TECHNOLOGY · SECURITY · DATA PROTECTION

Technology, security and data protection

Connections, network traffic, assessment logic, data storage, imports, protective measures, third-party components and AI assistant.

Version 3.0.0 · 12 Nov 2026
HanselCraft · otscan.hanselcraft.de

1 Purpose and principles

This document describes for IT security, data protection and operations what OTScan 3 does technically, which data is created, where it is stored and which connections the program establishes. It is based on program version 3.0.0.

- **Local:** all scan, inventory and report data stays on the computer or in folders chosen by the user.
- **No telemetry:** OTScan 3 does not send usage, crash or device data to HanselCraft or third parties.
- **Read-only:** no write commands to devices, no password attempts, no nmap scripts of the categories vuln, brute, exploit or dos.

2 Internet connections

Function	When	Destination	What is transmitted
License activation	when clicking **Activate**; if the server could not be reached, OTScan 3 retries the activation at program start (at most once every 24 hours) until it succeeds	HanselCraft license server (HTTPS)	license key, computer ID (SHA-256 hash of computer name and MAC address, truncated – not reversible), program version, product ID
Release computer	only when clicking "Release this computer"	license server (HTTPS)	license key and computer ID
Update vendor advisories	only when clicking **Update online**	public CSAF sources (e.g. Siemens ProductCERT, CERT@VDE, BSI, Bosch PSIRT, CISA), CISA KEV list, FIRST EPSS	only downloads of public files – no data about your devices or networks
AI assistant (optional)	only if you set up an assistant (e.g. Claude Desktop) and ask it questions	provider of the assistant (e.g. Anthropic) – the connection is made by the assistant, not by OTScan 3	whatever the assistant reads through the interface: network names, IP and MAC addresses, device names, vendors, open ports, findings, deadlines (see section 10)

> OTScan 3 works completely without internet: the license check during operation runs offline with a signed license file (public key in the program). The vendor advisories can also be prepared on another PC with `otsp_csaf_sync.py` and imported with **Import file ...**.

Proxy: for these downloads OTScan 3 uses the system proxy settings (environment variables HTTPS_PROXY/HTTP_PROXY, on Windows also the system setting). Mail drafts of the initial commissioning are only created as files (Outlook draft or `.eml`) and are never sent.

3 Network traffic in the plant network

Stage	Traffic
0 Neighbour detection	ARP requests (at most 20 packets/s); without administrator rights a short TCP connection attempt per address
1 Find devices	TCP connection setup to fixed OT port lists (at most 50 packets/s), occupied addresses only
2a Services	version probes to open ports, read-only OT queries only (e.g. S7 identity; Modbus device ID only on request)
2b Names	a few standard UDP queries (SNMP GET with "public", BACnet, KNX)
CAM	WS-Discovery and ONVIF GetDeviceInformation (read-only); with stored credentials at most 3 failed logins per run

One network, one scanner: OTScan 3 warns about other nmap processes. The approval tick ("approval of the plant owner is available") is valid for 30 days and does not replace a written approval. Schedule and network chain run unattended – only with organisational approval.

4 Assessment logic

Insecure services are assessed according to the **traffic rules** – a HanselCraft default aligned with IEC 62443 (zones and conduits) and general OT security practice. It is not a standard and does not quote one. Weight 3: services with remote control, command execution or file access (Telnet, r-commands, VNC, FTP, SMB); 2: clear-text login or information leakage (HTTP, SNMPv1/v2c, NetBIOS, RPC, NFS, LDAP ...); 1: secondary transports or services that may be acceptable when encrypted. One open port from the list results in YELLOW. To adapt: `verkehrsregeln.json` in the data folder.

Vendor advisories: detected models and firmware versions are compared offline with the supplied CSAF data set (match quality exact, model, vendor), supplemented by CISA KEV and EPSS.

5 Data storage

Data	Windows	Linux
Database, settings, scan MAC list, schedules, vendor rules, traffic rules, documentation database	`%APPDATA%\OTScan3`	`~/.local/share/OTScan3`
Scan results (XML) and reports	output folder (default: Documents)	Documents folder

Data	Windows	Linux
Inventory, Splunk storage, acceptances, templates, backups	Documents\OTScan3_...	Documents/OTScan3_...
Camera passwords	encrypted with Windows DPAPI (bound to the user account)	keyring (secret-tool)
License	signed license file in the data folder	same
AI assistant: setting, approval code (HMAC only), log	`%APPDATA%\OTScan3\ki_assistent.json`, `ki_schnittstelle.log`	`~/.local/share/OTScan3/…`
AI assistant: secret key per installation	`%LOCALAPPDATA%\HanselCraft\OTScan3\ki.schluessel`, bound to the user account with DPAPI	`~/.config/hanselcraft-otscan3/ki.schluessel` (only valid with permissions 0600 and owned by the user)
AI assistant: state counter	`ki.stand` next to the key (signed)	`ki.stand` next to the key (signed)

> The database is not encrypted. Protect it through the user profile and the disk encryption of the computer. All outputs contain IP addresses, MAC addresses, device names and locations and must be treated as confidential. Personal data is only created if users enter it themselves (e.g. name and phone number of the technician in the initial commissioning, or responsible persons in the CMDB).

6 Data imports

- **Inventory (CMDB):** Excel file, read only; addenda are created as a copy.
- **Firewall logs:** generic import of exports (e.g. a Splunk search over FortiGate logs, format v2: `<network>_<from>_<to>_regeln.csv` and `_inventar.csv`); no connection to Splunk itself.
- **Documentation:** JSON import for applications, systems and network ranges.

7 Protection with administrator rights

On Windows the program is located in `C:\Program Files\OTScan3` (only administrators can change it). With administrator rights, OTScan 3 starts nmap only from protected folders and only with options from a fixed list; scripts only from the nmap program folder. On Linux, nmap receives the capability `cap_net_raw` for the group `otscan3` only; adapters are reconfigured by a helper with strictly checked arguments and only for released adapters.

8 Retention and deletion

OTScan 3 does not delete anything automatically. Retention periods are defined by the operator. To delete a network completely: close the program, remove the files with the network name in the output folder and in the subfolders OTScan3_Inventar and OTScan3_Splunk, delete the state files under `…\OTScan3\stufenlauf` and remove the network in Data maintenance. Backups (ZIP) contain the same data.

9 Third-party components

nmap (Nmap Public Source License, installed separately), Npcap (own license, Windows), Python and libraries (openpyxl, python-pptx, Pillow, fpdf2, lxml, pandas), fonts Inter and Bricolage Grotesque (SIL OFL), icons Lucide (ISC). The license texts are located in the program folder (`THIRD_PARTY_NOTICES.txt` , `LICENSE_NPSL_Nmap.txt` , `assets/LIZENZ_*`). Terms of use: `EULA.txt` and `HAFTUNG_UND_NUTZUNG.txt` (currently in German only – see `docs/EULA_Lesehinweis.txt`).

10 AI assistant (optional)

On the **AI assistant** page, OTScan 3 can be registered as a local MCP interface (Model Context Protocol) in an assistant such as Claude Desktop. The interface is a **local bridge**: the assistant starts it as a program on the same computer and talks to it via standard input and output. It opens no network port and makes no internet connection of its own.

- **Reading:** only the OTScan 3 database, read-only (networks, scan runs, devices, findings, evidence & deadlines).
- **Transmission:** whatever the assistant reads, it sends to its provider for processing (e.g. Anthropic). This includes IP and MAC addresses, device and network names, vendors, open ports and findings. Clarify beforehand whether this data may leave your organization, and observe the provider's terms. Without an entry in the assistant the interface is not active.
- **Scans by the AI:** off by default. Only with the tick "AI may start scans" and a six-digit approval code that only the user interface shows (valid for 30 minutes, single use, expires after three wrong entries). Only networks that have been created (name and CIDR), only private IPv4 ranges up to /16, at most one AI scan at a time; no tools without a valid license or trial period.
- **Protection of the code:** only an HMAC with a secret key per installation is stored; the key lies outside the data folder (Windows: only encrypted with DPAPI – an unencrypted key file is not accepted there; Linux: only with permissions 0600 and owned by the user). The switch and the code are additionally signed with a running state counter: every change invalidates older versions of the settings file, so used and expired codes stay used even after a restart. Reading or writing the settings file alone does not yield a valid code.

Limits: the approval code protects against scans that an assistant triggers only through the interface. Anyone with write access to the user profile can reset the key, state and settings files together to an older state and so make a code that was already given out valid again. Anyone who can run programs under the user account (on Linux: anyone who can read or change the home folder) can bypass the approval entirely. Therefore do not give the assistant tools that may read or change files in the user profile or run programs – not even while scans by the AI are switched off.