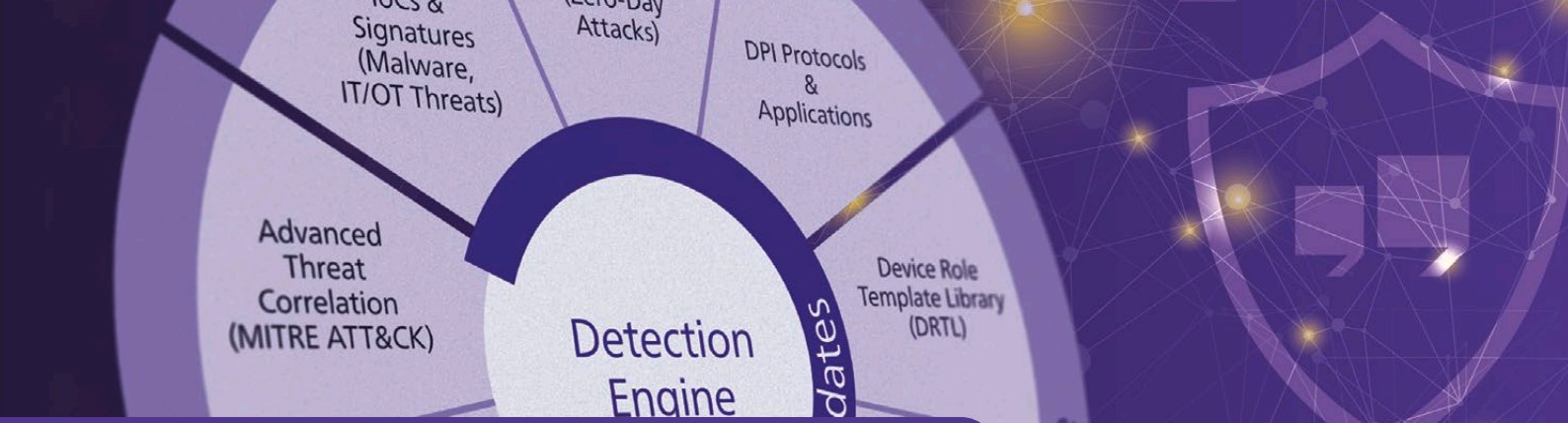


OMICRON Threat Intelligence

Detection Engineering für OT-Sicherheitsexpert:innen im Energienetz

omicron**cybersecurity**.com

OMICRON Threat Intelligence (OTI) ist ein Service-Paket, das speziell für die Erkennung und Abwehr von Cyberbedrohungen in IT- und OT-Netzwerken der Energieversorgung entwickelt wurde. OTI kombiniert detaillierte Threat-Intelligence-Daten mit tiefgreifendem OT-Know-how, Herstellerinformationen und umfassender Protokollunterstützung – und schließt damit die Wissenslücke zwischen IT-Sicherheit und Schutztechnik.

Typische Anwendungsszenarien

Echtzeit-Erkennung von Cyberangriffen, unerlaubten Aktivitäten und Fehlkonfigurationen in Schaltanlagen und Leitstellen.

Schwachstellen-Management: Automatisches Mapping von Sicherheitshinweisen der Hersteller (Security Advisories) zu den tatsächlich vorhandenen OT-Assets.

Compliance-Unterstützung: Erfüllung regulatorischer Anforderungen (NIS2, NIST, ISO 27001).

SOC-Integration: Anreicherung von SIEM-Plattformen (z. B. Splunk, FortiSIEM) mit OT-kontextualisierten Alarmen und MITRE ATT&CK-Mappings.

Nutzen für OT-Sicherheitsexpert:innen

Sofort einsatzbereit: Kein Trainingsphase dank Allowlist-Ansatz auf Basis der Systemkonfiguration

Minimierung von Fehlalarmen: Alle Signaturen und Regeln durchlaufen strenge funktionale Verifikation und Qualitätssicherung.

Detaillierte OT-Sichtbarkeit: Deep Packet Inspection für über 300 Protokolle (IEC 61850, IEC 104, DNP3, Modbus, ...) und 1.400+ Applikationen.

Lokaler Betrieb (On-Premise): Betrieb in vollständig isolierten OT-Zonen ohne Internetanbindung möglich.

Schwachstellen-DB: Dutzende OT-Hersteller werden systematisch überwacht und deren Sicherheitshinweise von Expert:innen aufbereitet; Schwachstellen werden exakt den vorhandenen Assets zugeordnet.

Regelmäßige Updates: Aktualisierungen für Signaturen, Verhaltenserkennung, Protokolle und Threat-Korrelation.

OTI-Komponenten im Überblick

Erkenunngsregeln (IoCs & Signaturen)
Regelmäßig aktualisierte Indicators of Compromise (IoCs): Suricata-Signaturen, Hashes schädlicher Dateien, bekannte bösartige IPs und Domains. Jede Regel wird vor der Freigabe funktional verifiziert und qualitätsgesichert.

Verhaltensbasierte Erkennung
Regelmäßige Verbesserungen der Erkennungslogik für neue Bedrohungsszenarien, optimierte Alarmqualität und erweiterte Visualisierung – in jedem StationGuard-Update direkt integriert.

Deep Packet Inspection
Über 300 Protokolle und mehr als 1.400 Applikationen. DPI-Modelle werden regelmäßig erweitert, auch proprietäre Protokolle können integriert werden.

Device Role Templates
Vordefinierte Allowlist-Profile für typische OT-Geräte: IEDs, RTUs, Gateways, SCADA-Systeme. Vereinfacht die Ersteinrichtung und reduziert den laufenden Wartungsaufwand

Advanced Threat Correlation (MITRE ATT&CK)
Detaillierte Ereignis-Aggregation, MITRE ATT&CK-Mappings und SIEM-Integrationen (z. B. Splunk) für die Erkennung komplexer Angriffsmuster.

SIEM-/SOC-Integrationen
Regelmäßig aktualisierte Konnektoren, APIs und Dokumentation für SIEM/SOC-Plattformen, z. B. Splunk & FortiSIEM.

Threat-Kontextualisierung & Dashboards
GridOps-Dashboards reichern Alarme und Schwachstelleninformationen mit Kontextinformationen an und unterstützen bei der Einhaltung von Compliance-Anforderungen.

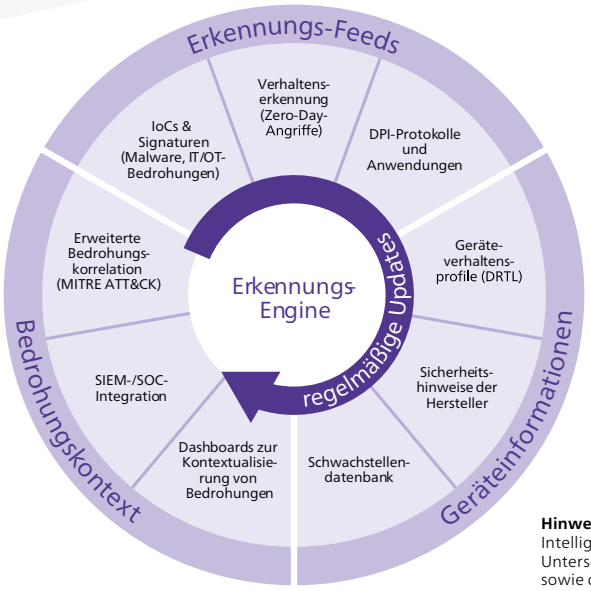
OT-Schwachstellen- & Gerätedatenbank
Systematisches Monitoring von Dutzenden OT-Herstellern. Spezialisierte Matching-Heuristiken mappen Schwachstellen präzise Ihren Assets zu.

Sicherheitshinweise der Hersteller
Offline-Zugriff auf die originalen Security Advisories zahlreicher OT-Hersteller. OMICRON überwacht diese Quellen kontinuierlich und aktualisiert die Inhalte einschließlich der Original-PDFs regelmäßig.

OTI VS. IT-THREAT-INTELLIGENCE

Herkömmliche IT-Threat-Intelligence-Lösungen sind auf IT-Umgebungen zugeschnitten und berücksichtigen OT-spezifische Protokolle, Gerätetypen und Betriebsanforderungen nur unzureichend.
OTI wurde gezielt für die Anforderungen der Sicherheit im Energienetz entwickelt:

Kriterium	OTI	IT-Threat
Protokoll-Abdeckung	IT- und OT-Netzwerke mit klarem Fokus auf die OT-Welt, insbesondere Schutz- und Leittechnik (Umspannwerke, Kraftwerke, Netzleittechnik).300+ IT- und OT-Protokolle (IEC 61850, IEC 104, DNP3, Modbus, ...)	Primär IT-Welt: Enterprise-Endpoints, Server, Cloud-Workloads, Web- und E-Mail-Infrastruktur. OT-Abdeckung nur eingeschränkt oder über separate ICS-/OT-Feeds, meist ohne tiefe Protokollkenntnis.
Verhaltenserkennung	OT-spezifische Verhaltenserkennung in StationGuard, die durch ein dediziertes R&D-Team kontinuierlich weiterentwickelt wird.	Verhaltensbasierte Erkennung typischerweise für IT-Endpoints und -Netze. Keine OT-spezifischen Baselines für Schutz- und Leittechnik
Schwachstellen-Datenbank	Systematisches Monitoring von Schwachstellen-Veröffentlichungen und Produkt-Updates zahlreicher OT-Hardware- und Softwarehersteller. Spezielle Matching-Heuristiken für zahlreiche OT-Produktfamilien ordnen Schwachstellen präzise den Assets im Inventar zu; die Heuristiken werden laufend gepflegt.	Starke CVE-/NVD-Abdeckung, mit Fokus auf IT-Produkte (Betriebssysteme, Browser, Enterprise-Software, Netzwerkkomponenten). Matching auf OT-Gerätetypen, Firmware- und Modulebene ist in der Regel nicht mit vergleichbarer Tiefe abgebildet.
Asset-Kontext	Enger Bezug zwischen Threat Intelligence und Asset-Inventar: Vulnerability- und Advisory-Informationen werden über spezialisierte Matching-Heuristiken konkreten OT-Geräten, Modulen und Firmware-Versionen zugeordnet. Dadurch lässt sich die Relevanz einer Bedrohung auf Asset-Ebene direkt bewerten; die Priorisierung von Patches und Maßnahmen wird deutlich erleichtert.	Asset-Bezug erfolgt typischerweise über IT-CMDBs, EDR-Telemetrie oder Vulnerability-Scanner-Ergebnisse (IT-Assets). Eine belastbare Zuordnung von Bedrohungen zu OT-Geräten auf Ebene Typ, Modul und Firmware ist in der Regel nicht vorgesehen.
Betrieb in isolierten Zonen	Bereitstellung über Update-Mechanismen, die auch in isolierten OT-Zonen anwendbar sind StationGuard/GridOps kann vollständig on-premise betrieben werden.	Echte Offline-/Air-Gap-Fähigkeit und on-premise-Betrieb sind nicht immer gegeben; in isolierten OT-Zonen oft nur eingeschränkt nutzbar.
OT-Fachexpertise	Energienetz-Expertise & Playbooks integriert	Generische Regeln, wenig OT-Kontext



Hinweis: Die Aussagen zum Vergleich mit IT-Threat-Intelligence basieren auf allgemein bekannten Unterschieden zwischen IT- und OT-Sicherheitslösungen sowie den Eigenschaften von OTI.

© OMICRON, 06 2026