SafeBreach
ANOMALI

JOINT SOLUTION BRIEF

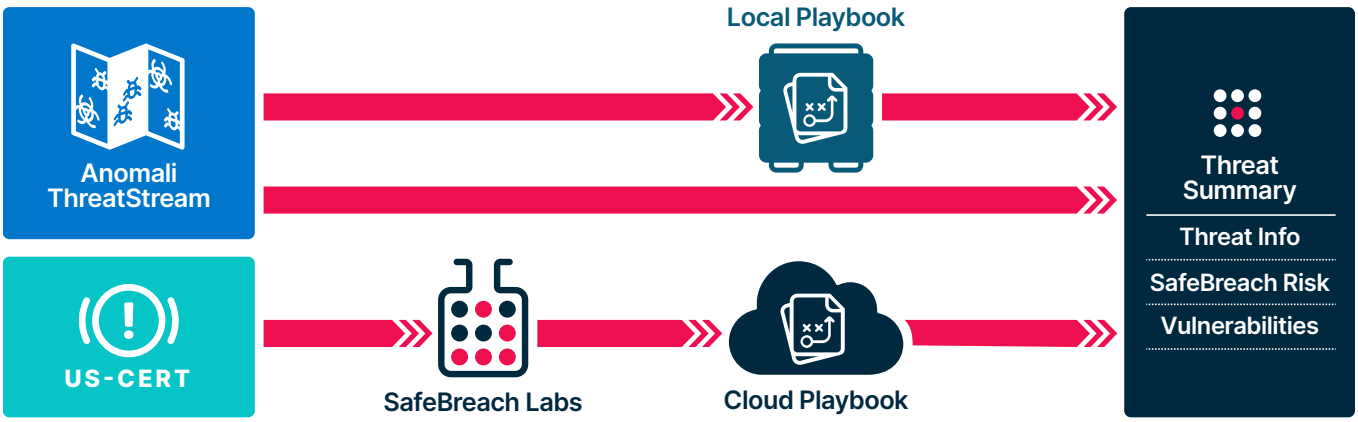
Contextualize Threat Intelligence with BAS: Continuously Validate Enterprise Security Posture Against Evolving Threats

Empower your security team with unparalleled visibility into the evolving threat landscape and the ability to optimize threat detection and response—powered by the SafeBreach breach and attack simulation (BAS) platform—with Anomali ThreatStream.

SAFEBREACH.COM

Security teams constantly engage in a complex battle to protect the organization against emerging threats delivered through novel tactics, techniques, and procedures (TTPs). Security teams seek timely and actionable threat intelligence to remain ahead of these threats and accelerate threat detection and response; however, each deployed security control may operationalize the information differently, potentially creating gaps or misconfigurations that attackers can exploit.

The joint solution from SafeBreach and Anomali assists security teams in protecting against advanced threats by providing complete visibility into the threat landscape and validating the effectiveness of deployed security controls. Combining continuous security validation from the SafeBreach breach and attack simulation platform with Anomali ThreatStream enables organizations to proactively test their defenses and improve their overall security posture.



How the Integration Works

SafeBreach integrates with Anomali ThreatStream to effortlessly assimilate contextual threat intelligence and correlate the ingested indicators of compromise (IOCs) with existing attacks detailed in our exhaustive Hacker's Playbook™. Additionally, security teams can use SafeBreach to construct customized attacks based on any IOCs and TTPs provided by Anomali that are applicable to their organization. This allows security teams to evaluate the effectiveness of their current security controls in light of the ever-changing threat landscape.

Benefits of the Integration

DISCOVER

Easily create new, customized attacks based on any specific IOCs and TTPs relevant to the organization provided by Anomali ThreatStream

PRIORITIZE

Prioritize SafeBreach simulation results based on their overall risk to the business

VALIDATE

Continuously validate and optimize organizational security control performance against the evolving threat landscape, leveraging TI provided by Anomali

USE CASE 1

Comprehensive Understanding of the Threat Landscape

Challenge

Threat intelligence can be a valuable asset for security teams, providing them with an understanding of the global threat landscape and enabling them to defend their organization against advanced threats. However, operationalizing threat intelligence can be challenging. Not all security teams possess the necessary expertise and capabilities to contextualize and integrate threat intelligence with existing security controls. Moreover, without the specialized capabilities provided by a qualified analyst and/or a specialized threat intelligence platform, it is difficult to gain insights into attacker intent and assess the impact of particular threats on the organizational security posture.

Solution

By providing actionable, customizable threat intelligence, Anomali enables organizations of all sizes to remain ahead of sophisticated attacks and protect their businesses. SafeBreach integrates with Anomali ThreatStream in order to rapidly correlate IOCs with existing attacks from our market-leading Hacker's Playbook™. In addition, SafeBreach makes it simple for security teams to construct new, customized attack simulations based on any relevant IOCs or TTPs related to the organization, allowing them to understand and enhance the performance of security controls against evolving threats.

USE CASE 2

Validate and Improve the Efficacy of Your Security Operations

Challenge

Security operations center (SOC) teams engage in a never-ending battle to defend their enterprise from adversary tactics that are constantly evolving. For the SOC to make informed decisions regarding detection, prioritization, and remediation, contextual threat intelligence is required. Due to the dynamic nature of the threat landscape, numerous IOCs may be ineffectively ingested by a variety of security controls. By prioritizing threats that require immediate attention, threat intelligence enhances the effectiveness of threat detection and response. However, not all threat intelligence sources are created equal; intelligence that is not properly operationalized has limited value and can even increase a security analyst's workload, leading to overburdened security teams and increased organizational vulnerability.

Solution

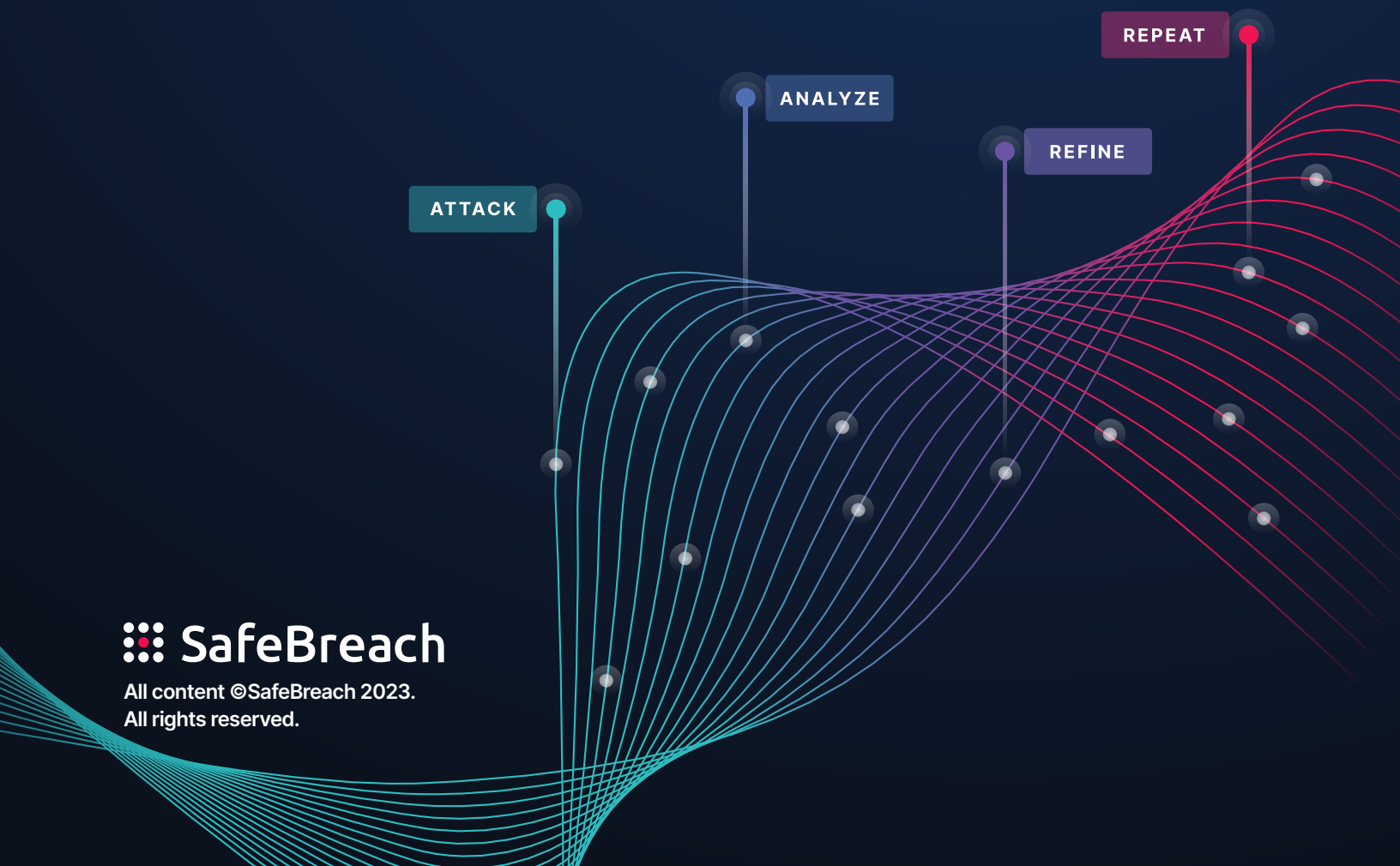
Security teams can utilize more than 25,000 built-in attacks from the SafeBreach Hacker's Playbook as well as custom attacks created using Anomali ThreatStream's contextual threat Intelligence to continuously validate the effectiveness of their deployed security controls against evolving threats. These validation results can be used to identify any changes to the baseline organizational security posture and to generate alert rules that can identify posture drift in the future in a reliable and dynamic manner. This enables your security teams to expedite threat detection, prioritization, and response and can strengthen your organizational security posture.

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 Anomali

Anomali is the leader in modernizing security operations with the power of analytics, intelligence, automation, and AI to deliver breakthrough levels of visibility, threat detection and response, and cyber exposure management. Anomali helps customers and partners transform their SOC by elevating security efficacy and reducing their costs with automated processes at the heart of everything. Founded in 2013, Anomali serves global B2B enterprise businesses, large public sector organizations, ISACs, ISAOs, service providers, and Global 1000 customers to help safeguard the world's critical infrastructure, companies, and people. Learn more at **anomali.com.**



SafeBreach