Staying Ahead of Attacks with Automation

Joint Solution Brief

SafeBreach + paloalto NETWORKS | CORTEX XSOAR BY PALO ALTO NETWORKS

To be proactive and fully prepared for cyber-attacks today, security teams must accurately understand the true effectiveness of countless security controls, security processes, and alerting. Breach and Attack Simulation (BAS) from SafeBreach shows organizations how well their defenses will protect—or not—against adversary attacks, so they can prioritize security efforts and make the most of their investments in security.

The integration of SafeBreach with Cortex XSOAR enables an effective closed-loop security solution. SafeBreach continuously simulates attacks against your network, endpoint, and cloud infrastructure using thousands of breach and attack methods contained in the SafeBreach Hacker's Playbook™. When the simulated attacks are missed, remediation of your security controls is required to ensure hackers cannot exploit vulnerabilities.

Remediation data is streamed to Palo Alto Networks Cortex XSOAR to automate the necessary changes across the enterprise environment—to identify and remediate defensive weaknesses before they are exploited by attackers.

Challenge

Security teams receive numerous indicators of compromise (IOC), such as hashes, domains and IP addresses, as well as behavioral indicators of compromise (BIOCs), such as the execution of suspicious host action usage of non-standard port and protocol exposures, which help prevent devastating brute force attacks. Both IOCs and BIOCs come from a host of security tools, but with a limited view of which indicators will actually compromise your enterprise. Your security team spends an excessive amount of cycles to gather all the various indicators, investigate to identify duplicates, research, prioritize, and approve updates to endpoint and network security configurations.

Use Case 1 - Automate Remediation of Non-Behavioral Indicators That Breach Your Enterprise

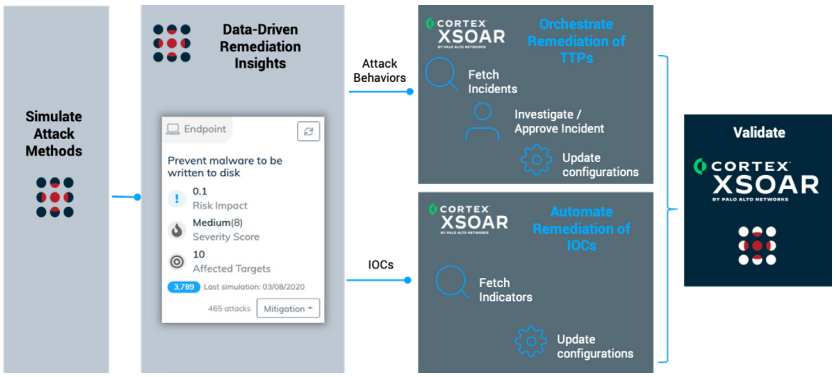
Solution

SafeBreach continuously tests your security defenses to determine which attacks will impact your enterprise, and supplies validated indicators to show where security defenses failed. Cortex XSOAR fetches the non-behavioral IOCs from SafeBreach that were missed by your security controls. The integration of SafeBreach with Cortex XSOAR for automated Data Enrichment and response automates the remediation steps to update your endpoint and network security controls. This unburdens your analysts, freeing them from low-level tasks so they can focus their attention on decision-making security improvements.

Use Case 2 - Orchestrate Remediation of Behavioral Indicators That Breached Your Enterprise

Solution

SafeBreach uncovers behavioral indicators of compromise (BIOCs) that are proven through simulated attacks to bypass your security controls. Non-behavioral IOCs are pulled into Cortex XSOAR for a closed-loop fully automated process so your analysts can focus their attention on the critical behavioral indicators (BIOCs) that need to be addressed. The Cortex XSOAR MarketPlace integration of SafeBreach Insight proves added value by correlating numerous BIOCs (e.g. exposed non-standard ports and protocols used for brute force attacks) for your security team to orchestrate investigation and approval of configuration updates. Cortex XSOAR will trigger the attacks to run again in SafeBreach to validate your security defenses are up-to-date. This enables quick, effective remediation to improve the organization's security posture and reduce business risk.



Automation of IOCs and orchestrate BIOCs with SafeBreach and Palo Alto Networks Cortex XSOAR (Demisto).

Use Case 3 - Orchestrate and Automate High-Priority Attack Methods That Bypassed Your Security Controls

Challenge

Security teams struggle to obtain visibility of which attacks, tactics, and techniques will succeed in bypassing their security controls. Because many vulnerabilities are detected, it is very challenging to remediate them through a manual process of investigation and updating numerous security controls. The focus has shifted to map to the MITRE ATT&CK framework, as this gives a useful, organized, and readily understood view of the overall security posture. Importantly, it highlights critical areas of exposure where remediation efforts should be focused to harden enterprise defenses more strategically and efficiently.

Solution

By running breach and attack simulations, SafeBreach helps security analysts identify high- priority weaknesses in their security defenses. The data-driven simulation results are mapped to the MITRE ATT&CK framework, validating the efficacy of your endpoint, network, email, and cloud security controls. The integration with Cortex XSOAR enables security analysts to push high-priority exposures, from an interactive MITRE ATT&CK framework heat map, to be orchestrated for remediation of your endpoint and network controls. Simulations are rerun to validate that hardening of your defenses was successful.

Streamline security configuration remediation and validation using Palo Alto Networks Cortex XSOAR (Demisto).

Benefits

- Discover security gaps with continuous breach & attack simulations.
- Reduce dwell time of attack simulations that have been validated to breach your environment.
- Unburden your security analysts by fully automating the remediation of low-level non-behavioral IOCs.
- Orchestrate remediation of behavioral IOCs for endpoint and network security controls.
- Maximize the effectiveness of your existing security controls.

SafeBreach

About SafeBreach

SafeBreach simulates thousands of attack methods to provide a hacker's view of an organization's security posture, paint a picture of the security exposures to an enterprise and prioritize remediation, securing against TTPs. SafeBreach Labs is dedicated to threat research from real-world investigation with the most extensive breach and attack methods in the industry with over 10,000 attack methods and growing. SafeBreach is privately held and is headquartered in Sunnyvale, California with an office in Tel Aviv, Israel.

For more information, visit www.safebreach.com.

paloalto NETWORKS | CORTEX XSOAR BY PALO ALTO NETWORKS

About Cortex XSOAR

Cortex XSOAR, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity.

For more information, visit www.paloaltonetworks.com/cortex/xsoar