XM Cyber | Case Study

Insurance

XM Cyber & IQUW: Focusing Effort Where it Matters Most

The Challenge

Traditional Vulnerability Management Can't Address Today's Challenges

As Group CISO of luxury re-insurer IQUW, industry veteran Stephen Owens knows it's impossible to fix all issues that could put a business at risk. Together with his expert security team, they employ a risk-based approach to fixing what matters most, and understanding where to concentrate remediation efforts. They used traditional approaches to Vulnerability Management, but all failed to provide the prioritization they needed to focus resources. "I've got a lot of experience in vulnerability management in different programs and it's very old fashioned. It strangles a business and IT to go to the old ways of 30, 60, 90 days. It's not the correct way for the business and handling their risks," says Owens.

The Solution

Seeing Immediate Value

Owens heard about XM Cyber hiking across the African desert. "I discovered XM Cyber in my wilderness period, had some demos and realized it's a great asset and capability to have in your armory. So as I landed at IQUW, I knew XM Cyber was going to help me focus where to spend our efforts. As soon as possible, I reached out and it really has landed well for us and helps us focus on the teams' particular efforts," says Owens.

The decision to implement XM Cyber came after extensive market research and consultation with industry peers. The selection process included a successful proof of concept that demonstrated immediate value, particularly in identifying previously undiscovered exposures in client-facing assets. "Six weeks in, there was a moment on one of our client-facing assets. We found an exposure where other security tools hadn't discovered it and XM Cyber had." This experience helped solidify their decision and they deployed the platform across their ecosystem. The implementation was notably smooth, with fast adoption facilitated by alignment with existing security concepts and strong API integration capabilities.

IQUW

Industry:
Insurance

Employees:
250-500

Speciality Reinsurance operating within the Lloyd's Market in London, with additional operations in Bermuda and a general insurance division focusing on luxury cars.

Knowing that not everything can be fixed, they seek to focus efforts where they matter most. A data-first company, IQUW manages 15+ lines of business, including property and cyber reinsurance. Their operations are built around making swift, data-driven decisions in partnership with brokers and business partners.

Read the Case Study ▶

Context Based Understanding

Owens and team found that with XM Cyber, they could actually understand how exposures interconnect from a cyber threat perspective. Using multiple threat feeds to enrich assets based on the crown jewels, XM Cyber helped them take their context-based understanding to the next level. "XM Cyber for me and how it can give you information of assets and what you have, is not just about vulnerability management – it goes a lot wider," says Owens. The attack graph capabilities enable his team to filter out false positives from theoretical exploitability and focus on what's truly exploitable and high-risk in their environment.

"A hidden gem of XM Cyber is the quality of their remediation advice and depth of analysis. And I've used lots of the top three tier vendors of vulnerability management tools and their level of remediation advice. With XM Cyber there's often two or three different options of how to remediate it. (We can) literally just transplant all of that information to our IT colleagues and they feel enabled straight away. It doesn't require a security engineer to constantly translate it. It makes us a lot more efficient in the security team.'

"It's a very good, universal tool, giving you a barometer of your internal estate. It really does lower risk appetite for us."

Much More Than Vulnerability Management

According to Owens, XM Cyber distinguishes itself by going beyond traditional vulnerability management, offering comprehensive visibility across Windows and Linux environments without requiring server reboots for deployment. The system provides crucial context for vulnerability prioritization, identifies credential issues and misconfigurations, and offers 24/7 red team-like monitoring.

The team also uses the External Attack Surface Monitoring capabilities, including dark web surveillance and threat feed integration, "The depth of thinking and the quality in this one particular area besides doing the standard attack techniques is they are listening for credentials on different telegram channels, dark web channels, marketplaces and correlating it to your environment. That's very powerful. We could achieve it elsewhere with different threat tools, but it provides that automation."

"When I saw the compelling moment of that time to value, that was it. I didn't prolong the proof of concept. We just adopted it and have been using it since."

The Results

Quantifiable Risk Reduction

XM Cyber has helped Owens and his team significantly reduce costs. "It's probably saved over 70% of a classical IT remediation program. There are monetary terms from a salary perspective, but the hidden benefits are it's freeing up those individuals if we're going through a digital transformation to focus on other business processes, which generate a higher revenue. So on the face of it, yes, you're saving approximately 70% of cost. But in actual fact, there's a larger business benefit. You're enabling other team members to do other business-focused activities as well. So there are some big benefits from a cost saving perspective and revenue generation perspective."

Lowered Risk Appetite

But equally, says Owens, "it lowers risk with choke points, where multiple attack paths come together – And if you nip that bud in, it makes it very difficult to perpetuate that attack down the chain. So, really it does lower that risk appetite for us…. XM Cyber really helps us on the metrics and to define that resistance." This is because addressing choke points enables teams to cut off multiple pathways to damaging attack paths at once.

Better Demonstration of ROI

The company faces ongoing challenges in quantifying security investments and optimizing resources during digital transformation. They've addressed these challenges through a structured approach to risk management, using tools like the FAIR framework and XM Cyber's capabilities to provide concrete metrics for security investment decisions. This approach has enabled them to better demonstrate ROI for security initiatives and make more informed decisions about resource allocation.

Looking forward, they continue to balance security requirements with business efficiency while managing a diverse IT infrastructure. The implementation of XM Cyber has positioned them well to address these challenges, particularly through its industry-first capability to correlate external attacks with internal vulnerabilities. The strong product roadmap and vision suggest continued advancement in security capabilities, maintaining their competitive advantage in the security solution space.

"I would recommend it to fellow CISOs….Once you have XM Cyber in your environment, once you see the problems, you can't unsee it. That's very powerful. And you can't turn a blind eye. So it's like a red team in a way, 24/7, not just looking at vulnerability management. It goes a lot wider than that, for example, on credentials, misconfigurations. And it really helps security and wider IT teams to focus their efforts and it reduces the time spent in the return on investment a lot faster."

> **"Once you have XM Cyber in your environment, once you see the problems, you can't unsee them. That's very powerful. And you can't turn a blind eye to that."**
>
> Stephen Owens, CISO

> **"I think they have the right vision.....you can see that clarity of vision on XM Cyber. So I feel I am backing the right horse."**

70%
reduction in remediation costs

6-week
implementation to value

24/7
automated security monitoring

Multiple remediation options per vulnerability/ exposure