Request for Proposal: Deception Technology Software Solution

Table of Contents

1. Introduction and Background

Our organization seeks proposals for a comprehensive deception technology software solution to enhance our cybersecurity infrastructure. The solution will create and manage decoy assets to detect, analyze, and respond to potential threats within our network environment.

The selected solution must provide proactive cybersecurity capabilities designed to lure attackers away from valuable assets by creating decoys—including credentials, files, servers, and network nodes—that appear as real targets within the network.

2. Project Objectives

1. Deploy an enterprise-grade deception technology platform that creates and maintains convincing decoy assets
2. Enhance detection capabilities for advanced threats and lateral movement
3. Reduce false positives in threat detection through high-fidelity alerts

4. Generate actionable threat intelligence from attacker interactions
5. Integrate deception capabilities with existing security infrastructure
6. Improve time to detect and respond to potential threats

3. Scope of Work

Implementation Requirements

1. Full deployment of deception technology platform
2. Creation and configuration of decoy assets across network layers
3. Integration with existing security tools and infrastructure
4. Alert system configuration and customization
5. Implementation of automated response capabilities

Operational Requirements

1. Ongoing management of deceptive assets
2. Regular updates to deception scenarios
3. Maintenance of threat intelligence feeds
4. Support for incident response activities
5. Regular effectiveness assessment and optimization

4. Technical Requirements

Network Integration

1. Support for multiple network segments
2. Integration with existing network security tools
3. Support for virtual environments
4. Cloud infrastructure compatibility
5. Support for IoT and SCADA/ICS environments

Security Features

1. Encrypted communications

2. Secure management console access
3. Role-based access control
4. Audit logging capabilities
5. Secure data storage

Performance Requirements

1. Minimal impact on network performance
2. High availability configuration options
3. Scalable architecture
4. Real-time monitoring capabilities
5. Rapid deployment capabilities

5. Functional Requirements

5.1 Honeypot and Honey Token Management

Tip: Effective honeypot deployment requires a balance between authenticity and manageability. Focus on creating believable decoys that match your environment's characteristics while maintaining operational efficiency. Consider both active (interactive) and passive (monitoring) honeypots based on your threat intelligence needs.

Requirement Category	Feature	Y/N	Notes
Deployment Capabilities			
	Automated creation and deployment of various honeypot types		
	Customizable honey token generation		
	Dynamic adjustment of decoy sophistication levels		
	Geographical distribution controls		

	Asset lifecycle management		
Asset Types Support			
	Network honeypots (TCP/IP services, network protocols)		
	Application honeypots (web servers, databases, APIs)		
	Credential-based honey tokens		
	File-based decoys		
	Email-based traps		
	Cloud service decoys		

5.2 Automated Alert System

Tip: Alert fatigue is a common challenge in security operations. Design your alert system to prioritize high-fidelity signals and implement intelligent correlation to reduce noise while maintaining visibility of genuine threats.

Requirement Category	Feature	Y/N	Notes
Alert Generation			
	Real-time alert creation for decoy interactions		
	Customizable alert thresholds		
	Priority-based alert classification		
	Context-rich alert details		
	Correlation of related alerts		
Alert Management			

	Central alert dashboard		
	Alert triage capabilities		
	False positive reduction features		
	Alert suppression rules		
	Historical alert tracking		

5.3 Integration Capabilities

Tip: Integration success depends on standardized data formats and robust APIs. Ensure your integration strategy includes both real-time and batch processing capabilities, with clear error handling and data validation procedures.

Requirement Category	Feature	Y/N	Notes
SIEM Integration			
	Bidirectional data flow		
	Custom log formats support		
	Real-time log streaming		
	Historical data import		
	Correlation rule creation		
Security Tool Integration			
	Firewall integration		
	IDS/IPS integration		
	Endpoint security integration		
	Network monitoring tool integration		
	Threat intelligence platform integration		

5.4 Orchestrated Response

Tip: Automated response actions must be carefully designed to prevent unintended consequences. Implement graduated response levels and ensure human oversight for critical actions that could impact production systems.

Requirement Category	Feature	Y/N	Notes
Response Automation			
	Predefined response playbooks		
	Custom response action creation		
	Conditional response triggers		
	Response effectiveness tracking		
	Automated containment actions		
Environment Manipulation			
	Dynamic decoy modification		
	Network segment isolation		
	Service availability control		
	Traffic manipulation		
	Asset interaction tracking		

5.5 Management Console Requirements

Tip: An effective management console should balance comprehensive functionality with usability. Focus on intuitive visualization capabilities and ensure that critical information is easily accessible without overwhelming operators.

Requirement Category	Feature	Y/N	Notes
Dashboard Features			

	Real-time attack visualization with attack path mapping		
	Decoy asset status monitoring with health metrics		
	Interactive network topology visualization		
	Advanced attack pattern analysis tools		
	Geographic attack origin mapping		
	Risk scoring dashboard for detected threats		
Administrative Controls			
	Granular role-based access control		
	Multi-tenant architecture support		
	Comprehensive audit logging		
	Advanced configuration management		
	Automated backup and recovery tools		
	Remote administration capabilities		

5.6 Deceptive Asset Customization

Tip: Successful deception requires assets that closely mirror your production environment. Implement a systematic approach to asset creation that includes regular updates and authenticity verification to maintain credibility.

Requirement Category	Feature	Y/N	Notes
Network Deception			
	Custom network service emulation		
	Protocol-specific deception capabilities		

	Network segment replication		
	Traffic pattern matching		
	Dynamic port allocation		
	Service vulnerability simulation		
Data Deception			
	Customizable file content generation		
	Database honeypot creation		
	Sensitive data simulation		
	Document watermarking capabilities		
	Custom metadata injection		
	File access tracking		

5.7 Advanced Detection Capabilities

Tip: Layer your detection capabilities to catch both known attack patterns and novel threats. Use machine learning to enhance detection accuracy while maintaining explainability for investigation purposes.

Requirement Category	Feature	Y/N	Notes
Behavioral Analysis			
	Advanced pattern recognition		
	Anomaly detection engines		
	Machine learning-based threat detection		
	Attack technique classification		
	Attacker toolkit identification		