Request for Proposal (RFP) for
SOC/SIEM Solution

Questions & Answers

1. Wanted to check regarding if this work requires onsite presence OR can it be done offshore with just coordination from onshore?
   Answer: As indicated in Section IV. Mandatory Requirements, NYeC requires utilization of onshore resources only to conduct this work.

2. Is it existing work that's being extended/renewed OR entirely new? If existing then please help me with the name of the incumbent vendor currently responsible for the project.
   Answer: This question is not relevant to the scope of work of this project.

3. The current budget allocated for the solicitation.
   Answer: Budgets will be provided by each applicant and scored according to the criteria outlined in the RFP.

4. Also, we would like to know the spend amount of last year under this contract.
   Answer: This question is not relevant to the scope of work of this project.

5. Do all SOC analysts need to be U.S. based? Or can the personnel be global, as long as the data is stored in the US?
   Answer: See response to question 1.

6. Referencing the "10 tests on the system every month to verify the effectiveness of the SOC/SIEM setup," What types of tests are you requiring? Are these tests for the intention of ensuring the SIEM software is operating correctly, or are these tests intended to be a simulated attack with the intention to test response?
   Answer: These tests reflect both types of scenarios to ensure the correct implementation of SOC/SIEM policies and few simulated attacks to validate the capabilities of tool during the real incidents.

7. Do all logs need to have a specific parsing format? Or is it just a requirement to have all the logs ingested? i.e. Snowflake is not a pre-built event parser, but we have the ability to pull in custom logs.
   Answer: Tool meets the requirements as long as we have ability to ingest the logs and run some analysis to populate required information and generate alert when needed. Vendor should be able to ensure the ingestion of custom logs and analysis of it to populate required information from other way around if current parsing algorithms does not digest the logs from mentioned source directly.

8. For alerting that requires additional information on NYeC's user behavior (whether or not it is an expected behavior- i.e. a password reset, multi-country authentication event)- is it acceptable that this type of alert response falls to NYeC? Or is it required that all alert types are responded to by the SOC?

   Answer: SOC is responsible to escalate those alerts to NYeC Staff if any alert needs NYeC attention. SOC will be the primary responder for any alerts generated by the tools.

9. May we redline the MSA and include our legal terms with the proposal submission?

   Answer: An applicant may elect to include redlines to the MSA with their proposal submission; however, such redlines will **not** be evaluated as part of the proposal. Any contractual modifications would be negotiated after an award is made.

10. When does NYeC require submission for the corresponding legal terms outlined in the RFP?

    Answer: The Mandatory Requirements in Section IV are required to enter into a contract with NYeC. Any proposed modifications to contractual terms and conditions would be negotiated after an award is made.

11. Are we able to meet with the NYeC security team prior to the contract award to provide an overview of our offering and how we can align to their needs?

    Answer: As indicated in Section IX. Contract Award, NYeC reserves the option to select finalists for one-on-one interviews.

12. How did NYeC come to include a particular vendor in this RFP?

    Answer: This question is not relevant to the scope of work of this project.

13. Does NYeC have a preferred reseller that they intend to purchase through? If not, is NYeC willing to work with one of an applicant's preferred resellers (opposed to purchasing direct)?

    Answer: NYeC does not have a preferred reseller from which it intends to purchase a SIEM solution. As stated in the RFP, in addition to security operations center services, NYeC is seeking proposals from applicants who can "[p]rocure, provide, setup, support, tune, update, maintain, and fully manage a Security Information & Event Management (SIEM) solution." Responses should therefore explain how applicants propose to procure or provide a SIEM solution.

14. Does NYeC require a formal quote with submission of our proposal, or is it acceptable to provide list cost within our proposal?

    Answer: As indicated in Section VI, the proposal must include a detailed budget for all services outlined in the scope of work. Please provide a separate breakdown of SOC and SIEM services.

15. In regard to client references, does NYeC need customer reference names for written attestation, or does NYeC need applicants to facilitate/ schedule customer reference call(s), or does NYeC need customer contact information to reach out to the customers themselves?

Answer: As indicated in Section VI, the applicant must provide three (3) references including company name, contact name, title, email address and phone number from current customers or customers in the last year similar in product size and scope of this RFP. If applying as a collaborative partnership, please provide the required three (3) references for each company. Proof of being an authorized reseller is also required if applicable.

16. If included in the service offering, is NYeC interested in implementing a vulnerability management solution in tandem with the SIEM/ SOC?
    Answer: While this question is not relevant to the scope of work of this project, it is noted that if an applicant elects to include other service offerings in their proposal, such offerings will **not** be evaluated as part of the proposal. Anything outside the scope of work of this project that is included, will count toward the page limit.

17. How many total users do you have?
    Answer: SIEM Users? - max 10 user accounts required

18. How many firewalls do you have? Vendor?
    Answer: 4, Cisco

19. What is the Qty of Domain Controllers?
    Answer: 4 DCs (2 on-prem, 2 Azure)

20. What is the Qty of Server Host Highly Sensitive or Compliance Information (HIPPA, PCI, etc)?
    Answer: Approx – 35

21. What is the Qty of On-Prem Email Servers?
    Answer:1

22. What is the Qty of Public-Facing Servers?
    Answer: Less than 15

23. Endpoint Protection? Vendor?
    Answer: SIEM Coverage/Bitdefender

24. Are you using MFA? Vendor? How many Users?
    Answer: Azure MFA/ Approx - 30

25. Do you use SD-WAN? Vendor? Qty of Sites?
    Answer: No

26. Do you have DNS Protection? Vendor?
    Answer: No

27. Do you have Cloud Security? Vendor?
    Answer: Yes, by Cloud Provider's native tools, AWS/Azure

28. Do you have Email Security? Vendor?
    Answer: Microsoft/O365

29. Do you have Cisco ISE? Qty seats?
    Answer: No

30. Do you have Lateral Detection? Vendor? Sensors?
    Answer: Yes, from current SIEM tools and that will be decommissioned after implementing the new SIEM.