CASE STUDY: COMMUNICATIONS INDUSTRY

Communications Firm

Executive Summary

This communications company is a Fortune 500 company that 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. This company engages in extensive engineering, research, and development functions.

> "AttackIQ's implementation of MITRE ATT&CK™ in its breach and attack simulation platform is a highly effective tool with which we can closely assess the state of our cyber defense programs defending our global networks. Our weekly sprints, using MITRE ATT&CK to validate chosen areas, have proven highly productive. In just two to three months, we found many areas requiring improvement and implemented special team programs to get the required mitigations in place."

Communications Company Cybersecurity Operations

Over the past few years of increasing cyber threat activity, it was deemed critically important by this communications company that it be able to more accurately assess the performance of its security controls, personnel, and processes for all of its global facilities and networks. The company chose AttackIQ as the breach and attack simulation (BAS) platform to operationalize MITRE ATT&CK in several areas, and it expects to complete global deployment over the next few years.

The Challenge

This communications company's intellectual property is under constant threat of theft by both organized crime and nation-state-affiliated cyber attackers. 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 significant risk to the company's business operations.

It is important to this communications company that it has ongoing visibility into the performance of its security controls. That has always been a central issue for the company's cybersecurity team. The team wants to be immediately aware of gaps, especially those caused by accidental misconfiguration, on a priority basis. The company also wants to be able to assess its network defenses against the known threats that it is most likely to face and wants to be able to simulate exactly how those threats would target and penetrate its internal networks.

The Situation

This communications company must protect and defend nearly 200 offices in dozens of countries around the world. Compliance requirements vary globally and must be implemented correctly and supported by security controls. Each facility and the personnel it supports have differing requirements for application access, and these requirements must be supported securely in the local environment.

The company wants to be able to implement a BAS platform efficiently and effectively and feels that the MITRE ATT&CK framework provides the best overall taxonomy for the organization of attacker techniques. The company also has access to multiple threat intelligence services that provide a continual stream of data. The cybersecurity team wants to operationalize this data rapidly and ensure that its global facilities have the necessary security controls in place to meet and stop these new threats.

The Solution

AttackIQ's BAS technology allowed this communications company to automatically simulate the full attack and expanded Kill Chain against enterprise infrastructure. The large depth and breadth of capability provided by AttackIQ BAS allowed for continuous validation of the company's security program. This enabled the company to find the performance gaps, strengthen its security posture, and improve its overall incident response capabilities. AttackIQ's BAS platform has also enabled the company to assess readiness and validate that its enterprise security controls are performing as expected. Automation enables the platform to work autonomously and to scale to meet the company's current and future needs.

AttackIQ's BAS platform also provided essential support for the live production environments used by this company. This was a critical capability required by the company. It was concerned that small changes to configurations or administration could open new vulnerabilities in its cyber defense. This is the ever-present gap between test environments and live production environments that, undetected, could ultimately compromise the company's security program.

Once the BAS platform was installed, the company's live production environments were tested frequently with the same Kill Chain of emulated activities that an attacker would most likely seek to execute.

Outcomes

This communications company is now able to objectively report on the status of its security controls on a worldwide basis. It has implemented an important use case to rationalize various controls put in place by its blue team. It uses Jira extensively to document found issues for each technique in the MITRE ATT&CK matrix. All of this has reduced the company's perceived risk and has made the organization more confident in its ability to sustain and prevail against likely cyber threats.

This company has also found a significant return on investment, as it no longer has to implement its own attack scenarios, develop corresponding scripts, and double-check all of the work. MITRE ATT&CK gives it everything it needs to implement scenarios quickly and correctly, using industry best practice scenarios.

Finally, and critically important, new threats, as identified by the company's threat intelligence team, are now rapidly modeled with the AttackIQ BAS platform so that global company security controls, procedures, and personnel can be validated to meet and defeat these new and dangerous threats.

ATTACKIQ

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

About AttackIQ

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ® supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit **www.attackiq.com** and follow us on **Twitter**, **Facebook**, **LinkedIn**, and **YouTube**.