ATTACKIQ

Industry Brief

State and Local Government Boost Defenses with AttackIQ's Security Optimization Platform

State and Local Government Challenge

State and local government agencies must grow and expand cybersecurity resiliency and effectiveness as the demands for information technology services continue to grow. This requires a delicate balance between delivering the necessary services the public needs and meeting the financial constraints that must be successfully managed.

State and local government agencies must be able to deploy and scale effective cybersecurity services across all application access that they must support. This might include student records, personally identifiable information (PII), financial documents, tax records, contractual documents and files, intellectual property, email correspondence, and much more.

Yet many state and local governments have been unable to spend and allocate dollars to best the current cyberthreats that continue to devastate government institutions. While state and local governments have many security controls, they are uncertain as to their effectiveness and coverage, especially in the wake of so many successful cyberattacks upon government infrastructure. From late 2018 to early 2020, state and local governments were assaulted by a barrage of cyberattacks of unanticipated size and scale. These attacks cost municipalities millions of unbudgeted dollars and stopping and curtailing essential government services, in some cases, for many months.

Some of these attacks included:

- **December 13, 2019:** The city of New Orleans declared a state of emergency due to a severe cyberattack. This cyberattack may cost the city over $7 million.
- **December 2019:** The city of Pensacola, Florida, was infected by Maze ransomware. It paid $1,000,000 to regain access to city data and unlock critical services.
- **July 25, 2019:** City Power, the municipal electric utility for Johannesburg, South Africa, disclosed a significant ransomware attack.
- **June 26, 2019:** Lake City, Florida, was hit with a serious ransomware attack. It cost approximately $500,000 to regain access to encrypted files.
- **June 20, 2019:** Riviera Beach, Florida, was faced with a ransomware attack. It cost $600,000 to regain access to encrypted files.
- **May 7, 2019:** The city of Baltimore, Maryland, was hit with a RobinHood ransomware attack that brought down most of the city's servers and some essential government applications. It was estimated that this ransomware attack may cost the city over $18 million.

State and Local Government Institutions Implement Attack IQ's Security Optimization Platform

A Major City in the Western United States.

This city chose MITRE ATT&CK as the primary cybersecurity framework for its team to use to assess its cyberdefense and chose the AttackIQ Security Optimization Platform to provide visibility and reduce risk. This major United States city government serves well over 1 million residents. It delivers law enforcement, public safety, libraries, parks and recreation, zoning, and similar services to its residents. All of these services have underlying information infrastructure that must be protected. Many of these services are also utilized by tens of millions of visitors every year. 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 by using AttackIQ's Security Optimization Platform.

A State Government in the United States

This state government uses the AttackIQ Security Optimization Platform to help secure all of its state departments and agencies such as agriculture, the office of the attorney general, budget and finance, taxation, the state legislature, the state judicial branch, and more. With over 50,000 employees widely dispersed across the state, the safety and resilience of its information technology infrastructure are of paramount importance to it. There is also a strong military presence in this state — this is also a driving factor for improving cybersecurity and protecting critical state services.

- **April 2019:** Cleveland Hopkins International Airport in Ohio suffered a ransomware attack that shut down its email and also brought down the in-airport flight and baggage displays.
- **April 2019:** The city of Augusta, Maine, suffered a highly targeted malware attack that froze the city's entire network and forced the city center to close.
- **April 2019:** A cyberattack upon the city of Tallahassee, Florida, cost the city approximately $500,000.
- **March 2019:** The city of Albany, New York, suffered a ransomware attack that impacted police department systems, including scheduling and email applications accessed over the internet. The attack also affected computers in patrol cars.
- **March 2019:** The government of Jackson County in Georgia paid cybercriminals $400,000 after a cyberattack shut down the county's computer systems.

Many of the officials in these city, county, and state governments will tell you that they have spent considerable funds adding and layering security controls and putting in place the procedures to support them. The challenge is that they are not sure that these controls are performing as they expect. In many cases, they believed that they had security controls that would detect and stop many of the ransomware attacks that, instead, devastated their operations.

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 in state and local government and other regional government organizations. These are also involved in evaluating or responsible for their organizations' technology investments. These were the summary results of this important survey:

- 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.

State and Local Government Institutions Implement Attack IQ's Security Optimization Platform

The Ministry of Finance.

This international government chose the AttackIQ Security Optimization Platform to provide security for its ministry of finance. Its department of finance is the principal body for controlling state expenditure, budget reporting, and collecting taxes and duties. It implemented security optimization across all of its operations, including departments within the ministry for agriculture, petroleum, roads, railway, labor, pension services, urban projects, and more.

State and Local 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 expected as they are currently configured and optimized for your production environment.

Purple Teaming.

Purple teaming uses a methodology that fosters and supports collaborative communication between 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 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.

The Solution for State and Local Government

Security Optimization

AttackIQ's Security Optimization Platform is a leading offering for the state and local government breach and attack simulation (BAS) market. Our platform supports the automation and operationalization of the MITRE ATT&CK® framework. This gives state and local governments a powerful capability to continuously test, 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 healthcare enterprise 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 enterprises, 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.

AttackIQ's Security Optimization Platform brings scale and flexibility for any state or local government organization. AttackIQ automation enables the platform to work autonomously and to scale. This 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 government test environments and the live production environments that, undetected, will ultimately compromise the entire organization.

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

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.)

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.

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.