PORT OF OAKLAND

Purchasing Department
530 Water Street
Oakland, CA 94607

November 3, 2021

ADDENDUM No. 1

RFP No.: 21-22/15 – Managed IT Security Monitoring Detection and Response Services

This Addendum modifies the original RFP Documents for the above-mentioned RFP. **Acknowledge receipt of this addendum in the space provided on the RFP Acknowledgement and Signature Form (Attachment 3). Failure to do so may disqualify your proposal.**

The following question were submitted by the deadline and are answered in this addendum.

1. **Question:** Is the Port subject to any regulations (e.g., CCPA, HIPAA, SOC 2, CJIS Background checks) that will flow-down to the service provider?

   Answer*: PCI for the SIEM, other regulations are around reporting on incidents.*

2. **Question:** Is a US based remote solution sufficient or does staff need to work onsite?

   Answer*: It is intended that staff would be located in the US at their place of business, not onsite at the Port.*

3. **Question:** Does the Port have any long-term log retention requirements after the 7 year period?

   Answer*: No.*

4. **Question:** Does the Port have a current security team and if so how many people are on it?

   Answer*: Yes, Both physical and cyber. Staff number will not be disclosed.*

5. **Question:** As the Port works with several locations (Oakland seaport, Oakland International Airport, Commercial Real Estate, SF International Airport, etc.) does the Port require multiple escalation channels or will it all be directed to one location / team? If not how, please specify how many escalation channels will be required.

   Answer*: One location, and anticipating two escalation channels, also note SF International is not part of the Port of Oakland.*

6. **Question:** Does the Port have a current SOC team and / or is it outsourced?

   Answer*: Yes, current onsite employees monitor and respond to incidents.*

7. **Question:** Is the Port in compliance with current security regulations or is an uplift needed to bring it into compliance?

   Answer*: Yes, the is in compliance with current security regulations.*

8. **Question:** Project Overview: This section references an IT Security Monitoring, Detection and Response System (MDR).

   a) Is this referring to just services or the inclusion of an End Point Detection & Response tool along with 24x7 associated services?

   Answer*: Both*

   b) Does the Port of Oakland have and EDR / MDR tool installed and if so what it is?

   Answer*: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

   c) Is the EDR / MDR tool fully deployed on the 5000 Endpoints in scope?

   Answer*: Yes*

   d) Is the EDR / MDR tool owned by the Port of Oakland or does it need to be replaced within the contract?

   Answer*: Being replaced. Some EDR solutions such as anti- virus will remain.*

   e) Can the EDR / MDR tool be installed in the EDR / MDR vendors cloud? Should it be licensed in the Port's name so the Port owns all the logs?

   Answer*: Yes and yes all data will need to be registered in the Port's name.*

   f) What are the log retention requirements?

   Answer*: 5 years*

9. **Question:** Project Overview: This section references that the Port is looking for a new Security Event Incident Management (SEIM) solution.

   a) Does the Port of Oakland have a current SIEM installed and if so, what it is?

Answer*: Yes, This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

b) Is the SIEM fully monitoring the 5000 Endpoints in scope?

Answer*: No*

c) Is the SIEM owned by the Port of Oakland or does it need to be replaced within the contract?

Answer*: The Port would like to move to an enterprise SIEM solution, so the intent is a new solution on all in scope endpoints.*

d) Can the SIEM tool be installed in the SIEM vendors cloud or it required to be on-prem in the Port's datacenter? Should it be licensed in the Port's name so the Port owns all the logs?

Answer*: Yes and yes all data will need to be registered in the Port's name.*

e) What are the log retention requirements?

Answer*: Please see the response to question number 8f.*

f) Please provide a list of security tools and other systems that will need to be ingested into the SIEM so it can be correlated to standard and custom collectors and the appropriate SIEM can be chosen.

Answer*: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

10. **Question:** Scope of Services: Bullet D states "Unlimited data and events per second"

a) Unlimited is a very broad term; Can this be further defined to include a large cap for costing purposes like 100GB, 250GB, 1TB / day?

Answer*: The Port would like to have unlimited for future growth without having to change ongoing costs or contract language. If unlimited is not offered, the Port will accept costs for the different bandwidth caps.*

b) What data is being considered for ingestion into the SIEM (beyond items listed in Bullet E) that is creating the requirements for Unlimited data?

***Answer**: The Port would like to have unlimited for future growth without having to change ongoing costs or contract language. If unlimited is not offered, the Port will accept costs for the different bandwidth caps. Detail of ingested data will not be offered at this time.*

c) Some SIEM vendors charge by daily ingestion such as Splunk; Is Splunk an allowed SIEM even though it has a licensable ingestion cap?

***Answer**: The Port would like to have unlimited for future growth without having to change ongoing costs or contract language. If unlimited is not offered, the Port will accept costs for the different storage caps. Splunk would be acceptable, but details of ongoing costs will be needed.*

11. **Question:** Scope of Services: Bullet E - 4 states a requirement: That the SIEM Ability to integrate with Endpoint Protection

a) Is it acceptable to monitor the SIEM separately from the EDR / MDR tool as response times are faster when directly working with an EDR tool and storage fees are much lower if logs are not required to be duplicated?

***Answer**: Yes*

b) Is the desire to put EDR on endpoints and use the SIEM to collect logs from items that can't run EDR?

***Answer**: More to meet current PCI requirements.*

12. **Question:** Scope of Services: Bullet G - 4 states a requirement: Strategic security advice and answers to Port IT team security questions within 30 minutes

a) Is the Port anticipated a requirement to keep a full engineering compliment online 24x7 or just the monitoring staff to support this requirement?

***Answer**: In the event that an issue is detected and needs to escalate beyond monitoring staff, it is expected higher level staff to be available 24x7 to isolate and\or remediate the issue.*

b) Is the 30 min response time to have a discussion or does a resolution need to be identified within 30 minutes?

***Answer**: Discussion within 30 minutes to discuss remediation plan.*

13. **Question:** Scope of Services: Bullet G - 5 states a requirement: Provide Unlimited Reporting within 30 minutes

a) Is the Port anticipated a requirement to keep a full engineering compliment online 24x7 or just the monitoring staff to support this requirement?

Answer*: In the event that an issue is detected and needs to escalate beyond monitoring staff, it is expected higher level staff to be available 24x7 to isolate and\or remediate the issue.*

b) Is the 30 min response time to have a report created, generated and provided?

Answer*: Initial contact on incident within 30 minutes, not report.*

c) How many custom reports per day should be anticipated?

Answer*: It is not anticipated to regularly require custom reports. Most reporting can be created during the implementation of the system.*

14. **Question:** Scope of Services: Bullet I - 2 states a requirement: 24/7 hunting for internal vulnerabilities, system misconfigurations, and account takeover exposure on the dark web

    a) "internal vulnerabilities" Is it anticipated that a tool would be configured to operating 24x7 instead of having the scans scheduled on a weekly or monthly basis?

    Answer*: Yes*

    b) "system misconfigurations" Is it anticipated that a tool would be required to be installed to operating 24x7 instead or is it acceptable to have this deduced via the SIEM?

    Answer*: Vendors should propose their best process\solution from their experience working with companies like the Port.*

    c) "account takeover exposure on the dark web" Does the Port require access to this tool or an API ingestion into the SIEM sufficient?

    Answer*: API is fine.*

15. **Question:** Scope of Services: Bullet J states a requirement: Dark Web Data Source Vulnerability Assessments

    a) This request could mean different things to different security companies. Can you please elaborate on the request?

    Answer*: Using your sources to look for accounts or infrastructure information about the Port on the Dark Web.*

16. **Question:** Scope of Services: Bullet M states a requirement: Enable a Dynamic Perimeter and Zero-Trust model.

    a) Is this referring to inclusion of an End Point Detection & Response tool or is a specific Zero-Trust program (collection of about many tools) being requested?

***Answer**: The new solution should support these models and best practice. The port does not want to implement a solution that does not follow that model or any future solutions for dynamic perimeter.*

b) Does the Port of Oakland have an Zero-Trust set of tool installed and if so what are they?

***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

c) Is the Zero-Trust fully deployed on the 5000 Endpoints in scope?

***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

d) Are the Zero-Trust tools owned by the Port of Oakland or does it need to be replaced within the contract?

***Answer**: It is not intended to be replaced with this contract.*

17. **Question:** Scope of Services: Bullet P - 3 states a requirement: Reporting capabilities including Audit and Compliance.

a) Is this just referring to reports that may be needed from the SIEM or EDR tool or is something more detailed being requested like a SOC 2 report on the service provider?

***Answer**: Basic reporting such as detections, response time, type of event, etc. While not required, a SOC 2 report would be seen as a plus.*

New current SIEM Solution (page 9 of 60) states “The proposed SEIM must also be able to integrate with the MDR solution.”

a) Is the Port requiring an integrated solution from a single product vendor or is the ability to ingest logs from the EDR to the SIEM sufficient?

***Answer**: Ingesting logs from EDR to SIEM is acceptable.*

18. **Question:** Port Policy and Other Requirements states: “Respondent acknowledges that in the course of performing services under the Agreement, the selected Consultant/Contractor will come into possession of sensitive information subject to Port of Oakland regulation. The selected Consultant/Contractor will be required to comply strictly with the Port of Oakland’s policies and practices for sensitive information.”

a) Will the port require any formal certifications from the service provider?

Answer: *No*

19. **Question:** we would like to know if the Port can provide a device list.

    Answer*: Please see the response to question number 58.*

20. **Question:** Will SCADA Systems be considered for the scope?

    Answer*: Yes*

21. **Question:** What operational technologies / assets will be covered in this scope?

    Answer*: All Port systems.*

22. **Question:** Is there any existing security monitoring, detection, response software/tech installed? If yes, can you please share what software/technology is being used?

    Answer*: Yes, This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

23. **Question:** Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - are they eligible to bid on this project and can you please provide incumbent contract number, dollar value and period of performance?

    Answer*: No*

24. **Question:** Specify the VLAN details how many is included in the Scope?

    Answer*: For cost estimating use 250 VLANS.*

25. **Question:** Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc.

    Answer*: Please see the response to question number 58.*

26. **Question:** Approximately how many computer endpoints do you have (desktop PCs, laptops, servers)?

    Answer*: Please see the response to question number 58.*

27. **Question:** Can you tell the total number of endpoints you want protected?

Answer*:5000*

28. **Question:** What’s your headcount of users (employees + contractors+interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely?

    Answer*: 650 user accounts. 40 remote users.*

29. **Question:** How much (%) of the infrastructure is in cloud?

    Answer*: 4%*

30. **Question:** What is the size of the IT environment?

    Answer*: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

31. **Question:** How many physical locations?

    Answer*: 4*

32. **Question:** What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)?

    Answer*: <1 gbps*

33. **Question:** Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

    Answer*: Managed by Port IT.*

34. **Question:** What is the approximate budget?

    Answer*: No budget amount has been set.*

35. **Question:** Are any vendor products installed for Security Incident & Event Management (SIEM)? If yes, please provide currently used SIEM product name.

    Answer*: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

36. **Question:** Is there EDR, Anti-virus, Anti-malware in place today?

    Answer*: Yes*

37. **Question:** Is there a current log collection (SEIM) service? If so, is it internally or externally managed?

    ***Answer**: Yes, Internally.*

38. **Question:** What security tools are already in place? I.E., firewalls, endpoint protection, vulnerability management, email, identity access management, networking (routers, switches, access points), user behavior analytics, network threat analytics, security orchestration automation, response (SOAR), etc.

    ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

39. **Question:** How is the network architected? I.E. How many sites will be in scope, all coming back or decentralized (stand-alone sites, mesh network, hub and spoke, SD WAN)?

    ***Answer**: Hub and spoke.*

40. **Question:** What percentage of your servers are virtual versus physical?

    ***Answer**: 98% Virtual.*

41. **Question:** How many Internet connections exist, and what is the speed of each connection? (This is to help us understand the monitoring of all incoming and outgoing Internet activity. For example, an organization may have 2 main offices, each office connecting with 1Gbps links.)

    ***Answer**: Two 300MB, one 50MB.*

42. **Question:** Physical network information.
    a) Please identify each physical location with direct ingress or egress to the internet
        i. Are any of these locations tunneling data through another data center? If so, please list

    ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

        ii. For each location, please provide interface type & speed (copper or fiber, 200Mbps, 1G, 10G, etc)

    ***Answer**: Fiber, Two 300MB, one 50MB.*

        iii. For each location, please provide sustained and peak traffic rates (i.e. 500 Mbps). This can often be obtained through a firewall or edge switch.

***Answer**: Please provide the bandwidth requirement for your solution in your proposal.*

b) Do your switches support port mirroring (SPAN)?

***Answer**: Yes*

c) Switch manufacturer and model

***Answer**: Cisco, multiple models.*

d) Switch utilization (will it drop packets?)

***Answer**: No*

e) Network Flow records [NetFlow, Jflow, Sflow, IPFIX (East-West)].

***Answer**: Unclear to what the question is. If it is in regard to what do we have the ability to support. Please list any protocols required for your solution.*

43. **Question:** Current and projected number of users.

a) How many network users (at a workstation most of the day)?

***Answer**: Expect up to 650.*

b) 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)?

***Answer**: 50*

c) Do you have any outward facing web applications for which authentication monitoring is in scope? If so, how many users?

***Answer**: Yes, 50.*

44. **Question:** Do you have Office 365?

***Answer**: Yes*

45. **Question:** 3 Required References: For privacy and compliance reasons we do not publicly share references. However, we can provide current case studies and can schedule reference calls with multiple customers directly between Port of Oakland and the Proposer's customer. Would this be acceptable? Or how would you like us to approach this?

***Answer**: No, we would want references listed so that we can contact them directly. Please use your best judgment in providing this information as we are a public entity and proposals are subject to the Public Record Act. If you are making any exceptions to this* *requirement, please make sure to note this in your proposal response under the Submission Requirements Section--Company Information. Exceptions are discouraged and may result in lower evaluation points during the Port's evaluation of your proposal.*

46. **Question:** Contract Terms: Are you looking for a 7-year contract paid up front or annually?

    ***Answer**: Paid Annually.*

47. **Question:** US Based Security team: We can assign Port of Oakland a US based security team but we do have some security analysts that are based in Canada. Will this be an issue?

    ***Answer**: While a US based team is preferred, the Port will consider teams in Canada.*

48. **Question:** How many Servers do you have on prem/virtual?

    ***Answer**: 200*

49. **Question:** How many servers/instances do you have in Azure?

    ***Answer**: 10*

50. **Question:** Would you like O365 monitoring included in the scope of this project? If so, how many O365 users do you have?

    ***Answer**: Yes. 650 users.*

51. **Question:** How many points of Egress does port of Oakland have? Would you be willing to share a network diagram? Happy to sign an NDA if needed.

    ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

52. **Question:** What is the total number of Windows, Linux, MacOS machines in the environment? (Laptops, Desktops, Servers (physical or virtual), VDI sessions, etc..?

    ***Answer**: Please see the response to question number 58.*

53. **Question:** How many total data centers? Primary/Backup or Active/Active, etc…

    ***Answer**: 4 Primary All Active.*

54. **Question:** What is the speed of the Internet connection at each data center? (100MBps, 500MBps, 1GBps, etc…)

    ***Answer**: Please see the response to question number 41.*

55. **Question:** Total number of Oakland employees with actual email addresses?

Answer: Please see the response to question number 50.

56. **Question:** What is the backend core switching speed? (1GBps, 10GBps, 40GBps, etc..)

Answer: 10GBps

57. **Question:** In terms of routing out to the Internet, do all offices/locations go to the Internet through the data centers internet connections?

Answer: Yes

a) Goal here is to inspect all outgoing/incoming traffic, so does all traffic to the Internet go through a choke point like a data center Internet Connection?

Answer: Yes

b) Or does each location/office access the Internet directly, without going through a data center? If so… how many offices access the Internet directly?

Answer: No

58. **Question:** In order to better assess your context, we would like to obtain the following information:

Answer:

Device-Based	**Units**
Workstations	600
Servers Windows (low volume)	140
Servers Windows	32
Servers Linux/Unix	8
Hypervisor	30
Network Devices	5000
NetFlow	NA
Firewall Datacenter	10
Firewall Remote office/site	0
Security Platforms (e.g. Web Proxy)	NA
User-based	**Users**

Security Endpoint (e.g. AV)	650
SaaS Platforms (e.g. O365)	700

59. **Question:** Please provide the estimated quantity of logs per day (in GB) and the retention period.

    Answer*: Use your experience providing EDR\MDR\SIEM solutions and the device breakdown in response to question 58 to estimate the total size. Five years retention.*

60. **Question:** How many users in scope?

    Answer*: Please see the response to question number 28.*

61. **Question:** Do you expect services to be provided from within the U.S., or can we proposed the use of offshore resources?

    Answer*: Please see the response to question number 2.*

62. **Question:** Do you have your own SOC?

    Answer*: Yes*

63. **Question:** What is your current SIEM solution?

    Answer*: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

64. **Question:** In section II – Scope of Services, Item D, you request unlimited data and events per second, What is your average MPS and data consumption per month?

    Answer*: Please see the response to question number 10b.*

65. **Question:** In section II – Scope of Services, Item F, you request Access to the MDR solution for Port IT Staff. Is read only access acceptable?

    Answer*: Yes, read only for both MDR and SIEM.*

66. **Question:** In section II – Scope of Services, Item I, you request "Continuous Vulnerability Assessments".

    a. Will you accept an agent based solution?

       Answer*: Yes*

67. **Question:** In section II – Scope of Services, Item J, please elaborate on what you are looking for on Dark Web Data Source Vulnerability Assessments.

***Answer**: Please see the response to question number 15.*

68. **Question:** Do you have a vulnerability management solution, or should one be quoted?

    ***Answer**: Please propose any tools you suggest be used to meet this scope for monitoring.*

69. **Question:** Do you expect services to be provided from within the U.S., or can we proposed the use of offshore resources?

    ***Answer**: Please see the response to question number 2.*

70. **Question:** Is the Port of Oakland looking for a fully managed SIEM offering (i.e. the SIEM is owned and administered by the provider) or is the Port looking for a co-managed SIEM offering (i.e. the license is sold by the provider and the SIEM is built and maintained by the provider but the Port owns the license and environment at the end of the contract)?

    ***Answer**: Co-managed was the intent.*

71. **Question:** Can the Port estimate what their current rate of ingest is into their current SIEM on a GB/Day or EPS scale? Or can the Port estimate what their GB/Day will be once a new SIEM is onboarded?

    ***Answer**: Please see the response for question number 10c.*

72. **Question:** How are you using Azure? For Active Directory?

    ***Answer**: Yes*

73. **Question:** Are there any additional server instances within Azure? How many?

    ***Answer**: No*

74. **Question:** Are you using Office365 for email?

    ***Answer**: Yes*

75. **Question:** Are any vendor products installed for Governance, Risk, and Compliance (GRC) tracking?

    ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

76. **Question:** Are any vendor products installed for Security Incident & Event Management (SIEM)? If yes, please provide the currently used SIEM product name.

***Answer**: yes,*

77. **Question:** What is the anticipated or expected date of contract completion.

    ***Answer**: Implementation Dec 2022, Contract seven years after that.*

78. **Question:** Do you have specific requirements or restrictions for the team composition (e.g. US citizenship, etc.)

    ***Answer**: Please see the response to question number 2.*

79. **Question:** How many and what types of operating systems are in scope?

    ***Answer**: 3*

80. **Question:** What types and versions of databases are in scope?

    ***Answer**: MS SQL, latest versions.*

81. **Question:** Will site visits be required? If so, how many sites location will be involved?

    ***Answer**: Yes, 4 locations.*

82. **Question:** Will the vendor be required to provide training for software installed? If yes, what are the total number of employees (workforce, management, executive) that the vendor needs to provide training?

    ***Answer**: Yes, 30 employees.*

83. **Question:** Are there any specific certification requirements for personnel who will be placed on the project?

    ***Answer**: No*

84. **Question:** Can you estimate what percentage of work can be done onsite and what percent can be done remotely?

    ***Answer**: No*

85. **Question:** Can reference for subcontractors be included?

    ***Answer**: Yes, so long as they represent and demonstrate your company's ability to provide the requested service listed in the RFP.*

86. **Question:** How many workstations?

    ***Answer**: Please see the response to question number 58.*

87. **Question:** Does “the Port” have the desired start and end date for all services covered within the RFP?

    Answer*: Start around July 2022, Contract 7 years after acceptance of implementation.*

88. **Question:** Will the assessment include a sampling of both on-premise, cloud and remote endpoints?

    Answer*: Yes*

89. **Question:** Do you want to allocate full-time Support personal for this project?

    Answer*: Propose based on your experience providing EDR/MDR and SOCaas solutions and services.*

90. **Question:** Are vendors allowed to include travel cost?

    Answer*: Yes*

91. **Question:** What is the system configuration time?

    Answer*: Propose based on your experience providing EDR/MDR and SOCaas solutions and services.*

92. **Question:** What is the Data Retention period?

    Answer*: Please see the response to question number 8f.*

93. **Question:** What type of help desk does “the port” need is it a security help desk that will Monitor Detect and Respond (MDR) or I.T Help desk responsible for responding to daily IT issues?

    Answer*: For this RFP, MDR only.*

94. **Question:** Specific compliance framework outside of PCI that was mentioned on the conference? NERC CIP for SCADA system, other?

    Answer*: TSA-PNA-14-01A.*

95. **Question:** Why do you have 2 EDR mechanisms/agents? Why is 1 of the agents being replaced - conflict with other solutions, too many false positives, lack of threat detection and response capabilities?

    Answer*: Since EDR can be used to describe many solutions such as anti-virus, the port has multiple solutions that could be considered EDR.*

96. **Question:** Is a new EDR solution a hard requirement for this RFP or is it purely MDR with optional / recommended technologies?

***Answer**: Vendors should propose what they think is the best solution and method for collecting endpoint data.*

97. **Question:** Per the Unlimited logging, no restrictions on data storage comment from the conference, could you give us an estimate on the total throughput? We need this to accurately quote GB/TB per day/week?

    ***Answer**: The Port is unable to estimate this amount since we would be logging more data then currently. Vendor should estimiate based on device list in response to question 58. Also review response to question 10 regarding a cost table for different storage caps instead of unlimited.*

98. **Question:** For Section H and I of the RFP:

    H. Provide visibility across all Port networks, on-premises, ***cloud Solutions*** and endpoints.

    I. Vulnerability scanning: 1. Continuous external and internal vulnerability scans and management.

    - 24/7 hunting for internal vulnerabilities, system misconfigurations, and account takeover exposure on the dark web.

    a) **Question:** Are you able to share the specific cloud solutions you're using (SaaS, IaaS, PaaS - combination)?

    ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

    b) **Question:** Do you currently have a vulnerability management tool? what about a cloud security posture management (CSPM), or cloud workload protection platform (CWPP) in place?

    ***Answer**: Not one that the Port would be offering the vendor to use or interface with. Please provide any solution needed to meet the requirements in the scope.*

    c) **Question:** Are you using any microservices such as containers or serverless functions?

    ***Answer**: Yes*

99. **Question:** What is the Port currently using for a SIEM solution?

    ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

100. **Question:** Is the Port currently using an MSSP for security operations support? If not, has the port used one in the past?

Answer: Yes and Yes

101. **Question:** How many firewalls?

Answer: 10

102. **Question:** How many EDR endpoints? Who is the EDR vendor?

Answer: Use 1000 in your estimate

103. **Question:** How many Linux servers? How many Windows servers?

Answer: Please see the response to question number 58.

104. **Question:** What is used for directory services/authentication?

Answer: MS Active Directory.

105. **Question:** Does the Port use email protection products? If so, which ones?

Answer: Yes, This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

106. **Question:** Are there WAF products in place? If so, please provide name(s) of tools.

Answer: No

107. **Question:** Are there web proxies in place?

Answer: No

108. **Question:** What cloud infrastructure exists (AWS, Azure, Google)?

Answer: Azure

109. **Question:** What other security infrastructure (IPS, IDS)?

Answer: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

110. **Question:** Does the Port currently have a vulnerability management platform? If so, what VM platform/product(s)? If not, does the Port have a preferred product?

Answer: Please see the response to question number 98b.

111. **Question:** Specifically, what is meant by Dark Web Data Source Vulnerability Assessments? (Please clarify) In the Pre-Proposal Meeting, it was mentioned that while the Port expected continuous monitoring, it expects quarterly reports. Does the Port require (1) quarterly automated and manual vulnerability and/or pen testing assessments, (2) quarterly automatic scans, or (3) the ability to run quarterly reports?

Answer: Please see the response to question number 15. For reporting, please provide type and frequency that you recommend.

112. **Question:** Does the Port currently have configuration management, asset management, and/or CMDB tools? Please specify tools.

Answer: Yes, This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

113. **Question:** Is the Port open to licensing and/or support models for terms consisting of fewer than seven (7) years? If so, what is the minimum number of years acceptable? If not, is the Port open to pre-paid or partially pre-paid contracts?

Answer: The Port is requiring a 7-year agreement. The Port will not enter into a pre-paid contract.

114. **Question:** How many staff make up the Port's security organization?

Answer: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

115. **Question:** Will there be any SIEM/MDR users or subscribers outside of the security organization? If so, approximately how many users?

Answer: Estimate for 30 user's total.

116. **Question:** Is the Port subject to audits? If so, please explain (e.g. type(s), time-table).

Answer: Yes, at the discretion of the Board.

117. **Question:** Will the Port of Oakland be discontinuing the use of the current SIEM (used primarily for compliance reporting) if the new chosen solution includes a SIEM? If the

old SIEM is to be retired, what will the requirements be for the length that logs are retained?

***Answer**: Yes, 5 years.*

118. **Question:** We are unable to provide a quote that includes unlimited device log ingestion/storage but can provide tiered pricing options if we are able to obtain more detailed information. Can the Port of Oakland provide details, or a close estimate on the number of devices and the EPS of those devices for the following device types (see chart below)?

 ***Answer**: The Port will not breakdown its end points any further than what is in question 58 and 130.*

119. **Question:** What A/V or Endpoint Protection vendor is the Port of Oakland currently using as its primary endpoint protection?

 ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

120. **Question:** Is the Port looking to replace its current Endpoint solution with a joint EDR/EPP tool?

 ***Answer**: Yes*

121. **Question:** Do you have budget range for a monthly spend?

 ***Answer**: Please see the response to question number 34.*

122. **Question:** Can we get a diagram of your network and your workflow to better understand your current environment?

 ***Answer**: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

123. **Question:** How many subnets for each location; will you create a VPN for us to access?

 ***Answer**: We will not be disclosing total subnets by each location. Please specify if VPN access is a requirement for your solution.*

124. **Question:** Do the four sites mentioned on the Pre Bid call connect to one single network or are the four sites networked independently?

 ***Answer**: All four sites are connected.*

125. **Question:** Do the sites have independent internet connections? How many external IP Addresses are active and used?

__Answer__: Currently two sites have internet and the other two are connected with fiber. This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

126. **Question:** Need clarity on the number of endpoints listed e.g. do they all run functions requiring them to be monitored? Are there 5000 user end points?

__Answer__: Please use the 5000 number for estimating total endpoints.

127. **Question:** How many total Data Center Locations are in commission for Port of Oakland? Please share their locations (city/state) and notate primary and Backup/DR (if applicable)

__Answer__: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

128. **Question:** We understand there are roughly 5000 devices to be monitored as part of the overall scope of service. Provide estimated counts of devices by types as listed below:
    - # of Firewalls
    - # of Switches
    - # of Network Devices (Switches/Routers, etc.)
    - # of Number of Domain Controllers
    - # of Workstations
    - # of Servers (both Physical and Virtual) (breakdown by OS would be great)
    - Others

__Answer__: Some details have been provided in response to question number 58. Use the following for additional information:
Firewalls – 10
Routers – 20
Cisco Switches – 300
DNS – 12

129. **Question:** DUO MFA - How many end users will be enrolled for Duo MFA? Is it only employees accessing applications within the network, or will you need to add controls for access outside the network/ geographical zone/country?
    - List and type of Servers (Linux, Internal or External Windows, etc)

__Answer__: DUO MFA has been deployed for all Port users, contractors, etc. See device breakdown in question 58 & 130.

130. **Question:** What compliance/regulatory requirements are pertinent to the scope for Port of Oakland?

__Answer__: Please see the response to question number 94.

131. **Question:** Storage and Availability Requirements – What is the retention Period requirements for Data?

__Answer__: Please see the response to question number 8f.

132. **Question:** Would you prefer the SIEM to be on-prem or in the cloud? If on-prem, the hardware would be provided by the Port of Oakland?

__Answer__: Propose whatever solution you think is the best fit for the Port. If hardware needs to be provided by the Port, please note in your proposal.

133. **Question:** What type of portal access is required for IT Staff for the SIEM platform-read-only or admin level?

__Answer__: Please see the response to question number 65.

134. **Question:** What is the level of access needed on MDR solution for Port IT staff? Is it read only or admin level access?

__Answer__: Please see the response to question number 65.

135. **Question:** Can you please describe in detail your SLA requirements for this service? Based on a 30 min initial acknowledgement of an incident, it would align to our GOLD level but want to make sure we understand SLA/SLO requirements clearly.

__Answer__: The Port is open to reviewing the offerings my vendors. Please provide the different SLA levels you offer and a cost for each.

136. **Question:** In the RFP it states: "Must be trained and credentialed with proven past historical experience of incident management and remediation." We will be providing you with sample resumes of all different types of resources you can expect to be engaged while providing services to Port of Oakland and their respective level of experience and certifications. Is that sufficient?

__Answer__: Yes

137. **Question:** Is a ticketing solution expected to be integrated as a part of the MDR implementation? If so what solution you will be providing for us to use (such as ServiceNow, etc.)?

__Answer__: Not at this time.

138. **Question:** Does the Port have any existing solution in place which can be used to perform soft scan to gather Asset Inventory?

***Answer**: Yes*

139. **Question:** Zero Trust Model: Does the organization have processes in place to conduct periodic review of access for every employee to and provide access based on groups - to enforce Zero trust within the organization? This includes administrative accounts and root access to servers. If not, is this part of the scope?

***Answer**: Yes, and no these reviews are not included in the scope of this project.*

140. **Question:** Does the organization have a privileged access management program in place for vaulting of high-risk accounts/passwords?

***Answer**: Yes*

141. **Question:** Does the organization use multi-cloud hosting for its applications? Are there any on-prem applications to be monitored as well?

***Answer**: No, not at this time.*

142. **Question:** Does the organization use any tool for visibility of assets across all the cloud an on-prem environments?

***Answer**: Yes*

143. **Question:** Will the Port accept electronic submission?

***Answer**: No*

144. **Question:** Will businesses located in Santa Clara County be considered as a local responder to this RFP?

***Answer**: No*

145. **Question:** How many proposals do you anticipate be down selected and will there be a vendor interview for the short list?

***Answer**: We anticipate two to four but depending on the number of proposals we receive, we may increase or decrease those numbers.*

146. **Question:** Item C, detect and respond endpoint and network or just endpoint?

***Answer**: Endpoint and Network.*

147. **Question:** Do you have a current RMM?

***Answer**: No*

148. **Question:** Do you have your own SOC?

Answer: Yes

149. **Question:** Do you need 24/7/365?

Answer: Yes

150. **Question:** Are they tracked in the SIEM today - the OT?

Answer: Only the ones that fall in the PCI scope are tracked currently.

151. **Question:** How do you handle operational technology - OT now? SCADA related systems?

Answer: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

152. **Question:** G2, what do you mean deep dive?

Answer: The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.

153. **Question:** Ability to integrate and also monitor effectively depends on the technologies you may be using for firewall, endpoint protection, etc. If we find the current solutions not up to par, are you open to replacing them with better technology?

Answer: Yes

154. **Question:** Is there a current NDR solution in place?

Answer: Yes

155. **Question:** Is there a documented change control process the service responder must adhere to or will this process be detailed during the assessment phase?

Answer: The Port has a change control process, this will be negotiated with the selected proposer.

156. **Question:** How many external IP addresses; Automatic external IP, domain and sub-domain detection.

Answer: For estimating purposes, 40 External IP's, 6 domains and no sub-domains.

157. **Question:** What ticketing system are you using?

Answer*: ServiceNow*

158. **Question:** Will you expect the MDR to do the full triaging of incidents and respond/take action on the events which are not deemed false positive?

     Answer*: Yes*

159. **Question:** What is the desired response time for onsite triage?

     Answer*: The Port is not expecting onsite triage with this contract.*

160. **Question:** Do you have an isolated networking environment for surveillance system ongoing to it is managed in a united network separate VLANs also how many VLANs total

     Answer*: This question relates to confidential infrastructure information that is critical for security and cannot be shared at this time. This information is also not necessary at this time for producing a fully responsive proposal. The Port will provide additional information to the proposed awardee as necessary for finalizing the agreement.*

161. **Question:** Would you prefer to map to SP800-53 controls for the MDR solution? Any other components to map to?

     Answer*: The port would like the vendors recommendation.*

162. **Question:** If SIEM was implemented for PCI requirements, does it include the complete data set that is reporting to the MDR, and is that number still 5000 devices?

     Answer*: It does not, but for the proposal, please assume 5000 devices.*

163. **Question:** Will you provide access to Pre-proposal recording?

     Answer*: No*

There are no other questions to RFP 21-22/15.