REPORTS

Reading reports

Traffic light and traffic rules, PDF, Excel, action list, Network check, Device details, CMDB delta and addendum, overall inventory, site report.

1 Which report for whom?

Reader	Report	File
Plant owners	PDF compact report	`<network>_<time>_stufenlauf.pdf`
Engineering, trades	Excel per network, action list	`…_stufenlauf.xlsx`, `…_Massnahmen.xlsx`
Management	PowerPoint	`…_manager.pptx`
Audit, specialists	Detailed PDF, Network check, Device details	`…_ausfuehrlich.pdf`, `…_Netzwerk-Check.pdf`, `…_Geraete-Details.pdf`
Inventory management	CMDB delta, CMDB addendum, overall inventory	`…_CMDB-Delta.xlsx`, `…_CMDB-Nachtrag.xlsx`, `OTScan3_Gesamtinventar_<date>.xlsx`
Site management	Site report, Device directory	`OTScan3_Standortbericht_<date>.pdf`, `OTScan3_Geraeteverzeichnis_<date>.pdf`

The file names are the same in every language. The report language is set in the program (Data maintenance → language); PDF, Excel per network, action list and PowerPoint are then written in English. The inventory files CMDB delta, CMDB addendum and overall inventory are currently produced in German (column and sheet names); this guide explains their German terms.

All illustrations come from the fictitious **Musterwerk Halle 3** sample plant (6 production networks, 115 devices: assembly plant network, press machine network, paint shop control room, test field, power distribution, camera network). Names, addresses and networks are invented; device types, firmware versions and open services correspond to typical findings in grown production networks. OTScan 3 opens the same files in the window **Reports …** with **View sample** (English samples: `assets/muster/en`).

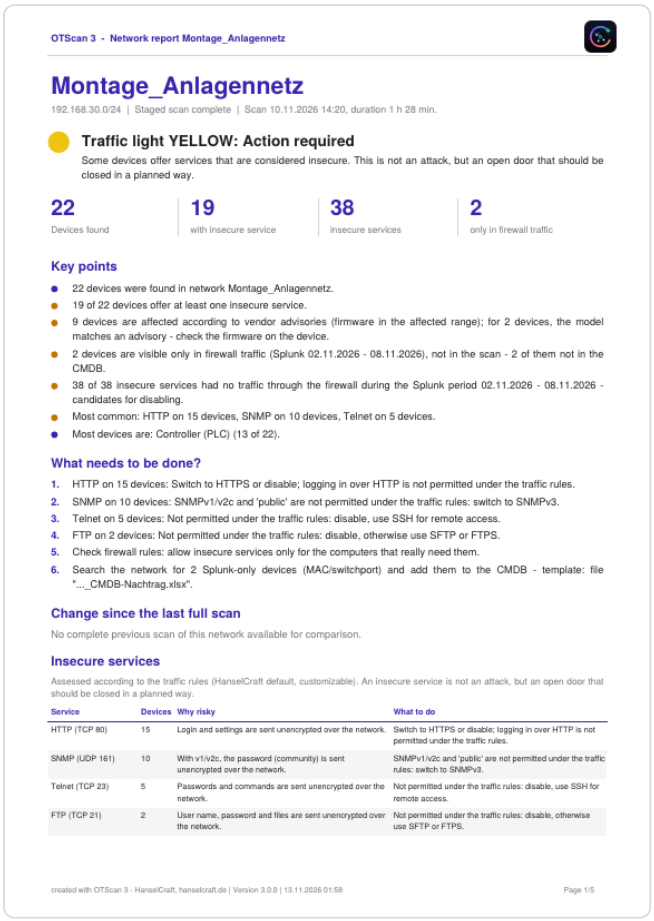
2 The traffic light and the traffic rules

Traffic light	Meaning	What to do
GREEN	No open service that the traffic rules classify as insecure.	Nothing urgent; repeat the scan regularly.
YELLOW	At least one port from the traffic rules is open (e.g. Telnet, FTP, HTTP, SNMPv1/v2c, SMB, VNC).	Clarify with the operator and close in a planned way.
GREY	No assessment possible: devices responded but did not provide details about their services.	Repeat the scan with a gentler profile.

If the footer of a report says "INCOMPLETE" (e.g. host timeouts or an aborted stage), repeat the scan before drawing conclusions.

> The **traffic rules** are a HanselCraft default for insecure IT protocols in OT networks, aligned with IEC 62443 (zones and conduits). They are not a standard. Weights (1–3 per port) add up to a device's risk value. To adapt them: `verkehrsregeln.json` in the data folder (remove or add ports, change weights and texts; takes effect after a restart).

3 PDF compact report



OTScan 3 - Network report Montage_Anlagennetz

Montage_Anlagennetz

192.168.30.0/24 | Staged scan complete | Scan 10.11.2026 14:20, duration 1 h 28 min.

Traffic light YELLOW: Action required

Some devices offer services that are considered insecure. This is not an attack, but an open door that should be closed in a planned way.

22	19	38	2
Devices found	with insecure service	insecure services	only in firewall traffic

Key points

- 22 devices were found in network Montage_Anlagennetz.
- 19 of 22 devices offer at least one insecure service.
- 9 devices are affected according to vendor advisories (firmware in the affected range); for 2 devices, the model matches an advisory - check the firmware on the device.
- 2 devices are visible only in firewall traffic (Splunk 02.11.2026 - 08.11.2026), not in the scan - 2 of them not in the CMDB.
- 38 of 38 insecure services had no traffic through the firewall during the Splunk period 02.11.2026 - 08.11.2026 - candidates for disabling.
- Most common: HTTP on 15 devices, SNMP on 10 devices, Telnet on 5 devices.
- Most devices are: Controller (PLC) (13 of 22).

What needs to be done?

1. HTTP on 15 devices: Switch to HTTPS or disable; logging in over HTTP is not permitted under the traffic rules.
2. SNMP on 10 devices: SNMPv1/v2c and 'public' are not permitted under the traffic rules: switch to SNMPv3.
3. Telnet on 5 devices: Not permitted under the traffic rules: disable, use SSH for remote access.
4. FTP on 2 devices: Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.
5. Check firewall rules: allow insecure services only for the computers that really need them.
6. Search the network for 2 Splunk-only devices (MAC/switchport) and add them to the CMDB - template: file "..._CMDB-Nachtrag.xlsx".

Change since the last full scan

No complete previous scan of this network available for comparison.

Insecure services

Assessed according to the traffic rules (HanselCraft default, customizable). An insecure service is not an attack, but an open door that should be closed in a planned way.

Service	Devices	Why risky	What to do
HTTP (TCP 80)	15	Login and settings are sent unencrypted over the network.	Switch to HTTPS or disable; logging in over HTTP is not permitted under the traffic rules.
SNMP (UDP 161)	10	With v1/v2c, the password (community) is sent unencrypted over the network.	SNMPv1/v2c and 'public' are not permitted under the traffic rules: switch to SNMPv3.
Telnet (TCP 23)	5	Passwords and commands are sent unencrypted over the network.	Not permitted under the traffic rules: disable, use SSH for remote access.
FTP (TCP 21)	2	User name, password and files are sent unencrypted over the network.	Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.

created with OTScan 3 - HanselCraft, hanselcraft.de | Version 3.0.0 | 13.11.2026 01:58 Page 1/5

Page 1: traffic light, key figures, key points



OTScan 3 - Network report Montage_Anlagennetz

Service	Devices	Why risky	What to do
SMB (TCP 445)	2	Old versions (SMBv1) are a common path for malware.	Disable SMBv1 (not permitted under the traffic rules), use SMBv3 with signing, restrict access.
VNC (TCP 5900)	2	Screen, input and often the password are sent unencrypted over the network.	Not permitted under the traffic rules: disable or use only encrypted (TLS, VPN, SSH tunnel).
RPC (TCP 135)	2	Common attack point; shows which Windows services are running.	Only if technically necessary and only for approved computers; otherwise block via firewall.

Open but not used through the firewall (Splunk 02.11.2026 - 08.11.2026): 38 insecure services without permitted traffic. These are the first candidates for disabling. Splunk only sees traffic through the firewall, not within the network - clarify with the plant owner beforehand.

Service	open	no traffic	Addresses without traffic
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

Known vulnerabilities (vendor advisories)

Comparison of the detected models and firmware versions with the vendors' security advisories (Siemens, Bosch, CERT@VDE, CISA, etc., as of 2026-10-27). "exact" = firmware is in the affected range, "model" = model matches, firmware unknown or not comparable - check on the device. KEV = actively exploited according to CISA.

Advisory	Model / firmware	Devices	CVSS	KEV	Quality	Vendor-recommended action
SSA-452276	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exact	Update to V2.9.9 or later version
SSA-591731	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exact	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	-	exact	Restrict TIA project download to trusted personnel only.
SSA-699386	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exact	Update to V4.5 or later version
SSA-710008	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exact	Update to V4.4 or later version
SSA-723487	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.0	-	exact	Update to V4.6 or later version
SSA-552702	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	8.8	-	exact	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	-	exact	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	-	exact	Update to V3.2.17 or later version
SSA-382653	CPU 1516-3 PN/DP 2.9.4	1	7.5	-	exact	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	-	exact	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	-	exact	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	-	exact	Update to V3.2.16 or later version

created with OTScan 3 - HanselCraft, hanselcraft.de | Version 3.0.0 | 13.11.2026 01:58 Page 2/5

Insecure services explained

1. **Header**: network, CIDR, scan type, date and duration.
2. **Key figures**: devices found, devices with an insecure service, number of insecure services, devices only in firewall traffic.
3. **Key points** in sentences; **What needs to be done?** as numbered steps.
4. **Insecure services**: devices per service, why it is risky, what to do.
5. "Without firewall traffic" means: no traffic through the firewall during the Splunk period – a candidate for disabling, but no proof (Splunk does not see traffic within the network).

4 Excel per network and action list

Sheet	Content
Overview	traffic light, profile, key figures, key points, what needs to be done
Device list	one row per device: IP, MAC, vendor, device, model, firmware, open ports, insecure services, Splunk traffic
Only in Splunk	addresses from firewall traffic without a response in the scan
Vulnerabilities	vendor advisories per device with match quality (exact, model, vendor), CVSS, KEV
Communication	connections from the firewall export (partners, ports, zones, policy)
CMDB view / Shadow	CMDB rows of the network; devices that are not in the CMDB
Hosts, Ports, Scripts	raw data of the scan

The **action list** has one row per device and finding with urgency, location and trade from the CMDB, and columns to tick off. Urgency "high" means: can probably be fixed without side effects (e.g. a non-permitted service without firewall traffic), or an actively exploited vulnerability. Urgency describes how quickly and easily something can be fixed – not the risk.

Example: controllers whose ports cannot be disabled

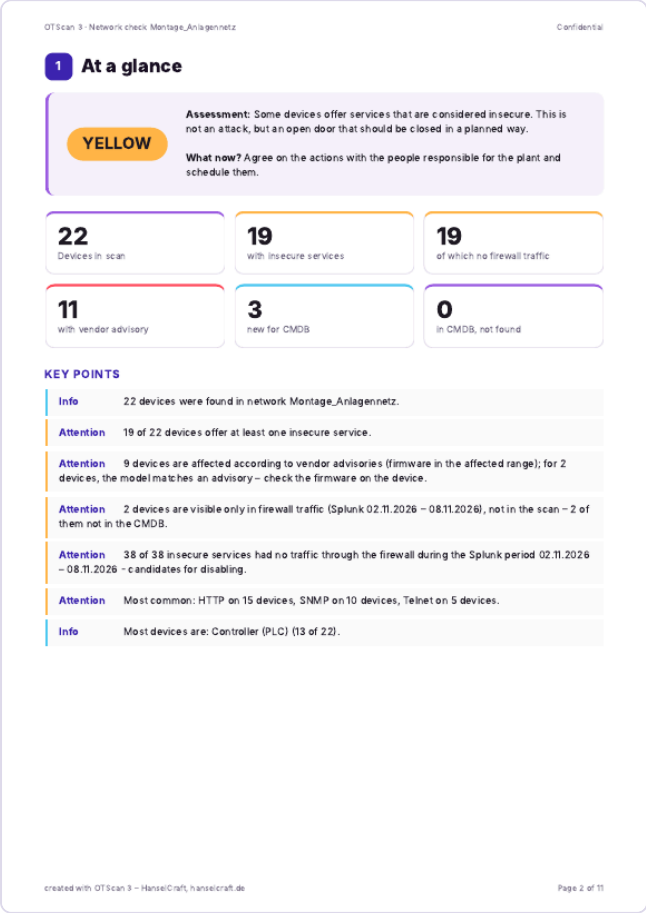
In the sample plant, the assembly plant network shows a typical situation: PLCs with **S7comm (TCP 102)**, **Modbus/TCP (502)**, **CODESYS (TCP 1200)** and **PROFINET (UDP 34964)**. These protocols are required for operation, usually have no authentication or encryption of their own – and cannot simply be disabled. OTScan 3 therefore does not rate them as an "insecure service" (the traffic light is not affected by them); they appear in the device list, in the **Ports** sheet, in the device details and – if the vendor has published a vulnerability – in the **Vulnerabilities** sheet and in the action list as "check firmware/update". You define the protective measures yourself; this order has proven itself:

Measure	How	Where you see it in the report
Segmentation / zones	Put the controllers of a plant into a zone of their own (own network/VLAN); keep office, camera and energy equipment separate (IEC 62443: zones).	Device list: PLCs, cameras and PCs mixed in one network
Firewall rules / conduits	Allow only the required connections, e.g. TCP 102 exclusively from the control system and the engineering station; block and log everything else.	Communication sheet: which partners really use port 102/502/1200
Consolidate networks	Move controllers of the same kind that are spread over several networks into one zone – a manageable rule set is then sufficient.	Site report: the same PLC ports in several networks
Secure remote access	No direct remote maintenance on the PLC (e.g. CODESYS 1200 from the DMZ); use central remote access with authentication, approval and logging instead.	Communication: connections from Z-DMZ to controller ports

Measure	How	Where you see it in the report
Firmware update where possible	Read the vendor advisory and plan the update for the next shutdown; where no update exists (discontinued controller), make the measures above mandatory and plan a replacement.	Vulnerabilities sheet: match quality "exact" and CVSS
Close secondary services	Disable FTP, Telnet, HTTP and SNMPv1/v2c on controllers – they are usually not needed.	Action list: "disable or secure service"

> In short: **protect controller ports instead of closing them** – zone, rule, remote access, update. The other insecure services on the same devices (FTP, Telnet, HTTP, SNMP) are listed with urgency in the action list.

5 Network check and device details


OTScan 3 · Network check Montage_Anlagennetz Confidential

1 At a glance

YELLOW

Assessment: Some devices offer services that are considered insecure. This is not an attack, but an open door that should be closed in a planned way.

What now? Agree on the actions with the people responsible for the plant and schedule them.

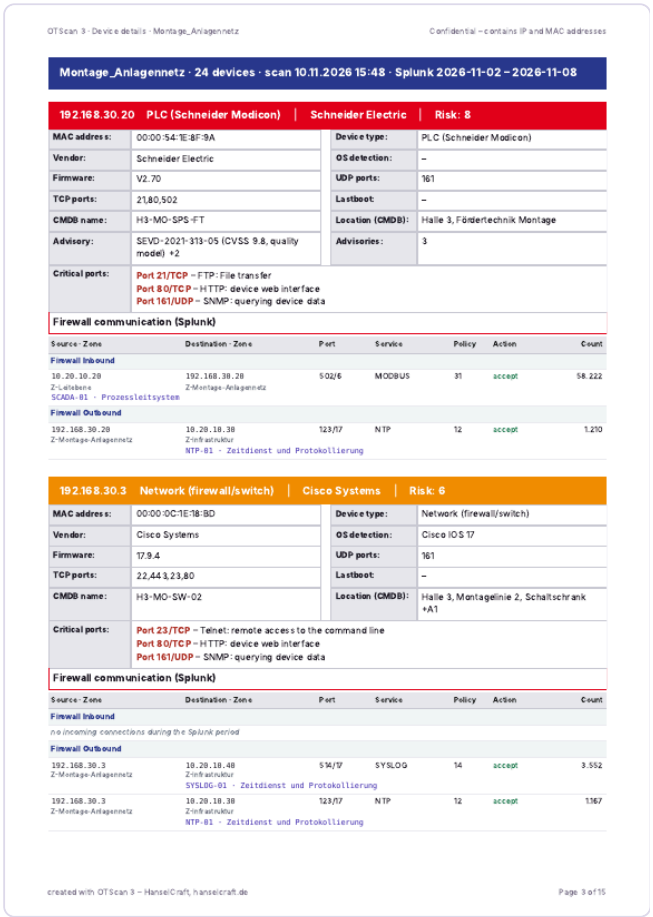
22 Devices in scan
19 with insecure services
19 of which no firewall traffic
11 with vendor advisory
3 new for CMDB
0 in CMDB, not found

KEY POINTS

Info 22 devices were found in network Montage_Anlagennetz.
Attention 19 of 22 devices offer at least one insecure service.
Attention 9 devices are affected according to vendor advisories (firmware in the affected range); for 2 devices, the model matches an advisory – check the firmware on the device.
Attention 2 devices are visible only in firewall traffic (Splunk 02.11.2026 – 08.11.2026), not in the scan – 2 of them not in the CMDB.
Attention 38 of 38 insecure services had no traffic through the firewall during the Splunk period 02.11.2026 – 08.11.2026 – candidates for disabling.
Attention Most common: HTTP on 15 devices, SNMP on 10 devices, Telnet on 5 devices.
Info Most devices are: Controller (PLC) (13 of 22).

created with OTScan 3 – HanselCraft, hanselcraft.de Page 2 of 11

Network check: at a glance


OTScan 3 · Device details · Montage_Anlagennetz Confidential – contains IP and MAC addresses

Montage_Anlagennetz · 24 devices · scan 10.11.2026 15:48 · Splunk 2026-11-02 – 2026-11-08

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

MAC address:	00:00:54:1E:8F:9A	Device type:	PLC (Schneider Modicon)
Vendor:	Schneider Electric	OS detection:	–
Firmware:	V2.70	UDP ports:	161
TCP ports:	21,80,502	Lastboot:	–
CMDB name:	H3-MO-SPS-FT	Location (CMDB):	Halle 3, Fördertechnik Montage
Advisory:	SEVD-2021-313-05 (CVSS 9.8, quality model) +2	Advisories:	3

Critical ports: Port 21/TCP – FTP: File transfer; Port 80/TCP – HTTP: device web interface; Port 161/UDP – SNMP: querying device data

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
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 Network (firewall/switch) | Cisco Systems | Risk: 6

MAC address:	00:00:0C:1E:18:BD	Device type:	Network (firewall/switch)
Vendor:	Cisco Systems	OS detection:	Cisco IOS 17
Firmware:	17.9.4	UDP ports:	161
TCP ports:	22,443,23,80	Lastboot:	–
CMDB name:	H3-MO-SW-02	Location (CMDB):	Halle 3, Montagelinie 2, Schaltschrank +A1

Critical ports: Port 23/TCP – Telnet: remote access to the command line; Port 80/TCP – HTTP: device web interface; Port 161/UDP – SNMP: querying device data

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
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

created with OTScan 3 – HanselCraft, hanselcraft.de Page 3 of 15

Device details: one card per device

The **Network check** summarises traffic light, services, vendor advisories, inventory status and applications in firewall traffic. The **Device details** report shows the critical ports of each device in plain language and the firewall communication with source/destination zone, service, policy, action and count – per direction the five most frequent allowed and all blocked connections. Risk: 2 points per critical port

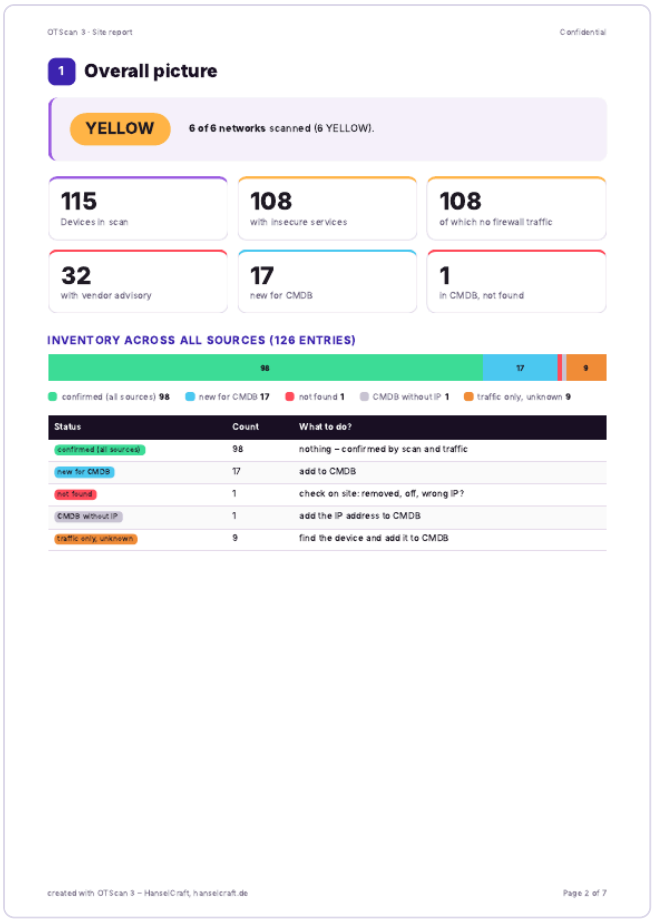
(at most 8), +2 for a vendor advisory with CVSS ≥ 7, +1 for a weaker advisory. Partners are assigned to applications via the documentation database.

6 CMDB delta, CMDB addendum and overall inventory

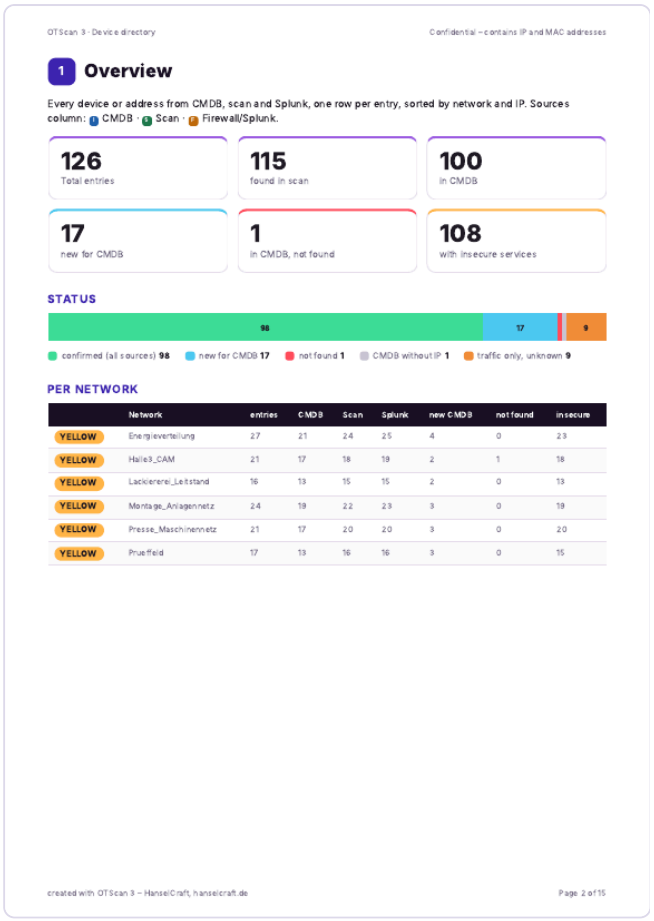
File	Colours / content	What to do
CMDB-Delta	new (green), changed (orange, e.g. MAC), missing in the scan (grey), notes (blue)	check sheet "CMDB" and transfer to your own CMDB
CMDB-Nachtrag (addendum)	devices only in firewall traffic, in the layout of the CMDB template; search aid with partners and ports	locate on site (MAC, switch port), then add
Gesamtinventar (overall inventory)	one row per device from CMDB, scan and Splunk, each value with its source; inventory status with "Was tun?" (what to do)	initial inventory, work through deviations

Inventory status (German term in the file)	Meaning
Bestätigt (alle Quellen) – confirmed (all sources)	CMDB, scan and firewall traffic match
Bestätigt (CMDB + Scan) – confirmed (CMDB + scan)	responds, but no traffic through the firewall
Neu für die CMDB – new for the CMDB	in the scan, missing in the CMDB
In der CMDB, nur Verkehr – in the CMDB, traffic only	does not respond to the scan – check firewall/device
Nicht gefunden – not found	neither in the scan nor in traffic – removed, switched off, wrong IP?
Nur Verkehr, unbekannt – traffic only, unknown	shadow device: locate and record it

7 Site report and device directory



Site report



Device directory

The **Site report** shows all networks with traffic light and status, the most frequent services, vendor advisories and applications. The **Device directory** lists every device of all networks in one row. Both are created at the end of a network chain or with `Create overall reports now (all networks)`.

8 Reading vendor advisories correctly

Match quality	Meaning
exact	model detected and firmware verifiably within the affected range
model	model matches, firmware unknown or ambiguous – check on the device
vendor	only the vendor matches – weak indication

> The offline data set does not replace the vendor's original advisory (link in Excel and in the action list). All reports contain addresses and are confidential; only pass on documents without addresses to external parties.