Case Study

Preparing for Cyber Attacks – How Glitre Nett found the right intrusion detection system for their networks

GlitreNett

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.

Innovative security

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 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 seems almost overwhelming.

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

GLITRE NETT

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

https://www.glitrenett.no/

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 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.

"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

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 man-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 Ripegutu. 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."

SOME OF THE 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 scan

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 Ripegutu 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."

"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

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 equipment 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.

OMICRON is an international company that works passionately on ideas for making electric power systems safe and reliable. Our pioneering solutions are designed to meet our industry's current and future challenges. We always go the extra mile to empower our customers: we react to their needs, provide extraordinary local support, and share our expertise.

Within the OMICRON group, we research and develop innovative technologies for all fields in electric power systems. When it comes to electrical testing for medium- and high-voltage equipment, protection testing, digital substation testing solutions, and cybersecurity solutions, customers all over the world trust in the accuracy, speed, and quality of our user-friendly solutions.

Founded in 1984, OMICRON draws on their decades of profound expertise in the field of electric power engineering. A dedicated team of more than 1.250 employees provides solutions with 24/7 support at over 20 locations worldwide and serves customers in more than 170 countries.

For More **INFORMATION**

For a detailed overview of our products and services, additional literature, and contact information for our worldwide offices, please visit us at:

www.omicroncybersecurity.com
www.omicronenergy.com

or contact us directly via email:
info@omicroncybersecurity.com