Request for Proposal (RFP): Security Information and Event Management (SIEM) Software Solution

Table of Contents

1. Introduction and Background

Our organization is seeking proposals for a comprehensive Security Information and Event Management (SIEM) solution to enhance our security operations and threat detection capabilities. The SIEM solution will serve as our centralized system for threat detection, aggregating security alerts from multiple sources, simplifying threat response, and facilitating compliance reporting.

The SIEM platform must help our security program operate by collecting security data for future analysis, storing these data points, correlating them to security events, and facilitating analysis of those events. We require deployment of sensors across digital assets to automate data collection, with sensors relaying information back to the SIEM's log and event database.

2. Project Objectives

1. Create a centralized security monitoring and management system that aggregates data from multiple sources

2. Enhance threat detection and response capabilities through advanced analytics and automation
3. Streamline security operations and incident response workflows
4. Improve compliance reporting and audit readiness
5. Reduce mean time to detect (MTTD) and mean time to respond (MTTR) to security incidents
6. Enable proactive threat hunting and security posture improvement

3. Scope of Work

Implementation Services

- SIEM platform installation and configuration
- Integration with existing security infrastructure and tools
- Data source configuration and log collection setup
- Development and implementation of detection rules and correlation logic
- Dashboard and reporting configuration

Training and Documentation

- Administrator training for system configuration and management
- Security analyst training for threat detection and incident response
- Complete system documentation and architecture diagrams
- Standard operating procedures for common tasks

Ongoing Support

- 24/7 technical support with defined SLAs
- Regular system updates and security patches
- Threat intelligence feed management
- System health monitoring and optimization

4. Technical Requirements

Core SIEM Capabilities

1. Data Collection and Aggregation
    - Multi-source log collection and normalization
    - Real-time event processing and correlation
    - Scalable data storage architecture
    - Automated data retention management
2. Security Analytics
    - Real-time correlation and analysis
    - Machine learning-based anomaly detection
    - Behavioral analytics capabilities
    - Custom detection rule creation

5. Functional Requirements

5.1 Activity Monitoring

Tip: This capability focuses on real-time surveillance and documentation of all system activities across your infrastructure. A robust activity monitoring system serves as your first line of defense by establishing normal behavior patterns and quickly identifying potential security incidents through deviation detection.

Requirement	Sub-Requirement	Y/N	Notes
Activity Monitoring	Real-time endpoint activity tracking and documentation		
	Automated alert system for incidents and abnormal activities		
	Network connection monitoring and analysis		
	User activity profiling and baseline creation		
	Access point documentation and tracking		

	Process execution monitoring and validation		
	Network traffic analysis and profiling		
	Session monitoring and recording		
	Privilege use monitoring		
	Remote access monitoring		
	Database activity monitoring		
	Application activity tracking		
	Cloud service usage monitoring		
	Critical system changes tracking		

5.2 Asset Management

Tip: Asset management provides a comprehensive inventory and oversight system for all organizational resources. This foundation is crucial for maintaining security control and ensuring complete visibility across your infrastructure, helping prevent shadow IT and unauthorized asset usage.

Requirement	Sub-Requirement	Y/N	Notes
Asset Management	Automated discovery of new assets accessing the network		
	Real-time asset inventory maintenance		
	Asset classification and categorization		
	Configuration management and tracking		
	Hardware asset tracking		
	Software asset inventory		
	Cloud asset management		

	Virtual asset tracking		
	Asset relationship mapping		
	Asset risk scoring		
	License compliance monitoring		
	Asset performance monitoring		
	End-of-life tracking		
	Asset location tracking		
	Mobile device management integration		
	IoT device discovery and monitoring		
	Asset baseline configuration monitoring		
	Change tracking and validation		

5.3 Log Management

Tip: Log management is the cornerstone of security analysis and compliance reporting. An effective log management system not only collects and stores logs but also ensures their integrity, accessibility, and usefulness for both real-time analysis and historical investigation.

Requirement	Sub-Requirement	Y/N	Notes
Log Management	Secure repository for event logs		
	Automated log collection and aggregation		
	Log parsing and normalization		
	Custom log source integration		
	Log integrity verification		
	Chain of custody maintenance		

	Log compression and archival		
	Log search and retrieval		
	Log rotation management		
	Compliance-driven retention policies		
	Log source health monitoring		
	Log format standardization		
	Raw log access		
	Log forwarding capabilities		
	Log filtering options		
	Historical log analysis		
	Log correlation capabilities		
	Automated log cleanup		

5.4 Event Management

Tip: Event management transforms raw log data into actionable security intelligence. This system correlates and analyzes events across multiple sources to identify potential security incidents, reducing false positives and enabling faster incident response.

Requirement	Sub-Requirement	Y/N	Notes
Event Management	Real-time event monitoring		
	Event correlation across multiple sources		
	Custom correlation rule creation		
	Event prioritization and categorization		
	Event workflow automation		

	Event source management		
	Historical event analysis		
	Event trend analysis		
	Event filtering capabilities		
	Event enrichment		
	Event deduplication		
	Event timeline creation		
	Root cause analysis		
	Impact assessment		
	Cross-platform event correlation		
	Event contextual analysis		

5.5 Automated Response

Tip: Automated response capabilities enable immediate action against identified threats, reducing response times and maintaining consistency in incident handling. This system acts as a force multiplier for your security team by automating routine responses while allowing human oversight.

Requirement	Sub-Requirement	Y/N	Notes
Automated Response	Predefined response playbooks		
	Custom response workflow creation		
	Automated threat containment		
	System isolation capabilities		
	Malware quarantine		
	Account lockout automation		