Automatisierte Angriffserkennung und Schwachstellen-management im Stromnetz nach IEC 62443

IEC 62443 - Security for Industrial Automation and Control Systems, 10.10.23, ÖVE Academy, Wien

Christian Brauner, Andreas Klien, OMICRON, Österreich

OMICRON

OMICRON

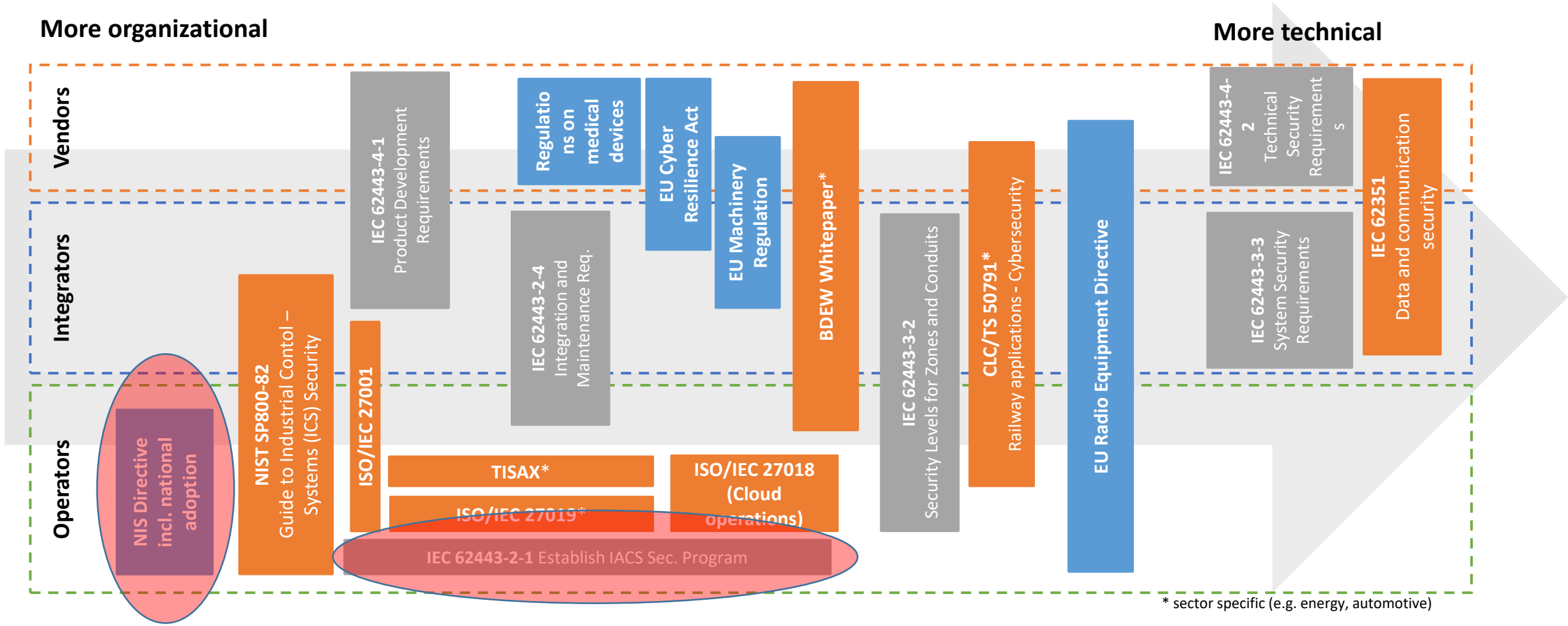
Wir sind Weltmarktführer

Prüftechnik in der elektrischen Energieversorgung

OMICRON im Überblick

- **Gegründet 1984 durch Rainer Aberer, heute im Eigentum der OMICRON Stiftung**
- **Zentrale in Klaus/Vorarlberg**
- **Innovative Prüf-, Diagnose und Monitoringlösungen für die elektrische Energieversorgung (Schutz-, Leittechnik und Primärtechnik)**
- **1.081 Mitarbeiter, 180 Mio. € Umsatz, 98% Export, >15% FE Anteil**
- **Niederlassungen in 24 Ländern, Kunden in über 170 Ländern**

EU NIS vs. IEC 62443 Security Standards für Energieversorger



Spannungsfeld IT-OT Abteilung

Wie machen wir das Stromnetz sicher?

- IT- und OT-Menschen müssen zusammenarbeiten, um das Stromnetz vor Cyberangriffen zu schützen.

- Security-Tools müssen hierfür auch einen Beitrag leisten.

Zusammenarbeit im Schwachstellenmanagement

OMICRON

„Patcht endlich!“ – sagt die IT

- „Warum sind da immer noch tausende Schutz- und Steuergeräte
  - mit jahrealter Firmware,
  - mit jahrealten Schwachstellen,
  - und sogar mit bekannten Exploits?”

NIS-Factsheet 9/2022:

Der Betreiber stellt sicher, dass die eingesetzten Systemversionen aus sicherheitstechnischer Sicht auf dem aktuellen Stand sind. Der Betreiber überprüft Herkunft und Integrität der jeweiligen Systemversion vor ihrer Installation beziehungsweise vor ihrer Aktualisierung und analysiert die technischen und betrieblichen Auswirkungen dieser Version auf das betreffende Netz- und Informationssystem.

Patchen im Stromnetz

Das Risiko, einen Patch aufzuspielen, **kann höher sein, als ihn nicht aufzuspielen**.

- Patches haben neue Bugs.
- Patches verhalten sich auf verschiedenen HW-Versionen unterschiedlich.
- Patches können Nebeneffekte auf die eigene programmierte Logik haben.

- Wie teste ich Leittechnik und Kommunikationsfunktionen?

Risiko-Management statt blindes Patchen

1. Welche Schwachstellenmeldungen gibt es für meine Hersteller überhaupt?

2. Welche meiner Geräte sind davon betroffen?

3. Entscheidung pro Gerät: Patchen, Risiko mindern, oder akzeptieren?
   - Ist das Gerät in einem kritischem Netzsegment?
   - Würde ich in dieser Anlage ein Ausnutzen der Schwachstelle detektieren?

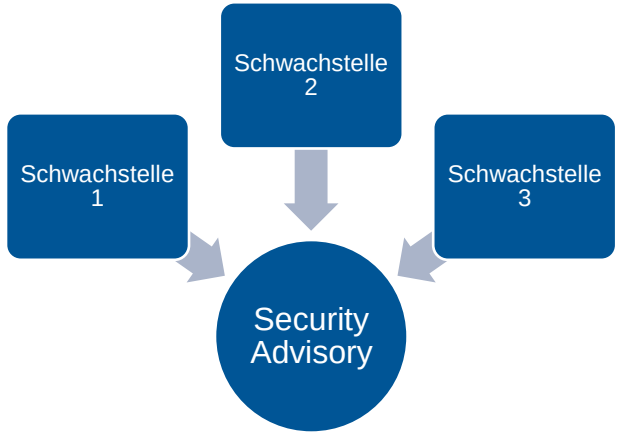
4. Was könnten wir tun, bis wir patchen können?
   - technische Minderungsmaßnahmen
   - Angriffserkennung überprüfen

Unterschied Security Advisory vs. Schwachstelle

- **Schwachstelle** (Vulnerability)
  - Softwarefehler in einer SW-Komponente, der ausgenutzt werden könnte.

- Schutz- und Leittechnikgeräte bestehen aus hunderten SW-Komponenten.
  - Hersteller müssen alle Komponenten überwachen.
  - Wenn im Endprodukt ein Risiko „durchschlägt“, *sollten* sie Kunden informieren.

- **Security Advisory**: Sicherheitshinweis über Security-Probleme in Produkten.
  - Risiko – Wann trifft es auf mich zu?
  - Gegenmaßnahmen – Wie kann ich mich schützen?

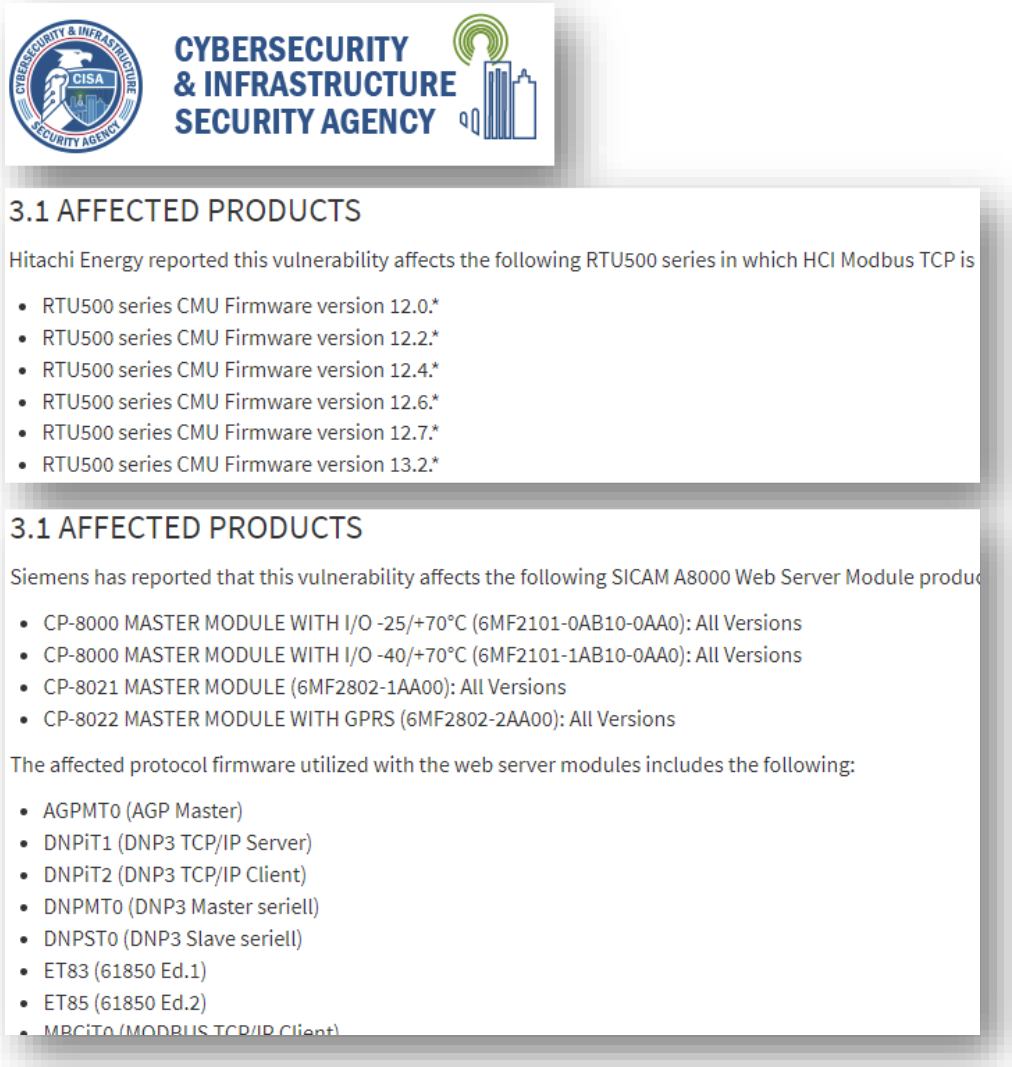


- Für EVUs sind Security Advisories relevant.

Welche meiner Geräte sind betroffen?

- Ich bin nur betroffen, wenn
  - das **Gerätemodell**, **Modulkonfiguration**
  - und **Firmware**-Version übereinstimmen
  - und die betroffenen Dienste zugänglich sind.

- Woher kriege ich Security Advisories?
  - Von jedem Hersteller separat.



Ein paar Zahlen

- Top 3 der Schutz- und Leittechnikhersteller veröffentlichten diese Anzahl an Security Advisories:

2022	2023	Gesamt bis heute
262	335*	>2350

- Jedes Security Advisory
  - enthält ~3 Schwachstellen,
  - betrifft 10-20 verschiedene Gerätetypen,
  - erfordert zwischen 5 Minuten und 8 Stunden Zeitaufwand, um herauszufinden, ob ich betroffen bin.

*hochgerechnet im September 2023

Präzises Anlageninventar nötig

NIS-Verordnung:
Vermögenswerte, die im Zusammenhang mit Netz- und Informationssystemen stehen, sind strukturiert zu analysieren und zu dokumentieren.

IEC

ISA/IEC 62443-3-3 SR 7.8

SR 7.8 – Control system component inventory
11.10.1 Requirement .....
11.10.2 Rationale and supplemental guidance .
11.10.3 Requirement enhancements .....

Mit zu wenig Geräteinformationen treffen **zu viele** Schwachstellen zu, oder man **übersieht** Schwachstellen.

- Beispiel: ICSA-22-195-16; Denial-of-Service in EN100 Ethernet module ... all firmware versions prior to v4.40

OMICRON

Licht am Ende des Tunnels

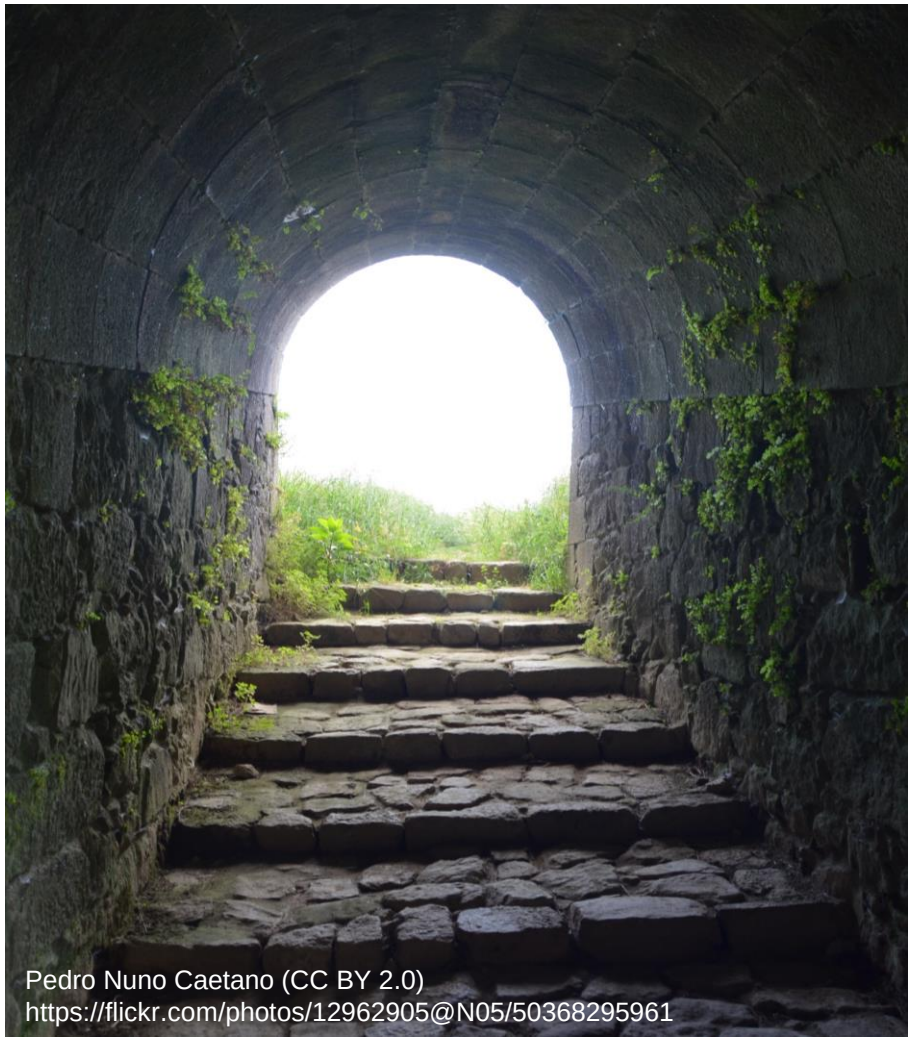
Automatisierbarkeit!

1. Man kann das Anlageninventar **automatisch** erstellen und aktuell halten.

2. Es gibt **maschinenlesbare** Beschreibungen von Security Advisories.

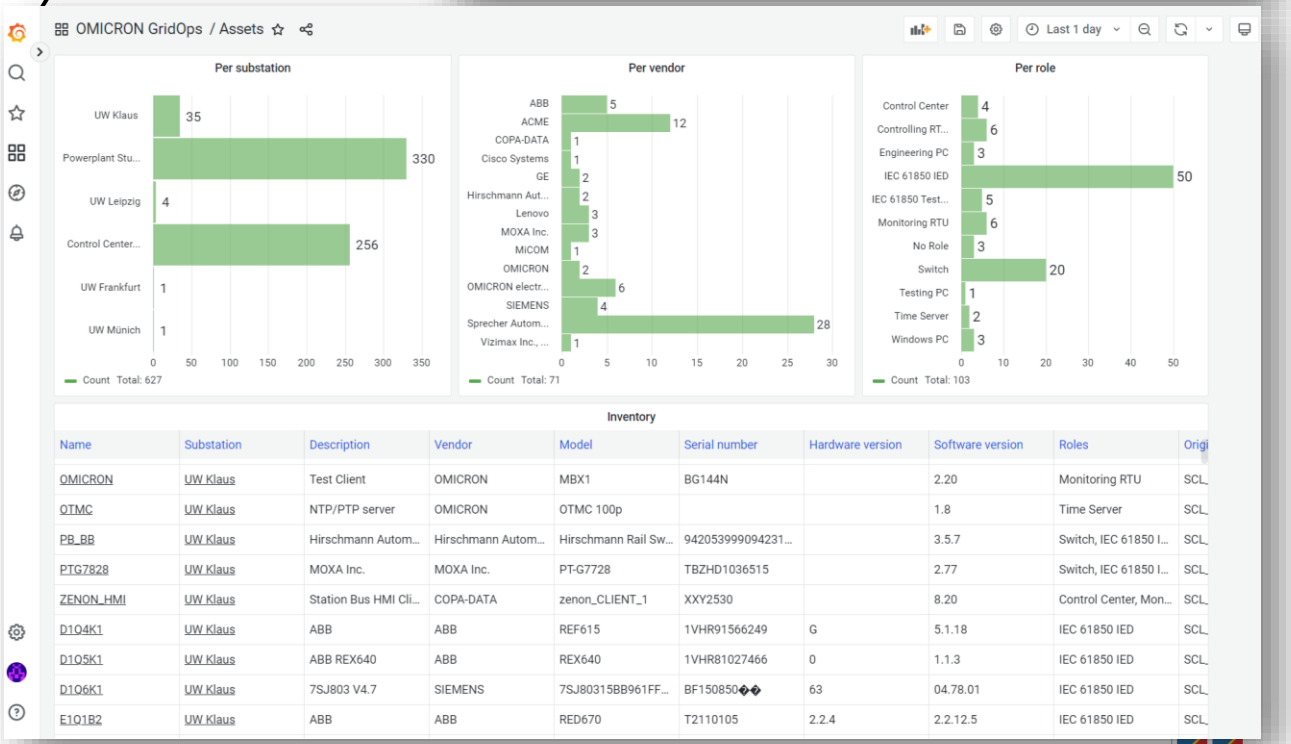
CSAF

https://csaf.io



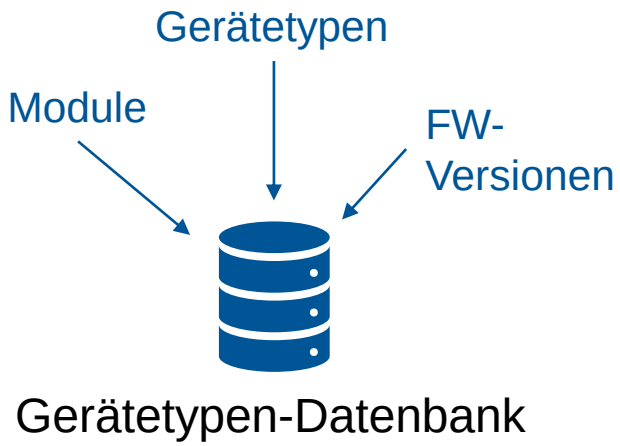
Automatische Inventar-Erstellung

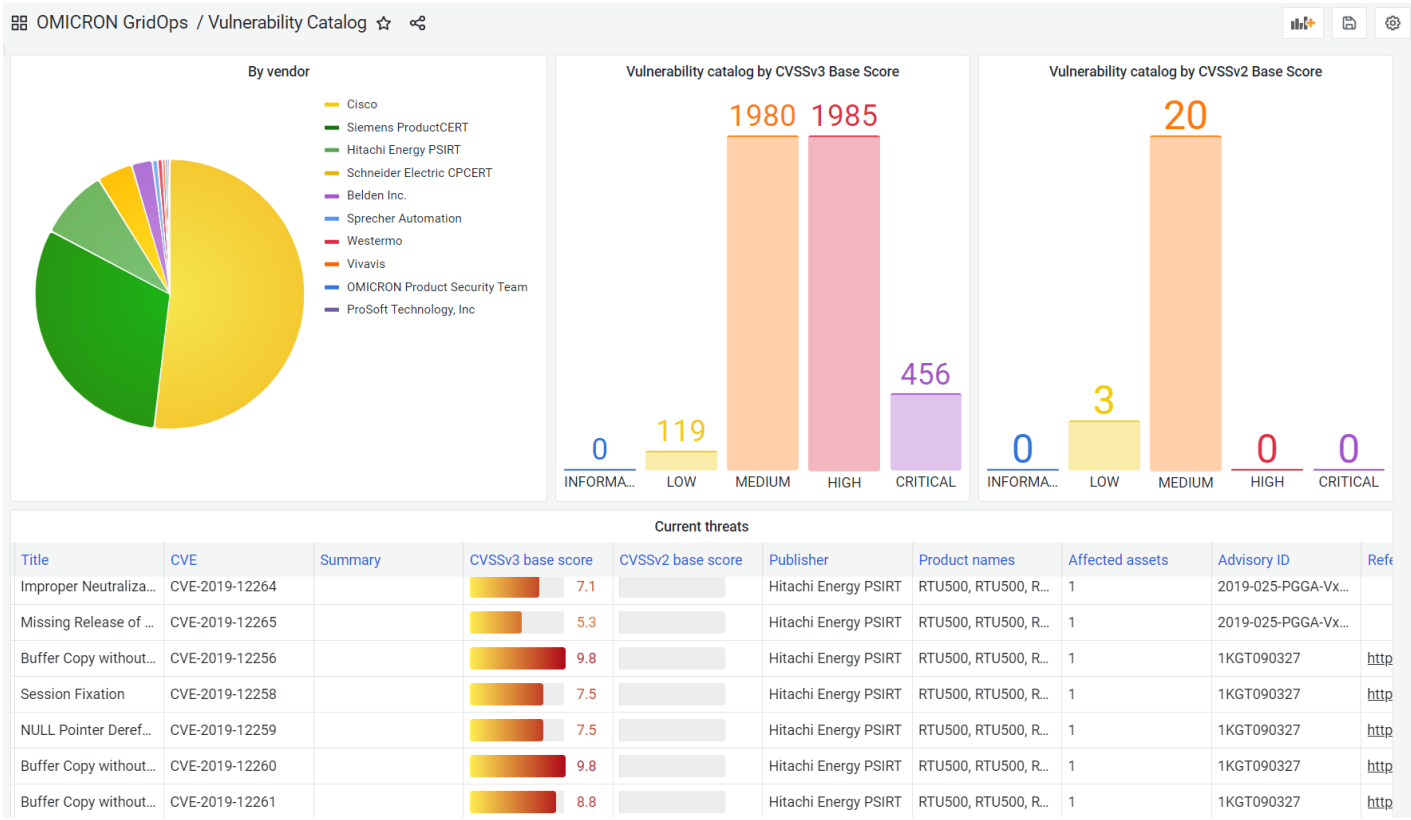
- Erfassung von Geräteinformationen mittels Tool (z.B. OMICRON StationGuard)
  - Passive Detektion im Netzwerk
  - Importieren von Engineering-Dateien (CSV, SCL)
  - Aktive Geräteabfrage über MMS-Protokoll
- Export und Import für Synchronisierung
  - mit ERP-Systemen (→CSV)
  - mit Daten aus Asset Management Systemen z.B. OMICRON ADMO



Wie lösen wir dieses Problem?

- OMICRON-Schwachstellen-Datenbank mit Geräte-Metainformationen.
- Damit melden wir nur die *wirklich zutreffenden* Schwachstellen.





Welche Hersteller unterstützen wir?

Unterstütze Hersteller

- Cisco
- Hirschmann/Belden/ProSoft
- Hitachi
- ABB
- Schneider Electric
- Siemens
- Sprecher
- Westermo
- Vivavis
- Fortinet
- Moxa
- ...

In Arbeit

- a-eberle
- GE
- ...

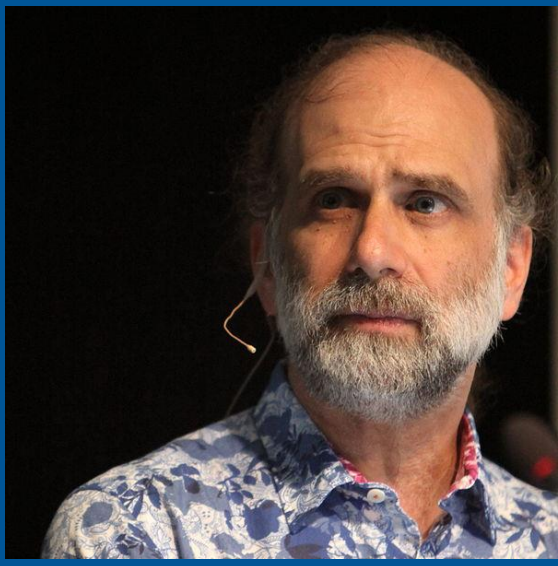
OMICRON

Zusammenarbeit in der Angriffserkennung

OMICRON

“You can't defend. You can't prevent. The only thing you can do is detect and respond.”

Bruce Schneier, einflussreicher Verschlüsselungs- und Securityexperte



Rama (Cc-by-sa-2.0-fr)

OMICRON

Angriffserkennung

- Eine Firewall alleine reicht nicht aus.
- Es gibt viele Angriffsvektoren auf Leitstellen, Kraftwerke und Schaltanlagen, die hinter der Firewall stattfinden.
- Netzwerkbasierte IDS identifizieren bösartige und unerlaubte Aktivitäten in Echtzeit.

NIS-Verordnung:

Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.

IEC ISA/IEC 62443-3-3 SR 6.2

SR 6.2 – Continuous monitoring .....
10.4.1 Requirement .....
10.4.2 Rationale and supplemental guidance
10.4.3 Requirement enhancements .....
10.4.4 Security levels .....

OMICRON

Warum Angriffserkennung oft scheitert

- Zunächst waren die Sekundärtechniker nicht in das Projekt eingebunden
  - *„Toll, jemand anderes kümmert sich um Security!“*
- Sie wurden später jedoch immer mehr hineingezogen:
  - *„Warum tut diese IP-Adresse dies?"*
  - *„Was bedeutet dieser IDS-Alarm?"*
- Mehr als 100 Warnmeldungen pro Monat:

  “MMS ConfirmedReques::Write on process variable ...PROTRPurcbSTa3.rptEna”
- SOC-as-a-Service Partner konnte auch nicht helfen ohne Schutz- und Leittechniker.

OMICRON

Ansatz in der OMICRON IDS StationGuard

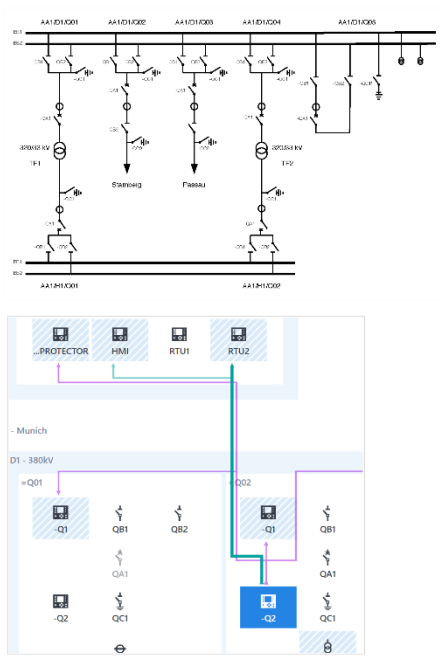
StationGuard *kennt* die Anlage

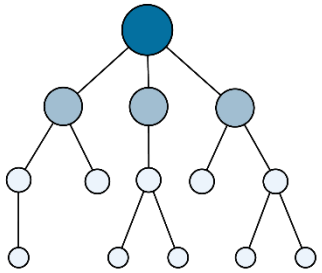
- Funktion jedes Geräts bekannt aus zugewiesenen Rollen
- Jedes Paket wird gegen dieses Systemmodell ausgewertet
  - Allowlist-Prinzip (Whitelist)
- Wartung und Prüfungen sind Teil des Modells

- Detaillierte Verifikation der gesamten Kommunikation
- Entdeckt nicht nur Cyber-Bedrohungen, sondern auch Fehlfunktionen

Funktionale Sicherheitsüberwachung

Anlagen-Beschreibung



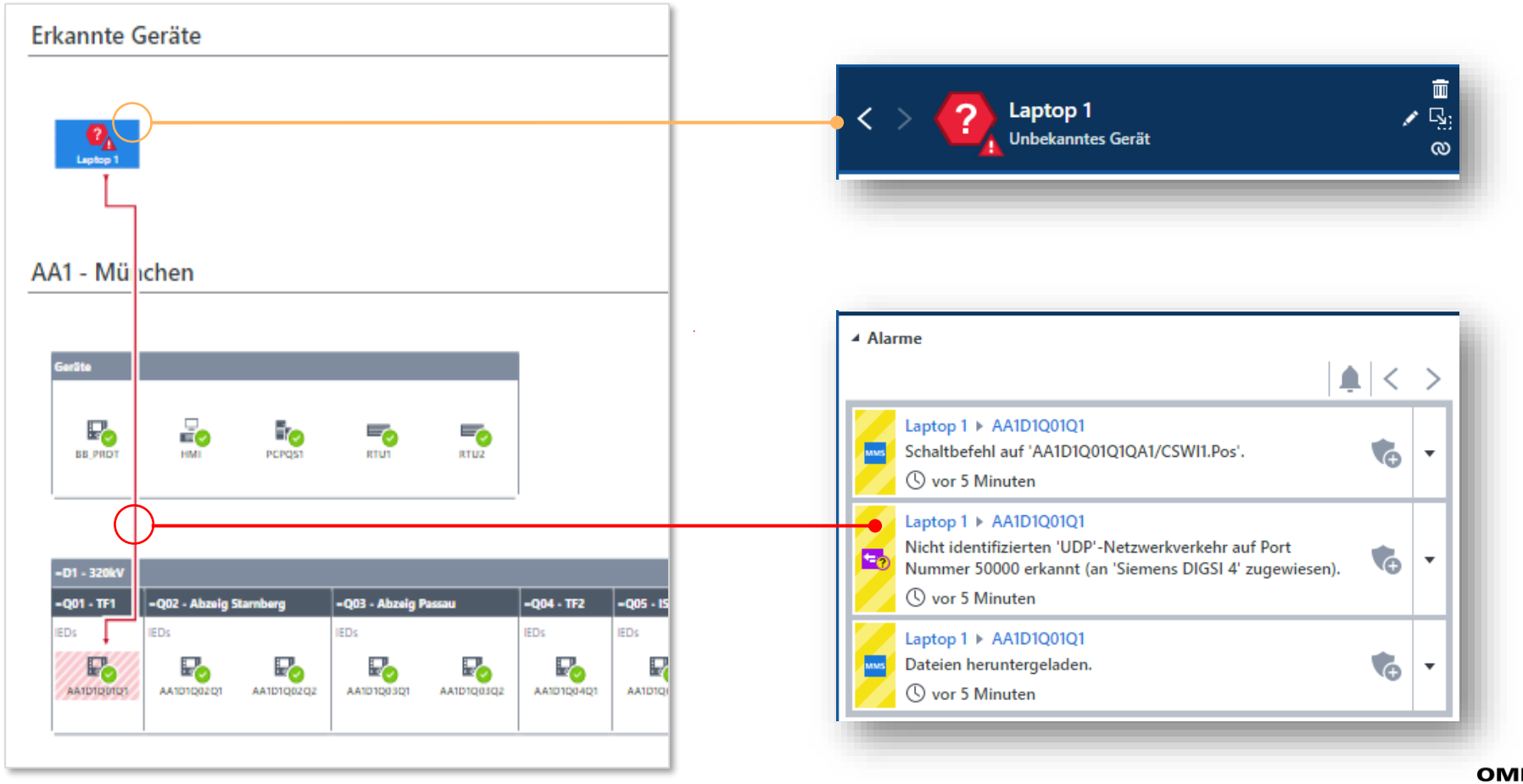


Systemmodell

OMICRON

Eingebautes OT-Wissen unterstützt Reaktionsprozesse

- Beispiel: IT-Security-Team sieht folgende IDS-Alarme:



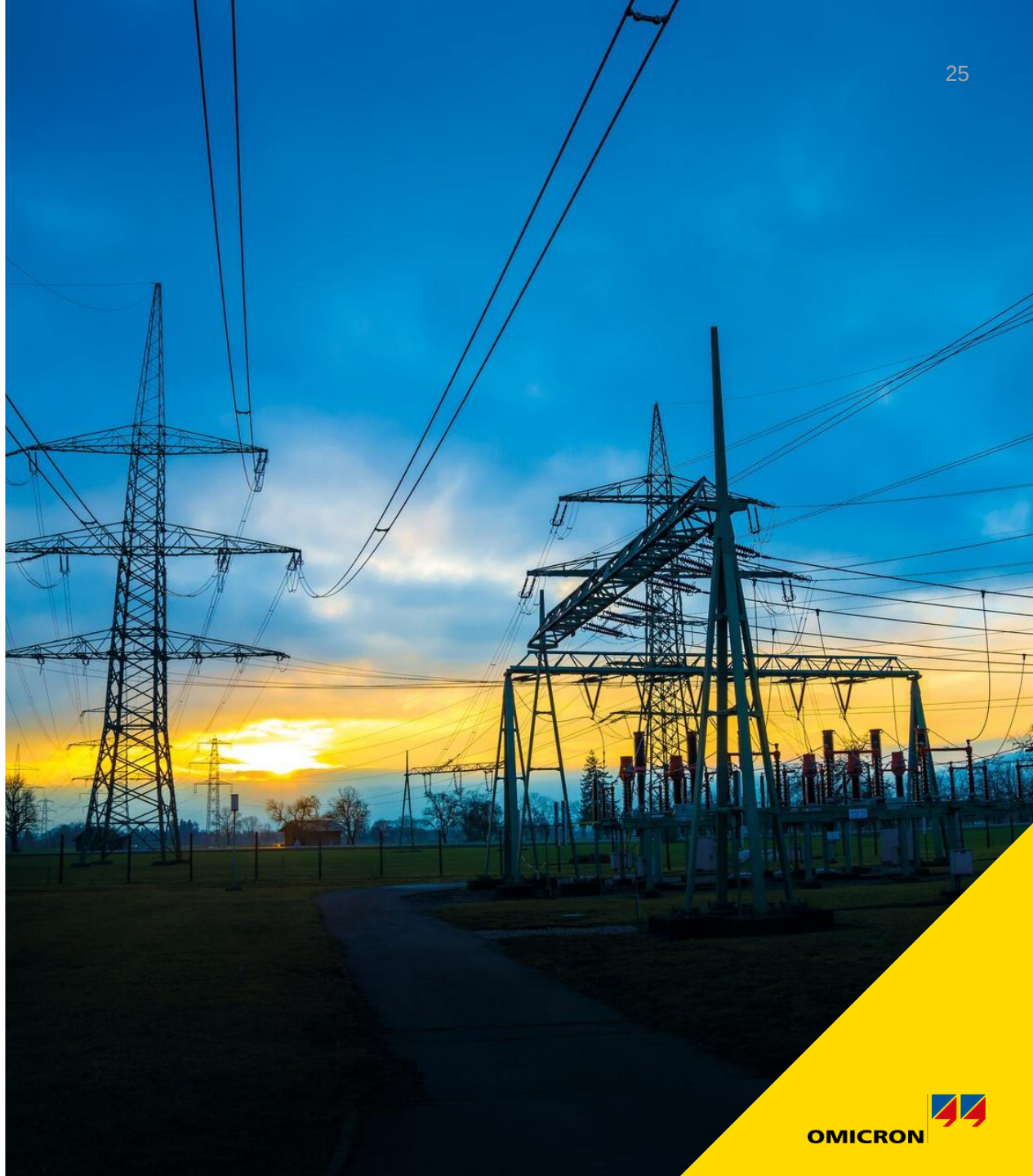
OMICRON

Zusammenfassung

- Nur ein gutes Asset-Inventory ermöglicht wirksames Schwachstellenmanagement.
- Automatisierung ist bei beidem möglich.

- Security-Tools mit eingebautem „OT-Wissen“ sparen Arbeit und ermöglichen zusammenarbeit.

Vielen Dank für die Aufmerksamkeit!



OMICRON