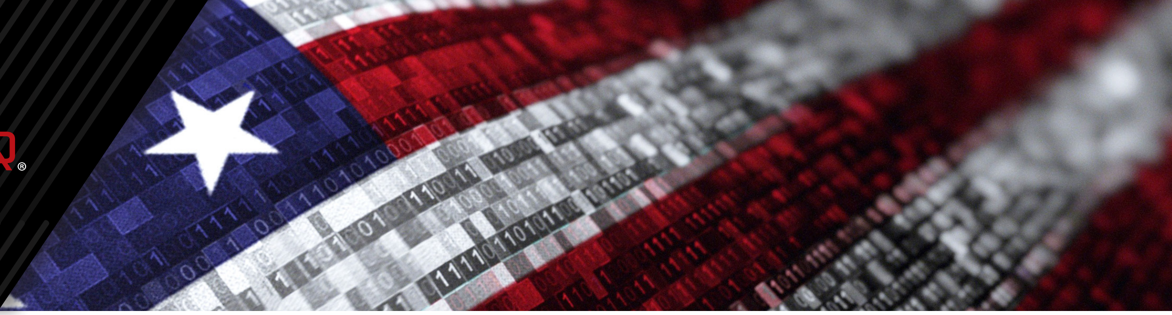
ATTACKIQ®



CASE STUDY: STATE AND LOCAL GOVERNMENT

State and Local Government

Executive Summary

This major United States city government serves well over 1 million residents. It provides law enforcement, public safety, libraries, parks and recreation, zoning, and similar services to its residents. Many of these services are also utilized by tens of millions of visitors every year.

Over the past several years, a rapidly increasing wave of ransomware-as-a-service and other malware cyber attacks have continued to strike municipality, city, and state governments. These attacks have cost tens of millions of dollars to remediate and have impacted critical services and support provided by the government entities to its residents.

> "In the face of increasing targeted threats against cities like ours, it became highly important to the city to better understand if our cybersecurity infrastructure could protect us against the most likely cyber threats we might face. AttackIQ's platform has given us that increased visibility and allowed us to assess our risks in a highly objective and data-driven way."

City Cybersecurity Operations

The city chose MITRE ATT&CK™ as the primary cybersecurity framework for its team to use to assess its cyber defenses and, after considerable evaluation of the many alternatives, chose AttackIQ, Inc. to operationalize MITRE ATT&CK in support of these efforts.

The Challenge

Like any municipality, this city has to increase the capabilities of its cyber defenses and manage this within necessary budget constraints. The city felt that breach and attack simulation (BAS) offered it some important capabilities, but could not grow its staffing and wanted the deployment and support to fall within budget guidelines.

The city was also highly concerned about the increasing threat environment facing cities and the volume of threat intelligence pouring in about the risks associated with ransomware-as-a-service. It wanted to be able to validate that its security controls could identify and mitigate these types of threats.

Also critical, the city wanted these capabilities integrated with security orchestration and an automated response platform so that remediation could be automatically implemented as gaps were discovered. It was essential that a vendor could provide this integration to support overall operations objectives.

The Situation

The delivery of the city's technology services spans over 30 city departments, hundreds of locations, nearly 12,000 employees, and well over 1 million residents. Staffing for the city's technology services is supported by dozens of city IT professionals and dozens of public-safety radio engineers and support staff. In addition to the city staff members, the services are supported by contracts, including contracts to manage the city's hundreds of applications.

Through 2018 and most of 2019, the city has averaged more than one cyber attack each second. The city's cybersecurity team is paramount to protect every aspect of the city's IT systems 24 hours a day, seven days a week. The cybersecurity team protects the city's data and technology and manages the business risk of city IT operations.

The Solution

AttackIQ's BAS technology now allows this city to automatically simulate the full attack and expanded Kill Chain against enterprise infrastructure using software agents, virtual machines, and other means. The AttackIQ BAS platform allows for the continuous validation of the city's security program and allows the city to find the performance gaps, strengthen its security posture, and improve overall incident response capabilities. The AttackIQ BAS platform assesses readiness and definitively validates that the city's security controls are performing as originally intended. Automation enables the AttackIQ BAS platform to work autonomously and to scale to meet future requirements.

AttackIQ's BAS platform has also proven essential in providing support for live production environments used by the city. Small changes to configurations or administration can open new vulnerabilities in the city's cyber defense. This is the ever-present gap between test environments and live production environments that, undetected, could compromise city operations. The AttackIQ BAS platform has been implemented so that the city's live production environments are subject to the same Kill Chain of emulated activities that an attacker would seek to execute.

Outcomes

AttackIQ's BAS platform has provided the city with the capabilities it requires at a highly competitive cost that will stay within its current and projected budgets. The city is now able to accurately assess the status of its security controls in near real-time and has directly addressed risks from known and likely ransomware-as-a-service based threats. The AttackIQ BAS has enabled the city to report objectively on the threats it faces, the gaps that require remediation, and the personnel and processes necessary to improve these important enhancements.

Operationalizing BAS around MITRE ATT&CK enables the city to model the most likely attacks and threats and to organize planning and response in a logical and well thought out way. The city finds MITRE ATT&CK to be comprehensive and notes that MITRE ATT&CK provides a common taxonomy to its cyber defense team that makes it easier and faster to communicate regarding urgent and acute threat challenges.

As an early customer and development partner, the city continues to provide AttackIQ with important suggestions for new capabilities and functionality.

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**.