FORTINET | OMICRON

SOLUTION BRIEF

Fortinet and OMICRON Holistic Security Solution

Tailor-made, In-depth, and Automated Solution for Optimal IT Security Thanks to Fundamental OT Understanding and Functional Monitoring of the Power Grid

Executive Summary

Fortinet and OMICRON combine their efforts to enable IT security officers and power engineers to achieve an unprecedented level of cybersecurity through cross-industry expertise. The solution features efficient alert analysis, immediate in-depth protection based on StationGuard's unique "allow list" approach, a user interface that enables efficient collaboration between IT and OT teams, and integration with Fortinet's Security Fabric for optimal security protection.

Challenge

In recent years, there has been an increase in the number of cyberattacks against critical control systems in production facilities and energy supply companies. Many utilities are therefore introducing processes to reduce the risk of cyberattacks. Until now, these measures mainly concentrated on IT networks. However, control centers, power plants, and substations also represent critical attack vectors. Consequently, the operation and maintenance processes of these systems must also be included in the cybersecurity risk assessment.

To ensure that the power grid is thoroughly protected against cyberattacks, the security strategy must address all levels. Security for the power grid extends from physical access control, through digital access monitoring, to the detection of suspicious or forbidden activities in the network. This requires systems that offer a high level of security with low maintenance effort in the long term. Moreover, they should be easily integrated into operational and maintenance workflows.

Joint Solution

OMICRON and Fortinet have partnered to deliver an industry-leading security solution to address these challenges. The first step is the integration of OMICRON's StationGuard into Fortinet's FortiSIEM. Through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, the integrated solution delivers efficient alert and in-depth analysis to detect and defuse safety risks in the power grid even before they occur. *StationGuard for FortiSIEM* identifies any type of protocol communication and protects the power grid through a unique allow list approach without requiring a learning phase. This efficient solution is combined with an easy-to-use interface for customers to react as quickly as possible on security threats.

Joint Solution Components

- Fortinet FortiSIEM
- OMICRON StationGuard

Joint Solution Benefits

- Effectively tracing alarms to real-world events in the power grid. These highly intelligent alert messages are directly available to security operations center (SOC) analysts to make the right decision immediately.
- FortiSIEM enables direct response processes and deeper analysis of StationGuard events in correlation with other messages. These are integrated in Fortinet's user and entity behavior analytics (UEBA) engine.
- OMICRON's OT expertise and know-how is anchored in the SOC. This results in improved visibility of OT threats in the enterprise and provides comprehensive protection against attacks on IT as well as OT.

FORTINET FABRIC-READY

Joint Solution Components

The Intrusion Detection System (IDS) StationGuard monitors Ethernet networks in control centers, power plants, and substations to identify cyber threats. Regardless of whether your system is based on IEC 60870-5-104, DNP3, Modbus TCP, or IEC 61850, StationGuard deeply inspects all communication to find potential threats, while documenting all assets and their protocols and services. Its deep knowledge of power utility automation systems even enables StationGuard to detect malfunctions in the monitored system.

Fortinet FortiSIEM brings together visibility, correlation, automated response, and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and even prevent breaches.

The FortiSIEM architecture enables unified data collection and analytics from diverse information sources, including logs, performance metrics, security alerts, and configuration changes. FortiSIEM combines the analytics traditionally monitored in separate silos of the security operations center (SOC) and network operations center (NOC) for a more holistic view of the security and availability of the business.

Joint Solution Integration

All StationGuard alarms—including its OT intelligence—are transmitted to FortiSIEM and collected in one place. Over 130 event types with their corresponding event type groups and an easy-to-understand dashboard help SOC analysts to secure IT and OT faster and more comprehensively.

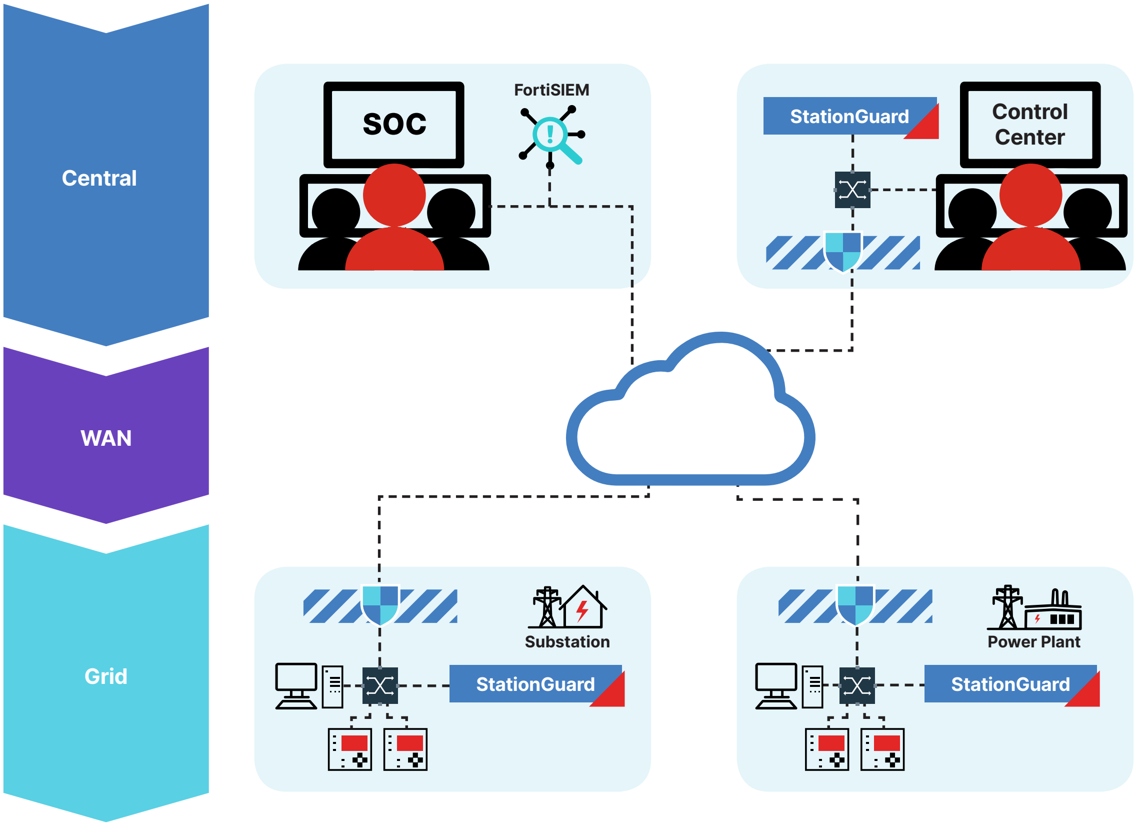

Figure 1: StationGuard network integration with FortiSIEM.

Joint Use Case

StationGuard for FortiSIEM delivers alert messages with all relevant OT information to the SOC-as-a-Service provider. This OT knowledge supplied by StationGuard combined with the capabilities of FortiSIEM improves the incident response speed for OT alerts and minimizes false positives.

New, specific rules, which have been prefabricated by OMICRON (e.g., for reporting man-in-the-middle techniques for OT control or normal TCP/UDP communication), help to quickly categorize and collect the events associated with the incident. This leads to faster response times, which result in significantly lower costs compared to other solutions.

About OMICRON

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 900 employees provides solutions with 24/7 support at 25 locations worldwide and serves customers in more than 160 countries.

February 3, 2022 5:45 AM
1439867-0-0-EN