Request for Proposal: Breach and Attack Simulation (BAS) Software Solution

Table of Contents

1. Introduction and Background

Our organization seeks proposals for a comprehensive Breach and Attack Simulation (BAS) software solution to enhance our cybersecurity testing and validation capabilities. We require a robust system that continuously tests our security controls through automated attack simulations and provides actionable insights for improvement.

Current Environment

We maintain a complex cybersecurity infrastructure that includes:

- Network security controls (firewalls, IDS/IPS)
- Endpoint protection platforms
- Email security solutions

- Cloud security tools
- Security information and event management (SIEM) system
- Security orchestration and automated response (SOAR) platform

Business Drivers

- Need for continuous security validation
- Requirement to test against emerging threats
- Compliance with industry regulations
- Resource optimization for security testing
- Improved security ROI measurement

2. Project Objectives

The primary objectives for implementing a BAS solution are:

Enhance Security Validation

- Implement continuous testing of security controls
- Validate effectiveness of existing security investments
- Identify security gaps before they can be exploited

Improve Response Capabilities

- Enable realistic attack scenario testing
- Strengthen incident response procedures
- Validate detection and prevention capabilities

Support Compliance Requirements

- Demonstrate security control effectiveness
- Generate compliance-ready reports
- Maintain audit trail of security testing

Optimize Security Resources

- Automate routine security testing
- Prioritize remediation efforts

- Provide clear metrics for security improvements

3. Scope of Work

The selected vendor will be responsible for:

Software Implementation

- Installation and configuration of BAS platform
- Integration with existing security tools
- Configuration of initial attack scenarios
- Setup of reporting and dashboards

Knowledge Transfer

- Administrator training
- Security team training
- Documentation delivery
- Best practices guidance

Ongoing Support

- Technical support
- Platform updates
- Threat intelligence updates
- Regular health checks

4. Technical Requirements

4.1 Platform Requirements

Deployment Options

- Support for cloud-based deployment
- On-premises deployment capability
- Hybrid deployment support
- Multi-site deployment support

System Requirements

- Minimum server specifications
- Network bandwidth requirements
- Storage requirements
- Database requirements

Security Requirements

- Encryption for data at rest
- Encryption for data in transit
- Role-based access control
- Multi-factor authentication
- Audit logging

4.2 Integration Requirements

Required Integrations

- SIEM integration
- SOAR platform integration
- Vulnerability scanner integration
- Ticket system integration
- Active Directory/LDAP integration

API Requirements

- RESTful API availability
- API documentation
- Custom integration support
- Webhook support

5. Functional Requirements

5.1 Attack Simulation Capabilities

Tip: Attack simulation capabilities form the core of any BAS solution. Focus on breadth of coverage across different attack vectors and the ability to safely execute these simulations without impacting production environments. Ensure the solution provides both depth and safety in testing.

Category	Requirement	Y/N	Notes
Core Simulation Engine - Framework Alignment	Full MITRE ATT&CK framework coverage		
	Custom framework support		
	Mapping of techniques to security controls		
	Real-time framework updates		
	Technique chaining capabilities		
Core Simulation Engine - Execution Control	Granular simulation controls		
	Real-time execution monitoring		
	Kill-switch functionality		
	Rollback capabilities		
	Simulation scheduling		
	Concurrent execution support		
Core Simulation Engine - Environment Protection	Sandboxing capabilities		
	Production safeguards		
	Resource throttling		
	Impact analysis		
	Environmental checks		

	Recovery procedures		
Network Attack Simulation	Lateral movement techniques		
	Network protocol attacks		
	Man-in-the-middle scenarios		
	DNS attack simulation		
	Network tunneling detection		
	Data exfiltration scenarios		
	Command and control simulation		
	Network segmentation testing		
	Zero-day exploit simulation		
	Custom payload support		
Endpoint Attack Simulation	Process injection techniques		
	Memory manipulation		
	Credential theft simulation		
	Registry manipulation		
	File system attacks		
	Driver manipulation		
	Boot sector attacks		
	PowerShell attack simulation		
	Living-off-the-land techniques		
	Fileless malware simulation		

Email Security Testing	Spear-phishing campaigns		
	Business email compromise		
	Malicious attachment simulation		
	URL-based attacks		
	Social engineering scenarios		
	Newsletter subscription abuse		
	Email spoofing detection		
	DMARC/DKIM/SPF testing		
	Email gateway validation		
	User awareness metrics		
Web Application Testing	SQL injection patterns		
	Cross-site scripting (XSS)		
	CSRF attacks		
	Authentication bypass		
	Session hijacking		
	API security testing		
	Web service attacks		
	Cookie manipulation		
	Input validation testing		
	Business logic abuse		
Cloud Security Testing	Cloud misconfigurations		

	Identity access testing		
	Storage security validation		
	Serverless function testing		
	Container security		
	Cloud service enumeration		
	Resource exposure testing		
	Cross-account attacks		
	Cloud API abuse		
	Service integration testing		

5.2 Control Validation Framework

Tip: Control validation is crucial for measuring defense effectiveness. Ensure the solution can test across the full spectrum of security controls - from prevention through detection to response - while providing clear metrics for control effectiveness and failure points.

Category	Requirement	Y/N	Notes
Prevention Controls	Firewall rule validation		
	IPS signature testing		
	Anti-malware effectiveness		
	Web filtering accuracy		
	DLP policy validation		
	Access control testing		
	Encryption verification		
	Network segmentation		