Request for Proposal: Security Orchestration, Automation, and Response (SOAR) Software Solution

Table of Contents

1. Introduction and Background

Our organization seeks proposals for a comprehensive Security Orchestration, Automation, and Response (SOAR) Software solution to enhance our cybersecurity infrastructure and streamline security operations. The selected solution must coordinate, execute, and automate tasks between various IT workers and tools while providing comprehensive threat management capabilities.

The solution must enable rapid response to cybersecurity attacks while facilitating observation, understanding, and prevention of future incidents. It should provide a centralized view of existing security systems while consolidating security data to improve operational efficiency.

The selected SOAR solution will be a critical component of our security infrastructure, enabling automated incident response, standardized workflows, and improved threat detection capabilities. We expect this implementation to significantly reduce response times, optimize resource utilization, and strengthen

our overall security posture through advanced automation and orchestration capabilities.

2. Project Objectives

2.1 Security Operations Enhancement

- Create a unified view of existing security systems
- Centralize security data collection and management
- Improve operational efficiency and productivity
- Enable faster and more accurate security responses
- Reduce manual task workload
- Strengthen threat and vulnerability management

2.2 Incident Response Optimization

- Improve coordination of security incidents
- Reduce response time to security threats
- Streamline communication between security teams
- Enhance accuracy of incident resolution
- Enable containment, eradication, and recovery of crucial data
- Support real-time collaboration for investigations

2.3 Automation Implementation

- Automate manual security tasks
- Generate automated responses to common security attacks
- Implement standardized response processes
- Enable consistent and transparent security procedures
- Create documented workflow processes
- Establish automated threat hunting capabilities

3. Scope of Work

3.1 Implementation Requirements

- Full solution deployment and configuration
- Integration with existing security infrastructure
- Development of automated workflows
- Data migration from existing systems
- User and administrator training
- Documentation and knowledge transfer

3.2 Core Functionality Delivery

- Threat and vulnerability management system
- Security incident response automation
- Security operations automation
- Asset discovery and management
- Integration with existing security tools
- Playbook development and implementation

3.3 Ongoing Support

- 24/7 technical support
- Regular maintenance and updates
- Performance monitoring and optimization
- Continuous improvement recommendations
- Regular security updates and patches

4. Technical Requirements

4.1 System Architecture

- Cloud-based or on-premises deployment options
- High availability configuration
- Scalable infrastructure

- Secure communication protocols
- Data encryption capabilities
- Backup and recovery mechanisms

4.2 Integration Requirements

- API-based integration capabilities
- Support for standard security tools
- Active Directory/LDAP integration
- Email system integration
- SIEM integration
- Ticketing system integration

4.3 Security Requirements

- Multi-factor authentication
- Role-based access control
- Audit logging capabilities
- Data encryption at rest and in transit
- Secure API endpoints
- Regular security assessments

5. Functional Requirements

5.1 Device Control and Network Access Management

This core module focuses on comprehensive device visibility and access control across the enterprise, enabling granular management of all network endpoints while maintaining security compliance and operational efficiency.

Requirement	Sub-Requirement	Y/N	Notes
Core Device Management	Real-time device monitoring system		

	Automated device discovery and classification		
	Device connection tracking and logging		
	Hardware and software inventory management		
	Device risk assessment capabilities		
	Configuration management tracking		
	Usage pattern analysis and reporting		
Access Control Framework	Role-based access management		
	Geographic location controls		
	Time-based access restrictions		
	Network type differentiation		
	Security posture assessment		
	Compliance status verification		
	Policy inheritance structure		
	Emergency override procedures		
Storage Control	USB device management		
	External drive control		
	Removable media monitoring		
	Data transfer tracking		
	Content inspection		
	Encryption enforcement		

	Key management system		
Mobile Device Controls	Smartphone management		
	Tablet device control		
	Mobile app management		
	Platform-specific policies		
	BYOD support		
	Mobile security enforcement		
	Remote device management		

5.2 Security Operations Management

This section encompasses the core incident handling and response capabilities, providing automated workflows and intelligence-driven threat management to streamline security operations and reduce response times.

Requirement	Sub-Requirement	Y/N	Notes
Incident Response	Automated alert triage		
	Incident classification system		
	Response workflow automation		
	Investigation management		
	Evidence preservation		
	Remediation tracking		
	Impact assessment		
	Root cause analysis		
Threat Management	Real-time threat detection		

	Behavioral analysis		
	Signature-based detection		
	Machine learning capabilities		
	Threat intelligence integration		
	Indicator management		
	Attack pattern recognition		
Automation Framework	Customizable playbooks		
	Workflow automation		
	Task scheduling		
	Conditional execution		
	Script integration		
	Process documentation		
	Version control		
	Error handling procedures		
	Rollback capabilities		
	Performance monitoring		
	Success rate tracking		
	Integration testing		
	Automated documentation generation		
	Quality assurance checks		

5.3 Asset Security Management