Request for Proposal (RFP): Managed Detection and Response (MDR) Software Solution

Table of Contents

1. Introduction and Background
2. Project Objectives
3. Scope of Work
4. Technical Requirements
5. Functional Requirements
6. Vendor Qualifications
7. Evaluation Criteria
8. Submission Guidelines
9. Timeline
10. Contact Information

1. Introduction and Background

Our organization seeks proposals for a comprehensive Managed Detection and Response (MDR) software solution that combines advanced technology with human expertise to proactively detect, analyze, and respond to threats across our IT environment. The solution must provide continuous monitoring, threat intelligence integration, and skilled analyst support to deliver comprehensive protection against evolving cyber threats.

2. Project Objectives

The implementation of an MDR solution aims to:

- Establish 24/7 security monitoring and threat detection capabilities
- Enable rapid incident response and threat containment

- Integrate advanced threat intelligence and behavioral analytics
- Automate routine security operations and response procedures
- Enhance visibility across our entire IT infrastructure
- Strengthen compliance with industry security standards
- Reduce mean time to detect (MTTD) and mean time to respond (MTTR)
- Improve overall security posture through proactive threat hunting

3. Scope of Work

The selected vendor will be responsible for:

- Deploying a comprehensive MDR solution integrating SIEM, EDR, and SOAR capabilities
- Establishing 24/7 proactive security operations center (SOC) alerts monitoring
- Implementing automated threat detection and response workflows
- Providing threat hunting and incident response services
- Delivering regular security assessments and recommendations
- Supporting compliance monitoring and reporting requirements
- Conducting staff training and knowledge transfer
- Maintaining solution updates and threat intelligence feeds

4. Technical Requirements

4.1 Technology Stack Requirements

SIEM Capabilities

- Real-time log collection and correlation
- Advanced analytics and threat detection
- Custom rule creation and management
- Historical data retention and analysis

- Automated alert prioritization

EDR Functionality

- Continuous endpoint monitoring
- Real-time threat detection and response
- Endpoint isolation capabilities
- Behavioral analysis and anomaly detection
- Automated remediation actions

Network Analysis

- Deep packet inspection
- Network behavior analytics
- Traffic pattern monitoring
- Protocol analysis
- Anomaly detection

SOAR Integration

- Automated incident response
- Customizable playbook creation
- Multi-tool orchestration
- Case management
- Workflow automation

5. Functional Requirements

5.1 Threat Detection and Response Capabilities

Tip: ***Critical security monitoring and incident response capabilities that provide comprehensive coverage across all attack surfaces while maintaining fast detection and response times. Focus on automation capabilities to reduce manual intervention requirements.***

Requirement	Sub-Requirement	Y/N	Notes
Real-time Monitoring	Continuous network traffic analysis with sub-second processing		
	Real-time endpoint activity monitoring across all managed devices		
	Live memory analysis and process monitoring		
	Active directory and user behavior monitoring		
	Application stack monitoring and analysis		
	Infrastructure configuration change detection		
	Cloud service and resource monitoring		
	Container and orchestration platform monitoring		
Threat Detection Methods	Signature-based detection with daily updates		
	Machine learning-based behavioral analysis		
	Statistical anomaly detection		
	Heuristic-based detection algorithms		
	Indicator of Compromise (IoC) matching		
	MITRE ATT&CK framework mapping		
	Fileless malware detection		
	Living-off-the-land attack detection		
	Zero-day threat detection capabilities		
Response Automation	Automated threat containment procedures		

	Endpoint isolation mechanisms		
	Network segment isolation		
	Automated malware quarantine		
	User account suspension		
	Access token revocation		
	System restore capabilities		
	Automated evidence collection		
	Chain of custody maintenance		

5.2 Security Operations Center Integration

Tip: ***SOC team platform interaction capabilities that streamline analyst workflows while maintaining clear documentation and enabling effective collaboration across teams.***

Requirement	Sub-Requirement	Y/N	Notes
Analyst Workflow	Tiered analyst assignment system		
	Case management and tracking		
	Investigation workflow automation		
	Evidence collection tools		
	Forensic analysis capabilities		
	Collaboration tools for analyst teams		
	Knowledge base integration		
	Shift handover automation		
	Investigation playbook execution		

Incident Management	Incident categorization system		
	Severity level assignment		
	Impact assessment tools		
	Stakeholder notification system		
	Escalation procedure automation		
	War room creation and management		
	Post-incident review automation		
	Lessons learned documentation		
	Incident timeline reconstruction		

5.3 Threat Intelligence Integration

Tip: ***Solution capabilities for aggregating and operationalizing threat intelligence from multiple sources while maintaining data quality and relevance to the specific environment.***

Requirement	Sub-Requirement	Y/N	Notes
Intelligence Sources	Commercial threat feed integration		
	Open-source intelligence incorporation		
	Industry-specific threat feeds		
	Government advisory integration		
	Peer-group intelligence sharing		
	Dark web monitoring		
	Social media threat tracking		
	Vulnerability database integration		