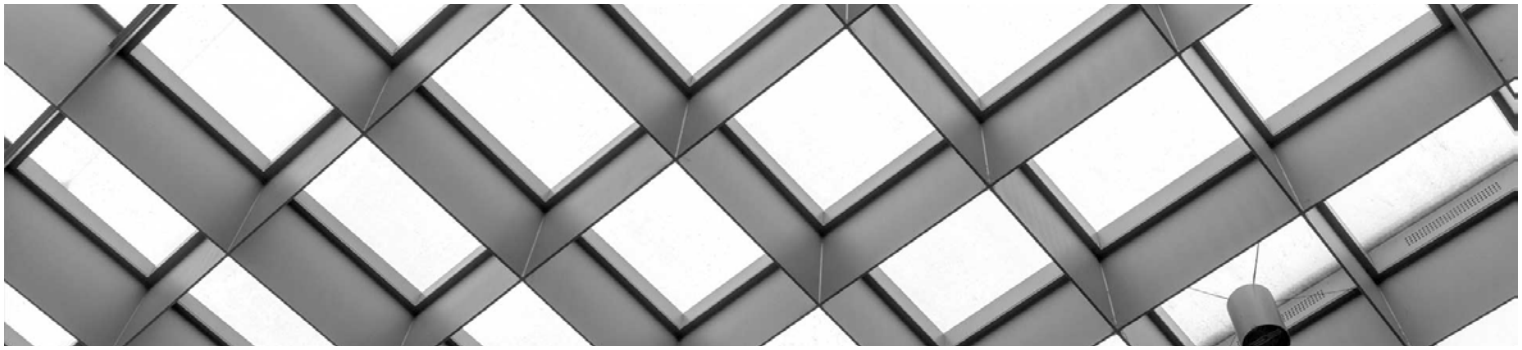

Modul

# Managed XDR

CERUNO



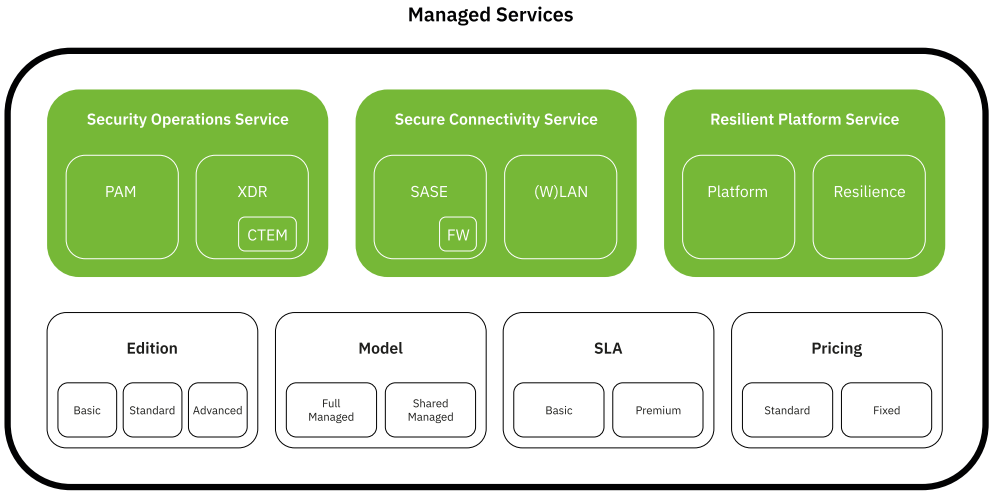
# Beschreibung

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.

Wählen Sie aus drei Editionen: **Basic, Standard** oder **Advanced**. Während Basic eine solide Grundlage mit reduziertem Identitätsschutz bietet, erweitert Advanced den Schutz durch Threat Hunting & Intelligence und Forensik-Funktionen, um selbst anspruchsvollste Sicherheitsanforderungen zu erfüllen. Das reicht nicht? Fordern Sie eine individuelle Variante an.

Mit unserem flexiblen **Shared Managed Model** unterstützen wir gezielt in einzelnen Bereichen, während das **Full Managed Model** den kompletten Betrieb in unsere erfahrenen Hände legt. Unsere **SLA-Optionen – 8x5** oder **24x7** – garantieren dabei schnelle Unterstützung und zuverlässige Reaktionszeiten, wann immer Sie uns brauchen.

Setzen Sie auf einen Service, der Ihre Sicherheit in den Fokus stellt – individuell, skalierbar und effizient!



# Umfang

- 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

# Leistungen

- Lifecycle mit Renewalprozess und Lizenzmanagement
- Agentüberwachung hinsichtlich Abdeckung, Versionen und Funktionskontrolle
- Best Practices für Policies, Exclusions, Blacklists, Netzwerk- und Gerätekontrolle (USB, Bluetooth), etc.
- Lifecycle zur Reduzierung der Vulnerabilities und Misconfigurations
- Dashboards, KPI’s und regelmässige Report
- Incident Response

# Funktionen

| | |
|---|---|
| **AI Assistant** | Nutzt als Foundations generative KI zur Alarmzusammenfassung oder Suche in Telemetriedaten in natürlicher Sprache. Als SOC Analyst bietet er Unterstützung in der Triage und erweiterten Nachforschungen. |
| **Cloud Native Security** | Scannt Ihre Cloud Umgebung, gibt Ihnen einen Überblick über die vorhandenen Assets und bewertet diese nach den gängigen Compliance Frameworks wie SOC2. Erkennt Angriffe in Echtzeit durch die Offensive Security Engine. |
| **Data Lake** | Ermöglicht die Speicherung, Korrelation und Angriffserkennung zusätzlicher Log-Daten, direkt aus dem Marketplace oder über eigene Integrationen. 10 GB pro Tag sind bereits enthalten. |
| **Data Retention** | Daten für Incidents werden standardmässig ein Jahr aufbewahrt. Darüber hinaus können die Rohdaten der Endpunkte und Log-Daten im Data Lake für verschiedene Zeiträume aufbewahrt werden. Standardmässig sind 14 Tage enthalten. |
| **Detection Rules** | Über 1500 vorgefertigte Detection Rules und die Möglichkeit diese anzupassen oder eigene zu erstellen ermöglichen umfassende Erkennung über den Endpunkt hinaus. |
| **Endpoint Detection & Response** | Verhaltensbasierter Echtzeitschutz für Ihre Endpunkte mit kompletter Visibilität und granularen Wiederherstellungsoptionen. Zusätzliche Kontrolle über angeschlossene Geräte per USB, Bluetooth und Thunderbolt als auch der lokalen Firewall. |
| **Forensics** | Forensische Artefakte werden manuell oder automatisiert von Ihren Endpunkten extrahiert. Die Resultate können ihm Data Lake oder auch in Tools von Drittanbietern untersucht werden. |
| **Hyperautomation** | Mit No- und Low-Code Workflows werden weitere Schritte automatisiert. Auf der eigenen Plattform oder über API auf anderen Plattformen. |
| **Identity Detection & Response** | Erkennt laufende Identitätsangriffe auf Domänencontroller und Endgeräte, die von verwalteten oder nicht verwalteten Geräten mit beliebigem Betriebssystem ausgehen, und blockiert den Fortschritt des Angreifers, bevor er Privilegien erlangt. Scannt zusätzlich nach kompromittierten Accounts. |
| **Identity Security Posture Management** | Scannt Ihre Active Directory als auch Ihre Entra ID und gibt Ihnen einen Überblick über Angriffsvektoren anhand von Best Practices. Unterstützt bei der Behebung von Fehlkonfigurationen und erkennt einfache Angriffe. |
| **Threat Hunting & Intelligence** | Sämtliche Indicator of Compromise wie IP-Adresse oder Datei-Hash werden direkt mit dem Threat Intelligence Feed von Mandiant abgeglichen und die Findings entsprechend ergänzt. Zudem sucht ein spezialisiertes Team von SentinelOne in Ihrem System regelmässig nach aktuellen Threats. |
| **Vulnerability Management & Network Discovery** | Scannt Ihr Netzwerk und Ihre Endpoints und gibt Ihnen einen Überblick über die im Unternehmen vorhandenen Systeme und Applikationen. Zeigt ungeschützte Geräte als auch Software Vulnerabilities auf Betriebssystem- und Applikationsebene auf und ermöglicht deren Bearbeitung. |

# Service Katalog

| Edition | Basic | Standard | Advanced |
|---|---|---|---|
| **Feature** | | | |
| Endpoint Detection & Response | ■ | ■ | ■ |
| Identity Security Posture Management | ■ | ■ | ■ |
| Vulnerability Management & Network Discovery | ■ | ■ | ■ |
| AI Assistant | ■ | ■ | ■ |
| AI SIEM[1] | | ■ | ■ |
| Identity Detection & Response | | ■ | ■ |
| Threat Hunting & Intelligence | | | ■ |
| Forensics | | | ■ |

| Model | Full Managed | Shared Managed |
|---|---|---|
| **Incident Response** | | |
| Handlungsempfehlung (Unresolved >~ 4h) [2] | | ■ |
| Bearbeitung auf Kundenwunsch [3] | | ■ |
| Automatische Bearbeitung durch Engineer | ■ | |
| **Housekeeping** | | |
| Exclusions Management | ■ | |
| Agent Upgrades | ■ | |

[1] Data Lake, Detection Rules & Hyperautomation

[2] Erfolgt innert zwei Arbeitstagen keine Rückmeldung durch den Kunden, wird der Incident durch das CCSC bearbeitet und nach den Standard-Stundensätzen verrechnet.

[3] Die Verrechnung der anfallenden Stunden erfolgt nach den Standard-Stundensätzen.

# Service Katalog

| SLA | Basic | Premium |
|---|---|---|
| **Service Zeiten** | **8x5** | **24x7** |
| **Alarmierung (Monitoring)** [4] | | |
| Mo – Fr / 8:00 – 12:00 & 13:00 – 17:00 | ■ | |
| Mo – So / 24h | | ■ |
| **Rufbereitschaft** | | |
| Mo – Fr / 8:00 – 12:00 & 13:00 – 17:00 | ■ | |
| Mo – So / 24h | | ■ |
| **Reaktionszeit während Rufbereitschaft** [5] | | |
| 4h | ■ | |
| 1h | | ■ |

[4] Die Alarmierung kann ausserhalb der Arbeitszeiten nur erfolgen, wenn der Kunde ebenfalls eine 24x7 Organisation hat.

[5] Die Reaktionszeit misst die Zeit zwischen dem Eingang des Kundenanrufes an die Hotline der Ceruno und dem Rückruf des verantwortlichen Engineers bzw. die Zeit zwischen der automatischen Eröffnung bzw. Eskalation eines potentiell sicherheitskritischen Tickets durch das CCSC und der Erstbeurteilung durch den verantwortlichen Engineer.

# Service Katalog

| Pricing | Standard | Fixed |
|---|---|---|
| Onboarding | Projektpreis | Projektpreis |
| Lizenzen | | |
| Plattform- und Servicebetrieb | | |
| Alert Handling | nach Aufwand | |

**Abgrenzungen**

Wird die enthaltene Lizenzmenge dauerhaft um mehr als 5% oder 100 Endpoints überschritten wird der Service angepasst.

# Optionen

- Cloud Native Security
- Zusätzliche Data Retention: ab 30 Tagen
- Data Lake: GB pro Tag

**Release Notes**

**v2026.06**

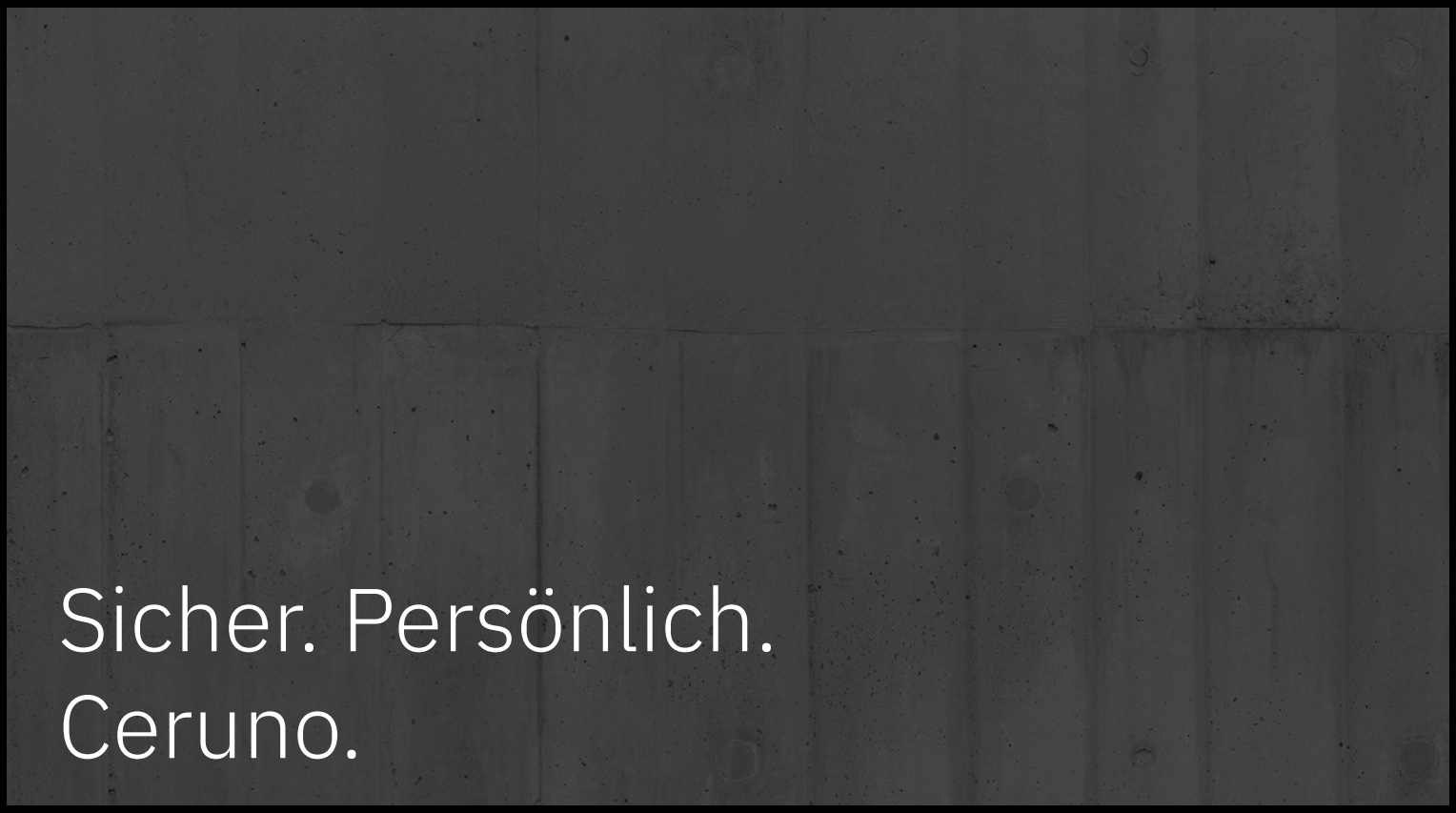
- Anpassung an neue Service Struktur

**v2025.08**

- Aufnahme von neuen Funktionen
- Präzisierung der Erreichbarkeit bzw. Bürozeiten
- Vereinheitlichung der Formulierung (Erreichbarkeit → Rufbereitschaft)
- Präzisierung der Reaktionszeit

**v2024.11**

- Initial Release



# 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