

Wie entscheiden?

Kriterien für die Auswahl
eines Security Operations
Centers

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
- ...

Definition der Kernaufgaben eines Security Operations Centers

Kernaufgaben

Erkennung

Analyse

Abwehr



... von Cyber Angriffen

Compliance

- Dora
- TISAX
- ...



OT

Leittechnik,
Medizintechnik etc. ...

Other sources

Datenbanken,
Applikationen,
...



IT-Systeme

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

Security Operations Center by 8com

Cloud / SaaS

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



Network

...

Identity

Active Directory, Azure
AD, Okta
...



1

Fähigkeiten zur
Angriffserkennung &
Abwehr

2

Erfahrungen und
Kontinuität des
SOC-Anbieters

3

Sicherheit des
SOCs selbst

4

Organisation

1

Fähigkeiten zur
Angriffserkennung &
Abwehr

2

Erfahrungen und
Kontinuität des
SOC-Anbieters

3

Sicherheit des
SOCs selbst

4

Organisation

Produkte



Security Information and Event Management (SIEM)

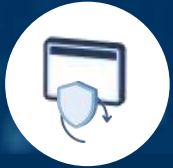


Extended Endpoint Detection and Response

UEBA, Telemetrie-Monitoring, Threat Hunting, Forensik-Tool-Set, Incident Response etc.



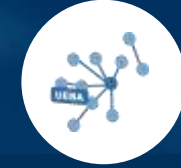
Network Detection and Response (NDR)



Mobile Threat Defense (MTD)



Threat Intelligence Plattformen



User and Entity Behavior Analytics (UEBA)



Intrusion Detection and Prevention Systems (IDS/IPS)



Deception-Technologien

(Honeypots, Honeyuser, Honeytokens)



Security Orchestration, Automation, and Response (SOAR)



Fähigkeiten zur Angriffserkennung

- ✓ Eignung der Technologien für den Einsatzzweck
- ✓ Integration und Zusammenführung der Technologien
- ✓ Multimandantenfähigkeit und Trennung
- ✓ Technologische Kompetenz des Anbieters (Referenzen)
- ✓ Ausreichende Anzahl von SOC-Analysten für 24/7/365
- ✓ Kompetenz der Mitarbeiter
- ✓ Präsenz der Analysten im SOC
- ✓ Exklusive Fokussierung auf die SOC-Tätigkeiten

Fähigkeiten zur Angriffsabwehr

Angriffe passieren – immer wieder!

Fähigkeiten zur Angriffsabwehr

Angriffe passieren – immer wieder!



Ein SOC **muss jederzeit, rund um die Uhr, einsatzbereit** sein – auch mitten in der Nacht auch an Feiertagen!
Es ist entscheidend, dass Sicherheitsvorfälle routiniert und effizient abgearbeitet werden können.

Um nach der Erkennung eines Angriffs erfolgreich zu reagieren, **muss ein SOC über umfassende Angriffsabwehrfähigkeiten verfügen**. Diese gliedern sich in mehrere entscheidende Bereiche:

Erfahrungen und Kontinuität des SOC-Anbieters

Angriffe passieren – immer wieder!



Fähigkeiten zur Angriffsabwehr

- ✓ Incident Response: Verfügbarkeit und Reaktionsfähigkeit
- ✓ SLA (24/7/365), max. 1 Stunde
- ✓ technische Eingriffsmöglichkeiten

SOC: Incident Response

Schnelle Eindämmung und Wiederherstellung
nach Angriffen mit flexibler Reaktion



Fähigkeiten zur Angriffsabwehr



- ✓ Incident Response: Verfügbarkeit und Reaktionsfähigkeit
- ✓ SLA (24/7/365), max. 1 Stunde
- ✓ technische Eingriffsmöglichkeiten
- ✓ (vertrags)rechtliche Eingriffsmöglichkeiten (+ Übungen)

1

Fähigkeiten zur
Angriffserkennung &
Abwehr

2

Erfahrungen und
Kontinuität des
SOC-Anbieters

3

Sicherheit des
SOCs selbst

4

Organisation

Erfahrung und Kontinuität des SOC-Anbieters



- ✓ Wie lange im Cyber Security Markt aktiv?
- ✓ Welche Services wurden vor 20 Jahren, 15, 10 und 5 Jahren angeboten?
- ✓ Trendhopper oder Kontinuität - nur ein Hype (Hopp-On / Hopp-Off) oder auch noch in 5 Jahren im Portfolio?
- ✓ Relevanz des SOC-Betriebes für den Anbieter
- ✓ Skalierbarkeit: Die Fähigkeit, mit dem Wachstum und den sich ändernden Bedürfnissen des Unternehmens Schritt zu halten.

1

Fähigkeiten zur
Angriffserkennung &
Abwehr

2

Erfahrungen und
Kontinuität des
SOC-Anbieters

3

Sicherheit des
SOCs selbst

4

Organisation

Sicherheit des SOC selbst



Ein zentraler Aspekt bei der Auswahl eines SOC-Anbieters ist die Sicherheit des SOC selbst. In einer Zeit, in der staatliche Akteure und andere organisierte Angreifer gezielt IT-Service Provider und Sicherheitsdienstleister angreifen, um über diese in die Systeme ihrer Kunden einzudringen, **muss das SOC als Herzstück der Sicherheitsinfrastruktur besonders geschützt sein.**

Ein aktuelles Beispiel ist der Angriff auf **Südwestfalen IT**, bei dem die IT-Dienstleistungen für bis zu **72 Kommunen** beeinträchtigt wurden. Dies verdeutlicht die zunehmende Bedrohungslage und zeigt, dass auch SOC besonders attraktive Ziele für Angreifer sind. Ein gehacktes SOC stellt ein Risiko für alle Kunden des Anbieters dar, daher müssen besondere Sicherheitsvorkehrungen getroffen werden.



Digitale Sicherheit des SOC selbst



- ✓ ISO 27001 auf Basis von BSI IT-Grundschutz (keine reine ISO)
- ✓ Regelmäßige externe Audits und Penetrationstests (Recht auf Einsicht der Berichte)
- ✓ Strikte Trennung von SOC und Office-IT
- ✓ Eigenständige SOC-IT-Administration
- ✓ Keine direkten Internetzugriffe von SOC-Systemen (Surfen, Mailen etc.)
- ✓ 24/7/365 Monitoring, tägliches Vulnerability Management

Gebäudesicherheit des SOC selbst



Physische Trennung SOC-Bereich und Office-Bereich



Einbruchssicherheit (Türen, Fenster, Wände etc.) RC4 oder höher



Strikte Zugangskontrollen für den SOC-Bereich (SOC only)



Logging und Auswertung von Zugangsdaten



Live-Videoüberwachung, EMA . . .

1

Fähigkeiten zur
Angriffserkennung &
Abwehr

2

Erfahrungen und
Kontinuität des
SOC-Anbieters

3

Sicherheit des
SOCs selbst

4

Organisation

Organisation (SOC-Betreiber)



Die organisatorischen Voraussetzungen eines SOC-Anbieters spielen eine entscheidende Rolle bei der Auswahl des richtigen Partners, insbesondere für deutsche Unternehmen und Behörden.

Organisation (SOC-Betreiber)



✓ Standort: Deutschland: Datenhoheit und Souveränität

✓ Internationaler Hauptsitz und Niederlassungen

✓ Bietet das SOC alle notwendigen Leistungen selbst an?

✓ Stabilität der Mitarbeiterstruktur

✓ Technologieunabhängigkeit des SOC-Anbieters

✓ Größe und Relevanz des Kunden für den Anbieter

Sie haben noch Fragen?
Sprechen Sie mich gerne an!

Götz Schartner



goetz.schartner@8com.de
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

Di. & 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
Nur eine Teilnahme pro Messestand durch Abgabe der Postkarte am 8com Stand während der Messetage. Keine Ballkuschelung. 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.