Cymulate

How BAS Enhances Your SOC

Using Breach and Attack Simulation to Continuously Challenge and Optimize the Effectiveness of Your Security Controls

The Challenge: Exposure Data Sprawl

Enterprise security infrastructures average 80 security products[1], creating "security sprawl" and a big management challenge for security operation center (SOC) teams. Multiple security controls generate hundreds of daily alerts, making it difficult to identify priorities, assign remediation tasks, and validate that corrective steps taken are, in fact, effective. Even with data from Security Information and Event Management (SIEM) tools, Security Orchestration, Automation and Response (SOAR) platforms, vulnerability management solutions, and Endpoint Detection and Response (EDR) tools, SOC teams still must integrate and interpret the aggregated data before they can prioritize mitigative activities.

Integrating BAS with SOC Operations

Organizations need to know that they're safe—now. Breach and Attack Simulation (BAS) addresses this need, making it an essential addition to SOC teams. But BAS can deliver even more. Integrating BAS with your SOC empowers your team to unify actionable information, enrich event and alert data, prioritize alerts accurately, validate remediation effectiveness, and continually improve your security posture.

SIEM Integration

As SIEM platforms lie at the heart of the SOC, it's vital to ensure they effectively pickup events and alerts. By integrating BAS, SOC teams can:

- Validate SIEM integrations with other security controls across the organization's infrastructure, ensuring that events and alerts are being picked up by the SIEM
- Refine SIEM rules using forensic artifacts—such as hash values, domain names, host artifacts, etc.—provided in attack simulation analyses
- Assess effectiveness of preventative controls, such as EPP, Web Gateway, Email Gateway, Firewall, IPS, and more
- Assess effectiveness of detection controls, such as EDR, EUBA, deceptions, honeypots, and other behavior-based tools

The BAS dashboard provides specific assessment details about myriad controls' ability to detect suspicious activity. For example, the SOC team can launch an Immediate Threats Intelligence assessment to simulate the latest threats seen in the wild. Once the simulation is completed, the SOC team can pull BAS results into the SIEM, where they can parse it, create alerts, and use it for remediation purposes. Data from lateral movement, data exfiltration, and other attack vector simulations also can be pulled into the SIEM, enabling teams to take corrective steps.

SOAR Integration

Similarly to SIEM integration, BAS-generated data can be pulled into SOAR platforms, enabling SOC teams to:

- Refine SOAR incident-response playbooks
- Assess effectiveness of post-breach controls
- Assess effectiveness of monitoring and response workflows
- Prioritize mitigation efforts according to heuristic cyber exposure scores

SOC teams can run BAS on an ongoing basis—daily, hourly, or continuously—and pull results into the SOAR for insight that can be incorporated into automated playbooks or assigned as tasks in SOAR workflows. Team members can prioritize remediation and take corrective steps right from the SOAR dashboard, allowing security effectiveness testing to become part of everyday activities.

1 Are there too many cybersecurity companies? HelpNet Security, March 30, 2018, https://www.helpnetsecurity.com/2018/03/30/too-many-cybersecurity-companies/

Integration with GRC Systems

Governance, Risk, and Compliance (GRC) tools, such as RSA Archer, give organizations a way to quantify and address corporate risk. Besides helping them manage compliance risk, companies increasingly need to manage risks occurring as a result of digital transformation efforts and third-party or supply-chain relationships. BAS results can be integrated with GRC solutions to provide granular data for risk assessment.

Automated BAS helps teams identify and preempt potential adverse impacts of IT configuration changes, software updates, and new technology deployments. It enables them to validate and quantify control effectiveness at specific points in time and over time. BAS continuously challenges controls securing touchpoints with partners, such as portals, email and web gateways, and endpoints—helping teams reduce supply chain risk.

Integration with Vulnerability Management Tools

By pulling information from vulnerability scanners into the BAS platform, SOC teams can:

- View common vulnerability and exposure (CVE) data combined with attack simulation results
- Identify machines that can potentially be exploited using known CVEs and other vulnerabilities along a simulated lateral movement route
- Accelerate prioritization and remediation of unpatched systems according to various parameters, such as asset type, user privileges, and proximity to your organization's most critical digital assets (crown jewels)

Integration with EDR Tools

By integrating BAS with EDR tools, the SOC team can verify that these solutions are effectively detecting IoCs and attack techniques of the latest simulated threats, whether they mimic ransomware, cryptominers, Trojans, worms or other types of cyber attacks. They also can verify that—when needed—response tools will work as expected, enable them to contain threats, block communications, or perform other countermeasures. Whether using customizable or out-of-the-box templates, SOC teams can simulate specific threat behaviors on their endpoints. For example, they can simulate ransomware or Trojan behavior. BAS also enables teams to methodically run simulations mapped to MITRE ATT&CK techniques to proactively challenge and optimize their security controls.

The Cymulate API

SOC teams use the Cymulate API to integrate BAS results with their own platforms. API integration enables them to retrieve all assessment results from simulated attacks—including IoCs, TTPs, payload names, mitigations, other data—and move into their own environments. BAS results can be used in many different ways to automate daily tasks and procedures.

Integration Benefits

- **Immediate insights:** BAS results and data are always at the SOC team's fingertips, enabling them to incorporate it with other SOC tools
- **Latest threat intelligence:** Detailed attacker TTP data and daily threat updates give SOC teams the latest insight on threat landscapes without requiring expert interpretation
- **Unified visibility:** Combining BAS results with SOC tools maximizes team productivity for decision-making and prioritizing remediation or mitigation
- **Mitigation guidelines:** Teams receive guidance mapped to the MITRE ATT&CK™ framework for accelerating remediation of potential paths to crown jewel assets, together with professional mitigation guidelines written by the Cymulate Lab
- **Comprehensive coverage:** BAS challenges controls across all vectors, as well as the entire kill chain, for comprehensive coverage and visibility
- **Continuous automated testing:** Automation enables SOC teams to continuously challenge controls and immediately identify infrastructure changes or security gaps before they are exploited
- **Control optimization:** BAS testing repeatability provides consistent control assessment across the kill chain and ensures that mitigation efforts deliver the expected benefit

Cymulate

Cymulate's SaaS-based breach and attack simulation platform makes it simple to test, measure, and optimize the effectiveness of your security controls any time, all the time. With just a few clicks, Cymulate challenges your security controls by initiating thousands of attack simulations, showing you exactly where you're exposed and how to fix it—making security continuous, fast, and part of everyday activities.

Assessment results include objective, quantifiable exposure scores, as well as mitigation guidelines, making it easy to prioritize responses and communicate complex security concepts to stakeholders.

With Cymulate, you can surface new threats daily, defend against advanced stealth techniques, preempt adverse effects of continuous IT change, maximize team productivity, and ensure that security controls maximize protection against state-sponsored threat actors and complex supply-chain attacks.

About Cymulate

Cymulate helps companies stay one step ahead of cyberattackers with a unique breach and attack simulation service that empowers organizations with complex security solutions to safeguard their business-critical assets. By mimicking the myriad strategies hackers deploy, the system allows businesses to assess their true preparedness to handle cyber security threats effectively.

Cymulate is trusted by companies worldwide across industries, from small businesses to large enterprises. They share our vision—to make it easy for anyone to protect their company with the highest levels of security. Because the easier cybersecurity is, the more secure your company—and every company—will be.

Integrating with the Leaders:

RAPID7 IBM QRadar tenable

Vulnerability Scanners

Symantec. VirusTotal HYBRID ANALYSIS

Threat Intel Sources & Sharing

splunk> IBM QRadar SIEM

Analytics & SIEM

DEMISTO

SOAR Solutions

RSA

Enterprise Governance Risk and Compliance (eGRC)

Ready to Cymulate? Get started with a free trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: 31W 34th Street, 8th floor, New York, New York, 10001 | +1 212 6522632