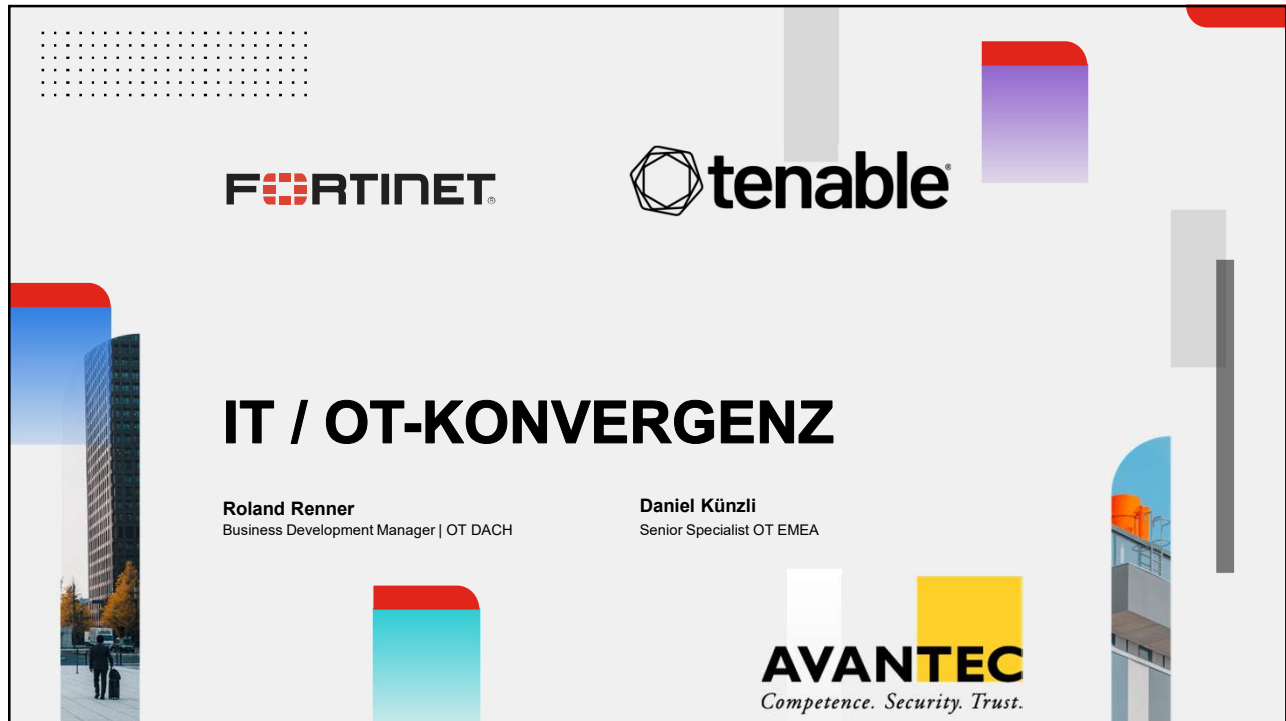


IT/OT-Security Webinar 07. & 12. September 2023



FORTINET **tenable**

IT / OT-KONVERGENZ

Roland Renner
Business Development Manager | OT DACH

Daniel Künzli
Senior Specialist OT EMEA

AVANTEC
Competence. Security. Trust.



OT IST ÜBERALL

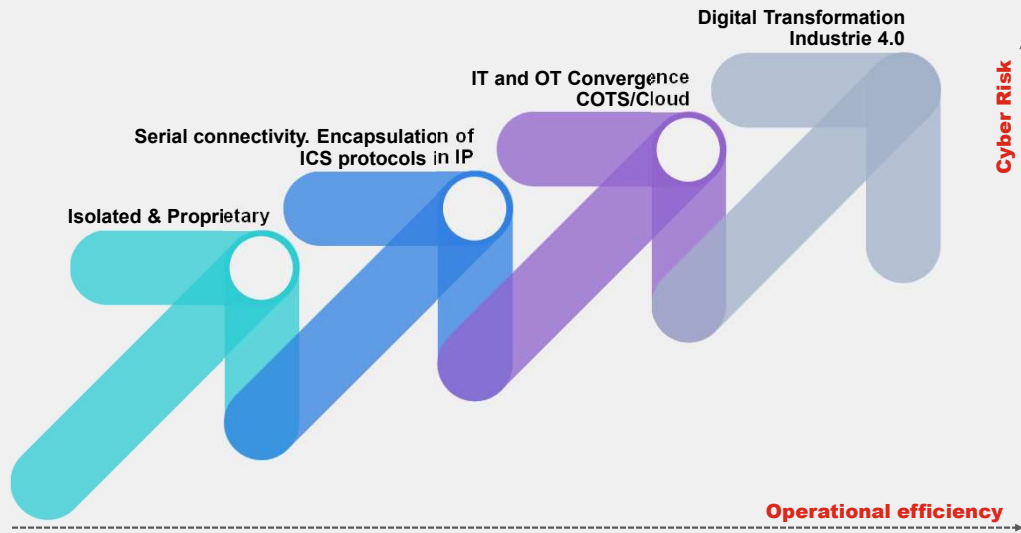


tenable

IT/OT-Security Webinar

07. & 12. September 2023

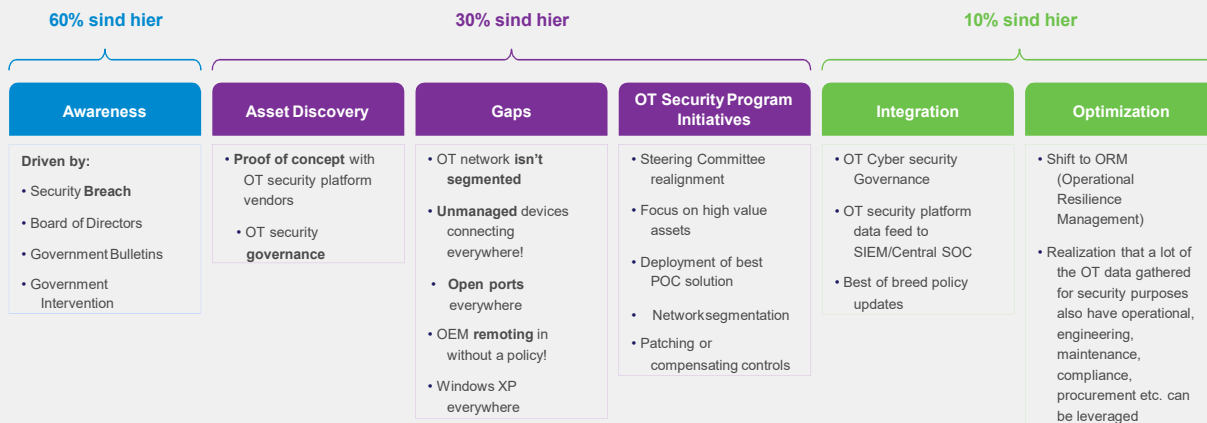
Evolution & Transformation OT



© Fortinet Inc. All Rights Reserved.

3

Aktueller Stand in der Industrie



Source – Gartner 2021



© Fortinet Inc. All Rights Reserved.

4

IT/OT-Security Webinar 07. & 12. September 2023

und die wichtigsten Herausforderungen sind

#	Herausforderungen
1	Schlechte OT-Sicherheitsrichtlinien, Risikolage, Sicherheits-Governance, Cyber-Sicherheitsfähigkeiten und -prozesse für OT-Netzwerke.
2	OT-Bedrohungsüberwachungsplattform zur Behebung von Problemen wie fehlender Asset-Inventarisierung, Sichtbarkeit von Sicherheitslücken, Netzwerkkonnektivität und potenzieller Angriffsfläche usw.
3	Führen Sie eine Netzwerktrennung zwischen IT- und OT-Netzwerken und eine OT-Netzwerksegmentierung durch.
4	Implementieren Sie Sicherheitskontrollen - Sicherer Fernzugriff, Zugriffsverwaltungsrichtlinien, Schwachstellen- und Patch-Management, Endpunktschutz, Firewall usw.
5	Zentralisierte Sicherheitsüberwachung und Sicherheitsbetrieb für OT-Netzwerke

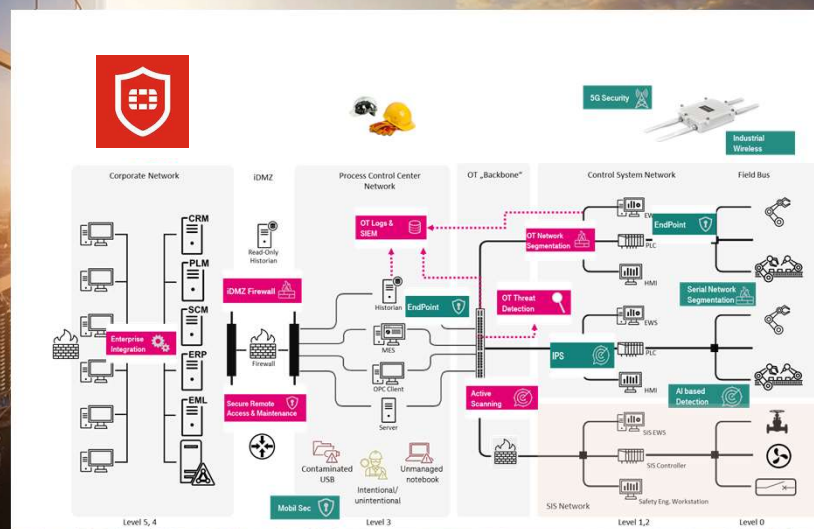


© Fortinet Inc. All Rights Reserved.

5

Derzeitige Verteidigungsmodelle und "Leitplanken"

- IEC 62443
- MITRE ATTACK ICS
- NIST
- ISO 27xxx
- SANS Sliding Scale for ICS
- KRITIS / NIS 2
- Security „Good Practice“



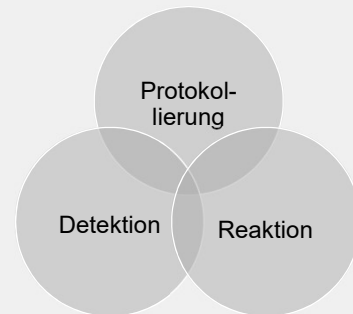
IT/OT-Security Webinar

07. & 12. September 2023

NIS2: Richtlinie für Netz- und Informationssicherheit

Mehr Kooperation mit & innerhalb der EU → Incident Response on EU Level

- **NIS-Richtlinie §12 möchte** „zur Entwicklung von Vertrauen zwischen den Mitgliedstaaten beitragen und **eine rasche und wirksame operative Zusammenarbeit** fördern“
- Technisch: **CSIRT-Zusammenschluss** (CSIRT = computer security incident response team) für Informationsaustausch innerhalb der EU (EU-CSIRT Netzwerk)
- Politisch: Aufsicht und **Zusammenarbeit** in der EU **zwischen Behörden und Betreibern** werden vertieft **durch CyCLONE** (Cyber Crises Liaison Organisation Network) für ein EU-weites Incident- & Krisenmanagement



© Fortinet Inc. All Rights Reserved.

7

InfoSec Teams auf der ganzen Welt haben die Aufgabe, die **gesamte** Angriffsfläche zu schützen

IT/OT-Security Webinar

07. & 12. September 2023

Aber ein
Schwachstellen- und
Sicherheitsprogramm
**kann nicht effektiv
sein...**



Aber ein
Schwachstellen- und
Sicherheitsprogramm
**kann nicht effektiv
sein...**



...es sei denn, es
inkludiert auch
OT-Geräte
mit ein

IT/OT-Security Webinar

07. & 12. September 2023



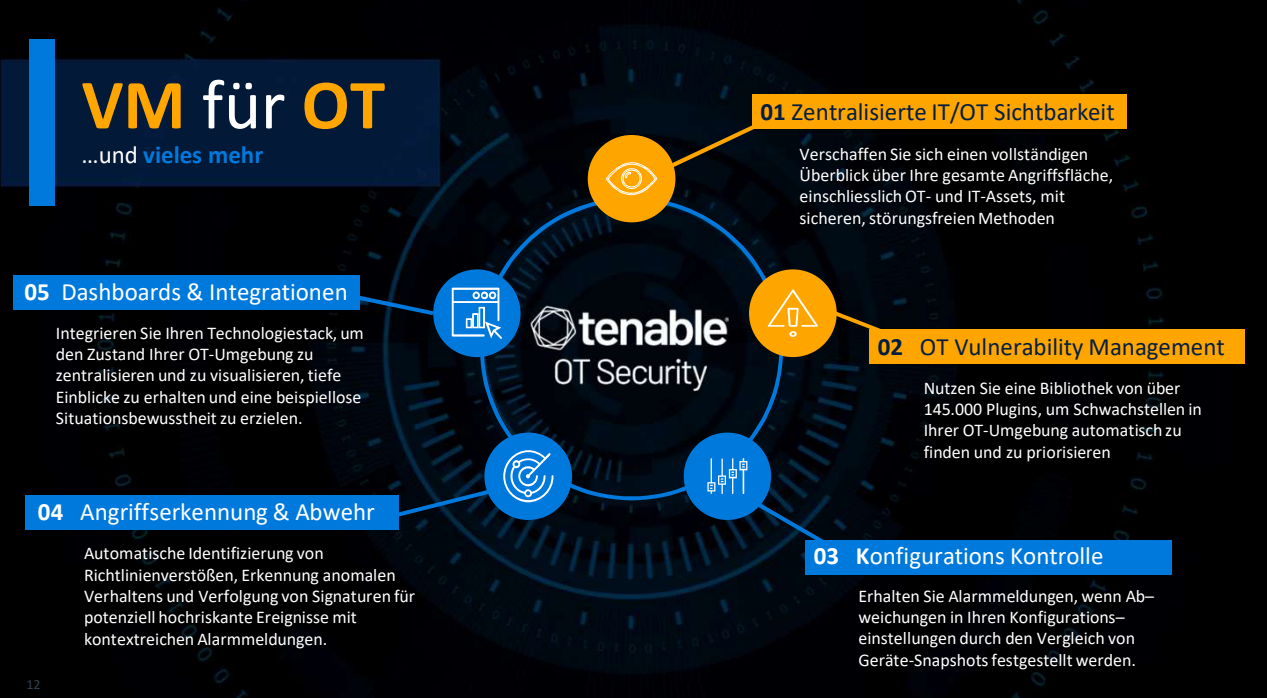
tenable OT Security

Erweitern Sie Ihr Schwachstellenmanagement auf Risiken für ihre **OT-Assets**.

tenable

VM für OT

...und vieles mehr



01 Zentralisierte IT/OT Sichtbarkeit

Verschaffen Sie sich einen vollständigen Überblick über Ihre gesamte Angriffsfläche, einschliesslich OT- und IT-Assets, mit sicheren, störungsfreien Methoden

02 OT Vulnerability Management

Nutzen Sie eine Bibliothek von über 145.000 Plugins, um Schwachstellen in Ihrer OT-Umgebung automatisch zu finden und zu priorisieren

03 Konfigurations Kontrolle

Erhalten Sie Alarmmeldungen, wenn Abweichungen in Ihren Konfigurationseinstellungen durch den Vergleich von Geräte-Snapshots festgestellt werden.

04 Angriffserkennung & Abwehr

Automatische Identifizierung von Richtlinienv Verstößen, Erkennung anomalen Verhaltens und Verfolgung von Signaturen für potenziell hochriskante Ereignisse mit kontextreichen Alarmmeldungen.

05 Dashboards & Integrationen


Integrieren Sie Ihren Technologiestack, um den Zustand Ihrer OT-Umgebung zu zentralisieren und zu visualisieren, tiefe Einblicke zu erhalten und eine beispiellose Situationsbewusstheit zu erzielen.

tenable OT Security

12

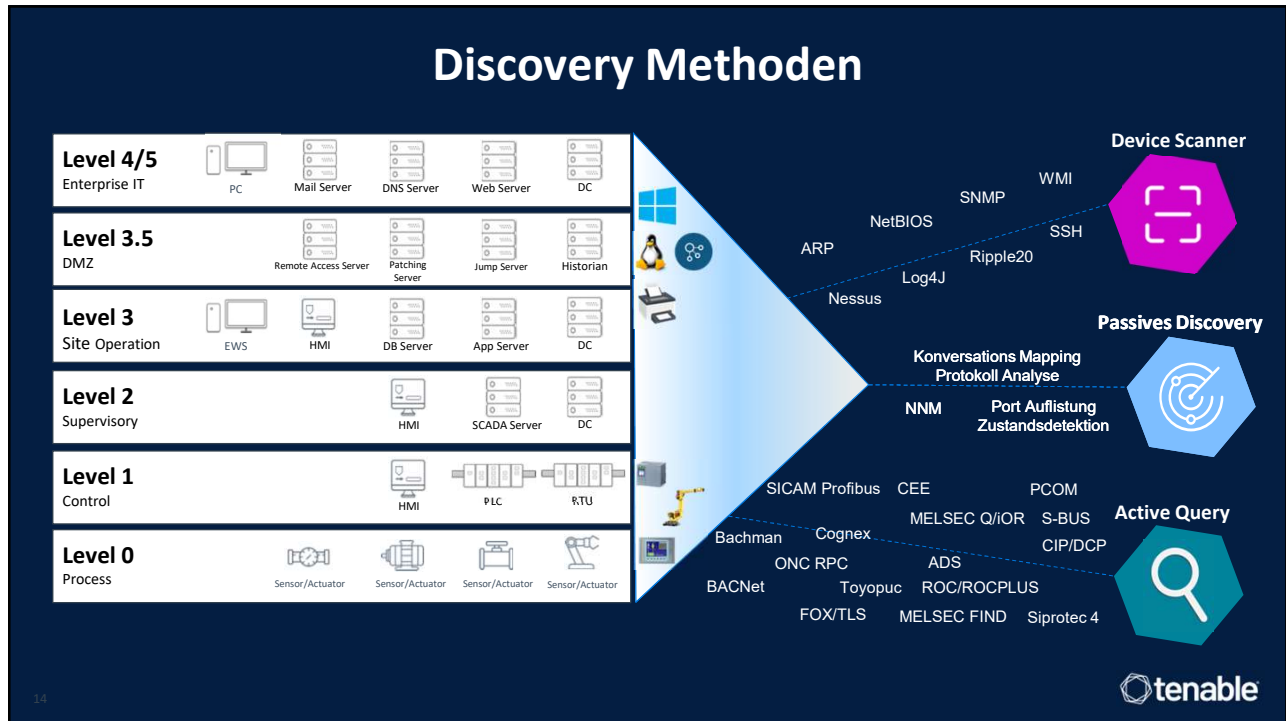
IT/OT-Security Webinar 07. & 12. September 2023

OT Dogma



Du sollst
nicht
scannen!!


13



14

IT/OT-Security Webinar 07. & 12. September 2023

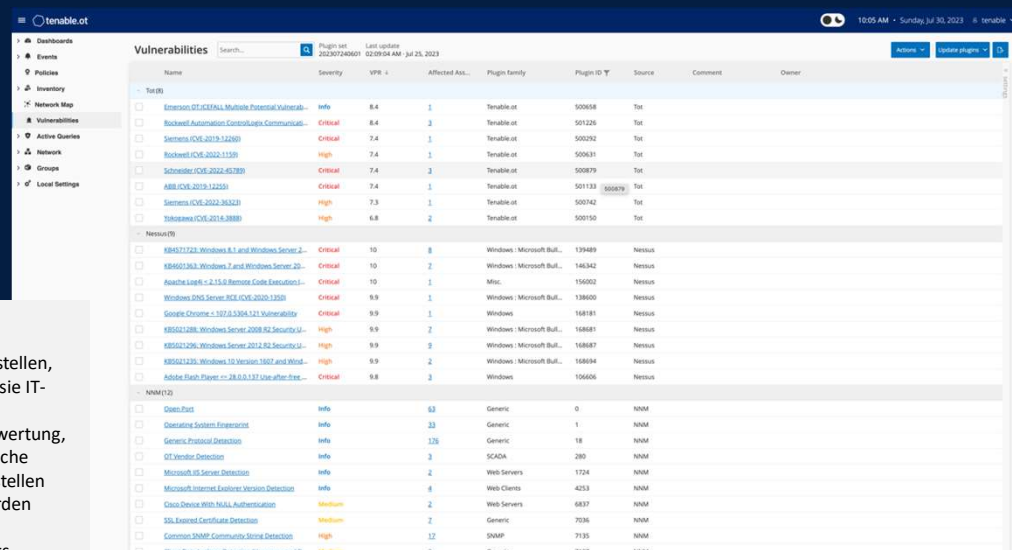
Hybrides Discovery – Asset Inventory



Vorteil Aktiver Anfragen:

- Patentierte Technologie
- Umfassende Situationskenntnis für sämtliche Assets
- Einblicke in Geräte, die nicht über das Netzwerk kommunizieren
- Genaues und stets aktualisiertes Anlagenverzeichnis
- Feinabstimmungsmöglichkeiten für die Durchführung aktiver Abfragen
- Sicher und unauffällig

Verfolgen und Priorisieren von Vulnerabilities



Vorteile:

- Verfolgen Sie Schwachstellen, unabhängig davon, ob sie IT- oder OT-basiert sind
- Nutzen Sie die VPR-Bewertung, um zu priorisieren, welche signifikantesten Schwachstellen zuerst angegangen werden sollten
- Nutzen Sie die Leistungs-fähigkeit und Erkenntnisse der Tenable-Forschung

IT/OT-Security Webinar 07. & 12. September 2023

Konfigurations-Kontrolle

Vorteile:

- Verfolgen Sie alle Änderungen, die an PLC's vorgenommen wurden
- Schnapsschüsse können zeit-, ereignis- oder benutzergesteuert sein
- Alle Abweichungen zwischen dem vorherigen und dem aktuellen Schnapsschuss werden hervorgehoben und alarmiert

The screenshot shows the Tenable OT console interface for a Yuval_L71 PLC. The main area displays a 'Code Revision' table with columns for Version, Date, and Name. The current version is 8, dated 03:25:03 PM - Sep 9, 2022. Below this, a detailed view of Version 8 is shown, including a tree structure of components like MainTask, Programs, and Routines. A 'Snapshots List' on the right shows various snapshot types and their timestamps.

Bedeutungsvolle Ereignisse und Kontext

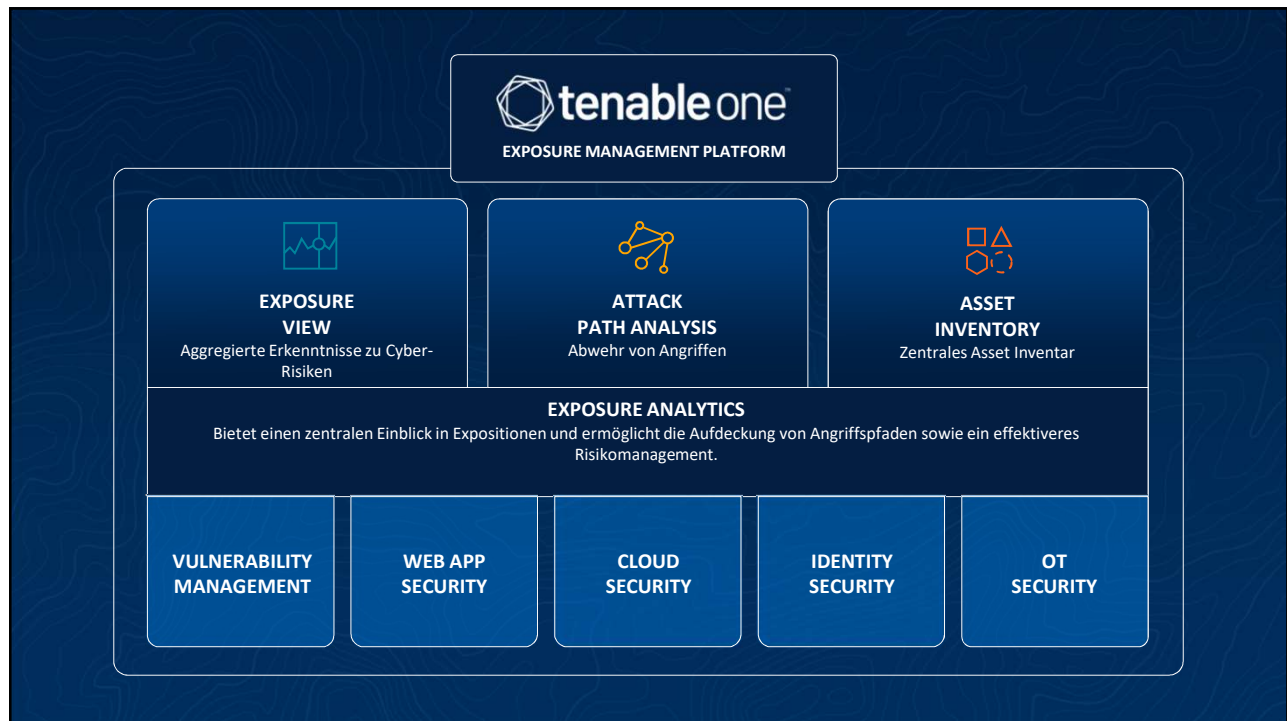
- CMDB Digitaler Zwilling – besserer Kontext, tiefere Einblicke
- Treffen Sie bessere Entscheidungen bei Ereignissen



The screenshot shows the Tenable OT console interface for a PLC configuration. The main area displays a 'Details' section with fields for Name, Description, Location, and Events. A 'Backplane View' section shows a diagram of the PLC backplane with modules and their connections.

IT/OT-Security Webinar

07. & 12. September 2023

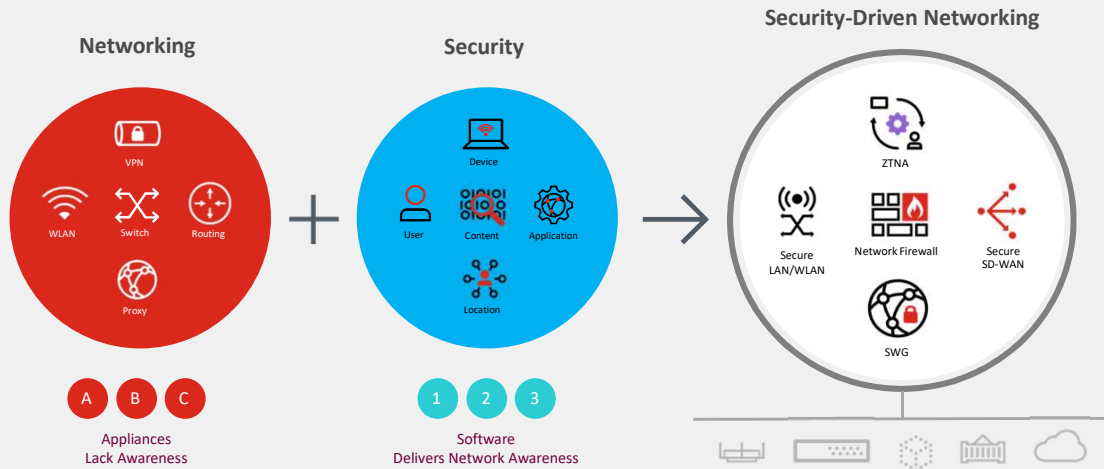


IT/OT-Security Webinar

07. & 12. September 2023

Konvergenz von Netzwerk und Security

Security Driven Networking



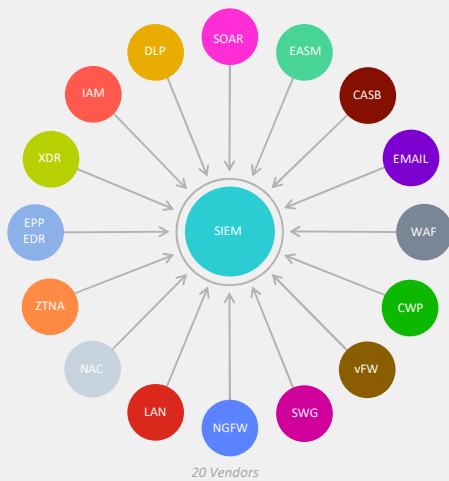
© Fortinet Inc. All Rights Reserved.

21

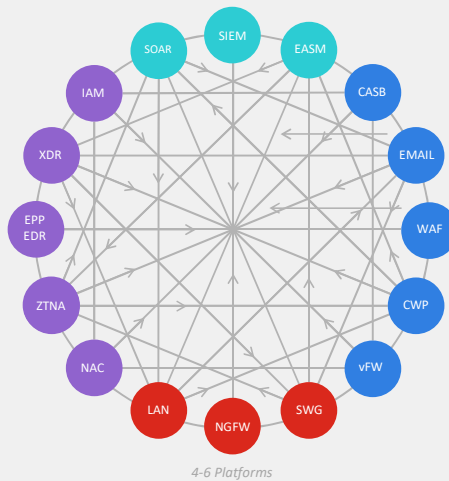
Konsolidierung von Anbietern von Sicherheitspunktprodukten

Gartner Cybersecurity MESH Architecture (CMSA)

Cybersecurity Point Products



Cybersecurity Platform Approach



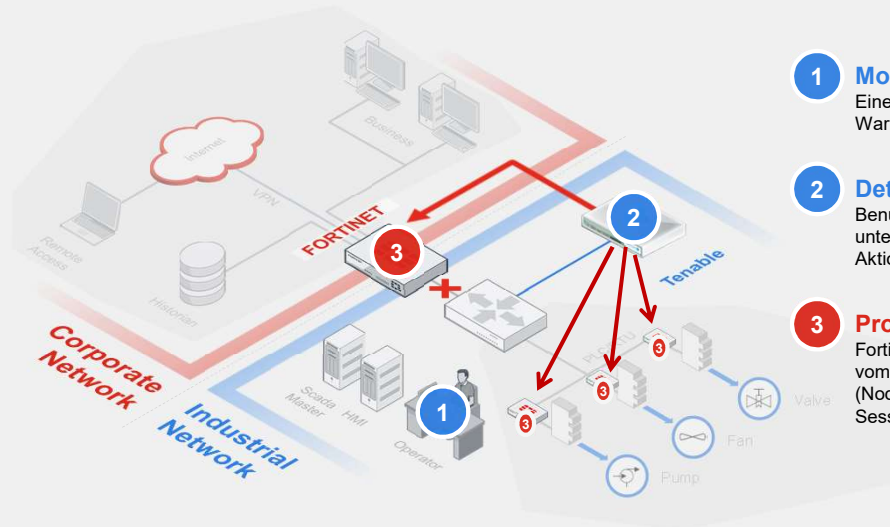
© Fortinet Inc. All Rights Reserved.

22

IT/OT-Security Webinar

07. & 12. September 2023

Reaktion auf Bedrohungen in Echtzeit



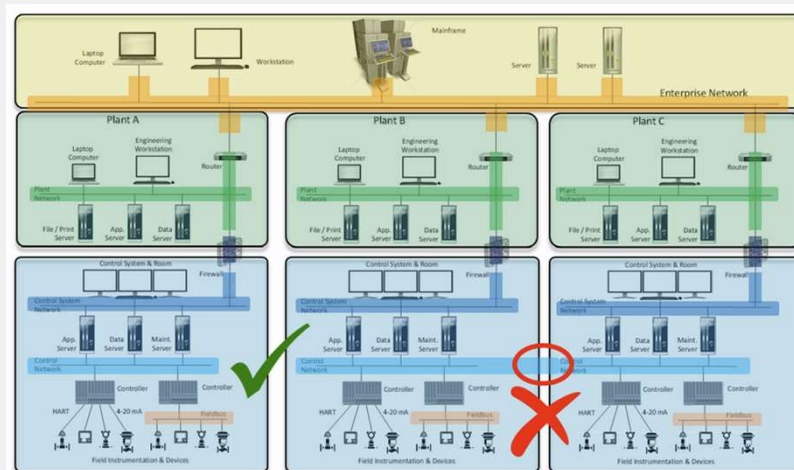
- 1 Monitor**
Eine Bedrohung wird erkannt und eine Warnung generiert
- 2 Detect**
Benutzerdefinierte Richtlinien werden untersucht und die entsprechende Aktion ausgelöst
- 3 Protect**
FortiGate reagiert entsprechend der vom Benutzer konfigurierten Aktion (Node Blocking, Link Blocking oder Kill Session), um das Problem zu beheben



© Fortinet Inc. All Rights Reserved.

23

Zonen / Zellen absichern (Micro-Segmentierung)



© Fortinet Inc. All Rights Reserved.

24

IT/OT-Security Webinar

07. & 12. September 2023

Fazit

Cyber Security ist kein Risiko für die Produktion wenn:



- Ich meine Ausgangssituation kenne und verstehe (OT-Umgebung, Assets und Schwachstellen, Ressourcen, Skills, Risiken)



- Ich die Umsetzung (Was, Wie, Reihenfolge, Abhängigkeiten) sorgfältig plane und Prozesse und Technologien teste



- Werkzeuge und Plattformen einsetze, die Komplexität verringern



- Externen Support einbinden, wenn mir intern Ressourcen oder KnowHow fehlt

Fortinet and Tenable



Better together

Detaillierte Konvergierte
Asset-Inventarisierung

Next-Generation Firewall
with Integrated Threat
Intelligence:

Verbesserte Reaktionszeit bei
Vorfällen

Risiko basiertes
Schwachstellenmanagement
für sämtliche Asset Typen

Zero Trust Network Access &
Secure SD-WAN:

Automatisierte &
Konfigurierbare Workflows

Bedrohungserkennung &
Konfigurationskontrolle:
(Früherkennung von
Sicherheitsrisiken)

End-to-End Visibility & AI-
Driven Security Operations:

Vereinheitlichte Sicherheitslage
durch 360-Grad-Überblick und
Compliance-Management

IT/OT-Security Webinar 07. & 12. September 2023

fordern Sie uns heraus



Roland Renner
Business Development Manager
Operational Technology DACH
☎ +49 173 66 29 423
rrenner@fortinet.com
<https://ready.fortinet.com/ot>
<https://www.fortinet.com/industrydemo>



Daniel Künzli
Sr. Specialist OT Security EMEA
☎ +41 79 449 40 16
dkunzli@tenable.com
<https://www.tenable.com/products/tenable-ot>
<https://www.tenable.com/solutions/it-ot>