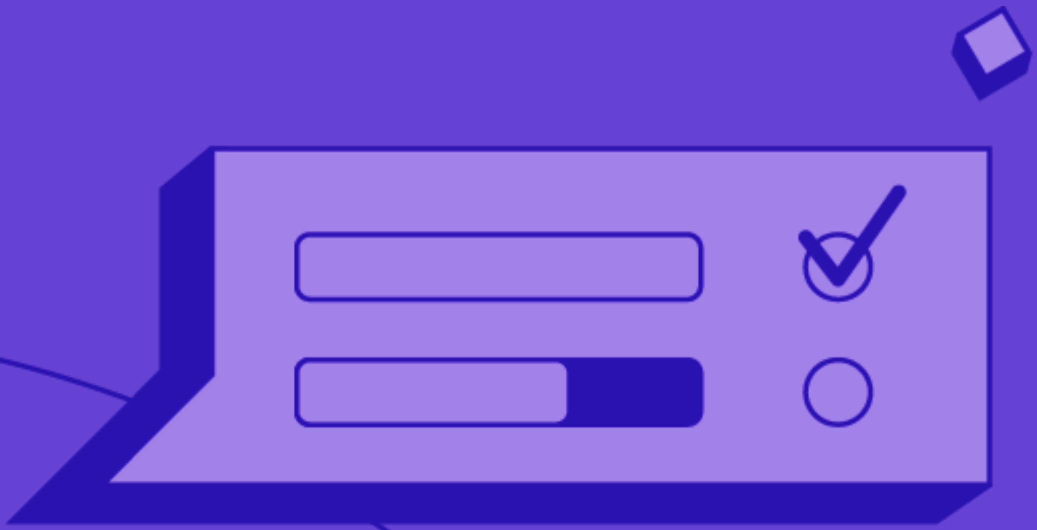
ATTACKIQ



Case Study

Protecting the Reputation of a Top-Tier Historically Black College: Morgan State University and AttackIQ

As one of the nation's premier historically black colleges (HBCs), Baltimore-based Morgan State University is dedicated to preparing diverse and competitive graduates for success in an interdependent global society. One aspect of preparing graduates to take on the world is keeping the school's 7,000 students, as well as its 2,000 faculty and staff, safe. That task has become increasingly difficult as Morgan State's reputation for research has grown.

"Like every organization around the world, we face threats such as phishing and spamming from small-time attackers," says Paco Rosas-Moreno, the university's chief information security officer (CISO). *"But we also talk about becoming a Research 1 [very high doctoral research activity] institution, and putting it out there that we are doing that level of research expands the attack surface in terms of the types of people who want to gain access to our data."*

> *"Morgan State University is a national treasure. Having the AttackIQ Security Optimization Platform improves our ability to protect Morgan State and make it safer than it is today."*
>
> – Paco Rosas-Moreno, CISO,
> Morgan State University

Rosas-Moreno says two threats keep him — and every other CISO in higher education — up at night. The first is ransomware. *"I saw one estimate that ransomware attacks in the education sector increased by more than 380% from Q2/2020 to Q3/2020,"* he says. *"Attackers are changing their TTPs [tactics techniques, and procedures] and getting more sophisticated. Once they infiltrate a network, they're moving slowly, taking steps such as erasing or corrupting backups."*

The other insomnia inducer for Rosas-Moreno is data security. *"That is particularly top-of-mind here in Maryland right now, since the state discovered hundreds of millions of dollars in fraudulent unemployment claims,"* he explains. *"It's important for institutions like Morgan State to monitor security to provide assurances to our internal audit team and to state auditors. We also need to be able to tell our employees and students, 'We know your data is secure because we're constantly testing.'"*

Security Assurances Needed, but at a Reasonable Cost

The Morgan State security team was already using a well-designed process for risk assessments that they based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The team categorized all areas of its IT infrastructure, determining what controls should be in place. Then it leveraged solutions designed to provide those types of controls. However, it was missing a process for routinely validating that the controls it had put in place were working.

CUSTOMER

Morgan State University

LOCATION

Baltimore

INDUSTRY

Education

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Control Auditing
- Investment Decision Support
- Compliance Mapping
- Security Pipeline Validation

BUSINESS IMPACT

- Improved security-investment decisions, based on evidence of security gaps
- Confidence among university leadership that the network is secure
- Assurances to students, faculty, and staff that their data is effectively protected
- Streamlined Cybersecurity Maturity Model Certification (CMMC) compliance, through demonstrations of security control effectiveness

Rosas-Moreno has a great deal of experience implementing security controls and performing penetration testing, so he understands the value of both validating the university's controls and proving that they are functioning as they're supposed to. *"Leadership always wants assurances that systems are secure and the security team is doing what we need to do,"* he says. *"I feel it's almost a disservice when a security program is doing the right things in terms of securing systems without also providing the ongoing assurance to leadership they are meeting those controls."*

His challenge was that he did not have the budget to dedicate a staff member to red team testing full-time nor to hire external experts to run continuous penetration testing. *"The average cost of a pen test can be anywhere from $10,000 to over $100,000, depending on details of the engagement,"* Rosas-Moreno says. *"And that's just a one-time event. Like a lot of universities, we were struggling with how to validate all our controls."*

He and his team set out to select and deploy a tool that would automate penetration testing. "*We were looking for a breach and attack simulation [BAS] solution that would attack our network components in a controlled fashion,"* Rosas-Moreno says. *"We needed the tool to essentially provide penetration testing as a service because we do not have the staff resources to manage the process on a regular basis."*

The Goldilocks of Breach and Attack Simulation

Morgan State considered several BAS solutions. It researched its options extensively, through both conversations with vendors and live demos. The university found that some of the products in this space had such a steep learning curve that it would require more staff attention than Rosas-Moreno could afford. Others required a significant resource commitment just in the upfront installation and configuration. Some covered network-based attacks but not web applications. Others tested only specific types of environments.

"Many of the solutions that were automated failed to cover all the bases we need here at Morgan State," Rosas-Moreno reports. *"The AttackIQ Security Optimization Platform allows us to automate tests that provide actionable results across all the different platforms that the university has to support. It does so without requiring too many resources, given the size of our security staff and their other obligations. It was neither the most expensive option we considered, nor the cheapest, and it doesn't require as much work at startup as most of its competitors. For what we need, AttackIQ fits the bill."*

Use Case 1: Effective Security Control Validation

Just after Morgan State selected the AttackIQ platform, COVID-19 sidetracked the project. "*We've been totally focused on adapting the university to operating in the new and constantly changing environment,"* Rosas-Moreno says. "*We are still working on integrations with our security infrastructure."*

Nevertheless, he says, *"my team is so excited about this tool. It's going to enable us to validate and verify the effectiveness of the controls we have in place, and also to understand any weaknesses in our environment."*

When the platform is fully deployed, Rosas-Moreno and his team will use it to close the testing gap in their existing risk assessment process. Then they will map the controls implemented through those risk assessments to the MITRE ATT&CK framework. *"We will validate the controls we have in place, and we'll expand the testing to see whether there are any significant risks we aren't effectively protecting against,"* he says. *"If we have concerns in any area, we will use AttackIQ to open up that can of worms and see how much of an issue we really have.*

"The AttackIQ platform will provide a lot of value to our security program," he adds. *"We will have evidence that our IDS [intrusion detection system], IPS [intrusion prevention system], and endpoint solution are working great. Or, if they're not, we'll know that too — and before the bad guys discover it, so we will be able to fix the problem. We are looking forward to leveraging the platform to find any shortfalls in our security controls."*

> *"The AttackIQ platform will provide a lot of value to our security program. We will have evidence that our IDS, IPS, and endpoint solution are working great. Or, if they're not, we'll know that too — and before the bad guys discover it."*
>
> – Paco Rosas-Moreno, CISO,
> Morgan State University

Use Case 2: Compliance Considerations

The AttackIQ Security Optimization Platform can also provide evidence of how an organization's defenses comply with specific compliance requirements, serving as not only a security control validation platform, but also a compliance validation platform. If and when Morgan State University learns that it needs to be compliant with DoD's Cybersecurity Maturity Model Certification (CMMC), for example, the team will use AttackIQ to validate compliance effectiveness.

Some of Morgan State's research projects may ultimately require CMMC audits. This means the university's cybersecurity practices would need to follow the best practices of the NIST framework, from identifying risk and developing appropriate infrastructure protections to detecting threats, responding, and recovering.

"Every system affected by CMMC requires specific controls and validations, and a lot of systems could be in scope," Rosas-Moreno explains. *"If you get contact information through an email, that email system has to be in CMMC. Your contracting system is in scope because it contains contract numbers. We've put proper safeguards in place to keep CMMC projects isolated. But we're very fortunate that our university leadership has the foresight to give us the means to strengthen our security technologies."*

Use Case 3: Validation of Security Investments

Rosas-Moreno also intends to use the AttackIQ platform to prove the value of individual security tools, and of the security function as a whole. *"When we mimic an attack,"* he says, *"the platform will show the role of each of our security tools in response. That will demonstrate the value of our investment in those solutions."* At the same time, for any holes the platform identifies, Rosas-Moreno and his team will have proof that their infrastructure requires a new security solution.

"After a test that reveals a security gap, we will explain to the executive leadership team what we've done and what we saw," Rosas-Moreno says. *"We will point out the gaps and shortcomings we currently have in our program. We will describe our roadmap for getting better. And they will see that we're not just managing security for the purposes of compliance, but in a way that's meaningful and protecting the data."*

Most important, he continues, *"we will use the AttackIQ platform to show the value of our cybersecurity program overall. We will be able to answer a lot of the questions from our executive leadership, such as: 'What's the status of our security controls?' And 'how are we doing with cybersecurity?' Being able to give them that ground-level truth is going to speak to everything that we're doing with the Morgan State security program."*

> *"We will use the AttackIQ platform to show the value of our cybersecurity program. We will be able to answer questions from our executive leadership. [Giving] them that ground-level truth is going to speak to everything that we're doing with the Morgan State security program."*
>
> – Paco Rosas-Moreno, CISO,
> Morgan State University

Conclusion: Better Cybersecurity Helps Preserve a National Treasure

At the end of the day, Rosas-Moreno says, his team's implementation of the AttackIQ platform enables it to better protect the brand and reputation of the university.

"We will see the results that an actual attack would generate, but in a controlled situation," he says. *"We will see how fast our incident response team picks it up. We will be able to make sure all our technology is working properly. If we find indicators of compromise, we will record those in our playbook and respond before they result in a real-world data breach."*

He compares the AttackIQ platform to a doctor's diagnostic tool. It will show the team problems with the health of the security environment and will help them determine treatments to solve those problems.

"Morgan State University is a national treasure, and we're going to continue to educate leaders who will make a difference in the world. That's something we are proud of," Rosas-Moreno concludes. *"Having the AttackIQ Security Optimization Platform improves our ability to add value to the university and help make Morgan State an even better place than it is today."*

ATTACKIQ

U.S. Headquarters
2901 Tasman Dr. Suite 112
Santa Clara, CA 95054
+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 Engenuity's Center for Threat Informed Defense

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.