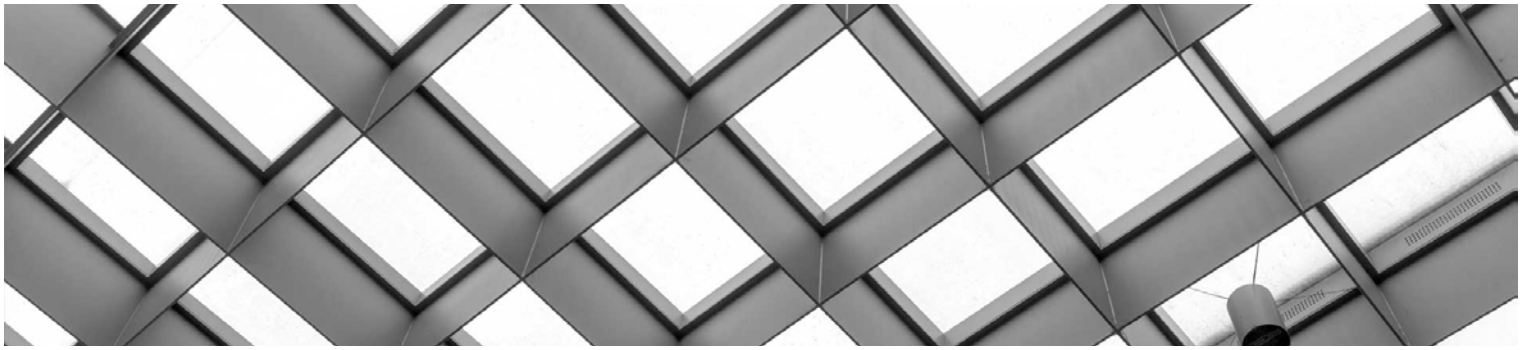
Modul

Managed CTEM

CERUNO



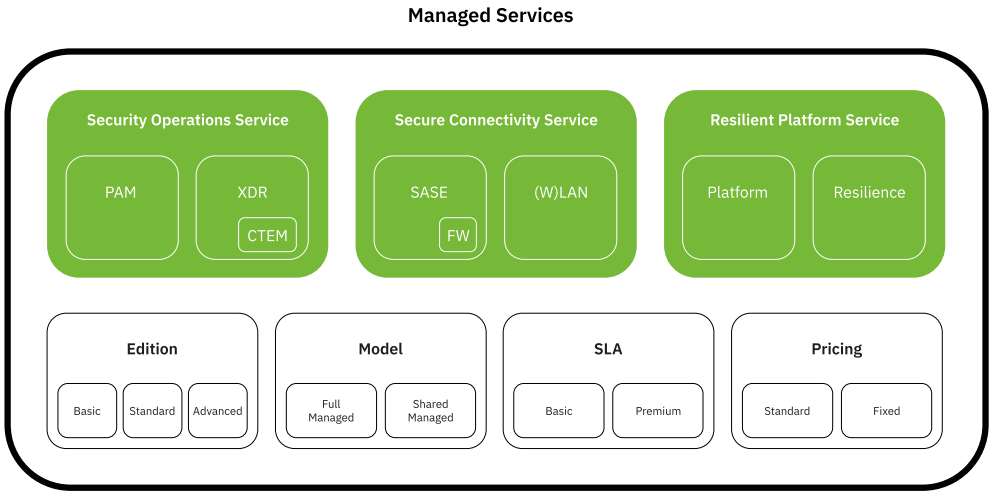
Beschreibung

Unser Managed CTEM (Continuous Threat Exposure Management) Modul bietet einen modernen, ganzheitlichen Ansatz zur Sicherung Ihrer digitalen Infrastruktur, der weit über das klassische Schwachstellenmanagement hinausgeht.
In einem kontinuierlichen Zyklus (Scoping, Discovery, Prioritization, Validation und Mobilization) schaffen wir vollständige Transparenz über Ihre Angriffsfläche. Wir identifizieren externe Assets wie IP-Adressen, Domains, Subdomains, Zertifikate und exponierte Services, prüfen diese laufend auf Schwachstellen, Fehlkonfigurationen und unnötige Exponierung und unterstützen bei der Priorisierung der Behebung.

Der Service konzentriert sich bewusst auf Exposure Management von aussen: also auf die Erkennung und Bewertung öffentlich erreichbarer Systeme und Dienste. Im Unterschied zu internen Vulnerability-Scans oder agentenbasierten Lösungen erfolgt die Sicht auf Ihre Umgebung aus externer Perspektive – so, wie sie auch für potenzielle Angreifer sichtbar ist. Internes Scanning ist dennoch als zusätzliche Optionen möglich.

Mit unserem flexiblen **Shared Managed Model** unterstützen wir Sie gezielt bei der Bewertung und Priorisierung, während das **Full Managed Model** den gesamten operativen CTEM-Zyklus in unsere erfahrenen Hände legt.

Setzen Sie auf einen Service, der blinde Flecken eliminiert und Ihre Cyber-Resilienz durch kontinuierliche Validierung und Anpassung an die aktuelle Bedrohungslage nachhaltig stärkt.



Umfang

- Identifikation von Domains, Subdomains, IP-Adressen, Zertifikaten und öffentlich erreichbaren Services (Scoping)
- Kontinuierliche Angriffsflächenanalyse, Vulnerability und Web App Scanning (Discovery)
- Risikobasierte Priorisierung der Findings nach Kritikalität und Exponierung (Prioritization)
- Validierung der Findings und prüfen möglicher Massnahmen, Attack Path Analysis (Validation)
- Reporting und Unterstützung bei der Umsetzung der Massnahmen (Mobilization)

Leistungen

- Lifecycle mit Renewalprozess und Lizenzmanagement
- Onboarding und Initial-Abgleich der zu überwachenden Scopes mit Domains, IP-Ranges, etc.
- Laufende Überwachung der externen Assets und Scan-Abdeckung
- Priorisierung nach Kritikalität, Erreichbarkeit und Angriffsrelevanz
- Dashboards, KPI’s und regelmässige Reports
- Benachrichtigung bei kritischen Exposures und schwerwiegenden Schwachstellen
- Unterstützung bei Handlungsempfehlungen und bei der Nachverfolgung von Remediation-Massnahmen

Funktionen

External Attack Surface Monitoring	Erkennt internet-exponierte Assets und deren Ports, Dienste und Technologien und führt diese in einem konsolidierten Überblick zusammen.
External Vulnerability Scanning	Prüft öffentlich erreichbare Assets regelmässig auf bekannte Schwachstellen, veraltete Softwarestände und sicherheitsrelevante Konfigurationsmängel (nicht authentisiert).
Certificate & Domain Monitoring	Überwacht Zertifikate und domänenbezogene Informationen, um ablaufende Zertifikate, unerwartete Veränderungen oder zusätzliche, bisher unbekannte externe Präsenz frühzeitig sichtbar zu machen.
Risk-Based Prioritization	Bewertet Findings nach Schweregrad, Exponierung, Ausnutzbarkeit und betroffener Angriffsfläche, damit die Bearbeitung auf die wichtigsten Risiken fokussiert werden kann.
Reporting & Remediation Tracking	Stellt die Ergebnisse in Dashboards und Reports bereit und unterstützt bei der Nachverfolgung offener Risiken und vereinbarter Massnahmen.
Advanced Web App Scanning	Exponierte Web Applikationen werden mit authentisierten Scans detailierter und mit spezifischen Scanner-Vorlagen gezielt nach gewünschten Kriterien gescannt (Compliance, APIs, TLS, etc.).
Exposure Management & Attack Path Analysis	Schafft eine ganzheitliche Übersicht über das komplette Inventar, zeigt die Risiken und erstellt automatisch Attack-Path Analysen, gekoppelt an das MITRE ATT&CK™ Framework.
Internes Vulnerability Scanning	Interne Systeme werden mittels authentisierter und nicht authentisierter Nessus-Scans kontinuierlich auf Schwachstellen, Fehlkonfigurationen und fehlende Sicherheitsupdates überprüft.
OT Security	Industrielle Netzwerke und OT-Systeme werden kontinuierlich überwacht, um Anlagen, Steuerungssysteme und industrielle Geräte zu inventarisieren sowie Schwachstellen und Fehlkonfigurationen frühzeitig zu erkennen.

Service Katalog

Edition	Standard	Advanced
Feature		
External Attack Surface Monitoring	■	■
External Vulnerability Scanning	■	■
Certificate & Domain Monitoring	■	■
Risk-Based Prioritization	■	■
Remediation Tracking	■	■
Reporting	■	■
Advanced Web App Scanning		■
Exposure Management		■
Attack Path Analysis		■

Model	Full Managed	Shared Managed
Betrieb		
Durchführung und Überwachung der Scans	Ceruno AG	Ceruno AG
Pflege des Service Scopes	Ceruno AG	Gemeinsam
Review neuer externer Assets	Ceruno AG	Gemeinsam
Triage und Priorisierung der Findings	Ceruno AG	Kunde
Scan-Tuning	Ceruno AG	Kunde
Remediation Koordination und Nachverfolgung	Ceruno AG	Kunde
Umsetzung technischer Behebungen	Kunde	Kunde

Service Katalog

SLA	Basic
Service Zeiten	**8x5**
Alarmierung (Monitoring)	
Mo – Fr / 8:00 – 12:00 & 13:00 – 17:00	
Rufbereitschaft	
Mo – Fr / 8:00 – 12:00 & 13:00 – 17:00	
Reaktionszeit während Rufbereitschaft [1]	
4h	

[1] 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
Onboarding	Projektpreis
Lizenzen	
Plattform- und Servicebetrieb	
Finding Triage & Scan-Tuning	nach Aufwand

Abgrenzungen

- Der Service fokussiert auf **extern erreichbare** Assets und Risiken. Interne Netzwerkscans und agentenbasierte Endpoint-Analysen sind optionale Features.
- Die Behebung von Schwachstellen und Fehlkonfigurationen auf Zielsystemen erfolgt grundsätzlich durch den Kunden oder durch separate Umsetzungsleistungen.

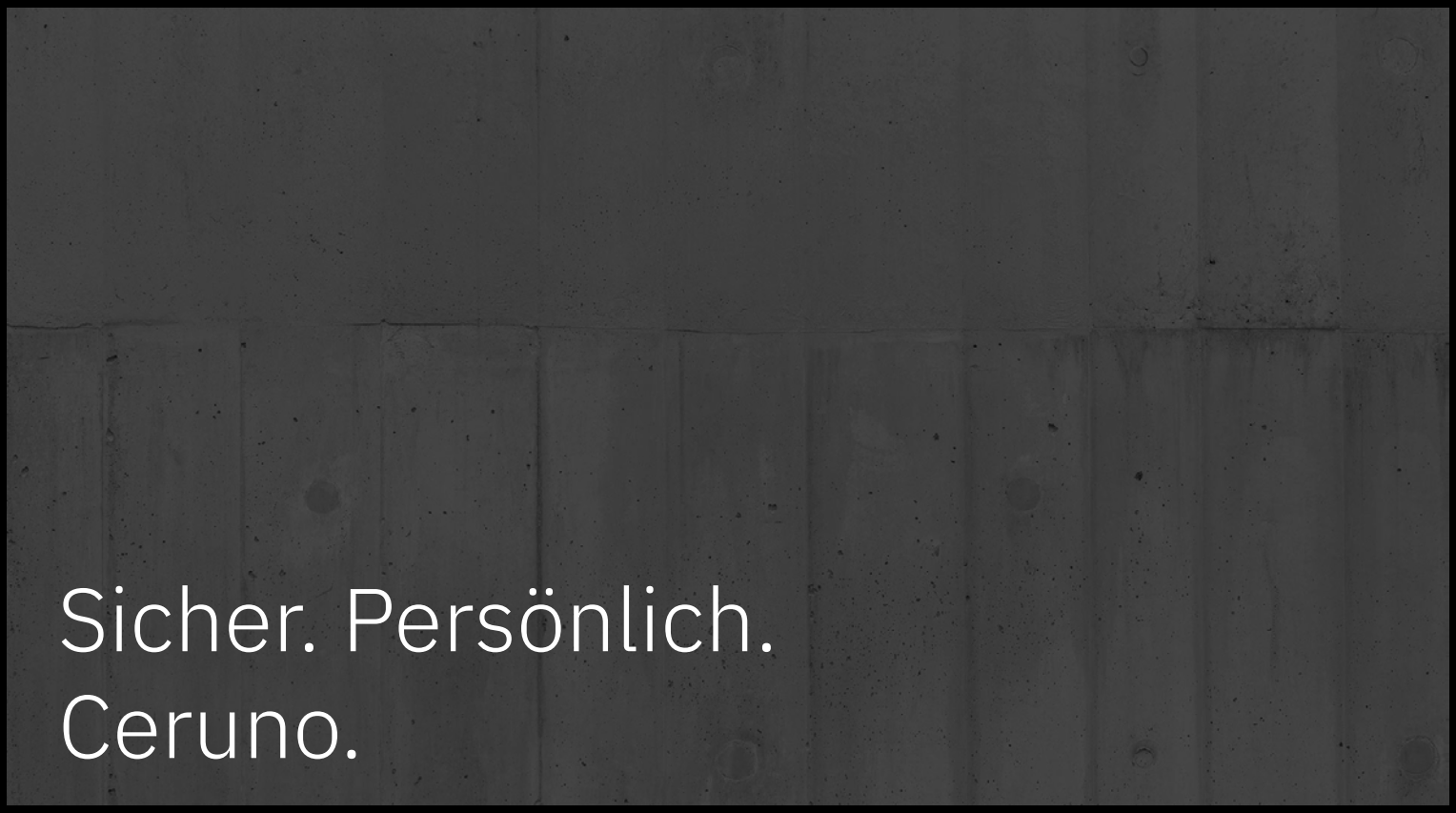
Optionen

- Internes Vulnerability Scanning
- OT Security

Release Notes

v2026.07

- 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