INDIANA SECRETARY OF STATE
DIEGO MORALES

Indiana Secretary of State

Proposal ID: SOS-26-012
Cloud Log Correlation and Security Event Management Platform Implementation

Questions Submitted with Responses

1. RFP Section: Overview

Bidder Question: Can the State clarify whether the new SIEM platform must completely replace existing tools (e.g., Wiz.io, Trellix, Mandiant), or is the vendor expected to integrate with and extend these platforms?

State Response: The new SIEM platform is not intended to replace existing specialized security tools like Wiz.io, Trellix, or Mandiant. The State expects the proposed SIEM solution to serve as the central hub for security data, integrating with these tools to ingest their alerts, findings, and relevant logs. Bidders should describe their approach to integrating with these and other common security platforms.

2. RFP Section: Overview

Bidder Question: For the three major enterprise systems, will the State provide detailed architecture diagrams and log types during project kickoff, or can we request these during the Q&A stage?

State Response: Detailed architecture diagrams, log source specifications, and other sensitive documentation will be provided to the awarded vendor after contract execution and signing of a Non-Disclosure Agreement (NDA). This information will not be made available during the Q&A stage.

3. RFP Section: Overview

Bidder Question: Does the State prefer a COTS SIEM platform, a vendor-built SIEM, or is either approach acceptable as long as requirements are met?

State Response: The State is platform-agnostic. Either a COTS SIEM platform or a vendor-built/managed SIEM solution is acceptable, provided that the solution is hostable within the State's cloud systems and available for implementation at contract award.

4. RFP Section: Objectives

Bidder Question: Can the State confirm whether BigQuery must serve as the long-term storage platform even if the vendor's SIEM natively uses a different storage backend?

State Response: Yes, this is a mandatory requirement. While the proposed SIEM may use its own native storage for hot/warm data and real-time analytics, all logs must be forwarded to the State's Google BigQuery environment for cost-effective, long-term storage (7 years) and archival. This ensures data ownership and accessibility for historical analysis independent of the SIEM platform.

5. RFP Section: Objectives

Bidder Question: Are there current or anticipated plans to integrate with the Indiana IOT's statewide SIEM or SOC environment?

State Response: While direct integration with the Indiana IOT's statewide environment is not in scope for Phase 1 of this project, the proposed solution should be architected in a way that facilitates future data sharing and collaboration.

6. RFP Section: Objectives

Bidder Question: Does the State require AI/ML models to be explainable (XAI), or is a black-box detection engine acceptable?

State Response: The State has a strong preference for explainable AI/ML models (XAI). Bidders must describe how their solution provides transparency into why a particular detection or anomaly was flagged. Solutions that rely exclusively on "black-box" models will be considered less favorable.

7. RFP Section: Proposal Components

Bidder Question: Does the State require a signed letter of commitment for each key personnel resource?

State Response: Yes. A signed letter of commitment is required for all individuals proposed as key personnel and change to staffing must be approved by the State.

8. RFP Section: Proposal Components

Bidder Question: Should pricing include licensing/subscription costs for 7 years of data retention, or only implementation-year costs?

State Response: Data will be retained within the States control and as such we will bear the cost for storage retention. Only the implementation cost should be expressed.

9. RFP Section: Vendor Requirements

Bidder Question: For GovRAMP/FedRAMP, does the requirement apply only to components hosted by the vendor, or must the entire platform be FedRAMP authorized?

State Response: The GovCloud/FedRAMP authorization requirement applies to all cloud-hosted components of the solution that are managed by the vendor and process or store State data. State’s cloud tenant or on-premise components of those in the deployed within the State's environment do not fall under this requirement.

10. RFP Section: Log Collection & Normalization

Bidder Question: Can SOS provide a list of all AWS/GCP accounts, projects, and approximate log volume (GB/day)?

State Response: Specific account details will be provided to the awarded vendor. For the purposes of this RFP, bidders should base their proposals on the system descriptions provided and describe their pricing model's scalability (e.g., cost per GB/day or per EPS) to handle variable log volumes.

11. RFP Section: Log Collection & Normalization

Bidder Question: For on-prem/hybrid logs, will SOS provide existing agents, or must the vendor supply and configure agents?

State Response: There is no on-prem/hybrid environment.

12. RFP Section: Log Collection & Normalization

Bidder Question: Does the State require support for Windows event logs, Linux syslogs, firewall logs, and application logs beyond what is listed?

State Response: Yes. The listed log sources are not exhaustive. The proposed solution must support a wide range of common enterprise log sources out-of-the-box. Bidders should provide a list of supported log types and parsers with their proposal.

13. RFP Section: Log Enrichment & Threat Intelligence

Bidder Question: Which internal systems (HR, CMDB, Identity systems) will be available for enrichment and will APIs be provided?

State Response: There will be no connections to the internal systems.

14. RFP Section: Log Enrichment & Threat Intelligence

Bidder Question: Are there preferred threat intelligence providers (e.g., DHS AIS, ISACs)?

State Response: The solution must integrate with mandated federal and state threat intelligence feeds, including DHS AIS and relevant ISACs (e.g., MS-ISAC). The platform should also support the integration of other leading commercial and open-source threat intelligence feeds.

15. RFP Section: Real-Time Event Correlation

Bidder Question: The RFP requires <5-second ingestion latency—can SOS confirm which log sources must meet this requirement?

State Response: The sub-5-second ingestion latency requirement applies to critical, time-sensitive security logs, including but not limited to firewall, IDS/IPS, endpoint detection and response (EDR), and authentication logs. A higher latency may be acceptable for less critical, verbose log sources.

16. RFP Section: Real-Time Event Correlation

Bidder Question: Does SOS require historical backfill correlation?

State Response: Yes. The capability to run correlation rules against historical data (e.g., after onboarding a new threat intelligence feed) is a mandatory requirement.

17. RFP Section: Advanced Search & Network Forensics

Bidder Question: Does SOS anticipate packet capture (PCAP) ingestion or just flow logs?

State Response: The primary requirement is for the ingestion and analysis of network flow data (e.g., VPC Flow Logs, NetFlow). While full PCAP ingestion is not a requirement for all

network traffic, the solution should be capable of ingesting targeted PCAP files for specific forensic investigations.

18. RFP Section: Advanced Search & Network Forensics

Bidder Question: Does the State require encrypted packet inspection capabilities?

State Response: This is a required function to that needs to be provided.

19. RFP Section: AI & ML Analytics

Bidder Question: Should AI/ML detections be SOC-ready out of the box, or can they mature during phase 2?

State Response: A baseline set of high-fidelity, SOC-ready AI/ML detections for common threats (e.g., UEBA) must be operational at the end of Phase 1. Further tuning, maturation, and development of custom models are expected activities for Phase 2.

20. RFP Section: Alerting, Notification, Workflow

Bidder Question: Which ticketing platform does SOS prefer for incident creation—ServiceNow, Jira, ADO, or others?

State Response: The solution must provide robust, bi-directional integration with ADO.

21. RFP Section: Alerting, Notification, Workflow

Bidder Question: Should the SIEM serve as the system of record for case management?

State Response: No. The SIEM will serve as the primary detection and investigation platform. ADO will serve as the system of record for incident and case management.

22. RFP Section: Reporting & Dashboards

Bidder Question: What compliance frameworks are in scope? (NIST 800-53, CIS, SOC2, SEA 5, etc.)

State Response: The primary compliance frameworks in scope are NIST 800-53, CIS Controls, and any specific requirements stemming from Indiana SEA 5. The solution must provide pre-built and custom reporting capabilities to support audits against these frameworks.

23. RFP Section: Reporting & Dashboards

Bidder Question: Will SOS require custom executive dashboards beyond what the SIEM natively provides?

State Response: Yes. The vendor will be required to work with State stakeholders to design and build custom executive and operational dashboards tailored to the State's specific reporting needs.

24. RFP Section: SOAR Integration

Bidder Question: Does SOS already have a SOAR platform, or must the vendor propose one?

State Response: The State does not have an existing enterprise SOAR platform. Bidders must propose a solution that includes SOAR capabilities.

25. RFP Section: SOAR Integration

Bidder Question: Are automated playbooks required in Phase 1, or is readiness sufficient?

State Response: The development and implementation of a limited set of high-priority automated response playbooks (e.g., for phishing response, host isolation) are required in Phase 1. A broader library of playbooks will be developed in Phase 2.

26. RFP Section: Data Lakehouse & Storage

Bidder Question: Will the vendor need to manage BigQuery cost optimizations (partitioning, tiering), or is this handled by SOS/IOT?

State Response: The vendor is responsible for ensuring the data they forward to BigQuery is structured and configured correctly for cost optimization (e.g., proper partitioning and clustering). The State will manage the underlying BigQuery account and billing.

27. RFP Section: Data Lakehouse & Storage

Bidder Question: Are there limitations on storage tier movement (standard/cold/archive)?

State Response: The proposed solution must not impose technical limitations that prevent the State from leveraging BigQuery's native storage tiering capabilities for cost management.

28. RFP Section: Security & Compliance

Bidder Question: Are there additional Indiana-specific logging, encryption, or access-control standards beyond IOT published policies?

State Response: All solutions must adhere to the published IOT policies and standards. Any additional requirements specific to this project will be identified and provided to the awarded vendor.

29. RFP Section: Implementation Services

Bidder Question: Should the vendor include penetration testing or security validation in the implementation plan?

State Response: Yes. The vendor's implementation plan should include a phase for independent, third-party security validation or penetration testing of the deployed solution before final acceptance. The vendor does not need to provide the third-party.

30. RFP Section: Technical Environment

Bidder Question: For existing tools (Wiz, Trellix, Mandiant), what integration methods are supported (API, event streaming, webhook)?

State Response: The State prefers modern, real-time integration methods such as APIs and event streaming. The awarded vendor will be provided with technical contacts and documentation to facilitate these integrations.

31. RFP Section: Technical Environment

Bidder Question: Will the SIEM require integration with Indiana IOT's Active Directory/Entra ID tenant?

State Response: There will no integration into IOT's Active Directory, but there will be integration and monitoring of SOS's Active Directory tenant.

32. RFP Section: Project Approach

Bidder Question: Can the State clarify expectations for hybrid Agile—e.g., sprint length, ceremonies, documentation style?

State Response: The State's hybrid Agile approach typically involves two-week sprints, participation in standard ceremonies (daily stand-ups, sprint planning, reviews, retrospectives), and the maintenance of a product backlog. Documentation should be sufficient for operational handoff and architectural review.

33. RFP Section: Project Approach

Bidder Question: Are there any mandatory architecture documentation formats (IOT EA templates)?

State Response: Yes. The awarded vendor will be required to complete and maintain architecture documentation.

34. RFP Section: Staffing Approach

Bidder Question: Does the State require specific roles such as Data Engineer, SIEM Architect, SOC Analyst, ML Engineer, or can the vendor define role mappings?

State Response: While the State anticipates the need for skills covering these areas, bidders may define their own specific roles and titles. The proposal must clearly map the proposed roles and responsibilities to the project requirements and demonstrate that all necessary capabilities are covered by the proposed team.

35. RFP Section: Timeline

Bidder Question: The RFP states system must be deployed within 7–8 months—does this include: ingestion of all log sources? AI/ML tuning? SOC use-case development? UAT + go-live?

State Response: We have updated the RFP – we are looking for implementation for each use case within 4 weeks, and additionally dashboard and results tuning of the system completed in 1-3 months. This includes the ingestion of all identified Phase 1 log sources, initial tuning of AI/ML models, implementation of core SOC use cases, and successful completion of User Acceptance Testing (UAT) leading to go-live.

36. RFP Section: Cost

Bidder Question: Should the cost table separate licensing, implementation, support, and managed SOC services?

State Response: Yes. Bidders must provide a detailed cost breakdown that clearly separates one-time implementation costs from recurring costs such as software licensing/subscriptions, ongoing support/maintenance, and any optional managed services.

37. RFP Section: Budget

Bidder Question: What is the budget allocated for this Project?

State Response: The State has not disclosed the budget for this project. Bidders should propose a cost-effective solution that meets all requirements outlined in the RFP.

38. RFP Section: Incumbent

Bidder Question: Who is the current incumbent for this Project?

State Response: There is no single incumbent for this scope of work. This RFP represents a new, consolidated security analytics and monitoring initiative.

39.

Bidder Question: What is the approximate daily log ingestion rate (GBs) from AWS and GCP?

State Response: This is currently unknown. SOS is going through a drastic rebuild and the amount of data that will be received has yet to be determined. The State has 4 enterprises level systems hosted in the cloud in addition to approximately 6 smaller hosted systems.

40.

Bidder Question: How many employees are there at the Secretary of State

State Response: Approximately 90 staff. This number has no impact on the RFP or project.

41.

Bidder Question: Offer optional managed services or co-managed SOC integration. Is there a preference for a fully managed solution?

State Response: Provide an option for either.