



***Cyber Defense Center
(CDC)***

K-Businesscom Security Strategy



Aufdecken von Schwachstellen sowie Ablauf- und Struktur- problemen

Security Audit und Red Teaming
Information Security
Management
Risikomanagement
Architektur-Reviews

Konkrete Leistungen, die nach einem Angriff wichtig werden

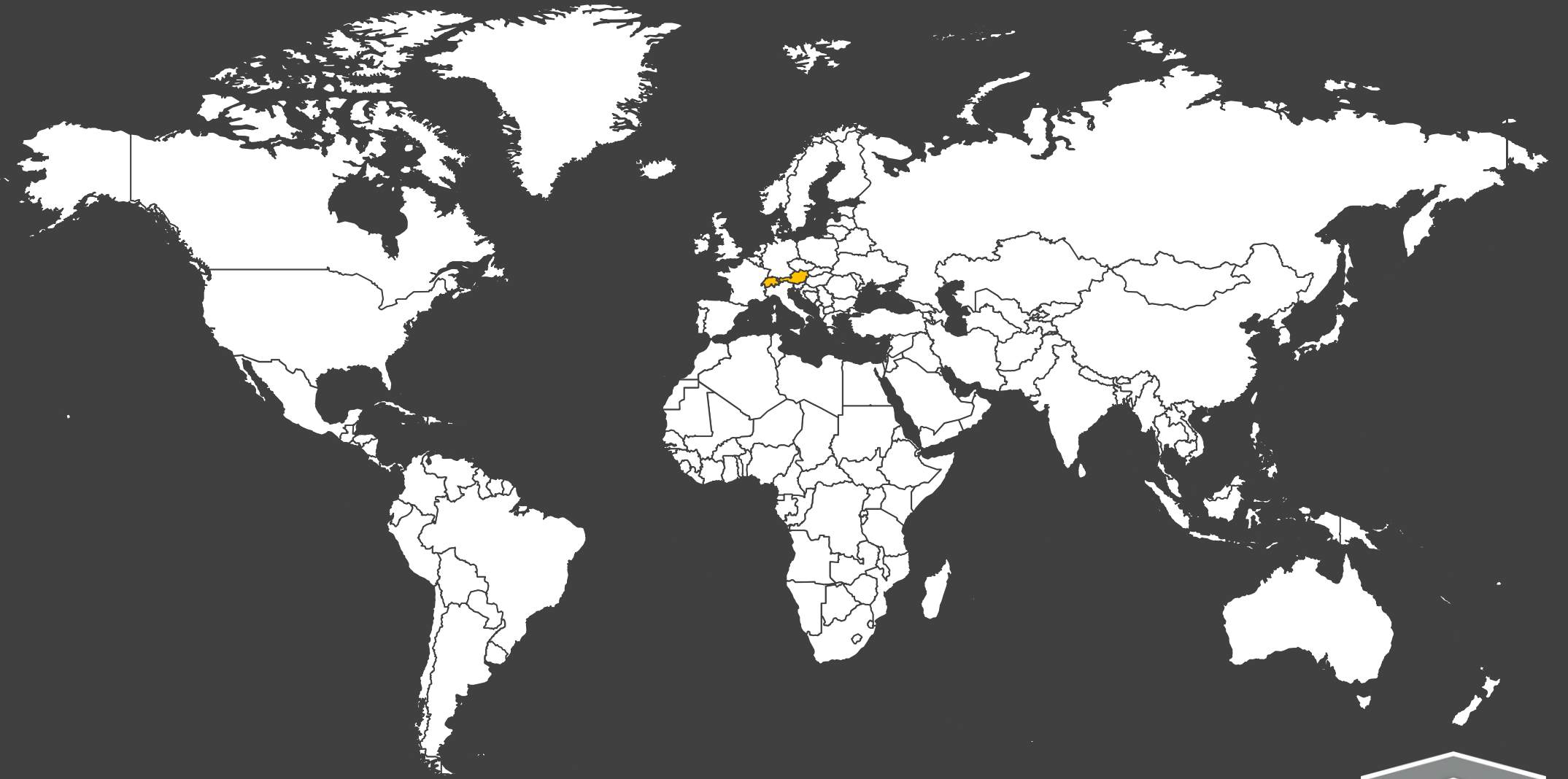
Incident Response
Forensische Analyse
Incident Response Manager/
Vorfallbegleitung
PURPLE Teaming

Die Klassiker unter den Security- Lösungen, von der Firewall bis zur Encryption

Network Security
Endpoint Security
Cloud Security
Content Security

Erkennen von vorhandenen Systeminfektionen

Security Operations Center
Vulnerability Management
Managed SIEM
Endpoint Detection and Response
Threat Intelligence/Brand and
Credential Monitoring



Ein Österreichisches Service für den weltweiten Einsatz

Uns vertrauen mehr als 50 Kunden auf 4 Kontinenten und in 45 Ländern



CDC Module

Network Security Monitoring (NSM)

Netzwerkverkehr aufzeichnen
automatisierte und manuelle Analyse
Anomalieerkennung
Netzwerkforensik

Log Analyse (LOG)

Log Aggregation und Auswertung
Statistische Analysen
Daten Korrelierung

Threat Intelligence (TI)

Threat Landscape
Threat Actor & Campaign Tracking
Brand & Credential Monitoring

Endpoint Detection & Response (EDR)

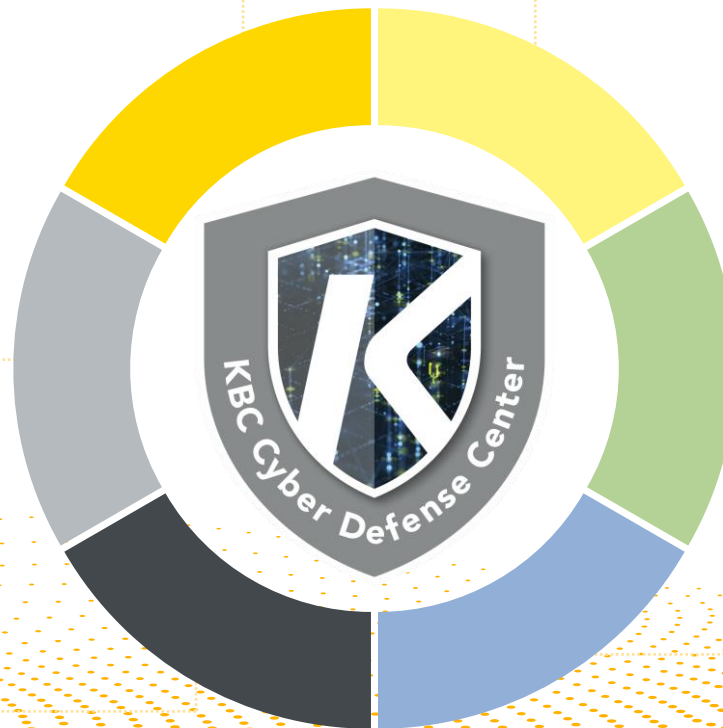
Endpoint Visibility
Live Remote Analyse
Remote Datensammlung
Endpoint Isolierung

Vulnerability Management (VULN)

Asset Discovery
Reporting von Schwachstellen
Proaktive Nachverfolgung
Anreicherung durch Threat Intelligence

Operational Technology Monitoring (OTM)

Spezialisierung auf OT Geräte und Protokolle
kontinuierliche Überwachung
Übersicht über Assets und Kommunikationsflüsse
Erkennung von Angriffen und Schwachstellen





Contact Us

<https://cdc.k-business.com/>