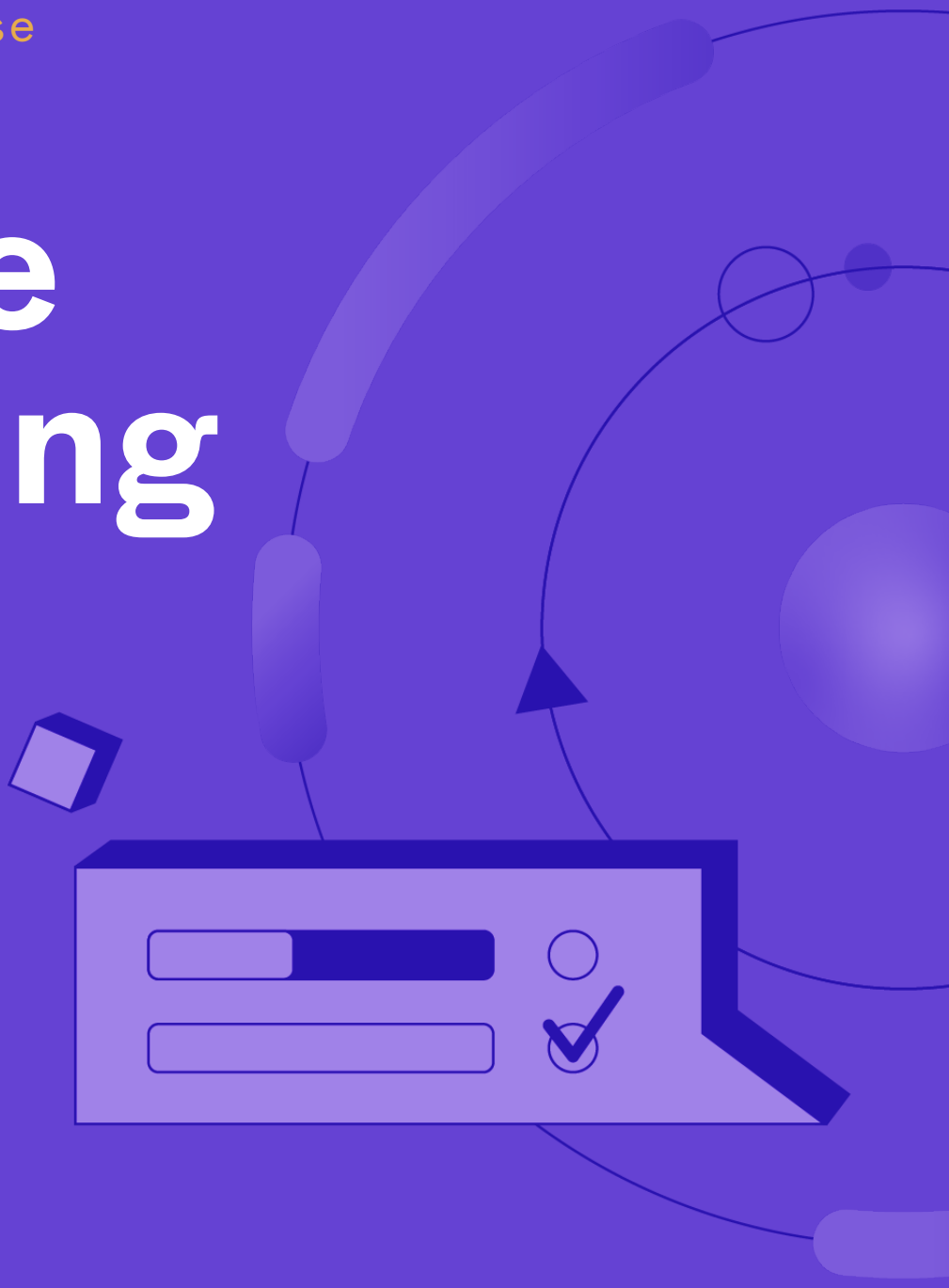
ATTACKIQ

Breach and Attack Simulation Use Case

Purple Teaming



Purple Teaming

Purple teaming is a methodology that fosters and supports collaborative communication between the red and blue teams. Purple teaming enables the blue team to participate in the security assessment of its people, process, tools, and technologies while fostering coordinated action and the sharing of threat intelligence, testing methodology, findings, and remediation recommendations. Purple teaming is predicated on a threat-centric posture, a central element of threat-informed defense®.

Successful purple teaming helps the entire cybersecurity operations organization rapidly and efficiently improve cyberdefenses. Deployment of the AttackIQ Security Optimization Platform, in conjunction with the common lexicon provided by MITRE ATT&CK®, provides clear success criteria, roles, responsibilities, communication, and insights better to support the activities and outcomes of a purple team exercise.

Case Study Industry: Energy

A leading highly diversified global energy infrastructure company with more than 10,000 employees and tens of thousands of miles of electric transmission lines and millions of consumers has an information security awareness program including periodic communications, company-wide events and campaigns, mandatory annual web-based training, facility-specific town hall events, and a cross-business advocacy program. This energy leader believed that incorporating purple team exercises into its security program would optimize communication between the red team, blue team, and other groups. It chose AttackIQ's Security Optimization Platform to automate and operationalize this effort.

Purple teaming was a means to an end for this major energy company. It wanted improved communications and faster iterative improvement across the security organization order to rationalize controls better and optimize its security program. The company also wanted to identify and resolve control gaps, better assess control risk, and adjust the mix to improve its overall security posture.

The Challenge

Increasing cyberthreats worldwide, coupled with the growth in compliance requirements, place mounting pressure on energy industry companies to more rapidly assess and improve their cyberdefenses. Energy and utility organizations have always been high-profile targets for cybercriminals and hostile nation-states and remain highly vulnerable.

Compliance also played a substantial role in setting the course for this energy leader's cybersecurity teams. The Energy Policy Act of 2005 gave the Federal Energy Regulatory Commission (Commission or FERC) the authority to oversee the reliability of the power grid and the authority to approve mandatory cybersecurity reliability standards. The North American Electric Reliability Corporation (NERC), which FERC has certified as the nation's Electric Reliability Organization, developed the Critical Infrastructure Protection (CIP) cybersecurity reliability standards.

The pressure of compliance-driven penalties looms large in the energy industry. FERC and the NERC are also moving to publicly identify violators of cybersecurity standards in the bulk electric system (BES). There are many existing standards in place and many others coming. This increases the requirements for this energy company to maintain a compliant infrastructure.

Understanding the Use Case

The energy company's cyberthreat intelligence (CTI) team uses multiple threat intelligence feeds and industry information to identify the most likely current and near-term threats regularly. This information supports its initiative to deploy a threat-informed defense. All of this is evaluated in a continuous testing and improvement cycle.

The cyberthreat intelligence team maps its threat intelligence feeds to MITRE ATT&CK, identifies key scenarios, builds assessments, and shares those assessments with the threat and vulnerability assessment team. The threat and vulnerability assessment team then performs the testing and communicates the results and remediation recommendations to the management, security operations center (SOC), and incident response (IR) teams. These results address many different questions: What threats were emulated, and why were they relevant to the organization? What security technologies prevented the chosen attack scenarios? What events and alerts were triggered, and did the SOC respond?

The threat and vulnerability assessment team produces post-reports that include AttackIQ Security Optimization Platform insights to communicate the company's security posture across various stakeholder teams. The reports also provide remediation recommendations that originate from both the AttackIQ platform and internal recommendations from key stakeholders to make the necessary changes. This information is shared with the IT operations team, who then make a decision based on these strategic considerations. This creates a transparent and collaborative communication process of planning, testing, measuring, remediation, and optimization, improving the overall security posture of the organization.

The AttackIQ Security Optimization Platform allows the company to continuously measure the performance of its security controls and assess the state of its global defenses. Where it has visibility into gaps, it can now correct them. Security optimization is a management practice of maximizing the efficiency and effectiveness of your total security program by ensuring that existing security investments are measured, monitored, and modified continuously from a threat-informed perspective. Optimization includes people, security controls, and processes.

With the AttackIQ Security Optimization Platform, the energy company conducts regular purple team exercises supported by automated testing. The company can rapidly analyze the results to improve existing controls and identify where new controls are needed. Members that participate in the purple team exercises also participate in department staff meetings and safety forums to provide perspective and continuous training on cybersecurity issues. Individual employees across the company support these efforts as cybersecurity leaders sharing relevant information with their teams.

The implementation of purple teaming through AttackIQ saved this energy company time and resources while helping to reduce its risk. The Security Optimization Platform supports close, effective, and highly collaborative communication between the red team, the blue team, and other critical internal organizations.

ATTACKIQ

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