NTS SECURITY

THREAT DETECTION SERVICE | OT
OMICRON STATIONGUARD

RELAX, WE CARE

OMICRON

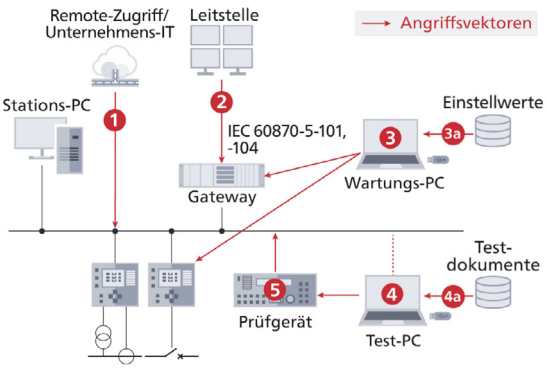
THREAT DETECTION SERVICE | OT
OMICRON STATIONGUARD

Mit zunehmender Digitalisierung und der Konvergenz von IT und OT (Operational Technology) wird Cybersicherheit immer wichtiger. Das beweist der Anstieg von Cyberattacken auf Produktions- und Energieversorgungsunternehmen in den letzten Jahren.

UMFASSENDE SICHERHEITSSTRATEGIE

Ein Sicherheitskonzept für Schaltanlagen sollte von der physischen Zugangskontrolle, über die digitale Überwachung des Zugriffs, bis hin zur Überwachung verdächtiger oder nicht autorisierter Aktivitäten im Netzwerk reichen. Dies erfordert Systeme, die ein hohes Maß an Sicherheit bei langfristig geringem Wartungsaufwand bieten. Zudem sollten sich diese Systeme einfach in die Betriebs- und Wartungsabläufe integrieren lassen.

Leitstellen und deren Computer (1) sind nicht die einzigen Eintrittspunkte für Cyberangriffe auf das Stromnetz – auch Schaltanlagen sind attraktive Ziele. Der am häufigsten verwendete Angriffsvektor ist die Verbindung zur Unternehmens-IT (2) bzw. schlecht abgesicherte Fernwartungszugänge. Aber auch kompromittierte oder infizierte Wartungs-(3) und Test-PCs (4) bzw. Prüfgeräte (5), sowie eine hohe Anzahl an bekannten und unbekannten (sog. zero-day) Schwachstellen von OT-Systemen erhöhen zusätzlich das Risiko.



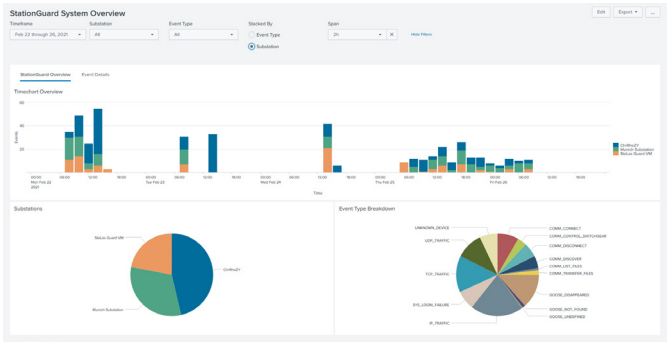
Angriffsvektoren einer Schaltanlage

Um diese Bedrohungen rechtzeitig zu erkennen, kooperiert NTS für sein **Threat Detection Service | OT** mit dem Unternehmen **OMICRON**.

BRÜCKE ZWISCHEN 2 WELTEN: IT & OT

Gemeinsam mit **OMICRON** liefern wir Security-Lösungen, die alle Anforderungen zur Cybersicherheit und des Smart Grids meistern. Durch diese Partnerschaft schlagen wir eine Brücke zwischen IT und OT und gewährleisten durch branchenübergreifendes Fachwissen ein hohes Maß an IT- und OT-Sicherheit.

OMICRON ist der Experte für Schutz- und Leittechnik und ergänzt mit dem Omicron Stationguard perfekt das Security-Portfolio von NTS. Somit ermöglichen wir Kunden ein bislang unerreichtes Level an Sicherheit. Das **NTS Threat Detection Service | OT** vereint beide Kompetenzfelder und bietet einen ganzheitlichen Ansatz.



OMICRON StationGuard for Splunk

RELAX, WE CARE

T/OT-Konvergenz: Es wächst zusammen, was (nicht) zusammengehört. Wir schlagen die Brücke zwischen den zwei Welten.

→ **www.nts.eu**

Dabei werden alle sicherheitsrelevanten Informationen, rund um die IT- und OT-Infrastruktur, im **NTS Threat Detection Service** in Echtzeit analysiert und korreliert, um Cybersecurity Vorfälle schnellstmöglich zu erkennen. Ein speziell geschultes NTS Defense Team analysiert alle verdächtigen Ereignisse und bewertet sie hinsichtlich Gefährlichkeit und Dringlichkeit. Die mit OT-Wissen angereicherten Alarmmeldungen und ein leicht verständliches Dashboard helfen den Analysten des Security Operations Center (SOC) Alarme zu beurteilen und schnell darauf zu reagieren. Dabei stehen das NTS Defense Team und das **OMICRON** OT Security Team im ständigen Austausch.

Wir informieren Sie nur über tatsächlich riskante Ereignisse und greifen nur bei ernstzunehmenden Gefährdungen ein. Daraus resultiert eine verbesserte Sichtbarkeit von OT-Bedrohungen, sowie ein umfassender Schutz vor Angriffen auf IT und OT.

DER STATIONGUARD-ANSATZ

Der StationGuard ist eine Überwachungslösung zur Erkennung von Cyberbedrohungen und Kommunikationsproblemen in Schaltanlagen. Schaltanlagen und OT-Systeme sind deterministisch, das bedeutet, dass das Verhalten klar definiert ist. Das gilt auch in Ausnahmesituationen, wie zum Beispiel bei Schutzereignissen. Da der StationGuard, im Gegensatz zu signatur- und baselinebasierten Intrustion Detecion Systemen (IDS), die Funktion jedes einzelnen Geräts kennt, kann es ein Systemmodell der Schaltanlage erstellen und jedes einzelne Netzwerkpaket mit diesem Live-Systemmodell vergleichen. Das entspricht einem sogenannten Allowlist-Ansatz (Whitelist), bei dem erlaubtes Verhalten beschrieben wird.

Alles was davon abweicht, löst standardmäßig einen Alarm aus. Mit diesem Ansatz werden auch völlig neue Angriffe erkannt. So können nicht nur Cyberbedrohungen und verbotene Aktivitäten festgestellt werden, sondern auch Probleme in den Automatisierungs- und Leittechnikfunktionen. Diese Kombination aus Angriffserkennung und Funktionsüberwachung wird auch funktionale Sicherheitsüberwachung genannt.

© OMICRON

VORTEILE DER STATIONGUARD-LÖSUNG

- Einfache Konfiguration ohne Lernphase und damit sofortiger Schutz
- Deep Packet Inspection von IEC 61850, IEC 60870-5-104, DNP3, Modbus TCP, PRP/HSR und vielen mehr
- Funktionale Sicherheitsüberwachung in Schaltanlagen führt zu zuverlässiger Erkennung erlaubter Aktivitäten und Fehlfunktionen
- OT/ICS Asset Inventar zur Bestandserfassung
- Geringe Fehlalarmquote: Erkennung der Vorgänge in der Anlage inkl. „Wartungsmodus“
- Hohe Verständlichkeit der Alarme, auch ohne Protokollkenntnisse
- Einfache Integration von Alarmmeldungen durch Binärkontakte inkl. Syslog-Schnittstelle

RELAX,
WE CARE

INTERESSE?

Für weitere Auskünfte wenden Sie sich bitte an Ihren Key Account Manager.

sales@nts.eu

www.nts.eu

THREAT DETECTION SERVICE | OT
OMICRON STATIONGUARD

RELAX, WE CARE

OMICRON

NTS NETZWERK TELEKOM SERVICE AG
DATA CENTER | NETWORK | COLLABORATION | SECURITY | SUPER SERVICES
GRAZ | WIEN | LINZ | INNSBRUCK | SALZBURG | DORNBIRN | KLAGENFURT
BOZEN | FRIEDRICHSHAFEN | AUGSBURG | ROSENHEIM | LEIPZIG | REUTLINGEN

www.nts.eu