CASE STUDY

Lighting the Way with Intelligence: Elexon Gets Ahead of Threats with Recorded Future

National financial reconciliation provider uses Recorded Future Intelligence Cloud to protect brand reputation and proactively manage risk to the energy infrastructure

Use Case:

Using the Intelligence Cloud to proactively understand risk and prioritize mitigating actions in day-to-day company defense, brand and supplier protection operations, and business transitions such as cloud migration and BYOD adoption.

Challenge:

Understanding risk from domains, credentials, supply chain, compliance mandates, and global threats to the energy industry, and taking mitigating actions after risks are identified

Solution:

The Recorded Future Intelligence Cloud, including:

- Brand Intelligence
- Threat Intelligence
- SecOps Intelligence
- Vulnerability Intelligence

Outcomes:

- Visibility into threats previously undetected through targeted monitoring and alerting
- Proactive approach to understanding risks involved in IT and business transitions such as cloud migration and BYOD adoption
- Protection of brand reputation across the nation's energy ecosystem
- Maintains compliance with ISO 27002's threat intelligence mandate
- Delivers actionable intelligence to SOC analysts, suppliers, and company stakeholders

Illuminating Risk Keeps Defenders a Step Ahead

Elexon plays a vital role in the UK's energy industry, administering the nation's Balancing and Settlement Code (BSC) that governs financial reconciliation between electricity providers. Information Security Manager Stuart Toner credits the Recorded Future Intelligence Cloud with helping to secure the company by enabling the team to effectively identify and prioritize threats that jeopardize Elexon and the energy industry, understand their third-party and brand risks, and maintain compliance with ISO 27002 controls.

"Before we brought Recorded Future on, everything we did was highly manual," Toner recalls. "We spent a lot of time checking news feeds on Twitter and in various other places, and it was easy to miss something important. They've given us an early warning system that we didn't have before. Now, through intelligence-led security enabled by Recorded Future, our team has been able to be much more proactive in our approach."

Intelligence to Prioritize Risk

Threat, Brand, and Vulnerability Intelligence equip Elexon analysts with actionable insight to prioritize cyber risk and streamline security operations. "We don't have an unlimited cybersecurity budget so Recorded Future is very useful in helping to maximize the resources we do have available," says Toner. "The intelligence we get makes us aware of things we wouldn't normally have knowledge about – like potential typosquatted domains – and gives us an early warning system to see where hacking groups are moving next and where we need to take action."

> **Before we brought Recorded Future on, everything we did was highly manual. We spent a lot of time checking news feeds on Twitter and in various other places, and it was easy to miss something important. They've given us an early warning system that we didn't have before."**
>
> *Stuart Toner,*
> *Information Security Manager at Elexon*

While helping them prioritize the most dangerous and most likely threats, Recorded Future alerts the team to wide-ranging potential risk from typosquats and malicious domain activity, mentions on code repositories, leaked credentials, and global threats to the energy industry. Timely insights allow Elexon's security team to anticipate and proactively avoid risk as the threat landscape changes, using intelligence to lead their security efforts and priorities.

"Recorded Future is our first 'go to' resource," Toner notes. "They provide us with targeted intelligence to the systems we actually have in place, and insights into the things we care about most."

Enhanced Vulnerability Management

Recorded Future's Vulnerability Intelligence keeps the Elexon team current on zero-day vulnerabilities and helps to assess potential when patches aren't available. Rich context on vulnerability disclosure and weaponization complements Elexon's existing vulnerability management capabilities to keep defenders aware of "threats in the wild."

Safeguarding Stakeholder Confidence – Monitoring Risk Across the Global Supply Chain

Elexon carefully protects its brand reputation to maintain the trust and confidence of the energy companies it serves — and help these retail and wholesale providers do the same. The task includes monitoring threats to suppliers that run services on its behalf and to the energy infrastructure overall.

Elexon takes an intelligence-led approach to monitoring risk associated with the third parties they do business with. "If we see that the risk associated with a supplier we work with suddenly goes up in Recorded Future, we can query the platform to drill down and see what may have happened." Toner explains. "Then we can reach out directly to the supplier to share our intelligence and ask about any issues."

Along with helping them monitor ever-evolving supplier risk, Recorded Future alerts Elexon analysts when credentials from suppliers suddenly appear on the Dark Web. The team also receives a suite of threat landscape and custom reports on threats to providers and the energy industry overall.

Custom Reports Drive Strategic Decision-Making

On a quarterly basis, Recorded Future's research team, Insikt Group, develops a threat landscape report for the Elexon team, which informs their leadership, including executives and board members, of threats to the industry and the company. "Hackers keep getting smarter and more professional with what they're doing," Toner reports, "Recorded Future lets us see trends, like ransomware-as-a-service groups like REvil coming up again and again, and that they tend to use the same kinds of mechanisms to access."

Elexon also relies on Recorded Future's custom reports to help inform the team on potential risks of both IT and business decisions. For example, Elexon recently employed Insikt's research as a key consideration when moving their company from corporate mobile devices to a Bring Your Own Device (BYOD) approach. Recorded Future provided a proactive look at the potential risks this move could subject the business to so that Elexon could get ahead of them and identify risk mitigating tactics. "The BYOD Report lets us see and understand the risks and put a plan in place to mitigate potential downfalls before moving forward," Toner says. "Now that we have that insight, we're considering adding resources to strengthen our endpoint management to support security with the BYOD approach."

Similarly, when Elexon made the decision to move their legacy systems to the cloud, they first called on Recorded Future to analyze the threats associated with the decision and prepare accordingly. This helped the team define its strategy for deploying monitoring and security controls throughout migration.

"As we go through the process, we're looking at how we can best mitigate any risk before it's at all exploitable," Toner explains. "The intelligence we get from Recorded Future gives us a proactive tool – rather than reactive – that helps our security operations center (SOC) build controls that plug holes in our infrastructure before someone can access it."

Timely Intelligence for Nation-State Threats

In light of recent global events, Elexon's team took great interest in threats arising from the Russia-Ukraine conflict and China's increased investment in global infrastructure. When Russia invaded Ukraine, Recorded Future's experts and thought leaders delivered timely threat briefings to help allay stakeholder concerns and provide clients with clear intelligence regarding where they should be spending their time and resources to address potential cyber and physical threats.

"When the invasion of Ukraine happened, the Elexon Board was quite anxious about potential attacks from Russia. Threat briefings and the Ukraine Resource center really helped the company understand what was going on in that uncertain time," Toner said.

> Recorded Future was the only solution that met all our requirements. It had everything we needed to give stakeholders advanced warning about threats."

Meeting ISO 27002 Compliance Standards

As industry standards and certifications globally begin to recognize the criticality of threat intelligence, ISO 27002 prescribes implementing threat intelligence controls with the overall purpose of "providing awareness of the threat environment that can impact the organization so that the organization can take appropriate mitigation actions." Recorded Future gives Elexon confidence that the ISO 27002 controls are in place to protect their organization and customers.

Putting Defenses to the Test

Along with proactive alerting on evolving external threats, Recorded Future's real-time monitoring always catches pen testing exercises and other internal tests that involve simulating threats like fake domains and phishing sites, Toner says. "Recorded Future picks up the typosquatted domains we create for testing purposes every time," Toner reports. "So far, they have a 100% hit rate." This gives the security team confidence that Recorded Future also sees and alerts on the important threats in the wild with high accuracy.

Why Recorded Future?

Before engaging Recorded Future, Elexon's cybersecurity team evaluated five potential vendors. "Recorded Future was the only solution that met all our requirements," Toner recalls. "It had everything we needed to give stakeholders advanced warning about threats." Noting that setting up the initial tech stack was easy, he adds, "It's very useful to be able to proactively monitor risk. It keeps us ahead of the game with threats coming down the line."