BERICHTE

Berichte lesen

Ampel und Verkehrsregeln, PDF, Excel, Maßnahmenliste, Netzwerk-Check, Geräte-Detailansicht, CMDB-Delta und -Nachtrag, Gesamtinventar, Standortbericht.

1 Welcher Bericht für wen?

Leser	Bericht	Datei
Anlagenverantwortliche	PDF-Kompaktbericht	`<Netzwerk>_<Zeit>_stufenlauf.pdf`
Technik, Gewerke	Excel je Netzwerk, Maßnahmenliste	`…_stufenlauf.xlsx`, `…_Massnahmen.xlsx`
Management	PowerPoint	`…_manager.pptx`
Audit, Fachleute	PDF ausführlich, Netzwerk-Check, Geräte-Detailansicht	`…_ausfuehrlich.pdf`, `…_Netzwerk-Check.pdf`, `…_Geraete-Details.pdf`
Inventarisierung	CMDB-Delta, CMDB-Nachtrag, Gesamtinventar	`…_CMDB-Delta.xlsx`, `…_CMDB-Nachtrag.xlsx`, `OTScan3_Gesamtinventar_<Datum>.xlsx`
Standortleitung	Standortbericht, Geräteverzeichnis	`OTScan3_Standortbericht_<Datum>.pdf`, `OTScan3_Geraeteverzeichnis_<Datum>.pdf`

Alle Abbildungen stammen aus dem erfundenen **Musterwerk Halle 3** (6 Netzwerke der Fertigung, 115 Geräte: Anlagennetz Montage, Maschinennetz Presse, Leitstand Lackiererei, Prüffeld, Energieverteilung, Kameranetz). Namen, Adressen und Netze sind erfunden; Gerätetypen, Firmwarestände und offene Dienste entsprechen typischen Funden in gewachsenen Fertigungsnetzen. Dieselben Dateien öffnet OTScan 3 im Fenster **Berichte & Muster …** mit **Muster ansehen**.

2 Die Ampel und die Verkehrsregeln

Ampel	Bedeutung	Was tun
GRÜN	Kein offener Dienst, den die Verkehrsregeln als unsicher einstufen.	Nichts Dringendes; Scan regelmäßig wiederholen.
GELB	Mindestens ein Port aus den Verkehrsregeln ist offen (z. B. Telnet, FTP, HTTP, SNMPv1/v2c, SMB, VNC).	Mit dem Betreiber klären und geplant schließen.
GRAU	Keine Bewertung möglich: Geräte haben geantwortet, aber keine Angaben zu ihren Diensten geliefert.	Scan mit einem schonenderen Profil wiederholen.

Steht in der Fußzeile eines Berichts „UNVOLLSTÄNDIG“ (z. B. Host-Timeouts oder abgebrochene Stufe), den Scan wiederholen, bevor Sie Schlüsse ziehen.

> Die **Verkehrsregeln** sind eine HanselCraft-Voreinstellung für unsichere IT-Protokolle in OT-Netzwerken, angelehnt an IEC 62443 (Zonen und Conduits). Sie sind keine Norm. Gewichte (1–3 je Port) ergeben den Risk-Wert eines Geräts. Anpassen: `verkehrsregeln.json` im Datenordner (Ports entfernen, hinzufügen, Gewichte und Texte ändern; wirkt nach Neustart).

3 PDF-Kompaktbericht



OTScan 3 - Netzwerkbericht Montage_Anlagennetz

Montage_Anlagennetz

192.168.30.0/24 | Stufenlauf komplett | Scan 10.11.2026 14:20, Dauer 1 Std. 28 Min.

Ampel GELB: Handlungsbedarf

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

22	19	38	2
Geräte gefunden	mit unsicherem Dienst	unsichere Dienste	nur im Firewall-Verkehr

Das Wichtigste

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

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".

Veränderung seit dem letzten vollständigen Scan

Kein vollständiger früherer Scan dieses Netzwerks zum Vergleich vorhanden.

Unsichere Dienste

Bewertet nach den Verkehrsregeln (HanselCraft-Voreinstellung, anpassbar). Ein unsicherer Dienst ist kein Angriff, aber eine offene Tür, die geplant geschlossen werden sollte.

Dienst	Geräte	Warum riskant	Was tun
HTTP (TCP 80)	15	Anmeldung und Einstellungen gehen unverschlüsselt durchs Netzwerk.	Auf HTTPS umstellen oder abschalten; Anmelden über HTTP ist laut Verkehrsregeln nicht erlaubt.
SNMP (UDP 161)	10	Bei v1/v2c geht das Passwort (Community) unverschlüsselt durchs Netzwerk.	SNMPv1/v2c und 'public' sind laut Verkehrsregeln nicht erlaubt: auf SNMPv3 umstellen.
Telnet (TCP 23)	5	Passwörter und Befehle gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten, für Fernzugang SSH nutzen.
FTP (TCP 21)	2	Benutzername, Passwort und Dateien gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten, sonst SFTP oder FTPS nutzen.

erstellt mit OTScan 3 - HanselCraft, hanselcraft.de | Version 3.0.0 | 13.11.2026 01:52 Seite 1/5

Seite 1: Ampel, Kennzahlen, das Wichtigste



OTScan 3 - Netzwerkbericht Montage_Anlagennetz

Dienst	Geräte	Warum riskant	Was tun
SMB (TCP 445)	2	Alte Versionen (SMBv1) sind ein häufiger Weg für Schadsoftware.	SMBv1 abschalten (laut Verkehrsregeln nicht erlaubt), SMBv3 mit Signierung, Zugriff begrenzen.
VNC (TCP 5900)	2	Bild, Eingaben und oft das Passwort gehen unverschlüsselt durchs Netzwerk.	Laut Verkehrsregeln nicht erlaubt: abschalten oder nur verschlüsselt (TLS, VPN, SSH-Tunnel).
RPC (TCP 135)	2	Häufiger Angriffspunkt; zeigt, welche Windows-Dienste laufen.	Nur wenn technisch nötig und nur für freigegebene Rechner; sonst per Firewall sperren.

Offen, aber über die Firewall nicht genutzt (Splunk 02.11.2026 - 08.11.2026): 38 unsichere Dienste ohne erlaubten Verkehr. Das sind die ersten Kandidaten zum Abschalten. Splunk sieht nur Verkehr über die Firewall, nicht innerhalb des Netzwerks - vorher mit dem Anlagenverantwortlichen klären.

Dienst	offen	ohne Verkehr	Adressen ohne Verkehr
HTTP (TCP 80)	15	15	192.168.30.3, 192.168.30.4, 192.168.30.10, 192.168.30.11, 192.168.30.15, 192.168.30.16, 192.168.30.20, 192.168.30.21, 192.168.30.22, 192.168.30.25, 192.168.30.26, 192.168.30.30, 192.168.30.31, 192.168.30.101, 192.168.30.102
SNMP (UDP 161)	10	10	192.168.30.1, 192.168.30.2, 192.168.30.3, 192.168.30.4, 192.168.30.10, 192.168.30.11, 192.168.30.20, 192.168.30.30, 192.168.30.31, 192.168.30.102
Telnet (TCP 23)	5	5	192.168.30.3, 192.168.30.4, 192.168.30.30, 192.168.30.31, 192.168.30.102
FTP (TCP 21)	2	2	192.168.30.20, 192.168.30.22
RPC (TCP 135)	2	2	192.168.30.60, 192.168.30.61
SMB (TCP 445)	2	2	192.168.30.60, 192.168.30.61
VNC (TCP 5900)	2	2	192.168.30.25, 192.168.30.26

Bekannte Schwachstellen (Herstellermeldungen)

Abgleich der erkannten Modelle und Firmware-Stände mit den Sicherheitsmeldungen der Hersteller (Siemens, Bosch, CERT@VDE, CISA u. a., Stand 2026-10-27). "exakt" = Firmware liegt im betroffenen Bereich, "Modell" = Modell passt, Firmware nicht bekannt oder nicht vergleichbar - am Gerät prüfen. KEV = laut CISA aktiv ausgenutzt.

Meldung	Modell / Firmware	Geräte	CVSS	KEV	Güte	Maßnahme laut Hersteller
SSA-452276	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exakt	Update to V2.9.9 or later version
SSA-591731	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exakt	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
SSA-688146	CPU 1516-3 PN/DP 2.9.4	1	9.1	-	exakt	Restrict TIA project download to trusted personnel only.
SSA-699386	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exakt	Update to V4.5 or later version
SSA-710008	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exakt	Update to V4.4 or later version
SSA-723487	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.0	-	exakt	Update to V4.6 or later version
SSA-552702	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	8.8	-	exakt	Update to V4.4 or later version
SSA-224824	CPU 1214C DC/DC/DC 4.2.3; CPU 1214C DC/DC/DC 4.4.1; CPU 1215	3	7.5	-	exakt	Update to V4.7 or later version
SSA-349422	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15	2	7.5	-	exakt	Update to V3.2.17 or later version
SSA-382653	CPU 1516-3 PN/DP 2.9.4	1	7.5	-	exakt	Update to V2.9.7 or later version
SSA-392349	CPU 1516-3 PN/DP 2.9.4; CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN	3	7.5	-	exakt	As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SSA-473245	CMDB: Siemens TP1200 Comfort V16; CPU 315-2 PN/DP 3.2.14; CP	4	7.5	-	exakt	Restrict network access to affected devices
SSA-480230	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15; SIMATIC HMI	3	7.5	-	exakt	Update to V3.2.16 or later version

erstellt mit OTScan 3 - HanselCraft, hanselcraft.de | Version 3.0.0 | 13.11.2026 01:52 Seite 2/5

Unsichere Dienste erklärt

1. **Kopf**: Netzwerk, CIDR, Scan-Art, Datum und Dauer.
2. **Kennzahlen**: Geräte gefunden, mit unsicherem Dienst, Anzahl unsicherer Dienste, Geräte nur im Firewall-Verkehr.
3. **Das Wichtigste** in Sätzen; **Was ist zu tun?** als nummerierte Schritte.
4. **Unsichere Dienste**: je Dienst Geräte, warum riskant, was tun.
5. „Ohne Firewall-Verkehr" heißt: im Splunk-Zeitraum kein Verkehr über die Firewall – Kandidat zum Abschalten, aber kein Beweis (Verkehr innerhalb des Netzwerks sieht Splunk nicht).

4 Excel je Netzwerk und Maßnahmenliste

Blatt	Inhalt
Übersicht	Ampel, Steckbrief, Kennzahlen, das Wichtigste, was zu tun ist
Geräteliste	eine Zeile je Gerät: IP, MAC, Hersteller, Gerät, Modell, Firmware, offene Ports, unsichere Dienste, Splunk-Verkehr
Nur in Splunk	Adressen aus dem Firewall-Verkehr ohne Antwort im Scan
Schwachstellen	Herstellermeldungen je Gerät mit Güte (exakt, modell, hersteller), CVSS, KEV

Blatt	Inhalt
Kommunikation	Verbindungen aus dem Firewall-Export (Partner, Ports, Zonen, Policy)
CMDB-Ansicht / Shadow	CMDB-Zeilen des Netzwerks; Geräte, die nicht in der CMDB stehen
Hosts, Ports, Scripts	Rohdaten des Scans

Die **Maßnahmenliste** hat eine Zeile je Gerät und Befund mit Dringlichkeit, Ort und Gewerk aus der CMDB und Spalten zum Abhaken. Dringlichkeit „hoch“ heißt: lässt sich wahrscheinlich ohne Folgen abstellen (z. B. verbotener Dienst ohne Firewall-Verkehr) oder aktiv ausgenutzte Lücke.

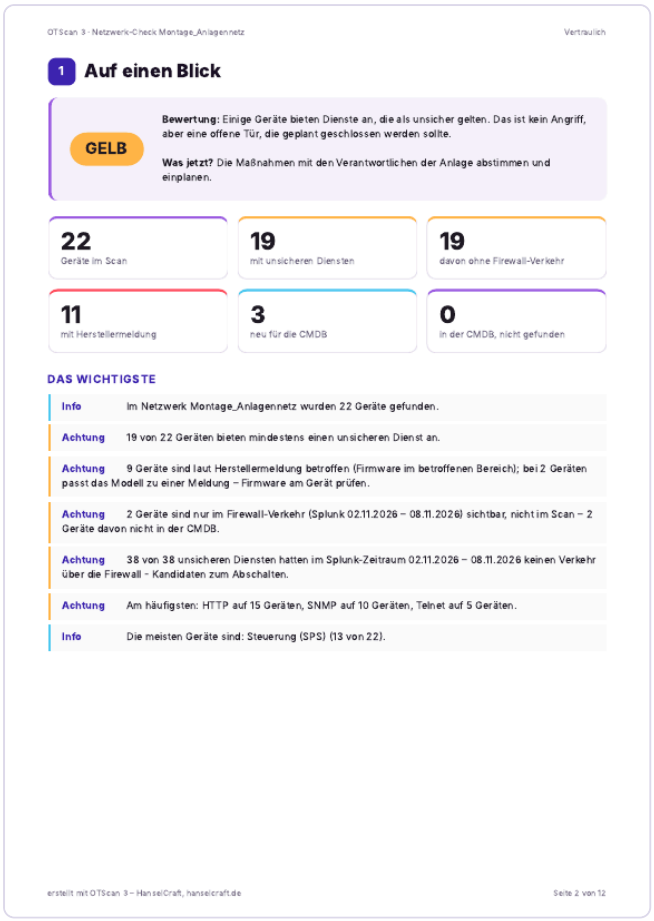
Beispiel: Steuerungen, deren Ports sich nicht abschalten lassen

Im Musterwerk zeigt das Anlagennetz Montage eine typische Lage: SPS mit **S7comm (TCP 102)**, **Modbus/TCP (502)**, **CODESYS (TCP 1200)** und **PROFINET (UDP 34964)**. Diese Protokolle sind für den Betrieb nötig, haben meist keine eigene Anmeldung oder Verschlüsselung – und lassen sich nicht einfach abschalten. OTScan 3 bewertet sie deshalb nicht als „unsicheren Dienst“ (Ampel bleibt davon unberührt); sie erscheinen in der Geräteliste, im Blatt **Ports**, in der Geräte-Detailansicht und – wenn der Hersteller eine Lücke gemeldet hat – im Blatt **Schwachstellen** und in der Maßnahmenliste als „Firmware/Update prüfen“. Die Schutzmaßnahmen dafür legen Sie selbst fest; bewährt hat sich diese Reihenfolge:

Maßnahme	So geht's	Woran man es im Bericht sieht
Segmentierung / Zonen	Steuerungen einer Anlage in eine eigene Zone (eigenes Netzwerk/VLAN) legen; Büro-, Kamera- und Energietechnik getrennt halten (IEC 62443: Zonen).	Geräteliste: SPS, Kameras und PCs gemischt in einem Netzwerk
Firewall-Regeln / Conduits	Nur die nötigen Verbindungen erlauben, z. B. TCP 102 ausschließlich vom Leitsystem und von der Engineering-Station; alles andere sperren und protokollieren.	Blatt Kommunikation: welche Partner Port 102/502/1200 wirklich nutzen
Netze zusammenführen statt verstreuen	Gleichartige Steuerungen, die über mehrere Netzwerke verteilt sind, in eine Zone zusammenführen – dann reicht ein überschaubarer Regelsatz.	Standortbericht: dieselben SPS-Ports in mehreren Netzwerken
Fernzugang absichern	Keine direkte Fernwartung auf die SPS (z. B. CODESYS 1200 aus der DMZ); stattdessen zentraler Fernzugang mit Anmeldung, Freigabe und Protokoll.	Kommunikation: Verbindungen aus Z-DMZ auf Steuerungsports
Firmware-Update, wo möglich	Herstellermeldung lesen, Update im nächsten Stillstand einplanen; wo kein Update existiert (abgekündigte Steuerung), die Maßnahmen oben verbindlich machen und Ersatz einplanen.	Schwachstellen-Blatt: Güte „exakt“ und CVSS
Nebendienste schließen	FTP, Telnet, HTTP und SNMPv1/v2c auf Steuerungen abschalten – diese sind meist entbehrlich.	Maßnahmenliste: „Dienst abschalten oder absichern“

> Kurz: **Steuerungsports schützen statt schließen** – Zone, Regel, Fernzugang, Update. Die übrigen unsicheren Dienste auf denselben Geräten (FTP, Telnet, HTTP, SNMP) stehen mit Dringlichkeit in der Maßnahmenliste.

5 Netzwerk-Check und Geräte-Detailansicht



OTScan 3 · Netzwerk-Check Montage_Anlagennetz — Vertraulich

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.

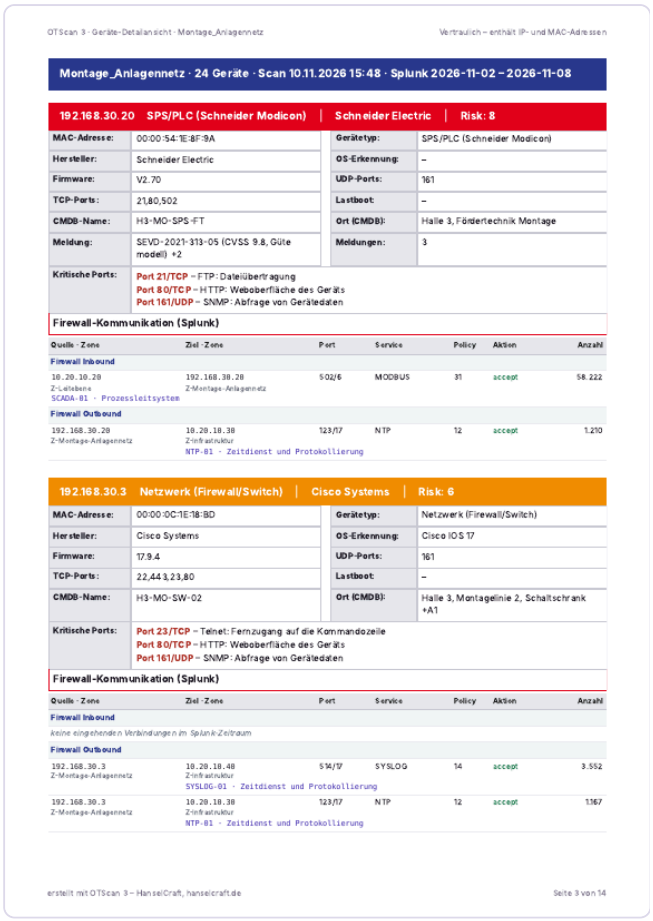
22	19	19
Geräte im Scan	mit unsicheren Diensten	davon ohne Firewall-Verkehr
11	**3**	**0**
mit Herstellermeldung	neu für die CMDB	in der CMDB, nicht gefunden

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).

erstellt mit OTScan 3 – HanselCraft, hanselcraft.de — Seite 2 von 12

Netzwerk-Check: Auf einen Blick



OTScan 3 · Geräte-Detailansicht · Montage_Anlagennetz — Vertraulich – enthält IP- und MAC-Adressen

Montage_Anlagennetz · 24 Geräte · Scan 10.11.2026 15:48 · Splunk 2026-11-02 – 2026-11-08

192.168.30.20 SPS/PLC (Schneider Modicon) | Schneider Electric | Risk: 8

MAC-Adresse:	00:00:54:1E:8F:9A	Gerätetyp:	SPS/PLC (Schneider Modicon)
Hersteller:	Schneider Electric	OS-Erkennung:	–
Firmware:	V2.70	UDP-Ports:	161
TCP-Ports:	21,80,502	Lastboot:	–
CMDB-Name:	H3-MO-SPS-FT	Ort (CMDB):	Halle 3, Fördertechnik Montage
Meldung:	SEVD-2021-313-05 (CVSS 9.8, Güte modell) +2	Meldungen:	3
Kritische Ports:	Port 21/TCP – FTP: Dateiübertragung Port 80/TCP – HTTP: Weboberfläche des Geräts Port 161/UDP – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	192.168.30.20 Z-Montage-Anlagennetz	502/6	MODBUS	31	accept	58.222
Firewall Outbound						
192.168.30.20 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.210

192.168.30.3 Netzwerk (Firewall/Switch) | Cisco Systems | Risk: 6

MAC-Adresse:	00:00:0C:1E:18:BD	Gerätetyp:	Netzwerk (Firewall/Switch)
Hersteller:	Cisco Systems	OS-Erkennung:	Cisco IOS 17
Firmware:	17.9.4	UDP-Ports:	161
TCP-Ports:	22,443,23,80	Lastboot:	–
CMDB-Name:	H3-MO-SW-02	Ort (CMDB):	Halle 3, Montagelinie 2, Schaltschrank +A1
Kritische Ports:	Port 23/TCP – Telnet: Fernzugang auf die Kommandozeile Port 80/TCP – HTTP: Weboberfläche des Geräts Port 161/UDP – SNMP: Abfrage von Gerätedaten		

Firewall-Kommunikation (Splunk)

Quelle · Zone	Ziel · Zone	Port	Service	Policy	Aktion	Anzahl
Firewall Inbound						
keine eingehenden Verbindungen im Splunk-Zeitraum						
Firewall Outbound						
192.168.30.3 Z-Montage-Anlagennetz	10.20.10.40 Z-Infrastruktur SYSLOG-01 · Zeitdienst und Protokollierung	514/17	SYSLOG	14	accept	3.552
192.168.30.3 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.167

erstellt mit OTScan 3 – HanselCraft, hanselcraft.de — Seite 3 von 14

Geräte-Detailansicht: Karte je Gerät

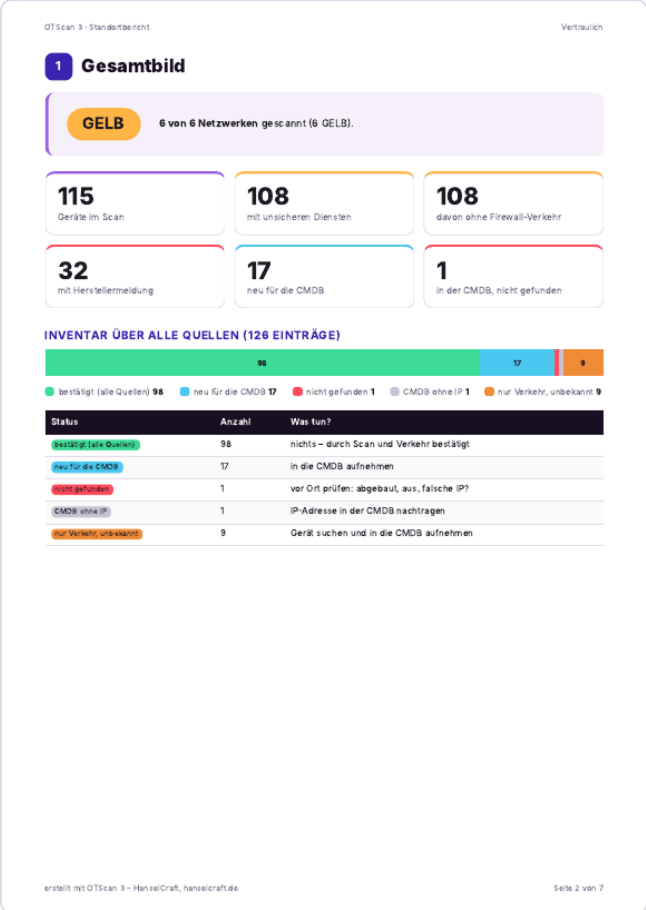
Der **Netzwerk-Check** fasst Ampel, Dienste, Herstellermeldungen, Inventarstatus und Applikationen im Firewall-Verkehr zusammen. Die **Geräte-Detailansicht** zeigt je Gerät die kritischen Ports im Klartext und die Firewall-Kommunikation mit Quell-/Zielzone, Service, Policy, Aktion und Anzahl – je Richtung die fünf häufigsten erlaubten und alle geblockten Verbindungen. Risk: 2 Punkte je kritischem Port (höchstens 8), +2 bei einer Herstellermeldung mit CVSS ≥ 7, +1 bei schwächerer Meldung. Partner werden über die Dokumentations-Datenbank Applikationen zugeordnet.

6 CMDB-Delta, CMDB-Nachtrag und Gesamtinventar

Datei	Farben / Inhalt	Was tun
CMDB-Delta	neu (grün), geändert (orange, z. B. MAC), fehlt im Scan (grau), Hinweise (blau)	Blatt „CMDB“ prüfen und in die eigene CMDB übernehmen
CMDB-Nachtrag	Geräte nur im Firewall-Verkehr, im Aufbau der CMDB-Vorlage; Suchhilfe mit Partnern und Ports	vor Ort suchen (MAC, Switchport), dann nachtragen
Gesamtinventar	eine Zeile je Gerät aus CMDB, Scan und Splunk, je Wert mit Quelle; Inventar-Status mit „Was tun?“	Erstinventarisierung, Abweichungen abarbeiten

Inventar-Status	Bedeutung
Bestätigt (alle Quellen)	CMDB, Scan und Firewall-Verkehr stimmen überein
Bestätigt (CMDB + Scan)	antwortet, aber kein Verkehr über die Firewall
Neu für die CMDB	im Scan, fehlt in der CMDB
In der CMDB, nur Verkehr	antwortet nicht auf den Scan – Firewall/Gerät prüfen
Nicht gefunden	weder im Scan noch im Verkehr – abgebaut, aus, falsche IP?
Nur Verkehr, unbekannt	Shadow-Gerät: suchen und aufnehmen

7 Standortbericht und Geräteverzeichnis


OTScan 3 · Standortbericht Vertraulich

1 Gesamtbild

GELB 6 von 6 Netzwerken gescannt (6 GELB).

115 Geräte im Scan
108 mit unsicheren Diensten
108 davon ohne Firewall-Verkehr
32 mit Herstellermeldung
17 neu für die CMDB
1 in der CMDB, nicht gefunden

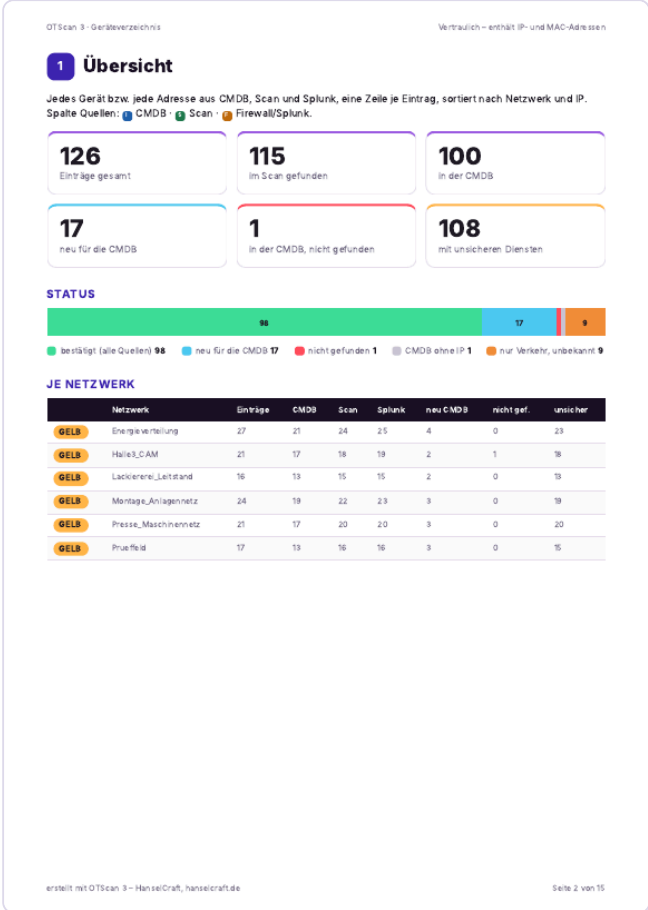
INVENTAR ÜBER ALLE QUELLEN (126 EINTRÄGE)

bestätigt (alle Quellen) 98 · neu für die CMDB 17 · nicht gefunden 1 · CMDB ohne IP 1 · nur Verkehr, unbekannt 9

Status	Anzahl	Was tun?
bestätigt (alle Quellen)	98	nichts – durch Scan und Verkehr bestätigt
neu für die CMDB	17	in die CMDB aufnehmen
nicht gefunden	1	vor Ort prüfen: abgebaut, aus, falsche IP?
CMDB ohne IP	1	IP-Adresse in der CMDB nachtragen
nur Verkehr, unbekannt	9	Gerät suchen und in die CMDB aufnehmen

erstellt mit OTScan 3 – HanselCraft, hanselcraft.de Seite 2 von 7

Standortbericht


OTScan 3 · Geräteverzeichnis Vertraulich – enthält IP- und MAC-Adressen

1 Übersicht

Jedes Gerät bzw. jede Adresse aus CMDB, Scan und Splunk, eine Zeile je Eintrag, sortiert nach Netzwerk und IP.
Spalte Quellen: C CMDB · S Scan · F Firewall/Splunk.

126 Einträge gesamt
115 im Scan gefunden
100 in der CMDB
17 neu für die CMDB
1 in der CMDB, nicht gefunden
108 mit unsicheren Diensten

STATUS

98 · 17 · 9

bestätigt (alle Quellen) 98 · neu für die CMDB 17 · nicht gefunden 1 · CMDB ohne IP 1 · nur Verkehr, unbekannt 9

JE NETZWERK

	Netzwerk	Einträge	CMDB	Scan	Splunk	neu CMDB	nicht gef.	unsicher
GELB	Energieverteilung	27	21	24	25	4	0	23
GELB	Halle3_CAM	21	17	18	19	2	1	18
GELB	Lackiererei_Leitstand	16	13	15	15	2	0	13
GELB	Montage_Anlagennetz	24	19	22	23	3	0	19
GELB	Presse_Maschinennetz	21	17	20	20	3	0	20
GELB	Prueffeld	17	13	16	16	3	0	15

erstellt mit OTScan 3 – HanselCraft, hanselcraft.de Seite 2 von 15

Geräteverzeichnis

Der **Standortbericht** zeigt alle Netzwerke mit Ampel und Stand, die häufigsten Dienste, Herstellermeldungen und Applikationen. Das **Geräteverzeichnis** listet jedes Gerät aller Netzwerke in einer Zeile. Beide entstehen am Ende einer Netzwerkkette oder mit **Gesamtberichte jetzt erstellen (alle Netzwerke)**.

8 Herstellermeldungen richtig lesen

Güte	Bedeutung
exakt	Modell erkannt und Firmware nachweislich im betroffenen Bereich
modell	Modell passt, Firmware unbekannt oder nicht eindeutig – am Gerät prüfen
hersteller	nur der Hersteller passt – schwacher Hinweis

> Der Offline-Bestand ersetzt nicht die Originalmeldung des Herstellers (Link in Excel und Maßnahmenliste). Alle Berichte enthalten Adressen und sind vertraulich; nach außen nur Unterlagen ohne Adressen weitergeben.