BERICHTE & MUSTER

Welche Berichte gibt es?

Alle Berichtsarten von OTScan 3 mit Muster aus dem erfundenen Musterwerk Halle 3.

Welche Berichte gibt es?

Alle Berichtsarten von OTScan 3 mit Muster – zum Aussuchen. Die Muster zeigen das erfundene **Musterwerk Halle 3** (6 Netzwerke der Fertigung, 115 Geräte, Firewall-Export und CMDB); die Einzelberichte gehören zum **Anlagennetz Montage**. Die Haken im Fenster **Berichte & Muster …** legen fest, welche Berichte entstehen; **Muster ansehen** öffnet die Datei. Englische Fassungen liegen unter `assets/muster/en` (Dateinamen mit _EN).

> Steuerungsports wie S7comm 102, Modbus 502, CODESYS 1200 oder PROFINET 34964 lassen sich nicht abschalten. Wie man sie trotzdem schützt (Zonen, Firewall-Regeln, Fernzugang, Firmware), steht in **Berichte lesen**, Kapitel 4.

Bericht	Wann	Was steht drin	Muster
Excel-Bericht je Netzwerk	nach jedem Lauf	Alle Blätter: Übersicht, Geräteliste, Nur in Splunk, Schwachstellen, Kommunikation, CMDB-Ansicht, Hosts, Ports.	`Muster_01_Excel_Netzwerk.xlsx`
PDF Kompaktbericht	nach jedem Lauf	Der kurze Netzwerkbericht mit Ampel, Kernaussagen und Maßnahmen.	`Muster_02_PDF_Kompakt.pdf`
PDF ausführlich (zusätzlich)	nach jedem Lauf	Der lange technische Bericht mit allen Hosts – z. B. für Audits.	`Muster_03_PDF_ausfuehrlich.pdf`
PowerPoint (Manager)	nach jedem Lauf	Folien für die Besprechung mit Verantwortlichen.	`Muster_04_PowerPoint_Manager.pptx`
Maßnahmenliste (Excel)	nach jedem Lauf – immer	Unsichere Dienste und Herstellermeldungen je Gerät mit Ort, Gewerk, Dringlichkeit und Spalten zum Abhaken.	`Muster_05_Massnahmen.xlsx`
CMDB-Delta (Excel)	nach jedem Lauf – immer	Neu / geändert / fehlt gegenüber der CMDB, im Aufbau der CMDB-Vorlage.	`Muster_06_CMDB-Delta.xlsx`
CMDB-Nachtrag (Excel)	nach jedem Lauf – immer	Geräte, die nur im Firewall-Verkehr (Splunk) sichtbar sind – zum Nachtragen.	`Muster_07_CMDB-Nachtrag.xlsx`
Netzwerk-Check (PDF, neues Design)	nach jedem Lauf	Ampel, Kennzahlen, Dienste, Herstellermeldungen, Inventar und Applikationen im Firewall-Verkehr.	`Muster_08_Netzwerk-Check.pdf`

Bericht	Wann	Was steht drin	Muster
Geräte-Detailansicht (PDF)	nach jedem Lauf	Karte je Gerät mit Firewall-Kommunikation: Quell-/Zielzone, Service, Policy, Aktion, Anzahl, Applikation.	`Muster_09_Geraete-Detailansicht.pdf`
Gesamtinventar CMDB · Scan · Splunk (Excel)	alle Netzwerke	Eine Zeile je Gerät aus allen Quellen, je Wert mit Quelle – für die Erstinventarisierung.	`Muster_10_Gesamtinventar.xlsx`
Standortbericht (PDF)	alle Netzwerke	Gesamtbild, alle Netzwerke mit Ampel, Dienste, Meldungen, Applikationen je Netzwerk.	`Muster_11_Standortbericht.pdf`
Geräteverzeichnis (PDF)	alle Netzwerke	Alle Geräte aller Netzwerke, eine Zeile je Gerät (Querformat).	`Muster_12_Geraeteverzeichnis.pdf`

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

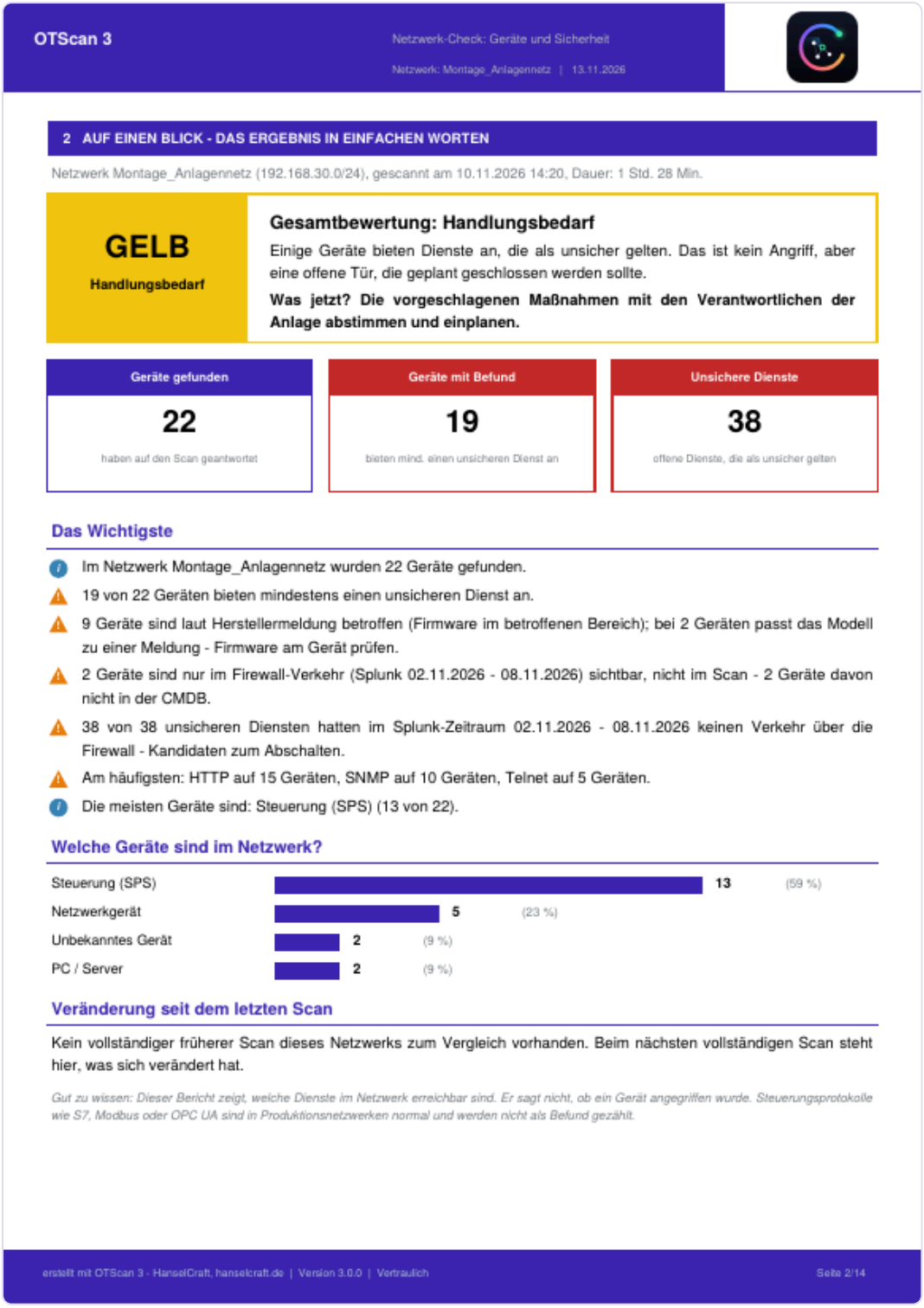
Bewertet nach den Verkehrsregeln (HanselCraft-Voreinstellung, anpassbar). Ein unsicherer Dienst ist kein Angriff, aber eine offene Tür, die geplant geschlossen werden sollte.

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

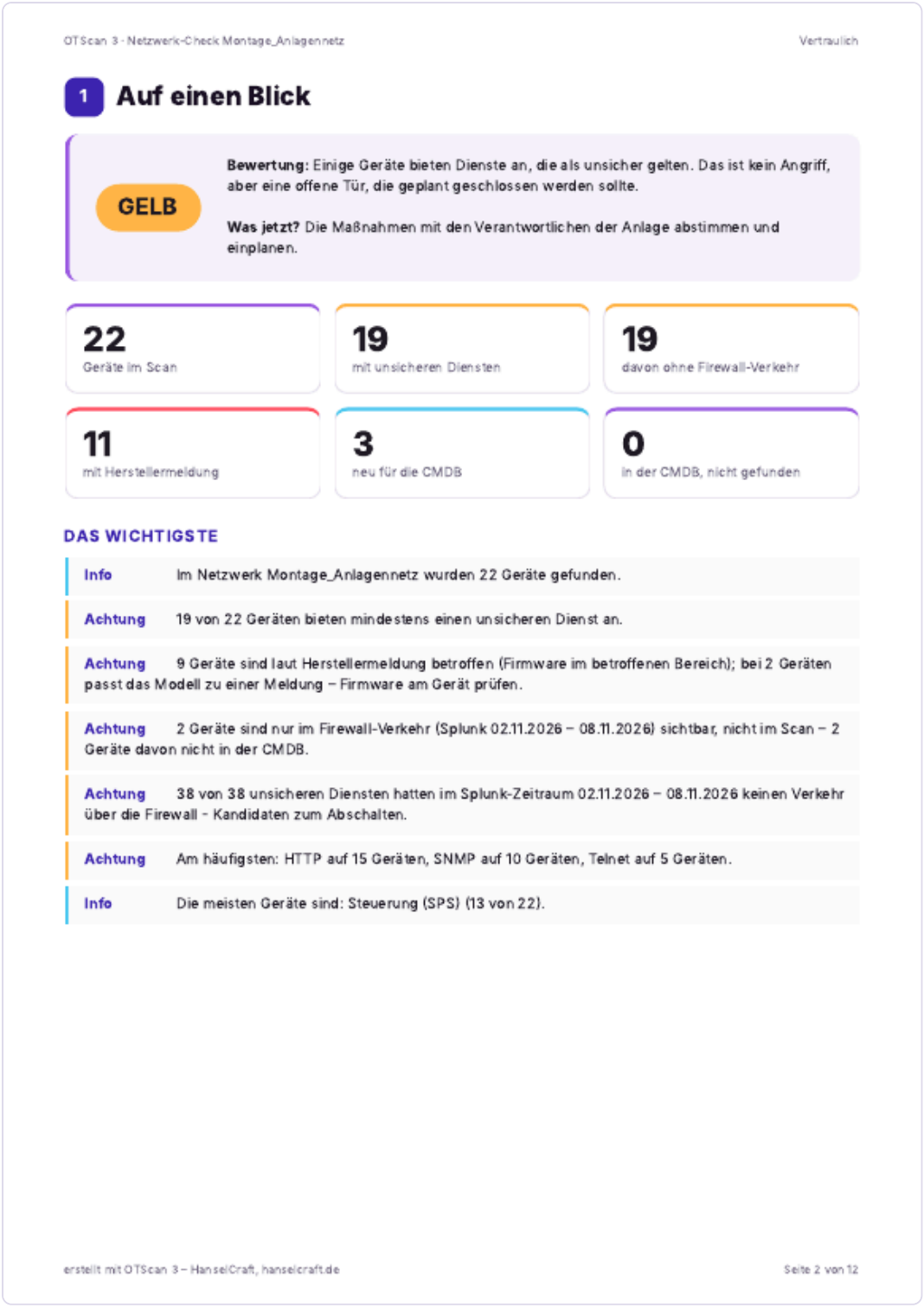
Muster_02_PDF_Kompakt.pdf

PDF ausführlich (zusätzlich)



Muster_03_PDF_ausfuehrlich.pdf

Netzwerk-Check (PDF, neues Design)



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 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).

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

Muster_08_Netzwerk-Check.pdf

Geräte-Detailansicht (PDF)



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

So lesen

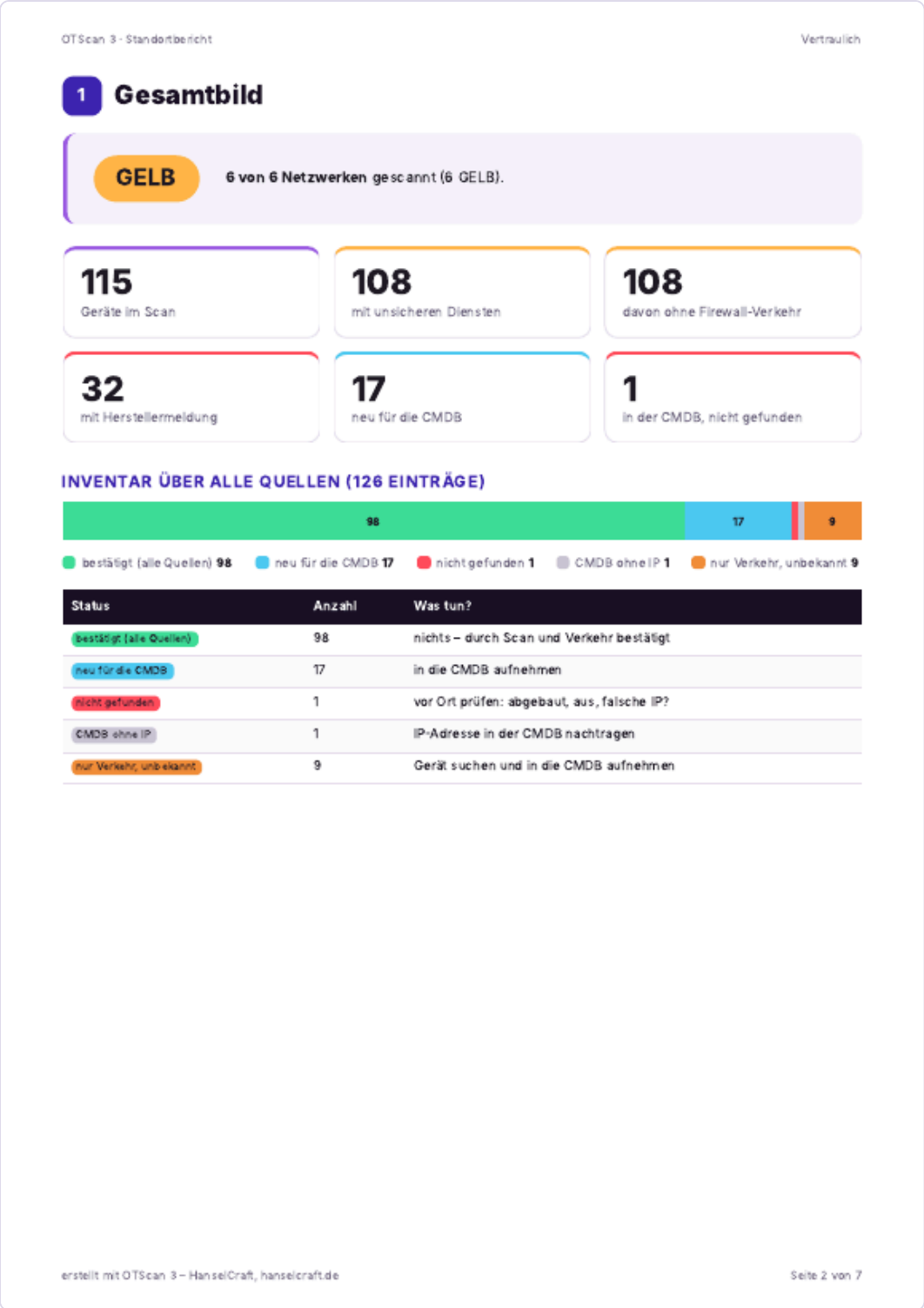
Je Gerät: Angaben aus dem Scan, Name und Ort aus der CMDB und die Kommunikation über die Firewall aus Splunk – je Richtung die 5 häufigsten erlaubten Verbindungen und alle geblockten, je mit Quell- und Zielzone, Service, Policy, Aktion und Anzahl. Kritische Ports stehen voll ausgeschrieben mit Klartext-Erklärung. Unter dem Partner steht, soweit bekannt, das System bzw. die Applikation aus der Dokumentations-Datenbank.

	Risk 7–10: mehrere kritische Ports und/oder Herstellermeldung CVSS ≥ 7
	Risk 4–6
	Risk 1–3
	Risk 0: keine kritischen Ports
	nur im Firewall-Verkehr (Splunk), nicht im Scan

erstellt mit OTScan 3 – HanselCraft, hanselcraft.de — Seite 2 von 14

Muster_09_Geraete-Detailansicht.pdf

Standortbericht (PDF)



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)

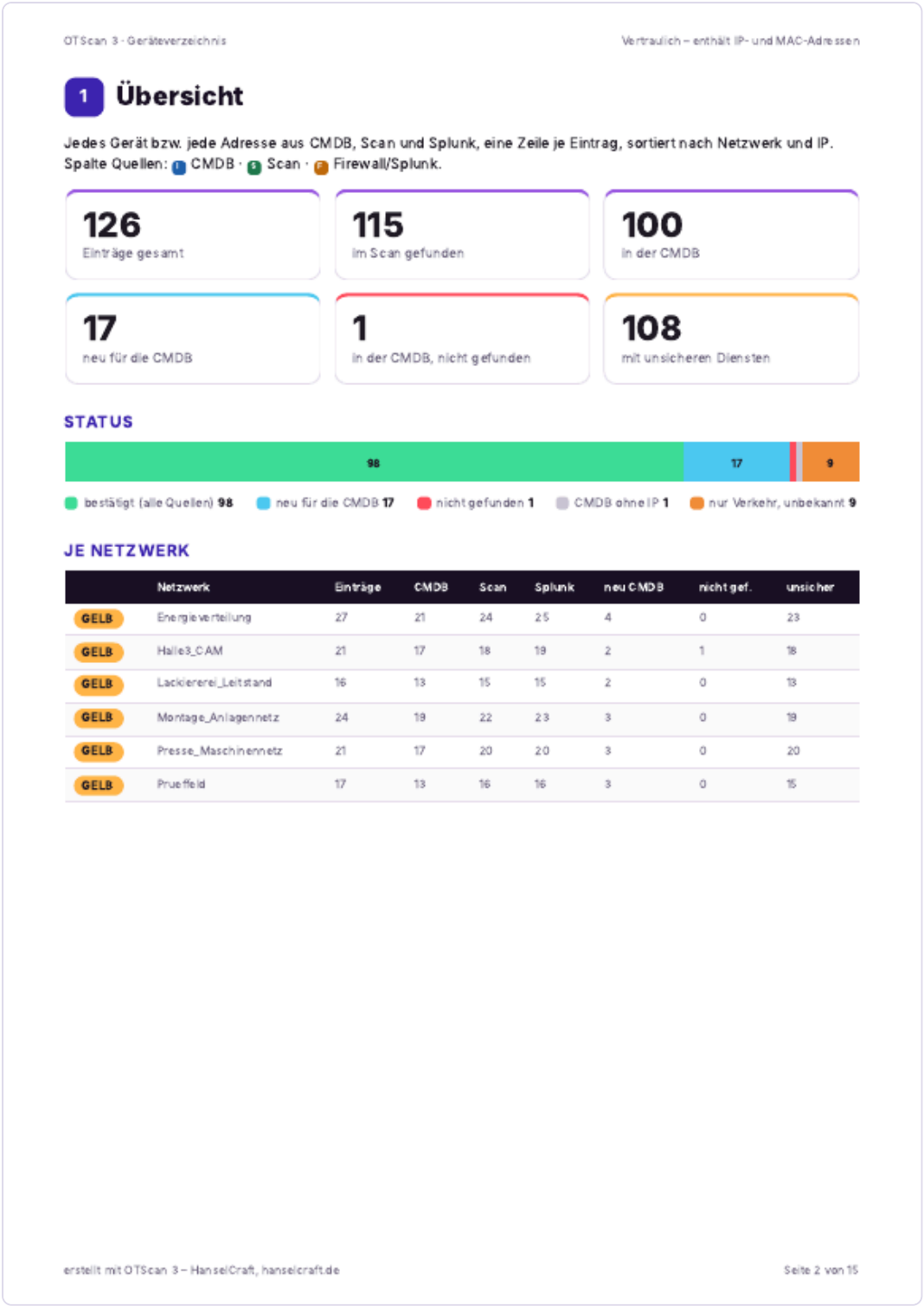
bestätigt (alle Quellen) **98** · neu für die CMDB **17** · nicht gefunden **1** · CMDB ohne IP **1** · nur Verkehr, unbekannt **9**

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

Muster_11_Standortbericht.pdf

Geräteverzeichnis (PDF)



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	115	100
Einträge gesamt	im Scan gefunden	in der CMDB

17	1	108
neu für die CMDB	in der CMDB, nicht gefunden	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

Muster_12_Geraeteverzeichnis.pdf