Validate your Palo Alto Networks Security Controls with SafeBreach

Joint Solution Brief

Security Operations teams understand how critical it is to maintain the effectiveness of their network security controls, in large part because configuration and policy drift can occur at any time. Most security teams lack the tools to accurately and continuously test and visualize their security posture. SafeBreach provides continuous validation of security controls and rapid remediation for Palo Alto Networks Panorama.

The integration of SafeBreach, the leading Breach and

Attack Simulation (BAS) solution, and Palo Alto Networks® Security Operating Platform, which prevents successful cyberattacks through intelligent automation, enables security professionals to simulate attack methods against their deployed network security controls. The simulation results are correlated and enriched with network-related security data. This continuously validates an organization's security posture against cyber-attacks and automates the combined processes of breach investigation, remediation, and prevention.

Use Case #1

Validate next-gen firewall configurations and policies are set to best protect your enterprise:

SafeBreach's patented simulation technology and the most comprehensive Hacker's Playbook in the industry allows you to continually and safely test and report on the readiness of network infrastructure against real-life cyber attacks. You can simulate attack methods by threat groups, TTPs, specific malware or create your own attack method. The capability to visually display attack paths and security gaps makes it faster and easier to analyze, prioritize and continuously improve your network security posture.

SafeBreach enables security teams to:

- automatically correlate simulation results against Panorama to quickly identify
- any configuration or policy gaps
- analyze which attack methods were stopped, prevented, detected or missed
- identify network paths to quickly highlight where data can be exfiltrated from the
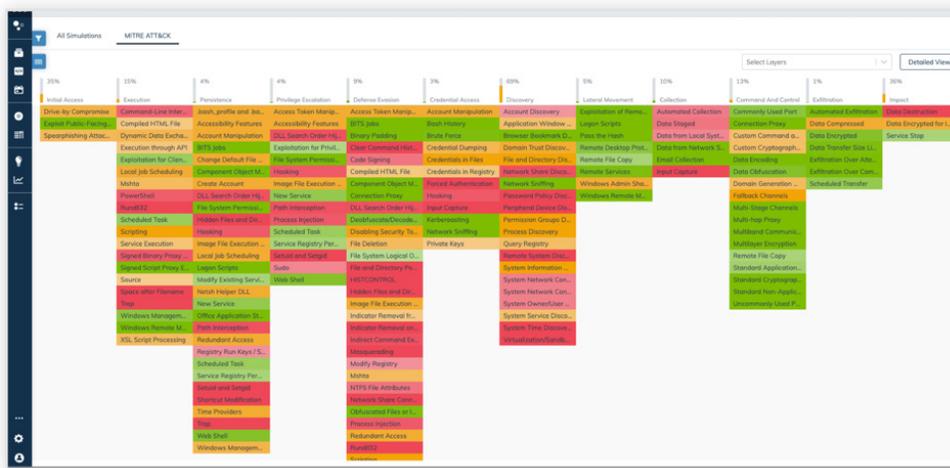
SafeBreach MITRE ATT&CK heat map simulation results based on threat group, tactics and techniques or specific malware type.

Breach and Attack Simulation

For Security Control Validation

Simulate attacks to
test your defenses

Visualize your
security posture with
data-driven results

Remediate holistically to
defend your enterprose

Use Case #2

Easily prioritize and remediate all vulnerabilities and issues that are identified by simulated attacks.

SafeBreach mitigation insights for network access and network inspection security controls and configurations can be shared with Palo Alto Networks Panorama. As a result, security and network teams can holistically and effectively remediate the organization's critical exposures. Users can resolve numerous simulations simultaneously, using detailed mitigation data collected from Palo Alto Networks Panorama.

Key Benefits

1. Validate that Palo Alto Networks Panorama security controls are deployed correctly and configured optimally, ensuring protection against known threats.

2. Reduce the time to detect, prevent, and respond to attacks.

3. Reduce overall attack surface by optimizing Palo Alto Networks Panorama security controls based on real-life attack scenarios