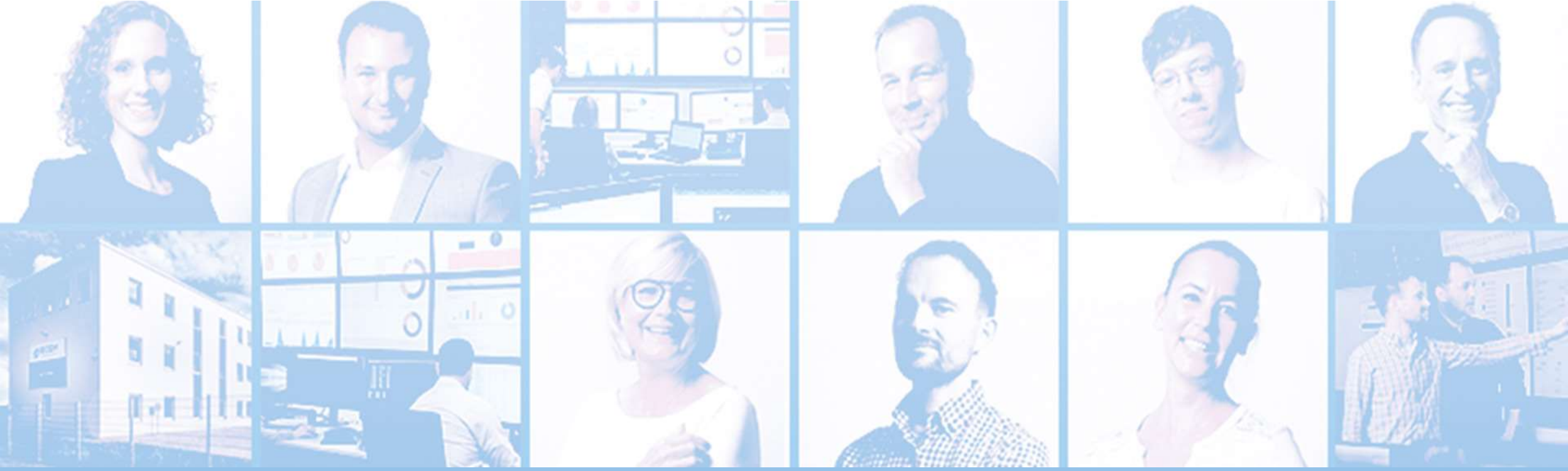
8 COM
CYBER SECURITY

Schlüsselüberlegungen bei der Wahl eines SOC-Anbieters

It-sa Expo 2023

Mittwoch, 11. Oktober 2023



8com-Vorstellung

Wir l(i)eben Sicherheit

Halle 7A, Stand 606

8COM CYBER SECURITY

89

Mitarbeiter*innen

seit 2004

Cyber Security

82

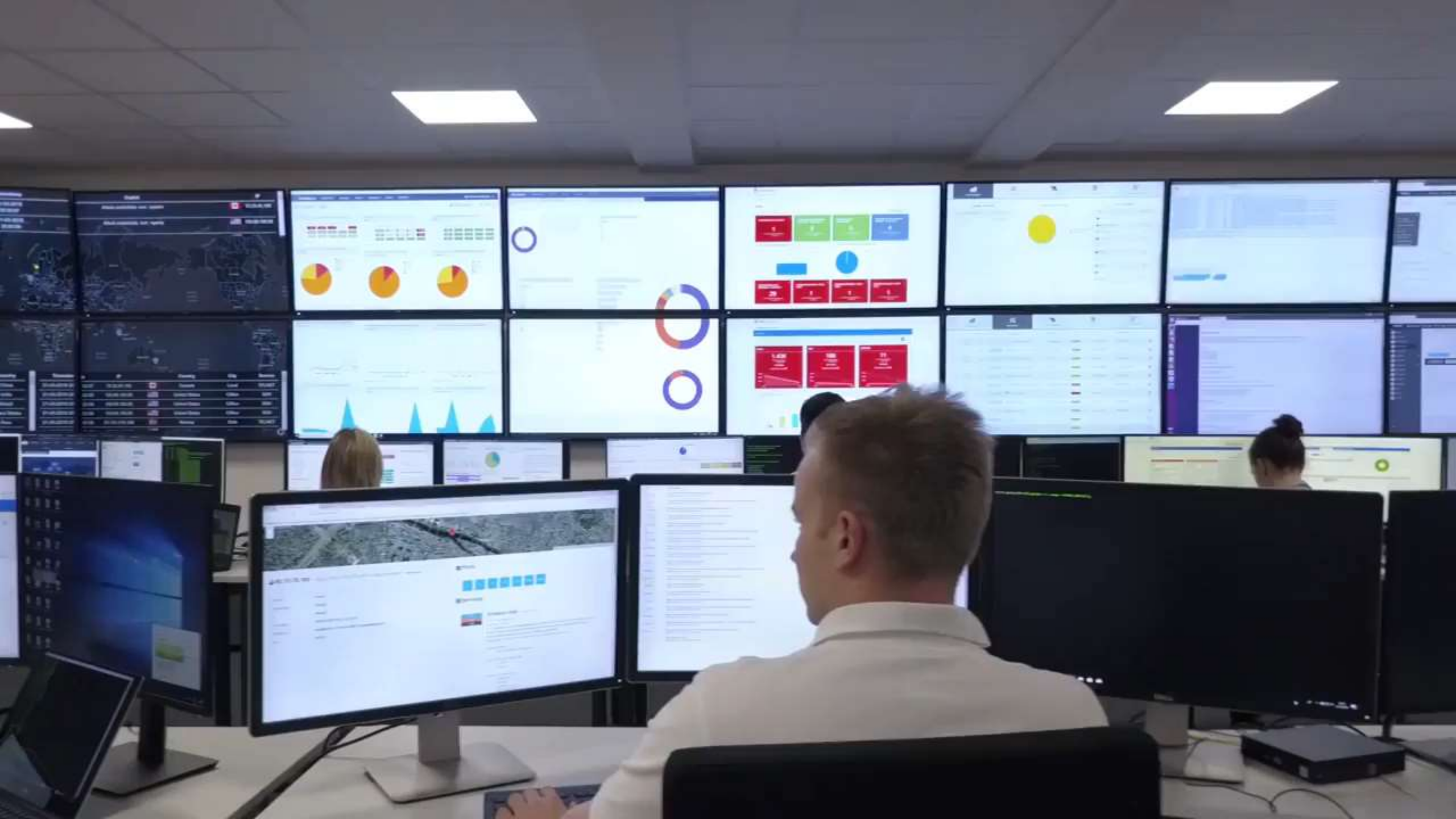
Security Operations Center Kunden

> 600

IT-Forensik, Incident Response, Penetration Testing und Awareness-Kunden

Halle 7A, Stand 606

8COM CYBER SECURITY



Definition der **Kern**aufgaben eines Security Operations Centers

8COM CYBER SECURITY

Kernaufgaben

- Erkennung
- Analyse
- Abwehr

. . . von Cyber Angriffen

Kriterien für die Auswahl eines passenden SOC-Anbieters

1

Fähigkeiten zur Angriffserkennung & Abwehr

2

Erfahrungen und Kontinuität des SOC-Anbieters

3

Sicherheit des SOCs selbst

4

Organisation

Halle 7A, Stand 606

8COM CYBER SECURITY

1

Fähigkeiten zur Angriffserkennung & Abwehr

2

Erfahrungen und Kontinuität des SOC-Anbieters

3

Sicherheit des SOCs selbst

4

Organisation

Halle 7A, Stand 606

8COM CYBER SECURITY

Fähigkeiten zur Angriffserkennung & Abwehr

Halle 7A, Stand 606

8COM CYBER SECURITY

Fähigkeiten zur Angriffserkennung

Technologieeinsatz

- Technologien zur Erkennung (SIEM/UEBA/EDR/NDR etc.)
- Sind die Technologien für den Einsatzzweck geeignet?
- Beherrscht der Anbieter die Technologien überhaupt?
- Wie werden die einzelnen Technologien zusammengeführt?
- Multimandantenfähigkeit und Trennung gewährleistet?
- Threat Intelligence Feeds?

Personelle Aufstellung

- Ausreichende Anzahl von SOC-Analysten (3-Schichtbetrieb 24/7/365)
- SOC-Analysten sitzen 24/7/365 im SOC, nicht Homeoffice, nicht per Rufbereitschaft
- Kompetenz der Mitarbeiter (in Gesprächen zu prüfen, Referenz einholen – nicht auf Zertifizierungen verlassen)
- Mitarbeiter arbeiten ausschließlich im SOC, nicht zusätzlich als Consultant, Penetration Tester, Forensiker, Auditor, Administrator etc.
- Sprache der Analysten muss Verhandlungssicher in der Muttersprache des Kunden angeboten werden
- Erfahrung: Wie viele Jahre Erfahrung hat das Team in der Cyber Security?

Fähigkeiten zur Angriffsabwehr

- Hat der Anbieter eigene Incident Response Teams, die im Incident Fall auch verfügbar sind?
- Wie schnell reagiert das SOC auf Vorfälle - SLA?
- Kann das SOC aktiv eingreifen (rechtlich, technisch, organisatorisch) ?

- Incident-Response-Planung: Vordefinierte und gut strukturierte Prozesse
- Welche Technologien werden zur Analyse und zur Eindämmung verwendet?
- Sind Analysetools immer verfügbar oder müssen diese nachträglich aktiviert und sogar installiert werden?

- Unterstützung im Krisenmanagement – Krisenkommunikation vorhanden?

1

Fähigkeiten zur Angriffserkennung & Abwehr

2

Erfahrungen und Kontinuität des SOC-Anbieters

3

Sicherheit des SOCs selbst

4

Organisation

Halle 7A, Stand 606

8COM CYBER SECURITY

Erfahrung und Kontinuität des SOC-Anbieters

- Wie lange im Cyber Security Markt aktiv?
- Wie ist die Service Qualität des Anbieters insgesamt (wie relevant ist die Zufriedenheit der Kunden für den Anbieter)?
- 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.

Halle 7A, Stand 606

8COM CYBER SECURITY

1

Fähigkeiten zur Angriffserkennung & Abwehr

2

Erfahrungen und Kontinuität des SOC-Anbieters

3

Sicherheit des SOCs selbst

4

Organisation

Halle 7A, Stand 606

8COM CYBER SECURITY

Sicherheit des Security Operations Center selbst

- ISO 27001 auf Basis von IT-Grundschutz oder nach einer ähnlich hohen Sicherheitszertifizierung zertifiziert?
- Sind die SOC-Systeme und Netze, welche beim SOC-Anbieter für die Leistungserbringung des SOC-as-a-Service betrieben werden, zu 100% von der restlichen IT des Unternehmens (andere Fachbereiche, Office IT etc.) getrennt?

- Besteht eine eigene SOC IT-Administration, welche ausschließlich für das jeweilige SOC arbeitet?
- eigenständige Backup Systeme (B2D/B2T)
- Werden die IT-Systeme des SOC-Anbieters täglich auf Sicherheitslücken untersucht?
- Können die Untersuchungsberichte der letzten 12 Monate von Kunden bei Bedarf eingesehen werden?
- Keine direkten Internetzugriffe
- …

Physikalische Sicherheit

- Trennung SOC, RZ und restliches Unternehmen
- Zugang (Türen und Fenster - Widerstandsklasse RC4 oder höher) – wer hat Zugtrittsberechtigungen und Möglichkeiten – wer nicht? Lassen Sie sich Zutrittskonzepte vorlegen.
- EMA, Live-Videoüberwachung, Logging Zugänge etc.

Halle 7A, Stand 606

8COM CYBER SECURITY

1

Fähigkeiten zur Angriffserkennung & Abwehr

2

Erfahrungen und Kontinuität des SOC-Anbieters

3

Sicherheit des SOCs selbst

4

Organisation

Halle 7A, Stand 606

8COM CYBER SECURITY

Organisation des Security Operations Center

- Standort in Deutschland – für deutsche Unternehmen und Behörden:
  - Datenhoheit
- Wo hat der SOC-Anbieter seinen Hauptsitz – in welchen weiteren Ländern hat er Niederlassungen – welchen Rechtsprechungen unterliegt dieser etc.

- Eigenbetrieb vs. Outsourcing:
- Inwiefern werden Leistungen in-house erbracht oder ausgelagert?

- Stabilität der Mitarbeiterstruktur (Kununuu Bewertungen ansehen)

- Besteht eine Technologieunabhängigkeit des SOC-Anbieters? Kann der Partner die Technologien austauschen, wenn es notwendig sein sollte?

- Passt der Partner

- Sie müssen „relevant“ für den Partner sein, aber auch nicht zu übermächtig

Last but not Least

Besuchen Sie den ausgewählten SOC-Anbieter – lernen Sie das SOC selbst (auch Sicherheitsmaßnahmen) und vor allem die handelnden Personen (SOC-Management, Analysten Level 1, 2 und 3, Service Management, ISB/CISO) kennen.

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

Götz Schartner

goetz.schartner@8com.de

www.8com.de

Halle 7A, Stand 606

8COM CYBER SECURITY