Automate Breach Investigation and Remediation using Continuous Security Control Validation with SafeBreach and IBM Security™ QRadar® SIEM

IBM Security™ + SafeBreach

Joint Solution Brief

Organizations are failing at early breach detection despite owning a sprawling security stack. Preventive security tools often drift over time with their existing configurations no longer sufficient to protect against evolving attacks. Organizations rely on SIEMs to manage their threat detection and response, but security controls may not always provide contextual insights needed to comprehensively protect their crown jewels. Breach and Attack Simulation from SafeBreach shows organizations how their defenses will—and will not—protect against attacks by enabling the automatic execution of thousands of attacks (including the latest ones). This is done in a safe and continuous manner to validate and improve the effectiveness of an organization's security controls and reduce the attack surface. This also allows for SIEM detection rules to be optimally tuned by exposing it to real attack scenarios.

SafeBreach integrates with IBM Security™ QRadar® SIEM to provide an additional layer of detection and validation by automatically correlating simulated attacks with alerts and events from multiple sources, to grant real-time visibility into the effectiveness of those controls. Additionally, actionable insights provided by SafeBreach can help automate the process of breach investigation and remediation, making it more effective and efficient, allowing you to fix your security gaps faster.

Challenge

Organizations own and operate dozens of security tools, including a security information and event management (SIEM) tool to protect and defend their enterprise. SIEM tools help analysts automate the detection, prioritization, and remediation of critical events and threats within their environment. SIEMs aggregate and correlate alerts and events from multiple security controls to provide analysts with a comprehensive understanding of their organizational environment. However, given the constantly evolving threat landscape, there is a clear lack of visibility into the ability of security controls to detect, alert, or prevent newer attack TTPs. Misconfigured or drifted security controls may not correctly alert the SIEM against new attacks causing security teams to struggle with maintaining a hardened security posture. Additionally, SIEM detection rules may need to be optimized and tuned to ensure they are able to correctly detect real threats and breaches.

Use Case 1

Accurate visibility of security control performance

Challenge

The cyberthreat landscape is highly dynamic, while security controls are static. This impedes security teams from achieving a proactive security posture. Security teams struggle to bring visibility of which attacks, tactics, and techniques will bypass their security controls. SIEM tools can correlate alerts and events to notify analysts of critical threats, however drifting security controls can paint a false picture leading to missed threats. Threat intelligence is often used to prioritize alerts in SIEMs, but given the dynamic nature of the threat landscape, solely relying on threat intelligence to drive security decisions may not comprehensively protect your business against evolving threats. There is a need to continuously discover the security gaps in your organization (something not highlighted in your SIEM), remediate these gaps, and validate them against rapidly changing threats.

Solution

SafeBreach executes attacks from known threat groups, safely and continuously, to bring visibility into which controls prevented an attack and which attacks evaded security controls. The dedicated SafeBreach Labs team monitors the threat landscape for the changes in IOCs to ensure the SafeBreach Hacker's Playbook is safely executing attacks with the latest IOCs. By executing these attacks in real, production environments, SafeBreach can prove where security can withstand attacks—and where it needs to be improved. SafeBreach's integration with IBM QRadar provides security teams an additional layer of detection by automatically correlating simulated attacks with alerts and events from multiple security controls to provide real-time visibility into the effectiveness of those controls.

Use Case 2

Harden your defenses with automated remediation of identified security gaps

Challenge

To combat the threats posed by cyber attackers, security teams continually implement and enhance a range of security controls. However, given the dynamic threat landscape, security control configurations can quickly become obsolete and might need constant tweaking to ensure they are able to accurately detect, prevent, and mitigate advanced threats. Failure to do so can lead to attackers bypassing organizational defenses leading to massive business losses.

Solution

With SafeBreach, security teams can maximize the efficiency and effectiveness of the security controls by monitoring and validating their performance during an attack. This allows analysts to identify which solutions prevent, detect, or completely miss attack techniques. SafeBreach Insights allow teams critical information to identify and prioritize security gaps. These insights can be imported into IBM QRadar to trigger remedial workflows to update security control configurations. SafeBreach then closes the loop by running attacks to ensure that the updated configurations can successfully detect or prevent the attack. This continual security control validation ensures a hardened security posture that can withstand advanced attacks.

Use Case 3

Validate and improve efficacy of your security operations

Challenge

A SIEM collects, normalizes, and analyzes security data from all the security controls owned by the organization. This data is correlated using user-defined rules to discover trends, detect threats and investigate alerts. However, given the constantly evolving threat landscape, data reported back to the SIEM by misconfigured or drifted security controls may not accurately indicate the severity of the threat or provide enough contextual information to make accurate remedial decisions. This can lead to incorrect correlation of threat data, reducing the efficacy of the SOC team causing them to miss critical threats and delay remedial threat response.

Solution

SafeBreach continually validates your security controls to ensure their efficacy against evolving threats. Insights from these validations can be correlated with Security Events to ensure their accurate tracking in your IBM QRadar deployment, thereby measuring the efficacy of your security controls. SafeBreach insights also provide the security team with the necessary contextual data required to build new alerts for previously missed threats thereby improving your SIEMs detection accuracy while reducing your MTTD and MTTR.

Use Case 4

Security posture drift detection and correction

Challenge

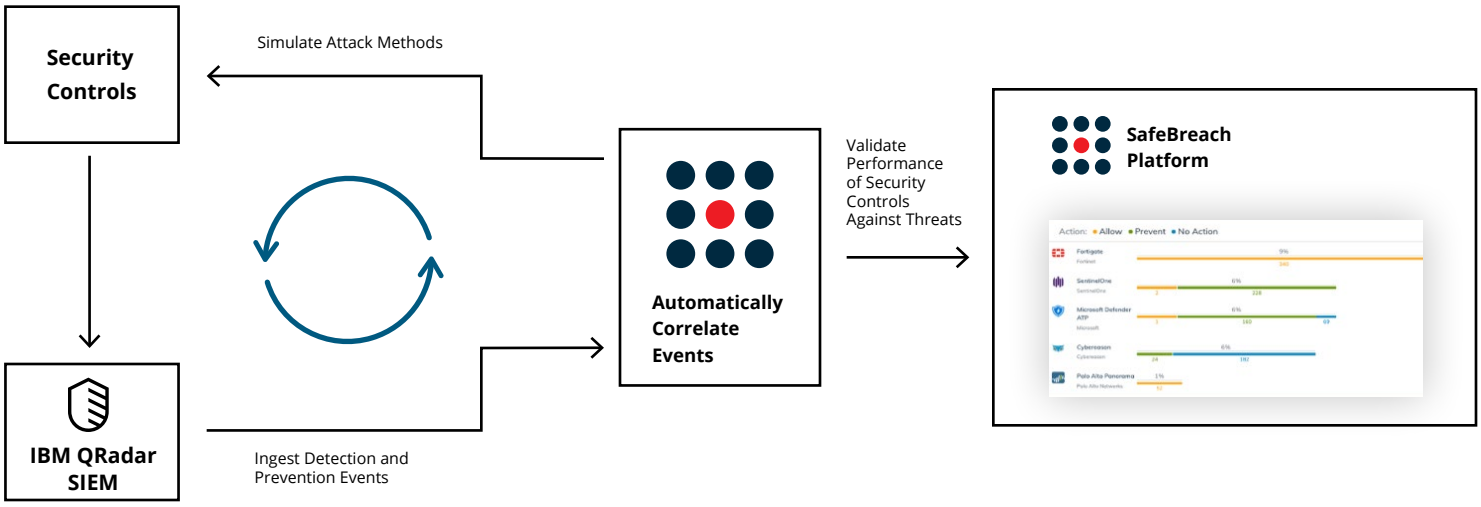
The fast-changing threat landscape requires security teams to continually tweak their security configurations to ensure that their security posture can withstand advanced evolving attacks. However, given the sprawl of security tools owned by organizations that is easier said than done. Hyper-vigilant security teams focus on stopping the next big attack while losing track of their baseline security posture. This can lead to vulnerabilities and backdoors that the threat actors can leverage to bypass your advanced defenses and wreak havoc.

Solution

Security teams often struggle to maintain their baseline security posture due to the evolving threat landscape. SafeBreach allows companies to safely test and validate their security controls against thousands of evolving attacks. These validation results can be used to define any changes to the baseline security posture and create alert rules that can reliably and dynamically identify posture drift in the future. This allows your security teams to always maintain a hardened security posture.

How the Integration Works

SafeBreach provides security teams with the utmost flexibility by supporting multiple deployment architectures. SafeBreach safely executes real attacks and then queries IBM QRadar security logs to determine if the impacted security controls had accurately triggered alerts and events. SafeBreach then automatically correlates the simulated attack with the SIEM results and detected actions. This allows SafeBreach to accurately determine if the integrated security control was able to detect or prevent an attack or the threat was simply able to bypass the security control. This additional context is available to security analysts via SafeBreach Insights which can be leveraged to appropriately update the security control to withstand such attacks in the future.



Value added by SafeBreach to IBM QRadar Customers

Continuously improve alerting accuracy and prevent drift in detection rules

Gain visibility into the effectiveness of your organizational security controls

Ensure rapid availability of correlated insights that speed up threat investigation and remediation

Benefits of the Integration – Together SafeBreach and QRadar SIEM:

- Provide unparalleled levels of visibility into security control performance and enterprise security posture
- Validate prevention and detection abilities of your existing security controls
- Detect which security controls were functional during an “attack” and what actions were taken by them by accurately tracking them in QRadar SIEM
- Automatically correlate simulation results and event logs to expose a comprehensive picture that covers both prevention and detection challenges
- Optimize SIEM detection rules and algorithms using real attack scenarios

SafeBreach

111 W. Evelyn Avenue Suite 117
Sunnyvale, CA 94086 408-743-5279
safebreach.com

About SafeBreach

SafeBreach is the world’s most widely used continuous security validation platform for enterprise companies. The company’s patented platform empowers CISOs and their teams to validate security controls, maximize their effectiveness, and drive down risk. SafeBreach provides a “hacker’s view” of an enterprise’s security posture by continuously validating security controls and presenting findings in customized dashboards to enable stakeholders to cleanly focus on the biggest risks to the organization. SafeBreach automatically and safely executes thousands of attack methods to validate network, endpoint, cloud, container and email security controls against its Hacker’s Playbook™, the world’s largest collection of attack data broken down by methods, tactics and threat actors. Data from SafeBreach validations can improve SOC team responses and inform management teams to make smarter decisions to better manage risk and invest resources.. SafeBreach is privately held and is headquartered in Sunnyvale, California with an office in Tel Aviv, Israel. **For more information, visit safebreach.com**