WAYNE STATE
UNIVERSITY

Division of Finance and Business Operations

Procurement & Strategic Sourcing
5700 Cass Avenue, suite 4200
Detroit, Michigan 48202
(313) 577-3734
FAX (313) 577-3747

August 15, 2022

Addendum #2 To
Request for Proposal
RFP Security Incident and Event Management 2022
dated August 18, 2022

Clarifications

This Addendum must be acknowledged on Schedule D.

Note: You must have attended the **mandatory** pre-bid meeting to be eligible to participate in this bid opportunity.

Please find the following questions and clarifications with regards to the above bid opportunity.

Answer: Question 1: Regarding the 600 servers, are any VM's, and if so, how many Hypervisors do you have?

Answer: Mostly virtual, I do not have a count for number of total hypervisors but we have at least three that I am aware of

Question 2: Of your 600 servers, please make rough approximation of quantities for how many are Windows operating systems vs Linux/Unix?

Answer: 80/20 Linux

Question 3: Can windows workstation & server logs be forwarded to one of your servers configured with the event collector role to then forward to our SIEM? If not, will it be acceptable to install an agent on every workstation and server?

Answer: Yes, either approach works. If we need a separate sever for forwarding please includes specs so we can calculate internal cost.

Question 4: How many Network Devices will send logs to the SIEM? (Access Points, Switches, Routers, etc (excluding firewalls))?

Answer: There are aprox 35 firewall across campus, we only collect auth and audit from network devices through TACACS

Question 5: Do you want to send NetFlow data to the SIEM? If so, please confirm what devices and expected traffic volume?

Answer: No

Question 6: How many Firewalls will send logs to the SIEM? Are any of those firewalls considered "Data Center Firewalls" and if so, how many?

Answer: Aprox 35, and there are three HA pairs that we would consider datacener

Question 7: Do you have any AV/NGAV to integrate? If so, please confirm the vendor and number of agents/seats.

Answer: Not at this time but will in the future, aprox 10K agents

Question 8: Do you have an EDR to integrate? If so, please confirm the vendor and number of agents/seats?

Answer: Not at this time, we are not releasing any vendor specific information as part of this RFP. We can discuss those specifics after a selection is made.

Question 9: Do you have any SaaS platforms? (ex: O365, Azure, Cisco Umbrella, Salesforce, Google Workspace, Zendesk, DocuSign, web conferencing system, etc.) If so, please confirm each vendor and number of seats each platform?

Answer: Yes, we are not disclosing vendors we have aprox 250,000 active mailboxes of those we have aprox 6500 employees

Question 10: Do you have any 2FA platforms that you would like to integrate? If so, please confirm each vendor and number of seats in their platform.

Answer: Yes, we are not disclosing specific vendor information for this RFP

Question 11: TRAINING
-- Size of Team
-- leadership of team (CISO)
-- How is an incident currently handled?
-- How will the solution assist / solve gaps / identify attack surface and vulnerabilities?
-- PS Training dollars
-- Fast track activation: VA sets up initial while WSU trains in parallel

Answer: These questions do not seem relevant to the product we are purchasing. We are asking for end user training on how to operate the solution at a per seat cost.

Question 12: How many log sources do they have?

Answer: Sizing for the RFP should be based on an average EPS of 15,000 or 6500 users

Question 13: How many Firewalls?

Answer: Aprox 35

Question 14: What vendors?

Answer: We are not providing specific vendor information as part of this RFP

Question 15: Any Intrusion Detection System (IDS)/ Intrusion Detection Prevention (IPS)?

Answer: Yes

Question 16: Any Web Application Firewalls (WAF)?

Answer: No

Question 17: How many Servers:

Answer: Sizing for the RFP should be based on an average EPS of 15,000 or 6,500 users

Question 18: Windows:
Domain Controllers?
Other, please state, e.g. DNS, DHCP, IIS?
Linux?
Other, please state, e.g. DNS, DHCP, SQL?

Answers: Sizing for the RFP should be based on an average EPS of 15,000 or 6500 users

Question 19: How many Flow Sources like routers/switches?

Answer: None

Question 20: What is your network throughput:
Capability? 40 G
Actual usage? Less than 10G

Answers:

Question 21: Any Wireless Access Points (WAP)?

Answer: yes

Question 22: What Endpoint Detection & Response (EDR) solution is in place?
How many endpoints are protected?

Answer: We are not releasing vendor specific information for the RFP. We have aprox 10K protected endpoints.

Question 23: What Email security solution is in place?

Answer: We are not releasing vendor specific information for the RFP

Question 24: Any File Integrity Monitoring (FIM)/Cloud Access Security Broker (CASB)?

Answer: No

Question 25: Cloud environments?

Answer: Yes

Question 26: What Multi Factor Authentication (MFA) is in place?

Answer: Multiple

Question 27: What Vulnerability Management solution is in place?

Answer We are not releasing vendor specific information for this RFP

Question 28: What virtual environments do you have in place?

Answer: We have several, We are not releasing vendor specific information for this RFP

Question 29: What SaaS solutions do you have, e.g. Salesforce, Box?

Answer: We are not releasing vendor specific information for this RFP

Question 30: Are they subscribed to any Threat Intelligence services, and if so which ones?

Answer Yes, We are not releasing vendor specific information for this RFP

Is there any automation required like automated Firewall Security Policy blocking?

Question 31: Many sites are there?

Answer: No

Question 32: One main, and how many hub/satellite sites?

Answer: One Campus

Question 33: What size connections do the sites have to each other?
Will an All in One (AiO) solution or Distributed Deployment (DD) be required?

Answer: One solution

Question 34: Log retention expectations? 1 Year, at least 30 days “hot”

Answer:

Question 35: Are they subject to any compliance standards?

Answer: The product does not need to be compliant with any specific regulations

Question 36: What are their main security concerns within their environment?

Answer: This is not relevant to the RFP

Question 37: Are there any specific use cases they have in mind?

Answer: Yes, we will discuss this after choosing a vendor. We expect the vendor will provide use cases they support not the other way around.

Question 38: Between the 7 members of your WSU SOC, can you provide each person's responsibilities & titles within your security org?

Answer: This is not relevant to this RFP

Question 39: During an incident, can you advise what your security personnel's responsibilities are?

Answer: This is not relevant to this RFP

Question 40: Are you personnel evenly divided between Tier 1, Tier 2, & Tier 3 support?

Answer: This is not relevant to this RFP

Question 41: Can you provide what the requirements are of your cybersecurity insurance policy?

Answer: NA

Question 42: What are WSU log retention requirements, 12 Month? 13? 24? 36?

Answer: 1 Year, at least 30 days “hot”

Question 43: Number of End-users in your organization (AD credentialed): 6,500 FTEs and 26,000 students (from RFP, please confirm)?

Answer: reference https://irda.wayne.edu/dashboards

Question 44: Please provide total end-user count?

Answer: reference https://irda.wayne.edu/dashboards

Question 45: Number of Servers (cloud or on-prem): 600 (from RFP, please confirm)?

Answer 600 servers

Question 46: Server OS types?

Answer: Windows and Linux

Question 47: Number of Network Firewalls?

Answer: aprox 35

Question 48: Brand of firewalls?

Answer: We are not releasing vendor specific information for this RFP

Question 49: Do the firewalls have IPS/IDS active or other security modules active?

Answer: Yes

Question 50: Number of Network Devices (Switches)?

Answer:Not in scope

Question 51: Number of Internet Connections and Sizes?

Answer: 1 40 Gig

Question 52: Number of Physical Locations – plant or offices?

Answer: 1 Campus

Question 53: Any cloud hosting - Azure/GCP/AWS?

Answer: Yes

Question 54: Using O365 or Google for email?

Answer: We are not releasing vendor specific information for this RFP

Question 55: Please describe student vs staff segmentation or indicate if all are under a single domain/tenant?

Answer: Single domain

Question 56: What is the Email protection solution?

Answer: We are not releasing vendor specific information for this RFP

Question 57: Do you have an estimate of the daily log volume produced in your organization?

Answer: For sizing an average of 15,000 EPS should be used

Question 58: What are your log retention requirements?

Answer: 1 Year, at least 30 days “hot”

Question 59: What compliance regulations or contracts exist that may obligate you to particular security controls? FERPA?

Answer: The solution does not have any specific compliance requirements

Question 60: Is there an IT and/or security ticketing system (e.g. ServiceNow) that should be integrated for incident ticketing?

Answer:No

Question 61: While WSU is fundamentally looking to replace their current SIEM, a mention of a data-lake being necessary to achieve the desired outcome was well received – may we respond with this portion of functionality only? (we’d augment the SIEM)

Answer: This RFP is for a SIEM not a data lake

Question 62: What is WSU’s expected data volume growth over the next few years (on average we see roughly 20%)?

Answer: We do not expect any significant growth as it applies to SIEM.

Question 63: Where does search speed rank in decision criteria?

Answer: The criteria for selection has been provided through the RFP

Question 64: Where does scalability rank in decision criteria?

Answer: The criteria for selection has been provided through the RFP

Question 65: Does WSU want to build their own content or are they expecting pre-configured content out of the box? Who will be responsible for tuning and refinement of said solution?

Answer: We expect the solution with have some amount of built in rules but need the capability for customization

Question 66: How is Wayne state leveraging falcon data? Is this data going in to your SIEM?

Answer: We are not releasing any vendor specific information for this RFP at this time we do not send our EDR information to our SIEM but may see value for this in the future

Question 67: What is WSU’s desired compression of data? Where does this factor in decision criteria?

Answer: The criteria for selection has been provided through the RFP

Question 68: How many technical vs non-technical users will be leveraging the platform?

Answer: Unknown at the time but less than 10

Question 69: What form of data pipeline tools or collection methods are being leveraged today?

Answer: Syslog, ODBC and some proprietary agents

Question 70: How much data will you be ingesting per day (GB/day)? Please fill out the attached sizing sheet to find an estimated ingestion amount per day and please send it to us if possible.

Answer: For sizing an average of 15,000 EPS should be used, any details needed for install will be provided once a vendor is chosen.

Question 71: What are your retention requirements?

Answer: 1 year with at least 30 days of "hot" storage

Question 72: Do you have any compliance requirements such as HIPPA/PCI?

Answer: The solution does not need to meet any specific compliance requirements

Question 73: What features are you seeking in a SIEM solution?

Answer: This has already been described in the RFP

Question 74: In the PDF, it states proposal needs to be valid for 120 days. In schedule E (excel document) it states 60 days. Please let us know whether the proposal needs to be valid for 60 or 120 days?

Answer: Vendors Proposal shall remain valid for 120 days.

Question 75: Are WSU alumni mailboxes retained indefinitely? If not, what is the amount of time an alumni mailbox is active?

Answer: Yes, for the lifetime of the Alumni.

Question 76: Will the University accept a proposal submission under the terms and conditions of consortium agreements such as MHEC?

Answer: The University's intent is to use its Standard Service Provider Agreement, sample was included in the back of the RFP Documents, watermarked "sample". The University is not seeking to enter into a contractual relationship with a consortium or cooperative via this bid opportunity.

Question 77: If your team would be willing to sign our mutual NDA so that we can share our Insurance details as requested in the RFP?

Answer: Answer: The University is subject to the Michigan Freedom of Information Act. Thus, any and all materials received in a vendor's proposal is subject to any FOIA requests, and an NDA would not exempt or curtail that. However, vendor who choose to do so can simply complete Schedule B indicating they are able to provide the coverages in Schedule B, once they've confirmed either with their person who oversees the company insurance or their insurance carrier. A copy of a certificate of insurance isn't required with submission of proposal, but would be required in the execution of a contract.

All questions concerning this project must be emailed to: Robert Kuhn, Procurement & Strategic Sourcing at 313-577-3712 Email: RFPTeam3@wayne.edu. The questions cut off was by 12:00 p.m., September 7, 2022.

Do not contact the Computing and Information Technology Department, or other University Units, directly as this may result in disqualification of your proposal.

Thank you

Robert Kuhn,
Senior Buyer, Purchasing
313-577-3712

CC: Garrett McManaway, Jill Zeller, Andrew Dold, Valerie Kreher Attendees list.

Attachments: