

# The Power of Testing Your Security Controls Against the Latest Threats



Because cyber threats are ever-shifting, security teams and security solutions have evolved to keep up and elevate their security stance to be more proactive. Threat Intelligence solutions are essential to keep organizations informed and up to date, but there is a gap between awareness and action. Threat Intelligence answers the question **“what threats in the wild should you be concerned with?”** but lacks the capability to address **“how will the latest threats impact the business?”**

SafeBreach, by combining breach and attack simulation with a threat intelligence solution delivers visibility into your security posture against specific threats that concern you the most. It does this quickly and effectively by exposing how your security controls will stand up to the attack to answer, **“how will the threat impact the business?”** Not only is the potential impact of the attack defined, but SafeBreach also tells you how to correct your security controls to reduce the risk of the attack.

## How does it work?

SafeBreach has an extensive set of attack methods across the full kill chain that are known to be used again and again once a hacker has infiltrated your network. SafeBreach Lab is a dedicated team of researchers that continuously update the SafeBreach Hacker’s Playbook™ with new attack scenarios, with an SLA for 48-hours for US-CERT Alert announcements. Integrating your threat intelligence solution with the SafeBreach platform means that queried active threats will be pushed in real-time to SafeBreach, where threats are correlated with the current breach and attack methods in the SafeBreach Hacker’s Playbook. New attack techniques are automatically made safe and built into the playbook. The combined set of existing and new attacks will be run across your infrastructure to expose how your security controls are working—or not working—to prevent, detect and alert your teams of the latest attacks used in the wild.





You will gain detailed insight into how well your security solutions (network, endpoint, SIEM, cloud, containers, DLP) are working together to define your security posture against the specific threat group. In addition, the solution will generate a remediation plan to close up security exposures to ensure you don't fall victim to the attack.

## Benefits:

**Obtain a strategic cybersecurity posture to effectively identify and mitigate risk to the business.**

- Ingest the latest threats that are relevant to your organization to SafeBreach.
- Correlate the latest threats to SafeBreach Hacker's Playbook™ of attacks and automatically build new attacks based on the threat feed.
- Simulate the attacks against your endpoint, network, SIEM, cloud, container, email and DLP solutions.
- Identify the security controls that are defending your enterprise, as well as those which need updates to properly identify and defend against the attack.
- Unburden your analysts by automating the remediation of the low-level or technical indicators, such as hashes, IP addresses, and domain names.
- Correlate the simulation results with your vulnerability scans to effectively prioritize the vulnerabilities at risk of exposure for the attack.
- Help your infrastructure team execute patch management, based on vulnerabilities that are prioritized because they are actually exploitable.
- Focus the attention of your security analysts to orchestrate on the remediation of behavioral indicators/TTPs that your security controls did not detect.
- Re-run the threat simulations after remediation to ensure that your security controls and your teams are positioned effectively to confront the potential attack.
- Strategically report on the impact of the attack to properly scope the potential risk to the business.
- Continuously test to ensure configuration changes have not opened an exposure in your organization.

Copyright © SafeBreach Inc. 2020

**SafeBreach**

111 W. Evelyn Avenue Suite 117  
Sunnyvale, CA 94086 408-743-5279  
safebreach.com

Learn how your team can answer  
"How will the latest threats impact the business?"

**Request a Demo**

[Here](#)