

# Immer eine gute Security Entscheidung



# Wir übernehmen Verantwortung für Security: Von Strategie über Anbieterauswahl bis Einführung und Interims-Management

## Security Management

1

### Strategie, Gap-Assessments, Architekturen und Roadmaps

Das Diagnostik Ergebnis der ... fällt in Summe „sehr gut“ aus und liegt im Rahmen des Benchmarks

Ergebnisübersicht

**Diagnostik-ScoreCard**

**Handlungsempfehlungen**

- Handlungsempfehlung: Die besten guten Prozess und die Stärken in der Geschäfts- und operativen Ebene zu berücksichtigen und "traditionellen Standards" umzusetzen. Ebenso gibt es eine Reihe von Handlungsempfehlungen, die sich nach in Umsetzung befinden.
- Handlungsempfehlung: Einmalige oder regelmäßige Schulungen der Mitarbeiter, um das Bewusstsein für die Wichtigkeit von Security zu erhöhen.
- Handlungsempfehlung: Die Integration von Security in die Business- und IT-Strategie zu fördern.
- Handlungsempfehlung: Die Integration von Security in die Business- und IT-Strategie zu fördern.

Typische Optionen zur Kombination der Angriffserkennung in IT und OT

**A) Häufiges Vorgehen**

- IT: SOC, SIEM
- OT: OT Anomalie-Erkennung

**B) Variante SIEM-zentriert**

- IT: SOC, SIEM
- OT: OT Anomalie-Erkennung (OT Logs)

**C) Variante XDR in IT**

- IT: XDR, XDR, XDR
- OT: OT Anomalie-Erkennung

Häufigste Form: „klassischer“ SIEM/SOC-Modell mit Anbindung gemittelter OT-Lösung

- Eigene Entwicklung welche SIEM-Lösung
- Eigene Absicherung, OT-Logs
- Aufwand, Kosten

Variante mit einem zentralen (ggf. externen) SIEM

- Datenkontrolle und Zugriff
- Eigene Entwicklung welche SIEM-Lösung
- Weniger Anbieter, höhere Kosten

Variante mit XDR/XDR-Konzept in IT und ohne Übergreifende Sicht

- Standardisierte, im Vergleich zu SIEM/SOC kostengünstigere XDR
- Überwachung für IT mit zügiger Incident-Response
- Überwachung Alarme aus OT intern
- Kein SIEM oder Produktanbindung, ggf. separat als Log-Sender

2

### Angebotsvergleiche + Ausschreibungen

Beispiel: Managed SOC RIP

Executive Summary mit wesentlichen Entscheidungskriterien

Kriterium	MSSP A	MSSP B	MSSP C	MSSP D	MSSP E	MSSP F
SOC-Infrastruktur	2000000	1500000	1800000	2200000	1900000	2100000
24x7-Überwachung	Ja	Ja	Ja	Ja	Ja	Ja
Incident-Response	24h	24h	24h	24h	24h	24h
Compliance	ISO 27001	ISO 27001	ISO 27001	ISO 27001	ISO 27001	ISO 27001

Beispiel Heat Map zur Evaluierung von ~30 MSSPs (outside-in und auf Basis von Anbieter-Interviews)

RIP für Managed Security Services

3

### Implementierung, Compliance, Transition

Compliance

- DSGVO
- ISO 27001
- EU AI Act
- BSI CS Testat
- OSGA
- TIA AVV
- AVV

Vereinfachter Zeitplan

Status 16.09.2024

4

### Interim CISO / ISB und Projektleitung

Status Overview: Service and Vendor Management

Aligned with Coordinators

EU SCC Transfer Impact Assessment (TIA)

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), including for complying with the EU Standard Contractual Clauses (EU SCC)

(Version for transfers to US)

see the notes at the end for more information on the scope and legal basis of this document. Read them in particular if you are a data exporter. Also consult the additional worksheets for more examples, infos and an illustration of the scenarios in which a TIA is required. The blue text in the template is mere sample text; the values and reasoning do not necessarily represent the author's opinion.

Step 1: Describe the intended transfer

a) Data exporter<sup>(1)</sup> (or the sender in case of a relevant onward transfer):

b) Country of data exporter:

c) Data importer<sup>(2)</sup> (or the recipient in case of a relevant onward transfer):

d) Country of data importer:

# Unser Ansatz: 100% Unabhängigkeit

0

Eigene Produkte oder  
Managed Services

0

Reseller-Verträge,  
Deal-Registrierung,  
Provisionen, Kickbacks,  
Referral Fees, Boni oder  
sonstige Projektvergütung  
von Anbieterseite

# Wenn Sie Kunde bei uns sind, befinden Sie sich in guter Gesellschaft

## >500

Unternehmenskunden  
und öffentliche Stellen

## >1.000

Security-, Compliance- und  
Identity Projekte



**Dr. Christoph  
Peylo**

Chief Cybersecurity  
Officer, Robert Bosch  
GmbH

Vorsitzender des  
Beirats,  
CyberCompare



**Prof. Dr. Petra  
Maria Asprion**

Leiterin Kompetenzzentrum  
Cybersecurity & Resilience,  
FH Nordschweiz



**Benjamin  
Bachmann**

CISO,  
Bilfinger SE



**Florian  
Brandner**

Global Information &  
Cybersecurity  
Director,

PUMA



**Dr. Daniel  
Bretschneider**

CISO,  
Miele & Cie. KG



**Stefan  
Würtemberger**

Leiter Corporate IT,  
Dürr Dental SE



**Daniel  
Fai**

Director, Information  
Security Leader DACH  
Procter & Gamble

Unser Beirat

# Mehr als 300 Gap-Assessments, Risikoanalysen und Benchmarking: Von Mittelstand bis Fortune 500, auf Basis NIS-2, ISO 27001, IEC 62443, NIST CSF, CRA, TRBS 1115

Der aktuelle Security-Reifegrad erreicht noch nicht das geforderte NIS2 Ziel-Niveau. 5 wichtige Maßnahmen als wichtige erste Schritte. Ergebnisübersicht

VERTRAULICH

Bewertungslegende: 1 = fehlend bis 4 = stark ausgeprägt IT Ergebnis Top-25%-Unternehmen

### Diagnostik-ScoreCard

### NIS2-Bewertung

Wichtige Maßnahmen sind noch zu ergreifen, um das Gesamtiveau der Security auf den geforderten NIS2-Stand zu heben. In der Vergangenheit wurden wichtige Maßnahmen wie ein Notfallplan, oder die Mitarbeiter-Sensibilisierung erfolgreich umgesetzt. Dennoch existieren weiterhin kritische Bausteine. Siehe dazu die Seiten 6 - 10.

**Handlungsempfehlungen<sup>1</sup>**

- Konsequenter Nutzung MFA:** Nutzung MFA auch außerhalb VPN Use Case v.a. für sensible Accounts (Admin), sowie kritische Anwendungen
- Security Organisation stärken:** Stärkung der Security Organisation mit Benennung eines ISB, erstmalige Durchführung Risikoanalyse auf Ebene Gesamternehmen und Start Aufbau ISMS mit den wesentlichen zentralen Regelungen und POCA-Zyklus
- Einrichtung Managed Service für EDR (MDR):** Die kontinuierliche Überwachung mittels EDR ist aktuell nicht im 7x24 Modus möglich. Vorschlag des Outsourcings an einen spezialisierten Dienstleister. Prüfung mittelfristige Erweiterung um z.B. NDR
- Stärkung Interne Netzwerk-Security:** Prüfen, ob IDS/IPS an der Perimeter-FW aktiviert werden kann. Interne Verschlüsselung stärken
- Netzwerksegmentierung stärken:** Erhöhung des Reifegrades der Netzwerkarchitektur, durch eine verstärkte Netzwerksegmentierung (v.a. I70T) und Erstellung eines Zonenkonzepts.

CyberCompare A BOSCH BUSINESS

### 2023 vs. 2021 plant results show progress across manufacturing network

Item	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Individual plants (anonymized)										
Item 1: How do you structure your cybersecurity management?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 2: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 3: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 4: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 5: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 6: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 7: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 8: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 9: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 10: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 11: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 12: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 13: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 14: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 15: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 16: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 17: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 18: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 19: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0
Item 20: Do you have a security policy or cybersecurity strategy?	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0	5.0

CyberCompare A BOSCH BUSINESS

### We use reliable methods and templates for risk assessments that have been used across > 200 manufacturing plants already

Report Info EN Risk Model 1. SPE Assessment 2. Incident Scenarios 3. Detailed Report 4. Treatments, Measures

CyberCompare A BOSCH BUSINESS

[Customer] cybersecurity maturity level is higher in IT than in OT, with clear potentials for improvement in both areas – focus on implementation needed

Maturity score overview along 4 assessments

**Key Takeaways**

- Slightly below benchmark<sup>1</sup>, key priorities:**
  - Governance: Implementation of policies, regular security audits with link to incentive / consequence mgmt.
  - Incident recovery plans and exercises based on business impact analyses and recovery time objectives
- Slightly above benchmark<sup>1</sup>, key priorities:**
  - Business continuity and disaster recovery plans based on business impact analyses
  - Actual thorough implementation of ISMS<sup>2</sup> instead of „paper tiger“ documents (e.g., privileged account management, multi-factor authentication, audits with consequences)
- Inferior results compared to the peer group<sup>1</sup>, key priorities:**
  - Systematic management infrastructure (e.g., defined OT security responsibilities, policies, coordination with IT security)
  - Emergency plans + exercises
- Expected compliance with 8 / 12 assessed requirements, based on the current state of legislation.**
  - Highest priority (critical / likely non-compliant):
    - Incident reporting policies + procedures (not implemented at all)
    - Multi-factor authentication (only partially implemented / not enforced)
    - Business continuity plans + exercises (missing / no systematic management)
    - Privileged account management (only partially implemented / not enforced)

1. IT benchmark based on Gartner peer benchmark (n = 210), OT benchmark based on CyberCompare industry benchmark (n = 18)  
2. Information Security Management System

CyberCompare A BOSCH BUSINESS

Overall spending and resource baseline of [Customer] is below industry benchmarks. Benchmark would equate to 4-5 additional FTE in security team – ideally internal hires, alternatively as external contractors

### Human resources, Cybersecurity FTE as % of IT FTE

### Financial resources, Cybersecurity as % of total IT spending

1. Assuming 445 IT FTE (0.8% of total IT FTE) and estimated 200 contractors and 18 Cybersecurity FTE | Assuming 120 million IT spending and 6.5 million Cybersecurity spending  
9. Source: Based on Gartner IT Key Metrics IT Security Measures 2025 (December 2024)

CyberCompare A BOSCH BUSINESS

[Customer] security team will realistically need ~4 additional FTE to implement a state of the art ISMS in practice

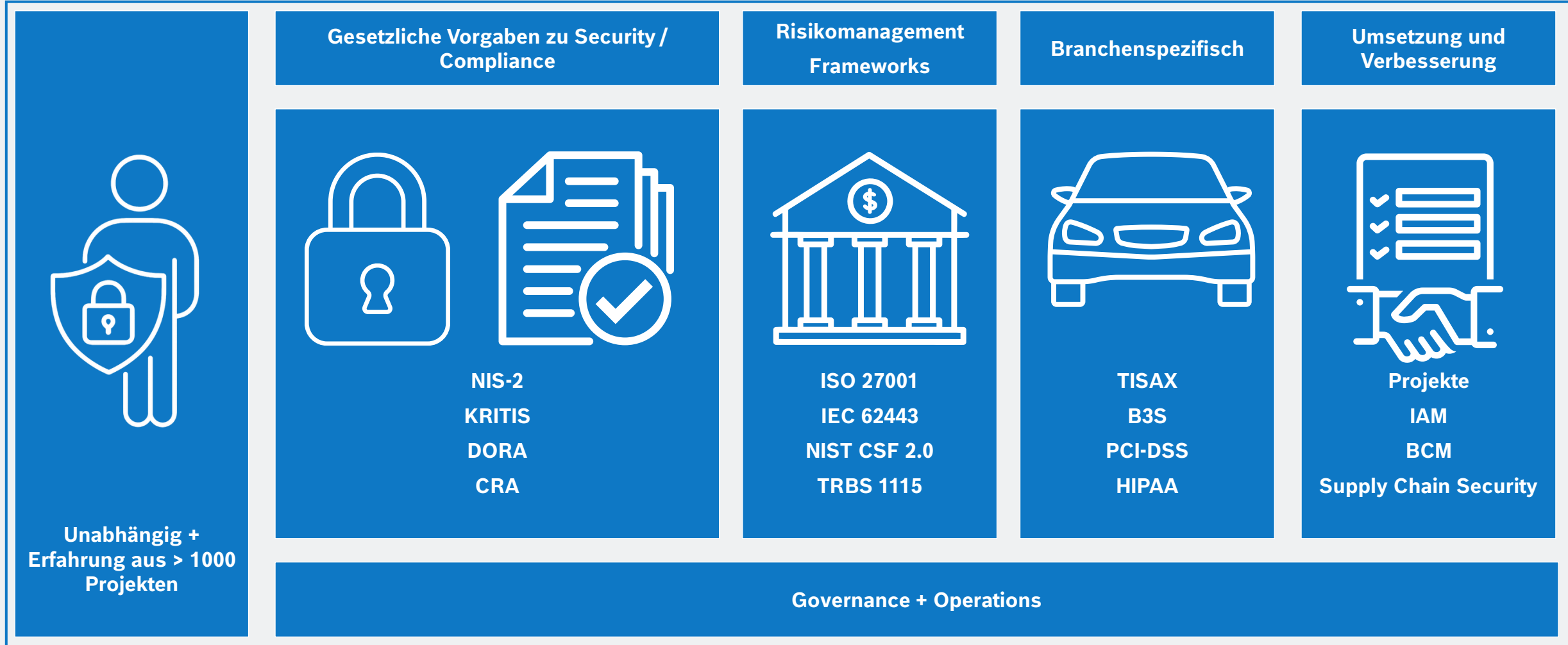
FTE (security team only) estimates to implement recommended improvements, #

**Comments**

- Security team is currently strong in technical profiles, but lacks project managers that enjoy persistent follow-ups
- In total probably ~1 FTE for central coordination + problem solving
- (already hired)
- ~1 FTE, either in security or internal controls team
- In total probably ~1 FTE for project management

CyberCompare A BOSCH BUSINESS

# Interim CISO / ISB: Vorbereitung von Zertifizierungen und Überbrückung von temporären Personalengpässen



# Interim CISO: Wie CyberCompare bei der Ausgründung von Business Units in eigenständige Unternehmen hilft (Carve-Outs)

Wertmaximierung bei gleichzeitiger Minimierung von Risiken

## Herausforderungen bei Carve-Outs

- **Aufbau eigener Security Governance + Operations**
- Asset-Inventarisierung
- Datenseparierung
- Übergang von Zugriffsrechten
- Entkoppelung der Infrastruktur
- IP Schutz
- Erfüllung von Compliance Vorgaben
- **Zeitdruck**

## Unsere bewährte Methodik

### Zieldefinition und Gap-Assessment

- **Bestandsaufnahme** Infosec
- Anforderungen an NewCo, z.B. **ISO27001**, CRA, **NIS2**
- Zielarchitektur
- Abnahmekriterien
- Make/Buy Analysen
- TSA Agreements

### Projektleitung Security-Workstream

- **Interim CISO**
- **Projekt-Management Office**
- Security Roadmap
- Maßnahmenplanung, -abstimmung und -verfolgung
- Risk Mitigation bei Betriebsübergang

### Umsetzung – auch über Closing hinaus

- **Etablierung von ISMS Policies + Prozessen**
- Aufbau Orga + Security Tech Stack
- Identity- u. Access-Management
- Ausschreibungen
- Steuerung von MSSP
- Business Continuity

# Identity & Access (IAM), Identity Governance & Administration (IGA), Privileged Access Mgmt. (PAM): Konzept + Umsetzung



## Zielkonzept & Auswahl

### Herstellerneutral + Best Practices:

- Anforderungsklä rung mit Fachabteilungen (z.B. Compliance, Rollen, Rezertifizierungen, Automatisierung)
- Ggf. Prozessoptimierungen (inkl. maschineller Identitäten und externen Nutzern)
- Zielarchitektur + Budgetschätzung
- Ausschreibungsprozess + Vertragsverhandlung



## Koordination & Umsetzung

### Klare Verantwortung, alle Fäden in einer Hand:

- Koordination von internen Teams und externen Partnern
- Gesamtsteuerung der technischen Implementierung inkl.
  - Onboarding von IdP und Zielsystemen (z.B. HR, SAP/ERP, CRM, M365...)
  - Konfliktmoderation zur Lösungsfindung
  - Testphase mit User Acceptance Tests
  - Abnahme
- Transparenz & Governance:
  - Festlegung von Rollen und Verantwortlichkeiten
  - Reporting an Lenkungsausschuss
  - Abstimmung von Lösungsvorschlägen
  - Monitoring von SLA

# Managed SIEM / SOC: Ca. 130 qualifizierte Anbieter im DACH Raum

## Auswahl SOC Anbieter:



## Auswahl SIEM/XDR Plattformen:



...Liste nicht abschließend

## Über 100 Kundenprojekte. Typische Beispiele:

**KRITIS** Unternehmen: **Kombiniertes SIEM/SOC Projekt** inklusive Anbindung der Operations Technology

Öffentliche **SOC** und **SIEM-Ausschreibungen** für **Krankenhäuser, Städte/Kommunen, ÖPNV, Flughäfen,...**

**Industrieunternehmen** mit 9.000 MA: **Start mit SIEM Auswahl.** Im **Projektverlauf** Fokussierung auf **Managed SOC**

**Mittelständler** mit 2.800 MA: Start **Spezifikation Managed SOC** – auf Basis der Ausgangslage dann **zunächst Ausschreibung** eines **MDR** für die **Endpoint Security**

**SIEM-Marktstudie** über 13 **Vendoren** inkl. RfI für **DAX-Konzern.** **Detail-Bewertung** im Rahmen von **Compare-Days**

**Ablösung** aktuelles **Managed SOC** für **Industrieunternehmen** mit ca. 20.000 MA **inkl. SIEM Lösung**

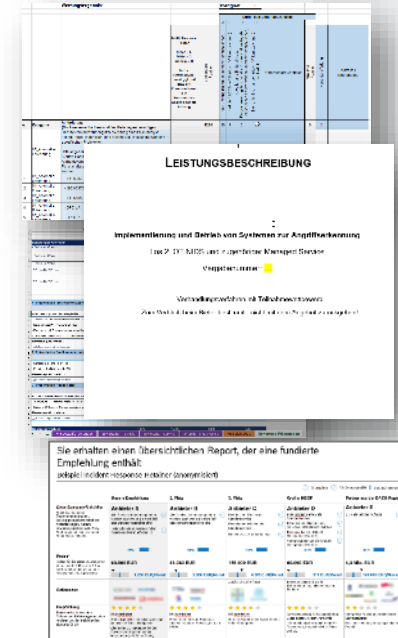
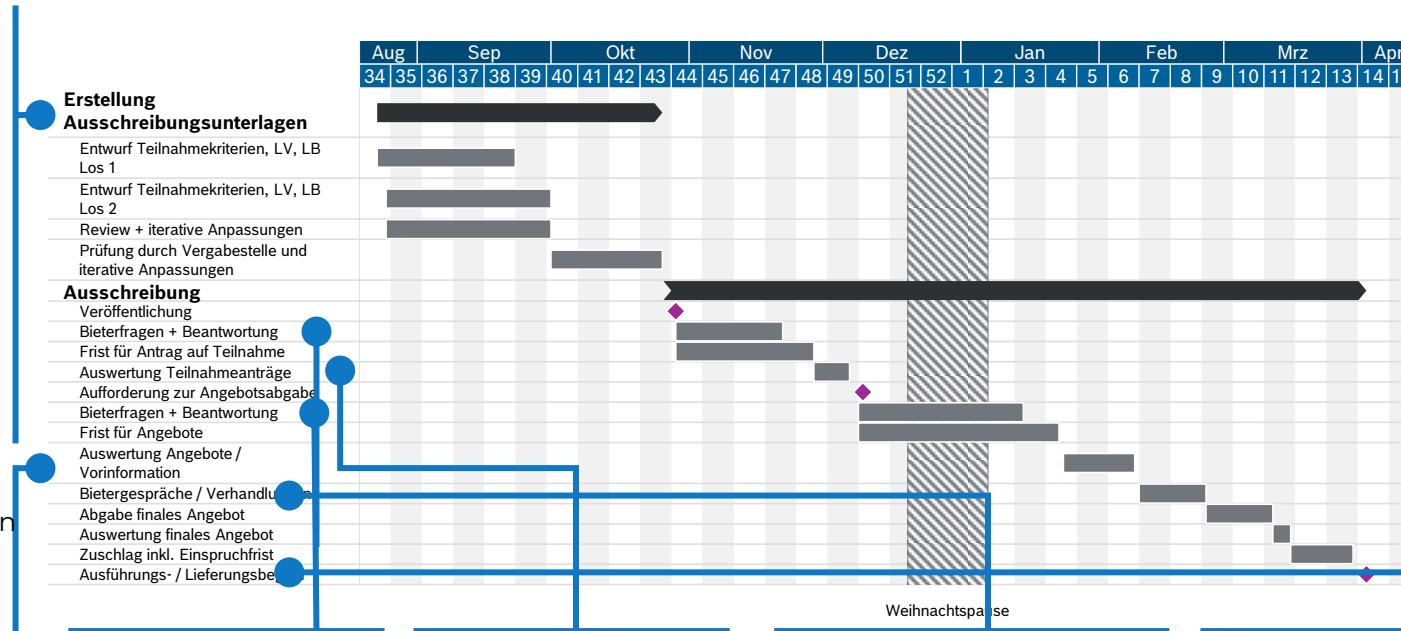
# Beispiel: Managed SOC RfP

## Executive Summary mit wesentlichen Entscheidungskriterien

Criteria	MSSP A	MSSP B	MSSP C	MSSP D	MSSP E	MSSP F
SOC analyst locations	EU country 1	EU country 2	EU country 3	Germany	Germany	Germany
# MSOC customers globally	200	200	400	350	50	Unclear
# MSOC customers in Germany	10	6	20	50	40	Unclear
Reaction time 365/24/7 for critical security incidents (start of L1 triage)	15 min	15 min	30 min	30 min	30 min	45 min
<b>Fulfilment functional criteria</b>	<b>93%</b>	<b>95%</b>	<b>92%</b>	<b>83%</b>	<b>88%</b>	<b>68%</b>
<b>Budget indications, TEUR</b>						
<b>MSOC 3 years</b>	500	1800	1700	2000	2800	1100
<b>MSOC 5 years</b>	1000	2800	2700	3100	4400	1800
<b>MSOC + IR 3 years</b>	700	2000	1800	2100	2900	1100
<b>MSOC + IR 5 years</b>	1200	3200	2800	3300	4600	1900
Main cost drivers	Alerts	Alerts	Log volume, endpoints	Log volume, endpoints, activated Defender modules	Log volume, endpoints and users	M365 E5 users
Price/performance ratio	★★★★★	★★★★☆	★★★★☆	★★★☆☆	★★★☆☆	★★★★☆
Comments	Best price performance ratio (fair for SOC location). ...	Necessary enhancement ...	Good alternative, strong security operations base ...	...	Most expensive offer, but ...	Not good fit for customer specific requirements in this case, as...

# Wir unterstützen bei öffentlichen Ausschreibungen – u.a. aktuell bei Europas größtem Cybersecurity-Beschaffungsprojekt

- Zielkonzept
- Leistungsbeschreibung, Bewertungsmatrix, Mindestanforderungen für ein Verhandlungsverfahren oder öffentliche Ausschreibung
- Eignungskriterien und Bewertungskriterien für Teilnahmewettbewerbe
- Weitere Ausschreibungsdokumente
- Abstimmung mit Einkauf, Vergabestelle und Fachabteilungen
- Auswertung der Angebote mit Bewertungsmatrix, Angebotsdokumenten und Prüfung von Anlagen
- Transparente Aufbereitung von kritischen Punkten
- Vorbereitung der Bietergespräche und Verhandlungen



- Fachliche Beantwortung von Bieterfragen
- Abstimmung mit der Vergabestelle
- Auswertung des Teilnehmeartrags mit Anlagen und Referenzen in Abstimmung mit der Vergabestelle
- Vorbereitung und Moderation (falls gewünscht) der Bietergespräche
- Bei Bedarf: Projektmanagement der Implementierung, von PoCs oder weiteren nachgelagerten Stufen

> 100 Referenzprojekte mit öffentlichen Auftraggebern

# Beispiel Heat Map zur Evaluierung von ~30 MSSPs (outside-in und auf Basis von Anbieter-Interviews)

RfP für Managed Security Services

Possible MSSP	Estimated size (FTE)	1000	4000	75	150	150	300	1500	110	1000	40 / 250	50	570	2000	60	3500	600	330	security	500	2000	2000	800	4000	6000	> 1000 (250)	2000	>10000	5000	
Locations		Germany, France, UK	Europe, US	Germany	Germany, Austria	Germany	Germany, Austria	Germany, US	Germany	Germany	Germany, Austria	UK, Greece	Global with HO	Germany	Austria	Global	Global, UK	Germany	Europe	EU, BR	Global	Global	Germany, Austria	CH	Global	Global	Global	Global	Global	Global
Capacity + footprint	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0	1	0.5	0.5	1	0.5	1	0.5	1	0.5	1	1	1	1	1	1	1	1	1
Customer focus/visibility	1	0	0.5	0.5	0.5	1	1	1	0.5	0.5	0.5	0.5	1	0.5	1	0.5	1	1	0.5	1	0.5	1	1	1	0	0.5	0	0.5	0.5	1
Reference VS-NID / NATO restricted customers	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
MS Defender for Endpoints	1	0	0	0.5	0	0.5	0.5	1	0.5	0.5	1	1	1	1	1	1	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Azure Sentinel S/EM	1	0	0	0	0	0.5	0	0.5	1	0.5	0.5	1	0.5	0.5	1	1	1	0.5	0.5	1	1	1	0.5	1	1	1	1	1	1	1
MS Azure Defender vulnerability management	1	0	0	0	0	0.5	0	0.5	1	0.5	0.5	1	0.5	0.5	1	1	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Azure Identity Protection	1	0	0	0	0	0	0	0.5	1	0.5	0.5	1	1	0	0.5	1	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Defender for IoT	1	0	0	0	0	0	0	0.5	0.5	0.5	0.5	0.5	1	0.5	0	1	0.5	0.5	0.5	1	1	1	0.5	1	1	1	1	1	1	1
MS Azure AD operation	1	0	0	0	0	0.5	0	0.5	0.5	0.5	0.5	1	1	2	0.5	1	1	2	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Key Vault cloud certificate management	1	0	0	0	0	0	0	0.5	0.5	0.5	0.5	1	0.5	0	0	0.5	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Application proxy	1	0	0	0	0	0	0	0.5	0.5	0.5	0.5	1	0.5	0	0	0.5	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Web App Gateway WAF	1	0	0	0	0	0	0	0.5	0.5	0.5	0.5	1	0.5	0	0	0.5	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Azure Front Door WAF	1	0	0	0	0	0	0	0.5	0.5	0.5	0.5	1	0.5	0.5	0	0.5	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
MS Information Protection (MIP) Data Classification	1	0	0	0	0	0	0	0.5	0.5	0.5	0.5	1	0.5	0.5	0	0.5	1	0.5	1	1	1	1	0.5	1	1	1	1	1	1	1
Cofem	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0.5	0	0	0	0	0	0.5	0.5	0.5	0.5	0.5	0.5
Dankr	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	2	0.5	0	0	0.5	0.5	0.5	0.5	0.5	0.5	0.5
McAfe	1	0	0	0	0	0.5	0	0	0	0	1	0	0	0	0	0	0	0.5	0.5	0	0	0.5	1	0	0.5	1	0.5	0.5	0.5	2
Proxy	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	2	0.5	0	0.5	0	1	0.5	0.5	1	0.5	0.5	0.5	1
CASB	1	0	0.5	0	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0.5	1	2	0	0.5	0	0.5	0	0.5	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0	0.5	1	2	0	0.5	0	0.5	1	0
Secur	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Oned	1	0	0	0	2	0.5	0	0	0	0	0.5	0	0	0	0.5	0	0	2	0.5	0	0.5	1	1	0.5	1	1	1	0.5	2	1
Tenab	1	0	0	1	0	0	1	1	0	1	0.5	1	1	1	1	1	1	0.5	1	0	1	1	1	1	1	1	1	1	1	1
FortiG	1	0	1	0	0	0	1	1	0	0	1	0	2	0	1	0	0	0	0.5	0.5	0	0	1	1	0.5	0.5	1	0.5	1	1
FS Big	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0.5	0.5	0	0	1	1	0.5	0.5	1	0.5	1	1
FS VP	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0.5	0.5	0	0	1	1	0.5	0.5	1	0.5	1	1
NSXT	1	0	0	0	0	1	0	0	0	0	1	0	0.5	0.5	0	0	1	0	0	0	0	0.5	1	1	1	1	0.5	1	1	1
Guard	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0.5	1	1	1	1	0
Boldo	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0	0.5	0	0	0	0	0	0	0	0.5	0.5	0.5	0.5	0.5	0.5
Indicative score outside-in		2.5	2.5	3.5	4	4	6	10	10.5	10.5	12.5	14	14	10.5	12	14	16.5	16.5	17	17.5	18.5	20	20.5	21.5	22.5	22.5	24.5	24.5	27	27.5
Comments		Managed SOC, IR, MDR, own products, Airbus uses Google office products	Quadar SIEM, Trend Micro Managed SOC/MDR, IR, vuln mgmt, Fortinet Firewall as a service, WAF/DDoS/CASB as a	Managed SOC, MDR, Tenable, LogPoint, Incident response, vuln mgmt	IAM / PAM operation s, BeyondTru st, Impriativa, Okta, Ping, Onedentit y, SailPoint	Micros oft, Identity + Access Management	Managed SOC auch für OT, Cloud, DDoS, vulnerability mgmt, managed firewall, IAM, patch mgmt, own security	Fortinet, Managed SOC also for OT, vuln mgmt, IR, managed EDR/NDR based on Micros oft, but also other vendors	Managed SOC (CrowdStrike or Micros oft Defender), Incident Response, Zscaler, own products	Managed security services, security outsourcing, vuln mgmt, industrial network monitoring, Micros oft, own products, Myra,	Managed Network & Security, e.g. Web Filter, Proxy Server, Firewalls, AV	Micros oft partner, SOC also for OT, vuln + asset mgmt, IAM	Managed SIEM, firewall, MDR, IAM, Email, vulnerability mgmt, Splunk, Palo Alto, NetApp, Micros oft,	MSOC based on Quadar SIEM, Incident response, MS gold partner, consulting, IAM/firewall/WAF/v uln mgmt, CISO as a service, Micros oft gold,	Managed SOC/MDR, Incident response, Managed infrastruct ure, Azure Sentinel, Azure SQL, Azure WAF, Splunk, Crowdstr	Managed SOC/MDR based on Azure Sentinel, also for OT, Vuln mgmt,	MDR/MS OC based on Micros oft (MISA) Defender Suite, Azure Sentinel, IAM, PKI, AV	Managed security services, cloud + hosting, Micros oft, VEEAM, Nutanix, Palo Alto	Micros oft based MDR, SIEM Splunk, Managed IAM, PKI, PAM	Managed operations, Cloud, Micros oft security, AWS, Trend Micro, Pixler, Sophos, Okta, Bitdefend er, Arcsight, Quadar,	SOC based on IMS tech, IAM, Okta, SailPoint	Managed services, SOC/MDR also for OT, secure infrastruc ture, managed firewall, IAM, WAF/DDoS, S, vulnerability mgmt,	Managed security services, vulnerability mgmt, MDR, log analysis, FS, Checkpoi nt, Symantec, Fortinet, Micros oft, Onedentit y,	MDR also for OT/ICS based on Micros oft suite, Managed vulnerability scanning, FS, Cisco, Fortinet, LogRhythm, Palo Alto Networks	MSOC/MDR also for OT, based on Azure Sentinel; all managed services (oper ations incl. IAM/PAM, CrowdStrike, Micros oft, CyberArk, Okta, Sailpoint,	Managed SOC/MDR also for OT, CERT, IAM, PAM, PKI, managed infrastruc ture, Micros oft, AWS, McAfee,	Managed Services in all categories, SOC with German speaking analysts, also for OT, MDR (Cynet, Micros oft, Crowds trike), Secure infrastruc ture, Managed	SOC/MD R, Vulnerability mgmt, incl. update/pa s toh mgmt, managed WAF, network FW, DLP ...	Managed security services in all categories (IAM, SOC/SIEM, Threat Hunting, Incident Response, Vulnerability Managem	Managed security services in all categories (IAM, SOC/SIEM, Threat Hunting, Incident Response, Vulnerability Managem

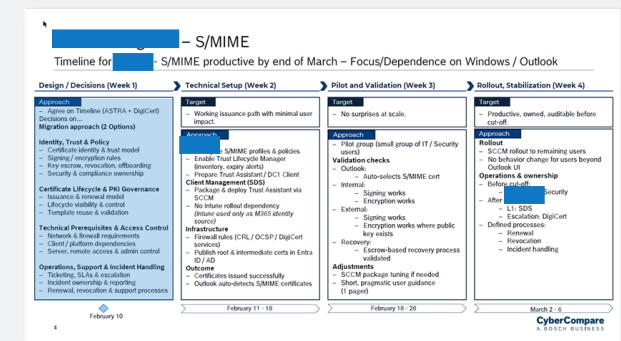
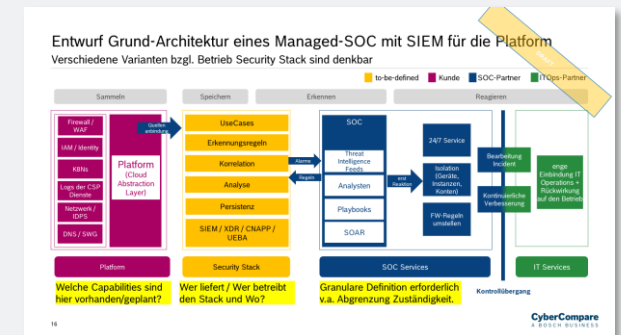
# Typische Fragestellungen – ein paar Beispiele

- SIEM / NDR on premise vs. Cloud bei KRITIS
- XDR vs. SIEM / MDR vs. MSOC
- Architekturen + Betriebskonzepte von SOC, PKI, Logmanagement oder Backup & Recovery-Systemen
- Skalierbare Segmentierung (SASE/ZTNA vs. Firewalling, NAC etc.) bei IT/OT
- Schwachstellenmanagement: Prozesse + Orga
- Vergleich von „Breach Warranties“ + Incident Response Service Level
- NIS-2 Management Schulungen

Wir empfehlen, SIEM als SaaS (vs. on prem) zuzulassen, um ein besseres Preis-/Leistungsverhältnis zu erreichen

Aspekt	Begründung für Empfehlung, auch SIEM als SaaS-Lösungen zuzulassen
Vorbereitung	<ul style="list-style-type: none"> <li>Auch bei anderen Betreibern kritischer Infrastruktur sind SIEM als SaaS inzwischen verbreitet, auf premise ist nicht mehr zwingend notwendig. Kein Präzedenzfall durch SWD</li> </ul>
Informations-sicherheits- und Datenschutz-Risiken	<ul style="list-style-type: none"> <li>Je nach Risiko und Bedrohung kundenspezifisch unterschiedlich, aber insgesamt nicht systematisch höher (s. auch Folienanhang)</li> </ul>
Post-Breach Incident Response (Reaktion bei einer Internetverbindung)	<ul style="list-style-type: none"> <li>Wahrscheinlicher Vorfall für IR mit on premise SIEM bei Ausfall der kompletten Internetverbindung, s. auch Stellungnahme ... (Premise CPHI hingegen zeitlicher bei Cloud SIEM)</li> <li>Dieser Vorteil wird bei ... jedoch abgefragt durch ... EDR on premise, OT NIDS on premise sowie Malware ... sowie generell durch lokale Puffer der Logdateien</li> <li>Grundsätzlich bei Cloud SIEM geringeres Risiko, dass auch SIEM-Server infiziert werden</li> </ul>
Auswahl an Anbietern	<ul style="list-style-type: none"> <li>On prem / Hybrid: 7 (Splunk, IBM Guard, Logpoint, Elastic, Wazuh, LogRhythm/Exabeam, Trend) / Cloud only: 4 (Microsoft Sentinel, Palo Alto, Google, CrowdStrike)</li> <li>Insbesondere der Ausschuss von Microsoft würde zu Einschränkung auf MSSP-Dienstleister führen, während ... bereits MSSP nutzt</li> </ul>
Betriebsaufwand	<ul style="list-style-type: none"> <li>Einkaufspreis Skalierung über die eigenen Daten sowie über Kunden hinweg (MSSP-Preissetzung)</li> <li>Bei gleicher Verfügbarkeit und Performance Kosteneinsparung von 20-30% realistisch</li> </ul>

CyberCompare  
A BUCH BUSINESS



# IT, Infosec und Compliance Projektleitung: Kundenprojekte (Beispiele)

1

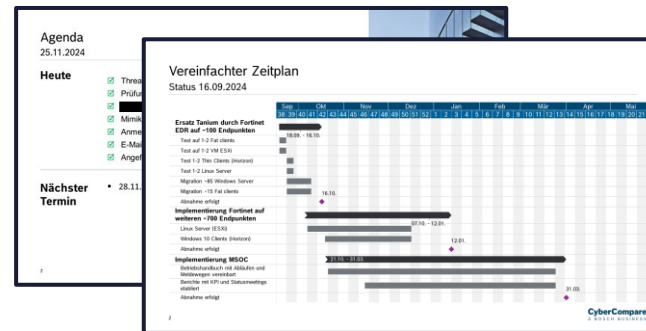
## Compliance Onboarding von Lieferanten u. Dienstleistern



- **Abstimmung** zwischen Fachabteilung, Einkauf, DSB, IT Security, externem Dienstleister etc.
- **Fachliche Prüfung von Security- und Compliance-Anforderungen** (z.B. Transfer Impact Assessment, AVV, Zertifizierungen) und bewährte Checklisten, wo hilfreich
- **Vorschläge zur pragmatischen Lösung** bei Nichterfüllung von Anforderungen
- **Auditsichere Dokumentation**
- **Stakeholdergerechte Unterlagen** z.B. für Betriebsrat

2

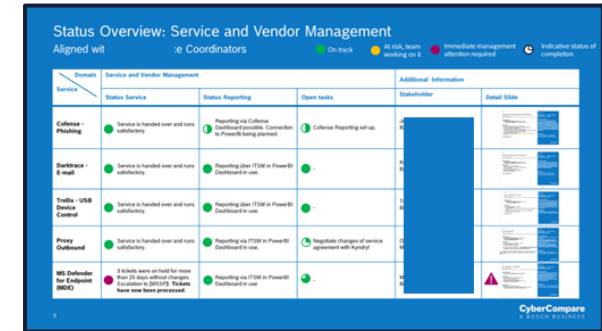
## Einführung neuer Security-Tools und –Prozesse (z.B. Managed SOC)



- **Projektmanagement auf Kundenseite**
- Organisation von **Regelmeetings und Updates für das Leitungsgremium**
- **Nachverfolgung** von Maßnahmen
- **Rechnungs- und Leistungsprüfung**
- **Entscheidungsvorlagen** z.B. bei Problemen wie Inkompatibilitäten **auf Basis marktüblicher Vorgehensweisen**

3

## Vendor-/Service- und 3rd Party Risk Management



- **Koordination von Transition und Neueinführung von Managed Services**
- Prüfung von Verträgen und **Leistungsscheinen (SLA)**
- Aufbau von **KPI-basiertem Service Mgmt.**
- **Verhandlung von Änderungen** (z.B. Anzahl Tickets), die nach Vertragsschluss notwendig sind
- Etablierung **3rd Party Risk Management**

# CyberCompare

Always a good decision



[www.cybercompare.com](http://www.cybercompare.com)



[contact@cybercompare.com](mailto:contact@cybercompare.com)

[jannis.stemann@cybercompare.com](mailto:jannis.stemann@cybercompare.com)