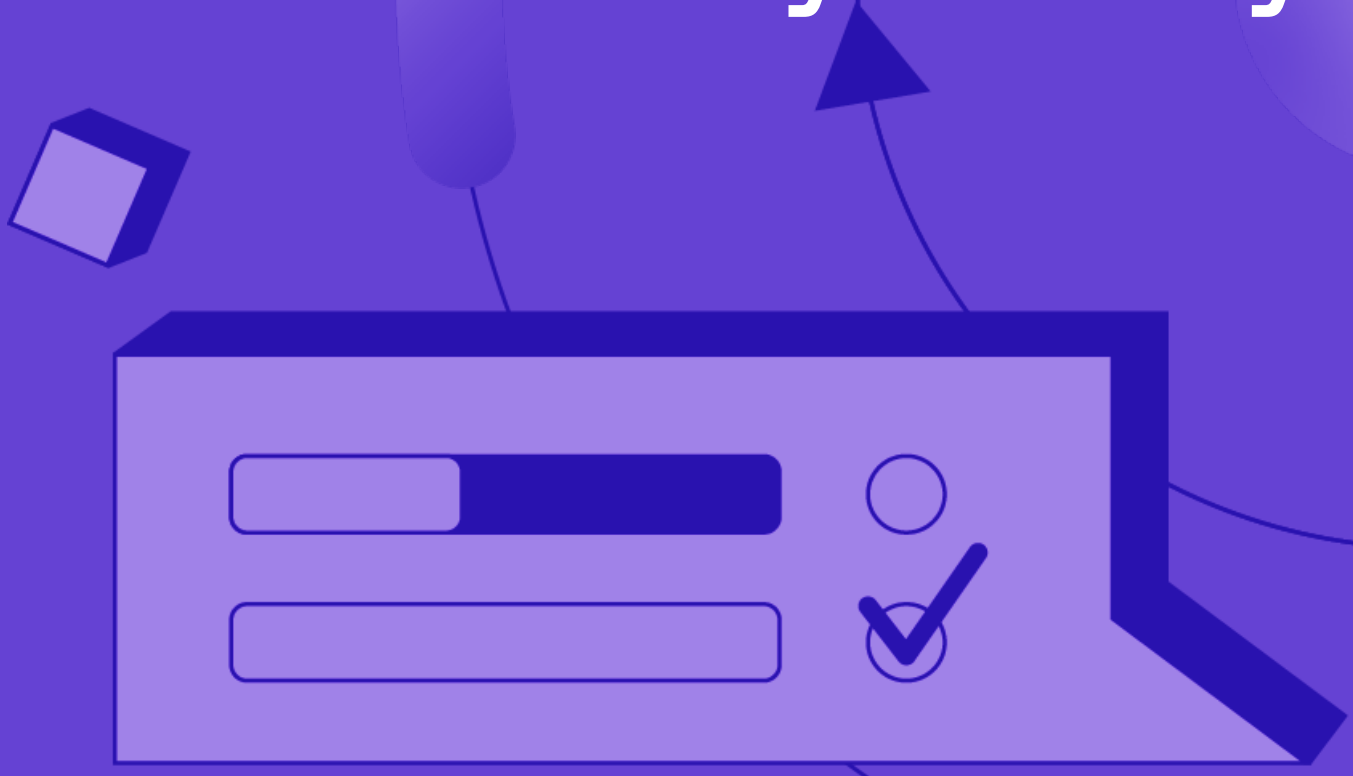
ATTACKIQ + ISS

Case Study

ISS World Services A/S, One of the World's Leading Facilities Management Providers, Finds Efficient Road to Security Visibility



For multinational corporations, facilities management can present significant challenges. These tasks are usually tangential to business success, yet they may draw management attention away from activities that are true competitive differentiators. Alternatively, without effective oversight, operations crews within globally dispersed offices and factories may miss opportunities to improve efficiency. That's why many of the world's most successful organizations turn to ISS World Services A/S.

ISS World Services A/S is a specialized facilities management provider with 430,000 employees spread across five continents. Its offerings range from cleaning and catering to such diverse services as maintenance of nuclear power plants, design of office interiors, and optimization of buildings' carbon dioxide emissions.

The company places a premium on IT security, and ransomware has recently emerged as a top concern. *"Our customers include some of the largest companies in the world, and many operate in sectors that are constantly under threat, like defense contractors and data centers,"* says Mark Kuhre Jensen, global information security manager at ISS World Services A/S.

> ***"The AttackIQ platform greatly accelerates the threat mitigation process. Instead of waiting a month for a penetration test to be completed, we can do it all in one combined workshop. It saves time and money."***
>
> – Mark Jensen, Global Information Security Manager, ISS World Services A/S

"If an attack on our systems shut down operations at a customer location, there would be enormous impacts. So, our aim is to integrate security into everything we do and to be the most secure facilities management company in the world."

A Change of Security Direction

Until 2020, dozens of largely independent teams handled day-to-day security management throughout the various business units of ISS World Services A/S. Then the company experienced a malware incident that led management to transform its strategy.

The company ended up restructuring its security function. Corporate leaders established a centralized internal security operations center (SOC) to handle incident response and began consolidating security responsibilities for the various business units within a handful of regional teams. They also rapidly grew the global information security team, based in Denmark, and tasked that group with establishing a baseline for security standards companywide.

CUSTOMER

ISS World Services A/S

LOCATION

Denmark

INDUSTRY

Facility Management Services

HIGHLIGHTED SOLUTION AREAS

- Automated Security Control Validation
- Investment Decision Support
- Mergers and Acquisitions

BUSINESS IMPACT

- Provides business-case support for needed security investments
- Confirms the value and success of solutions post-investment
- Accelerates time to mitigation for identified security gaps
- Improves decision-making around IT integration of acquisitions
- Confirms IT changes to accommodate organic growth do not create security vulnerabilities

"Now that the SOC takes care of security incidents, our team can focus on enacting architectural principles and response capabilities," says Martin Petersen, chief information security officer (CISO) of ISS World Services A/S. As the group mapped their path forward, they knew they needed more frequent and consistent penetration testing. *"When we build a capability, we shouldn't assume that our systems are secure,"* Petersen says. *"We need to go in and actively test them."*

The team projected that they would need to add two pen testing specialists to adequately increase the frequency and scope of their manual security-control assessments. However, breach and attack simulation (BAS) software offered a more cost-effective solution. *"We saw the opportunity to automate and run all sorts of attacks and techniques through it,"* Jensen says. *"We knew we could dramatically improve visibility into our security effectiveness, and be more efficient with our team resources."*

> ***"AttackIQ enables us to be more strategic with our security investments. What should we implement next to drive down risk? Automation is a smarter way of answering that question than manual pen testing because it reduces the cost of testing and increases the thoroughness of assessments."***
>
> – Martin Petersen, Chief Information Security Officer (CISO), ISS World Services A/S

ISS considered several options. A key criterion in the selection process was tight integration with the company's Microsoft security stack. *"Among the BAS solutions that Microsoft listed as officially integrated with its solutions, the AttackIQ Security Optimization Platform was the most mature,"* Petersen says. *"In addition, AttackIQ provided the best service throughout the sales process, which gave us confidence in their ongoing support."* The choice became indisputable when ISS ran proofs of concept for the platform on its shortlist.

"One of the other leading competitors had a vision of running tens of thousands of scenarios that are actual malware samples," Jensen says. *"That was a real pain for the people who had to resolve 20,000 alerts. And when you have that many different scenarios, you have to just look at the percentages. You might see 80% effectiveness in one area and think that seems pretty good, but the 20% of tests that weren't successful might indicate critical gaps. It made a lot more sense to us to run scenarios that are much more targeted to our specific needs."*

Step-by-Step Simulations Highlight Vulnerabilities

The global information security team rolled out the AttackIQ Security Optimization Platform, beginning with identifying all of the types of malware that the company had encountered in the past. They cross-referenced these threats against the comprehensive MITRE ATT&CK framework, created by the nonprofit MITRE Corporation, and broke each down into the discrete tactics, techniques, and procedures (TTPs) required to bring the attack to fruition. Next, they built simulations to pinpoint any vulnerabilities in their systems.

In one case, the team profiled a ransomware actor and created a series of scenarios that, in aggregate, mimic the ransomware actor's standard mode of operation. *"We built 150 custom scenarios in total, which was easy to do in the AttackIQ platform,"* Jensen reports. *"Then we created simulations to run against our systems. From that, we came to conclusions about how likely that particular ransomware actor was to succeed in an attack."*

Petersen emphasize that leveraging the MITRE ATT&CK framework helps the company accurately assess risk at each stage of a prospective attack. *"We might see, hypothetically, that we're good on protecting against 'initial foothold' with a particular type of malware, but we are not doing well in protecting data on a certain type of device from being exfiltrated. We can use that information to understand what we need to change. Maybe we see that we are preventing the first five steps of the attack, so it's unlikely that an attacker will get to the sixth step, where we might have a gap. Using the MITRE framework to break down attacks like this helps us decide where to invest additional resources."*

When the global team finds a security issue, they sit down with the appropriate regional security organization to work on mitigation. Whether the solution is investment in a new security tool, process update, policy change, or staff education, once it's implemented, the global information security group retests the security control to be sure it's performing as expected.

"AttackIQ greatly accelerates the threat mitigation process," Jensen says. *"Instead of building a solution, then ordering a penetration test, waiting a month for it to be completed, and turning to the blue team to resolve any remaining issues, we can do it all in one combined workshop. It saves time and money."*

Better-Informed Security Investment Decisions

Automated control validation has revealed vulnerabilities that the company was not previously aware of, enabling the company to transition away from certain managed service providers whose security was not up to ISS World Services A/S standards. In one case, Jensen reports, a business unit was relying on a hosted endpoint detection and response (EDR) solution. A third party had tested the control and provided a written report stating that it was secure, but AttackIQ revealed troubling security gaps.

> ***"It helps me provide detailed reports to the C-suite, the board, and auditors to create transparency around our return on investment as a corporate security function."***
>
> – Martin Petersen, Chief Information Security Officer (CISO), ISS World Services A/S

"Even internally, we have made some eye-opening discoveries," Jensen says. *"For example, we ran some scenario templates on different servers and operating systems to see what would be prevented and what would get through, to make sure our security controls perform the same on all systems. We were surprised to see how much difference there was among systems, even between different versions of Windows Server. AttackIQ makes those types of comparisons easy."*

The global information security team now performs continuous validations of the company's most important controls. They use the results of these tests to support the business case for needed security upgrades.

"AttackIQ enables us to be more strategic with our security investments," Petersen says. *"What should we implement next to drive down risk? Automation is a smarter way of answering that question than manual pen testing because it reduces the cost of testing and increases the thoroughness of assessments. It plays a crucial role in our security investment decisions."*

Attack Simulations: Trust but Verify

In addition to tuning and optimizing internal security controls, the Security Optimization Platform is playing a crucial role in ISS mergers and acquisitions (M&A). *"When we are going to acquire a new company, we can use the AttackIQ platform in the due diligence process,"* Petersen says. *"Testing controls in the target company before the deal closes enables us to understand their security hygiene. Does it make sense to integrate our security systems, or should we plan on fully absorbing them into our infrastructure because their current environment is just too risky? AttackIQ helps us make those decisions."*

Previously, the company would occasionally perform one-off integration tests on M&A targets, Jensen says, *"but there were a lot of things we simply couldn't test because doing so was too time-consuming. We might run a manual breach simulation at the OS level on a sample workstation and server. But otherwise, we might be relegated to reading their best-practice documentation and trusting that what they were doing was working."*

Petersen sees similar benefits as the company grows organically, moving into new geographic or service areas. *"As our IT strategy changes, we can utilize AttackIQ to make sure that our architecture will continue to work from a security perspective,"* he says.

> ***"There are still a lot of things that keep me up at night, but I am sleeping much better now than I did before we started working with AttackIQ."***
>
> – Martin Petersen, Chief Information Security Officer (CISO), ISS World Services A/S

Finally, the AttackIQ platform gives the global information security group proof of the success of the company's security investments. *"We're able to use it to document that our security stack and the processes around it are working as intended,"* Petersen says. *"It helps me provide detailed reports to the C-suite, the board, and auditors to create transparency around our return on investment as a corporate security function."*

"There are still a lot of things that keep me up at night," he concludes, *"but I am sleeping much better now than I did before we started working with AttackIQ."*

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.