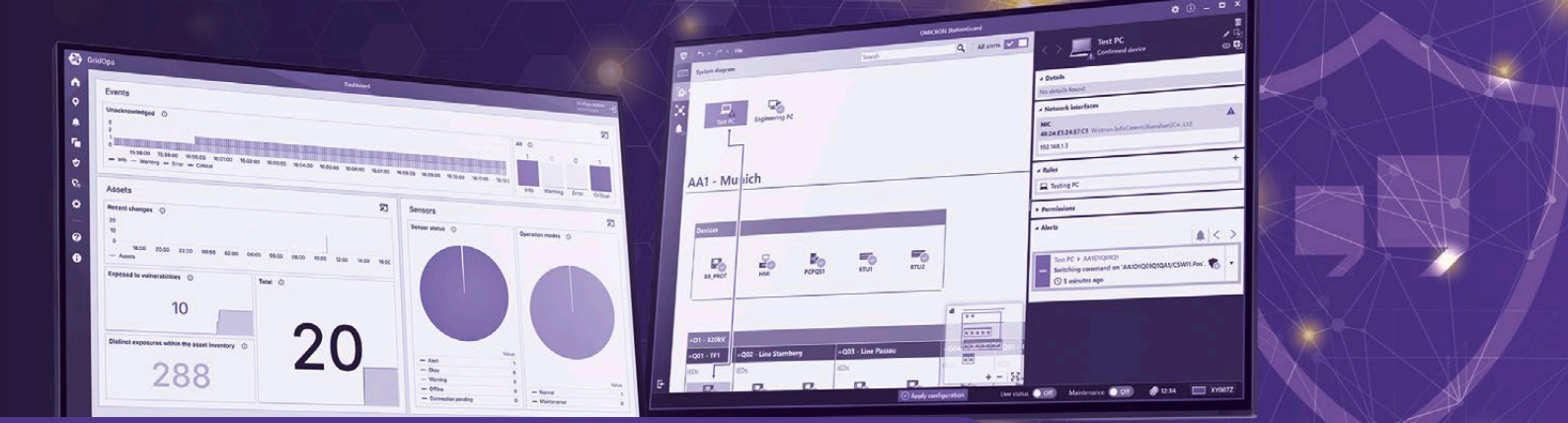


StationGuard OT-Security
für das Energienetz

omicron**cybersecurity**.com

Die StationGuard-Lösung schützt kritische Systeme vor Angriffen und Störungen. Neben der Erkennung von Eindringlingen umfasst StationGuard auch Funktionen zur Bestandsaufnahme aller OT-Assets, zur permanenten Überwachung des Netzwerk- und Asset-Zustands sowie zum Schwachstellen- und Bedrohungsmanagement.

Angriffserkennung

StationGuard erkennt Anomalien, Malware und bösartigen Netzwerkverkehr auf der Grundlage von Systemspezifikationen, Signaturen für bekannte Bedrohungen und Zulassungslisten. Es unterstützt weit über 300 Protokolle für die Deep Packet Inspection. Dadurch entfällt eine langwierige Systemtrainingsphase.

Identifikation der Assets

StationGuard unterstützt die Erstellung und Pflege von Asset-Inventaren, indem es die in OT-Netzwerken vorhandenen Assets identifiziert. Dies kann auf der Grundlage von technischen Informationen, Projektdateien, automatischer Netzwerkerkennung und, falls gewünscht, aktiven Abfragen auf der Grundlage von IEC 61850 MMES erfolgen.

Funktionsüberwachung

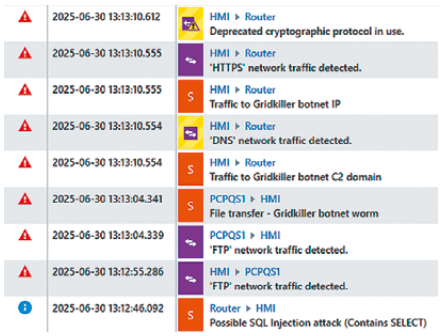
StationGuard bietet außerdem eine Funktionsüberwachung mit detaillierter Analyse aller relevanten Protokolle. Die sofortige Meldung von Vorfällen gewährleistet den kontinuierlichen Betrieb Ihres gesamten OT-Netzwerks.

Schwachstellen-Management

Welche Schwachstellen stellen ein echtes Risiko für Ihr System dar? GridOps zeigt Ihnen nur die Schwachstellen, die für Sie relevant sind – mit der detailliertesten und aktuellsten Datenbank, die von Expert:innen manuell zusammengestellt wurde. Diese sorgfältig aufbereiteten Informationen stellen sicher, dass Schwachstellen den vorhandenen Geräten genau zugeordnet werden, wodurch der Aufwand für das Patchen minimiert wird.

Threat Intelligence

Der OMICRON-Threat-Intelligence(OTI)-Service bietet kontinuierliche Updates, um IT- und OT-Netzwerke vor sich ständig weiterentwickelnden Cyberbedrohungen zu schützen. Auf Grundlage dieser Informationen können Sie OT-Cyberrisiken besser bewerten, die am besten geeigneten Maßnahmen festlegen und die richtigen Prioritäten setzen..



Intrusion Detection

Wissen, was normal ist. Erkennen, was gefährlich ist.

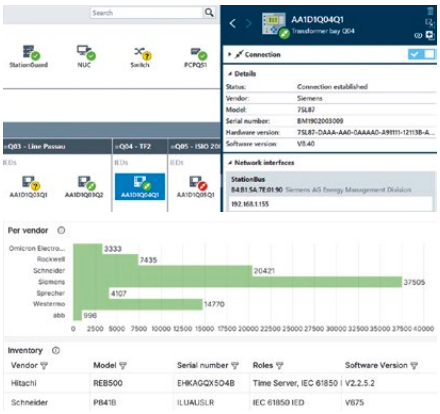
StationGuard überwacht Kommunikationsnetzwerke in Echtzeit und erkennt zuverlässig Cyberangriffe, unbefugte Aktivitäten und Fehlkonfigurationen:

- Angriffserkennung basierend auf definierten Verhaltensmustern
- Tiefgehende Analyse von OT-spezifischen Kommunikationsprotokollen
- Klare, umsetzbare Warnmeldungen mit technischem und sicherheitsrelevanten Kontext

Das Ergebnis: Sie haben vollständige Transparenz darüber, was in Ihrem Netzwerk geschieht – und ob ein Risiko besteht.

Identifikation der Assets

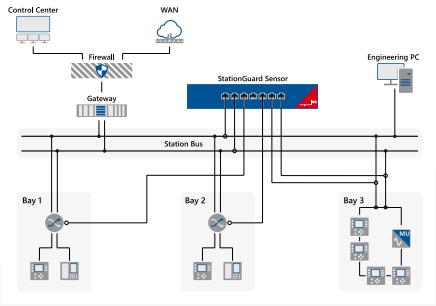
Entdecken, verstehen und schützen Sie Ihre Assets



Präzise und kontinuierliche Identifizierung aller Assets im Netzwerk – auch ohne aktives Scannen oder zusätzliche Sensoren.

- Automatische Erkennung und Klassifizierung von IEDs, RTUs, Gateways, SCADA-Systemen und mehr
- Extraktion wichtiger Gerätedaten wie Typ, Firmware-Version und Seriennummer
- Zuverlässige Identifizierung auch bei sporadischer Kommunikation oder passiven Assets

Das Ergebnis:Ein vollständiger, aktueller Überblick über Ihre OT-Landschaft.



Funktionsüberwachung

Sicherheit durch nahtlose Funktionskontrolle

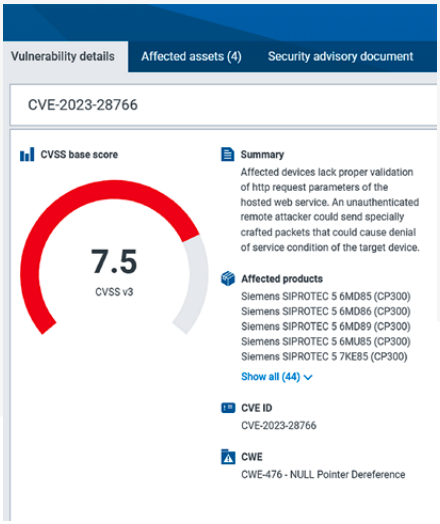
Kontinuierliche Überwachung der Funktionsfähigkeit Ihrer OT-Systeme, frühzeitige Erkennung von Abweichungen, Fehlern und potenziellen Störungen:

- Umfassende Überwachung kritischer Prozesse und Kommunikationswege
- Frühwarnsystem für Störungen und Anomalien
- Detaillierte Analyse zur schnellen Identifizierung der Ursachen

Das Ergebnis: Vertrauen, reduzierte Ausfallzeiten und schnelle Reaktion, wenn es darauf ankommt.

Schwachstellen-Management

Erkennen für die Daten. Unterscheiden für die Klarheit.



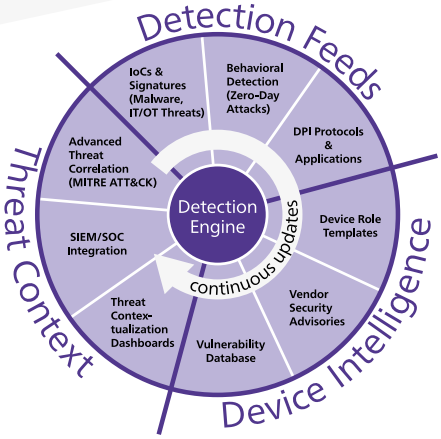
Sicherheitshinweise (Security Advisories) warnen Sie vor Bedrohungen für Ihre Assets. Allerdings stellt nicht jede bekannte Bedrohung tatsächlich ein Risiko für Ihr System dar. Sie müssen Folgendes wissen:

- Den genauen Gerätetyp, die Modulkonfiguration und die Firmware-Version, um festzustellen, ob Ihre IEDs und Netzwerkgeräte betroffen sind.
- Ob die betroffenen Dienste in Ihrem Netzwerk verwendet werden und wie kritisch ihre Schwachstellen sind.

Die StationGuard-Lösung bietet umfassende Informationen:

- Eine Datenbank mit bekannten Schwachstellen für Schutzsysteme und Steuerungssysteme, die von unseren Sicherheitsanalyst:innen manuell zusammengestellt wurde
- Eine umfassende Asset-Datenbank, um alle Assets zu identifizieren

Das Ergebnis: Sie wissen sofort, welche Schwachstellen für Ihr System relevant sind.



Threat Intelligence

Bleiben Sie informiert und treffen Sie die richtige Entscheidung

Der OMICRON-Threat-Intelligence(OTI)-Service liefert kontinuierliche Updates, um IT- und OT-Netzwerke vor sich ständig weiterentwickelnden Cyber-Bedrohungen zu schützen. Dazu gehören:

- Aktualisierte Erkennungsregeln (IOCs), einschließlich Suricata-Signaturen für bösartigen Netzwerkverkehr
- Verbesserte Anomalieerkennung
- SIEM/SOC-Integrationen
- Bedrohungskontext für Dashboard und erweiterte Bedrohungskorrelation
- Eine stets aktuelle OT-Schwachstellendatenbank

Das Ergebnis: Eine Erkennungstechnologie, die Ihre Assets schützt und Sie auf dem Laufenden hält.