StationGuard OT Security
for the Power Grid

omicron**cybersecurity**.com

The StationGuard Solution protects critical systems from attacks and disruptions. In addition to intrusion detection, StationGuard also includes functions for inventorying all your OT assets, permanent monitoring of network and asset health, and vulnerability and threat management.

Intrusion Detection

StationGuard detects anomalies, malware, and malicious network traffic based on system specifications, signatures for known threats, and allowlists. It supports well over 300 protocols for deep packet inspection. This eliminates the need for a lengthy system training phase.

Asset Identification

StationGuard supports the creation and maintenance of asset inventories by identifying the assets present in OT networks. This can be done based on engineering information, project files, automatic network detection, and, if desired, active queries based on IEC 61850 MMES.

Functional Monitoring

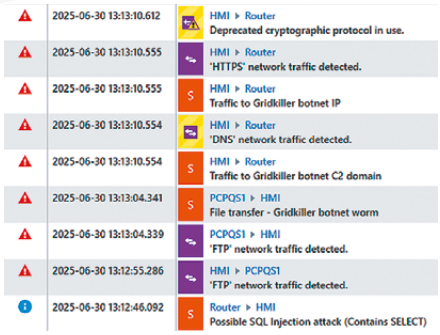
StationGuard also offers functional monitoring with in-depth analysis of all relevant logs. Immediate reporting of incidents ensures continued operation of your entire OT network.

Vulnerability Management

Which vulnerabilities pose a real risk to your system? GridOps only shows you the vulnerabilities that are relevant to you – with the most detailed and up-to-date database hand-curated by experts. This carefully prepared information ensures that vulnerabilities are accurately assigned to existing devices, thereby minimizing patching effort.

Threat Intelligence

OMICRON Threat Intelligence (OTI) provides continuous updates to secure IT and OT networks from constantly evolving cyber threats. Based on this information, you can better assess OT cyber risks, determine the most appropriate measures, and set the right priorities.



Intrusion Detection

Know What's Normal, See What's Dangerous

StationGuard monitors communication networks in real time, reliably detecting cyberattacks, unauthorized activities, and misconfigurations:

- Intrusion detection based on defined behavior patterns
- In-depth analysis of OT-specific communication protocols
- Clear, actionable alerts with technical and security context

The result: Full awareness of what's happening in your network – and whether it poses a risk.

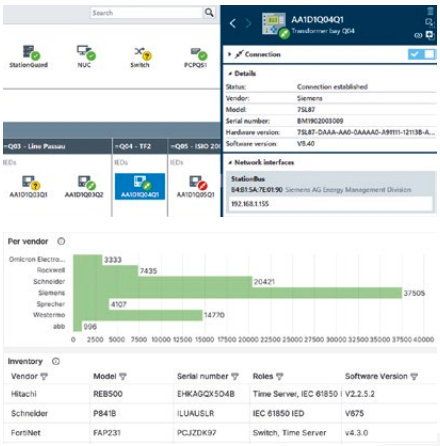
Asset Identification

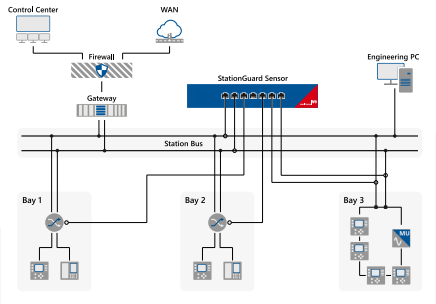
Discover, Understand, and Protect Your Assets

Precise and continuous identification of all assets in network – even without active scanning or additional sensors.

- > Automatic detection and classification of IEDs, RTUs, gateways, SCADA systems, and more
- > Extraction of key device data such as type, firmware version, and serial number
- > Reliable identification even with sporadic communication or passive assets

The result: A complete, up-to-date view of your OT landscape.





Functional Monitoring

Security Through Seamless Functional Control

Continuous monitoring of the functional health of your OT systems, detecting deviations, faults, and potential disruptions early:

- > Comprehensive monitoring of critical processes and communication paths
- > Early warning system for malfunctions and anomalies
- > Detailed analysis for fast root cause identification

The result: Confidence, reduced downtime, and swift response when it matters most.

Vulnerability Management

Detection is Basic, Distinction is Key

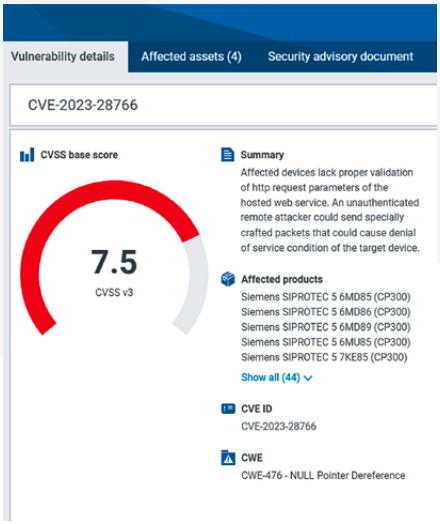
Security advisories warn you of threats to your assets, but, it is difficult to determine if the known threats actually pose a risk to your system. You need to know:

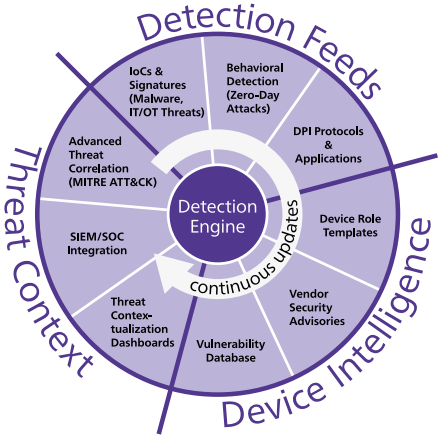
- > The exact device type, module configuration, and firmware version to determine if your IEDs and network devices are affected.
- > If the affected services are being used on your network and how critical their vulnerabilities are.

The StationGuard solution provides comprehensive information:

- > A database of known vulnerabilities for protection and control systems hand-curated by our security analysts
- > A comprehensive asset type database to identify all asset types

The result: You immediately know which vulnerabilities are relevant to your system.





Threat Intelligence

Stay informed & Make the Right Decision

OMICRON's Threat Intelligence (OTI) delivers continuous updates to protect IT and OT networks from evolving cyber threats. These include:

- > Updated detection rules (IOCs), including Suricata signatures for malicious network traffic
- > Enhanced anomaly detection
- > SIEM/SOC integrations
- > Threat context for dashboards and advanced threat correlation
- > Advanced threat correlation
- > An always up-to-date OT vulnerability database