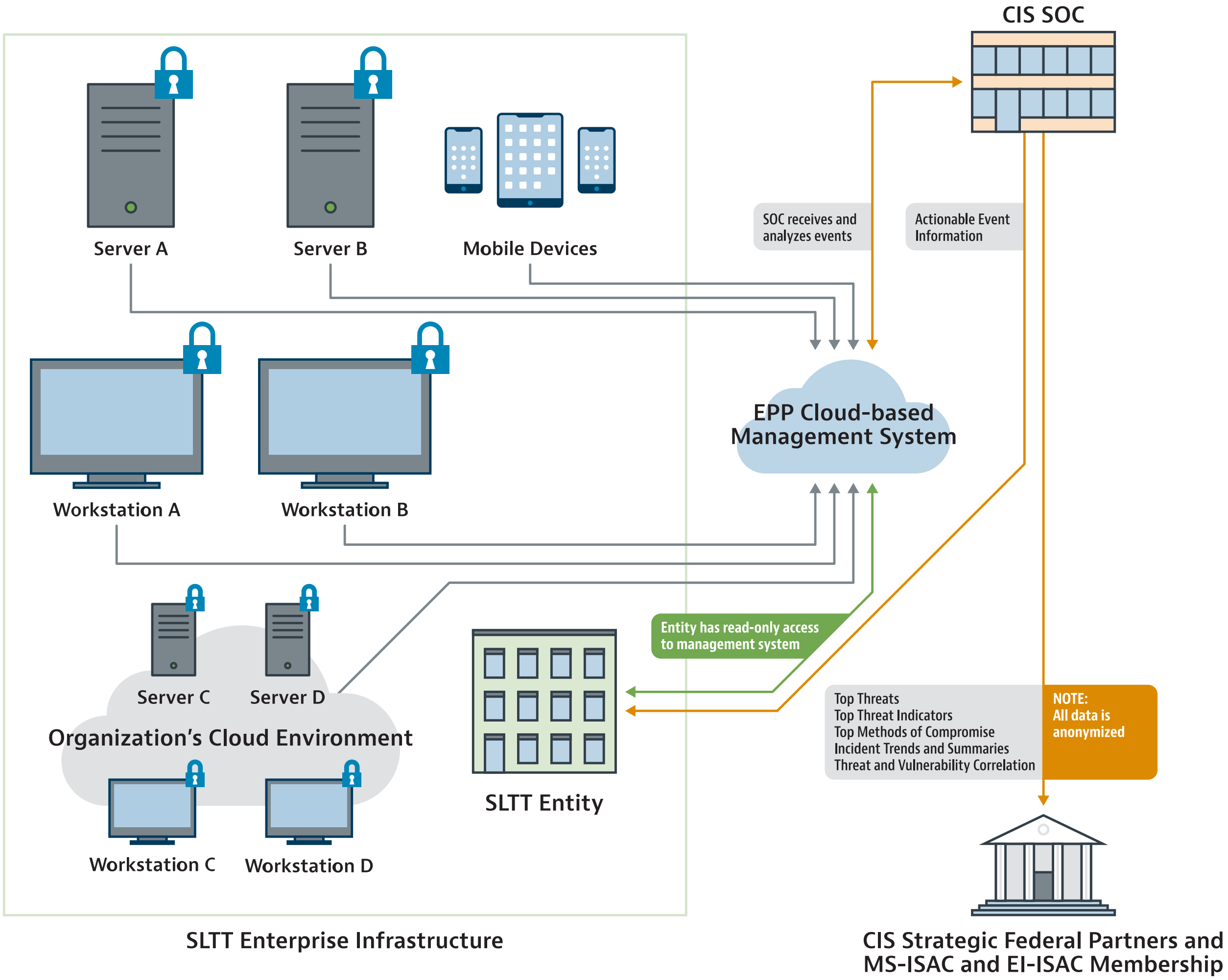
CIS SOC
Server A
Server B
Mobile Devices
SOC receives and analyzes events
Actionable Event Information
EPP Cloud-based Management System
Workstation A
Workstation B
Server C
Server D
Organization's Cloud Environment
Workstation C
Workstation D
Entity has read-only access to management system
SLTT Entity
Top Threats
Top Threat Indicators
Top Methods of Compromise
Incident Trends and Summaries
Threat and Vulnerability Correlation
NOTE: All data is anonymized
SLTT Enterprise Infrastructure
CIS Strategic Federal Partners and MS-ISAC and EI-ISAC Membership

Figure 1. EPP Pilot Data Flow

CIS SLTT EPP Managed Service

Based on the successful results of the EDR pilot, CIS is establishing a new CIS EPP service that will be offered to all SLTT organizations. Examples of how the EPP service may be utilized by SLTT organizations include, but are not limited to:

1. A fully managed solution where CIS would provide the EPP agents to the SLTT organization and act as an MSSP, responsible for configuration, monitoring, alerting, response and remediation, etc.

2. A partially managed solution where SLTTs may bring their existing EDR, NGAV, or EPP solution to CIS to manage and our SOC to monitor. This may include SLTTs managing and monitoring during regular business hours and CIS monitoring after hours.
3. A shared model for more mature organizations where both SLTTs and CIS can access the EPP portal for investigations and data queries.

SLTT organizations vary in size, scope, complexity, and variety of endpoint devices. The maturity of SLTT organizations to manage, protect, and monitor their network and endpoint devices ranges from limited capabilities to highly mature. CIS may offer and support multiple EPP solutions in order to accommodate SLTT organization's technical requirements and affordability constraints. We desire that each vendor respond to this RFI by explaining how their products satisfy the scope of the EPP requirements. If there are changes to the CIS SLTT managed EPP service offerings described above that we should consider, please provide information on that service offering.

Most of the EPP products and services will be purchased by SLTT members under the CIS Partner Paid program[1] to enable SLTT organizations to purchase products and services support using their funds. This concept is similar to another current CIS Partner Paid capability which is the Albert Intrusion Detection System (IDS) system that is managed and monitored by the CIS SOC. CIS expects Congressional funding for some initial portions of the SLTT EPP. The threat telemetry data from all selected CIS EPP vendor offerings will be integrated into the CIS SOC using a similar architecture used during the EPP pilot as portrayed in Figure 1 and the associated CONOPS.

Request for Information for SLTT EPP Program.

CIS intends to issue a Request for Proposal (RFP) leading to the award of multiple contracts to provide EPP software and a CIS SLTT EPP MSSP offering for SLTT government organizations.

This RFI is part of CIS's market research to determine the product and service capabilities of potential EPP commercial sources, as well as the details of planned future technical capabilities of your EPP solution. Your responses will be used to finalize the requirements for the CIS EPP RFP. This RFI will also be the basis for the selection of the vendors that will be issued a RFP for a 5-year EPP contract on behalf of SLTT government entities. These EPP capabilities will be integrated into the CIS SOC that currently supports MS-ISAC and EI-ISAC organizations and monitors security devices providing IDS, secure DNS, and EPP services supporting U.S. SLTT government organizations. The EPP capability may be installed, managed, and monitored on millions of SLTT endpoint devices.

The three attachments to this RFI provide the following:

Attachment 1. Specific questions and focus areas for responses to this RFI.

Attachment 2. Draft EPP technical requirements. We are soliciting your recommended changes and the associated rationale for the proposed changes.

Attachment 3. Information about the Planned EPP Demonstration in Response to the RFP.

[1] The Partner Paid program provides an opportunity for SLTT organizations to purchase products and services beyond the quantity funded by Congress. As an example, almost 800 'Albert' IDS systems and supporting monitoring are currently deployed to SLTTs. Approximately 200 of these are funded by Federal funds.

Interested parties should submit the RFI response materials identified below via email to Christina.Hilts@cisecurity.org by 2:00 PM EST on 19 March 2021.

1. Company Information.
    a. Company name, address, telephone number, fax number
    b. Point of contact for your contracting officer and EPP project manager (name, title, email address, and phone number).

2. Requested information:
    a. Responses to specific questions and focus areas for responses to the RFI (attachment 1). Responses are limited to a maximum of 15 single-spaced pages.
    b. Vendor comments on the Draft Technical Requirements (attachment 2) and Planned EPP Demonstration in Response to the RFP (Attachment 3). We are soliciting recommended changes and the associated rationale.
    c. An EPP capabilities package that is brief and concise. The capabilities package should clearly present evidence the interested party is fully capable of providing the required capability and may contain any information that the interested party deems relevant.
    d. Additional attachments may be provided but should be relevant information.

Key dates in the schedule are below:

Scheduled event	**Date**
RFI issued	2/22/2021
CIS Presentation to Vendors at **2:00 PM EST**	3/2/2021
Vendor RFI Response Due by **2:00 PM EST**	3/19/2021

At 2:00PM EST on 2 March 2021, CIS will conduct a virtual RFI session with vendors. During this session, CIS will make a presentation addressing CIS objectives, the EPP CONOPS, information about our SLTT customer base, the CIS business model, and additional information about the RFI. We will also address vendor questions that can be submitted via the chat functionality within WebEx or email. CIS will participate in a dialog with vendor participants. CIS leadership and key personnel will participate in this session. CIS will schedule and establish this WebEx video teleconference. Vendors interested in participating must submit their contact information via email to Christina.Hilts@cisecurity.org by 2:00 PM EST on 1 March 2021.

If further information/clarification is needed, please contact Ms. Christina Hilts, CIS Director of Procurement, M: 518.526.3937, Christina.Hilts@cisecurity.org.

ATTACHMENT 1

SPECIFIC QUESTIONS AND FOCUS AREAS FOR RESPONSES TO THIS RFI

The CIS objective for this RFI is to perform market research to better understand the current market and your plans for the future. CIS wants to avoid causing unnecessary creation of new materials when your existing materials/formats will adequately address the questions. It is acceptable for you to provide existing materials to address the questions and just provide a reference to the material in your response for the related question. If several questions are better addressed in a single consolidated response, it is acceptable to do so. You may also provide additional information beyond the items of CIS interest below. If you don't believe it is necessary to address certain questions because it is addressed in the aggregate of the materials you are providing, please note this.

1. **Strengths**. Describe the major strengths of your EPP solution that distinguish your solution in detecting and preventing known and unknown malicious attacks from your competitors.
2. Technology Roadmap. Describe major improvements, innovations, or substantive changes planned for your EPP product during the next 24 months. CIS is willing to sign an NDA to ensure appropriate protection of proprietary information if requested.
3. **Deployment.**
   a. Describe two customer operational implementations of your EPP solution that are of comparable size, scope, and complexity as the SLTT community described within this document. Specifically:
      i. One for an SLTT or Federal Government customer with the centralized EPP capability deployed within in a FedRAMP moderate or higher cloud environment.
      ii. One with an operations concept similar to that of CIS operating as your customer and serving as an MSSP, deploying and managing EPP for a federation of distinct small, medium, and large organizations.
   b. Describe how your solution allows for a federated/hierarchical organization model for use with the variety of SLTT organizations (e.g., in terms of size, scope, complexity, funding) supported by CIS. For example, if a state government wishes to deploy your solution to a variety of agencies, with different use cases and risk levels for agencies.
4. **Out of the box integrations and Applications Program Interfaces (API).**
   a. Describe what operating systems your product supports natively.
   b. Describe the capability of your EPP solution to easily integrate with other security and operations tools (e.g., SIEM, SOAR, email gateways, other EPPs, sandboxes, network defense tools, etc.). The description should include the current state of compatibility, technology used, protocols offered, and the maturity of APIs.
   c. Describe the capability to fully manage the administration, configuration, and deployment of the EPP capability at both the multi-organization and individual organization level. Discuss the complexity of deployment and uninstall of your EPP product.

5. **Cost**. Cost is the most important factor to many SLTT organizations. CIS has over 10,000 MS/EI-SAC members that represent SLTT organizations using over 14 million endpoints. These organizations range from having no EPP capability to mature implementations. The CIS goal is to provide a range of coverage for all SLTT organizations that is optimized for their level of risk and available funding.
    a. Describe your business model and pricing structure:
        i. In particular, CIS is interested in the ability to offer varying level of EPP capabilities at different price points for SLTTs based upon their level of risk and budget. Provide information on capability or module based pricing, if any.
        ii. Describe pricing in the context of CIS acting as an MSSP with your EPP product.
        iii. Describe any changes in pricing based on the number of deployed endpoints (e.g., tiered pricing models).

6. **MITRE's ATT&CK Matrix.** Describe how the MITRE ATT&CK Framework can be used with your EPP solution**.** Also**,** provide the percentage of threat techniques as defined by MITRE's ATT&CK Matrix for Enterprise and ATT&CK Matrix for Mobile that your EPP solution detects and what percentage are prevented (blocked).

7. **Support/Training**.
    a. Describe your company's recommended support services that should be included in the EPP contract with CIS (e.g., training, deployment support, level 1 and 2 technical support, onsite or virtual technical support to CIS SOC).
    b. Describe the training that is available and recommended to understand and work with your EPP solution to ensure that CIS and SLTT security operators have the required skills to put the capability to proper use.
    c. Confirm your ability to provide training and technical support using only U.S based U.S. citizens.

ATTACHMENT 2

DRAFT EPP TECHNICAL REQUIREMENTS

The CIS preliminary EPP technical requirements are stated below. We are soliciting your recommended changes and associated rationale.

Please do not address each requirement. You should only address areas such as those below:

- Requirements that need to be clarified or changed. Please provide the recommended change and associated rationale.
- Identify any requirements that as stated your solution can not fully meet. Please provide recommended changes and the rationale.
- Unnecessary requirements that should be deleted or that should be optional.
- Provide any insights that would be useful for CIS to consider in the RFP.

1. **Mandatory EPP Product Requirements**

   a. EPP agents deployed on endpoints to be centrally monitored and managed by CIS as an MSSP.
   b. EPP capabilities to include the detection and blocking of both known (signature-based) and unknown (behavior-based) threats on an endpoint in addition to detailed host visibility and statistics.
   c. Ability to deliver host-based threat detection capability to endpoints, regardless of device type or the location of the SLTT endpoint (e.g., cloud, on-premise or remote employee system, desktop, laptop, or mobile tablet/handheld device). The types of operating systems that shall be supported are Windows, Linux, and Mac OS operating systems. Mobile devices (i.e., iOS, Android) will be supported as well.
   d. Ability to manually quarantine compromised systems remotely to prevent further system compromise and/or attacker lateral movement, while still allowing an administrator to take remediation actions.
   e. Capability to detect and block unknown security threats (e.g., new malware, malware variants, or malicious threat actors interacting with compromised systems).
   f. Capability that includes signatureless protection and use of behavioral-based methods that use Machine Learning and/or Artificial Intelligence learned algometric models for threat detection and blocking.
   g. Capability of the EPP agent to gather and retain gathered endpoint activity metadata in a CIS specified centralized storage location for later examination.
   h. Capability of the EPP agent to retain all the metadata collected (e.g., a broad range of event metadata types such as event logs, process and thread callbacks, file system and process instantiations, and network connections).
   i. Capability to send captured EPP log data to a CIS specified log collection platform in a standard log format such as syslog, CSV, or JSON.
   j. Capability to use “zero touch” provisioning to rapidly implement the EPP agents on SLTT organizational devices. Installing, configuring, and operationalizing many

locations must be accomplished in a short period of time. Specifically, this should happen in hours, not days or weeks.

k. Capability to uninstall all vendor EPP related components rapidly from SLTT organization endpoints. This agent removal must support many locations.
l. Minimal system performance overhead on endpoint devices during initial installation, daily use, and uninstall (e.g., CPU overhead does not affect end-user productivity and no compatibility issues with other applications installed on endpoints).
m. Capability to provide federated controls for the purposes of limiting or granting access to SLTT EPP data (e.g., alerts, event data, and forensics) within a multi-level hierarchical structure that is controlled by CIS.
n. Ability to customize configurations for individual CIS customers' environments without affecting global configurations.
o. Capability for CIS and SLTT organizations to perform ad hoc queries on the EPP data being captured for their respective organizations.
    i. The EPP capability should be able to capture, store, index, and correlate real-time endpoint data in a searchable repository from which CIS can generate ad-hoc reports, alerts, dashboards, and visualizations for any specific SLTT organization, organizational subcomponent, a combination of CIS specified organizations, or all SLTT CIS supported organizations.
    ii. CIS desires at least 30 days of storage (e.g., for alerts and associated device logs). If provided as part of a cloud SaaS solution. Tiered pricing should be proposed (e.g.,14 days, 30 days, 60 days, and 180 days based on best commercial practices).
p. Capability of the proposed solution to align malicious activity detections with the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework and classify detected attacks based on the techniques described there. These include ATT&CK Matrix for Enterprise and ATT&CK Matrix for Mobile.
q. Allow for the EPP capability to be monitored by the SLTT organization leveraging the service in addition to the monitoring and management provided by CIS (see figure 1 and associated description).
r. Capability of the EPP tool to easily integrate with other security and operations tools, such as a SIEM, SOAR, additional EPPs, and network sandboxes. This includes access via mature product APIs to allow CIS applications, as well as other COTS products, and access to the EPP-generated data and EPP security events.
s. Availability of all commercially released fixes, updates, and upgrades for the proposed EPP product capability.
t. Capability for an administrator to request that an arbitrary file, process memory image or full-system memory image be uploaded on demand to a centralized location for the purposes of later analysis.
u. Ability to fully manage the administration, configuration, and deployment of the EPP capability at both the global and individual organization level from onboarding origin to operational monitoring through mature product APIs.
v. A way to enforce a limit on the total number of EPP endpoint agents for individual organizations within the CIS EPP program. This would be used when an organization has purchased fewer licenses or subscriptions than their total population of endpoints to avoid exceeding the limit imposed on usage.

w. Capability to be installed and then operate simultaneously in either Primary (Active) or Secondary (Passive) mode with widely available COTS antivirus software from other vendors currently used by SLTT organizations.
x. AWS or Azure GovCloud instances of the platform must be available.
y. Capability to automatically consume custom indicators of compromise or malicious behavioral patterns for the purposes of malicious activity detection.
z. At least 30 days of storage (e.g., for alerts and associated device logs).

2. **Desired EPP Product Features**

   a. STIX/TAXII and/or MISP protocols integration or another industry standard for threat intelligence sharing.
   b. Not require a reboot of endpoint devices after installation or removal of the endpoint agent or for periodic commercially released updates and upgrades.
   c. Use of machine learning and artificial intelligence capabilities to enhance detection of threats.
   d. A “device control” component for controlling and monitoring the external devices connected to a monitored endpoint.
   e. A real time response capability to allow Cyber Incident Response Team (CIRT) members to conduct live investigations into machines that are potentially compromised by malicious actors.
   f. API access to intelligence feeds based on the vendor’s global threat knowledge.
   g. Additional tools that empower proactive threat hunting activities across the monitored endpoints.
   h. Asset inventory and patch management capabilities.
   i. FedRAMP moderate or higher compliant infrastructure.
   j. Web filtering.
   k. Host firewall.

3. **Mandatory Antivirus Requirements if Offerors EPP capability requires use of the Offeror’s Antivirus solution.** There are several different Antivirus products in use across the SLTT organizations. If the proposed EPP capability requires the Offeror’s Antivirus capability, the following requirements apply.

   a. Ability for vendor’s Antivirus capability for SLTT endpoints to be centrally monitored and managed by CIS.
   b. Capability to prevent and protect endpoints from malware, exploits, malware-free intrusions, advanced persistent threats, and other attacks.
   c. Ability to use “zero touch” provisioning to rapidly implement the Antivirus capability on SLTT organizational devices. Installing and operationalizing many locations must be able to be accomplished in a short period of time (hours versus days and weeks).
   d. Capability to be installed and then operate simultaneously in either Primary (Active) or Secondary (Passive) mode with widely available COTS Antivirus software from other vendors that is currently used by SLTT organizations. If the SLTT organization requires continued use of their current Antivirus capability, CIS plans to offer the EPP solution with two options to detect and alert anomalous behavior. However, the vendors proposed costs and acceptability of the proposed options to SLTT organizations may result in changes to the options below:

   i. Option 1: The EPP vendor's Antivirus solution operating in Primary (active) mode with the SLTT's organizations current Antivirus solution operating in a Secondary (Passive) mode; or
   ii. Option 2: The EPP vendor's Antivirus solution operating in Secondary (passive) mode to detect and alert anomalous behavior, as a value-added capability, to augment the SLTT's organizations current Antivirus solution operating in a Primary (Active) mode.

e. Minimal system performance overhead on endpoint devices during initial installation, daily use, and uninstall (e.g., CPU overhead does not affect end-user productivity and no compatibility issues with other applications installed on endpoints).
f. Capability to automatically uninstall a competitor's well-known COTS Antivirus or EPP software on specified SLTT endpoints.
g. Capability to automatically uninstall the proposed Antivirus capability from specified endpoints without adversely affecting the endpoint, other endpoint applications or end-user experience.
h. Capability to disable the existing Antivirus capability on the endpoint, or re-enable and reconfigure the existing Antivirus to run as the secondary Antivirus solution and the proposed Antivirus solution to operate as the primary Antivirus capability.
i. Ability to fully manage the administrative, configuration, and deployment of Antivirus at both the global and individual organization level from onboarding origin to operational monitoring through mature product APIs.

ATTACHMENT 3

Planned EPP Demonstration in Response to the RFP

As part of the final RFP, CIS will request a demonstration from the offerors. The WebEx video teleconference will be setup by CIS for a 90-minute demonstration followed by up to a 90-minute CIS question and answer session. The instructions below apply to that demonstration. If you have comments, suggestions, or questions about the demonstration instructions, please include them in your RFI response.

1. Start with no more than twelve presentation slides to discuss the following features of your EPP solution to meet the Draft EPP Technical Requirements:
    a. The EPP product name and any additional products and/or purchases required to demonstrate the CIS EPP requirements stated in the CIS RFI and the demonstration tasks below in paragraph 2.
    b. Show the architecture of the solution. For example:
        i. What is the relationship between the management consoles, agents, databases, and threat intelligence?
        ii. Where can they be hosted?

2. Perform a demonstration of the following on a live management system or a representative management system:
    a. **Management**:
        i. Demonstrate how to install and uninstall the EPP capability on endpoint devices (e.g., Windows, Linux, Mac, iOS, and Android endpoints).
        ii. Demonstrate how roles-based access is implemented, how you implement end-to-end session encryption (e.g., TLSv1.3), and any integration options for multi-factor authentication.
        iii. Demonstrate capability to integrate with other security and operations tools (e.g., SIEM, and API's) .
        iv. Demonstrate information and management capabilities available to SLTT organizations.
    b. **Prevention**:
        i. Demonstrate how an administrator would find un-protected clients on the CIS-managed endpoints that do not have the proposed CIS EPP agent installed.
        ii. Show a dashboard or reporting showing the list of vulnerabilities and misconfigurations on endpoints under CIS MSSP EPP management.
        iii. Drill into the dashboard to show the options available to fix/remediate agent health issues for exposed agents and reported on the dashboard.
        iv. Show a report that outlines the configuration of the product for different groups of users. CIS needs to understand the common configuration(s) and also which users have exclusions or additional policy elements enabled. Show how conflicting rules are identified, resolved, and executed.
        v. Starting from a false positive alert, show how an administrator would properly clear the false positive alert and options to prevent similar future false positives.

c. **Detection**:
    i. Show how the EPP capability can automatically consume threat feeds to automate Indicator of Compromise (IOC) searching. These should not be batch updates.
    ii. Show the incident response investigation actions for an incident in which an adversary moves across multiple devices using different attack tools.
        1. Starting with the dashboard incident response event queue, demonstrate how to step through available information to answer the following questions:
            a. What is the extent of the breach?
            b. How did the breach happen (e.g., root cause and the connection between machines)?
            c. What did the hacker or malware do while it was active?
            d. How do we restore the system with confidence that all traces are destroyed?
            e. Is this a random attack, or a targeted attack, and if so what are the attacker's goals?
            f. How do we prevent it from happening again?
    iii. Demonstrate how PowerShell or script misuse is detected, and how 'approved' PowerShell or script use is monitored.

d. **Hunting**:
    i. Demonstrate a complex hunting query. Also, demonstrate automation of the query and create a rule to block the activity in the query from executing.
    ii. Search for and show all data you have for a non-malicious process used in the last 7 days for PC, Linux, Mac, iOS, and Android endpoints. Describe how/when off-line/disconnected clients respond to the queries above (i.e., real time query vs database search).

e. **Response**:
    i. Show remediation action options (such as kill process, or network isolate) across multiple machines impacted by the incident.
    ii. Show any automated actions and how automation can be modified.

f. **Other**: Show innovative features of your choice not already covered.

3. Perform a demonstration of the following scenarios on a live management system or a representative management system for the following CIS cybersecurity scenarios. The intent of these demonstrations is to allow CIS to better understand how your solution will help detect, mitigate, and provide insight into various cybersecurity threats affecting CIS customers. The scenarios below have been constructed based on real-world experiences and situations. For each of the scenarios, the demonstration should enable CIS to understand the following:

    a. How your product will detect the activity identified in the scenario?
    b. How your product will be able to mitigate the scenario?
    c. How the CIS SOC will be notified of this activity?
    d. What would CIS expect to see and how?
    e. What information will be available and how will it be made available?
    f. How could CIS add value to assist the affected entity?
    g. From a CIS SLTT customer standpoint - what would the affected entity see?

h. How effective is your EPP capability in preventing adverse effects if it is not installed on all of an organization’s endpoints?

Scenario 1 - Public Facing Server Compromise. A public facing server has Microsoft's Remote Desktop Protocol running and open to the Internet. Adversaries identify the service running on the server and bombard it with brute force login attempts, eventually brute forcing the password and successfully logging into the server.

Scenario 2 – Ransomware. An end-user's workstation has become infected with Ransomware. In addition to the questions above, how quickly does your solution detect the malware? Can your solution prevent the encryption key from being downloaded if the malware successfully executes? Can your solution stop the encryption process if the download of the key is successful? Can your solution protect network mapped files from being encrypted by a single infected endpoint?

Scenario 3 - Nation-state Threat Actor Compromise. An unsuspecting user opens a malicious Word document attached to an email, which places a backdoor onto the victim's system. The adversary then leverages the backdoor in order to remotely interact with the compromised system and later begins to move laterally throughout the network.

Scenario 4 - Malware Spreading via SMB. A local government experienced a malware infection that was able to spread across the entity's entire network due to the organization utilizing a "flat" network and allowing unrestricted Server Message Block (SMB) communication between systems. Ultimately, it was identified that the malware was able to propagate across the entire network by leveraging a well-known, unpatched Windows vulnerability.