Request for Proposal (RFP) for
SOC Solution

Questions & Answers

A. Existing Users

1. Please confirm the total number of internal NYeC users whose activity, identities, or endpoints are expected to fall under SOC monitoring.
    - Answer: Our organization currently has ~50 internal NYeC users.
2. Are there any nonemployee users (contractors, partners, external stakeholders) whose access or activity needs to be monitored by the SOC?
    - Answer: Yes, we have under ~900 external users who must also be monitored, as they actively work within our environment and contribute to operations. All external members currently hold guest organization accounts.
3. Are user numbers expected to remain stable during the contract term, or does NYeC anticipate fluctuations impacting SOC operations?
    - Answer: User numbers can fluctuate at any time.

B. Existing Technologies & Environment

4. Beyond AWS, Snowflake, and Office 365 explicitly mentioned, are there any additional on premises or cloud platforms currently generating security relevant logs that are in scope?
    - Answer: No there are not.
5. Please confirm whether all inscope environments (cloud and onpremises) are already integrated with Datadog SIEM, or if new integrations are expected as part of this engagement.
    - Answer: All cloud environments are currently already integrated with Datadog SIEM.
6. Are there any critical applications or systems within AWS or Snowflake that require special handling, prioritization, or custom alerting?
    - Answer: No, not for SOC monitoring besides PHI systems.
7. Please confirm whether Windows event logs and Syslog sources referenced in the RFP are already centrally collected or will require onboarding.
    - Answer: No, not at this time.

C. Tools / Technologies in Scope

8. The RFP specifies Datadog SIEM as the managed SIEM platform. Please confirm that Datadog is the only SIEM tool in scope for this engagement.
    - Answer: Datadog is the only SIEM in scope for this engagement.
9. Are there any other existing security tools (EDR, IAM, email security, cloud security tools) whose telemetry is expected to be monitored or correlated within Datadog SIEM?
    - Answer: There are existing security tools currently integrated and correlated within the Datadog SIEM, including the following:
        0. Cloud Security: GuardDuty and AWS Security Hub
        1. EDR: Microsoft Defender for Endpoint
        2. EDR: Microsoft Defender for Endpoint
        3. DLP: Microsoft Purview
        4. Email Security: Microsoft Defender for Office 365
10. Please confirm whether the SOC provider is expected to configure, optimize, or tune existing Datadog security use cases, or operate only on current configurations.
    - Answer: Presently, security configurations have been implemented in Datadog; however, NYeC is continuously looking for ways to improve current configurations. If the SOC provider has expertise in enhancing the current environment, NYeC is receptive to and encourages this engagement.

D. Monitoring vs. Incident Handling Responsibilities

11. The RFP references enhanced MDR with remediation. Please confirm whether the vendor is expected to provide:
    - Monitoring only, or
    - Answer: NYeC is seeking a vendor to perform--Monitoring and investigation and remediation actions.
12. For remediation activities, please clarify which actions the SOC provider is explicitly authorized to perform autonomously, outside of ransomware scenarios.
    - Answer: Yes, TBD.
13. Are there any incident categories that must always be escalated to NYeC prior to action, aside from those defined in SLAs?
    - Answer: All identified incidents must be escalated to NYeC prior to any remediation performed by the vendor.

E. Monitoring Coverage & Hours of Operation

15. Please confirm that 24x7x365 monitoring is required across all environments without exception.

    - Answer: 24/7/365 Monitoring is required across all environments without exception.

16. Are there any business hour only activities (e.g., reporting reviews, change discussions) expected in addition to 24x7 SOC operations?

    - Answer: Yes, in addition to 24x7 monitoring, business-hour activities include monthly MDR/SOC review meetings, alert tuning discussions, and/or coordination with internal teams for incident review and response.

17. Are there specific holiday coverage requirements beyond standard 24x7x365 operations?

    - Answer: No, standard 24x7x365 SOC coverage is sufficient, and no additional holiday-specific requirements are expected.

F. Tool Licensing vs. Managed Services

17. Please confirm that the scope of this RFP is for a fully managed SOC service and not limited to tool licensing only.

    - Answer: The scope of this RFP is for a fully managed SOC service to support NYeC's existing SIEM (Datadog), including monitoring, alerting, investigation, and response activities. This is not a tool licensing request.

18. Are there any Datadog licensing components that NYeC expects the selected vendor to provide or manage as part of the service?

    - Answer: NYeC currently manages all Datadog licensing internally. The selected vendor will not be responsible for providing licenses but may support configuration, optimization, and effective use of the platform as part of the service.

G. Post Implementation & Ongoing Support

19. Does NYeC expect the selected vendor to provide ongoing support post-implementation for the full contract term?

    - Answer: Yes, NYeC expects the selected vendor to provide ongoing support post-implementation for the full contract term. While the SIEM tool (Datadog) is already implemented, NYeC is open to enhancements and improvements to the current configuration, as well as continued monitoring, tuning, reporting, and collaboration with internal teams.

20. Please confirm whether post-implementation support includes:

    - Continuous monitoring

- Incident response
- Threat hunting
- Reporting and dashboards

- Answer: Yes, support is expected to include the following:
  - Continuous monitoring (as part of SOC activities)
  - Incident response (as part of SOC activities)
  - Threat hunting (as part of SOC activities)
  - Reporting and dashboards (as part of SOC activities; NYeC currently has a series of dashboards implemented, however is open to improvements)

21. Are there any defined support tiers or escalation levels expected beyond those covered in the SOC SLAs?

- Answer: No, there are no additional defined support tiers or escalation levels expected beyond those covered in the SOC SLAs. The SLAs included in the RFP reflect the standard requirements issued by the Department of Health, which serves as an overseer for NYeC.

H. Microsoft Licensing

22. The RFP specifies 90 Office 365 E5 licenses. Please confirm whether any other Microsoft license types (e.g., G3, G5, G5 Security) are currently in use.

- Answer: No, no other Microsoft license types are currently in use. NYeC recently transitioned away from other licensing models and is now operating solely on Office 365 E5 licenses.

23. Are all Office 365 E5 licenses in scope for SOC monitoring, or only a subset?

- Answer: All Office 365 E5 licenses are in scope for SOC monitoring.

24. Are there any plans to upgrade, downgrade, or change Microsoft licensing tiers during the foreseeable future that could impact SOC monitoring or telemetry?

- Answer: No.

I. Asset Inventory & Log Sources

25. Please provide a high-level list and count of assets in scope, including:
    - Cloud accounts: ~40 cloud accounts.
    - Servers: under ~100 Servers
    - Endpoints: under ~50 –60 active endpoints

- Network/security devices: N/A

- Are there any asset types explicitly out of scope for SOC monitoring?
- Answer: At this time, there are no major asset types explicitly out of scope for SOC monitoring. However, certain low-risk devices such as printers are not currently integrated into SOC monitoring activities.

26. Is NYeC able to share an asset inventory or CMDB to support accurate onboarding and monitoring?
    - Answer: Yes, an asset inventory list can be provided after SOW is completed.

J. Volumes, Scale & Operations

27. Does NYeC track or estimate the average daily alert volume currently generated in Datadog SIEM?
    - Answer: NYeC does not currently maintain a formal baseline for average daily alert volume within Datadog SIEM; however, this can be assessed and refined with vendor support as part of ongoing monitoring and tuning activities.
28. Are there any log retention requirements beyond what is currently configured in Datadog?
    - Answer: NYeC is currently reviewing log retention requirements. At present, log retention within Datadog is set to indefinite however, this will be updated to align with OHIP compliance requirements issued by the Department of Health.
29. Are there known environment changes or expansions planned (new systems, new cloud accounts, additional integrations) during the contract period?
    - Answer: TBD, but we will remain within our AWS environment.

K. General

30. Please provide clarification regarding the proposal submission deadline. The cover page mentions April 30, 2026, while the procurement timeline indicates May 1, 2026 (5:00 PM EST).?
    - Answer: Proposals are due May 1, 2026 5:00 PM EST. The RFP cover page has been updated to reflect this correction.
31. Please extend the submission date by 1 week.
    - Answer: We are unable to extend the submission deadline.
32. Will agency consider extending the proposal page limit from 10 pages to 30 pages (excluding the SLA and Cost Proposal). Given the scope and complexity of the requirements, a higher page limit would allow us to provide a more detailed and comprehensive response.
    - Answer: We will increase page limit to 15.

33. Are resumes required of our proposed resources?

    - Answer: The RFP does not specifically require resumes but bios or other descriptions outlining relevant experience and capabilities of staff who will be assigned to this work should be provided.

34. What will be the work Location of proposed team onsite or remote?

    - Answer: Remote.

35. Is there an incumbent on this contract? If so, please provide the incumbent name, current contract number, Period of performance, and value of the contract.

    - Answer: Not required.

36. Could you please provide list of Professional Staff required for task and provide details on their roles and responsibilities?

    - NYeC expects the selected vendor to provide qualified professional staff to support SOC operations. This includes, but is not limited to, SOC analysts, incident response support personnel, and other roles necessary to effectively deliver SOC services outlined in the scope of work.

37. Could you please confirm whether the following items can be excluded from the overall page limit?

    - Answer: NYeC strongly encourages proposers to limit additional appendices that do not specifically contribute to elaborating on the scope of work identified in the RFP. Any additional appendices, marketing materials, etc. that are not requested as part of the RFP may not be considered during the evaluation process.

    i. Sample reports generated by services as well as any details about data/report exporting for further action.
       Excluded. Please keep appendices to a reasonable limit.
    ii. Provide historical SOC/SIEM uptime metrics for the past year from at least two previous clients (without violating confidentiality). Highlight any downtime instances, their causes, and the corrective actions taken.
       Excluded. Please keep appendices to a reasonable limit.
    iii. Resumes
       Excluded. Please keep appendices to a reasonable limit.
    iv. RFP Attachments/ Appendices
       Excluded. Please keep appendices to a reasonable limit.
    v. References
       Included.
    vi. Cover Letter
       Included
    vii. Cover Sheet
       Excluded

viii. TOC
Excluded

ix. Mandatory Requirements
Included

x. Eligibility Criteria
Included

38. Can you provide log volume data to allow me to estimate Datadog costs, storage, or analyst workload?

- Answer: ~90M average logs daily ingested through Datadog platform. Additional questions can be further discussed after RFP process.

39. Alert volume baseline to ensure proper SOC staffing to meet SLAs?

- Answer: TBD

40. Infrastructure inventory of AWS accounts, endpoints, network devices all marked "TBD"

    - Cloud accounts: ~40 cloud accounts.
    - Servers: under ~100 servers.
    - Endpoints: under ~50 –60 active endpoints
    - Network/security devices: N/A

41. Current-state visibility, is Datadog already tuned? Are there existing runbooks? What's the false positive rate today?

- Answer:
    - Datadog is currently tuned; however, as the migration to the platform has been ongoing, NYeC recognizes that further improvements can be made in areas such as alert tuning, runbook development, and reduction of false positives.
    - At present, false positives are most associated with Microsoft 365 account activity (e.g., multiple sign-in attempts) that are ultimately determined to be non-malicious. Higher severity alerts (e.g., critical and high) have not typically resulted in false positives and have been validated as legitimate.

42. AWS Environment

- How many AWS accounts are in the Control Tower / LZA organization? Answer: ~40
- What is the current monthly CloudTrail event volume (approximate)? Answer: ~250M
- How many VPCs require full flow log ingestion? Answer: TBD
- Are GuardDuty and Security Hub already enabled across all accounts? Answer: Yes
- What is the current WAF deployment footprint (how many distributions/ALBs)? Answer: ~ under 20

43. Datadog / SIEM Current State

- What is the current daily log ingestion volume (GB/day)?
    - Answer: ~90M logs

- What is the current monthly alert volume by severity tier?
    - Answer:

      Below are sample volumes based on metrics from the past month:

        - Informational: ~200
        - Low: ~15
        - Medium: N/A
        - High: N/A
        - Critical: N/A *Additional details regarding metrics can be provided after RFP process, as the information requested is considered sensitive.

- What is the current false positive rate?
    - Answer: At present, false positives are most associated with Microsoft 365 account activity (e.g., multiple sign-in attempts) that are ultimately determined to be non-malicious. Higher severity alerts (e.g., critical and high) have not typically resulted in false positives and have been validated as legitimate.

- How many detection rules are currently active (OOTB vs. custom)?
    - Answer: Detection rules can be discussed after selection process.

- Are there existing runbooks/playbooks, or does the awarded vendor need to create these from scratch?
    - Answer: Detection rules can be discussed after selection process.

- What's the current Datadog license tier and any volume caps?
    - Answer: Detection rules can be discussed after selection process.

44. Snowflake
    - Answer: Additional details regarding this environment can be provided after the vendor selection process, as the information requested is considered sensitive.

- What is the total data volume across the 3 sub-environments?
- Approximate number of users/roles to monitor?
- Are audit logs already configured for export, or does this need to be built?

45. Microsoft 365 / Identity

- Beyond the 90 E5 licenses, are there additional M365 users (E3, Business, etc.)?
    - Answer: No
- Is Azure AD / Entra ID P1 or P2? (Affects available log types)
    - Answer: TBD
- Current MFA adoption rate?
    - Answer: 100% of users are required to use MFA.
- Are Conditional Access policies in place, or net-new?
    - Answer: Yes, Conditional Access policies are already in place and enforced.
- On-Premises / Network Infrastructure:
    - Answer: NYeC presently operates under a cloud AWS environment, so series of questions are NA to our environment.

    - How many Windows servers require event log forwarding?
    - How many domain controllers?
    - How many privileged workstations / jump hosts?
    - Complete inventory of network devices (firewalls, switches, VPN concentrators) — make/model/count
    - Complete inventory of security appliances (IDS/IPS, DLP, email gateway) — make/model/count

    - Answer:

        - ✓ SIEM: Datadog
        - ✓ EDR: Microsoft Defender for Endpoint
        - ✓ DLP: Microsoft Purview
        - ✓ Email Security: Microsoft Defender for Office 365
        - ✓ AWS Cloud: GuardDuty and Security Hub

46. Staffing & Operations

- Who currently handles security monitoring, is it in-house, another vendor, or is no one performing this activity?

- Answer: Presently, another vendor is providing security monitoring.

- What's the expected escalation volume to NYeC's internal security team?
  - Answer: TBD
- How many NYeC personnel will require dashboard/portal access?
  - Answer: This has already been established within our environment. Appropriate personnel currently have access to Datadog Dashboards and access.
- What's the expected cadence of environment changes (new accounts, new systems)?
  - Answer: NYeC experiences a generally low to moderate cadence of environment changes, including the provisioning of new accounts and onboarding of new systems.

47. Compliance & Process

- Does NYeC have an existing incident response plan, or do we need to develop one?
  - Answer: Yes, NYeC has an existing Incident Response Plan.
- Are there existing HIPAA/HITRUST compliance artifacts we inherit, or greenfield?
  - Answer: NYeC currently operates under HITRUST compliance and maintains existing compliance artifacts. This includes the collection and management of evidence to support control requirements and audit submissions.
- What is the current state of the BAA and compliance documentation?
  - Answer: NYeC maintains BAAs with applicable vendors and is actively maintaining and updating compliance documentation as part of ongoing HITRUST and Department of Health initiatives.