RFP Questions and Answers
Security Incident and Event Management (SIEM)
Solution and Professional Services for Implementation
Job # 05-21-IT
February 12, 2021

Questions and Answers

The following are the questions received by the February 5th, 2021 deadline and provided answers.

1. Q: Appendix A references column names that are not corresponding with the column names in the requirements spreadsheet. Is there newer documentation for us to follow?

   A: An updated requirements spreadsheet was posted to the City's website on 2/2/21. When you download the file, the name should be "05-21-IT RFP_SIEM Requirements – Vendors Rev2.xlsx

2. Q: What is the estimated daily ingest rate from the data sources you have identified for this project?

   A: We don't have a 100% way to gauge at this point (e.g. number of event). This will consist of ~450 devices, including Windows Server Security logs as well as routers, switch and firewalls. (154 Windows Servers, 10 LINUX Appliances and the balance being routers, switches, firewalls and Access Points)

   One of the areas we will need assistance with is tuning the devices so they are sending the appropriate level of information to the SIEM solution.

3. Q. What is the city's retainment policy on the data that is being ingested into this solution?

   A. For this type of data, we have 12-month retention policy

4. Q: Does Kirkland have itemized list of devices in scope for this project?

   A: See spreadsheet posted along with this document.

5. Q: The $80,000 budget allocated for the project - Does this include a pre-tax number, infrastructure costs, and implementation & training for Year 1 or software only?

   A: The $80,000 is a one-time cost budgeted for this project. It includes tax, infrastructure costs, training and support and maintenance for one year. Professional services for implementation are budgeted at $25,000 and not part of the $80,000.

6. Q: Sizing - How many end points and how many users?

   A. We believe this question is referring to end user workstations in addition to the number of users (approximately 760). Monitoring end user workstations was not accounted for in the budget for this project. Respondents are welcome to add this as a separate line item.

7. Q: Palo Alto FW

   A: This is a combined IDS/IPS, URL Filter and provides malware protection as well. It provides services for ~900 endpoints, including workstations, servers and network equipment. It also provides 3 site to site IPSEC connections and RAS VPN for two portals/gateways.

8. Q: Breakdown of endpoints used: How many workstations vs how many servers? Windows10 vs Mac? Servers - How many Windows vs Linux?

   A: Workstations standardize on Windows 10. See questions #4 and #6 for additional information.

9. Q: Windows shop - assuming AD - How many Domain Controllers in AD?

   A: Primarily Windows. 6 (3 On premise, 2 in Azure and 1 RO DC On premise)

10. Q: DNS Logs to be ingested? Primary technologies involved with implementation of DNS - Something like InfoBlocks or more sophisticated?

    A: Preferred, yes. Windows DNS for internal and AWS Route 53 for all external.

11. Q: Web Filtering Solution or cover by Palo Alto?

    A: See question #7

12. Q: Mail Proxy - O365 - Upgrade plan that does email scanning and phishing detection? Or using a minecast or proofpoint?

    A: We currently use the built-in tools with O365 for this.

13. Q: Vulnerability Scanners?

    A: Nessus

14. Q: Is 24/7/365 coverage an objective of this project?

    A: 24/7/365 coverage was not called out in the RFP document. If the solution is SaaS/MDR and provides for 3rd party monitoring with alert/response, provide that information in your response. If your solution is on-premise, support options can be discussed/proposed as part the vendor response process.

15. Q: Is the City's preference to dedicate an internal IT resource to manage a product, or use a managed service for coverage?

    A: See page 4 of the RFP document, PURPOSE OF REQUEST section. The City currently plans to have a person responsible for monitoring and maintaining the solution. However, managed services will be considered.

16. Q: How many physical locations are in scope? Do those locations backhaul data to a single point of egress? If not, how many points of egress are in scope?

    A: All city locations come back to a central location for egress. However, we will want to monitor the uplinks to all locations as part of the overall monitoring of the network equipment. There are 15 locations, including the primary

17. Q: Is the solution intended to address security events in O365 or other SaaS/cloud services?

    A: If the proposed solution has these capabilities, please address as a separate line item.

18. Q: Is monitoring “smart city” technology or other IoT in scope?

    A: If your proposed solution provides IoT, BYOD and/or “smart city” technology, please address as a separate line item.

19. Q: Is distributed work force monitoring in scope?

    A: If your proposed solution provides distributed work force monitoring, please address as a separate line item.

20. Q: What is the available bandwidth at each point of egress? (1Gb/s, 10Gb/s, etc.) Out of that available bandwidth, what is the actual throughput used?

    A: Today, this is 1G and we typically run at about 50-60% during a regular business day. Near future, we will be moving to a primary 5G egress with a 1G failover. There is only one egress location though.

21. Q: How many users?

    A: See question #6.

22. Q: How many devices? Please breakdown the number of devices by type.

    A: See question #4.

23. Q: How long do you need to retain logs?

    A: See question #3.