CASE STUDY: GOVERNMENT

Government Services Contractor for DOD

"In the face of increasing targeted threats against our networks and assets and those of our customers, it is highly important to us to better understand if our cybersecurity infrastructure could protect us against the most likely threats we might face. We believe that AttackIQ's breach and attack simulation platform can provide the real-time telemetry and objective assessment we need and provide the edge we need to stay ahead of current and future cyber threats."

Executive Summary

This award-winning government services contractor leads in the 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, enterprise capabilities, compliant enterprise services, support for tiered customer support, and integration of real-time enterprise communication services. These services are delivered to the contractor's clients with live, virtual, and/or constructive (LVC) training and training solutions to develop, measure, and ensure mission readiness around the world.

This contractor also has a rapidly growing cybersecurity and information assurance practice that services many branches of the Department of Defense. This team is constantly assessing ever-evolving threats and unauthorized access to enterprise systems, networks, applications, and data through integrated technologies, approaches, and best practices in both cybersecurity and information assurance.

Government Services Contractor

This contractor works with both the NIST and MITRE ATT&CK™ frameworks. It initially chose MITRE ATT&CK as the primary cybersecurity framework for its team to operationalize. In order to make these assessments, and after considerable evaluation of the many alternatives, it chose AttackIQ, Inc. to operationalize MITRE ATT&CK in support of these efforts.

The Challenge

This contractor is a readily growing and highly successful U.S. Federal Government contractor. Sensitive contracts require that it steps up its cyber defenses in the face of the steadily increasing volumes of sophisticated attacks. Configurations are often locked down, but then are subject to drift and misconfiguration over time. This needs to be caught immediately, as this may expose vulnerabilities that can be used by aggressive attackers.

The contractor also has a cybersecurity practice and is highly knowledgeable with respect to the current cybersecurity threats. The key requirement for the contractor is to detect attackers as soon as possible in the Kill Chain and prevent exfiltration. The contractor's best practices emphasize that if it can break the Kill Chain at any step, the attack can be shut down. It is also subject to compliance requirements, all of which require ongoing risk analysis and assessment. Given these requirements, it was determined that a breach and attack simulation (BAS) tool would provide high value in support of the contractor's security programs.

It was initially important to them to address two key use cases. First and foremost, the contractor wanted to support its MITRE ATT&CK self-evaluations and wanted the automation to power it going forward. Today, consultants come in to perform MITRE ATT&CK evaluations. The company wanted to move towards the automation provided by BAS to test, document gaps, and then enter suggested mitigations into their ServiceNow ticketing system, and, subsequently, gradually incorporate this with critical

security orchestration, automation, and response (SOAR) technology. It was also very important to the contractor's team to validate Carbon Black endpoint detection and response (EDR) is configured correctly and optimised to the techniques against which it protects. It also wanted to validate that alerts were sent at all times successfully to their security information and event management (SIEM) system.

The Situation

Multiple divisions of this contractor service dozens of government customers on different contracts. In many cases, its information technology assets must be integrated with government networks and other assets. All of this makes the perimeter more porous and presents opportunities for cyber threat penetration. Vulnerability management is a continual and ongoing problem. Even with a well-defined security baseline, it is difficult to keep the configurations stable over time.

The contractor runs regular red-team penetration tests on a weekly, monthly, and quarterly basis to help ensure that it has best practice implementations in place. It also uses tools like Nessus to perform network vulnerability scanning several times per day. Its security operations center team operates on a 24-hour basis, serving both internal needs and the contractor's customers.

The Solution

AttackIQ's BAS platform has allowed this contractor to simulate the full attack and expanded Kill Chain against enterprise infrastructure using software agents, virtual machines, and other means. This large depth and breadth of capability has allowed for the continuous validation of its information technology assets. This enables the contractor to find the performance gaps, strengthen its security posture, and improve overall incident response capabilities. AttackIQ's BAS platform assesses readiness and validates that the contractor's enterprise security systems are performing as originally intended. Automation enables the platform to work autonomously and to scale to meet future requirements.

AttackIQ's BAS platform also provided essential support for the live production environments used by the contractor. Small changes to configurations or administration that can open new vulnerabilities in cyber defense are now under constant scrutiny by the BAS platform. This identifies the ever-present gap between test environments and live production environments that, undetected, will ultimately compromise the entire organization. The contractor's live production environments are subject to the same Kill Chain of emulated activities that an attacker would seek to execute.

Outcomes

The contractor's risk council meets weekly to discuss any identified gaps found by the AttackIQ platform. AttackIQ enables the contractor to continuously validate cyber readiness. A key use case of the contractor that was successfully implemented is validating that the controls protect against exfiltration through known and identified techniques. All of this is in place and working to the contractor's security team's expectations.

This contractor's investment in AttackIQ BAS has been well rewarded. The objective assessment of security control performance, identification of gaps, and validation of remediation has enabled the contractor to meet and exceed its goals for the BAS implementation. It can immediately identify configuration drift or error, move its blue teams to implement necessary changes, and confirm that the changes are correct through BAS validation. The contractor is also pleased with the deep implementation of MITRE ATT&CK and considers the operationalization by AttackIQ to be highly impactful and beneficial.

This contractor continues to provide AttackIQ with a wealth of suggested improvements and enhancements which will serve the best interests of both parties.

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**.