ADDENDUM #1- Responses to Requests for Information

Posting Date 2/12/2024

Request for Proposals # 1855-24:
Security Operations Center as a Service

Note: If similar questions were received by multiple parties, questions were combined to form one question representing intent and answered below. In most instances, questions retain wording verbatim, so grammatical and other errors are not on behalf of EHPS.

1. It looks like you would like the SOCaaS provider to provide you with your SIEM and EDR tools? Is that correct, or will you all be providing the tools and vendor will managing them? Can you clarify on who you expect to own the tools?
    a. We are open to the vendor providing the tools, or using the tools we have (additional information will be provided to the awarded vendor), but we are currently looking to only have our Firewalls and Servers monitored at this time. All other offerings can be added as options.
2. Additionally, can you provide clarification on how this SOC is being monitored today? Are you leveraging a partner, if yes, why are you looking to move away from them?
    a. Currently, our Network Administration Team monitors the SIEM, XDR, and other security info.
3. Finally, if your current provider is giving you all their tools, would you be open to proposal that include a professional services option to build your own tools/create the policies and rules specific to your environment and then a MSSP to support that once it's created?
    a. We currently own our tools, and are open to continue to do that.
4. Can you provide information on the number and types of servers, endpoints, and network devices to be managed?
    a. This RFP covers 4 Firewalls (2 HA Pairs) and approximately 60 servers.
5. Is there an incumbent provider?
    a. No
6. Is there a local preference?
    a. No
7. Can you confirm the number of endpoints and users that you would like protected?
    a. 4 Firewalls (2 HA Pairs), approximately 60 servers. We currently have approximately 9,000 users.
8. What is the scope of network and system appliances that need to be monitored? Both make, model and quantity?
    a. FortiGate firewalls, Dell, Supermicro, and virtual servers.
9. Which logs need to be retained and what is the required retention period for these logs?
    a. We have no preference

10. Can you please provide an estimate of the amount and size of the logs that need to be retained per day?
    a. We are currently collecting approximately 30GB per day from the firewalls. We don't have an estimate for the server logs.
11. Do you require Contractor to provide an EDR product or has East Hartford Public Schools already deployed an EDR product which needs to be leveraged?
    a. We are open to any proposal, but we do currently have our own XDR product
12. How many endpoints, both end-user devices and servers, are in scope for the service?
    a. 4 Firewalls (2 HA Pairs), approximately 60 servers. We currently have approximately 9,000 users.
13. Does Contractor need to provide a SIEM or is there a SIEM in place which needs to be leveraged?
    a. We are open to all proposals, but EHPS does have a SIEM that we have the licensing for and we are willing to expand our current SIEM configuration
14. What are the expectations of a SIEM and what will the SIEM be used for?
    a. Collect and analyze server and firewall logs
15. Is the use of a SIEM solution a requirement by any standard or regulation that East Hartford Public Schools needs to adhere to?
    a. No
16. Please provide a detailed description of what is meant by SOC resilience.
    a. 24/7/365 monitoring from more than one SOC office to have coverage in the event of an outage
17. What is the overall size and scope of the environment which is to be monitored as part of the SOCaaS to be provided?
    a. 4 Firewalls (2 HA Pairs), approximately 60 servers. We currently have approximately 9,000 users.
18. Is day-to-day (operational) configuration management of East Harford Public Schools' controls in scope for this RFP?
    a. We are open to all proposals, and vendors can offer multiple options
19. Is East Harford Public Schools looking for a responsive, after-the-fact SOCaaS or rather a prevention-focused SOC which strives to structurally improve East Hartford Public Schools' security posture with each and every interaction?
    a. We would want both
20. Does East Hartford Public Schools require the SOCaaS-provider to have 24x7x365 eyes-on-glass availability of skilled and experienced SOC-analysts?
    a. Yes
21. Number of employees at EHPS?
    a. Approximately 1,900
22. Is onsite support required, or will remote support utilize tooling to isolate the endpoint where EPHS provides remediation to a known good state?
    a. On-site support would not be required.
23. Does EHPS have an existing logging pipeline solution in place today? If so, what tool/solution?
    a. We currently have a SIEM, as well as other tools. Details will be provided to the awarded vendor.
24. Number of endpoints at EHPS? How many are workstations and how many are servers?
    a. Endpoints are not part of the scope of this project. Approximately 60 servers.
25. Does EHPS have an existing EDR tool? If so what vendor?
    a. Yes. Details will be provided to the awarded vendor.

26. Will EHPS require the provider to use the existing EDR tool in place, or bring tooling in as part of the offering?
    a. EHPS has an XDR solution in place.
27. Will the provider be proactively engineering the EDR tool?
    a. Awarded vendor should be monitoring XDR solution, but EHPS will be creating the policies. We are unclear on the meaning of this question.
28. Does EPHS have a SIEM today? If so, what vendor?
    a. Yes. Details will be provided to the awarded vendor.
29. What is the volume of data ingested per day in GB?
    a. We are currently collecting approximately 30GB per day from the firewalls. We don't have an estimate for the server logs.
30. What are the data retention requirements of all logs?
    a. No preference
31. Is the solution provider to bring a new SIEM as part of the offering?
    a. We are open to all proposals, but EHPS does have a SIEM that we have the licensing for and we are willing to expand our current SIEM configuration
32. If the existing SIEM is to be used, are all data sources currently being ingested?
    a. No
33. Is Digital forensics in support of cybersecurity use cases, or for legal proceedings requiring Chain of custody and litigation support?
    a. Cybersecurity use
34. Does EHPS have an on-site evidence storage facility?
    a. No
35. Define Incident response
    a. The actions taken to protect a network environment in response to a data breach or cyber attack
36. Define Cyber hunt
    a. Deep diving to find malicious actors in your environment that have slipped past your initial security defenses
37. Define Logging-as-a-Service
    a. A cloud-based solution for the storage and analysis of event and security logs
38. Define Endpoint Detection and Response (EDR)
    a. Real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities
39. Define Managed Security Information and Event Management (SIEM)
    a. A central log repository that allows for the detection, analyzation, and response to security threats before they harm business operations
40. Define Client portal for metrics and dashboards
    a. A web portal to view current information regarding the security of our network
41. Define SOC resilience
    a. 24/7/365 monitoring from more than one SOC office to have coverage in the event of an outage
42. Define Forensics
    a. Identifying, acquiring, processing, analyzing, and reporting on electronic evidence
43. Define Onboarding and customer support
    a. Working together and keeping documentation on configuration and initial tasks needed for a service to commence

44. How many Users?
    a. Approximately 9,000 users
45. How many Servers?
    a. Approximately 60 servers
46. How many Firewalls?
    a. 4 firewalls (2 HA pairs)
47. How many Routers?
    a. Routers are not in the scope of this RFP
48. How many Devices (Laptops, Desktops, Ip Phones, Mobile, Tablets)?
    a. Endpoint devices are not in the scope of this RFP
49. Guidance/Information on storage requirements for logs, live, archive of data timeframes. Do we keep all history/information/records/events for 1 year, 2 years, or other?
    a. No preference
50. What security applications do currently have and run already: EDR, SIEM, MFA, FIM, etc.?
    a. XDR, SIEM, MFA
51. Do you currently possess any licenses, specific vendor and volume currently?
    a. We currently have licensing for XDR and SIEM
52. Do you have any regulatory compliance requirements and need a Cybersecurity Assessment?
    a. Our cyber insurance does have regulatory compliance requirements. We do not need a Cybersecurity Assessment as part of those requirements
53. Who is your incumbent provider(s) today, and what level of service are they providing in each area?
    a. We do not have a current incumbent provider
54. Are you comfortable with having a US Based SOC or do you prefer a US Based SOC?
    a. We have no preference as long as US data regulations are met, and all of the requirements of this RFP are met
55. Are you comfortable with a pure SaaS solution that has minimal or no up-front costs?
    a. We are open to all proposals, and vendors can offer multiple options
56. What is total number of systems within EHPS campus? Please share inventory of end point and systems, servers, network devices to be cover under this scope of work.
    a. 4 firewalls (2 HA pairs), approximately 60 servers
57. What is the current infrastructure posture? On premise, On cloud or Hybrid?
    a. The devices within the scope of this RFP are on-premise
58. What is current Endpoint Detection and Response tool used by EHPS?
    a. Details will be provided to the awarded vendor
59. What is current Network and System monitoring tool used by EHPS?
    a. Details will be provided to the awarded vendor
60. Can you describe the types and volumes of data you handle?
    a. Details will be provided to the awarded vendor
61. What are the primary security concerns or challenges that EHPS is facing?
    a. We are looking for SOCaaS to improve our security posture overall
62. Are there any specific threats you would like to share with us?
    a. No
63. What your expectations regarding the detection and response time for security incidents?
    a. The expected response time would depend on the severity of the security incident
64. Are there specific contractual terms, conditions, or SLA, EHPS is seeks from SOCaaS provider?

a. The contract would have to comply with the terms of the E-Rate Pilot Program

65. Are there specific regulatory or compliance standards EHPS needs to adhere to, such as FERPA or COPPA?
    a. No FERPA or COPPA related data is in scope of this RFP
66. What is the number of workstation/laptops?
    a. Workstations/laptops are not in the scope of this RFP
67. What is the number of servers?
    a. We have approximately 60 servers
68. How many endpoints are running on Windows OS?
    a. We have approximately 50 Windows Servers
69. How many endpoints are running on Linux OS?
    a. We have less than 10 Linux servers
70. How many endpoints are running on MAC OS?
    a. None that are covered under the scope of this RFP
71. What is the number of Firewalls?
    a. 4 firewalls (2 HA pairs)
72. What Cloud services do you have?
    a. None that are covered under the scope of this RFP
73. What email service do you have, (O365?) is there a SEG?
    a. Our email system is not in the scope of this RFP
74. Should Data Residency be in the USA or is Canada acceptable?
    a. We have no preference
75. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?
    a. We have no current or previous incumbent provider as relates to SOCaaS
76. How many physical locations?
    a. We have 18 buildings
77. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
    a. We manage our own datacenter
78. Are any security products installed (SIEM, EDR, Vulnerability management, Email security, Network threat analytics)? If yes, please provide product name. Internally or externally managed
    a. Of those relevant to this RFP, we have SIEM and XDR
79. Can you provide the number of endpoints to be monitored? How many Windows/Mac/Linux desktops/servers?
    a. Approximately 50 Windows Servers, less than 10 Linux Servers.
80. Can you provide the number of ingress/egress points to be monitored, average and max Mbps at each, and type of media connectivity?
    a. 4 firewalls (2 HA pairs). Max speed for each HA pair is currently 2Gbps. Average speed varies.
81. Can you provide a network diagram?
    a. Details will be provided to the awarded vendor.
82. Can you provide the number of email boxes to be monitored? Are you currently using Office 365? If so, are you using EOP/ATP?
    a. None are included in this RFP.

83. Can you provide the number of network users to be monitored? How many users are not on the network most of the day, but authenticate with a domain controller (such as remote workers, maintenance staff, etc.)?
    a. Approximately 9,000 users
84. Can you provide the number of Windows servers with a high EPS rate (~50 eps) to be monitored?
    a. We do not have an estimate of the amount of logs our severs generate.
85. Can you provide the number of Windows servers with a low EPS rate (~2 eps) to be monitored?
    a. We do not have an estimate of the amount of logs our severs generate.
86. Can you provide the number of Windows Workstations (5 / 1k users) to be monitored?
    a. Workstations are not in the scope of this RFP
87. Can you provide the number of Windows AD Servers to be monitored?
    a. Less than 5
88. Can you provide the number of Linux Servers to be monitored?
    a. Less than 10
89. Can you provide the number of DNS users (enter # per 1000 users) to be monitored?
    a. Approximately 9,000 users
90. Can you provide the number of routers to be monitored?
    a. Routers are not in the scope of this RFP
91. Can you provide the number of switches (NetFlow not supported) to be monitored?
    a. Switches are not in the scope of this RFP
92. Can you provide the number of Wireless LAN to be monitored?
    a. Wireless LAN are not in the scope of this RFP
93. Can you provide the number of Network Load-Balancers to be monitored?
    a. Network Load-Balancers are not in the scope of this RFP
94. Can you provide the number of WAN Accelerators to be monitored?
    a. WAN Accelerators are not in the scope of this RFP
95. Can you provide the number of other network devices to be monitored?
    a. 4 firewalls (2 HA pairs)
96. Can you provide the number of Firewall – internet users (enter # in 1000s of users) to be monitored?
    a. Approximately 9,000 users
97. Can you provide the number of Network Firewalls (Partner / extranets) to be monitored?
    a. 1
98. Can you provide the number of Network Firewalls (DMZ) to be monitored?
    a. 1
99. Can you provide the number of Network IPS/IDS to be monitored?
    a. IPS/IDS is enabled on our firewall hardware
100. Can you provide the number of Network VPN users (enter # in 100s of users) to be monitored?
    a. Approximately 100 users
101. Can you provide the number of Email AntiSpam users (enter # in 100s of users) to be monitored?
    a. Email is not in the scope of this RFP
102. Can you provide the number of Network Web Proxy users (enter # in 100s of users) to be monitored?

a. None

103. Can you provide the number of other security devices to be monitored?

a. None

104. Can you provide the number of web servers (IIS, Apache, Tomcat) to be monitored?

a. Approximately 10

105. Can you provide the number of databases (MSSQL, Oracle, Sybase – indicate # of instances) to be monitored?

a. Approximately 5

106. Can you provide the number of email server users (enter # in 1000s of users) to be monitored?

a. Email is not in the scope of this RFP

107. Can you provide the number of antivirus server users (enter # in 1000s of users) to be monitored?

a. Antivirus would only be monitored for the servers; server users are less than 20

108. Can you provide the number of other applications (email, DB, AV, etc.) to be monitored?

a. Antivirus/XDR for the servers

109. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

a. No

110. What is the size and complexity of your network environment in terms of number of users, devices, locations, subnets, and applications?

a. Approximately 9,000 users. 18 buildings. Additional details will be provided to the awarded vendor.

111. What operating systems and versions are used across your endpoints?

a. Windows Server (versions still supported by Microsoft). Linux/Ubuntu. Additional details will be given to the awarded vendor

112. What is the current SIEM platform in place? Are you looking to replace the current platform or just support the SIEM with a SOC?

a. Details will be given to the awarded vendor. We are open to all proposals, and vendors can propose multiple options.

113. Do you utilize any cloud services or SaaS applications that would need to be incorporated into monitoring and threat detection?

a. No

114. Have you conducted a risk assessment focused on critical data and systems? When was this last conducted and can we get an executive summary of the results?

a. Yes. Within the past year. Details will be given to the awarded vendor.

115. Do you have any legacy systems or applications that cannot be easily patched or updated?

a. No.

116. What tools do you currently use for endpoint protection, mobile device management, vulnerability scanning, penetration testing, and log analysis?

a. We have XDR, SIEM, and other tools. Details will be given to the awarded vendor.

117. What is your process and team structure for security operations, incident response, and threat investigation?

a. Details will be given to the awarded vendor.

118. Is East Hartford properly conducting inventories of all systems containing sensitive student data?

a. This is not in scope with this RFP

119. Are there any network segmentation strategies in place such as VLANs?
    a. Yes
120. What is your desired outcome from implementing a SOCaaS?
    a. We are looking for SOCaaS to improve our security posture overall
121. What is the expected budget for this initiative?
    a. No expectation
122. What is the expected timeline for rolling out a new SOCaaS?
    a. This is dependent on the e-Rate Pilot Program
123. Is FERPA data in scope and properly identified in the organization?
    a. No
124. What do you mean by SOC Resilience? Do you mean, 24/7 staffing and redundant data locations?
    a. 24/7/365 monitoring from more than one SOC office to have coverage in the event of an outage
125. What types and #counts of devices do you want to cover in SOC/SIEM/EDR?
    a. 4 firewalls (2 HA pairs), Approximately 60 servers
126. What level of forensics/remediation are you expecting to be included within the scope of the RFP?
    a. We are open to all proposals, and each vendor can propose more than one option
127. Will this security project be funding by ERATE?
    a. This project is dependent on funding from the e-Rate Pilot Program
128. How many full-time users are a part of the district?
    a. Approximately 9,000 users
129. Are students on the same network as the full-time users?
    a. Students are considered full-time users in the count above, but they are on separate networks
130. How many Data Centers are there for the district?
    a. 2
131. What is the bandwidth for these locations?
    a. 2Gbps at each egress point
132. Do you want O365 covered for this?
    a. No
133. Are there any cloud instances? If so what cloud and how many servers?
    a. No
134. Will any state contracts be required for this project?
    a. No, there is no requirement, but they can be used
135. Do you have any requirements that won't allow log data to be sent, stored, and processed in a cloud environment?
    a. It would have to meet the Student Data Privacy laws of CT
136. How many network users do you have that need monitoring by the security service? There is an agent to be deployed to PC's and Servers that allows our SOC to monitor and take action (XDR) – this number is per machine – what is this number?
    a. We have approximately 60 servers that will be monitored by this service. Workstations are not in scope of this RFP.
137. Number of network log sources required to be monitored such as firewalls, other network and security tools you already own, etc.
    a. 4 firewalls (2 HA pairs)

138. How many different sites require security monitoring?
    a. 18 buildings
139. Are all sites able to communicate with each other (site-to-site VPN, SD wan, etc.)?
    a. yes
140. What is the maximum internet bandwidth at each site – any sites over 1Gbps?
    a. 2Gbps
141. Will there be remote workers/users that need monitoring?
    a. Yes, through VPN connection
142. Do you have server infrastructure?
    a. Yes, we have approximately 60 servers that require monitoring
143. Where does server infrastructure reside? (On-prem, if in the cloud If in the cloud which IaaS services – Azure, AWS, GCP, etc.?)
    a. On-prem
144. Do you have datacenters with critical server infrastructure that require security monitoring? If yes, how many sites and servers? (Number of sites that have application servers, webservers, critical data)
    a. 18 buildings, approximately 60 servers
145. Do you have the ability to support VMware virtualization?
    a. Not at this time
146. To deploy things such as log collectors, vulnerability scanners, Honeypots/deception technology we will need 20-25 virtual CPU's. Can you support this type of deployment?
    a. Yes
147. How long do you need searchable logs stored (hot storage)?
    a. No preference
148. Do you need cold storage of logs for compliance (cold storage – not immediately searchable)
    a. No preference
149. Are you using SaaS services?
    a. No
150. Which services are you currently using today – O365, Gmail, Oracle Cloud, etc.?
    a. None that are in scope with this RFP
151. Any specific compliances you need to adhere to?
    a. All federal, state, local, and Student Data Privacy laws and regulations
152. What desktop/server operating systems do you currently use in your environment
    a. Windows Server (versions still supported by Microsoft). Linux/Ubuntu. Additional details will be given to the awarded vendor
153. How many facilities require electronic security systems?
    a. 18 buildings
154. Where is each facility located?
    a. East Hartford, CT
155. What electronic security systems (manufacturers/brands) are in place currently?
    a. We have XDR, SIEM, and other tools. Details will be given to the awarded vendor.
156. What is the count and device type that make up each of these systems?
    a. Details will be given to the awarded vendor.
157. Are there drawings/documentation for each site?
    a. Details will be given to the awarded vendor.

158. Is there IT support at each site?

a. Yes, they are centrally located

159. Is there currently a monitoring platform/software in place or using natively on systems?

a. Yes. Details will be given to the awarded vendor.

160. Is a digital/printed signature from the authorized representative acceptable, or do you require a wet signature?

a. Digital is acceptable, but submissions must be hard copies delivered to the address listed on the RFP