OTScan 3

OT-/ICS-NETZWERKSCANNER · HANSELCRAFT

NETZWERK-CHECK

Montage_Anlagennetz

Scan 10.11.2026 14:20 – 10.11.2026 15:48 · Stufenlauf komplett

GELB

GERÄTE	UNSICHERE DIENSTE	HERSTELLERMELDUNGEN	STAND
22	19 Geräte	11 Geräte	10.11.2026 15:48

1 Auf einen Blick

GELB

Bewertung: Einige Geräte bieten Dienste an, die als unsicher gelten. Das ist kein Angriff, aber eine offene Tür, die geplant geschlossen werden sollte.

Was jetzt? Die Maßnahmen mit den Verantwortlichen der Anlage abstimmen und einplanen.

22 Geräte im Scan	**19** mit unsicheren Diensten	**19** davon ohne Firewall-Verkehr
11 mit Herstellermeldung	**3** neu für die CMDB	**0** in der CMDB, nicht gefunden

DAS WICHTIGSTE

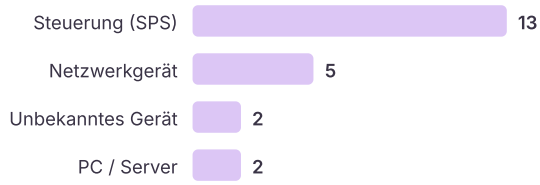
Info	Im Netzwerk Montage_Anlagennetz wurden 22 Geräte gefunden.
Achtung	19 von 22 Geräten bieten mindestens einen unsicheren Dienst an.
Achtung	9 Geräte sind laut Herstellermeldung betroffen (Firmware im betroffenen Bereich); bei 2 Geräten passt das Modell zu einer Meldung – Firmware am Gerät prüfen.
Achtung	2 Geräte sind nur im Firewall-Verkehr (Splunk 02.11.2026 – 08.11.2026) sichtbar, nicht im Scan – 2 Geräte davon nicht in der CMDB.
Achtung	38 von 38 unsicheren Diensten hatten im Splunk-Zeitraum 02.11.2026 – 08.11.2026 keinen Verkehr über die Firewall - Kandidaten zum Abschalten.
Achtung	Am häufigsten: HTTP auf 15 Geräten, SNMP auf 10 Geräten, Telnet auf 5 Geräten.
Info	Die meisten Geräte sind: Steuerung (SPS) (13 von 22).

2 Netzwerk und Geräte

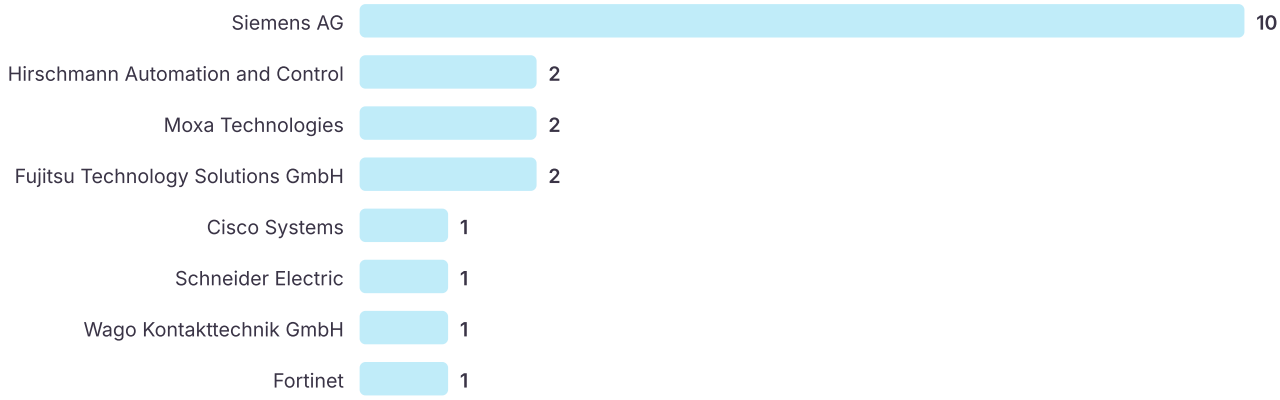
STECKBRIEF

Netzwerk	Montage_Anlagennetz
Scan von – bis	10.11.2026 14:20 – 10.11.2026 15:48
Dauer	1 Std. 28 Min.
Vollständig?	Ja
Scan-Profil	Stufenlauf komplett
Portauswahl	ICS_OT_CORE

GERÄTEKLASSEN

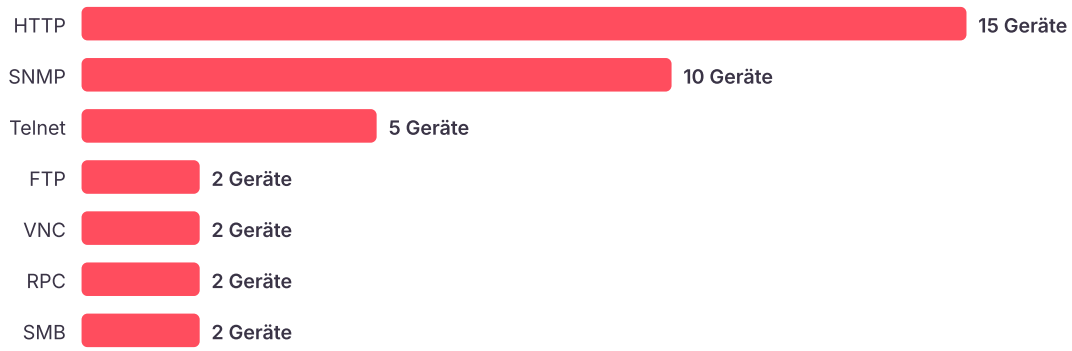


HERSTELLER



3 Unsichere Dienste

Dienste, die laut Verkehrsregeln nicht erlaubt sind oder abgesichert werden müssen. Dunkel = Anteil der Geräte ohne Verkehr über die Firewall – Kandidaten zum Abschalten.



WAS IST ZU TUN?

1. HTTP auf 15 Geräten: Auf HTTPS umstellen oder abschalten; Anmelden über HTTP ist laut Verkehrsregeln nicht erlaubt.
2. SNMP auf 10 Geräten: SNMPv1/v2c und 'public' sind laut Verkehrsregeln nicht erlaubt: auf SNMPv3 umstellen.
3. Telnet auf 5 Geräten: Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
4. FTP auf 2 Geräten: Laut Verkehrsregeln nicht erlaubt: abschalten, sonst SFTP oder FTPS nutzen.
5. Firewall-Regeln prüfen: Unsichere Dienste nur für die Rechner freigeben, die sie wirklich brauchen.
6. 2 Geräte nur aus Splunk im Netzwerk suchen (MAC/Switchport) und in die CMDB übernehmen – Vorlage: Datei „…_CMDB-Nachtrag.xlsx“.

17	99	17
Maßnahmen hoch	Maßnahmen mittel	Maßnahmen niedrig

Dringlichkeit = wie schnell und leicht sich etwas abstellen lässt, nicht das Risiko. Liste zum Abhaken: „…_Massnahmen.xlsx“.

4 Herstellermeldungen

Abgleich von Modell und Firmware mit den Meldungen der Hersteller. Güte „modell“ = Modell passt, Firmware am Gerät prüfen.

Meldung	Titel	Modell	CVSS	Güte	Geräte
SSA-001536	SSA-001536: Authorization Bypass Vulnerability in Siemens Industrial Edge Devices	SIMATIC HMI	10.0	hersteller	1
SEVD-2021-313-05	BadAlloc Vulnerabilities	Modicon M340 CPU, Firmware V2.70	9.8	modell	1
SSA-941426	SSA-941426: Multiple LLDP Vulnerabilities in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	9.8	modell	2
SSA-478893	SSA-478893: TightVNC Vulnerabilities in Industrial Products (Revoked)	SIMATIC HMI	9.8	hersteller	1
SSA-940818	SSA-940818: UltraVNC Vulnerabilities in SIMATIC HMIs/WinCC Products	SIMATIC HMI	9.8	hersteller	1
SSA-538778	SSA-538778: SmartVNC Vulnerabilities in SIMATIC HMI/WinCC Products	SIMATIC HMI	9.8	hersteller	1
SSA-452276	SSA-452276: Eval Injection Vulnerability in SIMATIC S7-1500	CPU 1516-3 PN/DP	9.6	exakt	1
SSA-591731	SSA-591731: Multiple Vulnerabilities in SIMATIC S7 PLCs Web Server	CPU 1516-3 PN/DP	9.6	exakt	1
SSA-699386	SSA-699386: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-	SCALANCE XC208 6GK5 208-0BA00-2AC2	9.1	exakt	1
SSA-710008	SSA-710008: Multiple Web Vulnerabilities in SCALANCE Products	SCALANCE XC208 6GK5 208-0BA00-2AC2	9.1	exakt	1
SSA-832641	SSA-832641: Path Traversal Vulnerabilities in Siemens Industrial Edge Devices	SIMATIC HMI	9.1	hersteller	1
SSA-688146	SSA-688146: Multiple Cross-Site Scripting Vulnerabilities in SIMATIC S7 PLCs Web Server	CPU 1516-3 PN/DP	9.1	exakt	1
SSA-723487	SSA-723487: RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCA	SCALANCE XC208 6GK5 208-0BA00-2AC2	9.0	exakt	1
SSA-552702	SSA-552702: Privilege Escalation Vulnerability in the Web Interface of SCALANCE and RUGGED	SCALANCE XC208 6GK5 208-0BA00-2AC2	8.8	exakt	1
ICSA-19-346-02	Omron PLC CJ and CS Series	Omron NX1P2 1.40	8.6	modell	1
SSA-328642	SSA-328642: "Copy Fail" Vulnerability in Multiple Industrial Products	SIMATIC HMI	7.8	hersteller	1
SSA-387223	SSA-387223: Unauthenticated Control Panel Escape Vulnerability on SIMATIC HMI Unified Comf	SIMATIC HMI	7.7	hersteller	1
SSA-712929	SSA-712929: Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industria	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC, CPU 1516-3	7.5	modell	7

Meldung	Titel	Modell	CVSS	Güte	Geräte
SSA-473245	SSA-473245: Denial of Service Vulnerability in Profinet Devices	CPU 315-2 PN/DP, CPU 317-2 PN/DP, SIMATIC HMI, Sie	7.5	modell	4
SSA-711309	SSA-711309: Denial of Service Vulnerability in the OPC UA Implementations of SIMATIC Produ	CPU 1516-3 PN/DP, Siemens TP1200 Comfort V16	7.5	modell	2
SSA-384224	SSA-384224: Denial of Service Vulnerability in SIMATIC HMI Panels	SIMATIC HMI, Siemens TP1200 Comfort V16	7.5	modell	2
SSA-593272	SSA-593272: SegmentSmack in Interniche IP-Stack based Industrial Devices	CPU 315-2 PN/DP, CPU 317-2 PN/DP	7.5	exakt	2
SSA-349422	SSA-349422: Denial of Service Vulnerability in Industrial Real-Time (IRT) Devices	CPU 315-2 PN/DP, CPU 317-2 PN/DP	7.5	exakt	2
SSA-480230	SSA-480230: Denial of Service Vulnerability in Webserver of Industrial Products	CPU 315-2 PN/DP, CPU 317-2 PN/DP, SIMATIC HMI	7.5	exakt	3
SSA-915282	SSA-915282: Denial of service Vulnerability in Interniche IP-Stack based Industrial Device	CPU 1214C DC/DC/DC, CPU 1516-3 PN/DP, CPU 315-2 PN	7.5	exakt	4
SSA-392349	SSA-392349: Denial of Service Vulnerability in Industrial Devices	CPU 1516-3 PN/DP, CPU 315-2 PN/DP, CPU 317-2 PN/DP	7.5	exakt	3
SSA-599968	SSA-599968: Denial of Service Vulnerability in Profinet Devices	CPU 1214C DC/DC/DC	7.5	exakt	2
SSA-224824	SSA-224824: Denial of Service Vulnerabilities in SIMATIC S7-1200 CPU Family Before V4.7	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC	7.5	exakt	3
ICSA-18-317-08	Siemens SIMATIC Panels	SIMATIC HMI	7.5	modell	1
SSA-307392	SSA-307392: Denial of Service in OPC UA in Industrial Products	SIMATIC HMI	7.5	hersteller	1
SSA-592380	SSA-592380: Denial of Service Vulnerability in SIMATIC S7-1500 CPUs and related products	CPU 1516-3 PN/DP	7.5	exakt	1
SSA-382653	SSA-382653: Multiple Denial of Service Vulnerabilities in Industrial Products	CPU 1516-3 PN/DP	7.5	exakt	1
SSA-244969	SSA-244969: OpenSSL Vulnerability in Industrial Products	CPU 1214C DC/DC/DC	7.4	exakt	2
SSA-264815	SSA-264815: Type Confusion Vulnerability in OpenSSL X.400 Address Processing in SIMATIC Pr	CPU 1516-3 PN/DP	7.4	exakt	1
SSA-717113	SSA-717113: Cross-Site Request Forgery (CSRF) Vulnerability in SIMATIC S7-1200 CPUs before	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC	7.1	exakt	3
ICSA-15-099-01E	Siemens SIMATIC HMI Devices Vulnerabilities (Update E)	SIMATIC HMI	6.8	hersteller	1
SEVD-2021-222-04	Modicon PAC Controllers and PLC Simulator for EcoStruxure™ Control Expert and EcoStruxure™	Modicon M340 CPU, Firmware V2.70	6.5	modell	1
SSA-542525	SSA-542525: Authentication Vulnerabilities in SIMATIC HMI Products	SIMATIC HMI, Siemens TP1200 Comfort V16	6.5	modell	2
SSA-285795	SSA-285795: Denial of Service in OPC-UA in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	6.5	modell	2

Meldung	Titel	Modell	CVSS	Güte	Geräte
SSA-592007	SSA-592007: Denial of Service Vulnerability in Industrial Products	CPU 315-2 PN/DP, CPU 317-2 PN/DP	6.5	exakt	2
SSA-478960	SSA-478960: Missing CSRF Protection in the Web Server Login Page of Industrial Controllers	CPU 1516-3 PN/DP, CPU 315-2 PN/DP, CPU 317-2 PN/DP	6.5	exakt	3
SSA-413565	SSA-413565: Multiple Vulnerabilities in SCALANCE Products	SCALANCE XC208 6GK5 208-0BA00-2AC2	6.5	exakt	1
SSA-293562	SSA-293562: Denial of Service Vulnerabilities in PROFINET DCP Implementation of Industrial	SIMATIC HMI	6.5	modell	1
SSA-772220	SSA-772220: OpenSSL Vulnerabilities in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	5.9	modell	2
SSA-423808	SSA-423808: Multiple NULL Pointer Dereference Vulnerabilities in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	5.9	modell	2
SSA-264814	SSA-264814: Timing Based Side Channel Vulnerability in the OpenSSL RSA Decryption in SIMAT	CPU 1516-3 PN/DP, CPU 315-2 PN/DP, CPU 317-2 PN/DP	5.9	exakt	3
SSA-179516	SSA-179516 OpenSSL Vulnerability in Industrial Products	SIMATIC HMI	5.9	modell	1
ICSA-20-196-04	Siemens SIMATIC HMI Panels	SIMATIC HMI, Siemens TP1200 Comfort V16	5.7	modell	2
SSA-446448	SSA-446448: Denial of Service Vulnerability in PROFINET Stack Integrated on Interniche Sta	CPU 315-2 PN/DP, CPU 317-2 PN/DP	5.3	exakt	2
SSA-725549	SSA-725549: Denial of Service of ICMP in Industrial Devices	CPU 1214C DC/DC/DC, CPU 1516-3 PN/DP, CPU 315-2 PN	5.3	exakt	4
SSA-195895	SSA-195895: User Enumeration Vulnerability in the Webserver of SIMATIC Products	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC	5.3	exakt	3
SSA-594364	SSA-594364: Denial-of-Service Vulnerability in SNMP Implementation of WinCC Runtime	SIMATIC HMI	5.3	modell	1
SSA-054046	SSA-054046: Unauthenticated Information Disclosure in Web Server of SIMATIC S7-1500 CPUs	CPU 1516-3 PN/DP	5.3	exakt	1
SSA-353002	SSA-353002: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-	SCALANCE XC208 6GK5 208-0BA00-2AC2	4.9	exakt	1
SSA-876787	SSA-876787: Open Redirect Vulnerability in SIMATIC S7-1500 and S7-1200 CPUs	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC, CPU 1516-3	4.7	exakt	4
ICSA-15-064-01	Siemens SIMATIC HMI Basic, SINUMERIK, and Ruggedcom APE GHOST Vulnerability	SIMATIC HMI	4.6	hersteller	1
ICSA-15-064-01A	Siemens SIMATIC HMI Basic, SINUMERIK, and Ruggedcom APE GHOST Vulnerability (Update A)	SIMATIC HMI	4.6	hersteller	1
SSA-482757	SSA-482757: Missing Immutable Root of Trust in S7-1500 CPU devices	CPU 1516-3 PN/DP	4.6	exakt	1
ICSA-18-317-03	Siemens SIMATIC Panels and SIMATIC WinCC (TIA Portal)	SIMATIC HMI	4.3	modell	1

Meldung	Titel	Modell	CVSS	Güte	Geräte
SSA-273799	SSA-273799: Message Integrity Protection Bypass Vulnerability in SIMATIC Products	SIMATIC HMI	3.7	modell	1
SESB-2019-214-01	Wind River VxWorks Vulnerabilities (URGENT/11)	Modicon M340 CPU, Firmware V2.70	0.0	modell	1

5 Inventar und Applikationen

Jedes Gerät aus CMDB, Scan und Firewall-Verkehr (Splunk) – zusammengeführt über IP, sonst MAC.



bestätigt (alle Quellen) **19** neu für die CMDB **3** nur Verkehr, unbekannt **2**

APPLIKATIONEN IM FIREWALL-VERKEHR

Zuordnung der Kommunikationspartner über die Dokumentations-Datenbank.

Applikation / System	Zone	Verbindungen
MES Produktionsdaten	Z-Produktion	927.005
Prozessleitsystem	Z-Leitebene	135.954
Zeitdienst und Protokollierung	Z-Infrastruktur	42.355
MES Produktionsdaten	Z-Engineering	1.449
Fernwartung	Z-DMZ	61

ZU KLÄREN (5)

Status	IP-Adresse	Name	Typ	Hersteller	Hinweis
neu für die CMDB	192.168.30.1	–	Netzwerkgerät	Fortinet	unsichere Dienste ohne Firewall-Verkehr – Abschalten prüfen
neu für die CMDB	192.168.30.17	–	Steuerung (SPS)	Siemens AG	
neu für die CMDB	192.168.30.26	–	Steuerung (SPS)	Siemens AG	unsichere Dienste ohne Firewall-Verkehr – Abschalten prüfen
nur Verkehr, unbekannt	192.168.30.90	–	–	Siemens AG	
nur Verkehr, unbekannt	192.168.30.91	–	–	Wago Kontakttechnik GmbH	

A Anhang: dringliche Maßnahmen (Auszug)

Nr.	IP-Adresse	CMDB-Name	Gerät	Was	Empfehlung
1	192.168.30.2	H3-MO-SW-01	Netzwerkgerät	SSA-699386: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family before V4.5	Update to V4.5 or later version
2	192.168.30.2	H3-MO-SW-01	Netzwerkgerät	SSA-710008: Multiple Web Vulnerabilities in SCALANCE Products	Update to V4.4 or later version
3	192.168.30.2	H3-MO-SW-01	Netzwerkgerät	SSA-723487: RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related P	Update to V4.6 or later version
4	192.168.30.3	H3-MO-SW-02	Netzwerkgerät	Telnet (TCP 23)	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
5	192.168.30.4	H3-MO-SW-03	Netzwerkgerät	Telnet (TCP 23)	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
6	192.168.30.12	H3-MO-SPS-L3	Steuerung (SPS)	SSA-452276: Eval Injection Vulnerability in SIMATIC S7-1500	Update to V2.9.9 or later version
7	192.168.30.12	H3-MO-SPS-L3	Steuerung (SPS)	SSA-591731: Multiple Vulnerabilities in SIMATIC S7 PLCs Web Server	Disable the webserver if not required on the affected systems. Restrict the access to Port 80/tcp and 443/tcp to trusted IP address only
8	192.168.30.12	H3-MO-SPS-L3	Steuerung (SPS)	SSA-688146: Multiple Cross-Site Scripting Vulnerabilities in SIMATIC S7 PLCs Web Server	Restrict TIA project download to trusted personnel only.
9	192.168.30.20	H3-MO-SPS-FT	Steuerung (SPS)	FTP (TCP 21)	Laut Verkehrsregeln nicht erlaubt: abschalten, sonst SFTP oder FTPS nutzen.
10	192.168.30.22	H3-MO-AS-01	Steuerung (SPS)	FTP (TCP 21)	Laut Verkehrsregeln nicht erlaubt: abschalten, sonst SFTP oder FTPS nutzen.
11	192.168.30.25	H3-MO-HMI-01	Steuerung (SPS)	VNC (TCP 5900)	Laut Verkehrsregeln nicht erlaubt: abschalten oder nur verschlüsselt (TLS, VPN, SSH-Tunnel).
12	192.168.30.26	–	Steuerung (SPS)	VNC (TCP 5900)	Laut Verkehrsregeln nicht erlaubt: abschalten oder nur verschlüsselt (TLS, VPN, SSH-Tunnel).
13	192.168.30.30	H3-MO-GW-01	Unbekanntes Gerät	Telnet (TCP 23)	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
14	192.168.30.31	H3-MO-GW-02	Unbekanntes Gerät	Telnet (TCP 23)	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
15	192.168.30.60	H3-MO-ENG-01	PC / Server	SMB (TCP 445)	SMBv1 abschalten (laut Verkehrsregeln nicht erlaubt), SMBv3 mit Signierung, Zugriff begrenzen.
16	192.168.30.61	H3-MO-BED-01	PC / Server	SMB (TCP 445)	SMBv1 abschalten (laut Verkehrsregeln nicht erlaubt), SMBv3 mit Signierung, Zugriff begrenzen.

Nr.	IP-Adresse	CMDB-Name	Gerät	Was	Empfehlung
17	192.168.30.102	H3-MO-GER-52	Netzwerkgerät	Telnet (TCP 23)	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.

B Begriffe

CMDB	Inventar (CMDB): die selbst gepflegte Geräteliste als Excel (Vorlage aus OTScan 3 oder eigene Liste). Liefert Name, Typ, Hersteller, Ort, Gewerk und Verantwortliche. OTScan 3 liest sie nur.
Gesamtinventar	Eine Excel mit allen Geräten aus CMDB, Scan und Splunk – je Wert mit Quelle. Grundlage der Erstinventarisierung.
Dokumentations-Datenbank	Applikationen, Server, Zonen und Netzwerkbereiche aus der Netzwerk- und Applikationsübersicht und dem Recherche-Register. OTScan 3 ordnet damit Kommunikationspartner Applikationen zu.
Scan / Stufenlauf	Aktive Erkennung durch OTScan 3 in Stufen (Erreichbarkeit, Dienste, Geräteangaben).
Splunk	Auswertung der Firewall-Logs: Adressen, Partner, Ports, Zonen. Verkehr innerhalb eines Netzwerks ist dort nicht sichtbar.
Ampel	GRÜN = keine unsicheren Dienste. GELB = unsichere Dienste – geplant schließen. ROT = besonders gefährliche Dienste – sofort klären.
Unsicherer Dienst	Dienst, den die Verkehrsregeln (HanselCraft-Voreinstellung, anpassbar) verbieten oder nur abgesichert erlauben (z. B. FTP, Telnet, HTTP-Anmeldung, SNMPv1/v2c).
Ohne Firewall-Verkehr	Der Dienst wurde im Splunk-Zeitraum nicht über die Firewall genutzt – Kandidat zum Abschalten.
Herstellermeldung	Sicherheitsmeldung eines Herstellers (CSAF, CISA ICS). Güte exakt / modell / hersteller.
Zone / Service / Policy	Aus dem FortiGate-Log: Sicherheitszone von Quelle und Ziel, Dienstname, Nummer der Firewall-Regel.
Risk (Detailansicht)	2 Punkte je kritischem Port (höchstens 8), +2 bei Herstellermeldung mit CVSS ≥ 7, +1 bei schwächerer Meldung.