

WAS C4SAM IST

Eine Plattform für Sicherheit, Automatisierung und IT-Betrieb — self-hosted.

C4SAM ist keine weitere Einzellösung. Es ist eine **zentrale Plattform, die sicherheits- und betriebsrelevante Funktionen bündelt** — Asset Discovery, Schwachstellenmanagement, SIEM, Automatisierung, Compliance und KI — in einer modularen Architektur mit gemeinsamer Datenbasis. **Bestehende Systeme werden eingebunden, nicht ersetzt:** C4SAM bindet die Tools ein, die Sie bereits betreiben, und ersetzt nur dort, wo es nachweislich Kosten spart.

~40

integrierte Open-Source- und proprietäre Komponenten, zentral gepflegt

100%

self-hosted — On-Premises, Private Cloud oder durch MSP betrieben

0

Hersteller-Lock-in — offene Standards, dokumentierte Schnittstellen, jederzeit wechselbar

AT

entwickelt und betreut in Österreich, EU-Rechtsrahmen

Plattform-Module

Modular — einzeln oder als kompletter Stack nutzbar

 Asset Discovery & CMDB Agenten- und netzwerkbasierte Discovery, Segmentzuordnung, Lifecycle-Tagging, Abbildung der Geschäftskritikalität. Native CMDB als führendes System.	 Schwachstellen- & Bedrohungserkennung Regel- und verhaltensbasierte Detection (Wazuh, Zeek, Suricata), laufendes Scanning, True-Risk-Priority-Bewertung über IT, OT und IoT hinweg.
 Patch-, Konfigurations- & Workflow-Automatisierung Orchestrierung via SaltStack: Patch-Rollout mit Verifizierung, Quarantäne-Logik, Eskalationspfade, Self-Healing und Drift-Korrektur.	 Log-Konsolidierung & SIEM Normalisierung von Syslog, Beats, Winlog, NetFlow und SNMP in ein einheitliches Schema. Korrelationsregeln, Alert-Deduplizierung, Bündelung zu Cases.
 Compliance & Reporting Control-Mapping für NIS2, ISO 27001, DSGVO und DORA. Revisionssichere Audit-Trails, Nachweis-Export, geplante Governance-Reports.	 Observability & Service Health Service-Checks von ICMP bis zum vollen HTTP-Check, Hypervisor- und System-Metriken, Netzwerk-Infrastruktur — zusammengeführt in Cockpit und Service Tree. Frühwarnung, bevor Storage, Zertifikate, Disks oder Netzwerk zum Ausfall führen; der Service Tree zeigt die Ursache.
 AI Layer & Cpt.SAM LLM-Gateway für Cloud- und lokale Modelle mit Budgets je Team. Cpt.SAM greift über den C4SAM MCP-Server auf Live-Daten der Plattform zu — unter derselben Rechtevergabe.	 Zertifikats-Lifecycle Automatisierte Discovery, Ausstellung, Erneuerung und Rollout — öffentliche CAs und interne PKI, ohne Internet-Abhängigkeit. Ausgelegt auf 47 Tage Gültigkeit.

Detection- & Response-Pipeline

Identisch für IT, OT und IoT

01 Events Logs, NetFlow, Telemetrie	02 Regeln Erkennungslogik	03 Alerts Relevante Signale	04 Anreicherung Asset, Owner, Exposure	05 Cases Alerts zusammengeführt	06 Triage True Risk Priority	07 Response Playbooks, Isolierung	08 Nachweis Audit-Trail
● Sehen Sammeln und erkennen	● Bewerten Kontext und Priorität	● Handeln Automatisiert reagieren	● Nachweisen Belege für Audits				

Deployment-Architektur

Docker-Swarm-Management-Ebene · WireGuard-Transport



Skaliert horizontal über zusätzliche Management Nodes und Minions. Mandantenfähig über Standorte, Tochtergesellschaften oder MSP-Kunden hinweg — mit Datentrennung je Mandant und delegierter Administration.

Schnittstellen & Integration

Offene Standards, dokumentierte APIs

Ingest	Syslog (RFC 3164/5424), Beats, Winlogbeat, NetFlow/IPFIX, SNMP v2c/v3, WMI, SSH, agentenbasierte Collectors
Identity	LDAP, Active Directory, SAML 2.0, OIDC, SCIM-Provisioning, MFA (TOTP, WebAuthn)
Outbound	REST API (OpenAPI 3), Webhooks, SMTP, Syslog-Forwarding, S3-kompatibler Objektspeicher für Archive
Ökosystem	ITSM- und Ticketing-Systeme, Drittanbieter-SIEM, Firewalls und NAC, Microsoft 365 und Entra ID, Hypervisoren und Cloud-APIs
AI	C4SAM MCP-Server, OpenAI-kompatible Endpoints, lokal betriebene Modelle (keine Daten verlassen die Installation)

Compliance-Abdeckung

Technische Maßnahmen und Nachweise ab Werk

NIS2 / NISG 2026	Asset-Inventar, Risikomanagement, Incident Detection und Meldeworkflows (24/72 h), Lieferkettenregister, Reporting für die Geschäftsführung
ISO/IEC 27001	Control-Mapping nach Annex A, Nachweiserfassung, interner Audit-Trail, Abweichungsverfolgung
DSGVO	Datenminimierung durch Self-Hosting, Zugriffsprotokollierung, Aufbewahrungsrichtlinien, Verarbeitung ausschließlich in der EU
DORA	IKT-Risikoregister, Nachweise aus Resilienz-Tests, Abbildung von Drittanbieter-Abhängigkeiten

Deployment-Optionen

Kein Integrationsprojekt erforderlich

	On-Premises Bare Metal oder virtualisiert, auch vollständig air-gapped betreibbar.		Private Cloud Ihre eigene Umgebung bei jedem Provider — kein gemeinsam genutztes C4SAM-SaaS.		Betrieb durch MSP Mandantenfähiger Betrieb mit Trennung je Kunde und delegierter Administration.
---	--	---	--	---	--

Enterprise-grade Open Source, von uns betrieben. Komponenten wie Elastic Stack, Wazuh, Zeek und SaltStack werden von C4SAM integriert, gehärtet, orchestriert und aktuell gehalten — mit definiertem Lifecycle und Support-Status je Komponente. Sie bekommen die Funktion, ohne den Integrationsaufwand zu tragen.