Case Study

Leading UK Energy Operator Achieves Mandated Compliance and Advances Innovation

> Without Gigamon, we would not see what we're seeing now. And that's a massive step forward for us.

MATTHEW, MBCS CITP CEIN
Cyber Security OT Engineering Manager,
Leading UK Energy Operator

Challenges

- Gaining complete visibility across the OT estate
- Feeding asset visibility and vulnerability management platforms with enriched data
- Complying with the NIS2 directive
- Adhering to the Cyber Assessment Framework (CAF) Enhanced Profile standard

Customer Benefits

- Heightened security maturity by achieving deep observability into devices on the network
- Gained visibility into vulnerable protocols for remediation
- Obtained observability into previously unknown assets to comply with the NIS2 directive
- Met asset, visibility, and vulnerability goals

Solution

- Gigamon G-TAP® M Series
- GigaSMART®
- GigaVUE HC Series
- GigaVUE-FM fabric manager

About Customer

Headquartered in the United Kingdom, this leading electricity distribution network operator (DNO) serves approximately 20 million people across 8.5 million homes and businesses in London and the regions known as the East and Southeast of England. The electricity distributor employs more than 6,000 people.

Cyber Security Operational Technology (OT) Engineering Manager, Matthew, leads a team of six within the overall cybersecurity team of 50. His team focuses entirely on operational technology, mainly on premises. He has been in the IT industry for 28 years—with 26 years specifically in the electricity distribution sector.

Business Challenge

The DNO is required to comply with Network and Information Systems (NIS) Regulations that originally went into effect in 2018 and were updated in 2022 to the NIS2 Directive. To help organizations adhere to the NIS2 directive, the UK's National Cyber Security Centre (NCSC) introduced the NCSC Cyber Assessment Framework (CAF), a resource that sets out principles and objectives within a systematic and comprehensive framework that organizations can use to assess and manage their cyber security. The CAF Enhanced Profile goes above and beyond the CAF standard for organizations facing elevated threat levels or operating critical national infrastructure.

To comply with the directives and standards, the organization requires to increase its visibility into assets, communications, and vulnerabilities across its entire OT estate. This demanded a solution that could feed its asset visibility and vulnerability management platforms with enriched data to provide a view into every single IP asset within its network.

Matthew explained that achieving the CAF Enhanced Profile would be a "massive challenge," but the organization has a vision and determination to complete the task by year-end—two years ahead of the expected 2027 deadline.

Resolution

Matthew led the deployment of multiple GigaVUE-HC1 devices across several locations at the electricity distributor, with both copper (UTP) and fiber cables. The technology is managed within GigaVUE-FM, which simplifies and automates the configuration, management, and operation of the Gigamon Deep Observability Pipeline.

Matthew described how the Gigamon team took him step-by-step through the design, implementation, troubleshooting, and upgrade processes. "I had a vision in my head of what was required, and I transcribed this into a diagram. Gigamon looked at this and offered back a design that exactly met my requirements with great attention to detail. It's probably one of the best engagements I've had with a technology provider. The enthusiasm and attention to detail was amazing," he emphasized.

"Before Gigamon, we knew roughly what assets we had on our network. But having deeper visibility into the network, where we can now see the amount and exact types of assets we have and what they're communicating with, enables us to make more intelligent and informed decisions," said Matthew.

Part of the deployment process involved integrating Gigamon with the organization's existing security and monitoring tools. Gigamon delivers context-rich, optimized network-derived telemetry to these tools so they can more efficiently detect and correlate threats across the organization in real time. GigaSMART applications, including de-duplication and header stripping, further reduce data volume, enabling tools to focus on the most relevant information for faster, more accurate threat detection.

Benefit

The result of the Gigamon deployment is deep observability into the organization's communications, assets, and vulnerabilities. Thanks to the data, the metadata, the network telemetry, and the network insights provided by Gigamon and the other security tools into which it feeds data, the organization has taken its security maturity to the next level.

Gigamon has allowed the DNO to meet its asset, visibility, and vulnerability goals, Matthew asserted. A key requirement of the NIS regulation is that organizations understand their entire asset estate and the protocols and communications on their networks.

"Gigamon feeds filtered, enriched data into our security tools, enabling us to see our assets, understand them, and get a view into the communications between them. It also gives us the ability to understand whether they're communicating over vulnerable protocols or whether they have vulnerabilities that need to be remediated," said Matthew.

One of the biggest benefits of Gigamon is how it helps Matthew and his team understand assets they didn't know about. "At least when you know about it, you can do something about it. If you don't know about it, it's a risk," he said. "Gigamon is helping us better manage risk and resolve issues more quickly and efficiently."

Gigamon is also helping the organization achieve its aim of meeting the CAF enhanced profile standards by the end of this year, two years ahead of the 2027 deadline. Matthew noted this would not be possible without Gigamon and the tools it integrates with: "Meeting the CAF Enhanced Profile is a massive step forward for us—and Gigamon makes it possible by getting us there so much faster."

As the DNO incorporates AI in its workflows and tools, Gigamon will potentially play a key role in securing AI innovation and usage. Matthew shared that the organization has just begun its AI journey, using the AI-powered reporting, queries, and detection capabilities built into its existing tools. With Gigamon securing the organizations environment, innovation can coexist with security and compliance.

Even though it's the age of AI, human nature doesn't change, Matthew pointed out. He shared an observation about how good actors sometimes attempt to do good things but end up creating problems without realizing it. "Engineers will always find ways around a problem, and they always look for the simplest solution. It may not be the best or the most secure, but they will find a solution," he explained. He pointed out that Gigamon helps him to track down these less-than optimal "simple" solutions and take corrective action.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

10.25_01