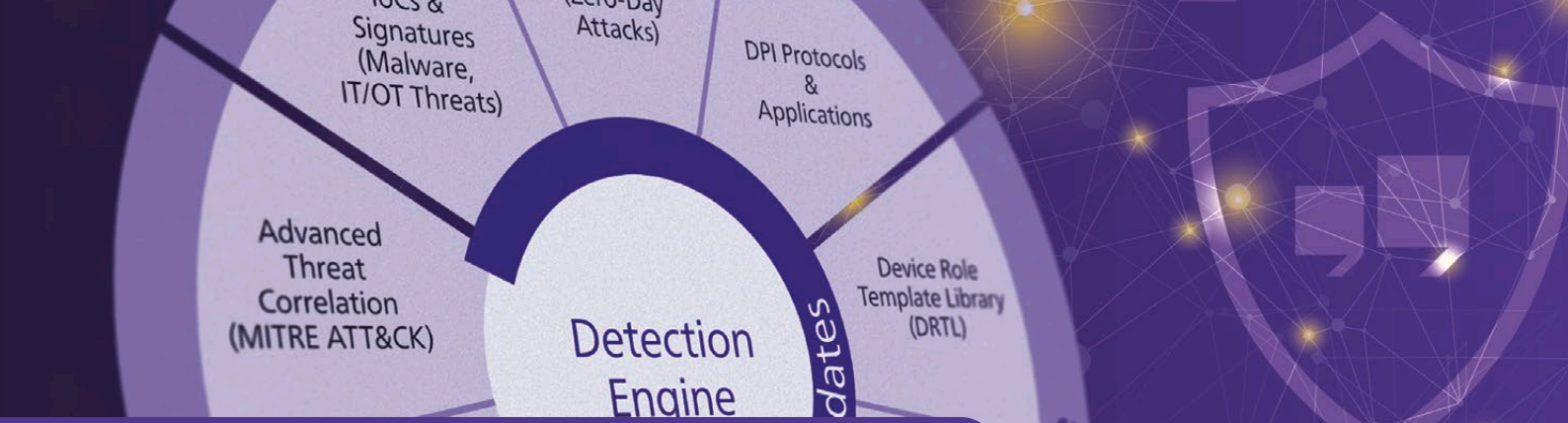


OMICRON Threat Intelligence

Detection Engineering for OT Security Experts in the Energy Grid

omicron**cybersecurity**.com

OMICRON Threat Intelligence (OTI) is a service package specifically designed to detect and defend against cyber threats in IT and OT networks within the energy sector. OTI combines detailed threat intelligence data with in-depth OT expertise, vendor information, and comprehensive protocol support, thereby closing the knowledge gap between IT safety and protection technology.

Typical Application Scenarios

Real-time Detection of cyber attacks, unauthorized activities, and misconfigurations in switchgear and control centers

Vulnerability Management: Automatic mapping of manufacturers' safety instructions to the actual OT assets in place

Compliance Support: Meeting regulatory requirements (NIS2, NIST, ISO 27001)

SOC Integration: Enriching SIEM platforms (e.g., Splunk, FortiSIEM) with OT-contextualized alerts and MITRE ATT&CK mappings

Benefits for OT Security Experts

Quick Setup: No training phase required thanks to an allow list approach based on system configuration

Minimization of False Positives: All signatures and rules are swept by rigorous functional verification and quality assurance.

Detailed OT Visibility: Deep packet inspection for over 300 protocols (e.g., IEC 61850, IEC 104, DNP3, Modbus) and 1 400+ applications

Local Operation (on-premise): Operation is possible in fully isolated OT zones without an internet connection.

Vulnerability Database: Dozens of OT manufacturers are systematically monitored, and their safety instructions are analyzed by experts; vulnerabilities are precisely mapped to existing assets.

Regular Updates: Updates for signatures, behavioral detection, protocols, and threat correlation

OTI Components at a Glance

Detection Rules (IoCs & Signatures)
Indicators of compromise (IoCs) are regularly updated: Suricata signatures, hashes of malicious files, known malicious IPs, and domains. Each rule undergoes functional verification and quality assurance before release.

Behavior-Based Detection
Regular improvements to detection logic for new threat scenarios, optimized alert quality, and enhanced visualization, directly integrated into every StationGuard update

Deep Packet Inspection
Over 300 protocols and more than 1 400 applications are inspected.
DPI models are regularly expanded, and even proprietary protocols can be integrated.

Device Role Templates
Predefined allow list profiles can be used for typical OT appliances: intelligent electronic devices (IEDs), RTUs, gateways, SCADA systems. This simplifies initial setup and reduces ongoing maintenance efforts.

Advanced Threat Correlation (MITRE ATT&CK)
Detailed event aggregation, MITRE ATT&CK mappings, and SIEM integrations (e.g., Splunk) for detecting complex attack patterns

SIEM/SOC Integrations
Regularly updated connectors, APIs, and documentation for SIEM/SOC platforms, such as Splunk and FortiSIEM

Threat Contextualization & Dashboards
GridOps dashboards enrich alerts and vulnerability information with contextual data and support compliance requirements.

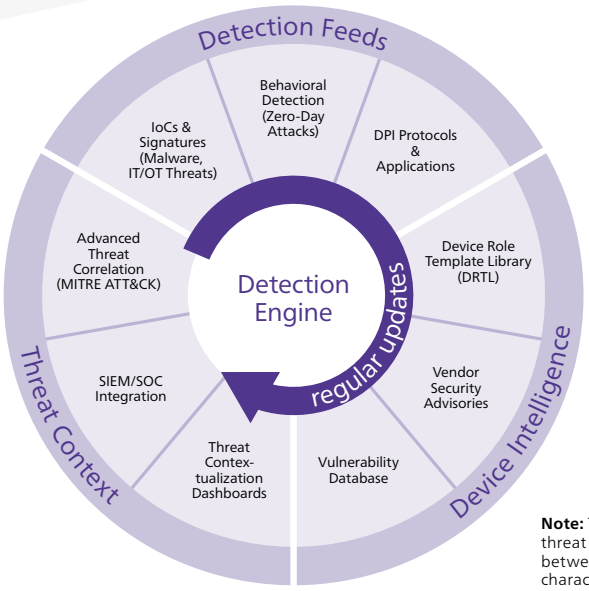
OT Vulnerability & Device Database
Includes systematic monitoring of dozens of OT vendors. Specialized matching heuristics precisely map vulnerabilities to your assets.

Vendor Safety Instructions
Offline access to the original security advisories from numerous OT manufacturers is available. OMICRON continuously monitors these sources and regularly updates the content, including the original PDFs.

OTI VS. IT-THREAT-INTELLIGENCE

Conventional IT threat intelligence solutions are tailored to IT environments and do not adequately account for OT-specific protocols, device types, and operational requirements.
OTI was specifically developed to meet the safety requirements of the power grid:

Criterion	OTI	IT Threat Intelligence
Protocol Coverage	IT and OT networks with a clear focus on the OT world, particularly protection and control systems (substations, power plants, and grid control systems) with 300+ IT and OT protocols (e.g., IEC 61850, IEC 104, DNP3, Modbus)	Focuses primarily on the IT world: enterprise endpoints, servers, cloud workloads, web and email infrastructure. OT coverage is limited or provided via separate ICS/OT feeds, usually without in-depth protocol knowledge.
Behavioral Detection	OT-specific behavioral detection in the StationGuard Sensor, which is continuously refined by a dedicated R&D team	Behavior-based detection is typically used for IT endpoints and networks. No OT-specific baselines for protection and control systems
Vulnerability Database	Offers systematic monitoring of vulnerability disclosures and product updates from numerous OT hardware and software vendors. Specialized matching heuristics for numerous OT product families precisely map vulnerabilities to the assets in the inventory; these heuristics are continuously updated.	Offers strong CVE/NVD coverage, with a focus on IT products (operating systems, browsers, enterprise software, network components). Matching based on OT device type, firmware, and module levels is generally not mapped with comparable depth.
Asset Context	Offers a close link between threat intelligence and the asset inventory: Vulnerability and advisory information is mapped to specific OT appliances, modules, and firmware versions using specialized matching heuristics. This allows the relevance of a threat to be assessed directly at the asset level; prioritizing patches and countermeasures is significantly simplified.	Asset reference is typically obtained via IT CMDBs, EDR telemetry, or vulnerability scanner results (IT assets). A reliable association process for threats with OT appliances at the device type, module, and firmware levels is generally not provided.
Operation in Isolated Zones	Deployment is conducted via update mechanisms that are also applicable in isolated OT zones. StationGuard/GridOps can be operated entirely on-premise.	True offline/air-gap capability and on-premises operation are not always available; in isolated OT zones, they are often only usable to a limited extent.
OT Expertise	Power grid expertise & playbooks integrated	Generic rules, little OT context



Note: The statements regarding the comparison with IT threat intelligence are based on well-known differences between IT and OT security solutions, as well as the characteristics of OTI.