ATTACKIQ

Breach and Attack Simulation Use Case

Security Control Technology Validation

Security Control Technology Validation

Security control technology validation measures security control efficacy based upon the expected technical capabilities of the security control. Security control technology validation starts with the technology — not the threat. It provides a technology-centric approach to validating that specific controls deliver the expected protection capabilities as configured and as expected and that they are optimized for your production environment.

Deploying the AttackIQ Security Optimization Platform and leveraging the MITRE ATT&CK® framework enables cybersecurity operations teams to test the security controls against specific selected tactics, techniques, and procedures (TTPs) within the MITRE ATT&CK framework to understand their security postures and exposure against relevant adversaries.

Case Study Industry: Communications

A leading communications company designs and manufactures digital telecommunications products and services. Its inventions and leading-edge technologies have transformed how the world connects, computes, and communicates. It also has a licensing business that includes a large patent portfolio and engages in extensive engineering, research, and development functions.

The company has implemented a practice and program around security control technology validation to assess its chosen security controls better. It chose AttackIQ's Security Optimization Platform to automate and operationalize this program.

The Challenge

The security team inside this communications company must protect thousands of employees across nearly 200 offices in dozens of countries around the world. Its intellectual property is under constant threat of theft by both organized crime and nation-state-affiliated cyberattackers. As the company has expanded, the mix of on-premise, cloud, and SD-WAN-connected remote facilities has required an increasingly complex set of differing security stacks for adequate defense and threat mitigation. The volume of ongoing attacks is significant and presents a considerable risk to the company's business operations. The security team must be able to assess the performance of its controls, personnel, and processes across all of the company's global facilities and networks.

Visibility into cybersecurity control performance is a critically important, central issue for the security team. It needs to be immediately aware of gaps, especially those caused by accidental misconfiguration, on a priority basis. It also wants to be able to assess its network defenses against the known threats that it is most likely to face and be able to simulate exactly how those threats would target and penetrate its internal networks.

Understanding the Use Case

This communications company must support compliance requirements that vary globally and must be implemented and supported correctly by the chosen security controls. Each facility and the personnel it supports have differing requirements for application access. These requirements must be supported securely in the local environment.

AttackIQ's Security Optimization Platform allowed the company's security team to systematically test and measure its current security controls against specific TTPs within the MITRE ATT&CK Framework. The depth and breadth support of MITRE ATT&CK provided by AttackIQ allowed the team to test, re-test, and provide evidence of coverage in a matter of days and weeks rather than months. This enabled the company to remediate any misconfigurations, find protection failures, and optimize its overall security posture.

AttackIQ's Security Optimization Platform has also enabled the company to assess readiness and validate that its enterprise security controls perform as expected. Automation allows the security team to mature its security validation capabilities and strive to work autonomously, scaling to meet current and future needs.

AttackIQ's Security Optimization Platform further provided essential support for the live production environments used by this company. Production environment support is a critical capability required by the company. The goal was to eliminate the ever-present gap between test environments and live production environments that can create a false sense of security. Once AttackIQ was installed, the company's live production environments and the primary and compensating controls it depended on became subject to regular testing.

Security control technology validation allows this communications company to objectively report its security controls to management through the lens of business risk. It can further rationalize and optimize the security controls managed by its blue team and other supporting organizations. All of this has reduced the company's perceived risk and has made it more confident in its ability to sustain operations under threat and prevail against likely cyberthreats.

This company has found a significant return on investment. It no longer has to implement its attack scenarios, develop corresponding scripts, and double-check all of the work to validate its security controls. The AttackIQ Security Optimization Platform enables security teams to identify their security controls, map their capabilities, measure the efficacy of those capabilities, and optimize their overall security posture. Finally, any new security technology control under consideration can be rationalized against the current security control set, and evidence can be provided to justify security investments.

The implementation of the security control technology validation use case using AttackIQ's Security Optimization Platform saved this communications leader time and resources as well as substantially reducing its risk by helping it understand if its security controls are working correctly and to its expectations.

ATTACKIQ

U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Center of Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.