IT-Network DocuScanner

Anleitung Version 2.12.4

Sat-iTec Systemhaus GmbH · Mai 2026

1. Was ist der IT-Network DocuScanner?

Der IT-Network DocuScanner ist eine vollautomatische On-Premise-Loesung zur Inventarisierung und Schwachstellen-Analyse von Windows- und Linux-Netzwerken. Statt manuell durch Active Directory zu klicken, Subnetze auszuwerten oder Excel-Listen zu pflegen, scannt das Tool autark im Hintergrund und liefert eine durchsuchbare, BSI-konforme Dokumentation Ihrer gesamten IT-Landschaft.

Alle Daten bleiben auf dem Kunden-Server. Es gibt keine Cloud-Pflicht, keine externen Telemetrie-Calls, keine Lizenz-Phone-Home zu Drittanbietern.

1.1 Komponenten ab v2.12.4

Ab v2.12.0 besteht die Installation aus drei selbstaendigen Windows-Diensten (auf Linux: drei systemd-Units):

- ITScannerDashboard — Web-Oberflaeche, REST-API, Datenbank-Manager (Port 8585)
- ITNetworkScanner — Discovery-Engine fuer AD, Subnetze, Shares, Software (lokal/remote)
- ITScannerCVE — CISA-KEV + NVD + EPSS-Sync und Schwachstellen-Matching (Port 8586, loopback)

2. Installation

2.1 Windows

- Setup-v2.12.4.exe als Administrator starten.
- Setup beendet die alten Dienste, installiert nach C:\Program Files\Sat-iTec\ITScanner und legt die drei Dienste neu an.
- Standard-URL nach Install: http://localhost:8585
- Beim ersten Aufruf wird das Admin-Login angelegt — Standard-Username admin, frei zu vergebendes Passwort (mindestens 12 Zeichen).

2.2 Linux (Debian/Ubuntu)

- sudo dpkg -i itscanner-server_2.12.4_amd64.deb
- sudo systemctl enable --now itscanner itscanner-cve
- Browser auf http://server-ip:8585

2.3 Linux (manuell, tar.gz)

- tar -xzf itscanner-linux-amd64-v2.12.4.tar.gz
- cd linux/ && ./start-server.sh

3. Trial-Lock und Lizenz

Ab v2.11.0 gilt eine harte 14-Tage-Trial-Phase. Ohne gueltige Lizenz nach Tag 14 reagiert die API mit HTTP 402 (Payment Required) und das Dashboard zeigt eine Bezahl-Pflicht-Sperre. Die Lizenz-Pflicht ist gegen Manipulation gesichert ueber Triple-Persistenz: Datenbank, .install.lock-Datei (SHA256+Salt) und Windows-Registry — Faelschungsversuche werden erkannt und blockieren die Dienste.

Eine Lizenz kann ueber https://www.itnetwork-docu.com/pricing/ bestellt werden — 49,50 EUR netto pro Jahr, automatische Verlaengerung nach 12 Monaten.

4. Scan durchfuehren

- Im Dashboard auf den Tab 'Scan' wechseln.
- Domain-Credentials hinterlegen (werden im Credential-Vault AES-256-verschluesselt gespeichert).
- Subnetz-Range eingeben oder 'auto-derive' aktivieren — der Scanner leitet die Subnetze aus den Default-Gateways der bekannten Hosts ab.
- 'Scan starten' druecken — Fortschritt ist live in der UI sichtbar.

4.1 Was wird gescannt

- Active Directory: User, Gruppen, OUs, Computer-Objekte, Group Policies (mit GPMC), member_of-Relationen.
- Subnetze: Ping-Sweep, Reverse-DNS, ARP-Tabelle, Routing-Info.
- Software-Inventar: WMI/CIM-DCOM, RemoteRegistry-Fallback fuer Workgroup-Hosts, OS-Vollbezeichnung.
- Server-Rollen: Win32_ServerFeature auf Windows-Servern (eigener Tab).
- Freigaben: SMB-Shares, NFS-Detection ab Port 2049/445 (Windows benoetigt 'Services for NFS').
- Schwachstellen: kontinuierliches Matching gegen CISA-KEV, NVD und EPSS — siehe Kapitel 6.

5. BSI-Hardening und Compliance

- Dynamische BSI-Checks: aus den eingelesenen DB-Daten leitet das Tool den Konformitaets-Status fuer typische BSI-IT-Grundschutz-Bausteine ab.
- Drift-Monitoring: jede Aenderung im Inventar wird mit Zeitstempel und Diff dokumentiert (Compliance-Wache).
- Audit-Log: jeder Login, jeder Scan, jede Konfigurationsaenderung ist nachvollziehbar — DSGVO-Auskunfts-API enthalten.
- MFA via TOTP-App (Google Authenticator, Microsoft Authenticator, FreeOTP) optional aktivierbar.

6. Schwachstellen-Scanner (CVE-Worker)

Der CVE-Worker laeuft als eigener Windows-Dienst (ITScannerCVE) und synchronisiert taeglich automatisch:

- CISA Known Exploited Vulnerabilities (KEV) — aktuell ausgenutzte Schwachstellen.
- NVD — National Vulnerability Database der NIST (CVSS-Scores).
- EPSS — Exploit Prediction Scoring System (Wahrscheinlichkeit einer Ausnutzung in den naechsten 30 Tagen).

Das Matching gegen das lokale Software-Inventar erfolgt nach jeder Sync- bzw. Scan-Runde.

6.1 Neuerungen in v2.12.4

Host-Namen statt nur IDs

Im Schwachstellen-Tab zeigt die Tabelle jetzt den DNS-Namen (oder NetBIOS-Namen) statt der numerischen host_id. Wer Operating ist sieht direkt welcher Rechner ein Problem hat.

Auto-Fix fuer geschlossene Findings

Findet ein Match-Cycle eine CVE-x-Software-Kombi nicht mehr (weil die Software gepatched oder deinstalliert wurde), wird das Finding automatisch mit fixed_at = Zeitstempel geschlossen. Vorher mussten geschlossene CVEs manuell quittiert werden.

Versions-Range-Check

Eine KEV-Entry 'Microsoft Office 2010' matcht jetzt nur noch Office 2010, nicht mehr alle Office-Versionen. Die Versions-Komponente wird aus dem product-Feld via Regex extrahiert (Jahres- oder Versionsnummer) und muss exakt uebereinstimmen. False-Positives-Reduktion typischerweise um Faktor 10.

Sync-Status-Reset

Wenn die CVE-DB existiert aber der Sync-Status leer ist (z.B. nach einer DB-Restore), wird der Status-Eintrag automatisch rekonstruiert. Sync-Buttons werden nicht mehr faelschlich gesperrt.

Severity-Mix korrekt

KEV-Eintraege mit knownRansomwareCampaignUse=Known werden als 'kritisch' eingestuft, alle anderen als 'hoch'. Im UI erscheint jetzt der Mix kritisch + hoch statt nur hoch.

7. MSP-Funktionen (optional)

Fuer Managed Service Provider und mehrstandort-Betreiber bringt v2.09.0 ein integriertes MSP-Pairing:

- Pairing-Code im Kunden-Dashboard erzeugen, beim MSP-Hub eintragen — fertig.
- Verschluesselter Reverse-Tunnel via ed25519-Keypair, kein offener eingehender Port noetig.
- MSP-Console sieht alle Kunden auf einer Karte, kann Schwachstellen-Reports erstellen und Alerts konsolidieren.
- High-Availability-Setup Augsburg-Bollnaes (Deutschland-Schweden-Failover) verfuegbar — siehe Trust-Center.

8. Pulse-Monitor und Wiki

- Pulse: Live Up/Down-Monitoring fuer alle bekannten Hosts mit Latenz-Trends.
- Wiki: integrierte Dokumentations-Plattform, jede Host-Seite kann mit Free-Text-Notes, Bildern und Schluessel-Wert-Listen angereichert werden.
- Vault: AES-256-verschluesselter Credential-Speicher fuer Scan-Credentials und beliebige Geheimnisse.

9. Tray-Icon und Updates

Auf Windows zeigt ein Tray-Icon den Dienst-Status. Linksklick oeffnet das Dashboard, Rechtsklick bietet 'Dashboard oeffnen', 'Dienst neustarten' und 'Beenden'.

Updates werden automatisch via GitHub-Release-Channel erkannt. Im Tab 'Einstellungen / Updates und Lizenz' kann mit einem Klick das neueste Setup heruntergeladen und installiert werden — Dienste werden sauber gestoppt, ueberschrieben und neu gestartet.

10. Support und Updates

- Webseite: https://www.itnetwork-docu.com
- E-Mail: support@sat-itec.de
- Online-Anleitung und Changelog: https://www.itnetwork-docu.com/anleitung/
- Sicherheits-Issues vertraulich an security@sat-itec.de — PGP-Key auf der Webseite.

Anhang A: Aenderungsverlauf v2.12.x

Version	Aenderungen
2.12.4	Host-Namen-Anzeige, Auto-Fix, Versions-Range-Check, Sync-Status-Reset, UNIQUE-Index Migration
2.12.3	DB-Lock-Fix via _pragma()-DSN-Format, asymmetric IsAvailable-Cache, Severity-Mix critical+high
2.12.2	Dashboard-Proxy fuer /api/vulnscan/* zum CVE-Worker
2.12.1	WAL-Mode-Verify, _txlock=immediate entfernt
2.12.0	CVE-Worker als eigener Dienst (ITScannerCVE), eigene cve.db, KEV+NVD+EPSS-Sync
2.11.2	Sidebar-Badges, Service-Mode-Race-Fix mit Health-Probe
2.11.1	Login-Form Hotfix, statische Felder
2.11.0	Trial-Lock 14 Tage hart, Triple-Persistenz-Lizenzpruefung
2.10.0	Senior-Quality-Hardening, Unit-Tests, CI/CD, Tray-Restart-after-Update
2.09.0	MSP-Pairing, Vault, Wiki, Pulse, Drift-Monitoring, MFA (TOTP), Vuln-Scanner