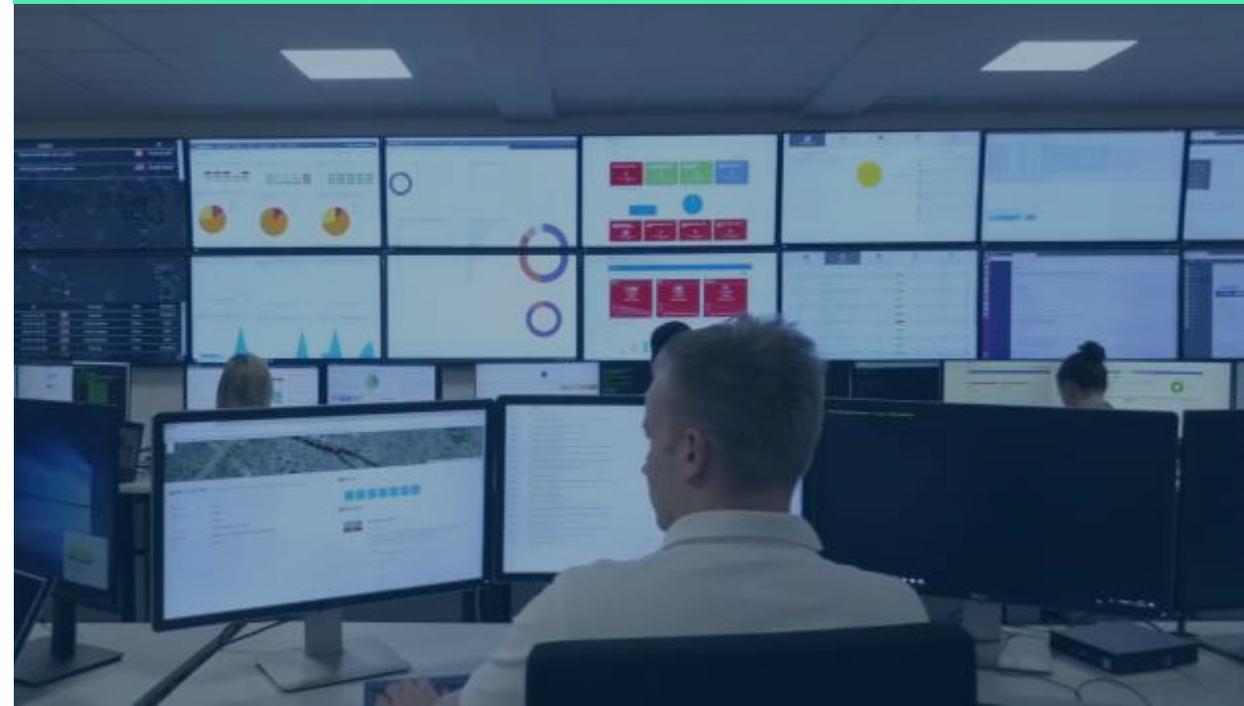


# Prozesse – Produkte – Personen: 3 x P für ein effizientes SOC

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

Security  
Operations  
Center by 8com



# 8com Kennzahlen

Stand September 2024

it-sa 2024

Halle 7A, Stand 406



105

Mitarbeitende

115

Security Operations Center-  
Kunden

seit 2004

Cyber Security



BSI IT-Grundschutz  
8com Security  
Operations Center

24/7/365  
3-Schicht-Modell

# 8com Services

## Security Operations Center by 8com

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

# Die drei Säulen eines effektiven SOC

... 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.

# Auszug: Organisationsprozesse

## 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:



### OT

Leittechnik,  
Medizintechnik etc. ...

### Other sources

Datenbanken,  
Applikationen,  
...



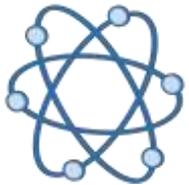
### IT-Systeme

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

# Security Operations Center

### Cloud / SaaS

M365, Azure, AWS,  
Google, Salesforce  
...



### Network

...

### Identity

Active Directory, Azure  
AD, Okta  
...



# 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**

...

# 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 SOC's

## Produkte:

Die technologischen Werkzeuge eines SOC



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

The screenshot shows the MITRE Engenuity ATT&CK Evaluations website. The header includes the MITRE Engenuity logo and 'ATT&CK Evaluations'. A navigation bar has 'Results', 'Resources', and a 'Get Evaluated' button. A banner below the header states: 'We are accepting participant applications for our Enterprise 2024 evaluation. Learn More'. The main content area is titled 'Home > Results > Enterprise'. On the left, there are filters for 'Evaluation' (Turla), 'Scenario' (Carbon), and 'Participant(s)'. The main content displays two scenarios: 'Turla (2023)' and 'Carbon'. The 'Turla (2023)' scenario description reads: 'Active since at least the early 2000s, Turla is a sophisticated Russian-based threat group that has infected victims in over 45 countries. [1] The group is known to target government agencies, diplomats, journalists, military groups, research and think-organisations. [2][3] Turla employs novel and sophisticated techniques to maintain operational security, including the use of a destructive command-and-control network in concert with their repertoire of using open-source and in-house tools. [4][5] Our evaluation puts security solution vendors that participate through a rigorous evaluation covering two scenarios named SNAKE and CARBON and leveraging various software, including Epic, Carbon, Follower, Mimikatz, Keylogger, Pegasus, Shrike, and LogPheonix.' The 'Carbon' scenario description reads: 'This scenario follows Turla's multi-phase approach to implant a watering hole for persistence on a victim's network as a way to compromise more victims of interest. Turla gains initial access through a spearphishing email, a fake software installer is downloaded onto the victim machine and execution of the PRC payload takes place. Once persistence and C2 communications are established, a botnet controller is discovered, and CARBON-DLL is ingested into victim network. Further lateral movement takes the attacker to a Linux Apache server, P0N3QUIN is copied to the server and used to install a watering hole.' Both scenarios have 'Learn More' and 'Collapse' links.

# Produkte



**Security Information and Event Management (SIEM)**



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

...

# Personen: Das Herzstück eines SOC's

# Personen:

## Das Herzstück eines SOC's



### 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

# Sie haben noch Fragen?

Sprechen Sie mich gerne an!

**Götz Schartner**



[goetz.schartner@8com.de](mailto:goetz.schartner@8com.de)  
[www.8com.de](http://www.8com.de)



it-sa 2024

Halle 7A, Stand 406





## Auslosung

Mi.: 17:30 Uhr

Do.: 12:30 Uhr

Halle 7A, Stand 406



### IT-SA Gewinnspiel

**Auslosung:**  
Dienstag & Mittwoch: 17:30 Uhr  
Donnerstag: 12:30 Uhr  
am 8com Stand 7A - 406

**Wir verlosen täglich am 8com Stand** unter allen Teilnehmenden des Tages (ab 18 Jahren):

- 1x Perimeter-Penetrationstest im Umfang von 2 Tagen
- 1x Phishing Test mit 3 simulierten Angriffsmails
- 1x Web-based Trainingsreihe „Grundlagen der Informationssicherheit“ für Ihre Mitarbeitenden

**Teilnahmebedingungen:**  
Mit der Teilnahme stimmen Sie der Datenverarbeitung im Rahmen des Gewinnspiels zu. Keine Datenweitergabe an Dritte. Es gelten unsere Datenschutzbestimmungen: [www.8com.de/datenschutzbestimmungen](http://www.8com.de/datenschutzbestimmungen)  
Nur eine Teilnahme pro Messetag durch Abgabe der Postkarte am 8com Stand während der Messetage. Keine Ballkuschlung. Die ausgelosten Teilnehmer werden nach der Auslosung per E-Mail benachrichtigt. Der Rechtsweg ist ausgeschlossen.

Name, Vorname

Geschäfts-E-Mail-Adresse\*

Hiermit stimme ich dem Erhalt des 8com Newsletter zu. Diese Einwilligung kann jederzeit widerrufen werden.

Hiermit stimme ich zu, im Nachgang zur Messe von 8com kontaktiert zu werden. Diese Einwilligung kann jederzeit widerrufen werden.