

ATTACKIQ

Case Study



# Ahead of the 2020 Elections, AttackIQ Is a Force Multiplier for One State's CISO

As prime targets for cyberattacks, state governments are challenged to manage the risks to their systems, applications, and data. One acute risk is foreign interference in U.S. elections to manipulate electoral outcomes. To prepare for each election cycle, state CISOs must ensure that all their existing cybersecurity controls are working as expected. If they need to procure additional security technology, CISOs must have an objective way to validate vendor claims regarding the efficacy of their products.

One state CISO, the head of a team that has been using the AttackIQ platform for the past year, explains how his department uses AttackIQ to achieve these goals. Overall, he views the platform as a tool for security optimization, a way to manage risk and improve the return on investment of security talent and technology.

## First, Close the Obvious Gaps

Security optimization is a management practice of maximizing the efficiency and effectiveness of your total security program (people, process, and technology), by ensuring that existing security investments are measured, monitored, and modified continuously from a threat-informed perspective. This sounds like a huge undertaking, especially for state IT departments with tight budgets. But there are relatively simple ways they can get started.

*"A common practice for incoming CISOs is to start with comprehensive assessments of their security programs," the state CISO says. "But generally, there will be basic deficiencies – such as lack of patching – that are easy to expose and may mitigate much of the risk. It's much more cost-effective to address those things first, before investing in assessments to expose the remaining gaps."*

***"AttackIQ is a force multiplier for our department's limited staff. It simplifies and lowers the cost of exposing security gaps."***

– CISO, State Government

When this CISO performs a cybersecurity assessment, he uses the AttackIQ breach and attack simulation (BAS) solution. *"AttackIQ is a force multiplier for our department's limited staff," the CISO says. "It simplifies and lowers the cost of exposing security gaps."*

The state's technology services department outsources most of its penetration testing. To make the best use of what can be a costly resource, it uses AttackIQ to automate the basic testing tasks, like validating that existing security controls perform as intended. *"We can then ask our external pen testers to tackle the more difficult issues," the CISO explains. "In this way, we get more value for the fee we pay, and they benefit from more interesting work."* Keeping pen testers engaged is not mere benevolence; it can help reduce turnover, a perennial problem in the cybersecurity industry, which suffers from a shortage of talent.

### CUSTOMER

State Technology Services  
Department

### LOCATION

Americas

### INDUSTRY

State and Local Government

### HIGHLIGHTED SOLUTION AREAS

- Audit and Testing
- Security Strategy and Investment Decision Support
- Threat Hunting
- COTS Security Control Evaluations
- Security Control Rationalization
- Analyst Training and Exercises

### BUSINESS IMPACT

- Optimization of security technology, staff, and processes
- Ability to validate vendor claims when selecting new security technology
- Simpler, faster, and lower-cost discovery of security gaps
- Validation of security infrastructure ahead of upcoming elections

Some of that more engaging work involves using AttackIQ to map testing scenarios against the more advanced threats. Although AttackIQ is designed for rapid deployment and includes a large set of the MITRE ATT&CK tactics, techniques, and procedures (TTPs), the platform is readily customized. *"More advanced staff can build out sophisticated scenarios, while the less experienced staff can run the reports,"* the CISO notes.

## Automated Testing Eases Pressure of Elections System Security

Ever since the Russian interference in the U.S. presidential elections in 2016 and the U.S. congressional elections in 2018, there has been widespread concern about the security of state voting systems. As they are considered critical infrastructure, the election systems come under the purview of the state CISO. The state's technology services department provides the cybersecurity monitoring, network management, and virtual server support to facilitate statewide elections. It also provides computing, communication network infrastructure, and many layers of cybersecurity protections for the digital assets of the state elections office.

Although the state's processes and systems that collect and count votes are not exposed to the internet at any time, the CISO needs to provide positive proof that they are, in fact, secure. A data-driven, threat-informed strategy helps him do that. *"We need to map out the external attack surface and ensure that our election systems are hardened and that we are able to shut down or disable whatever is unintentionally exposed,"* the CISO explains. *"AttackIQ helps us validate that the controls we have in place actually do that. It also helps us identify potential control gaps that we may have missed."*




*"We need to map out the external attack surface and ensure that our election systems are hardened. AttackIQ helps us validate that the controls we have in place actually do that. It also helps us identify potential control gaps that we may have missed."*

– CISO, State Government

As the next elections draw near, the pressure to minimize risk will increase, which is why the CISO favors the automated BAS capabilities in AttackIQ. *"Human error is the most problematic aspect of dealing with cyberattacks,"* he notes. With AttackIQ, busy security staff can set automated test scenarios to run continuously, and these can expose gaps that staff might otherwise miss.

Beyond election readiness, the state's technology services department must concern itself with the systems and applications at all the state agencies. The agencies make hundreds of datasets available to employees, contractors, analysts, and residents. To prevent data tampering and exfiltration, the state employs endpoint detection and mitigation controls.




*"Using AttackIQ gives us more comfort in knowing that our endpoints are appropriately configured. Because AttackIQ automates this process, it saves us a huge amount of time."*

– CISO, State Government

Errors in endpoint configuration enable bad actors to stealthily circumvent network security controls and enter the network without generating alerts. In the absence of these alerts, security staff falsely assume the controls are doing their job. *"Using AttackIQ gives us more comfort in knowing that our endpoints are appropriately configured,"* the CISO says. *"Because AttackIQ automates this process, it saves us a huge amount of time."*

## Using MITRE ATT&CK to Gage Vendor Maturity

AttackIQ was the first platform to operationalize the MITRE ATT&CK framework. For this CISO, the framework serves as a maturity model. *"The industry is excited about MITRE ATT&CK,"* he says, *"and it's a good methodology for us to follow."* It also turned out to be a good gauge of the maturity of prospective technology vendors. *"We ask vendors if they will participate in a MITRE ATT&CK review; if they do, it's a sign that their solution has probably been rigorously tested."*



*"AttackIQ was a core tool during our vendor evaluation. We used it to validate the solutions' protection and detection capabilities. Ultimately, we achieved a price savings by leveraging the best consolidated tool."*

– CISO, State Government

The CISO recently had the opportunity to put vendors to the test when evaluating endpoint detection and response (EDR) solutions. Recognizing that endpoint threat prevention and detection technologies were converging, the CISO sought a robust solution combining both capabilities, eventually shortlisting a couple of vendors. *"AttackIQ was a core tool during our vendor evaluation,"* he says. *"We used it to validate the solutions' protection and detection capabilities. Ultimately, we achieved a price savings by leveraging the best consolidated tool."*

# Conclusion

## Lessons Learned from Security Optimization

According to the CISO, security optimization plays a significant role in cybersecurity strategy. *"Solutions such as AttackIQ allow organizations to speed up and instrument their assessments,"* the CISO adds. *"They drive down human error from both the assessors' side and the defenders' side."*

As cyberthreats proliferate and state network attack surfaces expand, staffing budgets do not. *"Small organizations can use BAS solutions such as AttackIQ to leapfrog past older technologies and get more bang for their buck,"* the CISO explains. *"Larger organizations can save time and money and reallocate people to work on more sophisticated problems and more critical systems."*

#### 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](http://www.attackiq.com). Follow AttackIQ on [Twitter](#), [Facebook](#), [LinkedIn](#), and [YouTube](#).