

PREPARING FOR CYBER ATTACKS

How Glitre Nett found the right intrusion detection system for their networks

Our StationGuard Solution has been recognized for its exceptional performance in a recent attack simulation conducted by Glitre Nett, the largest electricity distribution system operator (DSO) in the south of Norway. Our intrusion detection system (IDS) excelled by detecting complex threats, highlighting its robust capabilities and effective integration in critical infrastructure environments.

The devil is always in the details

In the dimly lit office room, Ozan sat at his workstation, surrounded by the rhythmic hum of computer fans and the soft glow of multiple screens. The atmosphere was tense as the team sifted through the data, deciphering the recent cyber attack.

Ozan's eyes flew across the information on his screen. At the same time, he reflected on recent critical infrastructure attacks—such as the Ukrainian power grid incidents and breaches of Danish energy suppliers. These events underscored a sobering reality: attackers were becoming increasingly sophisticated, particularly with control systems. He wondered if these attackers were inexperienced individuals exploring new attack vectors, professionals seeking financial gain, or the most dangerous of all—state actors with advanced capabilities and resources.

"Check this out," Christoph called tensely. Ozan approached his colleague's workstation. "See that?

This device isn't sending data as expected. We've got gaps," Christoph scrolled through the interface of the StationGuard IDS and quickly accessed the device overview. "Here and here, and some suspicious activities."

Ozan frowned, absorbing the information. "What suspicious activities?"

Christoph pointed to a series of red alert icons. "After reconnecting, it sent a Gratuitous ARP, trying to validate its IP address by broadcasting it across the network. It also attempted to connect to the DHCP server but used an automatically generated private IP address. Look at the MAC address."

"It looks like it tried to reconnect after it was disconnected."

"Exactly," said Christoph, excited about his discovery. "I'm pretty sure we've got a device replacement scenario here. The device was cloned and planted, then reconnected to the network."

"They know that new IPs entering the network would trigger an alert, but if they replace a device by spoofing the IP and MAC address ... many IDSs wouldn't pick up on that." Ozan sighed. "They needed physical access to the station. It's not easy, but not impossible either. It's particularly dangerous for these remote substations that are only visited once every few months. Let's take a look at all the devices this cloned device has been in contact with and find out if anything else might be compromised."

Christoph began going through the list out loud, "An exploited remote connection, a portable device plugged in by an unsuspecting employee, and now a physical attack ... Did you check the GOOSE messages?"

"That's easy," said Ozan as he smiled, returning to his workstation. "I'd rather you check out any unauthorized HTTP messages sent to the switches." Then he added, "I sure am curious what else Glitre Nett's engineers have in store for us with this attack simulation."





Innovative security

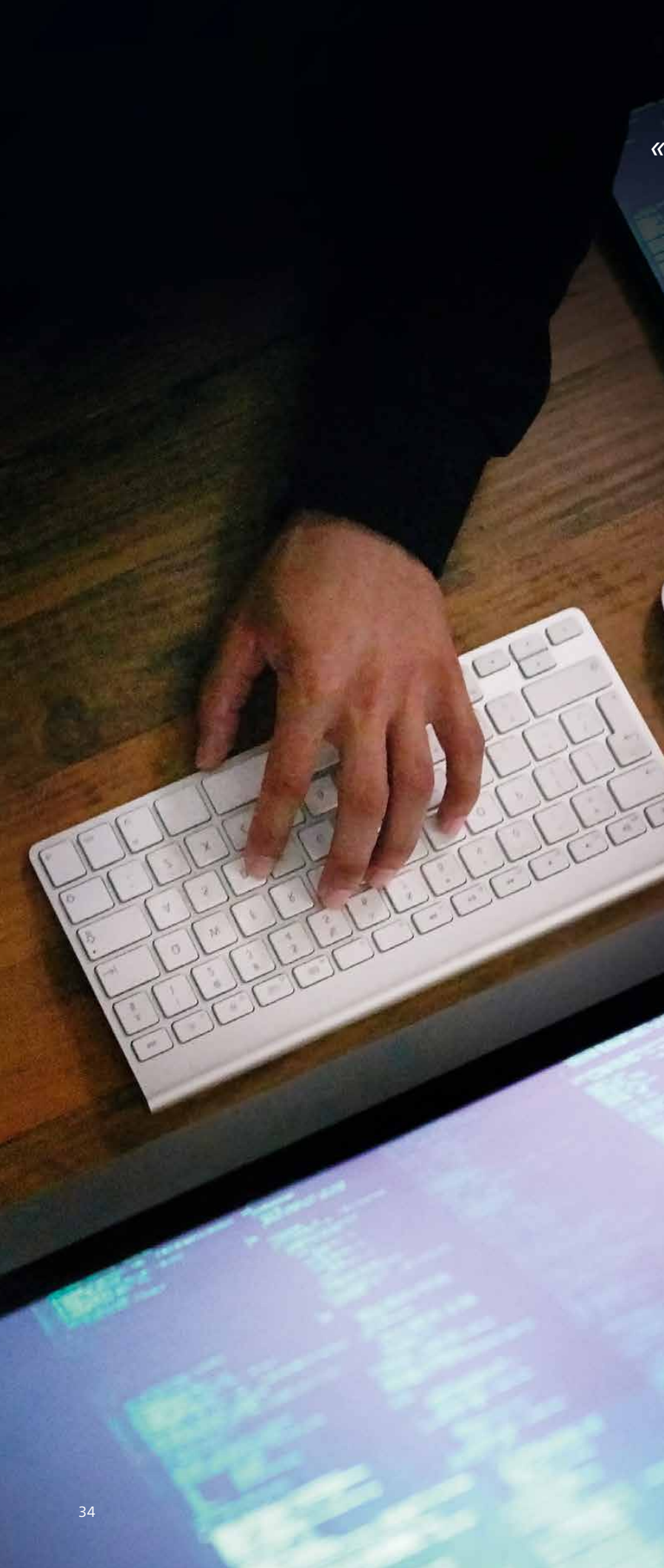
A similar scene has likely occurred during the attack simulation analysis, but let's draw back the curtain for this test. When it comes to an innovative approach to critical infrastructure, Glitre Nett, the largest DSO in Southern Norway, is recognized as a pioneer. Atle Ripegutu, the department head of Process Control at Glitre Nett, underscores the importance of this proactive stance: "For companies in critical infrastructure, innovation isn't just beneficial – it's essential. It's about being proactive and ready. If a major security incident occurs, the cleanup is a nightmare. Investing upfront may not be cheap, but it prevents much larger expenses further down the line."

To this end, Glitre Nett decided to test and evaluate IDSs by simulating real-world attacks within their live substations. This evaluation included solutions from multiple vendors. It evaluated the installation, configuration, and detection capabilities, the scalability and flexibility, the ►

**«If the grid goes down
for ten days, it's anarchy.
This project was about
preparing for critical
scenarios like these.»**



Vetle Norman,
System Engineer,
Glitre Nett



«They explored possibilities like an intruder leaving a disguised component or using an UDP trace route to discover the network topology.»

user-friendliness, the accuracy of alerts, the reporting, as well as the effectiveness of the support provided by each system.

Atle Ripegutu notes the unique challenges faced by substation networks compared to control centers: "Once you leave the station and use various protocols, much information is lost, making it difficult to monitor and secure the pipeline." With legacy codes, evolving IT needs, and the upcoming NIS2 directive being incorporated into Norwegian law, the demand for a comprehensive IDS solution is overwhelming.

After extensive evaluation, Glitre Nett selected our solution alongside those of two other candidates to participate in their attack simulation.

An attack simulation in a live substation

Glitre Nett was concerned about testing a running system, but they believed real-world scenarios offered the most accurate insights. Vetle Norman, a System Engineer at Glitre Nett explains the limitations of theoretical tests: "Research centers

«Given the critical nature of their infrastructure, even the most unlikely vulnerability required a thorough examination.»

ATTACK INDICATORS FOUND BY STATIONGUARD SENSOR

- › New IP and MAC addresses in the network
- › Illegal MMS interactions
- › Disappearing GOOSE messages
- › ARP spoofing
- › NetBIOS reconnaissance activity incl. UDP trace route, ping sweeps, and port scans

like EFA in Norway produce valuable theoretical case studies, but they often fall short of capturing the complexities of actual incidents. Real-world attacks unfold differently, and that's what we aimed to simulate."

Vetle Norman's team focused on recreating plausible intrusion scenarios and attack vectors in their operational substations. They explored possibilities like an intruder leaving a disguised component or using an UDP trace route to discover the network topology. Given the critical nature of their infrastructure, even the most unlikely vulnerability required a thorough examination.

Once each participant's system was installed and set up, all system access verifications were implemented, and operational stability was confirmed. Then, the systems ran autonomously for several months, gathering data and performing their assigned tasks before the test commenced.

Following the attack simulation, Vetle Norman requested a detailed analysis from each vendor, including recommendations based on their findings. "We needed to see how each IDS

performed under real-world conditions. Every storm tests the capacity of our control systems and breakers. The same applies to IDS. If nothing happens, you never know what it can detect," explains Vetle Norman. "This was OMICRON's exam. The results were insightful and helped determine our manufacturers' effectiveness and solutions."

Powerful IDS for detailed analysis

Between late 2022 and mid 2023, our StationGuard sensor was deployed in Glitre Nett's substation. The attack simulation test was conducted on two consecutive days, with all participating IDS providers unaware of the test's timing or attack scenarios. Glitre Nett only released the data they collected to each vendor after completing the exercise.

Our approach to data analysis is defined by a multi-disciplinary team. It includes OT engineers and protocol experts skilled in IEC 61850 and IEC 104 and is further enhanced by IT cybersecurity specialists. Fusing this knowledge is crucial for addressing a broad spectrum of security challenges. "Our dual expertise in power systems

and cybersecurity enables us to tackle complex issues effectively," says Cybersecurity Product Manager, Ozan Dayanc. "The collaboration between IT and OT is essential for robust incident response. It ensures informed decisions are made for alerts and incidents."

During the test, StationGuard and its central management system GridOps, collected critical data from Glitre Nett's network. Glitre Nett set up a remote connection to the StationGuard sensor that allowed us to obtain the system's configuration files, event logs, and packet captures (pcaps). We used these to analyze Glitre Nett's system communications, while GridOps helped organize the data into specific areas.

"This structured methodology enabled us to detect and categorize various potential attacks based on the patterns and anomalies we observed," explains Ozan.

"Initial analysis revealed common issues such as unauthorized devices, well-known attacks like TCP and UDP port scans, and ARP spoofing." Subsequent analyses focused on more sophisticated incidents, including physical and ▶

person-in-the-middle attacks. "After putting our findings together in a detailed report that we submitted to Glitre Nett, we were eager to find out how well we did," adds Ozan.

Attack simulation results

"After reviewing the results of the vendor analyses, OMICRON emerged victorious in the evaluation test. Their solution won by a landslide," asserts Atle Ripegut. StationGuard and the team not only detected 100% of the attacks and provided a detailed report with an accurate attack timeline but they were also the fastest team by far.

Vetle Norman's endorsement further underscores the success of our IDS solution: "I want StationGuard in all my substations," he declared. "It exceeded the capabilities of all the other IDSs. Firstly, the configuration process is surprisingly easy. You simply upload the configuration file, and it's ready to go. Secondly, merging devices is a seamless task. You can combine a

firewall, a switch, and a gateway into a single unit, which is perfect." He also highlights the intuitive user interface: "A system that can detect security incidents but requires lots of training and is difficult to use doesn't make sense for us operationally. The UI is straightforward, with simple commands for setting roles and communication paths, making working with it a joy."

Vetle Norman also praised StationGuard's dual-focus capabilities for system functionality and security: "StationGuard offers functionality analysis that other vendors can't provide. It fits perfectly, requiring minimal setup. It also integrates well with SCADA systems, RTUs, and signaling. From what I've seen, its level of integration and capability is unmatched."

Glitre Nett's feedback concluded with additional commendations for our service and customer engagement. Atle Ripegut remarked, "You gave an exemplary performance in every

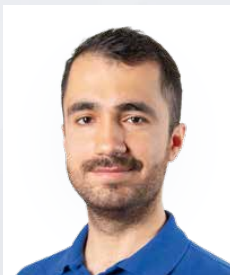
aspect of service—from handling equipment to on-site assistance. All inquiries were thoroughly addressed, and every issue was promptly resolved. The collaboration was exceptionally smooth, without a single problem remaining unresolved."

A promising future

The analysis of the attack simulation test underscores the critical role of an IDS for identifying cyber attacks. "By taking the testing out of the lab environment, the real comprehensiveness of an IDS solution can be properly evaluated," says Ozan. The evaluation demonstrated that many threats are detected accurately by an OT-specialized IDS like StationGuard, where even a single alert can potentially signal a serious attack.

Collaborating with Glitre Nett has been excellent. "We look forward to continuing our partnership and seeing where it takes us," says Vetle Norman. "We need your support and testing equip-

«It was a great experience for us. It verified our solution's capabilities and made us aware of our strengths and potential weaknesses.»



Ozan Dayanc,
Cybersecurity Product Manager,
OMICRON

GLITRE NETT


- › Founded: 2022 – merger between Agder Energi Nett (2000) and Glitre Energi Nett (1993)
- › Headquarters: Drammen, Norway
- › Employees: 350+
- › Electricity customers: 320,000+

 glitrenett.no

ment to manage the ongoing paradigm shift. In the cybersecurity space, we require the unique functionalities that your systems offer. We want to maintain a strong connection and keep you involved. We want to continue using your equipment in the future," he concludes.

Our solution demonstrated its efficiency to the Glitre Nett team. Yet, as always, there is room for improvement. "We have ambitious plans for the future," says Ozan. "We aim to refine our signature base detection, enhance network visibility, and introduce new security features. Enhanced asset inventory collection is also on the agenda. Beyond that, we're continuing to innovate and adapt to emerging threats." ■

If you'd like to learn more about our StationGuard IDS and vulnerability management, please visit our website at

 omicroncybersecurity.com/en/solutions



LISTEN TO THE PODCAST

Interested in this topic?

In this episode, we will learn how an OMICRON team of cybersecurity experts goes about analyzing incoming alarms and how even the smallest indicators can reveal hidden dangers that threaten the safety and operations of an entire system. Scan the QR-code or visit:

 omicron.energy/episode79

