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 from SafeBreach shows organizations how well their defenses will protect—or not—against attacks, so they can prioritize security efforts and make the most of their investments in security.

The integration of SafeBreach with Cortex XSOAR enables a 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 attacks are not blocked by security controls, 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 changes necessary across the enterprise environment—to identify and remediate defensive weaknesses before they are exploited by attackers.

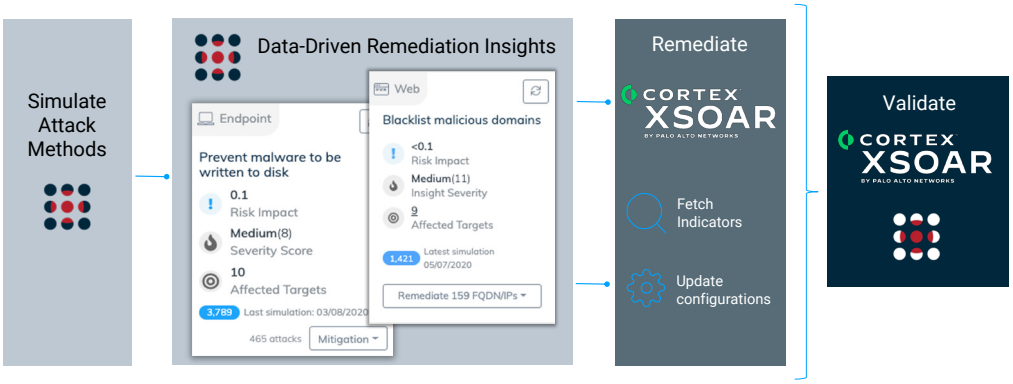
Use Case 1 — Automate Response of Indicators That Breach Your Enterprise

Challenge

Security teams receive numerous indicators of compromise (IOC) from a host of security tools, with limited view of which indicators will 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, network security configurations.

Solution

SafeBreach continuously tests your security defenses to determine which attacks will impact your enterprise, and supplies validated indicators to show which security defenses failed. The integration with SafeBreach allows Palo Alto Networks Cortex XSOAR to fetch IOCs from SafeBreach that identify the attacks which went unblocked by your security controls. From there, Cortex XSOAR Threat Intelligence helps security teams orchestrate and automate their mitigation actions, from investigation to approval and validation of endpoint and network security control updates, in a closed loop process.



Closed-Loop Automated Breach Remediation with SafeBreach and Palo Alto Networks Cortex XSOAR (Demisto) type.

Closed-Loop Automated Breach Remediation

Discover security gaps with continuous breach simulation

Remediate and validate missed IOCs automatically

Maximize the value of your existing security controls

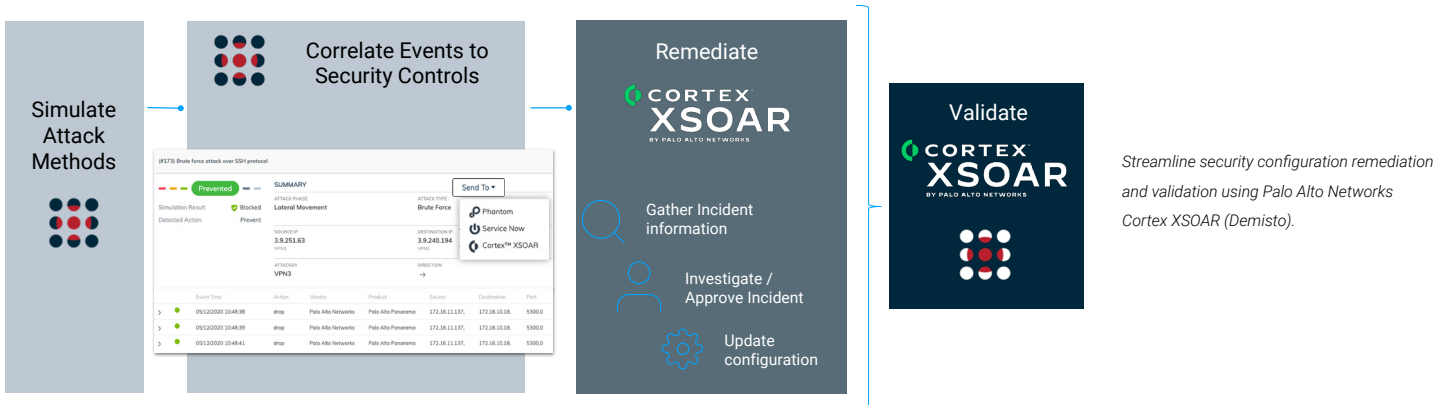
Use Case 2 — Automate Endpoint and Network Security Control Validation

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 of numerous security controls. The focus of CISOs is shifting to map to the MITRE ATT&CK framework, because this gives a useful, organized, and readily understood view of their security posture. Importantly, it highlights where remediation efforts should be focused to harden enterprise defenses. Mapping exposures to ATT&CK generates a large amount of data to analyze for remediation. The security team must also track the shifting landscape of security controls and the impact of policies that could open up new attack paths.

Solution

SafeBreach continuously runs breach and attack simulations to validate that your security controls have the correct indicators needed to block known attacks. SafeBreach automatically maps the simulation results to MITRE ATT&CK framework for a well-organized and consistent view of which specific attack techniques expose the enterprise to devastating cyber-attacks. The integration with Cortex XSOAR removes a significant burden from your security team by automating the mitigation of security gaps that enables successful breaches. Security analysts can easily identify the techniques that pose a real threat, and can trigger Cortex XSOAR, from the SafeBreach Platform, to generate a playbook for updating your endpoint, network and SIEM controls. Then, rerun the simulations to close the validation loop, ensuring that the controls in place are up to date.



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

Benefits

- With the deep integration of SafeBreach and Cortex XSOAR, analysts can simulate attacks, identify and remediate security weaknesses, and ensure that fixes work as intended, all in a closed-loop process.
- SafeBreach integrated with Threat Intel Management of Cortex XSOAR, orchestrates the mitigation efforts to block known attack methods which SafeBreach shows could be successful.
- Reduce dwell time of attack methods that have been validated to breach your environment.
- Orchestrate endpoint and network security control mitigation of weak points—that are revealed by IOCs—with a SafeBreach Cortex XSOAR playbook.

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 Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloudcentric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the fore-front of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

Learn more: www.paloaltonetworks.com