Request for Proposal: Threat Intelligence Software Solution

Table of Contents

1. Introduction and Background

Our organization seeks to implement an enterprise-grade threat intelligence software solution to enhance our cybersecurity capabilities through advanced threat detection, analysis, and response capabilities. The solution must integrate with our existing security infrastructure while providing comprehensive threat intelligence capabilities.

Current Environment

- Splunk SIEM deployment
- Palo Alto Networks firewalls
- CrowdStrike EDR solution
- AWS and Azure cloud infrastructure
- Three global SOC locations
- ISO 27001 and SOC 2 compliance requirements

Business Drivers

- Advanced persistent threat protection
- Supply chain risk management
- Regulatory compliance requirements
- Intellectual property protection
- Critical infrastructure security

2. Project Objectives

Primary Objectives

1. Reduce mean time to detect threats by 60%
2. Automate 80% of threat analysis tasks
3. Achieve 90% accuracy in threat detection
4. Decrease incident response time by 50%
5. Integrate with existing security tools
6. Enable proactive threat hunting

Success Metrics

- False positive reduction to under 10%
- Threat detection speed under 15 minutes
- Analysis automation rate above 80%
- Tool integration completion within 90 days
- Automated response to common threats within 5 minutes

3. Scope of Work

Implementation Requirements

1. Software deployment across three global locations
2. Integration with Splunk SIEM
3. Custom dashboard creation for each SOC team

4. Training for 50 security analysts
5. Migration of existing threat intelligence data
6. Development of standard operating procedures

Deliverables

1. Threat intelligence platform deployment
2. Custom integrations with security tools
3. Analyst and administrator training
4. Technical documentation
5. Support and maintenance procedures

4. Technical Requirements

Infrastructure Requirements

1. High availability configuration (99.99% uptime)
2. Maximum latency of 100ms for real-time analysis
3. Data encryption using AES-256
4. Multi-factor authentication integration
5. Load balancing across global locations

Integration Requirements

1. Bidirectional Splunk SIEM integration
2. Palo Alto Networks firewall integration
3. CrowdStrike EDR integration
4. RESTful API availability
5. STIX/TAXII 2.1 support

5. Functional Requirements

5.1 Centralized Management Console

Tip: This section focuses on the core interface requirements that enable effective threat intelligence management across the organization. A robust management console serves as the primary control center for all threat intelligence operations and should prioritize usability while maintaining strict security controls.

Requirement	Sub-Requirement	Y/N	Notes
5.1.1 Administrative Interface	Web-based console with HTML5 support		
	Role-based access control with minimum 5 privilege levels		
	Customizable dashboards for SOC analysts (threat monitoring)		
	Customizable dashboards for Incident responders (alert management)		
	Customizable dashboards for Threat hunters (investigation tools)		
	Customizable dashboards for Security managers (metrics and KPIs)		
	Customizable dashboards for Executive management (risk overview)		
	Multi-tenant architecture supporting 5 separate business units		
	Comprehensive audit logs retained for 365 days		
	Native mobile applications for iOS and Android		
	Secure remote access via SSL VPN		
5.1.2 Policy Management	Centralized policy creation and deployment		

	Minimum 50 customizable policy templates		
	Three-tier policy inheritance structure		
	Policy version control with 90-day history		
	Real-time policy enforcement monitoring		
	Automated policy violation detection		
	Customizable violation response workflows		

5.2 Data Collection and Processing

Tip: Essential capability for gathering and processing threat intelligence from multiple sources. The system must efficiently collect, validate, and normalize data from diverse sources while maintaining data quality and relevance.

Requirement	Sub-Requirement	Y/N	Notes
5.2.1 Threat Feed Integration	Integration with minimum 10 commercial threat feeds		
	OSINT feed aggregation from 20+ sources		
	Industry-specific feed support for financial services		
	Custom feed creation tool		
	Feed health monitoring with 5-minute intervals		
	Feed reliability scoring based on 10 metrics		
	Automated feed validation every 15 minutes		
5.2.2 Dark Web Monitoring	24/7 dark web scanning across major networks		

	Real-time credential exposure alerts		
	Automated brand mention monitoring		
	Data leak detection with pattern matching		
	Dark web marketplace surveillance		
	Automatic artifact collection and analysis		
	Multi-language content translation		
5.2.3 Social Media Analysis	Real-time monitoring of 6 major platforms		
	Automated threat actor profile correlation		
	Campaign tracking across platforms		
	Sentiment analysis with 85% accuracy		
	Automated evidence capture		
	12-month historical data analysis		

5.3 Threat Analysis

Tip: Advanced analytical capabilities combining machine learning and traditional analysis methods to identify and assess threats. The system should provide both automated and manual analysis tools for comprehensive threat evaluation.

Requirement	Sub-Requirement	Y/N	Notes
5.3.1 Machine Learning Capabilities	Supervised learning with 90% accuracy		
	Unsupervised anomaly detection		
	Real-time predictive analytics		
	Behavioral pattern analysis		