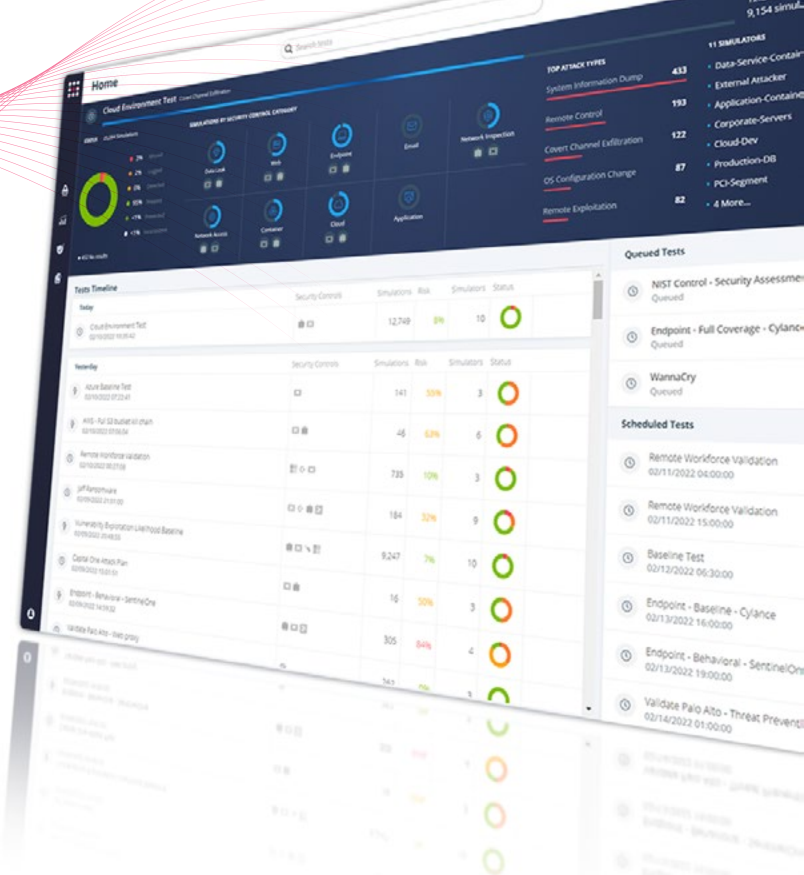
SafeBreach

TREND MICRO

JOINT SOLUTION BRIEF

Continuously Optimize Your Trend Micro™ Vision One XDR Performance to Improve Detection and Response Times

Empower your security operations against constantly evolving network and endpoint threats with a joint solution that combines continuous security validation—powered by the SafeBreach breach and attack simulation (BAS) platform—with Trend Micro™ Vision One XDR.



TOP ATTACK TYPES

System Information Dump	433
Remote Control	193
Covert Channel Exfiltration	122
OS Configuration Change	87
Remote Exploitation	82

11 SIMULATORS

- Data-Service-Contai
- External Attacker
- Application-Containe
- Corporate-Servers
- Cloud-Dev
- Production-DB
- PCI-Segment
- 4 More...

Queued Tests

NIST Control - Security Assessme
Queued

Endpoint - Full Coverage - Cylanc
Queued

WannaCry
Queued

Scheduled Tests

Remote Workforce Validation
02/11/2022 04:00:00

Remote Workforce Validation
02/11/2022 15:00:00

Baseline Test
02/12/2022 06:30:00

Endpoint - Baseline - Cylance
02/13/2022 16:00:00

Endpoint - Behavioral - SentinelOn
02/13/2022 19:00:00

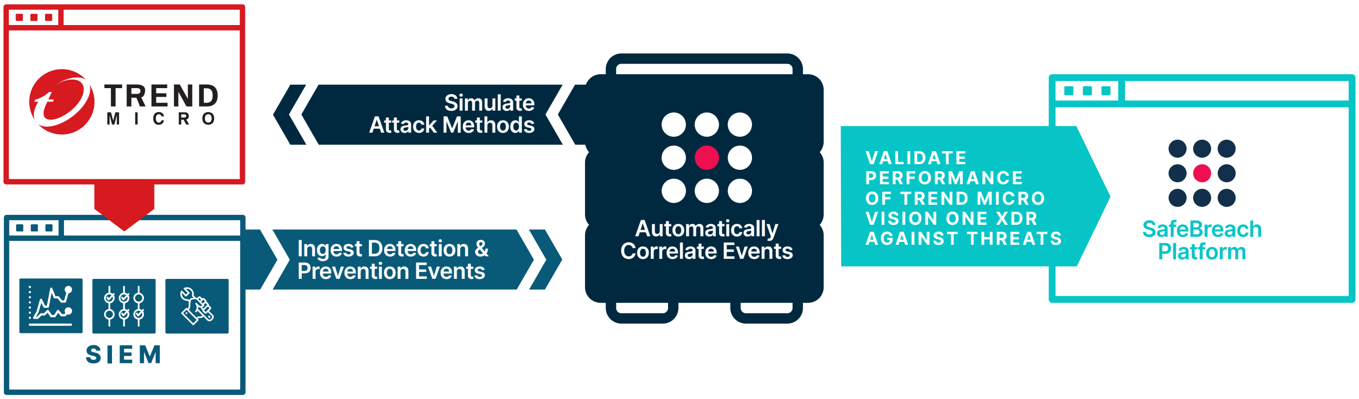
Validate Palo Alto - Threat Prevent
02/14/2022 01:00:00

Security operations teams are finding it increasingly difficult to maintain a hardened posture against the evolving threat landscape. Threat actors continually adapt their methods to evade traditional perimeter security solutions, and the increased complexity of the security stack can inhibit visibility into the performance of security controls. One small control misconfiguration can create a security gap that attackers can easily exploit.

The SafeBreach and Trend Micro joint solution helps security organizations combat these challenges by effectively validating and optimizing the performance of Trend Micro's Vision One XDR platform. The offering combines continuous security validation—powered by the SafeBreach breach and attack simulation (BAS) platform—with Trend Micro Vision One, a comprehensive extended detection and response (XDR) platform offering detection, response, and protection workflow automation. Together, SafeBreach and Trend Micro Vision One XDR empower security teams to proactively test their defenses against advanced attacks to continuously validate security controls, identify gaps, and take remedial action.

SafeBreach

FOR MORE INFORMATION OR TO REQUEST A DEMO, VISIT: **SAFEBREACH.COM**


TREND MICRO
SIEM
Simulate Attack Methods
Ingest Detection & Prevention Events
Automatically Correlate Events
VALIDATE PERFORMANCE OF TREND MICRO VISION ONE XDR AGAINST THREATS
SafeBreach Platform

How the Integration Works

SafeBreach safely executes various advanced attacks that trigger Vision One XDR's detection and prevention capabilities. The SafeBreach platform then continuously fetches and correlates security events and alerts from Vision One or through the connected security information and event management (SIEM) platform to determine if the Vision One XDR platform was able to detect or block the threat and ensure appropriate alerts are configured. This context (including the results of simulated attacks and associated remediation information) is available to security analysts to appropriately update the Vision One XDR configuration to detect and prevent such attacks in the future.

Benefits of the Integration

Provides unparalleled visibility into Vision One XDR performance and enterprise security posture

Enables continuous improvement of alerting accuracy and prevents drift in detection rules

Optimizes prevention and detection abilities of Vision One XDR against advanced endpoint and network threats

Automatically correlates simulation results and SIEM event logs to simplify and expedite threat investigation, analysis, and remediation

USE CASE 1

Validate Vision One XDR Configurations & Policies

Challenge

Hackers continuously modify indicators of compromise (IOC) such as hashes, IPs, and domains, while security teams struggle to keep up and ensure all controls are configured to block the IOCs. To maintain pace with the latest threats, teams need to update security control configurations on a regular basis, but they are hindered by uncertainty over whether updates could potentially open security gaps in their existing defenses. The lack of visibility into the performance of security controls leaves security teams unsure which IOCs will be blocked and prevented from enabling devastating attacks, and which continue to pose a danger by infiltrating the network.

Solution

The dedicated SafeBreach Labs team monitors the threat landscape 24/7 to ensure the SafeBreach Hacker's Playbook includes coverage for the latest IOCs and tactics, techniques, and procedures (TTPs). The SafeBreach platform then uses this coverage to validate an organization's security posture by safely and continuously executing advanced attacks to provide visibility into which controls prevented, detected, or missed an attack. The integration with Trend Micro Vision One XDR tests advanced attacks against the XDR platform to validate which threats and associated IOCs were blocked. When IOCs are missed, SafeBreach Insights provides security teams with raw IOC data that can be used to optimize Vision One XDR's threat detection.

USE CASE 2

Improve Efficacy of Security Operations Against Advanced Threats

Challenge

Security teams analyze and process network and endpoint alerts collected in a SIEM system. This data is often correlated using user-defined rules to discover trends, detect threats, and investigate alerts across network and cloud deployments. However, data reported back to the SIEM by misconfigured security controls may not accurately indicate the severity of the network/endpoint threat or provide enough contextual information to make accurate remedial decisions. This frequently leads to an incorrect correlation of threat data, reducing the efficacy of the security operations center (SOC) team and causing them to miss critical threats that delay remedial threat response.

Solution

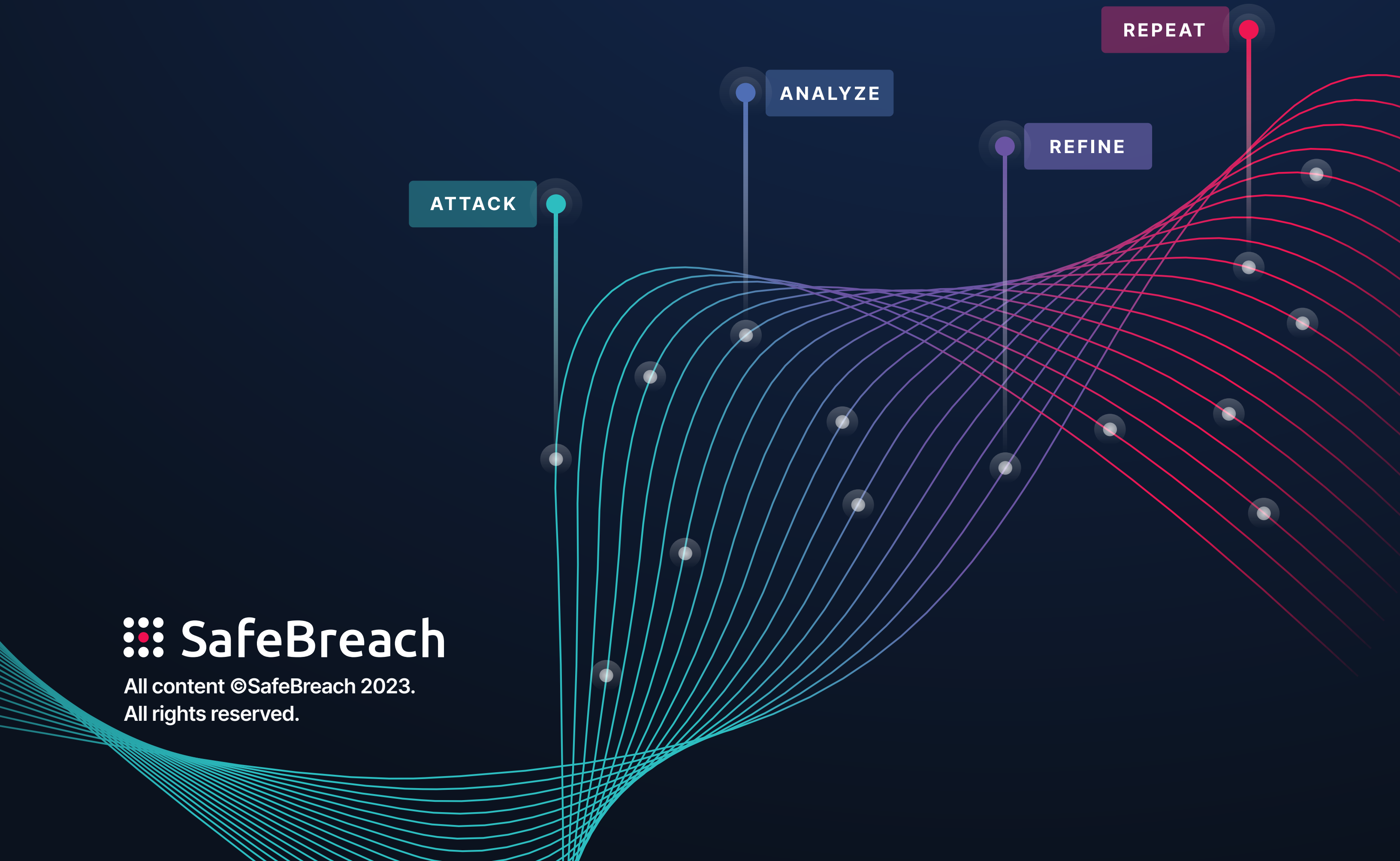
SafeBreach continually validates Trend Micro Vision One XDR to ensure its efficacy against evolving endpoint and network threats. Insights from this validation can be correlated with corresponding SIEM alerts/events to ensure they are accurately tracked in a SIEM, thereby measuring the efficacy of the Vision One XDR control. SafeBreach Insights also provide security teams with the necessary contextual data required to build new alerts for previously missed network/cloud threats, thereby improving the detection accuracy of Vision One XDR and reducing the mean time to detect and respond.

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 Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our cybersecurity platform protects 500,000+ organizations and 250+ million individuals across clouds, networks, devices, and endpoints. For more information, please visit **www.trendmicro.com.**



SafeBreach

All content ©SafeBreach 2023.
All rights reserved.