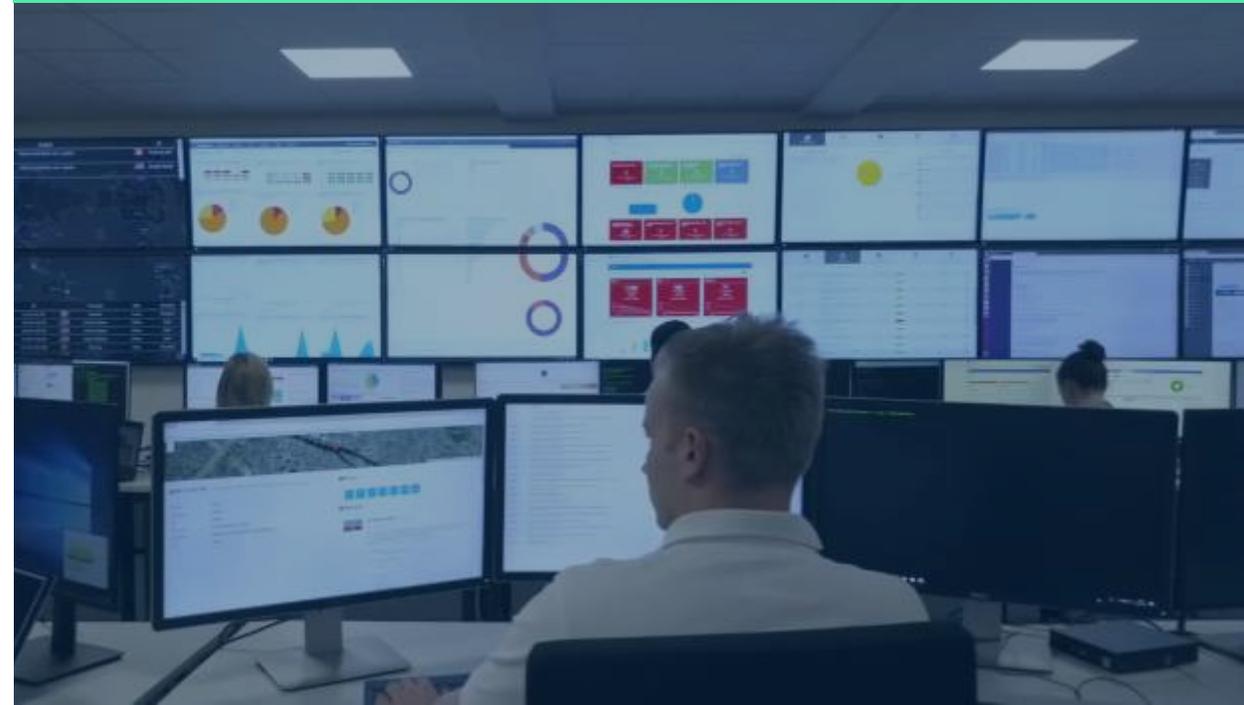


# SOC – Make or Buy? eine Entscheidungshilfe

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



24/7/365  
3-Schicht-Modell

BSI IT-Grundschutz  
8com Security  
Operations Center

# 8com Services

## Security Operations Center by 8com

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

# SOC: Make or Buy

## ... eine Entscheidungshilfe

# SOC: Make or Buy

... eine Entscheidungshilfe

Warum benötige ich ein Security Operations Center?



✓ Compliance (Alibi?)

✓ ... dann billiges SOC einkaufen – kostet nicht viel, bringt nicht viel 😊

✓ Erkennung und Abwehr von Cyberangriffen / Manipulationen?

# SOC: Make or Buy

... eine Entscheidungshilfe



**Kernfragen**

**Menschen – Technologie – Prozesse**



Kosten (Die Personalkosten machen den größten Anteil an den Gesamtkosten aus.)



Verfügbarkeit qualifizierter Cyber Security Spezialisten



Umsetzbarkeit, Skalierbarkeit und Flexibilität



Risiken

# Menschen:

## Das Herzstück eines SOC's (Mindestanforderungen)

# Menschen:

Das Herzstück eines SOC's (M)

12

Level 1 Analysten

Alarmbearbeitung, Phishing-Mail Analysen  
erste Containments

Ext-  
ern

6

Vulner + Technologie Scouts  
wie SIEM, XDR, SOAR 2-3  
Mitarbeiter, non productive

4

IT-Administration,  
Software Developer

Achtung: je nach Größe werden weitaus mehr Mitarbeiter benötigt, das sind nur die Mindestzahlen

# FTEs

# SOC: Make or Buy

... eine Entscheidungshilfe



**Kernfragen**  
Menschen – Technologie – Prozesse



Recruiting: Können Sie die notwendigen Stellen überhaupt besetzen?



Mitarbeiterbindung



Prozesse (einige hundert Prozesse müssen erstellt und gepflegt werden)



Risiken

# SOC: Make or Buy

... eine Entscheidungshilfe



... Scope beachten:





### OT

Leittechnik,  
Medizintechnik etc. ...

### Other sources

Datenbanken,  
Applikationen,  
...



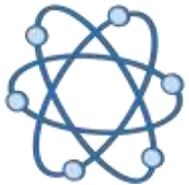
### IT-Systeme

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

# Security Operations Center

### Cloud / SaaS

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



### Network

...

### Identity

Active Directory, Azure  
AD, Okta  
...



# Produkte

## Die technologischen Werkzeuge eines SOC's

# Produkte

## Die technologischen Werkzeuge eines SOCs



**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**

...

# SOC: MAKE

## PRO

- ✓ Volle Kontrolle
- ✓ maßgeschneidertes SOC
- ✓ Vertraulichkeit
- ✓ „beliebige Changes möglich“ 😞

## CONTRA

- ✓ Hoher Personalaufwand
- ✓ Hohe Kosten
- ✓ enorme Komplexität

# SOC: BUY

## PRO

- ✓ aktuelle Technologien und Expertise
- ✓ Skalierbarkeit und Flexibilität
- ✓ Kostenkontrolle und Effizienz
- ✓ zeitnahe Implementierung
- ✓ Entlastung interner Ressourcen
- ✓ Haftungsübergänge (teilweise)

## CONTRA

- ✓ Eingeschränkte Kontrolle
- ✓ Datenschutz und Sicherheit
- ✓ Vertragsbindung und Anforderungsdefinition
- ✓ Integrationsherausforderungen
- ✓ Regulatorische Risiken
  - Compliance-Verantwortung bleibt beim Auftraggeber
  - Jurisdiktion: Ausland . . .

# Resümee

- ✓ Die Entscheidung für ein externes SOC ("Buy") bietet viele Vorteile, darunter Zugang zu spezialisierten Fachkräften, moderne Technologien und Kosteneffizienz.
- ✓ Nachteile sorgfältig abwägen

**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)



SOC as a SERVICE

SOC as a SERVICE

24/7/365 persönlich für Sie im Einsatz



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 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 Messestand durch Abgabe der Postkarte am 8com Stand während der Messetage. Keine Ballkugelschaltung. Die ausgelobten 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.