8COM CYBER SECURITY

it-sa 2024
Mittwoch, 23. Oktober 2024

SOC – Make or Buy?
eine Entscheidungshilfe

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

SOC: Make or Buy

. . . eine Entscheidungshilfe

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

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?

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

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

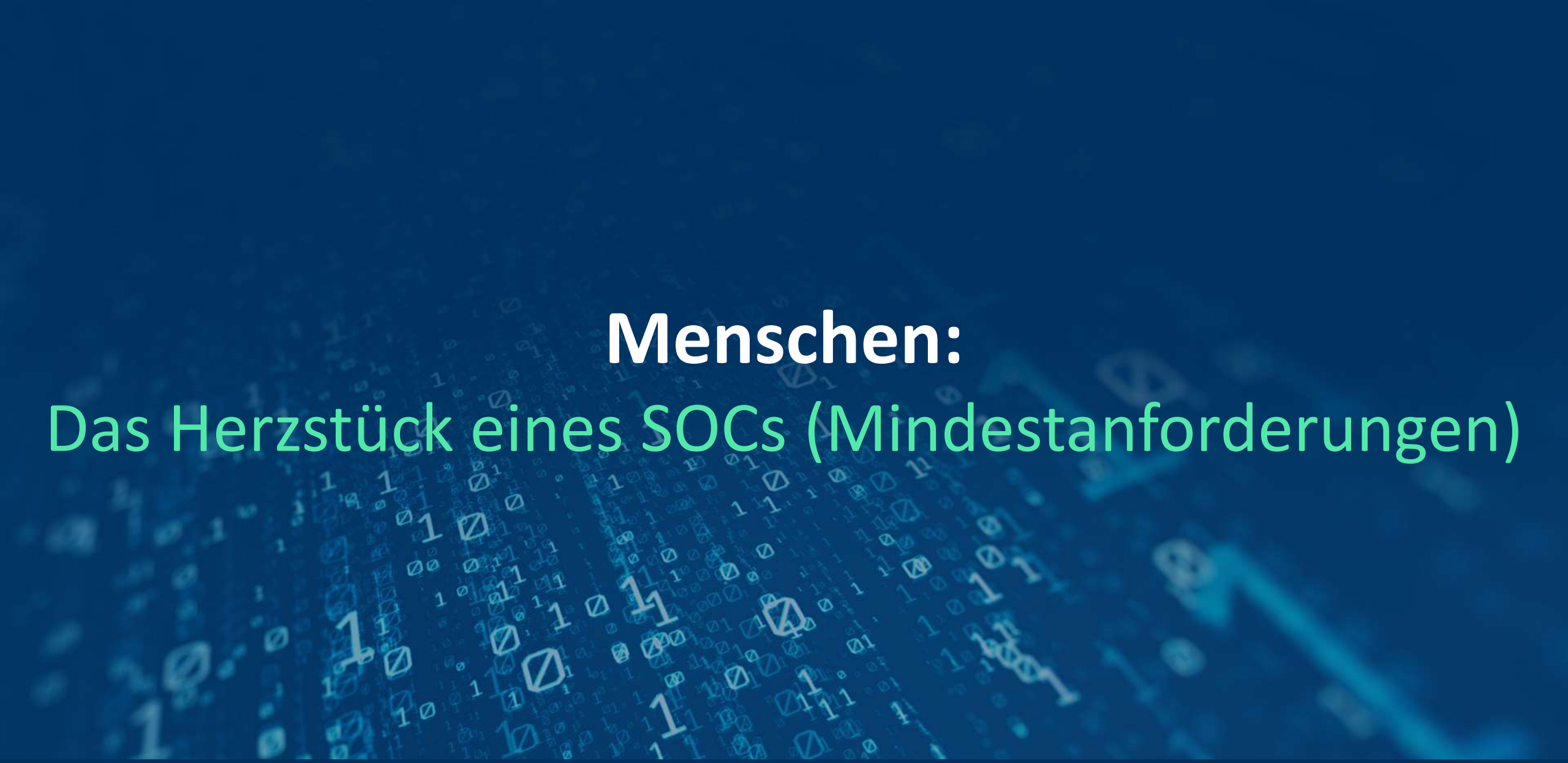
it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

Menschen:

Das Herzstück eines SOCs (Mindestanforderungen)



it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

Menschen:

Das Herzstück eines SOCs (M

12

Level 1 Analysten
Alarmbearbeitung, Phishing-Mail Analyse
erste Containments

Ext-
ern

6

wner + Technologie Scouts
t wie SIEM, XDR, SOAR 2-3
eiter, non productive

4

C IT-Administration,
oftware Developer

ca. 30

FTEs

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

it-sa 2024
Halle 7A, Stand 406

8COM CYBER SECURITY

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

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

SOC: Make or Buy

. . . eine Entscheidungshilfe

… 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

Produkte

Die technologischen Werkzeuge eines SOCs

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

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 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

...

it-sa 2024

Halle 7A, Stand 406

8COM CYBER SECURITY

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

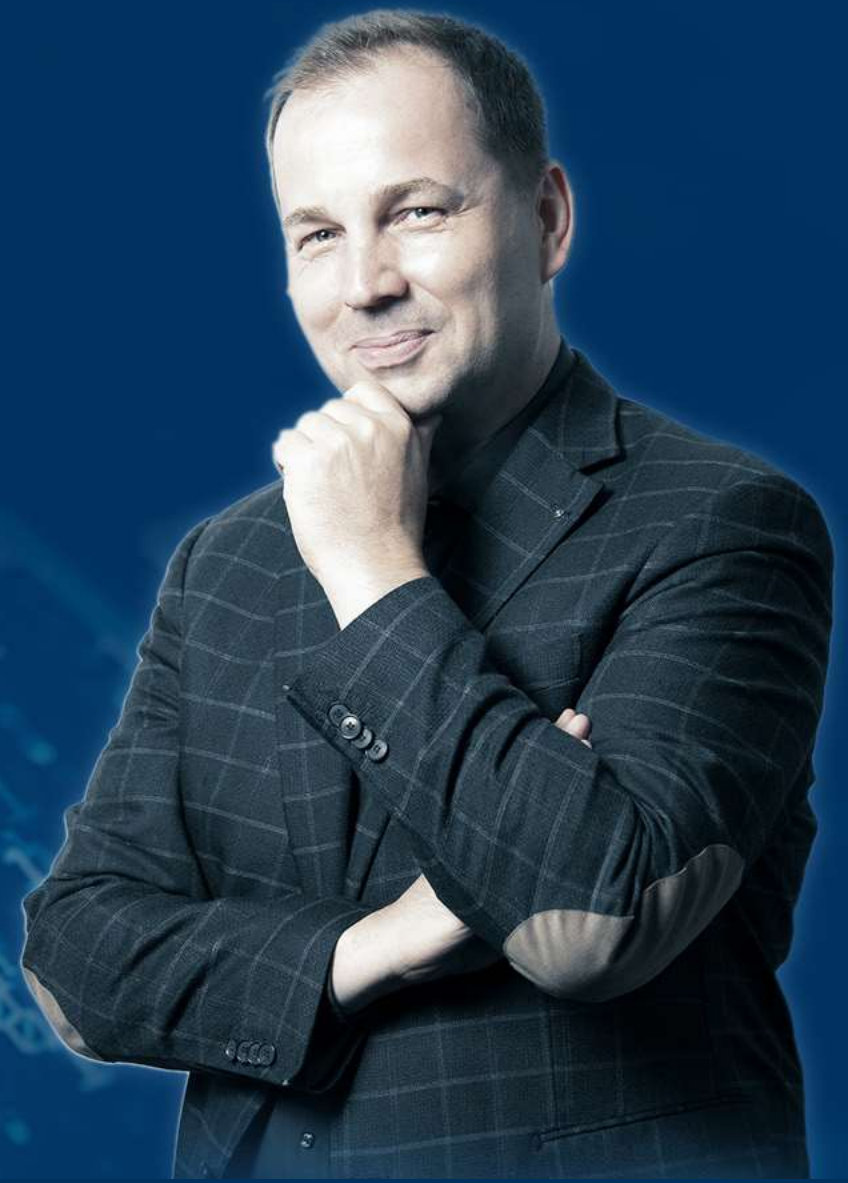
- Eingeschränkte Kontrolle
- Datenschutz und Sicherheit
- Vertragsbindung und Anforderungsdefinition
- Integrationsherausforderungen
- Regulatorische Risiken
  - Compliance-Verantwortung bleibt beim Auftraggeber
  - Jurisdiktion: Ausland . . .

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

www.8com.de

it-sa 2024

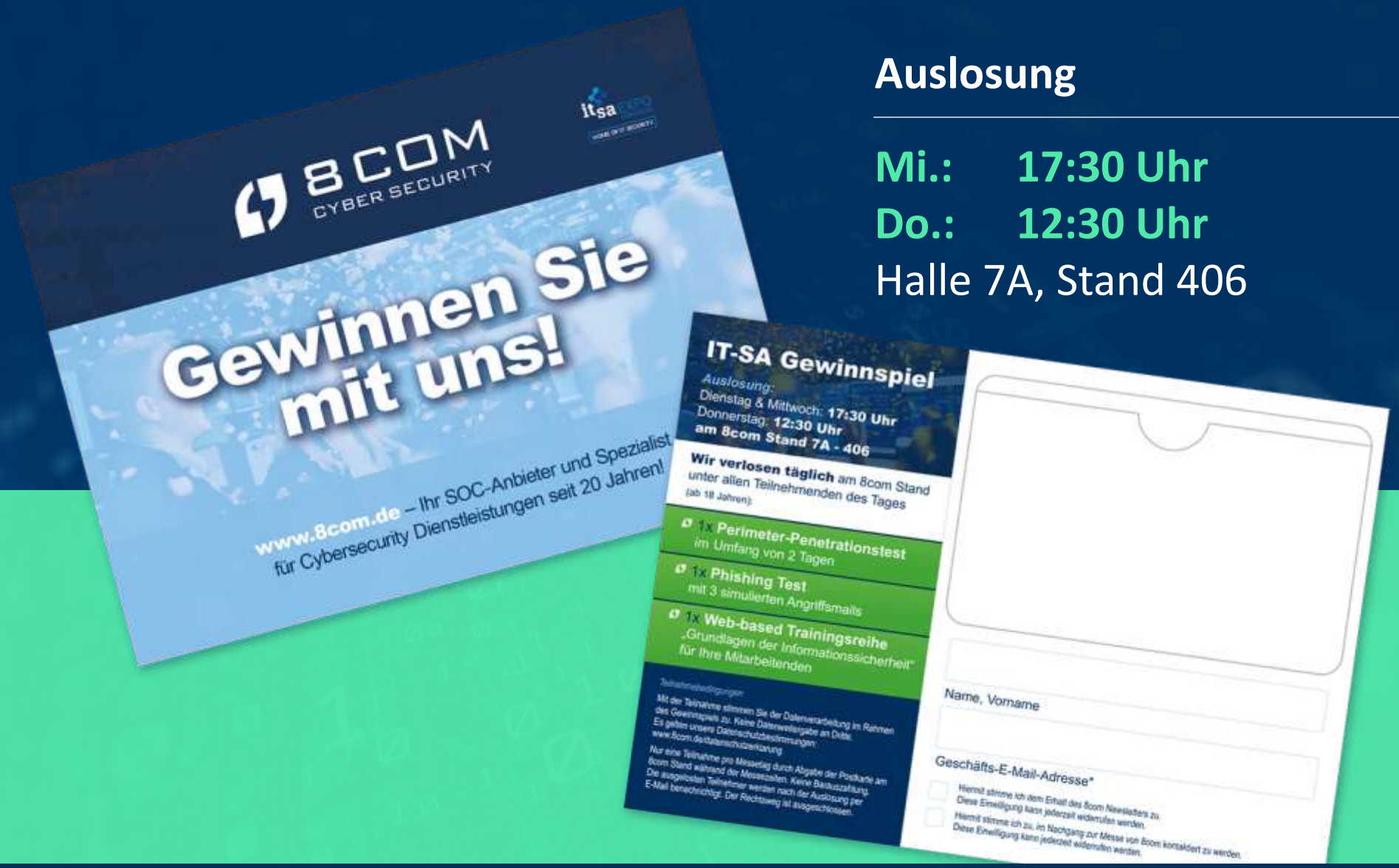
Halle 7A, Stand 406

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