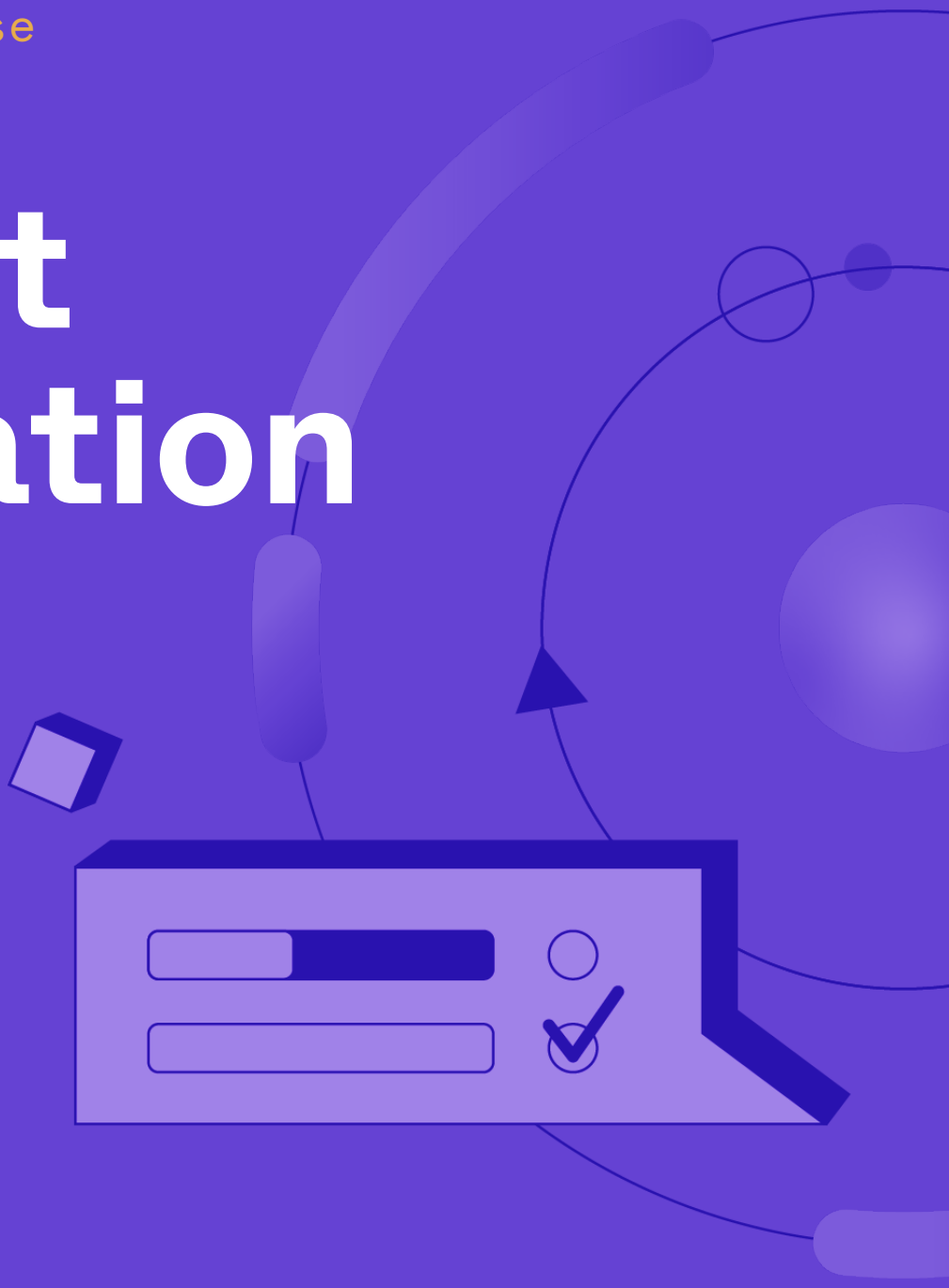
ATTACKIQ

Breach and Attack Simulation Use Case

Threat Emulation



Threat Emulation

Threat emulation enables organizations to safely emulate adversarial behavior, while empirically proving the existence and effectiveness of security controls and exposing gaps within the cybersecurity defense architecture. Cyberdefense teams can then provide current capabilities and best use existing resources and team members to optimize security control defenses. Threat emulation is driven by an adversary, attack intelligence, and a threat-centric viewpoint, an essential part of threat-informed defense®.

Deployment of the AttackIQ Security Optimization Platform, in conjunction with a clear communication plan and lexicon provided by MITRE ATT&CK®, supports the objective collaboration, testing, measurement, prioritization, and remediation required for threat emulation to be successful.

Case Study Industry: Insurance

A large insurance company delivers insurance products and a wide variety of investment and retirement-planning products. Its insurance products include term, universal, and whole life insurance; personal and business auto insurance; personal umbrella insurance; home insurance; motorcycle, boat, motor home, snowmobile, and car insurance; business liability key policy and business policy package insurance; farm and ranch liability insurance; and travel, trip cancellation, and global medical insurance.

This insurance leader moved to a threat-informed defense posture and chose to operationalize the MITRE ATT&CK framework to provide a common language for all of its cyberdefense teams. It selected AttackIQ as the security optimization platform to automate and operationalize its threat emulation use case requirements.

The Challenge

This insurance leader continues to go through a digital transformation. They are moving operations to the cloud, replacing branch and remote office leased lines with SD-WAN, addressing Internet of Things (IoT) device integration in its facilities, and providing mobile device access to internal networks for its agents and employees. This digital transformation, while necessary for its business operations, presents new opportunities for cyberattackers to penetrate and compromise the company's information technology resources.

Compliance activity is also an essential requirement for the company. Recently, the New York Department of Financial Services issued cybersecurity regulation 23 NYCRR 500, regulating financial institutions licensed within New York. Regulated parties include banks, brokerage firms, and insurance companies. The National Association of Insurance Commissioners (NAIC) developed a cybersecurity framework for the insurance industry. The New York legislation was rapidly followed by similar law in the state of Connecticut, and then by Ohio, Michigan, and South Carolina. All of this places additional requirements upon this insurance leader to identify and reduce cyberrisk per these new regulations.

Cyberthreats present substantial operational risks, as well as brand reputation risks. The company's security team was concerned about likely threats that face similar institutions in the industry. It was important for the team to understand if security controls are configured correctly and if these controls were able to address the likely chains of tactics, techniques, and procedures (TTPs) an attacker would use.

While the team had utilized threat intelligence to identify relevant threats categorically, they hadn't automated the process of systematically validating cyberdefenses. The team also needed to be able to document their operations and provide up-to-date, repeatable risk analysis to meet the compliance and auditing requirements.

Before implementing a security optimization platform, the organization had no visibility into the effectiveness of its security controls. It was unclear whether the controls were working as expected and could prevent, detect, and help the security team respond effectively. Validating the current security controls and identifying and exposing critical gaps were some of the requirements that the threat emulation use case would address and resolve.

Understanding the Use Case

The company's Cyber Threat Intelligence (CTI) team wanted the benefits of better implementing a threat-informed defense. It had also adopted MITRE ATT&CK to provide a knowledge base of attacker tactics, techniques, and procedures that it could use to map out expected adversarial behavior. This process was almost entirely manual — the company had no way to automate testing in a repeatable and consistent manner easily. The security team regularly identified and prioritized potential threats to its industry. It wanted to use this information to evaluate its overall security posture against expected threats. Where are we missing security controls? Are any of these security controls not working?

In support of its threat emulation use case, this insurance leader acquired the AttackIQ Security Optimization Platform. Now it could operationalize its threat intelligence feeds and its correlation of TTPs from MITRE ATT&CK to emulate adversarial behavior. This would enable validation of its security posture, identifying and exposing gaps and protection failures before the adversary to remediate its findings and optimize its security program.

The AttackIQ Security Optimization Platform supported the shift from manually testing the company's protection capabilities to fully automating testing across its production environment. Also, the MITRE ATT&CK framework was used to standardize communication with a common lexicon that improved the efficacy of remediation efforts and improved reporting risk mitigation to the business.

The AttackIQ platform's Integration Manager enabled the company's cybersecurity team to set up the critical integrations required to customize testing and provide direct access to measuring its capabilities across its entire security control stack. Its cybersecurity team can continuously measure and improve the prevention, detection, and response capabilities of its full security stack against known adversarial TTPs.

The entire process is automated — from assessment creation to the correlation of scenario attribution of events and alerts being pushed to the log aggregation points or SIEMs, nothing is done manually.

The implementation of the threat emulation use case using AttackIQ's Security Optimization Platform has saved this insurance leader time and resources, substantially reducing its risk by helping it understand if its security controls are working correctly and if they are addressing the threats it expects to face.

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.