ATTACKIQ

Industry Brief

Federal Government Defends Critical Infrastructure with AttackIQ's Security Optimization Platform

The Federal Government Challenge

As a leader of the free world, the U.S. continues to be a major target for cyberattacks from nation-states and ideologies across the globe. The U.S. Federal Government is perhaps the most prominent target and continues to face an increasing crescendo of sophisticated and malevolent cyberattacks higher than ever encountered before. This surge in cyberattacks and data breaches continues to impact federal operations.

The Federal Government has been on a fast track to getting ahead of the problem and is taking aggressive steps to meet and defeat these threats. New strategies have been implemented, including the move to proactive cyberthreat hunting, the increased use of threat intelligence data, continuous security monitoring, and the automated orchestration of security operations. All of this is designed to defend against and mitigate cyberattacks. However, many agencies are not able to react quickly enough to the accelerating cyberthreat.

Despite improvements, Federal Government agencies experienced over 31,000 cybersecurity incidents in 2018 alone. Federal agencies have a mandatory requirement to report cyberattacks and related incidents to the Office of Management and Budget (OMB) per the rules put in place by the Federal Information Security Modernization Act (FISMA) of 2002. In 2019, the White House noted that security incidents at federal agencies went down by 8 percent to 28,581, but the barrage of attacks still brought opportunity cost, the potential loss of data, and impairment of operations. Attackers used phishing and other email-based attack vectors to penetrate past endpoints and gain access to targeted federal networks. Nation-state attacks are among the most sophisticated and dangerous, and they are not easily detected.

To stem this massive tide of malicious cyberactivity, the Federal Government spent approximately $14.4 billion for unclassified cybersecurity efforts in 2018 alone. The FY 2019 President's Budget includes $15 billion of budget authority for cybersecurity-related activities, a $583.4 million (4.1 percent) increase above FY 2018. The classified expenditures are informally estimated to be much larger. This was insufficient to mitigate the damage due to the theft of critical data or impairment of often essential federal operations.

Security assessments of the Federal Government's high-value assets show hundreds of security gaps and architecture weaknesses that remain exposed and uncorrected, even as the Federal Government continues to acquire and deploy new security controls at a rate higher than ever before.

Security Control Performance Must Improve

Sponsored by AttackIQ, in 2019, the Ponemon Institute surveyed 577 IT and IT security practitioners in the United States who were knowledgeable about their organizations' IT security strategy and tactics. This survey included leaders from several federal agencies, including the Department of Defense and civilian agencies. These are also involved in evaluating or responsible for their agencies' technology investments. These were the summary results of this important survey:

Federal Government Customers Implement Attack IQ's Security Optimization Platform

A National Government Funded Laboratory.

This leading national laboratory uses the AttackIQ Security Optimization Platform to ensure the safety, reliability, and security of its information technology assets. With thousands of engineers and research staff members, this laboratory supports a wide variety of funded research initiatives. It works to enhance our defense, reducing the threat of terrorism.

A Defense Agency With Global Operations Reach.

This defense agency uses the AttackIQ Security Optimization Platform to assess security control performance and support threat modeling using the MITRE ATT&CK framework. This defense agency includes more than 30,000 officers, 200,000 enlisted personnel, and 200,000 civilian employees. AttackIQ supports this agency's mission in any corner of the world in which it may deploy.

A Leading Aerospace and Defense Contractor.

This leading aerospace and defense contractor uses the AttackIQ Security Optimization Platform to secure its delivery of comprehensive services in support of end-to-end IT engineering lifecycle services encompassing design, development, security, integration, operation, training, and maintenance. The contractor's wide variety of services include, but are not limited to, secure programs, enterprise capabilities, compliant enterprise services, support for tiered customer support, and integration of real-time enterprise communication services. These services are delivered to its Department of Defense customers to help ensure and maintain mission readiness. This defense contractor works with both the NIST and MITRE ATT&CK® frameworks. It chose the AttackIQ Security Optimization Platform to operationalize MITRE ATT&CK.

Security Control Performance Must Improve (cont.)

- 53 percent of these experts admit that they don't know if their security controls are working as they expect to protect the network;
- 45 percent say they do not know all of the gaps in their security posture;
- 63 percent reported that they had observed a security control indicating it blocked an attack when it failed to do so;
- 31 percent have no set schedule for penetration testing; and,
- 68 percent find that continuous security validation is effective in finding gaps and mitigating the risk of a data breach.

The Solution for Federal Government

Security Optimization

AttackIQ's Security Optimization Platform is a leading offering for the U.S. Federal Government breach and attack simulation (BAS) market. Our platform supports the automation and operationalization of the MITRE ATT&CK® framework. AttackIQ's Security Optimization Platform gives the Federal Government powerful capabilities to test continuously, measure, and validate the performance of security controls, personnel, and processes against the tactics and techniques in the MITRE ATT&CK framework.

AttackIQ's Security Optimization Platform uses MITRE ATT&CK to simulate the full attack chain against enterprise infrastructure. AttackIQ delivers continuous and objective measured validation of government security programs. You can find the performance gaps, strengthen your security posture, and improve your incident response capabilities. AttackIQ's Security Optimization Platform assesses readiness and validates that your enterprise security systems are performing as originally intended.

According to a 2020 presentation by Jon Oltsik, Senior Principal Analyst and Fellow at ESG, a typical enterprise may utilize from 10 to 75 or more security controls across the security organization, often with significant overlap and redundancy. The sheer number of cybersecurity vendors and unique security controls can become overwhelming in a large organization burdened by regulatory and compliance demands. For most of these organizations, it is unclear how well these security controls work and what areas and gaps require additional investment. AttackIQ's Security Optimization Platform helps you develop a smart strategy, validates that you have a resilient security control architecture, and objectively supports your budgeting decisions.

Often existing security controls are not configured correctly or integrated correctly with the security ecosystem. AttackIQ's Security Optimization Platform can identify potentially costly misconfigurations that could be found and targeted by malicious actors. In any scenario, your cyberdefense will not work if the security controls do not perform as you expect. AttackIQ's Security Optimization Platform will enable you to rapidly operationalize MITRE ATT&CK and get the most from the security controls, personnel, and procedures you have today.

Federal Government Use Cases Improve Defenses, Reduce Risk, and Deliver Return on Investment

Security Control Technology Validation.

Security Control Technology Validation is used to measure 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 offer the expected protection capabilities as they are currently configured as expected and optimized for your production environment.

Purple Teaming.

Purple teaming uses a methodology that fosters and supports collaborative communication between the red team and blue teams. Purple teaming enables the blue team to participate in the security assessment of its people, process, tools, and technologies while fostering agreement and the sharing of threat intelligence, testing methodology, findings, and remediation recommendations. Successful purple teaming helps the entire cybersecurity operations organization rapidly and efficiently improve cyberdefenses.

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 evidence of current capabilities and best use existing resources and team members to optimize security control defenses. Threat emulation is driven by adversary and attack intelligence and a threat-centric viewpoint, an essential part of threat-informed defense®.

Security Optimization (cont.)

AttackIQ's Security Optimization Platform brings scale and flexibility for the most significant federal organization. AttackIQ automation enables the platform to work autonomously and to scale. AttackIQ includes support for live production environments — even the small changes to configurations or administration can open new vulnerabilities in your cyberdefense. This helps identify and close the ever-present gap between Federal Government test environments and the live production environments that, undetected, will ultimately compromise the entire organization.

The AttackIQ Security Optimization Platform will also help you improve your total security program by ensuring that existing production investments are measured and monitored from a threat-informed perspective. The MITRE Corporation coined the term "threat-informed defense" as it made the MITRE ATT&CK framework operational. As MITRE says, a threat-informed defense strategy "applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks." MITRE ATT&CK is a foundational framework for testing your security against known threats. Only with accurate data about your team's performance against real-world threats can you make informed decisions to optimize your security program.

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.