ATTACKIQ®

Case Study

Bolstering Cybersecurity Controls Throughout a Large U.S. Military Service

Modern militaries face a plethora of threats, which are constantly—and rapidly—evolving. From electromagnetic warfare to emerging cyberattacks, technologies that seem like sci-fi movie plot points are today creating real-life security risks for governments around the world. That's why large military services run exercises to test their defenses against advanced technological threats. A couple of years ago, one military service added cyberthreat emulations into its exercises to test its defense capabilities.

"For more than a decade, we had broad challenges with testing and validating cybersecurity controls," says a capabilities development manager for one military service's cyber defense operations wing. "We needed to operationalize cyber testing. As I see it, cyberspace is just another plane for military maneuvers; the only difference is that the plane consists of ones and zeros. A firewall is an obstacle, just like a brick wall, and it too can be broken. Like the infantry, the cyber defense team needs to search for, identify, and then remediate vulnerabilities."

Due Diligence for Arming Cyber Defenders

This military service considered several breach and attack simulation tools before selecting the AttackIQ Security Optimization Platform. The goal was to move "out of being reactive, to a more proactive approach to defense," says the capabilities manager. "We wanted a tool for continuously assessing the effectiveness of our people and organizations against specific new threats we could see coming down the pike."

AttackIQ's Security Optimization Platform was appealing because of its attack simulation playbooks and its tight integration with the MITRE ATT&CK framework. "All of our cyber defense operations are aligned to the MITRE ATT&CK kill chain," says the capabilities manager. "When we are looking for adversarial activity to simulate, our defenders turn to the MITRE ATT&CK framework for guidance."

> *"Every other vendor we evaluated had developed its own malware. Running that malware opened up security holes on the systems and devices we were testing. By contrast, AttackIQ doesn't compromise the systems it is testing."*
>
> - Capabilities Development Manager, Cyber Defense Operations, Large Military Organization

Another consideration, according to a project officer who helps provide this military service's information technology and business systems, was that "we needed to be able to both emulate specific attacks and routinely scan the network for any threats that our HBSS [host-based security system] had not picked up." The Security Optimization Platform meets this need. It can periodically run automated simulations based on threats identified in the MITRE ATT&CK framework, and can perform one-off simulations at users' discretion.

CUSTOMER

Large Military Organization

LOCATION

United States

INDUSTRY

Military

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Control Auditing
- Investment Decision Support
- Analyst Training and Certification
- Internal Quality Testing: Development

PROJECT BUSINESS IMPACT

- Better understanding of cyber defenses' effectiveness against threats coming down the pike
- Acceleration of defenders' detection and response to specific threats
- Minimization of security vulnerabilities in mission-specific technology infrastructures
- Improved training and talent management for soldiers at all levels of cyber defense
- Faster procurement of key security technologies

Due Diligence for Arming Cyber Defenders (cont.)

"AttackIQ allows Cyber Defenders to see the different types of attack mechanisms and tactics that adversaries are likely to use," says the capabilities manager. He notes two additional reasons why this military service selected the Security Optimization Platform: "One is that the other vendors we considered follow a signal flow, where one step in the kill chain is dependent on the next step, which is dependent on the next step, and so on. With AttackIQ, users can run the entire kill chain if they want to, but they may also skip parts of the kill chain to get to the specific area of an attack that they want to emulate." Simulations targeting a specific section of the kill chain run more quickly and require less staff time to implement.

The other reason was that competitive products seemed to actually increase risk to customer systems. "Every other vendor we evaluated had developed its own malware," the capabilities manager says. "Running that malware opened up security holes on the systems and devices we were testing. By contrast, AttackIQ implements attack sequences in a benign way. It doesn't compromise the systems it is testing."

As part of its due diligence process, this military service tested the Security Optimization Platform at a power plant, using AttackIQ's open API threat intelligence function to incorporate classified capabilities into the testing. "We deployed one of our military service's cyber defense platforms onto the power plant's infrastructure, then used AttackIQ agents across that infrastructure to assess the security posture," the capabilities manager says. "Once we got the results, the team started implementing defense strategies to mitigate the security gaps it identified. In the first 30 minutes using AttackIQ during this exercise, I could see the potential for our organization."

AttackIQ Supports Military Operations

This military service began rolling out the AttackIQ Security Optimization Platform, but deployment was sidetracked by the nation's COVID-19 response and the solution isn't yet fully deployed. Still, prototypes are demonstrating its value in operational readiness assessments.

"AttackIQ holistically evaluates people, processes, and policies, as well as security technologies," the capabilities manager says. "We are building an AttackIQ environment that will simulate attack campaigns, with the goal of helping our defenders lower their time to detect and respond to specific threats. We intend to consistently push similar attack sequences to see whether responses get faster with each iteration. If the time isn't decreasing, we will need to determine whether our systems or processes need improvement, or our soldiers need training."

> *"We don't have the option to continuously do red teaming. Using AttackIQ enables us to do much more frequent control validations, and to retest as often as we want to make sure we're making progress."*
>
> - Capabilities Development Manager, Cyber Defense Operations, Large Military Organization

While human red teams can perform similar assessments, they could not do so as frequently as this military service wanted. "We don't have the option to continuously do red teaming," says the capabilities manager. "There are so few red teams available within our military, trying to get on their schedule is always a challenge for individual groups. And when a group does get a red team's time, once a year or so, they perform a one-off assessment, which usually ends up being a compliance check. Using AttackIQ enables us to do much more frequent control validations, and to retest as often as we want to make sure we're making progress."

AttackIQ Supports Military Operations (cont.)

The capabilities manager envisions an end state in which the military combines extensive internal threat intelligence with the MITRE ATT&CK framework and a regular flow of data from the nation's independent intelligence agencies. The military would then leverage this aggregated knowledge base when creating attack emulations within AttackIQ. "We would have a wide array of collection points that identified cyberattacks and trending threats," he says. "We would continuously review that intelligence and develop mitigation plans that we would test against on a daily or weekly basis. That would be a huge culture change for how our military operates."

In addition to routine security control validation, the capabilities manager expects the Security Optimization Platform to play a role in mission planning processes. Today, mission planning involves identification of tools and software that the unit will need for an upcoming deployment. Security is a consideration in this process, but this military service does not perform controls testing in advance. AttackIQ has the potential to change this. "Before a unit goes on a mission, they should undergo a security assessment," says the capabilities manager. "They should understand the threats they will face and how they're going to either clear, mitigate, or defend against those threats."

AttackIQ could also verify the effectiveness of solutions created by this military service's cybersecurity development team. "Once they develop a technique or a new tool, they could incorporate it into a playbook that the AttackIQ platform could use for automated testing against different security procedures," says the capabilities manager.

Assessing and Improving Cyberdefenders' Performance

Another area that is ripe for AttackIQ insights is cybersecurity education. "In my mind, training should be our military service's number-one priority for the Security Optimization Platform," says the capabilities manager. "Until operators are well-trained, they will not be proficient or effective enough to defend against adversaries. The benefit of adding AttackIQ to a training program is that it provides details on exactly how a system is being attacked and what commands the attacker is using. A defender can learn from AttackIQ simulations how to detect attacks that don't show up in our list of signatures or our behavioral detection techniques."

> *"We need to incorporate AttackIQ into our cybersecurity courses. If we do, our soldiers will start their careers with an understanding of the adversary's mindset and how the network might be attacked."*
>
> - Capabilities Development Manager, Cyber Defense Operations, Large Military Organization

The military service IT project officer concurs. "We need to incorporate AttackIQ into our cybersecurity courses," she says. "If we do, our soldiers will come out of the gate trained on how to not only defend the network, but also find the TTPs [tactics, techniques, and procedures] that our adversaries are using. They will start their careers as military cybersecurity defenders with an understanding of the adversary's mindset and how the network might be attacked."

The Security Optimization Platform also has potential to improve defenders' job-performance evaluations. "Threat emulations could really help with talent management in the cyber community," says the capabilities manager. "We could use AttackIQ to periodically perform pop quiz type assessments. We could customize the scenarios so that a host analyst, for example, is tested on her ability to identify threats on an endpoint."

Such assessments would identify areas where people need training. And if training opportunities fail to fix the problem, "we could ultimately use the platform to validate whether a soldier knows what he's doing," the capabilities manager says. "Assessments could help us make sure we have the right person in each position defending our country on the cyber front."

Faster, Data-Based Acquisitions

One other area in which the Security Optimization Platform may help the military effect real change is the procurement of security solutions. Each division within this military service could use AttackIQ to test the effectiveness of its existing security program during the decision cycle for new investments. Meanwhile, the military service could run a trend analysis to identify security challenges that permeate the entire organization.

"We could look at the trending attack sequences or TTPs and apply them across the domain," says the capabilities manager. "Sometimes our military service's acquisition group tends to stovepipe the needs of other divisions, but with cybersecurity, that isn't wise. I have already been working with them to rethink procurement of these solutions."

When a trend analysis identifies a problem, this military service could use AttackIQ data to quickly build a business case for investment. "Our military service has historically been slow to implement new things," says the capabilities manager. "Seeing trending risks and implementing mitigation solutions more quickly would help our overall security posture."

Conclusion

All told, this military service is on track to use the Security Optimization Platform to build a more strategic defense posture across acquisitions, talent management, and operations.

"Our military typically puts a Band-Aid on problems," the IT project officer says. "The cost-effective way to solve problems is to invest in long-term solutions to mitigate risks upfront vs applying a quick fix. When we see a broad challenge unfolding, we like to step back and ask, 'How do we defend against something like that? What mitigation strategies should we implement to prevent that from happening here?' The automated security control validation that AttackIQ provides will enable us to answer those questions anytime they arise."

ATTACKIQ®

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com