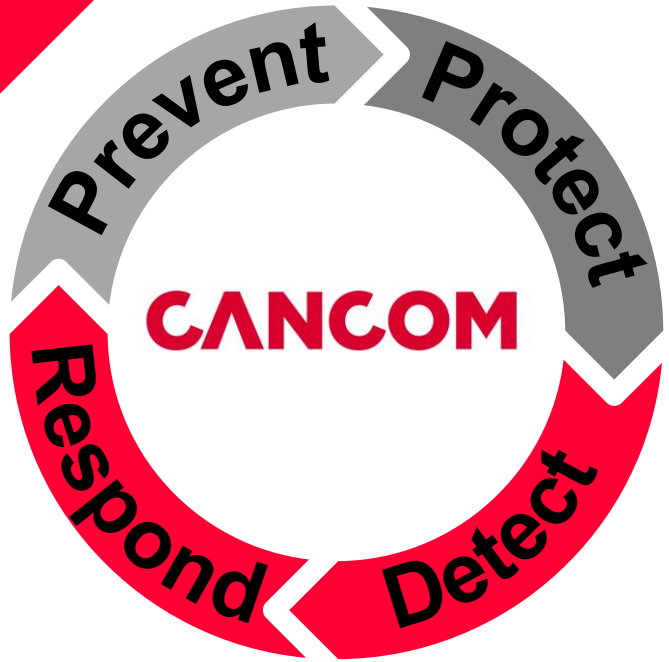
DETECT & RESPOND

Managed CDC & Incident Response



CANCOM

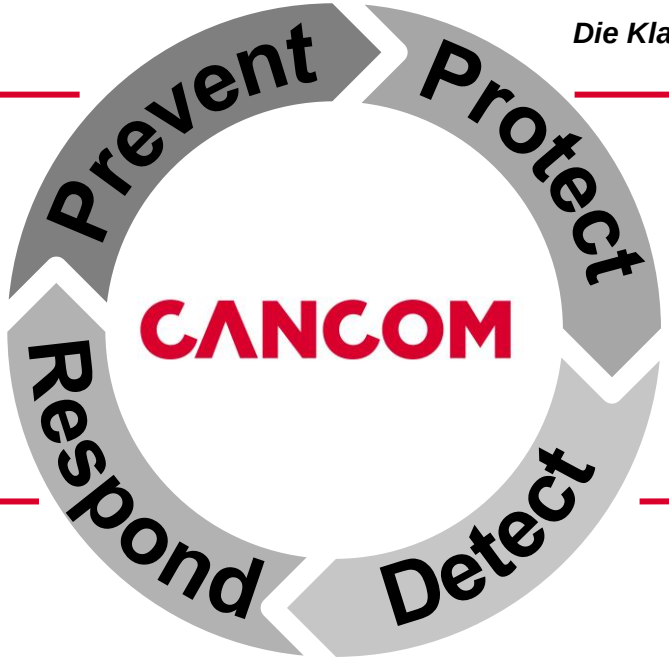
Security Solutions - Strategie

Aufdecken von Schwachstellen und Ablauf- und Strukturproblemen

Security Audit
Security Architecture Review
Backup Health Check
IT Risiko Management
Access Control
Preventive Service

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

Network Security
Content Security
APT Solutions
Application Security



Konkrete Leistungen , die nach einem Angriff wichtig werden

Hilfestellung nach Angriffen (z.B. Ransomware)
Incident/Emergency Response (Readiness)
Forensische Analyse

Erkennen von vorhandenen Systeminfektionen

Security Monitoring
Compromise Assessment
Vulnerability Assessment

Security Levels

Die Security Levels definieren den Reifegrad und Bedarf an Security Lösungen und Services in einem Unternehmen

BASIC

Netzwerk Security
- VLAN Segmente

Perimeter Security
- Web Security
- NextGen Firewall (NAT / IPS)

Endpoint Security
- Antivirus
- Endpoint Firewall
- Patch Management

E-Mail Security
- Sender Based Reputation
- Anti Virus

Secure Remote Access
- VPN

Security Audit / Cyber Security Dienstleistung
- Externes Audit

Regelmäßiges Backup

STANDARD

Netzwerk Security
- Port Security
- Makro-Segmentierung
- NextGen Firewall (App Control / IDS / IPS)
- Netzwerk und Endpunkt Visibilität
- Logging

Perimeter Security
- Sandboxing E-Mail/Web
- DNS-Security
- SDWAN

Endpoint Security
- Advanced Endpoint Protection

Identity Security
- MFA
- Privileged Access Management
- Password Management
- AD Tiering

Cyber Security Dienstleistung
- Internes Audit
- Social Engineering
- Cloud Security Audit
- Vulnerability Management

Immutable Backup

ADVANCED

Netzwerk Security
- Mikro Segementierung
- Network Traffic Analytics / Anomalie Erkennung
- Asset Detection
- Network Access Control / Threat Containment / Client Isolation

Perimeter Security
- Remote Browser Isolation
- Microservice Security
- Web Application Firewall
- DDoS Protection

Endpoint Security
- Endpoint Detection & Response

Identity Security
- Identity Access Management
- User Behavior Analytics
- Cloud Access Security Broker
- VM Hypervisor Security
- Zero Trust / Risk based Authentication

Cyber Security Dienstleistung
- Red Teaming (Simulation)
- Purple Teaming
- EDR
- NDR
- XDR
- SIEM
- IR-Management
- Threat Intelligence
- SOAR

Secure Disaster Recovery Architecture

Eckdaten

CANCOM

Defense Center

Top Experten
24/7/365
Alles aus einer Hand

110+ Mitarbeiter
Das CANCOM Purple Team

130+ Kunden im DACH-Raum

7.500+ Dienstleistungsstunden im Monat

16 Sprachen
werden im CDC gesprochen

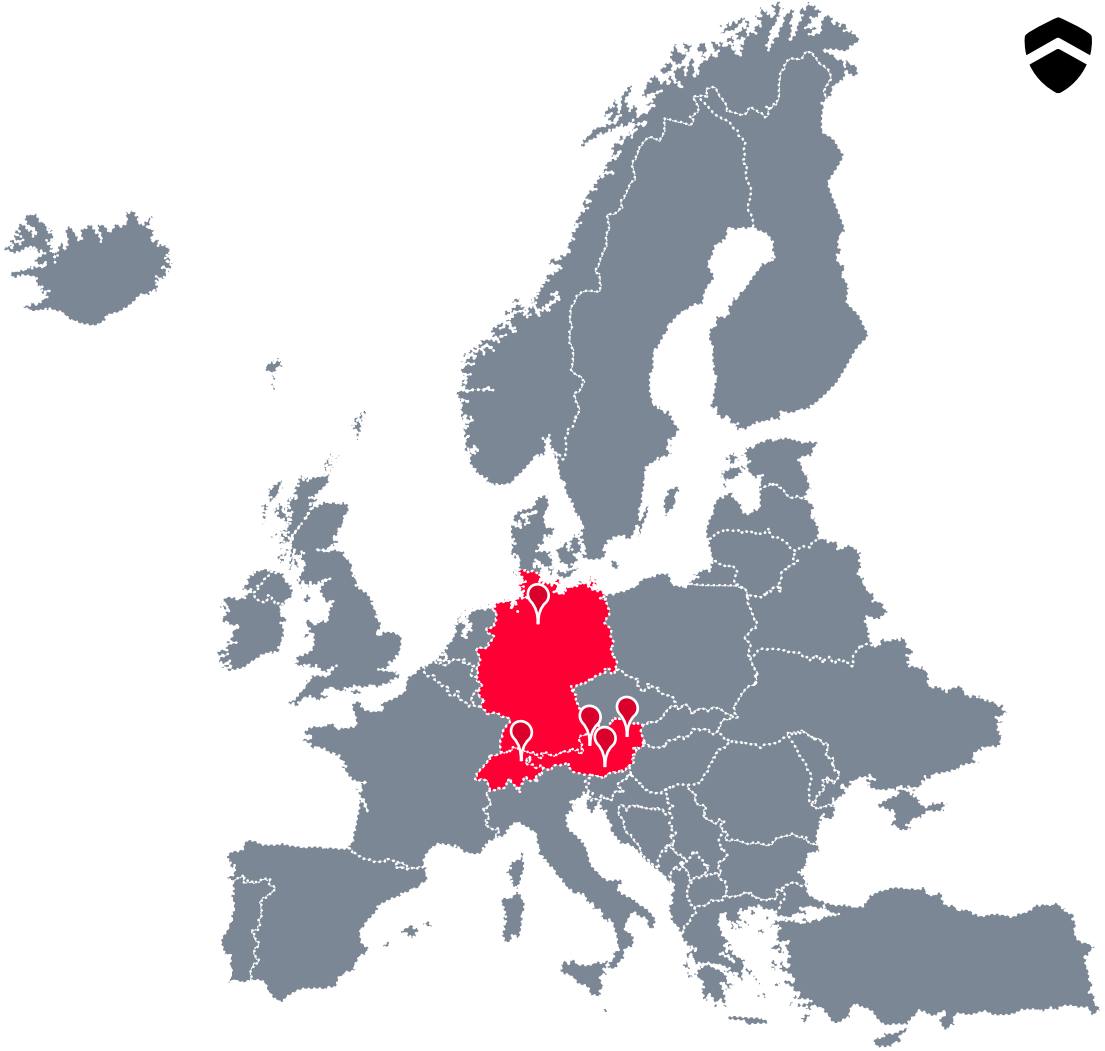
89% True Positive Rate

Lokationen

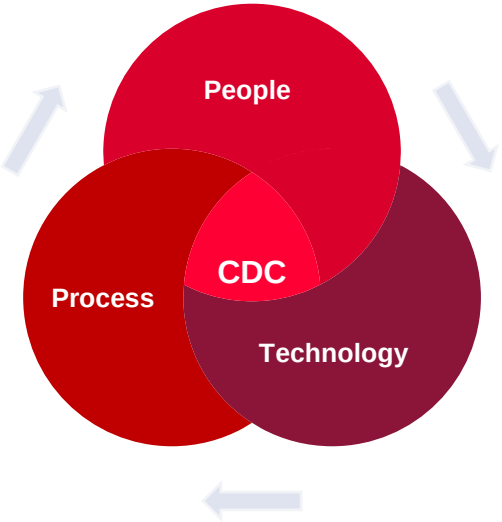
CANCOM

Defense Center

Wien
Linz
Klagenfurt
St. Gallen (CH)
Hamburg



Die wesentlichen Bereiche eines CDC



Mitarbeiter – Qualifikationen, Fähigkeiten & Erfahrungen

Allgemeine Zertifizierungen, z.B. Ü2-Überprüfung und Führungszeugnisse & Spezifische Zertifizierungen, z.B. CompTIA CySA+, CISSP, u.a.

Mehrfache **SANS Gewinner** und **CTF Weltmeister**

Prozesse – Höchsteffiziente Abläufe

Höchsteffiziente Abläufe

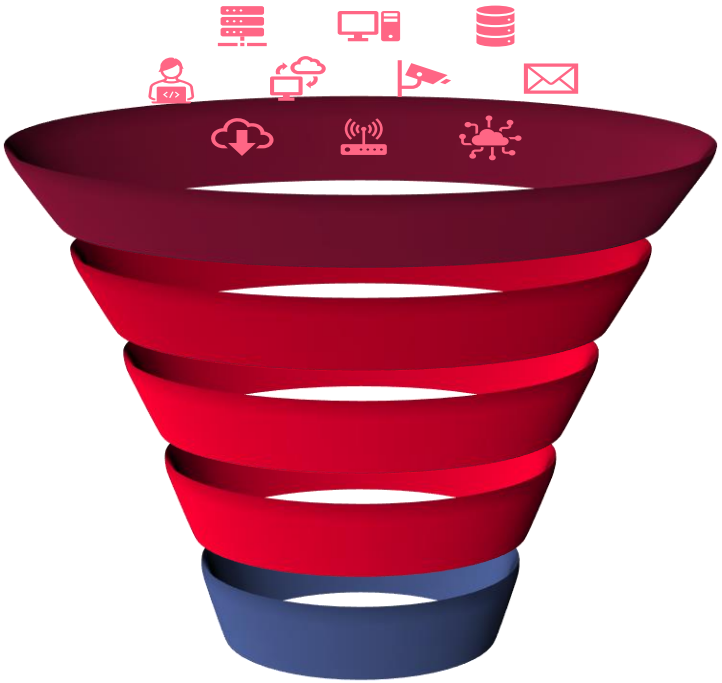
Erfahrungen und Optimierung aus dem täglichen Betrieb (240 Stunden täglich)

Technologie – Marktführender Anbieter

Eingesetzte Technologien (wie SIEM & SOAR) & regelmäßiges proaktives Feintuning der Services

Abgleich mit Threat Feed Datenbank

Unser Lösungsansatz



1 Input

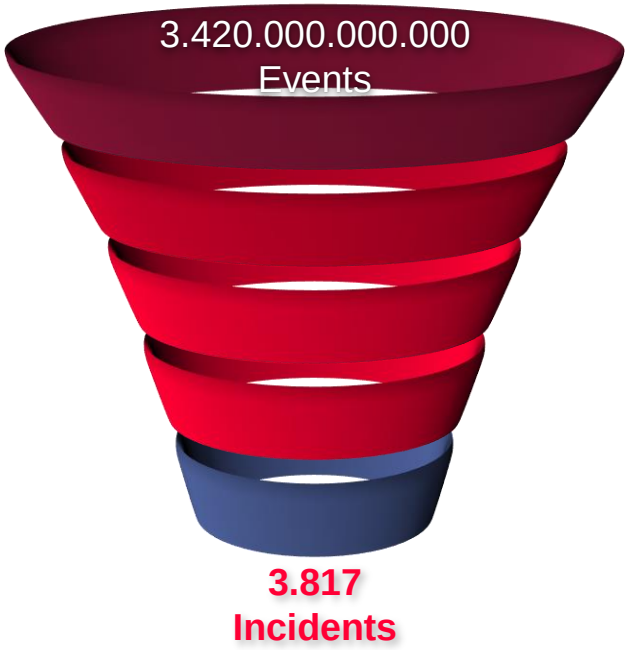
2 Korrelation & Triage

3 Techn. Analyse

4 Security Analysten

5 Dashboard & Reports

CDC Workload – Events und Alarme im Jahr 2023*



3,42 Billionen [+82%]
Events

31,7 Millionen [+64%]
Alarme generiert

1.849.000 [+42%]
kritische Alarme analysiert

3.817 [+257%]
Konsolidierte und verifizierte Vorfälle

*Analyse & Korrelation über 130+ CDC-Kunden innerhalb 12 Monate im Jahr 2023

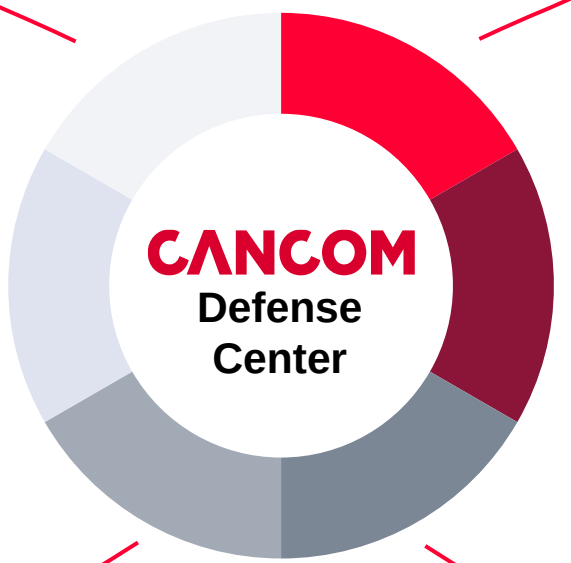
CANCOM Defense Center – modularer Aufbau

Network Security Monitoring (NSM)

Netzwerkverkehr aufzeichnen
Automatisierte und manuelle Analyse
Anomalieerkennung
Netzwerkforensik

Endpoint Detection & Response (EDR)

Endpoint Visiblity
Live remote Analyse
Remote Datensammlung
Endpoint Isolierung



Log Analyse (LOG)

SIEM
Log Aggregierung und Auswertung
Statistische Analysen
Daten Korrelierung

Vulnerability Management (VULN)

Asset Discovery
Reporting von Schwachstellen
Proaktive Nachverfolgung
Anreicherung durch Threat Intelligence

Threat Intelligence (TI)

Brand & Credential Monitoring
Threat Landscape
Threat Actor & Campaign Tracking

Operational Technology Monitoring (OTM)

Risiken identifizieren
Änderungen erkennen
Services und Assets erkennen

CDC Dashboard

- **Zentrale Übersicht**
  - Alle wesentlichen Indikatoren und Events
  - Basis der monatlichen Meetings
- **Reports**
  - Einfache verständliche Reports in unterschiedlichen Detailgraden

CANCOM DEFENSE CENTER

CDC Admin
admin@cancom.com

- Dashboard
- CDC Case Management
- Log Management (Splunk)
- Log Management (Sentinel)
- Endpoint Detection (EDR)
- Endpoint Detection (CrowdStrike)
- OT Security Management
- Threat Intelligence
- Vulnerability Management
- Reports
- Administration
- System
- CDC Portal Help
- Logout

English

Filter table

Status | Responsible | owner | Filter | Clear filter

ID ↓	Title	Tasks	Status	Open since	Responsible
378	[SEC] Testcase	0 | 0 | 0	Open	69 days	Kapsch CDC
343	[GEN] Test1	1 | 0 | 0	Open	88 days	Kapsch CDC
340	[SEC] Case Test	1 | 0 | 0	Open	88 days	Kapsch CDC
287	[SEC] Testing Case Notifications	0 | 1 | 2	Open	90 days	Raphael Eigner
286	[GEN] TEST _ WEM	1 | 1 | 1	Open	116 days	Kapsch CDC
221	[GEN] Test with xlsx test	0 | 1 | 0	Open	158 days	Kapsch CDC
220	[GEN] Test Task	0 | 0 | 0	Open	158 days	Kapsch CDC
219	Upload	0 | 0 | 0	Open	161 days	CDC Admin
198	General Ticket	0 | 0 | 0	Open	186 days	Kapsch CDC
197	[GEN] Security Test	0 | 0 | 0	Open	186 days	Kapsch CDC
195	[GEN] Test Case 2	0 | 0 | 0	Open	189 days	Kapsch CDC
194	[GEN] Test Case1 123	0 | 0 | 0	Open	189 days	Kapsch CDC
147	[SEC] new case 1016	0 | 0 | 0	New	208 days	
146	[SEC] large	0 | 0 | 0	New	208 days	
145	[SEC] new case 1234	0 | 0 | 0	New	208 days	
90	New test	0 | 0 | 0	Open	259 days	CDC Admin

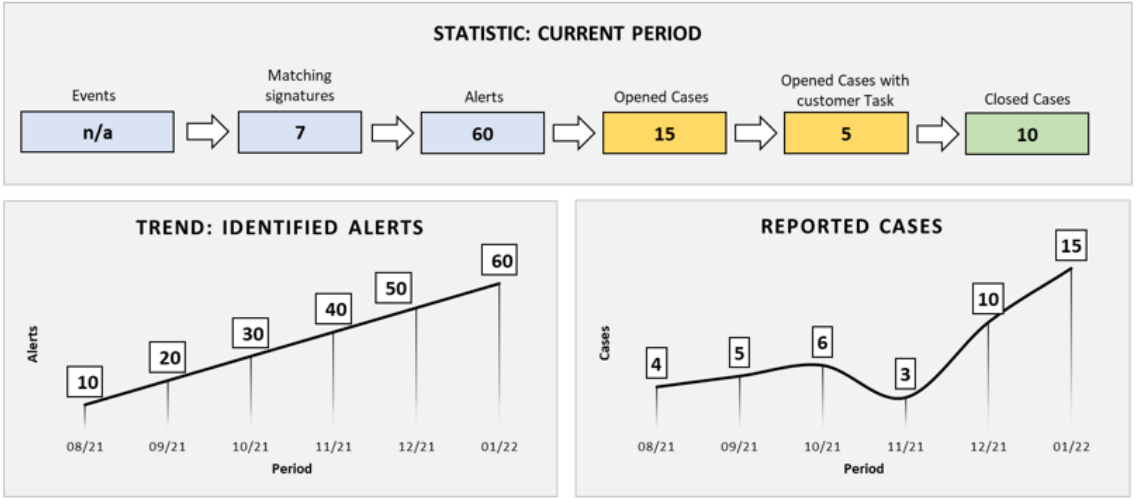
Report

Management Summary

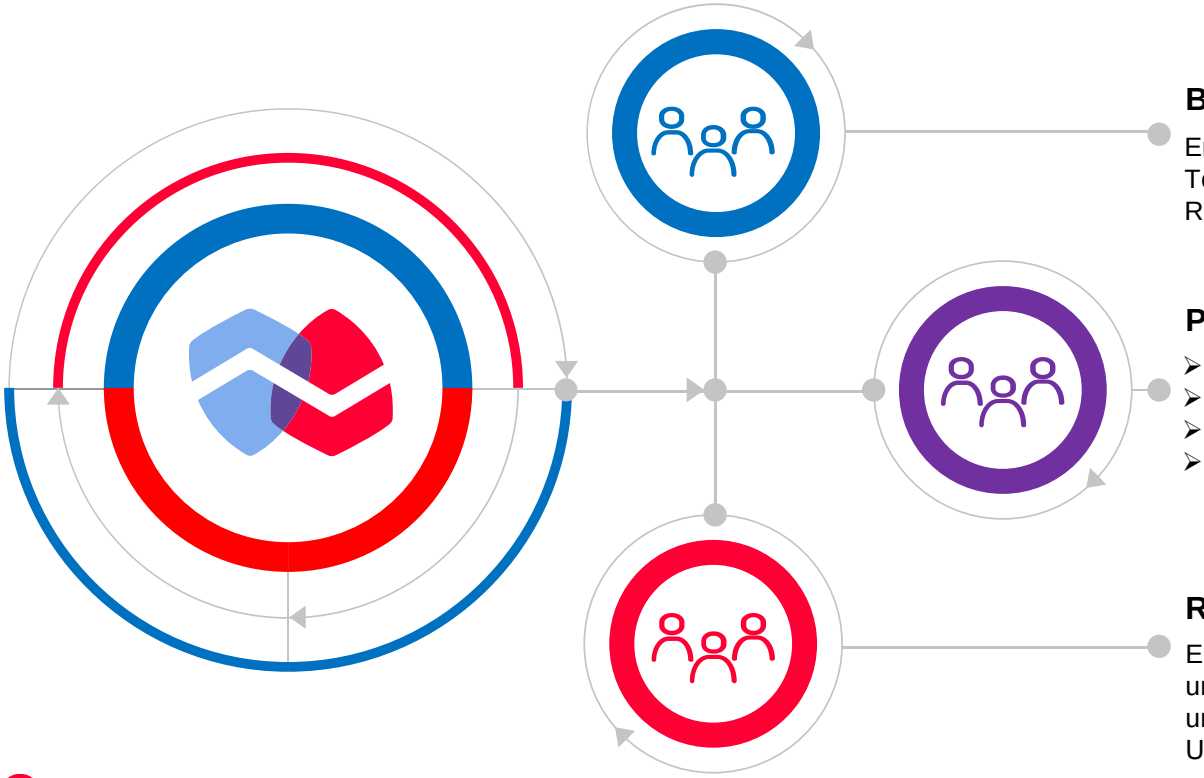
Overall Riskscore

The Riskscore is calculated based on the occurred events, alarms and performed analyzes in the current period, as well as the current security level of the organization (e.g. SSL-Interception, Proxy Policy, …). The Riskscore ranges between 0 and 100 – a higher score implies higher risk for the organization. The actual calculation of the Riskscore can be found in the Appendix.

Alert & Case Statistics



CANCOM Purple Team Ansatz – die neue Ära!



Blue Team

Erkennt einen Angriff oder Penetration Test/Red Teaming und gibt die eingesetzten Taktiken an das Red Team weiter zur weiteren Aufarbeitung

Purple Team

- Entwicklung von Indicators of compromise (IOCs)
- Training der aktiven Abwehr
- Kontrolle und Verbesserung von Prozessen
- Abstand zwischen „Angreifer haben die Nase vorne“ und „Verteidiger haben immer das Nachsehen“ wird stark minimiert

Red Team

Entwickelt neue Möglichkeiten und Angriffswege, um Security Maßnahmen in Unternehmen zu umgehen und testet diese in geschützter Umgebung

Managed Defense Service Architektur