securonix

SOLUTION BRIEF

Securonix Breach and Attack Simulations (BAS) Integration

Embed BAS to continuously test and measure the effectiveness of your threat detection and response program

Better Detection-Lifecycle Management

By integrating Breach and Attack Simulation solutions with Securonix Next-Gen SIEM and Open XDR, users can finally benefit from automated end-to-end security control validation built directly into their security monitoring architecture to support continuous, repeatable, and measurable detection lifecycle management.

BAS and Securonix Next-Gen SIEM work in concert to deliver a comprehensive development toolchain for purple teams, threat hunters, and detection engineers. Our combined solution allows you to design and develop new detection logic and analytics, and test and deploy them directly into production on the SIEM.

Why Securonix + BAS?

BAS solutions simulate the behavior of emerging and advanced cyber threat actors, allowing enterprises to validate the effectiveness of their security controls and identify gaps. Ultimately, this allows you to remediate threats before a real attacker can exploit them.

By simulating the latest attacks and adversaries as soon as intelligence about a new or existing threat emerges you can determine if an attack will be blocked or detected by your existing security controls. This ensures that your Next-Gen SIEM has sufficient visibility and is correctly configured for effective incident response and digital forensics.

Solution Benefits

Our joint solution lets you embed control validation into your detection and response programs and provides the following benefits:

Understand the Effectiveness of your Security Controls

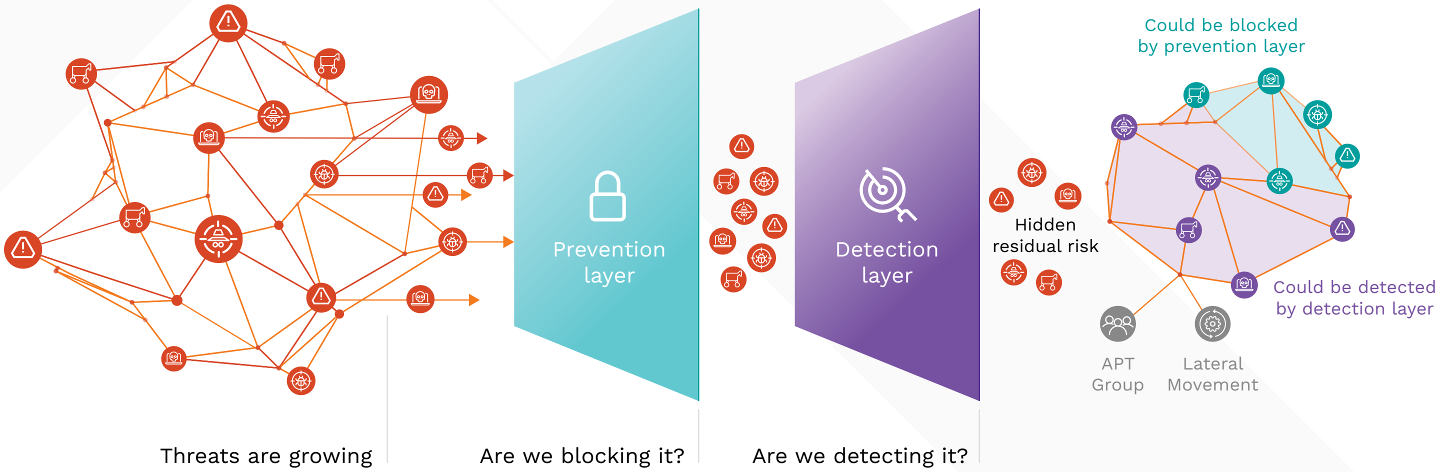
Rapidly assess your level of readiness against current and emerging cyber threats before an attack occurs. BAS allows you to validate the effectiveness of your security controls and detections across your environment and ensures you are capturing the right event data. This ensures sufficient visibility from sources such as web gateways, email gateways, firewalls, and more.

Automate Continous Security Validation

By automating the simulation of attacks before they occur, organizations can continuously test their defenses against the latest up-to-date adversary intelligence with low risk and effort. This enables threat hunters to build a proactive, threat-informed defense program.

Test New Circulating Threats Within your SIEM

Red-team exercises and penetration tests are periodic and only simulate a limited set of threat and attack scenarios. BAS solutions test and validate your SIEM in production continuously and in real-time based on the latest up-to-date and comprehensive threat intelligence. This ensures you always have sufficient coverage and reduces the window you are potentially left defenseless.



How it Works

BAS solutions typically deploy strategically positioned agents on different network segments and endpoints within your environment to send simulated threat traffic and activity to test endpoint or network your detection and response capabilities across your endpoints, network, web application firewalls, and more.

Security alerts and policy violations can then be reviewed to determine if potential attacks have been blocked or detected allowing gaps to be identified.

Integrating a BAS solution with Securonix Next-Gen SIEM allows organizations to:

- Ensure that relevant logs and events are being correctly and effectively collected.
- Evaluate findings from security events in Securonix against the simulation results to test and validate the detection and response actions taken across security controls and the security monitoring stack.
- Measure and quantify cyber resilience against cyberattacks through comprehensive risk scoring, and modeling against MITRE ATT&CK and adversary kill chains.

Securonix partners with reputable BAS vendors such as Picus, SnapAttack, and more.

5 Key BAS + Next-Gen SIEM Use Cases

Threat Hunters, SOC Managers, and Security Analysts alike benefit from a BAS integration with Next-Gen SIEM. Typical use cases for integrating your Securonix Next-Gen SIEM with a Breach and Attack Simulation tool include:

- Validating your logging coverage against diverse threats and attack techniques
- Optimizing your threat modeling
- Validating the effectiveness of your detection and incident response processes
- Improving data insights for threat hunters to build relevant hypotheses
- Reducing your mean-time-to-detect and respond to threats

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.
For more information visit securonix.com