Chicago Teachers' Pension Fund

Questions and Answers #1 Related to the RFP for

MANAGED SIEM AS A SERVICE (MSaaS)

11/21/2018

NOTE: Questions 18, 21, 24, and 26 involve confidential CTPF information and/or confidential technical specifications of CTPF assets. Any prospective respondent to this RFP who sends a signed CTPF Vendor NDA via email to the RFP contact, Rebecca Gonzales, at gonzalesr@ctpf.org will receive this confidential information via response email. The NDA is only for the purpose of CTPF providing our confidential information to prospective respondents and must be the CTPF NDA that is located on CTPF's website here: https://www.ctpf.org/post/non-investment-procurements. **Additional and reciprocal confidentiality provisions may be negotiated as part of any final contract.**

1. Can you verify if the RFP will be to manage your current AlienVault deployment / IT Environment?
   The currently deployed AlienVault solution needs replacing, although we are not opposed to evaluating an AlienVault USM Anywhere proposal.

2. Will CTPF be keeping the current license and renewing as they have in the past?
   The current licensing will not be kept or renewed.

3. I understand the initial purchase went through Sword and Shield; would they be involved in this transaction? Are you using any third-party add-on products that have been integrated with Dynamics SL?
   All vendors are welcome to bid alongside all other vendors. We are open to evaluating third-party add-on products that have been integrated with Dynamics SL.

4. How many employees are in the organization?
   140

5. How many sites or locations is the organization based at? (sites with servers ?)
   1 on-site data center, AWS and Azure tenancies, and 1 DR data center.

6. Are there any data centers in scope? Please describe.
   1 on-site data center.

7. How much of the environment is in the cloud or co-located with any third parties, MSA or MSSP?
   2 EC2 instances and 1 RDS instance in AWS and several directory accounts in Azure.

8. Do you have any regulatory or client contractual security compliance requirements or regulations that must be adhered to? (e.g. PCI, HIPAA, NIST, client contractual requirements)
    - While CTPF is not a HIPAA-covered entity, pursuant to its own administrative rules, CTPF complies with HIPAA standards.
    - Compliance with NIST 800-53 Rev 4 standards is strongly preferred, but not required.
    - Vendors are subject to applicable CTPF Administrative Rules regarding security, including, but not limited to CTPF's Acceptable Use Policy.
    - All of CTPF's contractual agreements contain mutual confidentiality provisions and generally will provide for acknowledgement by a goods or services vendor that CTPF is a public body that is subject to the Illinois Freedom of Information Act, 5 ILCS 140/ ("FOIA") and that, if it is not statutorily-exempt from FOIA, as determined by CTPF, confidential information may be disclosed by CTPF in accordance with FOIA if requested under FOIA.

9. Can you estimate the size in EPS (events per second) of overall syslog / logging data to feed into the proposed SIEM solution? Size / amount of data to ingest per day/week/month/year? (if not that's ok most clients don't know, this is why we ask all of the other questions so this metric can be estimated to size the solution accurately)
   EPS: 80-100 avg.; Total currently stored 100GB of data.

10. How is corporate email handled? On premise or hosted? (please describe, e.g. 200 mailboxes on Microsoft O365)
    Currently on-premises but later hosted.

11. How many servers are in the environment? (physical and virtual) What Operating Systems are in use? (a device inventory will be helpful if one can be provided)
    Approximately 60 prod, 10 dev, and 30 UAT servers, utilizing Windows Server 2008, 2012, 2016, and Cisco versions of RHEL and Ubuntu 16.04.

12. Please list the # of servers, their roles and functions, for example:
    a. AD domain controllers : 2
    b. File / print servers : 2 file servers / 1 print server
    c. Databases (SQL, Oracle, etc): 18 MSSQL servers
    d. Exchange / email: 1 Exchange
    e. Web servers: 22 (Nginx, Apache, IIS)
    f. Applications (please list / describe major applications such as CRM, ERP): SharePoint, Verba, Cisco UCCM/Unity, ApplicationXtender (EMC Documentum), MS Dynamics, FNTI Microfilm Storage, Symantec Enterprise Vault, McAfee ePO, WinINSTALL, Netwrix
    g. Citrix : None at this time
    h. VMware: 6 ESXi hosts.

13. What are the standard corporate applications that you are running?
    MS Office, SharePoint, Cisco UCCM/Unity, ApplicationXtender (EMC Documentum), MS Dynamics, Symantec Enterprise Vault, McAfee ePO.

14. Can you describe the high level attributes of your network?
    a. LAN: Cisco 2960x Stack, Cisco 3850 Stack
    b. WAN: BGP with XO and AT&T
    c. Wireless / WiFi: Cisco AIR-CT2504-K9

15. What internet connectivity is in place? (DSL, cable, t1, MPLS, etc) What speeds and ISPs?
    VOIP, 50Mbps fiber, AT&T and XO circuits with BGP

16. What firewall is in place? What type of security features are enabled on the firewall? How is this firewall monitored?
    Cisco ASA's with FirePOWER, NOC monitoring and alerting, SIEM reporting.

17. Is the network monitored by a NOC, and if so, 24x7?
    Yes, Yes

18. What other security technologies or processes are in place?
    a. Endpoint? What AV is running? : McAfee ePO
    b. URL / content filtering (web browsing): Zscaler
    c. Email filtering: Cisco IronPorts
    d. MDM – mobile device management: This information can be furnished upon CTPF's receipt of our signed NDA.
    e. Multi-factor authentication / 2 factor authentication: This information can be furnished upon CTPF's receipt of our signed NDA.
    f. Encryption (data at rest): This information can be furnished upon CTPF's receipt of our signed NDA.
    g. Encryption (data in motion): This information can be furnished upon CTPF's receipt of our signed NDA.
    h. DLP – data loss prevention: Cisco IronPort
    i. Security awareness training for end users: This information can be furnished upon CTPF's receipt of our signed NDA.
    j. CASB – cloud access security broker: This information can be furnished upon CTPF's receipt of our signed NDA.
    k. IDS/IPS – intrusion prevention: This information can be furnished upon CTPF's receipt of our signed NDA.
    l. Syslog – logging: AlienVault
    m. IR – incident response capability: This information can be furnished upon CTPF's receipt of our signed NDA.

19. Can you please provide a listing of every device, application, servers, cloud application, or other, that will be monitored for SIEMaaS under the desired / proposed solution?
    a. Servers: ~60
    b. Workstations: ~130
    c. Network switches: ~15
    d. Routers: ~4

e. Web servers: ~20
f. Application servers: ~20
g. Database servers: ~18
h. Cloud apps (if supported by vendor): 2
i. Any other syslog sources? No, to be implemented in 2019
j. Any other API sources? No
k. Any other SNMP sources: TBD

20. Does the organization have a vulnerability management program in place, conducting regular vulnerability scans (coupled into patching / remediation?) How many total assets are there to be scanned if we ran a vulnerability scan? (we request a total count, total # of active IP addresses in use to be scanned)
    Usually, ~500

21. Please provide a high-level network architecture diagram.
    This information can be furnished upon CTPF's receipt of our signed NDA.

22. Please provide approximate numbers for:
    i. Desktops / Laptops
        1. Windows
           ~160
        2. Mac OS
           0
        3. Linux / Unix
           5
    ii. Servers (physical and virtual)
        1. Windows Servers
           ~60
        2. Linux Servers
           ~20
        3. Unix Servers
           0
        4. Mainframe / Midrange (zSeries/iSeries)
           0
        5. Other (VM Hosts, appliances, etc.)
           ~10
    iii. Network devices
        1. Routers / Switches / Wireless controllers
           ~15
    iv. What are the active business hours (e.g. – when employees are active)?
           9am-5pm CDT/CST

23. Please list key applications and/or cloud-services in use (e.g., O365).
    i. Are there any internally developed applications specific to CTPF?
       Yes
    ii. AWS/Azure/Google Cloud in use?
       AWS

24. Does CTPF have a formalized Incident Response process that aligns with NIST/FISMA requirements?
    This information can be furnished upon CTPF's receipt of our signed NDA.

25. Does CTPF currently utilize any Security Information and Event Management (SIEM) solutions or otherwise centrally aggregate/correlate log data?
    AlienVault

26. Does CTPF employ any additional endpoint security controls beyond antivirus?
    This information can be furnished upon CTPF's receipt of our signed NDA.
    i. Which antivirus solution(s) are in use?
       McAfee

27. Would CTPF require support for deployment (e.g., assistance with firewall configuration changes)?
    Yes

28. How many servers?
    60

29. How many desktops?
    130

30. How many databases?
    18

31. How many email servers?
    2

32. How many HQ firewalls?
    2

33. How many network devices?
    ~500

34. Do you have AS400?
    No

35. Is AD in scope? If so, how many Domain Controllers?
    Yes, 2

36. If we have two different technology solutions with differing price points and capabilities, would CTPF allow us to submit two proposals (one for each)?
    Yes, submitting multiple proposals is allowed.

37. In order to properly scope/price either solution we will need the attached scoping documents completed. A SIEM solution is just too complex to properly scope without having detailed architecture information.
    Answers provided in separate attachment.

38. How many devices:
    a. Windows
       ~180
    b. Linux
       ~25

c. Network Devices
   ~500
d. Firewalls
   2
e. Other:
   N/A

39. Of the servers/workstations, how many need file integrity monitoring?
    All

40. Is there a SIEM solution in place today or any type of centrally managed event logging technology in use at CTFP?
    Yes

41. What types of devices and how many would be in scope? What are the feed counts?
    100-200

42. How many separate locations?
    The organization has 1 location.

43. Is CTPF looking for a fully managed SIEM or co-managed SIEM?
    Co-managed

44. Does CTPF require help developing runbook / remediation plan?
    Yes

45. Are you looking to monitor network traffic from mobile devices, or would you like control and response capabilities on the devices themselves?
    Yes, monitor network traffic from mobile devices. Open to evaluating control and response capabilities on the devices themselves.

46. Can you provide an example of what might fit into this category: Non-log infrastructure information
    Device data transmitted in real-time that may also be recorded to a log file.