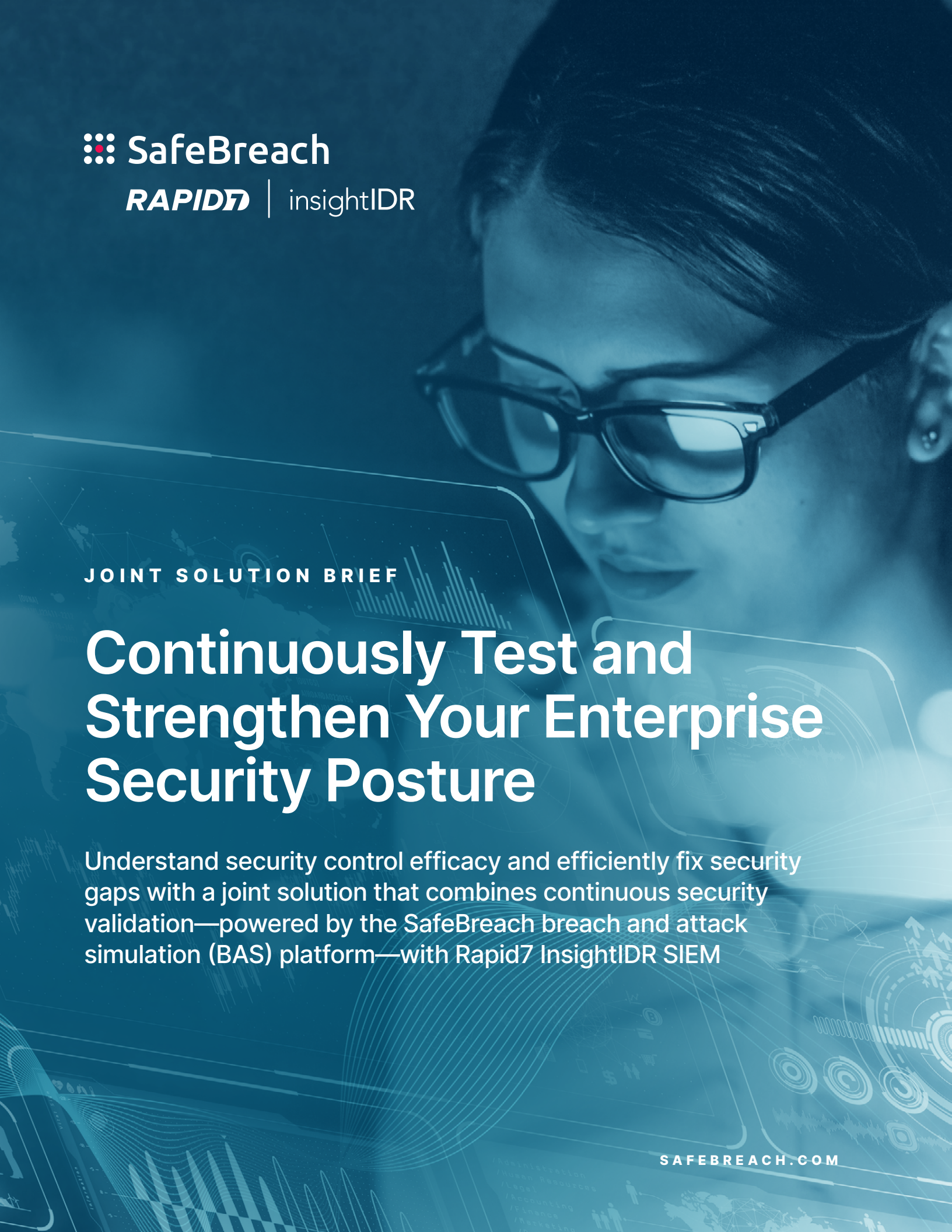


SafeBreach

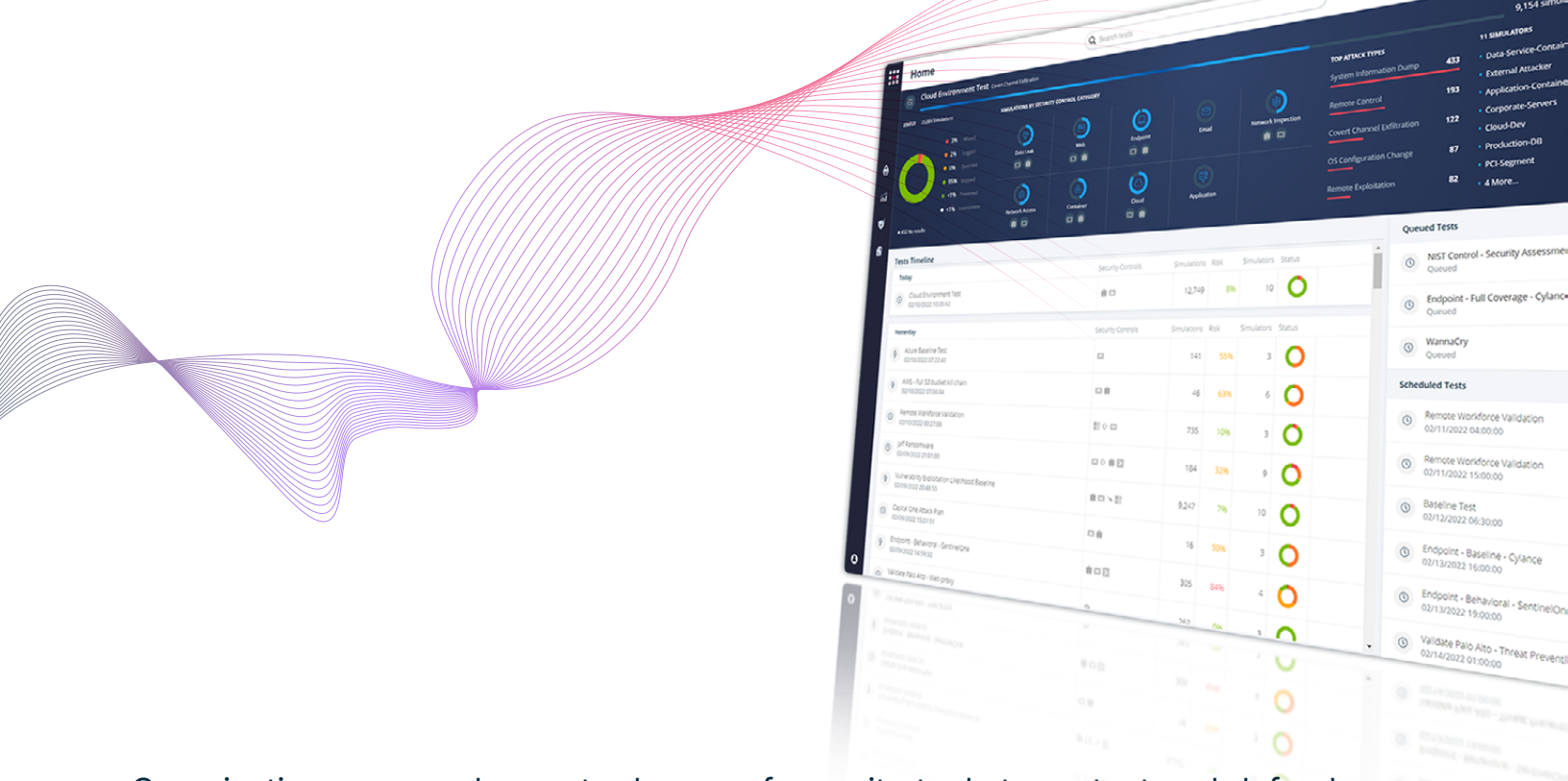
RAPID7 | insightIDR

JOINT SOLUTION BRIEF

Continuously Test and Strengthen Your Enterprise Security Posture

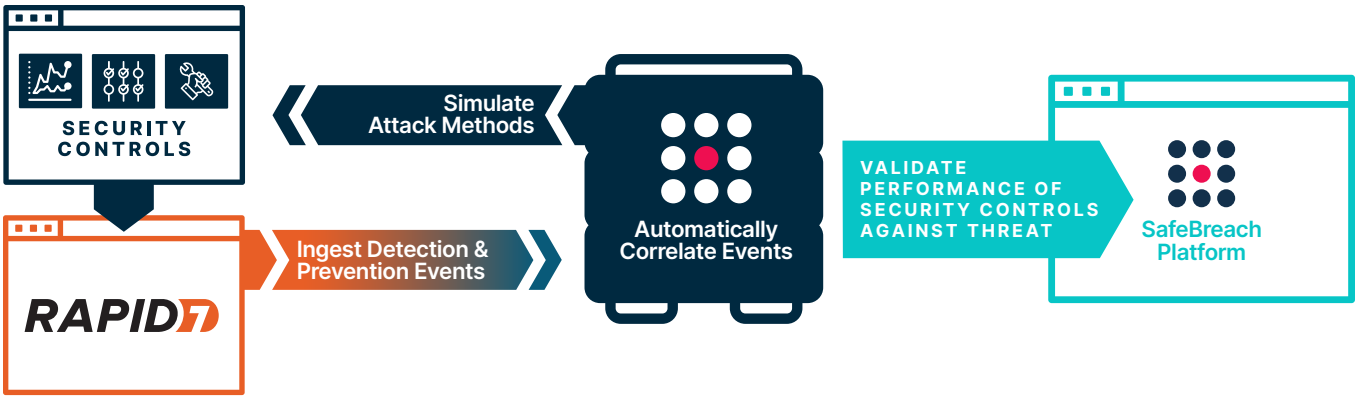
Understand security control efficacy and efficiently fix security gaps with a joint solution that combines continuous security validation—powered by the SafeBreach breach and attack simulation (BAS) platform—with Rapid7 InsightIDR SIEM

SAFEBREACH.COM



Organizations own and operate dozens of security tools to protect and defend their enterprise, including security information and event management (SIEM) technology. SIEMs aggregate alerts and events from multiple security controls (on-prem and cloud-based) to help analysts automate the detection, prioritization, and remediation of critical events and threats within their environment. However, given the continuously changing threat landscape, there is still a lack of visibility into the security controls' ability to detect, alert, or prevent newer attack tactics, techniques, and procedures (TTPs). This is especially true in the constantly evolving world of cloud TTPs, where 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.

The SafeBreach and Rapid7 joint solution helps organizations overcome these challenges by providing an additional layer of validation of various cloud, network, email, data loss protection (DLP), web filtering, container, and endpoint attacks. The offering automatically correlates thousands of simulated attacks from the SafeBreach BAS platform with the alerts and events received by Rapid7 InsightIDR SIEM from multiple connected security controls. This grants analysts real-time visibility into the effectiveness of the deployed security controls. Additionally, actionable insights provided by SafeBreach can help automate the process of breach investigation and remediation, enhancing the ability of security teams to effectively and efficiently fix security gaps.



How the Integration Works

SafeBreach provides security teams with the utmost flexibility by supporting multiple deployment architectures, including on-premises, cloud, and hybrid. SafeBreach safely executes real attacks against security controls and then queries Rapid7 InsightIDR SIEM's security logs to determine if the impacted security controls 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 the efficacy of the integrated security control and its ability to alert the SIEM of its actions. 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.

Benefits of the Integration – Together SafeBreach & Rapid7 InsightIDR SIEM:

- Provide unparalleled levels of visibility into security control performance, cloud readiness, and enterprise security posture
- Validate the prevention and detection abilities of existing controls, including network security, endpoint, email, DLP, web filtering, container, and cloud
- Detect which security controls were functional during a control and data-plane "attack" and what actions they took by accurately tracking them in the Rapid7 InsightIDR SIEM
- Automatically correlate simulation results and event logs to expose a comprehensive picture that covers both prevention and detection challenges

USE CASE 1

Accurate Visibility of Security Control Performance

Challenge

The cyber threat landscape is highly dynamic, while security controls are static. Security teams struggle to gain visibility into 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 that leads 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 in real production environments—to bring visibility into which controls prevented an attack and which attacks sailed past security controls. The dedicated SafeBreach Labs team monitors the threat landscape for changes in indicators of compromise (IOCs) to ensure the SafeBreach Hacker's Playbook is safely executing attacks with the latest IOCs. SafeBreach's integration with Rapid7 InsightIDR SIEM provides security teams an additional layer of validation by automatically correlating simulated attacks with alerts and events from multiple security controls to provide real-time visibility into the effectiveness of those controls. This helps improve the overall efficacy of security controls against rapidly evolving threats.

USE CASE 2

Harden Defenses with Automated Remediation of Identified 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 detect, prevent, and mitigate advanced threats accurately. 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 provide teams with critical information to identify and prioritize security gaps. These insights can be imported into Rapid7 InsightIDR SIEM to trigger remedial workflows that update security control configurations. SafeBreach then closes the loop by running attacks to ensure 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 & Improve the Efficacy of Security Operations

Challenge

A SIEM collects, normalizes, and analyzes security data from all the network security and cloud controls owned by the organization. Usually, this data is correlated using automated (vendor-provided) or 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 security operations center (SOC) team, and causing them to miss critical threats and delay remedial threat response.

Solution

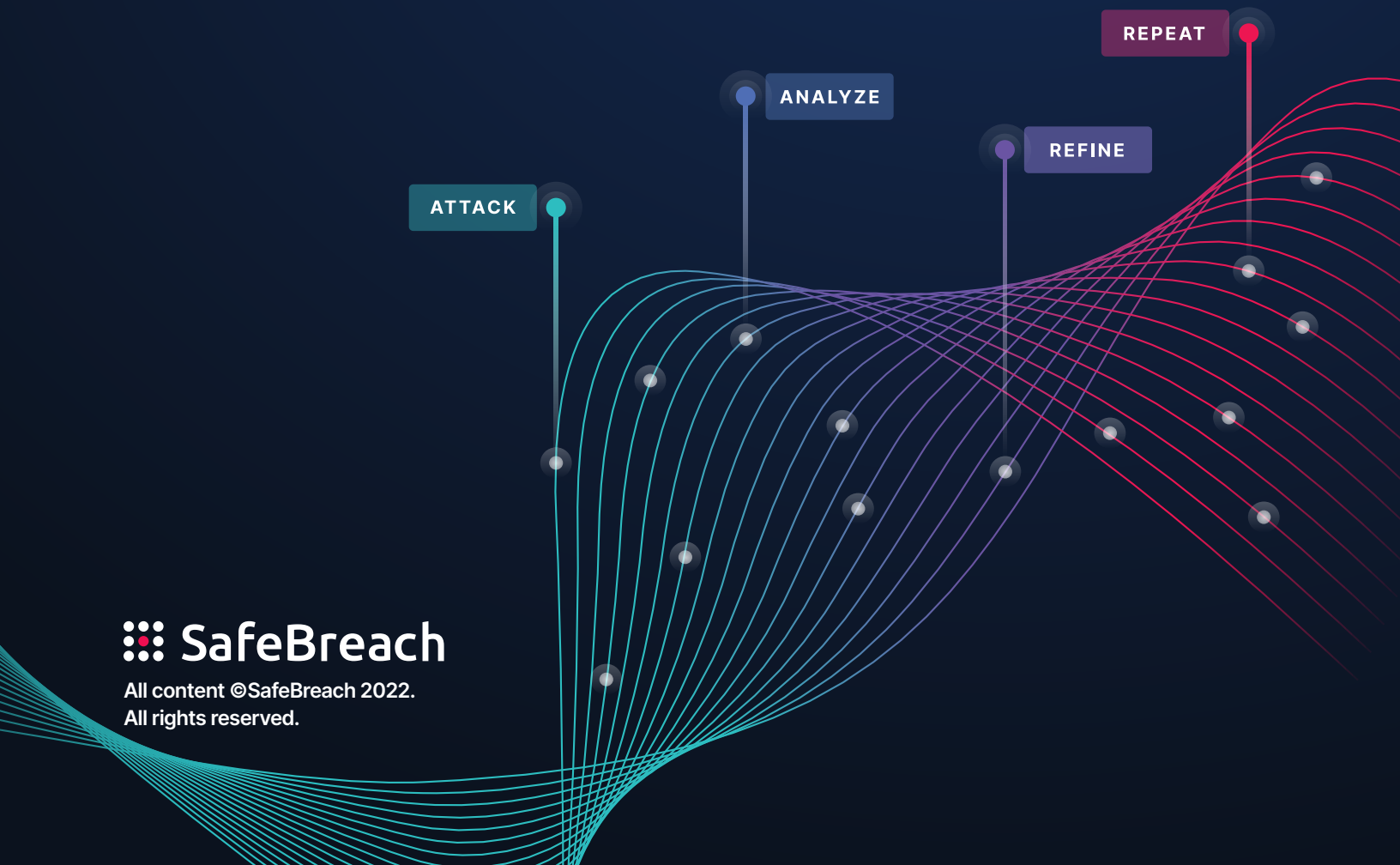
The SafeBreach platform continually validates security controls by running advanced attacks to ensure their efficacy against evolving threats. It then correlates validation results against events collected by Rapid7 InsightIDR SIEM to ensure a relevant alert was generated and communicated by the affected security control. This helps improve the overall efficacy of the SOC detection and remediation process. Additionally, SafeBreach Insights provide security teams with the necessary contextual data required to build new alerts for previously missed threats, thereby improving your SIEM's detection accuracy and reducing your mean time to detect (MTTD) and mean time to respond (MTTR).

About SafeBreach

Combining the mindset of a CISO and the toolset of a hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security validation platform. SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

About Rapid7

Rapid7 is advancing security with visibility, analytics, and automation delivered through its Insight cloud. Rapid7 solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. For more information, visit **www.rapid7.com**.



SafeBreach