8COM CYBER SECURITY

it-sa 2024
Mittwoch, 23. Oktober 2024

Prozesse – Produkte – Personen:
3 x P für ein effizientes SOC

Security Operations Center by 8com

Götz Schartner | CEO 8com
Halle 7A, Stand 406

8com Kennzahlen

Stand September 2024

it-sa 2024

Halle 7A, Stand 406

105
Mitarbeitende

115
Security Operations Center-Kunden

seit **2004**
Cyber Security

24/7/365
3-Schicht-Modell

BSI IT-Grundschutz
8com Security Operations Center

8COM CYBER SECURITY

8com Services

Security Operations Center
by 8com

- SIEM
- xDR/EDR
- NDR
- Mail-Analysen
- Vulnerability Management
- Digitale Forensik Incident Response
- . . .

it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY

Die drei Säulen eines effektiven SOCs

. . . leider nur auszugsweise auf 12min komprimiert

Prozesse

… legen fest, wie Aufgaben systematisch und effizient ausgeführt werden.

Produkte

… liefern die technologischen Werkzeuge zur Umsetzung der Prozesse.

Personen

… bringen das notwendige Fachwissen und die Fähigkeiten ein.

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

Auszug: Organisationsprozesse

it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY

Auszug: Organisationsprozesse

Schichtbetrieb – 24/7/365:
Personalbedarf, Kommunikation, Mitarbeiterbindung

- Level 1: mindestens 2-3 FTEs pro Schicht
- Level 2: mindestens 1 FTE pro Schicht
- Level 3: Rufbereitschaft möglich
- **Personalresilienz** (Springer-Schicht etc.)

Auszug: Organisationsprozesse

Technologie und Governance

- **Technologie Scouting**
- **Technologie Ownership** (Prozesse)
- **Aus- und Fortbildungs- Prozesse**
- **Service Management . . .**
- **Governance + Compliance**
- . . .

Security Monitoring Prozesse

… Scope beachten:

it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY

Security Operations Center

OT
Leittechnik,
Medizintechnik etc. ...

Other sources
Datenbanken,
Applikationen,
...

IT-Systeme
Clients, Server, Firewalls,
VPN-GW, Smartphones
...

Cloud / SaaS
M365, Azure, AWS,
Google, Salesforce
...

Network
...

Identity
Active Directory, Azure
AD, Okta
...

it-sa 2024
Halle 7A, Stand 406

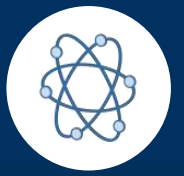
8COM CYBER SECURITY

Security Monitoring Prozesse

Log-Management und SIEM-Systeme (Sysmon etc.)

User and Entity Behavior Analytics (UEBA)

Endpoint Detection and Response (EDR/XDR)



Network Detection and Response (NDR)

Deception-Technologien (Honeypots, Honeyuser, Honeytokens)

Security Orchestration, Automation, and Response (SOAR)

Threat Intelligence Plattformen

Threat Hunting

Cloud Security Monitoring

Mobile Threat Defense (MTD)

Kontinuierliche Verbesserungsprozesse

...

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

Incident Response Prozesse

- **Preparation** (Incident Response Pläne, Playbooks SOAR, Definition Incident Teams usw.)
- **Detection and Reporting** (Identifikation Fales Positives)
- **Analysis and Triage**
- **Containment**
- **Eradication**
- **Recovery**
- **Lessons Learned**

Produkte:

Die technologischen Werkzeuge eines SOCs

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

Produkte:

Die technologischen Werkzeuge eines SOCs

Ein Security Operations Center ist auf eine umfangreiche Palette spezialisierter Technologien angewiesen, um Sicherheitsbedrohungen effektiv zu **erkennen**, zu **analysieren** und **abzuwehren**.

Diese Technologien bilden das **technische Fundament** des SOC und ermöglichen es, operative Aufgaben effizient und präzise auszuführen. Im Folgenden werden die zentralen Technologien vorgestellt, die ein SOC für seine internen Abläufe und operativen Tätigkeiten benötigt.

Beispiel: Technologie Scouting:
Was kann eine XDR-Technologie leisten?

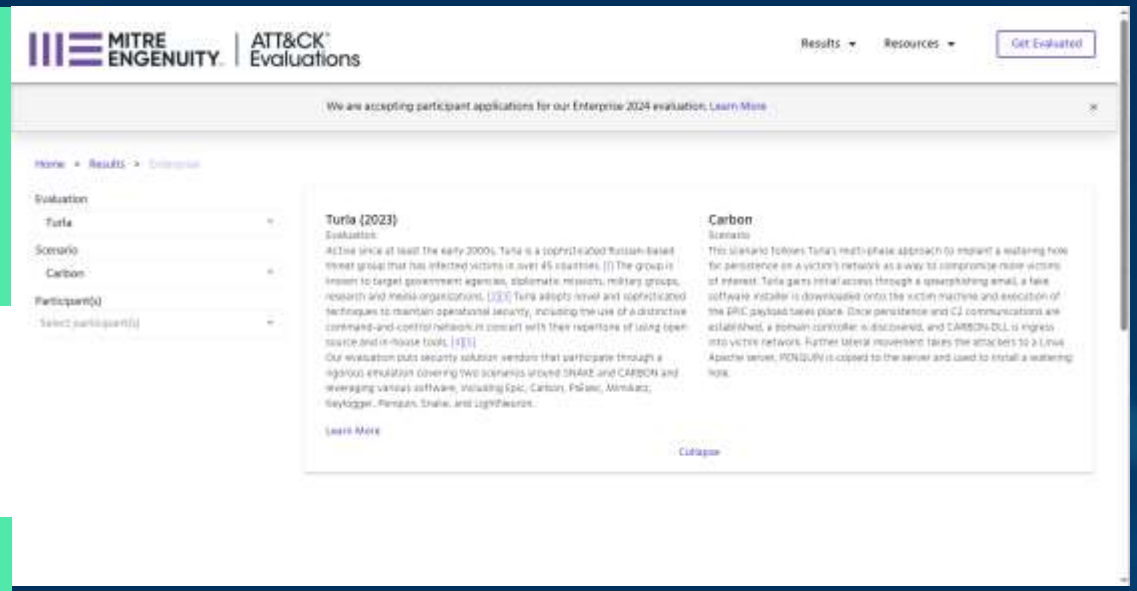
Erkennung und Abwehr

Achtung
EDR/XDR Lösungen haben häufig eine gute bis sehr gute Erkennung vom Hersteller implementiert

Da Hacker die Erkennung aber testen können, **gibt es immer häufiger XDR-Bypassing Attacks.**

Qualität in der Erkennung und Analyse

XDR ≠ XDR



it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY

Produkte

Security Information and Event Management (SIEM)

Extended Endpoint Detection and Response
UEBA, Telemetrie-Monitoring, Threat Hunting, Forensik-Tool-Set, Incident Respone etc.

Network Detection and Response (NDR)

Intrusion Detection and Prevention Systems (IDS/IPS)

Deception-Technologien (Honeypots, Honeyuser, Honeytokens)

Security Orchestration, Automation, and Response (SOAR)

Threat Intelligence Plattformen

User and Entity Behavior Analytics (UEBA)

Forensik- und Malware-Analyse-Tools

Vulnerability Management Systeme (CTEM)

Mobile Threat Defense (MTD)

Cloud-Sicherheitslösungen

Ticketing- und Fallmanagement-Systeme

BI für Reporting und Dashboarding

...

it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY

Personen:

Das Herzstück eines SOCs

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

Personen:

Das Herzstück eines SOCs

Level 1 Analysten + MoD
Alarmbearbeitung, Phishing-Mail Analysen, erste Containments

Level 2 Analysten
Threat Analyses, Threat Hunting, Malware Analysis, Incident Response

Level 3 Analysten
Forensik, Behandlung komplexer und neuartiger Bedrohungen

Product Owner + Technologie Scouts
pro Produkt wie SIEM, XDR, SOAR 2-3 Mitarbeiter, non productive

SOC Architekten

Incident Manager, Krisenmanager

Red Teaming

SOC IT-Administration, Software Developer, Service Manager

it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

Götz Schartner

goetz.schartner@8com.de

www.8com.de

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

Auslosung

Mi.: 17:30 Uhr
Do.: 12:30 Uhr
Halle 7A, Stand 406

it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY