OTScan 3

OT-/ICS-NETZWERKSCANNER · HANSELCRAFT

NETWORK CHECK · ALL NETWORKS

Site

6 networks · as of 13.11.2026

YELLOW

NETWORKS	DEVICES	INVENTORY	STATUS
6 of 6 scanned	115	126 entries	13.11.2026

1 Overall picture

YELLOW **6 of 6 networks** scanned (6 YELLOW).

115 Devices in scan	**108** with insecure services
108 of which no firewall traffic	**32** with vendor advisory
17 new for CMDB	**1** in CMDB, not found

INVENTORY ACROSS ALL SOURCES (126 ENTRIES)



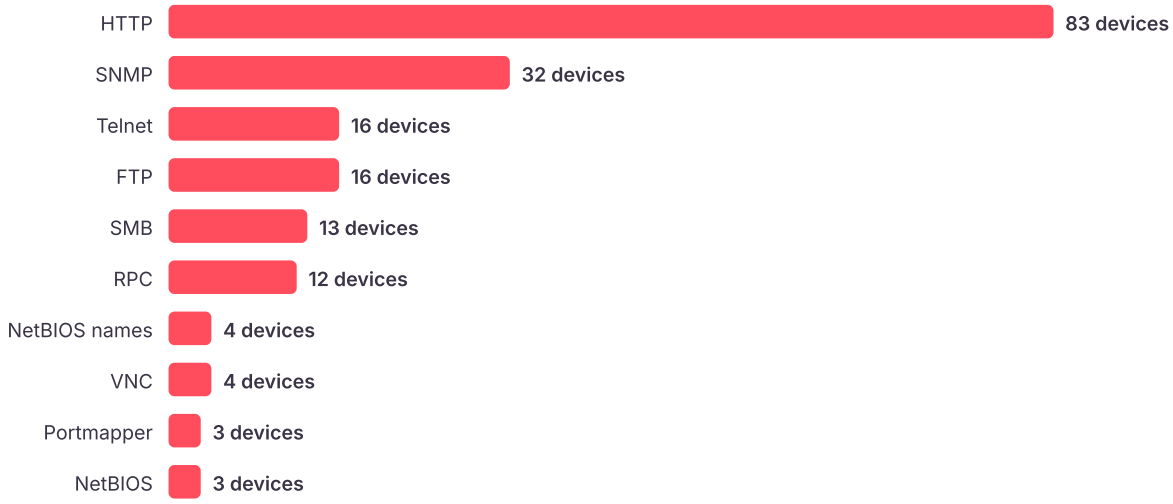
confirmed (all sources) **98** new for CMDB **17** not found **1** CMDB without IP **1** traffic only, unknown **9**

Status	Count	What to do?
confirmed (all sources)	98	nothing – confirmed by scan and traffic
new for CMDB	17	add to CMDB
not found	1	check on site: removed, off, wrong IP?
CMDB without IP	1	add the IP address to CMDB
traffic only, unknown	9	find the device and add it to CMDB

2 All networks at a glance

	Network	Devices	insecure	Advisory	Actions high	new CMDB	not found	Scan
YELLOW	Energieverteilung	24	23	5	6	4	0	10.11.2026 11:19
YELLOW	Halle3_CAM	18	18	0	1	2	1	09.11.2026 11:09
YELLOW	Lackiererei_Leitstand	15	13	5	8	2	0	10.11.2026 14:07
YELLOW	Montage_Anlagennetz	22	19	11	17	3	0	10.11.2026 15:48
YELLOW	Presse_Maschinennetz	20	20	9	22	3	0	10.11.2026 09:26
YELLOW	Prueffeld	16	15	2	7	3	0	10.11.2026 16:42

3 Insecure services and actions

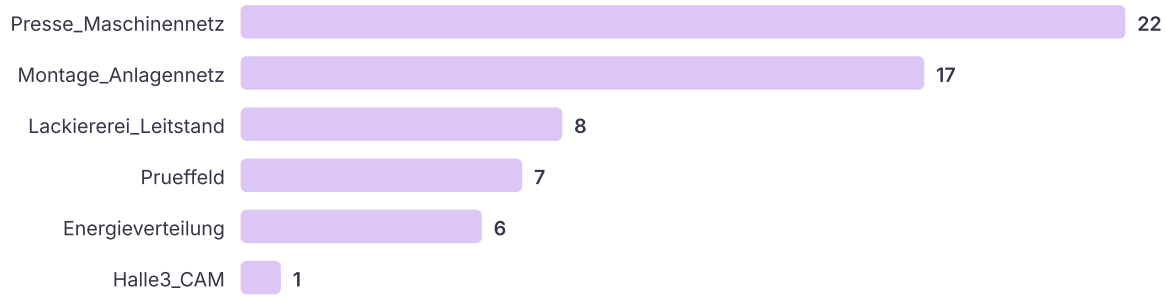


61
Actions high

300
Actions medium

30
Actions low

NETWORKS WITH THE MOST URGENT ACTIONS



4 Vendor advisories

32 devices in 5 networks match vendor advisories. The most common:

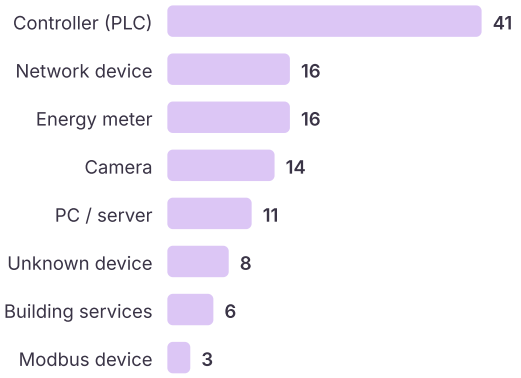
Advisory	Title	CVSS	Quality	Devices	Netw.
SSA-712929	SSA-712929: Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industria	7.5	exakt, modell	12	3
SSA-473245	SSA-473245: Denial of Service Vulnerability in Profinet Devices	7.5	exakt, modell	8	3
SSA-876787	SSA-876787: Open Redirect Vulnerability in SIMATIC S7-1500 and S7-1200 CPUs	4.7	exact	7	3
SSA-915282	SSA-915282: Denial of service Vulnerability in Interniche IP-Stack based Industrial Device	7.5	exact	6	3
SSA-725549	SSA-725549: Denial of Service of ICMP in Industrial Devices	5.3	exact	6	3
BOSCH-SA-741752	Multiple vulnerabilities in Rexroth IndraMotion and IndraLogic series	10.0	model	5	1
BOSCH-SA-475180	Vulnerabilities in CODESYS V2 runtime systems	9.8	model	5	1
BOSCH-SA-577411	Vulnerabilities in the communication protocol of the PLC runtime	8.1	model	5	1
SSA-224824	SSA-224824: Denial of Service Vulnerabilities in SIMATIC S7-1200 CPU Family Before V4.7	7.5	exact	5	3
SSA-392349	SSA-392349: Denial of Service Vulnerability in Industrial Devices	7.5	exact	5	3
BOSCH-SA-152060	Denial of Service in PLC Runtime affecting Rexroth IndraMotion Products	7.5	model	5	1
BOSCH-SA-350374	Vulnerability in the routing protocol of the PLC runtime	7.3	model	5	1
SSA-717113	SSA-717113: Cross-Site Request Forgery (CSRF) Vulnerability in SIMATIC S7-1200 CPUs before	7.1	exact	5	3
SSA-478960	SSA-478960: Missing CSRF Protection in the Web Server Login Page of Industrial Controllers	6.5	exact	5	3
SSA-264814	SSA-264814: Timing Based Side Channel Vulnerability in the OpenSSL RSA Decryption in SIMAT	5.9	exact	5	3

5 Applications and device landscape

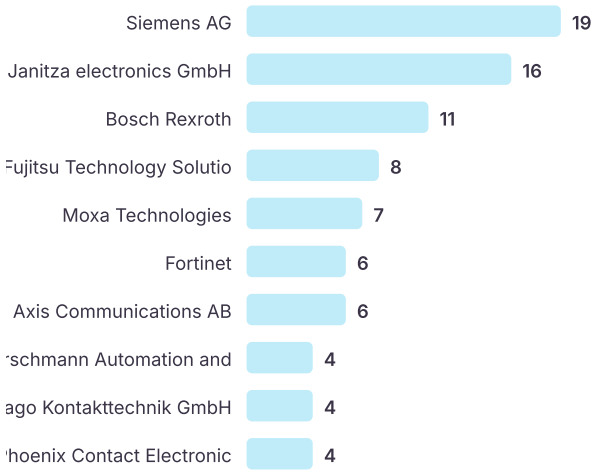
APPLICATIONS PER NETWORK (FIREWALL TRAFFIC, DOCUMENTATION DATABASE)

Network	most common applications (connections)
Energieverteilung	Energiemanagement (1.134.312), Zeitdienst und Protokollierung (39.671)
Halle3_CAM	Videomanagement (91.741), Zeitdienst und Protokollierung (30.698)
Lackiererei_Leitstand	MES Produktionsdaten (206.261), Prozessleitsystem (165.909), Zeitdienst und Protokollierung (32.894), Fernwartung (38)
Montage_Anlagennetz	MES Produktionsdaten (928.454), Prozessleitsystem (135.954), Zeitdienst und Protokollierung (42.355), Fernwartung (61)
Presse_Maschinennetz	MES Produktionsdaten (800.793), Zeitdienst und Protokollierung (32.803), Fernwartung (44)
Prueffeld	Qualitätsdaten (53.894), Zeitdienst und Protokollierung (35.614)

DEVICE CLASSES



VENDOR



6 Terms

CMDB	Inventory (CMDB): the self-maintained device list as Excel (template from OTScan 3 or your own list). Provides name, type, vendor, location, trade and responsible persons. OTScan 3 only reads it.
Overall inventory	One Excel file with all devices from CMDB, scan and Splunk – each value with its source. Basis for the initial inventory.
Documentation database	Applications, servers, zones and network areas from the network and application overview and the research register. OTScan 3 uses it to assign communication partners to applications.
Scan / staged scan	Active detection by OTScan 3 in stages (reachability, services, device details).
Splunk	Analysis of the firewall logs: addresses, partners, ports, zones. Traffic within a network is not visible there.
Traffic light	GREEN = no insecure services. YELLOW = insecure services – close in a planned way. RED = particularly dangerous services – clarify immediately.
Insecure service	Service that the traffic rules (HanselCraft default, customizable) prohibit or only allow when secured (e.g. FTP, Telnet, HTTP login, SNMPv1/v2c).
Without firewall traffic	The service was not used through the firewall during the Splunk period – candidate for disabling.
Vendor advisory	Security advisory from a vendor (CSAF, CISA ICS). Quality exact / model / vendor.
Zone / service / policy	From the FortiGate log: security zone of source and destination, service name, firewall rule number.
Risk (detail view)	2 points per critical port (max. 8), +2 for a vendor advisory with CVSS ≥ 7, +1 for a weaker advisory.