How AI is Protecting Norway's Energy Suppliers

As the energy sector undergoes a difficult balancing act between defending themselves from attack while maintaining business continuity, a unified approach to cyber defense across both IT and OT environments has never been more important.

At a Glance

- ✔ Protects more than 450 energy and utiltity organizations globally
- ✔ Self-learning AI which detects in-progress attacks
- ✔ Autonomously investigates, triages, and reports on all security incidents
- ✔ Provides complete visibility of RTUs and remote Operational Technology

DALANE ENERGI

SOGN OG FJORDANE ENERGI

GLITRE ENERGI

agder energi

One of the world's largest energy producers, Norway not only exports oil and natural gas but is leading the charge in renewables – with around 97% of the country's energy coming from hydro-electric power stations.

Over the past few years, energy providers across the board have faced some of the most advanced attacks as the industry's strategic importance grows. Of increasing concern is the threat posed by nation-state campaigns and advanced ransomware – with the fallout jeopardizing national security and the safety of essential personnel.

All this is happening against a backdrop of continued IT and OT convergence and advancing crime-as-a-service, with sophisticated threats such as machine-speed ICS ransomware increasingly in the hands of low-skilled mercenaries. As such, it has never been more critical to attain coverage and monitoring across the entire digital infrastructure.

Darktrace's Industrial Immune System is the only technology capable of autonomously detecting, investigating, and responding to novel and sophisticated threats across both IT and OT environments. Leveraging self-learning Cyber AI, Darktrace works by understanding what 'normal' looks like across every user, device, and controller, enabling the AI to identify the subtlest signal of threat – regardless of whether it appears on legacy tool deny lists or exploits novel zero-day vulnerabilities.

The Industrial Immune System provides complete visibility across OT, IT, and Industrial IoT (IIoT) in a single pane of glass, combining early stage threat detection with real-time asset identification and autonomous investigations, illuminating all points of IT/OT convergence.

Threats by Numbers

of organizations in the energy industry experienced a cyber-attack in the last 12 months.

$6.4 million is the average cost of a data breach in the energy industry.

"Phishing attacks are our biggest threat vector. Antigena Email has been crucial in catching the stealthy emails that slip through the net."

Kåre Teigland, Head of ICT, SFE

Glitre Energi Case Study

Glitre Energi is a renewable energy company that operates in power distribution, power production, and power sales in Norway. The company also has a technology division innovating digital power solutions.

Industrial Digitization Complexifies Security

Glitre prioritizes the digitization of its business, recognizing the benefits that technological transformation can bring. However, the composite equipment that makes up much of its infrastructure was not integrated with existing cyber security tools, leaving blind spots. The security team knew that to protect all of its environments, they needed a contextual, enterprise-wide approach to defense.

> "Digitalization and automation brings room for innovation to Glitre but it also makes us increasingly vulnerable to sophisticated cyber-attacks."

Kristine Salamonsen, ICT Security Consultant, Glitre Energi Nett

Cyber AI Illuminates Operational Technology

Before deploying Darktrace, Glitre lacked the visibility it needed into its OT network. It had an external SOC but no interface to use. Such poor visibility complicated the risk of rolling out digital transformation projects and extending supply chains, developments vital to fueling efficiency and providing a competitive organizational advantage. Additionally, when Glitre switched to Microsoft 365, it had issues with configuring old security tools to work with newer technologies – leaving gaps in coverage.

Darktrace's coverage extends to wherever users operate and data lives. Cyber AI provides Glitre with full visibility across their OT and IT infrastructure, with an award-winning user interface, the Threat Visualizer, graphically displaying the most important issues that the team needs to be aware of, having auto-triaged potential events of concern and alerts. The security team at Glitre are now able to achieve granular visibility into their organization at the subnet, device, and user level – ensuring their understanding of the threats facing the digital ecosystem is always up to date.

Infrastructure-Wide Protection With Cyber AI

On a daily basis, Glitre's security team use Darktrace to defend every corner of its cyber-physical ecosystem, looking at model breaches and threats from the corporate network, email, OT, and even employee devices. The security team are able to troubleshoot network issues with Cyber AI, thanks to the wealth of information Darktrace provides. Integrated to the Glitre Helpdesk, the team keeps the Threat Visualizer always open, able to view their entire organization from a single pane of glass and secure in the knowledge they have 24/7 defense across the digital business – protected against threats regardless of where and when they may strike.

> "With Antigena Email, we have seen a large decrease in spam. With the UI, we can see that it stops targeted and sophisticated email campaigns."

Kristine Salamonsen, ICT Security Consultant, Glitre Energi Nett

Sogn og Fjordane Energi Case Study

Sogn og Fjordane Energi (SFE) is an energy company that provides electricity directly to consumers. Headquartered in Sandane, Norway, SFE is made of up of several groups, including electrical, grid, marketing, hydro, and wind power. SFE's grid division is large, and it has a license to transmit electric power over an extensive area of the country. The organization has always had a strong focus on the integrity of its security, and with the Norwegian government mandating a specific set of regulations that energy providers must adhere to, including keeping data and resources secure, as well as assuring everyone in the area maintains reliable power, the company knew they need to leverage a technology that can autonomously detect and stop both known and unknown threats – no matter how sophisticated.

> "If we have a power outage or disruption, it would destroy our whole business model. Darktrace gives us peace of mind, we know Cyber AI is running 24/7 in the background, supporting us."
>
> **Kåre Teigland, Head of ICT, SFE**

Cyber AI Evolves Alongside Energy Infrastructure

SFE's traditional ICS security tools dealt with logs and traffic, requiring the security team to manually input responses to known threats; yet, they were blind novel attacks. The SFE security team turned to self-learning AI as a result; with its fundamental ability to learn 'on the job', it was a welcome divergence from traditional ICS solutions.

Cyber AI Put to the Test: Darktrace Proof of Value

SFE trialed Darktrace in a 30-day Proof of Value, installing and running Cyber AI in its own environment alongside existing security tools. During this time, Darktrace detected activity that bypassed all their other tools, including brute-forcing on an employee PC – a threat which was immediately flagged to the security team.

Antigena Email: The Self-Defending Inbox

Darktrace Antigena Email has repeatedly protected SFE from threats that would previously have slipped pass its legacy solutions. Traditional spam filtering only flags well-known phishing emails, with more stealthy and damaging attacks getting through. But with Antigena Email - the first technology to analyze email communications in the context of wider user behavior - targeted spear phishing, supply chain attacks, and other advanced email threats are stopped in their tracks – protecting SFE's dynamic workforce and workloads. Antigena Email has helped SFE stop TOR software as well as access to file sharing websites that go against company policy.

By learning 'on the job', Antigena Email is able to autonomously and accurately take action on emerging threats – without the need for human intervention. Only through its pervasive understanding of what 'normal' looks like across a user's digital footprint does Darktrace reveal seemingly benign actions to be malicious in the wider context of the business.