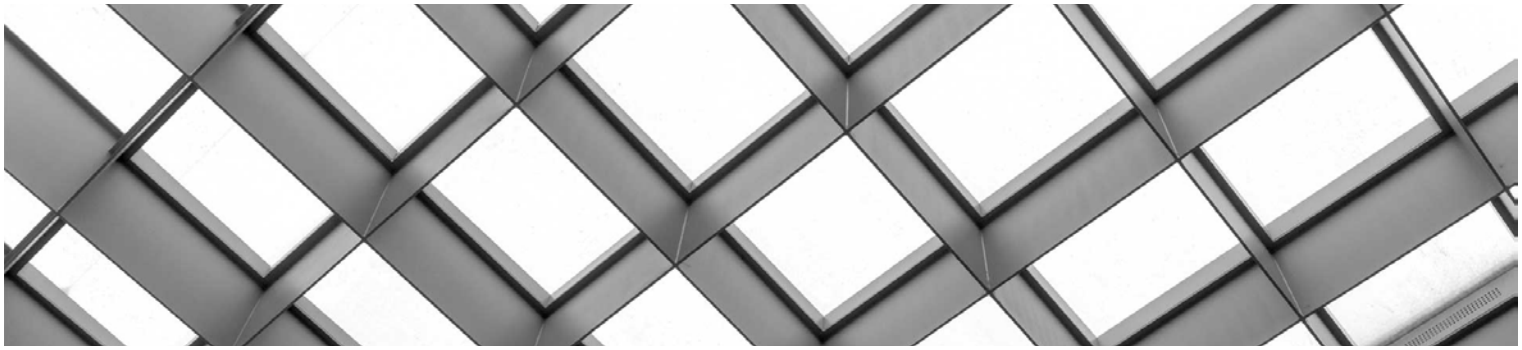
Service

Security Operations

CERUNO

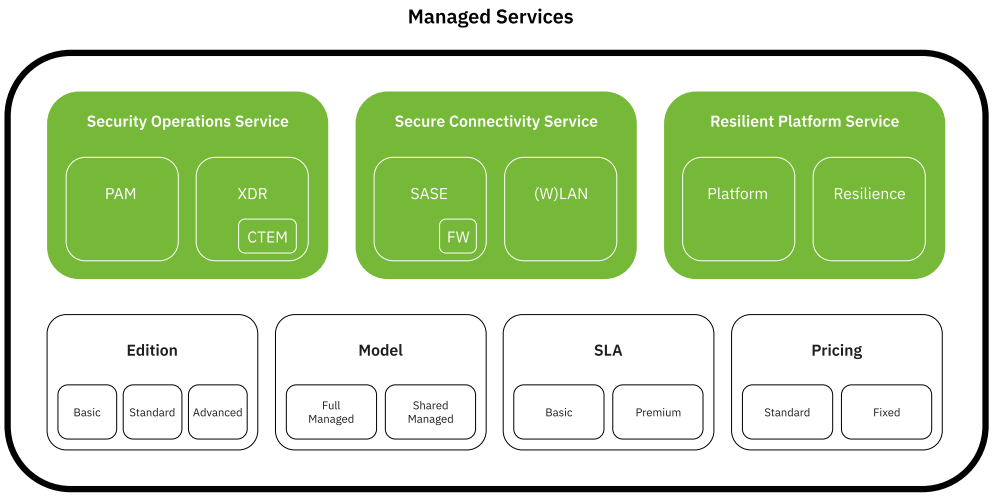


Unternehmenswerte schützen. *Sicher und flexibel.*

Wir schaffen eine maximale **Visibilität** über die gesamte digitale Landschaft, um Gefahren frühzeitig zu erkennen. Durch KI-gestützte **Automatisierung** und radikale **Einfachheit** in den Prozessen minimieren wir den Betriebsaufwand. So wandeln wir Komplexität in **Sicherheit** und ermöglichen es unserem Unternehmen, sich agil und geschützt auf das Kerngeschäft zu fokussieren.

Unser Fundament bildet ein konsequenter **Zero Trust** Ansatz: Wir schützen **Identitäten** als neuen Perimeter, härten sämtliche **Endpoints** und isolieren kritische Assets durch intelligente **Segmentierung**. Statt in einer Flut isolierter Tools den Überblick zu verlieren, setzen wir auf **Extended Detection & Response (XDR)**. Diese Plattform-Strategie bündelt unsere Abwehr, schafft **Synergien** und garantiert eine nahtlose, reaktionsschnelle Verteidigungsarchitektur.

Diese technologische Basis ist das Fundament – doch erst die kontinuierliche Überwachung macht sie wirksam. Mit unserem **Security Operations Service** übernehmen wir Ihre Verteidigung, damit Ihre IT-Ressourcen dort bleiben, wo sie den grössten Wert stiften: In Ihrer Innovation.



Kunden

- … minimieren ihr Cyber-Risiko signifikant, da Angriffe durch KI-gestützte Analysen in Echtzeit erkannt und durch Automation sofort gestoppt werden.
- … schliessen die Lücke im Identitätsschutz, indem sie den Zugriff auf kritische Ressourcen durch Identitäts-Härtung und moderne Vaulting-Lösungen absichern.
- … entlasten ihre IT-Ressourcen, da unser Expertenteam die Flut an Sicherheitsmeldungen filtert, priorisiert und nur bei relevanten Vorfällen gezielt unterstützt.
- … erfüllen Compliance- und Audit-Anforderungen, dank lückenloser Protokollierung, sicherem Privileged Access Management und transparentem Reporting.

Module

Managed XDR

Unser Managed XDR (Extended Detection and Response) Modul bildet das Gehirn Ihrer Cyber-Abwehr. Wir führen Sicherheitsdaten aus verschiedenen Quellen zusammen, um komplexe Angriffsketten sichtbar zu machen. Durch den Einsatz einer führenden KI-Plattform ermöglichen wir eine autonome Erkennung und Reaktion auf Endpunkten, in der Cloud und im Netzwerk.

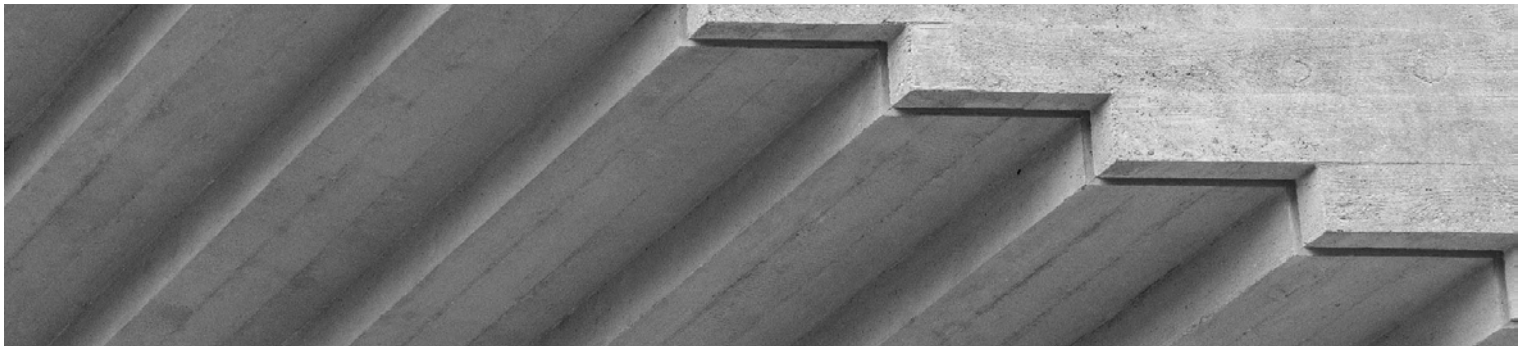
- Detection & Response für Endpoint, Identities & Cloud
- Exposure Management mit Network Discovery, Vulnerability Management sowie Best Practices für Active Directory und Entra ID
- Threat Intelligence und Forensik
- Hochperformanter und offener Telemetrie- und Log-Datenspeicher zur Einbindung weiterer Quellen - auch mit Langzeitspeicherung
- Strategische Unterstützung zur Weiterentwicklung des Sicherheitsdispositiv

Module

Managed PAM

Unser Managed PAM (Privileged Access Management) Modul schützt die kritischsten Identitäten Ihres Unternehmens, egal ob persönlich oder unpersönlich. Die zentral verwaltete, in das Modul Managed XDR integrierte Plattform stellt Privileged Access Management sowie einen VPN-losen Remote-Zugriff bereit. So wird der Zugriff auf Server, Applikationen und Infrastruktur für interne Administratoren ebenso wie für externe Partner sicher gesteuert, überwacht und lückenlos protokolliert.

- Passwort- und Credential-Management
- Just-in-Time (JIT) & rollenbasierte Zugriffskontrolle (RBAC)
- Kontrollierter Zugriff auf Infrastruktur inkl. Datenbanken
- Gesicherter Fern- und Drittanbieterzugriff
- Sitzungsüberwachung & -aufzeichnung
- Compliance & Audit-Fähigkeiten zur Erfüllung regulatorischer Anforderungen.

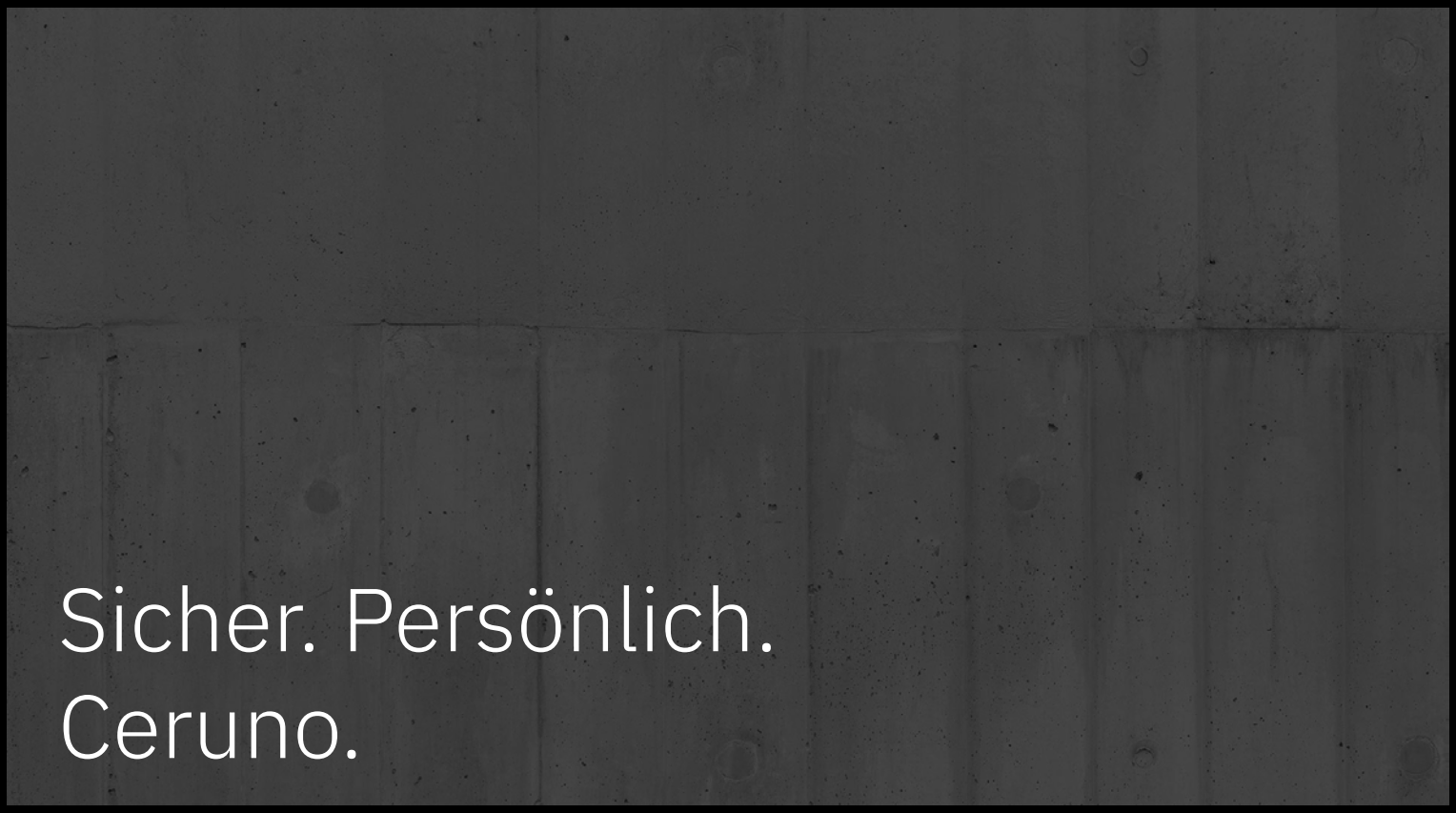


Betriebsmodelle

Wir bieten eine lückenlose Sicherheitsüberwachung, standardisierte Incident-Response-Prozesse sowie regelmässige Security-Audits und Reports. Unser Team fungiert als verlängerter Arm Ihrer IT-Sicherheit.

Shared Managed Model
Beim Shared Managed Model liegt der Fokus auf der technologischen Unterstützung und der Alarmierung. Während wir die Plattformen verwalten und kritische Alarme priorisieren, übernimmt das IT-Team des Kunden die finale Entscheidung oder Durchführung lokaler Anpassungen.

Full Managed Model
Im Full Managed Model übernehmen wir die volle Verantwortung für Ihre Security Operations. Dies umfasst das aktive Threat Hunting, die vollständige Bearbeitung von Incidents (Response), das Management der Identitäts-Policies sowie die kontinuierliche Optimierung der Sicherheits-Posture. Der Kunde erhält maximale Sicherheit bei minimalem eigenem Aufwand.



Sicher. Persönlich.
Ceruno.

Hauptsitz
Ceruno AG
Rosenbergstrasse 93
9000 St. Gallen

Chur
Hartbertstrasse 10
7000 Chur

Triesen
Landstrasse 123
9495 Triesen

+41 58 733 01 01
info@ceruno.ch
ceruno.ch

CERUNO