Request for Proposal: Malware Analysis Tools

Table of Contents

1. Introduction and Background

Our organization is seeking proposals for comprehensive malware analysis tools to enhance our cybersecurity capabilities. The solution should provide advanced capabilities for detecting, analyzing, and responding to malware threats across our security infrastructure.

Current Security Posture

- Integration requirements with existing security tools
- Current challenges in malware detection and analysis
- Types and volume of threats encountered
- Existing analysis workflows and processes

Project Objectives

- Implement comprehensive malware analysis capabilities
- Enhance threat detection and response effectiveness

- Improve analysis automation and efficiency
- Strengthen security incident investigation capabilities
- Enable advanced forensic analysis capabilities

2. Technical Requirements

A. Analysis Requirements

1. **Static Analysis**

- File metadata examination
- Code analysis without execution
- Header analysis capabilities
- Resource and string extraction
- Pattern matching functionality
- Technical parameter analysis
- Early-stage malware identification
- Signature-based detection

1. **Dynamic Analysis**

- Secure sandbox environment
- Complete host environment simulation
- Real-time behavior monitoring
- Process tracking and analysis
- Memory analysis capabilities
- Network activity monitoring
- File system tracking
- Registry monitoring
- API call analysis

1. **Hybrid Analysis**

- Combined static and dynamic capabilities
- Advanced threat detection
- Hidden malicious code identification
- Comprehensive indicators of compromise
- Behavioral pattern analysis
- Multi-layer analysis capabilities
- Pattern correlation
- Advanced heuristics

1. **Forensic Analysis**

- Post-compromise examination tools
- System change tracking
- Suspicious activity logging
- Artifact collection and preservation
- Timeline analysis
- Root cause identification
- Evidence preservation
- Chain of custody maintenance

3. Functional Requirements

A. Core Analysis Features

Tip: Focus on comprehensive analysis capabilities across binary, memory, and network layers. Ensure tools can handle both static and dynamic analysis while supporting advanced debugging and reverse engineering needs.

Requirement	Sub-Requirement	Y/N	Notes
Binary Analysis	Static binary examination		
	Dynamic binary analysis		
	Binary unpacking capabilities		
	Code flow analysis		
	Function identification		
	Library dependency analysis		
	Entry point analysis		
	Binary reconstruction tools		
Memory Analysis	Live memory analysis		
	Memory dump analysis		
	Memory mapping		
	Process memory inspection		
	Heap analysis		
	Stack analysis		
	Memory pattern matching		
	Memory reconstruction		
Network Protocol Analysis	Protocol decoding		
	Protocol reconstruction		
	Custom protocol analysis		
	Protocol anomaly detection		
	Traffic pattern analysis		

	Command and control detection		
	Protocol hierarchy analysis		
	Network session analysis		

B. Detection and Response

Tip: Prioritize solutions that combine automated detection with manual analysis capabilities, enabling both rapid threat identification and detailed investigation capabilities while supporting efficient incident response workflows.

Requirement	Sub-Requirement	Y/N	Notes
Malware Identification	Behavioral analysis capabilities		
	Process monitoring		
	File system tracking		
	Activity log analysis		
	IoC extraction		
	Pattern recognition		
	Signature detection		
	Heuristic analysis		
Threat Analysis and Triage	Initial malware sample triage		
	Suspicious artifact discovery		
	Debugging capabilities		
	Reverse engineering tools		
	High-fidelity alerting		
	Threat categorization		

	Priority assessment		
	Risk scoring		

C. Advanced Capabilities

Tip: Ensure comprehensive coverage of sophisticated evasion techniques and specialized analysis needs across various platforms, with particular focus on emerging threat types and advanced persistent threats.

Requirement	Sub-Requirement	Y/N	Notes
Anti-Evasion Techniques	Anti-VM detection counters		
	Anti-debugging prevention		
	Anti-sandbox detection		
	Time-based trigger detection		
	Environment-aware malware detection		
	Code obfuscation analysis		
	Packed malware analysis		
	Anti-analysis technique detection		
Specialized Analysis	Firmware analysis		
	Mobile malware analysis		
	IoT malware detection		
	Embedded system analysis		
	Custom protocol analysis		
	Advanced persistent threat analysis		
	Rootkit detection		

	Polymorphic malware analysis		

D. Automation and Intelligence

Tip: Focus on solutions that provide robust automation while maintaining analysis accuracy, with strong machine learning capabilities that can adapt to your environment and evolve with emerging threats.

Requirement	Sub-Requirement	Y/N	Notes
Process Automation	Automated sample extraction		
	Automated unpacking		
	Automated classification		
	Automated reporting		
	Automated correlation		
	Automated remediation		
	Automated quarantine		
	Automated prioritization		
Machine Learning Integration	Automated threat classification		
	Pattern recognition algorithms		
	Behavioral analysis automation		
	Predictive threat detection		
	Automated triage processes		
	Self-learning capabilities		
	Model training tools		
	Performance monitoring		

E. Analysis Environment

Tip: Prioritize highly configurable and secure analysis environments that provide complete isolation while supporting diverse testing scenarios and preventing cross-contamination.

Requirement	Sub-Requirement	Y/N	Notes
Sandbox Configuration	Multiple environment support		
	Custom environment creation		
	Resource allocation control		
	Network simulation options		
	Hardware simulation		
	Operating system diversity		
	Snapshot management		
	Environment reset capabilities		
Environment Isolation	Network isolation controls		
	Process isolation		
	Memory isolation		
	Storage isolation		
	Resource containment		
	Access control management		
	Data segregation		
	Cross-contamination prevention		

F. Reporting and Analytics

Tip: Look for comprehensive reporting capabilities that balance technical detail with actionability, supported by robust visualization tools that can effectively communicate findings to different stakeholders.