



MANAGEMENT-PRÄSENTATION · JULI 2026

C4SAM Cockpit

Sicherheit, Automatisierung und Management Ihrer IT-Infrastruktur — eine Plattform, ein Blick, unter Ihrer Kontrolle.

● Eine Plattform

● Self-hosted

● Made in Austria

Drei Entwicklungen setzen jede IT-Organisation unter Druck

01



Regulatorischer Druck

NIS2, DSGVO, ISO 27001, DORA: mehr Pflichten, mehr Nachweise — und persönliche Haftung der Geschäftsführung.

02



Tool-Wildwuchs & Fachkräftemangel

Dutzende Einzellösungen ohne gemeinsames Bild — und zu wenige Fachleute, um sie alle zu betreiben.

03



Kosten- und Erwartungsdruck

Das Business erwartet Sicherheit, Verfügbarkeit und KI-Fähigkeiten — bei gleichbleibendem Budget.

Das größte Risiko ist keine einzelne Bedrohung — es ist die Komplexität selbst.

Ein Cockpit statt Dutzender Konsolen

C4SAM sammelt und normalisiert Daten aus allen Security- und Infrastruktur-Tools in einem einheitlichen Bild — nutzbar auch ohne tiefes Security-Know-how.



Security

Schwachstellen, Angriffe und Anomalien erkennen — über IT, OT und IoT hinweg.



Observability

Service-Checks und Infrastruktur-Metriken — mit einem Service Tree, der zur Ursache führt.



Automatisierung

Patchen, reagieren, konfigurieren — automatisiert, konsistent, nachvollziehbar.



Management & Compliance

Assets, Services und Nachweise — zentral in der nativen CMDB.

Eine Plattform: **Sehen** → **Bewerten** → **Handeln** → **Nachweisen**

● Automatisiert Routinearbeit

● Auch ohne Spezialwissen bedienbar

● Bestehende Tools werden eingebunden

● Vom KMU bis Konzern skalierbar

Ein kuratierter App-Katalog, eine Oberfläche

Rund 40 integrierte Open-Source- und proprietäre Lösungen — zentral installiert, konfiguriert und aktuell gehalten. C4SAM bindet die Systeme ein, die Sie bereits betreiben, statt sie zu ersetzen.

~40 kuratierte Apps

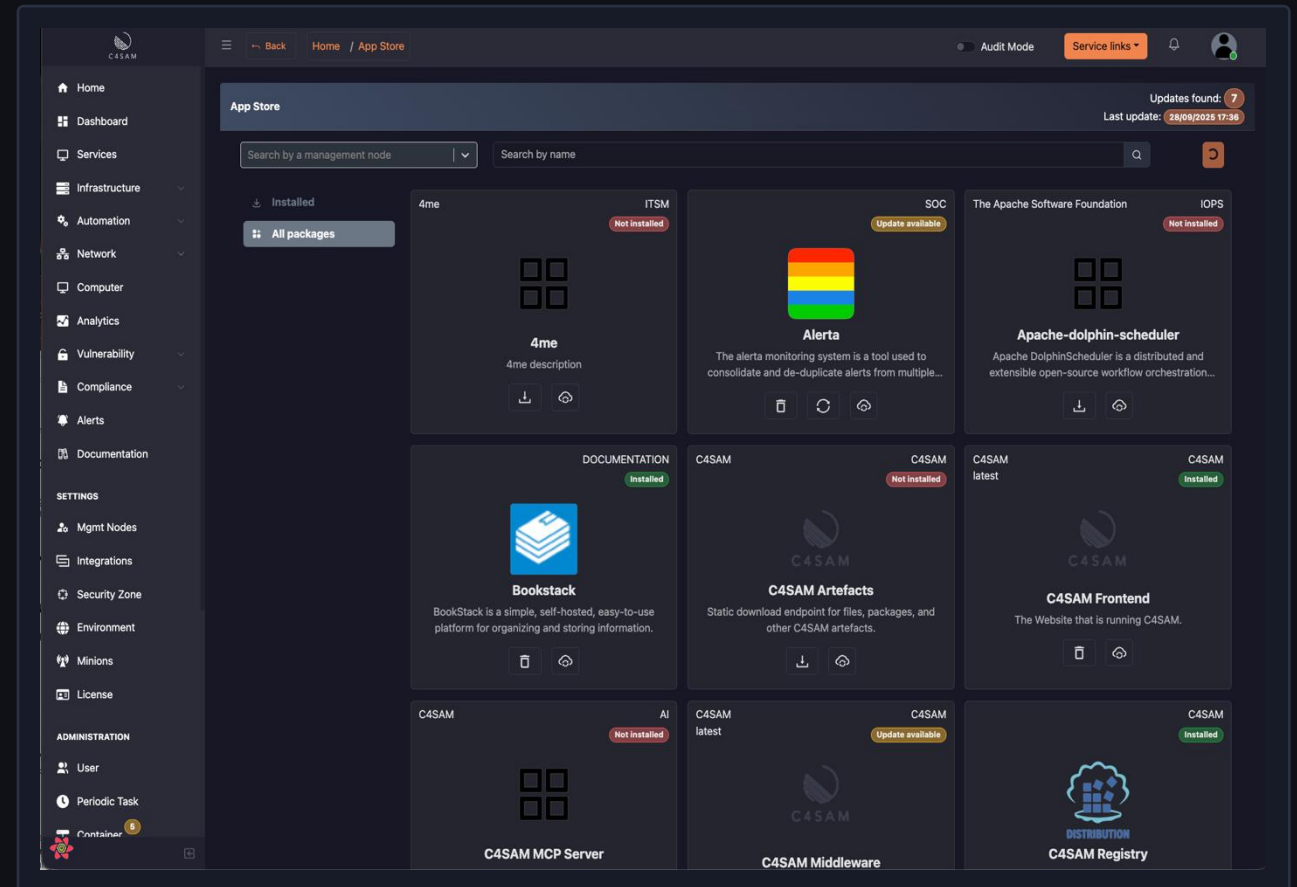
Open Source und proprietär, ein Katalog.

100% Managed Lifecycle

Zentral installiert, konfiguriert und aktuell gehalten.

0 erzwungene Ablösungen

Ihre bestehenden Tools bleiben im Einsatz und werden eingebunden — ersetzt wird nur dort, wo es nachweislich Kosten spart.



Vom rohen Event zum belastbaren Nachweis

Jedes Signal durchläuft dieselbe Pipeline — reproduzierbar, auditierbar und identisch für IT, OT und IoT.



Erkennen, bevor der Service ausfällt

Service-Monitoring von ICMP bis zum vollständigen HTTP-Check, Hypervisor-Metriken, System-Performance und Netzwerk-Infrastruktur — zusammengeführt im Cockpit und im Service Tree.



Von ICMP bis zum vollen HTTP-Check

Erreichbarkeit, Ports, TLS-Handshake, Antwortinhalt und Latenz-Schwellwerte.



Hypervisor- & System-Metriken

CPU, Memory, Storage und I/O über Hosts, VMs und Container.



Netzwerk-Infrastruktur

Switches, Router, Firewalls und Verbindungen via SNMP und NetFlow.

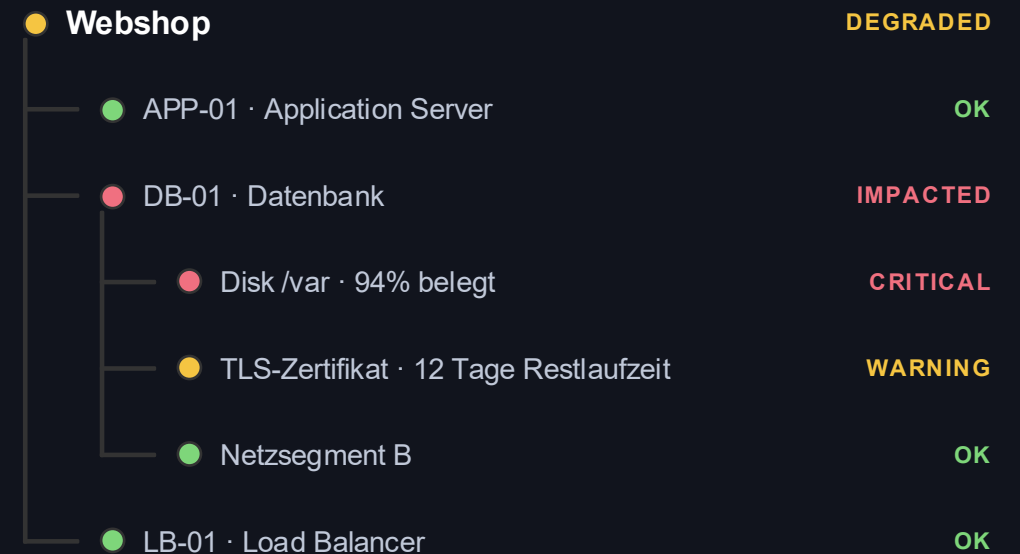


Service Tree

Jeder Check ist dem Business-Service zugeordnet, den er stützt.

SERVICE TREE

live



Ursache: Speicherbelegung auf DB-01 — erkannt, bevor der Service ausfiel.



Was zuerst? True Risk Priority gibt die Antwort

True Risk Priority

Scanner-Scores allein sagen nichts über Ihr Geschäft aus. C4SAM gewichtet Exposure, Geschäftskritikalität und Erreichbarkeit — und zeigt Ihnen, was zuerst zu beheben ist und warum.



Kontext statt reiner Scores

Exposure, Geschäftskritikalität und Erreichbarkeit gemeinsam gewichtet — nicht bloß ein CVSS-Wert für sich.



Priorität mit Begründung

Jede Schwachstelle erhält eine nachvollziehbare Priorität — samt der Gründe, die dazu geführt haben.



Verbindliche Fristen

Auditfeste Behebungsfristen nach internationalen Vorgaben (BOD-Systematik).

Automatisierung, die Routinearbeit übernimmt

Planen.
Ausführen.
Prüfen.

Jede Routineaufgabe läuft jedes Mal gleich ab — mit lückenlosem Audit-Trail. Wie viel manuellen Aufwand das in Ihrer Umgebung einspart, wird im Assessment mit Ihren eigenen Daten gemessen.



Patch-Management

Planen, ausrollen und prüfen — automatisch. Systeme bleiben aktuell, ohne Nachschichten.



Incident Response

Vordefinierte Reaktionen: Systeme isolieren, Regeln anpassen, Verantwortliche informieren — in Sekunden statt Stunden.



Betrieb & Konfiguration

Konsistente Umgebungen ohne manuelle Fehler — vom Deployment bis zum Zertifikat.

NIS2-Umsetzung: die Uhr läuft

1. Okt 2026

in Kraft in Österreich

Das österreichische NISG 2026, kundgemacht im Dezember 2025 — die Übergangsfrist läuft bereits.

~5.000

betroffene Unternehmen

18 Sektoren, ab 50 Mitarbeitenden oder 10 Mio. € Umsatz — plus Lieferkette.

10 Mio. €

Höchststrafe bzw. 2%

des weltweiten Umsatzes — mit persönlicher Haftung der Geschäftsführung.

24/72h

Meldefristen

Registrierung bei der nationalen Behörde, Vorfallsmeldung binnen 24 bzw. 72 Stunden.



C4SAM liefert die technischen Maßnahmen ab Werk: Asset-Inventar, Risikomanagement, Vorfallserkennung und -meldung — plus Governance-Reports für Audits und Behörden.

KI fürs Business — ohne Lock-in, ohne Cloud-Zwang



LLM-Gateway

Kontrollierter Zugang zu Cloud- und lokalen Modellen: Budgets, Berechtigungen und Nutzung je Team — Anbieter jederzeit austauschbar.



Ein Frontend für alle

Eine Oberfläche für jedes Modell und jeden Agenten — zentrale Benutzerverwaltung, Rechte je Modell und Tool, volle Transparenz über die Nutzung.

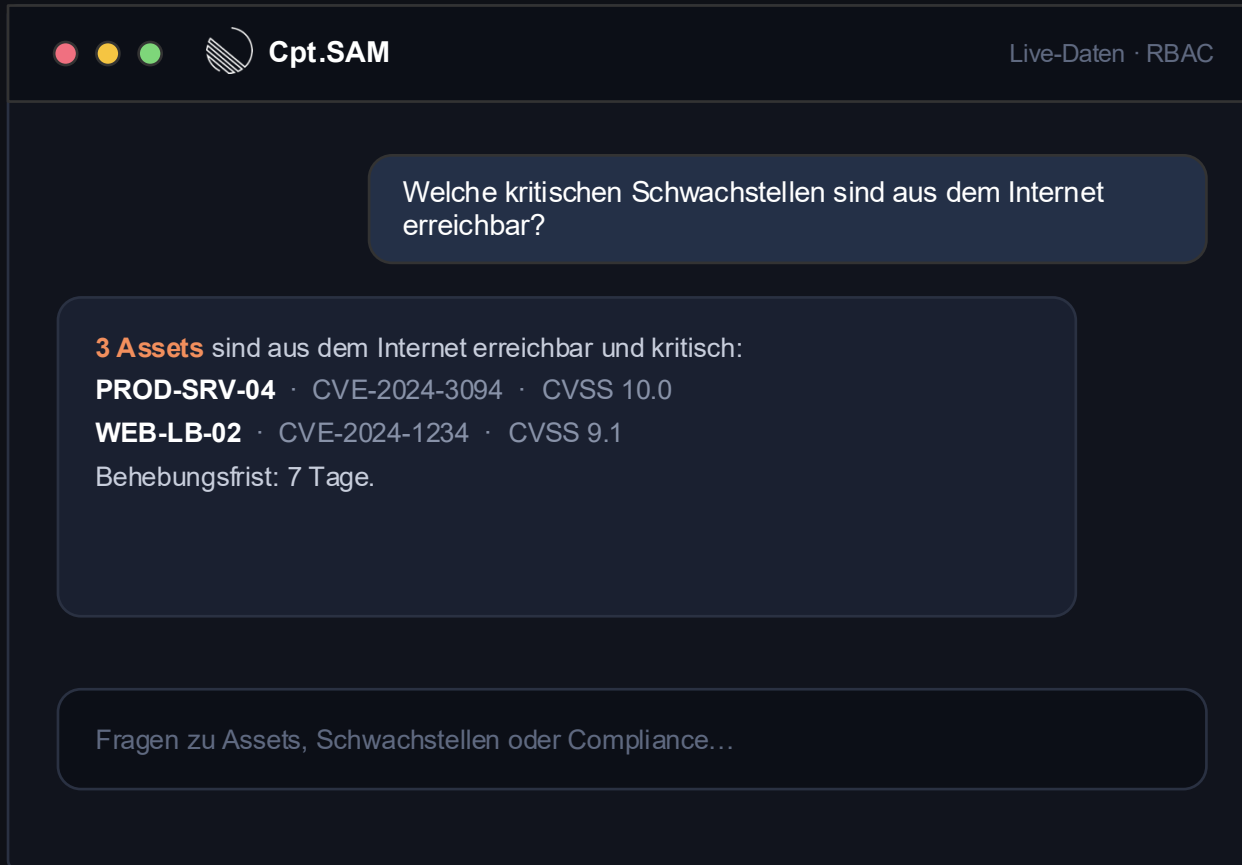


Persönliche KI-Agenten

Jeder Benutzer erhält einen eigenen, isolierten Agent-Container — mit eingegrenztem Modellzugriff und sicher verwalteten Credentials.

KI bereitzustellen ist die CIO-Aufgabe 2026: Das Business bekommt KI jetzt — die IT behält Kosten, Daten und Kontrolle.

Cpt.SAM: KI, die Ihre Infrastruktur kennt



Ihr Analyst im Cockpit

Fragen in natürlicher Sprache, beantwortet aus Live-Daten — ohne Tool-Wechsel, ohne Query-Sprache.



Security & Compliance von Haus aus

Datenzugriff über den C4SAM MCP-Server mit rollenbasierter Rechtevergabe — jeder sieht nur, was er sehen darf.



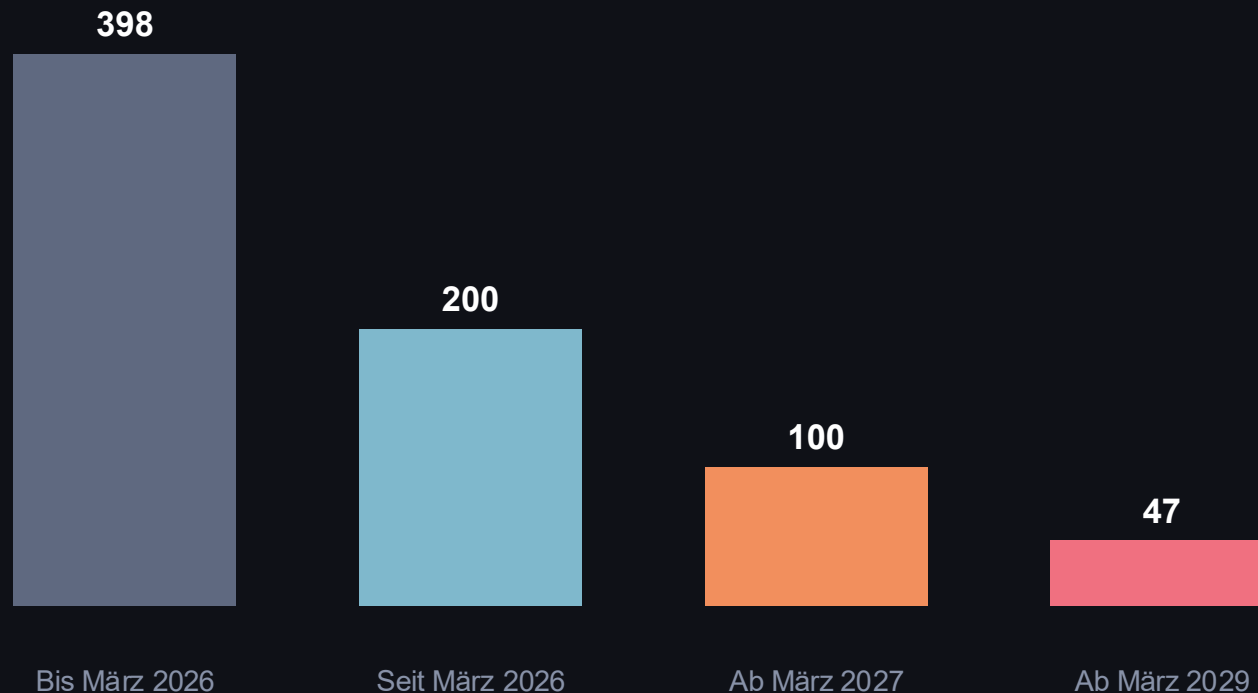
Läuft lokal

Ausführung in Ihrer eigenen Infrastruktur — DSGVO-konform durch Architektur, nicht durch Vertrag.

● Live-Demo verfügbar.

47-Tage-Zertifikate: Automatisierung wird Pflicht

Maximale Gültigkeit von TLS-Zertifikaten, in Tagen



Quelle: CA/Browser Forum, Ballot SC-081v3 (April 2025).

Was das bedeutet

- 8× häufigere Erneuerung — manuelle Prozesse skalieren das nicht
- Vergessene Zertifikate verursachen Ausfälle und Vertrauensverlust
- Domain-Validierung ab 2029 nur noch 10 Tage wiederverwendbar



Die C4SAM-Antwort

Vollautomatischer Lifecycle: Discovery, Ausstellung, Erneuerung und Rollout — inklusive interner PKI, ohne Internet-Abhängigkeit.

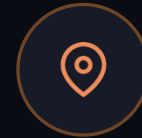
Ihre Infrastruktur, Ihre Daten, Ihre Regeln.

Europäische Datensouveränität ist kein nachträgliches Feature — sie steckt in der Architektur der Plattform.



Self-hosted & Open Source

Betrieb on-premises oder in Ihrer eigenen Cloud — kein US-SaaS-Zwang, keine Black Box.



Made in Austria

Entwickelt und betreut in Österreich — DSGVO und europäisches Recht als Fundament, nicht als Nachtrag.



Kein Lock-in

Offene Standards und Schnittstellen: Sie behalten jederzeit die Kontrolle — auch beim Wechsel.

Drei Gründe, die in der Geschäftsführung zählen

01



Konsolidierung & Kosten

Ein Vertrag, eine Plattform, eine Oberfläche — statt dutzender Lizenzen und Silos.

EIN ANBIETER

02



Sicherheit & Resilienz

Schneller erkennen, nach Priorität beheben, automatisiert reagieren — messbar kürzere Reaktionszeiten.

SCHNELLERE REAKTION

03



Zukunftssicher & investitionssicher

Ersetzt wird nur, was sinnvoll ist und Geld spart. KI und Zertifikatsautomatisierung sind bereits eingebaut.

KEINE ZWANGSABLÖSE

C4SAM macht IT-Sicherheit vom Kostenfaktor zu einem steuerbaren und nachweisbaren Prozess.

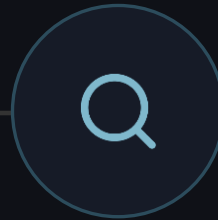
Vom Erstgespräch zum Proof of Concept



01

Erstgespräch & Betroffenheitsanalyse

NIS2-Betroffenheit, Zertifikatslandschaft, bestehende Tools — ein gemeinsames Bild Ihrer Ausgangslage.



02

Assessment

Sichtbarkeit über Assets, Schwachstellen und Compliance-Lücken in Ihrer Umgebung.



03

Proof of Concept

In Ihrer Infrastruktur — self-hosted, mit Ihren echten Daten.



C 4 S A M

C4SAM GmbH

Pülslgasse 4A, 1230 Wien, Österreich

+43 664 3518497

office@c4sam.com

www.c4sam.com



Deployment-Architektur: verteilt, verschlüsselt, self-hosted

Cockpit und Management Nodes bilden einen Docker Swarm (Overlay-Netzwerk). Minions in Standorten und Netzsegmenten binden sich über WireGuard VPN an.



Skaliert über zusätzliche Management Nodes und Minions — mandantenfähig über Standorte, Tochtergesellschaften oder Kunden hinweg.