

Breach and Attack Simulation

Validate Your Security Controls Through Automatic, Continuous Testing

Three things are true of security controls: They fail constantly. They fail silently. And their failures can have disastrous, costly impacts on your organization.

The best way to test the effectiveness of your security controls is to attack them as an adversary would. By safely simulating dozens of real-world attacks on your systems across the full cyber kill chain, Breach and Attack Simulation (BAS) allows you to spot the gaps in your security controls **before adversaries do.**

Why Leading Companies Choose SP6's BAS

PROACTIVE APPROACH TO SECURITY

Our services allow you to stay ahead of bad actors by identifying and remediating security gaps *before* they get exploited.

FAST DEPLOYMENT AND RESULTS

We can deploy BAS in hours or days, not weeks or months. You'll receive the results of the simulation within minutes, allowing you to take action now toward better security.

CONTINUOUS VISIBILITY

Rather than providing a point-in-time snapshot of your security controls, we use automation to produce a continuous, up-to-date picture of how your controls are operating.

CONCRETE REMEDIATION GUIDANCE

We'll provide you with a comprehensive report illustrating exactly where your security controls failed and how they can be fixed.

PRIORITIZATION BASED ON SEVERITY OF RISK

Our BAS software will aggregate the results from all simulations and rank them by severity, allowing you to prioritize remediation efforts based on risk to your organization.

JUSTIFICATION FOR SECURITY SPENDING

By testing how your organization would fare in a real-world attack, we reveal exactly which areas of your environment are making you vulnerable. This gives you hard-to-refute justification for securing additional tools, budget, or staff.

67%

of breaches evaded
pre-existing security
controls

91%

of cyberattacks
never generated
an alert

53%

of attacks
successfully infiltrated
environments without
detection

Source: Mandiant Security
Effectiveness Report

Breach and Attack Simulation

SP6 BAS Package Options

We offer three competitive package options that vary in cadence and simulation types.

ENGAGEMENT CADENCE	Foundational MONTHLY CADENCE BI-WEEKLY SCANNING	Proactive BI-WEEKLY CADENCE - WEEKLY SCANNING	Elite WEEKLY+ CADENCE AND SCANNING
Security Control Base Lining			
Endpoint Validation	☑	☑	☑
Network Perimeter Validation	☑	☑	☑
Email Validation	☑	☑	☑
Alert Validation	☑	☑	☑
Attack Path Validation		☑	☑
Data Exfiltration Validation		☑	☑
WebApp Validation		☑	☑
SIEM Validation			☑
Threat Informed Defense			
Emerging Threats Validation	☑	☑	☑
Known Threat Actor Validation			☑
Threat Intelligence Validation			☑
MITRE Alignment and Maturation			☑
Reporting and Remediation			
Remediation Recommendations	☑	☑	☑
Cadenced Progress Reports	☑	☑	☑
Customize Risk Based Reports Per Business Unit/Solution			☑

OPTIONAL PACKAGES – Customized for your needs

Compliance and Risk Management
 Risk Based Vulnerability Management
 NST 800-53 Validation
 Compliance Optimization

Cloud and Contoniorization
 Cloud Configuration Validation
 Container Validation (Docker)
 Cloud Threat Assessment

Hope is not a strategy.

**Test the effectiveness of your
security defenses now.**

**Start a Conversation
with SP6**