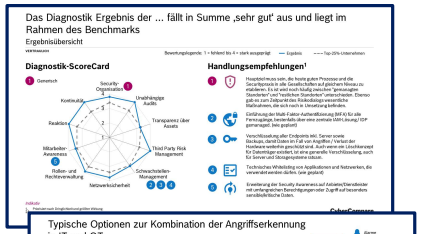
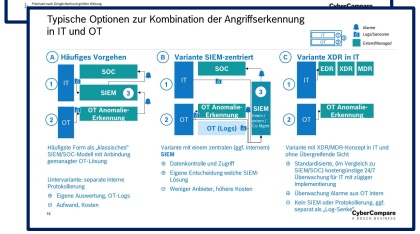

Immer eine gute
Security Entscheidung
CyberCompare
Always a good decision

Wir sind Security-Architekten und übernehmen Verantwortung von Strategie über Anbieterauswahl bis Einführung und Interims-Management

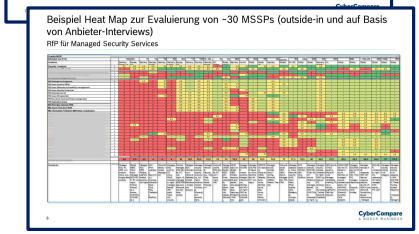
Projektmanagement

1 Strategie, Gap-Assessments, Architekturen und Roadmaps

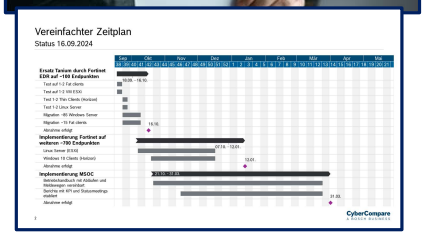




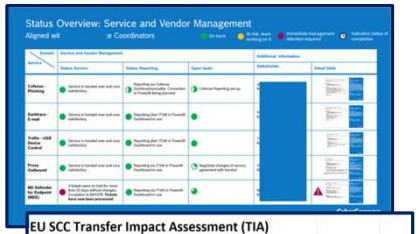
2 Angebotsvergleiche + Ausschreibungen

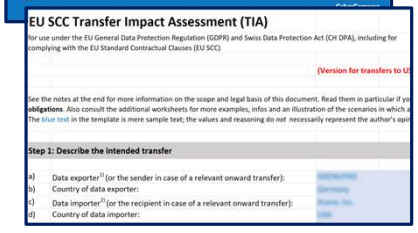


3 Implementierung, Compliance, Transition



4 Einführung, Vendor / Service und 3rd Party Risk Mgmt.





CyberCompare
Always a good decision

Unser Ansatz: 100% Unabhängigkeit

Eigene Produkte oder Managed Services

0

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

0

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

>450

Unternehmenskunden und öffentliche Stellen

>700

IT-, OT- und IoT-Security Projekte

Prof. Dr. Petra Maria Asprion
Leiterin Kompetenz-schwerpunkt Cyber-security & Resilience,
FH Nordschweiz

Benjamin Bachmann
CISO,
Bilfinger SE

Florian Brandner
Global Information & Cybersecurity Director,
PUMA

Dr. Daniel Brettschneider
CISO,
Miele & Cie. KG

Dr. Christoph Peylo
Chief Cybersecurity Officer,
Robert Bosch GmbH

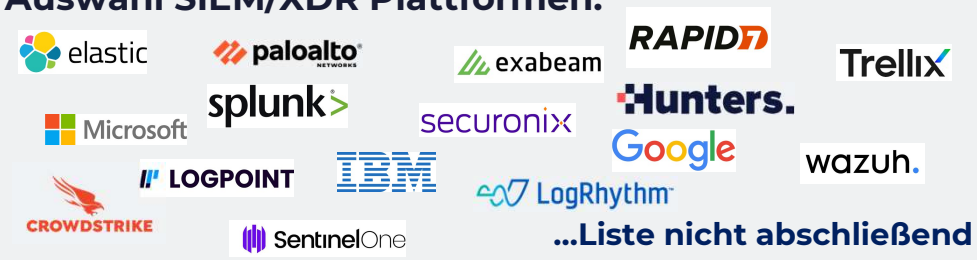
Stefan Würtemberger
Executive Vice President IT,
Marabu GmbH & Co. KG


Cybersecurity-Anbieter, Beratungsunternehmen, Managed Service Provider und Reseller
~7000
Anbieter im Cybersecurity Jungle
Der Umsätze bei Anbietern werden für Marketing und Vertrieb ausgegeben
~40%
des Anbieter Budgets

Managed SIEM / SOC

Auswahl SOC Anbieter:

Auswahl SIEM/XDR Plattformen:



...Liste nicht abschließend

Über 60 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**

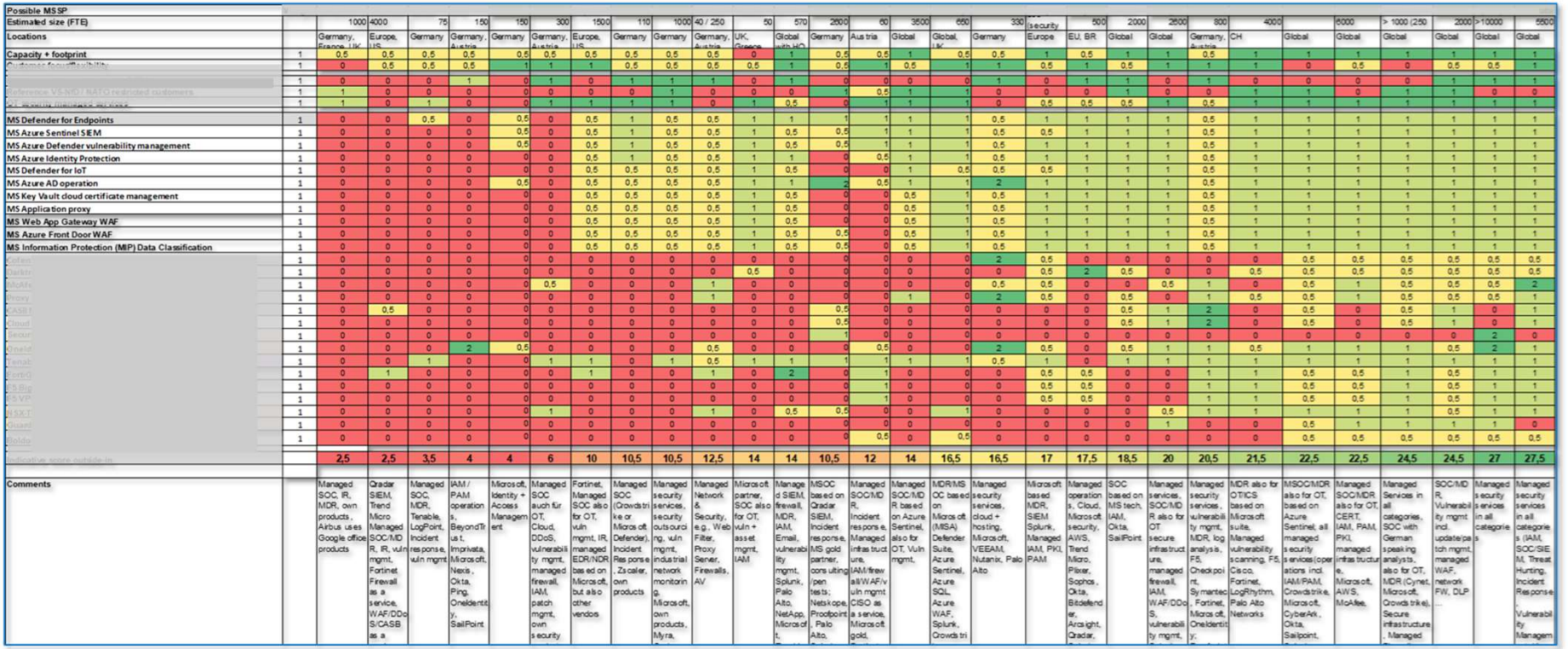
SIEM-Marktstudie über 13 Vendoren inkl. RfI für DAX-Konzern. Detail-Bewertung im Rahmen von Compare-Days

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

Beispiel: Managed SOC RfP

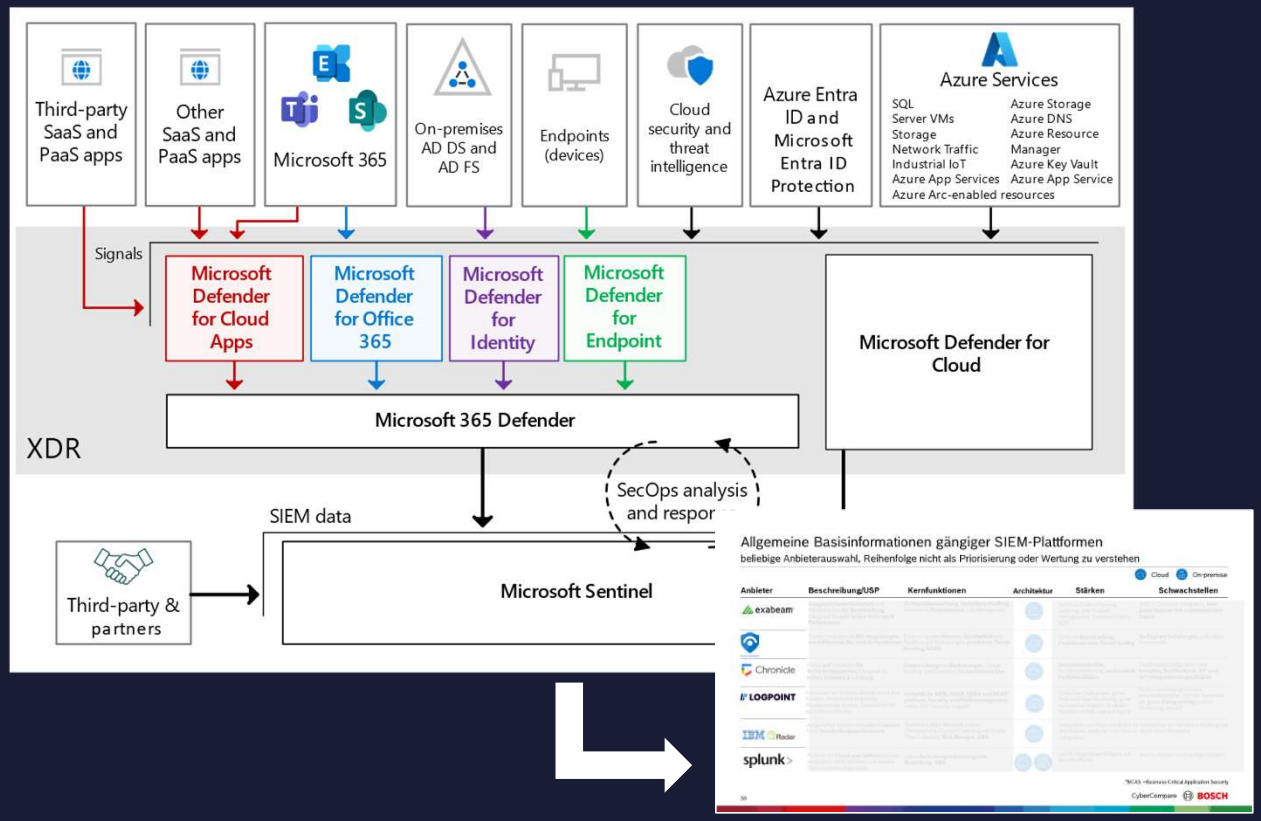
Criteria	MSSP A	MSSP B	MSSP C	MSSP D	MSSP E	MSSP F
SOC analyst locations	EU country 1	EU country 2	EU country 3	Germany	Germany	Germany
# MSOC customers globally	200	200	400	350	50	Unclear
# MSOC customers in Germany	10	6	20	50	40	Unclear
Reaction time 365/24/7 for critical security incidents (start of L1 triage)	15 min	15 min	30 min	30 min	30 min	45 min
Fulfilment functional criteria	**93%**	**95%**	**92%**	**83%**	**88%**	**68%**
Budget indications, TEURv						
MSOC 3 years	500	1800	1700	2000	2800	1100
MSOC 5 years	1000	2800	2700	3100	4400	1800
MSOC + IR 3 years	700	2000	1800	2100	2900	1100
MSOC + IR 5 years	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...

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



Possible MSSP																														
Estimated size (FTE)		1000	4000	75	150	150	300	1500	110	1000	40 / 250	50	570	2600	60	3500	650	330	security	500	2000	2600	800	4000		6000	> 1000 (250	2000	>10000	5500
Locations		Germany, France, UK	Europe, UK	Germany	Germany, Austria	Germany	Germany, Austria	Europe, UK	Germany	Germany	Germany, Austria	UK, Greece	Global with HQ	Germany	Austria	Global	Global, UK	Germany	Europe	EU, BR	Global	Global	Global	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	0,5	1	0,5	1	1	0,5	1	1	1	1	1	1	1
[illegible]	1	0	0,5	0,5	1	1	1	0,5	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
[illegible]	1	0	0	0	1	0	1	0	1	1	1	0	1	0	0	0	0	1	0	1	1	0	1	0	0	0	0	1	1	1
[illegible]	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0,5	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0
[illegible]	1	1	0	1	0	0	1	1	1	1	0	1	0,5	0	1	1	1	0	0,5	0,5	0,5	1	0,5	1	1	1	1	1	1	1
MS Defender for Endpoints	1	0	0	0,5	0	0,5	0	0,5	1	0,5	0,5	1	1	1	1	1	1	0,5	1	1	1	1	0,5	1	1	1	1	1	1	1
MS Azure Sentinel SIEM	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	1	0,5	0	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	0,5	0	0,5	0,5	0,5	0,5	1	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
[illegible]	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0,5	0	0	0	0	0,5	0,5	0,5	0,5	0,5	0,5
[illegible]	1	0	0	0	0	0	0	0	0	0	0	0,5	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
[illegible]	1	0	0	0	0	0	0,5	0	0	0	1	0	0	0	0	0	0	0	0,5	0,5	0	0,5	0	1	0	0,5	1	0,5	0,5	2
[illegible]	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	2	0,5	0	0,5	0	1	0,5	0,5	1	0,5	0,5	1
[illegible]	1	0	0,5	0	0	0	0	0	0	0	0	0	0,5	0	0	0	0	0	0	0	0	0,5	1	2	0	0,5	0	0,5	1	1
[illegible]	1	0	0	0	0	0	0	0	0	0	0	0	0,5	0	0	0	0	0	0	0	0	0,5	1	2	0	0,5	0	0,5	1	1
[illegible]	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	0
[illegible]	1	0	0	2	0,5	0	0	0	0	0,5	0	0	0	0,5	0	0	0	2	0,5	0	0,5	1	1	0,5	1	1	1	0,5	2	1
[illegible]	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
[illegible]	1	0	1	0	0	0	1	0	0	1	0	2	0	1	0	0	0	0	0,5	0,5	0	0	1	1	0,5	0,5	1	0,5	1	1
[illegible]	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0,5	0,5	0	0	1	1	0,5	0,5	1	0,5	1	1
[illegible]	1	0	0	0	0	1	0	0	0	0	1	0	0,5	0,5	0	0	1	0	0,5	0,5	0	0	1	1	1	1	1	0,5	1	1
[illegible]	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	Qradar 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 operations, BeyondTrust, Imprivata, Microsoft, Nexis, Okta, Ping, Oneldentity, SailPoint	Microsoft, Identity + Access Managem ent	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 Microsoft, but also other vendos	Managed SOC (Crowdstrike or Microsoft Defender), Incident Response, Zscaler, own products	Managed security services, security outsourcing, vuln mgmt, industrial network monitoring, Microsoft, own products, Myra,	Managed Network & Security, e.g., Web Filter, Proxy Server, Firewalls, AV	Microsoft partner, SOC also for OT, vuln + asset mgmt, IAM	Managed SIEM, firewall, MDR, IAM, Email, vulnerability mgmt, Splunk, Palo Alto, NetApp, Microsoft,	MSOC based on Qradar SIEM, Incident response, MS gold partner, consulting/pen tests; Netskope, Proofpoint, Palo Alto,	Managed SOC/MDR, Incident response, Managed infrastructure, IAM/firewall/WAF/vuln mgmt CISO as a service, Microsoft gold,	Managed SOC/MDR based on Azure Sentinel, also for OT, Vuln mgmt,	MDR/MSOC based on Microsoft (MISA) Defender Suite, Azure Sentinel, Azure SQL, Azure WAF, Splunk, Crowdstri	Managed security services, cloud + hosting, Microsoft, VEEAM, Nutanix, Palo Alto	Microsoft based MDR, SIEM Splunk, Managed IAM, PKI, PAM	Managed operations, Cloud, Microsoft security, AWS, Trend Micro, Plixer, Sophos, Okta, Bitdefender, Arcsight, Qradar,	SOC based on MS tech, IAM, Okta, SailPoint	Managed services, SOC/MDR also for OT secure infrastructure, managed firewall, IAM, WAF/DDoS, vulnerability mgmt,	Managed security services, vulnerability mgmt, MDR, log analysis, F5, Checkpoint, Symantec, Fortinet, Microsoft, Oneldentity;	MDR also for OT/ICS based on Microsoft suite, Managed vulnerability scanning, F5, Cisco, Fortinet, LogRhythm, Palo Alto Networks	MSOC/MDR also for OT, based on Azure Sentinel, all managed security services/operations incl. IAM/PAM, Crowdstrike, Microsoft, CyberArk, Okta, Sailpoint,	Managed SOC/MDR also for OT, CERT, IAM, PAM, PKI, managed infrastructure, Microsoft, AWS, McAfee,	Managed Services in all categories, SOC with German speaking analysts, also for OT, MDR (Cynet, Microsoft, Crowdstrike), Secure infrastructure, Managed	SOC/MDR, Vulnerability mgmt incl. update/patch mgmt, managed WAF, network FW, DLP, ...	Managed security services in all categories	Managed security services in all categories (IAM, SOC/SIEM, Threat Hunting, Incident Response, Vulnerability Managem

Marktrecherche Microsoft- und Cloud-Security



Ausgangslage:

- Unternehmen > 100.000 MA mit Microsoft Strategie
- Auftrag: differenzierenden Fähigkeiten und sinnvolle Alternativen erarbeiten

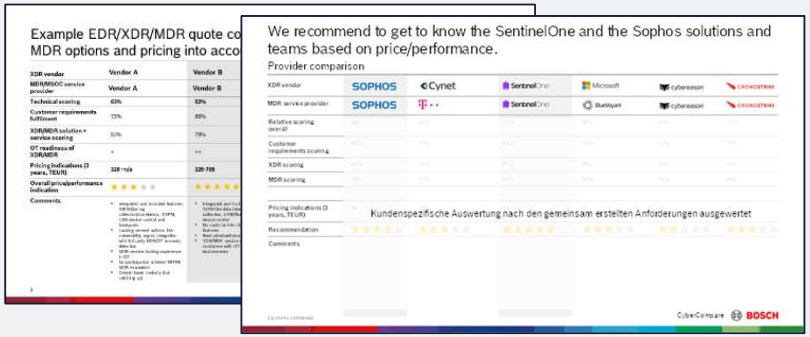
Erkenntnisse: (vereinfacht)

- Smarter Lizensierungsansatz und gute Positionierung bei der GF
- MS stark in Azure - Lücken in Multi-Cloud Strategie (Bsp. MS Cloud Vuln. Mgmt). Analog Herausforderungen bei diverser onPrem Umgebung (z.B. Linux)
- Cloud-Security Lösungsmarkt noch fragmentierter als IT-Sec mit vielen „Nischen-Tools“
- Starke Marktdurchdringung v.a. von MS Defender und Sentinel sorgt für Neupositionierung vieler MSSP

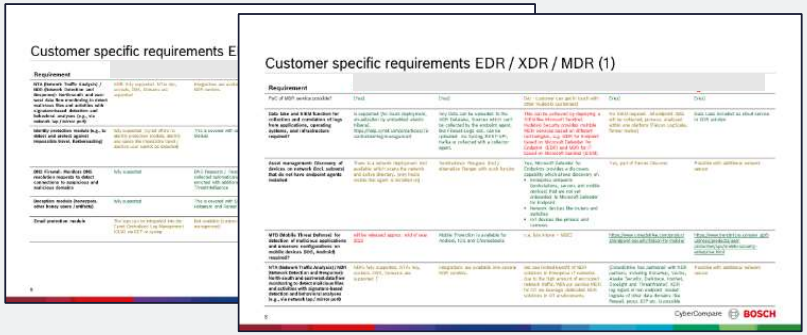
Quelle: https://learn.microsoft.com/de-de/security/operations/siem-xdr-overview

Empfehlungen basieren auf inhaltlichen, technischen und kommerziellen Auswertungen, um optimale Entscheidung zu ermöglichen

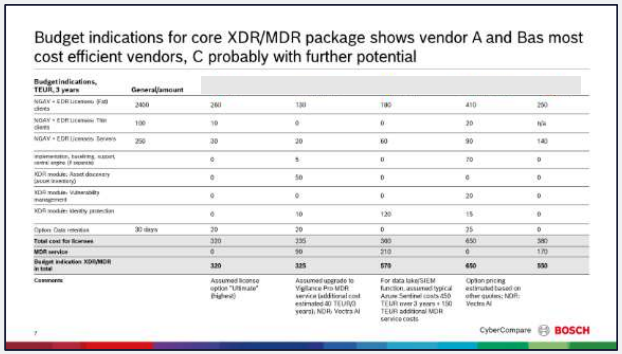
Management Summary



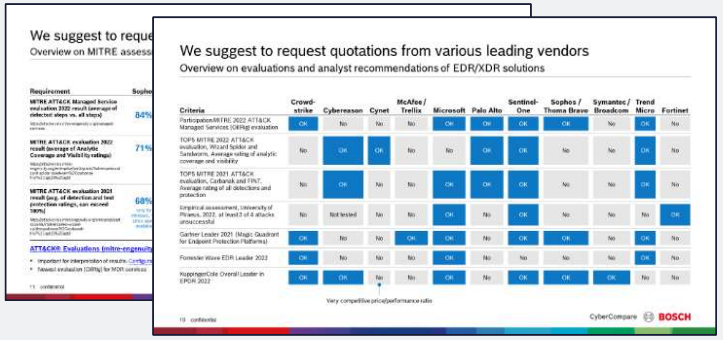
Erfüllung Anforderungen/ Leistungsbeschreibung



Kommerzielle Szenarien / TCO



Technische Bewertungen / CompareDays

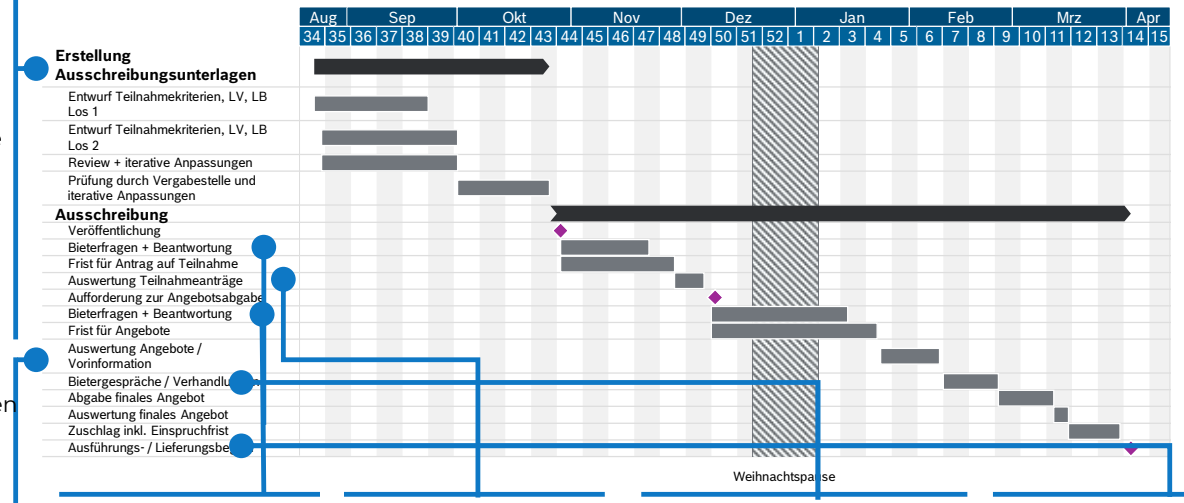


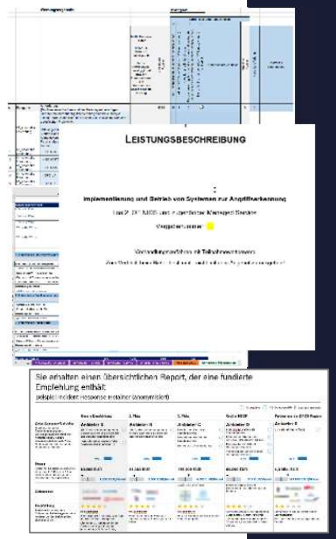
CyberCompare
Always a good decision

Wir unterstützen öffentliche Stellen bei Erstellung der Vergabeunterlagen, Auswertung von Angeboten und Ausschreibungsmanagement

- **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

> 50 Referenzprojekte mit öffentlichen Auftraggebern





- Fachliche **Beantwortung von Bieterfragen**
- Abstimmung mit der Vergabestelle

- **Auswertung des Teilnahmeantrags** mit Anlagen und Referenzen in Abstimmung mit der Vergabestelle

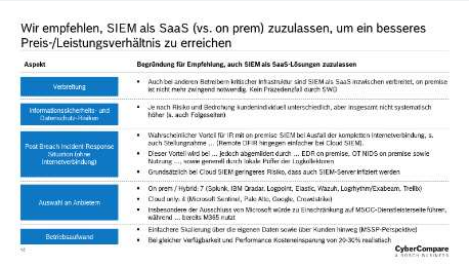
- **Vorbereitung und Moderation** (falls gewünscht) der Bietergespräche

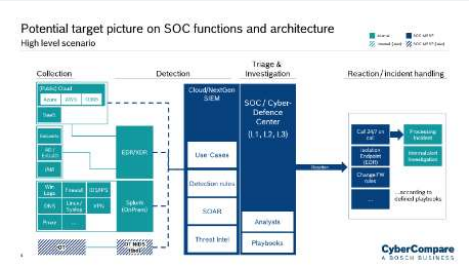
- Bei Bedarf: **Projektmanagement der Implementierung**, von PoCs oder weiteren nachgelagerten Stufen

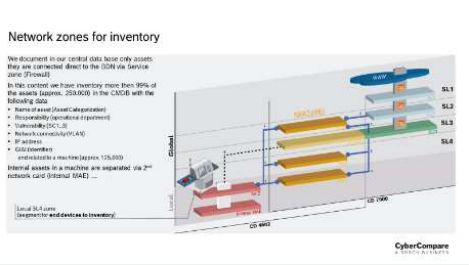
CyberCompare
Always a good decision

Typische Fragestellungen – ein paar Beispiele

- **SIEM on premise vs. Cloud bei KRITIS**
- **XDR vs. SIEM (MDR vs. MSOC)**
- **Betriebskonzepte**
- **Skalierbare Segmentierung (SASE/ZTNA vs. Firewalling, NAC etc.) bei IT/OT**
- **Schwachstellenmanagement: Prozesse + Orga**
- **Vergleich von MDR „Breach Warranties“**
- **Incident Response Service Level**
- **Vergleich von KI Assistenten bei SIEM/SOAR**







CyberCompare
Always a good decision

IT, Infosec und Compliance Projektleitung: Kundenprojekte (Beispiele)

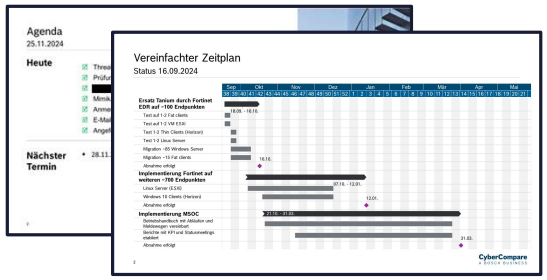
1

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

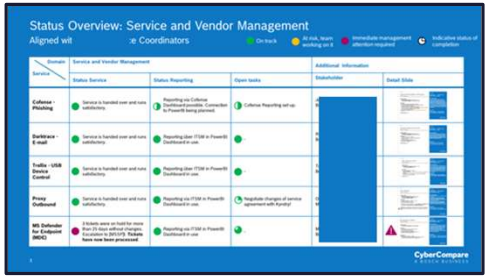
Einführung neuer Security-Tools und –Prozesse (z.B. Managed SOC)



- **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
jannis.stemmann@bosch.com