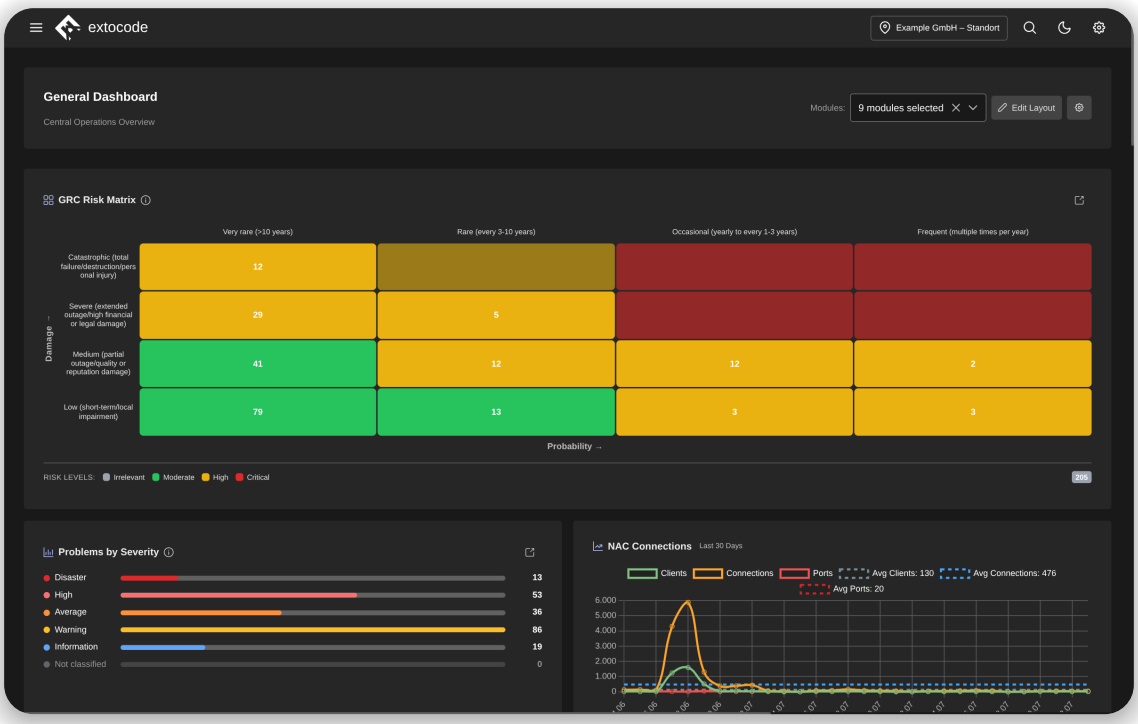
Central Operations Dashboard

Ihre gesamte IT-Infrastruktur. Eine Plattform.

Dokumentation, CMDB, Passwort-Manager, NAC, Firewall, Monitoring: **fünf Werkzeuge, fünf Wahrheiten, ein blinder Fleck.** Genau dort, zwischen dem was *läuft* und dem was *dokumentiert* ist, entstehen Sicherheitslücken, doppelte Arbeit und Audit-Stress. **COD macht damit Schluss.** Eine mandantenfähige Plattform führt Ihre komplette Infrastruktur herstellerübergreifend an *einem* Ort zusammen. Live, durchsuchbar, auditierbar und vollständig on-premise betreibbar.

COD auf einen Blick: mandantenfähig • modular • rollenbasiert (LDAP/AD) • on-premise oder Cloud • Multi-Norm-GRC (ISO 27001/27002, 9001, 22301, BSI 200-3, NIS2-Readiness) • Multi-Vendor-Firewall & VPN • NAC mit eigener PKI • TACACS+ (AAA) • Zabbix-Monitoring • Zero-Knowledge-Tresor • Angular 21 / Prisma • KRITIS-tauglich.



Ein Dashboard für alles: GRC-Risikomatrix, offene Probleme nach Schweregrad und NAC-Aktivität auf einen Blick.

Alle Module. Eine Oberfläche.

Kein Tool-Wildwuchs mehr: COD bündelt jede Disziplin des IT-Betriebs in *einer* konsistenten Plattform auf einem gemeinsamen, **lebenden** Datenbestand.

Netzwerk & Assets | **NAC & PKI** | **TACACS+** | **Firewall & VPN**

Monitoring | **Schwachstellen** | **Backup** | **Hypervisor**

GRC | **Captive-Portal** | **Automatisierung** | **OTP / 2FA**

Stronghold | **codPass** | **Integrationen** | **Plattform**

Das Herzstück: eine Plattform, die zusammenwächst

Multi-Mandanten & Rollen

Mehrere Kunden, Standorte oder Abteilungen in einer Plattform. Feingranulare Rollen- und Gruppenverwaltung mit Anbindung an LDAP/Active Directory oder an lokale Benutzer.

Zentrale Suche: First-Level-Support in Sekunden

Meldet ein Anwender ein Problem, sieht der Support sofort: Wo steht das Gerät? An welchem Switch und Port hängt es? Wie ist der Monitoring-Status? Wer ist zuständig? Gesucht wird über MAC, IP, Standort oder Name.

Zentrales Assetmanagement

Die automatisch gepflegte Grundlage für alle weiteren Module, statt händischer Listen mit Stand von gestern.

Die Module im Detail

Netzwerk & Asset-Management

Findet automatisch jedes IP-adressierbare Gerät, von IT bis OT, mit Live-Polling-Status je Gerät (SNMP/SSH/API). Dazu ein Asset-Workspace je Gerät, Räume/Racks mit Rack-Elevation, Layer-2-/Layer-3-Routing-Topologie und eine globale Suche über die gesamte Infrastruktur.

NAC & eigene PKI

802.1x- und MAC-Authentifizierung steuern Sie direkt im Browser, performant bis in den Millionenbereich. Inklusive eigener Certificate Authority (RSA/ECDSA/EdDSA), Client-Zertifikaten, CRLs und PKCS#12-Export, synchron mit FreeRADIUS.

TACACS+: Netzwerk-AAA

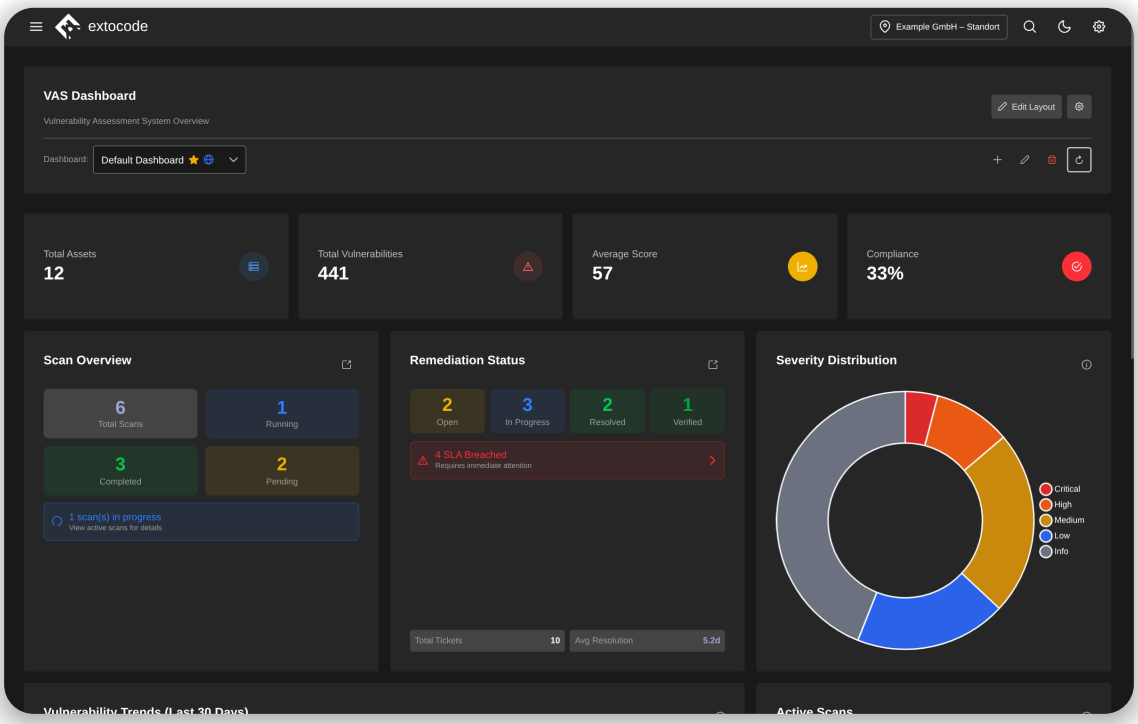
Zentrale Verwaltung des hauseigenen TACACS+-Servers nach **RFC 8907**: Nutzer, NAS-Clients, Autorisierungsregeln mit Rollen und Command-Sets, ein Rollen-Simulator zur Live-Policy-Auswertung und Accounting mit Live-Log.

Firewall & VPN

Herstellerübergreifendes Management von **AIMdefense, OPNsense, pfSense und Dyn-Fi**: zentrale Updates, Alias- und Zonen-Verwaltung, Zertifikatsüberwachung, Erreichbarkeitsüberwachung je Firewall (ICMP/TCP, E-Mail bei Ausfall) und SSH-Terminal im Browser. VPN-Verwaltung für WireGuard, OpenVPN und IPsec mit Verbindungs-Statusanzeige.

GRC: Governance, Risk & Compliance

Eine GRC-Plattform für mehrere Normen auf einer Datenbasis: versionierter Multi-Norm-Katalog (**ISO 27001, ISO 27002, ISO 9001, ISO 22301** und **BSI 200-3**, dazu **NIS2-Readiness**), Statement of Applicability, asset-basierte Risikobewertung nach BSI 200-3, Vorgänge/Incidents mit SLA, Dokumentenlenkung mit Freigabe-Workflow und append-only Audit-Log (per DB-Trigger gegen nachträgliches Ändern/Löschen geschützt).



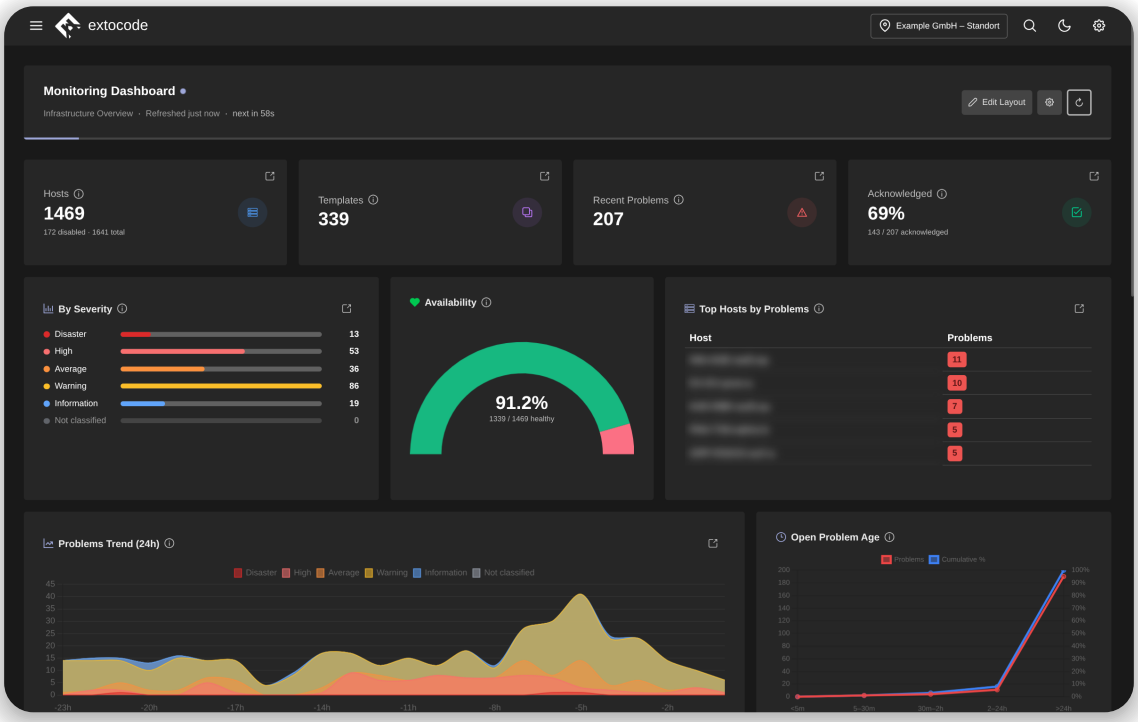
Schwachstellen-Management (in Vorbereitung): geplante Scan-Übersicht mit Remediation-Status und Severity-Verteilung, hier mit Beispieldaten.

Schwachstellen-Management (VAS)

Bringt Schwachstellen aus dem Netz in einen priorisierten Überblick, mit Remediation-Status, Severity-Verteilung und Trend. So gilt zuerst, was wirklich gefährlich ist, statt Listen ohne Kontext. *In Vorbereitung.*

Monitoring: Zabbix-Integration

Bindet Ihren (kunden-eigenen) Zabbix-Server in COD ein: konfigurierbares Dashboard, Verfügbarkeit und Probleme nach Schweregrad, Monitoring direkt am Asset. COD liest die Daten und quittiert Probleme (Acknowledge). Die Alarmierung selbst bleibt bei Zabbix.



Monitoring-Dashboard: Verfügbarkeit, offene Probleme nach Schweregrad und Verlauf der letzten 24 Stunden.

Backup

Sichert Netzwerk-, Embedded- und Linux/BSD-Systeme inklusive Konfigurationsvergleich, der jede Änderung sichtbar macht.

Hypervisor

Zentrale vSwitch Netzwerkverwaltung mit Netzwerkprofilen Ihrer VMware Umgebung.

OTP / Zwei-Faktor

Zentrale Verwaltung zeit- und ereignisbasierter Einmalpasswörter (TOTP/HOTP) für den COD-Login. Die OTP-Verwaltung wandert in Stronghold: Bestehende Token werden automatisch migriert, das Modul läuft übergangsweise als Fallback weiter.

Captive-Portal

Kontrollierter Gast- und Geräte-Zugang über ein anpassbares Onboarding-Portal.

Automatisierung

Wiederkehrende Pflichtaufgaben laufen automatisiert, etwa die tägliche Anlage von Maßnahmen für fällige Dokumentenprüfungen. Netzwerkaktionen fährt COD über eine interne Ansible-Runner-Engine.

Secrets-Management: Stronghold & codPass

Stronghold: Zero-Knowledge-Tresor

Neu in COD 3.6 und produktiv ausgeliefert: Ende-zu-Ende-verschlüsselter Passwort- und Secrets-Tresor direkt in COD (Argon2id / X25519 / AES-GCM): persönliche und geteilte Team-Tresore, gezielte Freigaben und eine Browser-Extension für Chrome und Firefox. Der integrierte Authenticator übernimmt zudem TOTP/HOTP-Codes.

codPass

Eigenständiger, quelloffener Passwort- und Secrets-Manager (`github.com/extocode/codpass`). On-premise, volle Datenhoheit, unabhängig von COD.

Herstellerübergreifend: Connect-Integrationen

COD spricht mit Ihren bestehenden Systemen, statt sie zu ersetzen:

Zabbix • i-doit • {php}IPAM • baramundi • RADIUS Server

Architektur & Betrieb

- **On-Premise oder Cloud**: volle Datenkontrolle, KRITIS-tauglich. Vorlagen-Updates (ISO-Controls, BSI-Katalog) lassen sich kontrolliert einspielen.
- **Moderne Architektur**: Angular 21 (zoneless, Signals), Prisma, Nx-Monorepo. Sensible Felder (Passwörter, SNMP-Communitys) sind standardmäßig aus Queries ausgeschlossen.
- **Rollenmodell**: Manager » SuperAdmin » Admin, durchgängig mandantenfähig.
- **White-Label**: App-Name, Logo und Farben ohne eine Zeile Code anpassbar.

Sehen Sie COD in Aktion.
Wir zeigen die Plattform praxisnah in Ihrer Umgebung, ohne Vertriebsdruck und ohne Verpflichtung.

extoco.de • extocode GmbH