

The background is a 3D isometric grid of gray squares. A path of yellow stars starts from the right side and leads towards a taller square in the center-right area. The text "Always a good security decision" is overlaid on the left side of the grid.

Always a good security  
decision

**CyberCompare**  
Always a good decision

The diagram illustrates the project management process flow. It consists of a dark blue horizontal bar with a white arrow pointing to the right. Inside the bar, the text "Projekt management" is written in white. Below the bar, there are four numbered circles: 1, 2, 3, and 4, arranged from left to right. The circles are white with dark blue numbers. The bar is divided into four segments by thin white lines, with the text "Projekt management" centered in the second segment.

[illegible][illegible]

**Compliance**

- ☐ DSGVO
- ☒ ISO 27001
- ☐ EU AI Act
- ☒ ISO CS Testat
- ☐ DSGA
- ☒ TA AVV
- ☐ AVV
- ☐
- ☐

**Status Overview: Service and Vendor Management**

Aligned with Coordinators In review At risk (not aligned) Not implemented Not yet started / incomplete

	Business Services	Safeguards Reporting	Open issues	Additional Information	Overall Status
<b>a) Processing</b>	1. Standardized processing of personal data	2. Standardized processing of personal data	3. Standardized processing of personal data	4. Standardized processing of personal data	5. Standardized processing of personal data
<b>b) Collection</b>	1. Standardized collection of personal data	2. Standardized collection of personal data	3. Standardized collection of personal data	4. Standardized collection of personal data	5. Standardized collection of personal data
<b>c) Transfer to a third party</b>	1. Standardized transfer of personal data	2. Standardized transfer of personal data	3. Standardized transfer of personal data	4. Standardized transfer of personal data	5. Standardized transfer of personal data
<b>d) Retention and deletion</b>	1. Standardized retention and deletion of personal data	2. Standardized retention and deletion of personal data	3. Standardized retention and deletion of personal data	4. Standardized retention and deletion of personal data	5. Standardized retention and deletion of personal data
<b>e) Access and disclosure</b>	1. Standardized access and disclosure of personal data	2. Standardized access and disclosure of personal data	3. Standardized access and disclosure of personal data	4. Standardized access and disclosure of personal data	5. Standardized access and disclosure of personal data
<b>f) Other</b>	1. Standardized other processing of personal data	2. Standardized other processing of personal data	3. Standardized other processing of personal data	4. Standardized other processing of personal data	5. Standardized other processing of personal data

**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 U.S.)**

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 **aligning**. Also consult the additional worksheets for more examples, info and an illustration of the scenario in which to use the TIA tool. The **blue text** in the template is more sample text; the values and reasoning do not necessarily represent the author's opinion.

**Step 1: Describe the intended transfer**

- Data exporter<sup>1)</sup> (for the sender in case of a relevant onward transfer):
- Country of data exporter:
- Data importer<sup>2)</sup> (for the recipient in case of a relevant onward transfer):
- Country of data importer:

## Our approach: 100% independence

Own products or  
managed services

0

Reseller contracts, deal  
registration,  
commissions, kickbacks,  
referral fees, bonuses, or  
other project  
compensation from the  
vendor side

0

**If you are our customer, you are in good company**

**>450**

Corporate customers  
and public bodies

**>700**

IT, OT und IoT security  
projects



**Prof. Dr. Petra  
Maria Asprion**  
Head of Cyber security  
& Resilience,  
University of Applied  
Sciences  
Northern Switzerland



**Benjamin  
Bachmann**  
CISO,  
Bilfinger SE



**Florian  
Brandner**  
Global Information &  
Cybersecurity  
Director,  
PUMA



**Dr. Daniel  
Brettschneider**  
CISO,  
Miele & Cie. KG

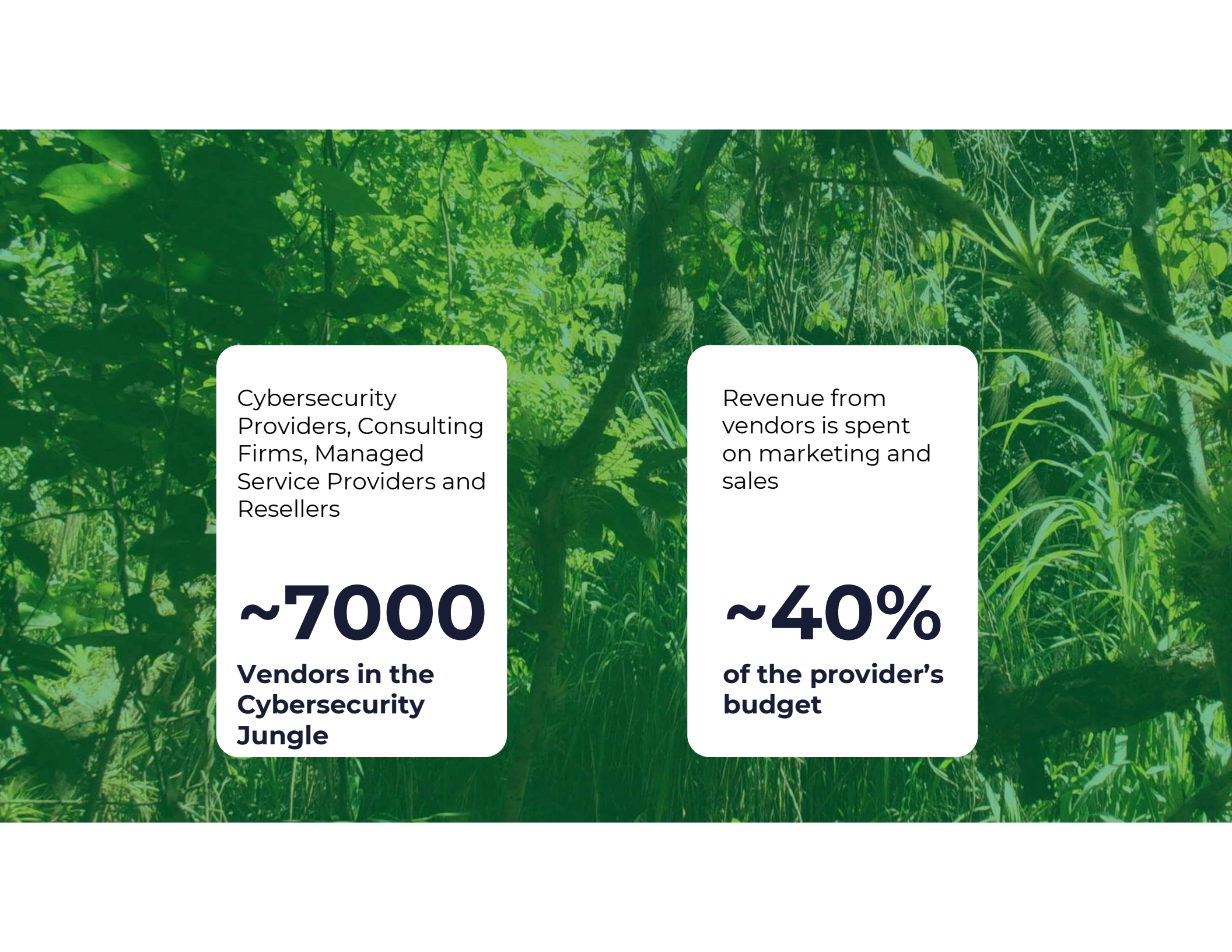


**Dr. Christoph  
Peylo**  
Chief Cybersecurity  
Officer,  
Robert Bosch GmbH



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





Cybersecurity  
Providers, Consulting  
Firms, Managed  
Service Providers and  
Resellers

**~7000**

**Vendors in the  
Cybersecurity  
Jungle**

Revenue from  
vendors is spent  
on marketing and  
sales

**~40%**

**of the provider's  
budget**

# Managed SIEM / SOC

## Selection of SOC vendors:



## Selection of SIEM/XDR platforms:



## Over 60 customer projects. Typical examples:

**KRITIS** Company: **Combined SIEM/SOC** project including connection of operations technology

Public **SOC** and **SIEM** tenders for hospitals, cities/municipalities, public transport, airports, ...

























**Industrial companies** with 9,000 employees: **Start with SIEM selection.** Focus on **Managed SOC** during the **course of the project**

**Medium-sized** company with 2,800 employees: Start of the **Managed SOC specification** – based on the initial situation, then **initially tender** for an **MDR** for **endpoint security**

**SIEM market study** on 13 vendors incl. RfI for DAX group. Detailed evaluation as part of Compare-Days

**Replacement** of current **Managed SOC** for industrial companies with approx. 20,000 employees **incl. SIEM solution**

## Example: 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
<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, TEURv</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...

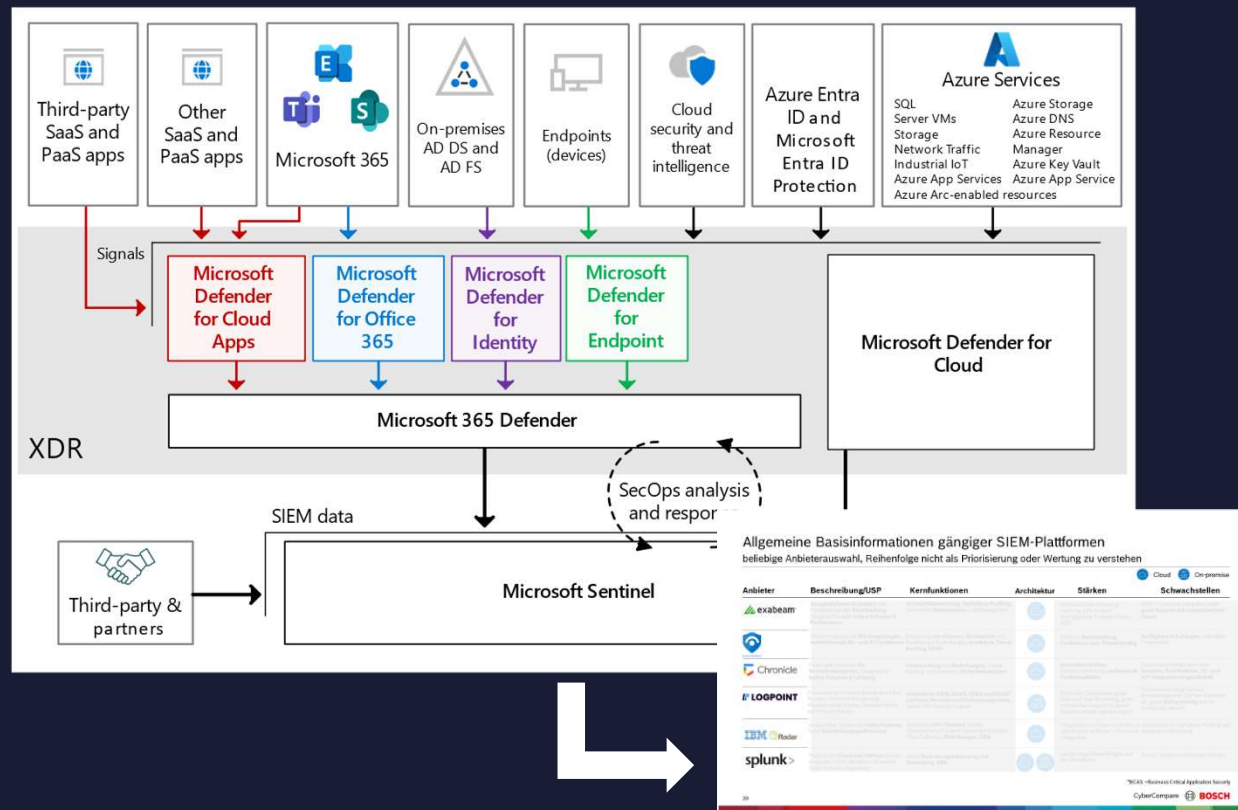


**Example heat map to evaluate ~ 30 MSSPs (outside-in and based on vendor interviews)**

Possible MSP			1000	4000	79	150	150	300	1500	110	1000	40 / 250	50	570	2600	80	3500	690	330	Security Europe	500	2000	2500	800	4000	6000	> 1000 / 250	2000	> 10000	5500
Locations			Germany, France, UK	Europe, UK	Germany	Germany	Germany	Germany	Europe, UK	Germany	Germany	Germany	UK, Germany	Global Sub-HC	Germany	Australia	Global	Global, UK	Germany	Europe	EU, BR	Global	Global	Germany, Australia	CH	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	0.5	1	1	1	1	1
Microsoft Azure Cloud Managed Services	1	0	0.5	0.5	0.5		1	1	1	0.5	0.5	0.5	0.5	1	0.5		0.5	1	1	0.5	1	0.5	1	1	1	1	0	0.5	0	0.5
Mitigation Vector Map or predicted outcomes	1	1	0	0	0	1	0	0	0	1	1	1	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1
All Microsoft products & services	1	1	0	0	1	0	0	1	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
MS Defender for Endpoints	1	0	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	1	0.5	1	1	1	1	1
MS Azure Sentinel SEM	1	0	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	1	0.5	1	1	1	1	1
MS Azure Defender vulnerability management	1	0	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	1	0.5	1	1	1	1	1
MS Azure Identity Protection	1	0	0	0	0	0	0	0.5	0.5	1	0.5	0.5	1	1	0	0.5	1	1	0.5	1	1	1	1	1	0.5	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	0	1	0.5	0.5	0.5	1	1	1	1	0.5	1	1	1	1	1
MS Azure AD operation	1	0	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	1	0.5	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	0.5	1	0.5	0	0	0.5	1	0.5	1	1	1	1	1	0.5	1	1	1	1	1
MS Application proxy	1	0	0	0	0	0	0	0.5	0.5	0.5	0.5	0.5	1	0.5	0	0	0.5	1	0.5	1	1	1	1	1	0.5	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	0.5	1	0.5	0	0	0.5	1	0.5	1	1	1	1	1	0.5	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	0.5	1	0.5	0	0	0.5	1	0.5	1	1	1	1	1	0.5	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	1	1	0.5	1	1	1	1	1
CyberArk	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	0.5	0.5	0.5	0.5	0.5
Datix	1	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0.5	2	0.5	0	0	0	0.5	0.5	0.5	0.5	0.5
Hobbit	1	0	0	0	0	0	0	0.5	0	0	0	0	1	0	0	0	0	0	0.5	0.5	2	0.5	0	0.5	1	0.5	0.5	0.5	0.5	2
Proxi	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	2	0.5	0	0.5	0	1	0.5	0.5	1	0.5	0.5	1
CASE F	1	0	0	0.5	0	0	0	0	0	0	0	0	1	0	0	0	0	0	2	0.5	0	0.5	0	1	0.5	0.5	1	0.5	0.5	1
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0.5	0	1	0.5	0.5	0.5	0.5	0.5	0.5
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0.5	1	2	0	0.5	0	0.5	1	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	2	0	0.5	0	0.5	1	0
Cloud	1	0	0	0	0	0	0.5	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0	0.5	1	0	0	0	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	1	0	0
Cloud	1</																													



# Market research Microsoft and cloud security



## Initial situation:

- Companies > 100,000 employees with Microsoft Strategy
- Mission: Develop differentiating skills and meaningful alternatives

## Insights: (simplified)

- Smart licensing approach and good positioning at GF
- MS strong in Azure - Gaps in multi-cloud strategy (e.g. MS Cloud Vuln. Mgmt). Analogous challenges in various onPrem environments (e.g. Linux)
- Cloud security solutions market even more fragmented than IT-Sec with many "niche tools"
- Strong market penetration, especially of MS Defender and Sentinel, leads to repositioning of many MSSPs

## Fulfilment of requirements/ service description

[illegible]

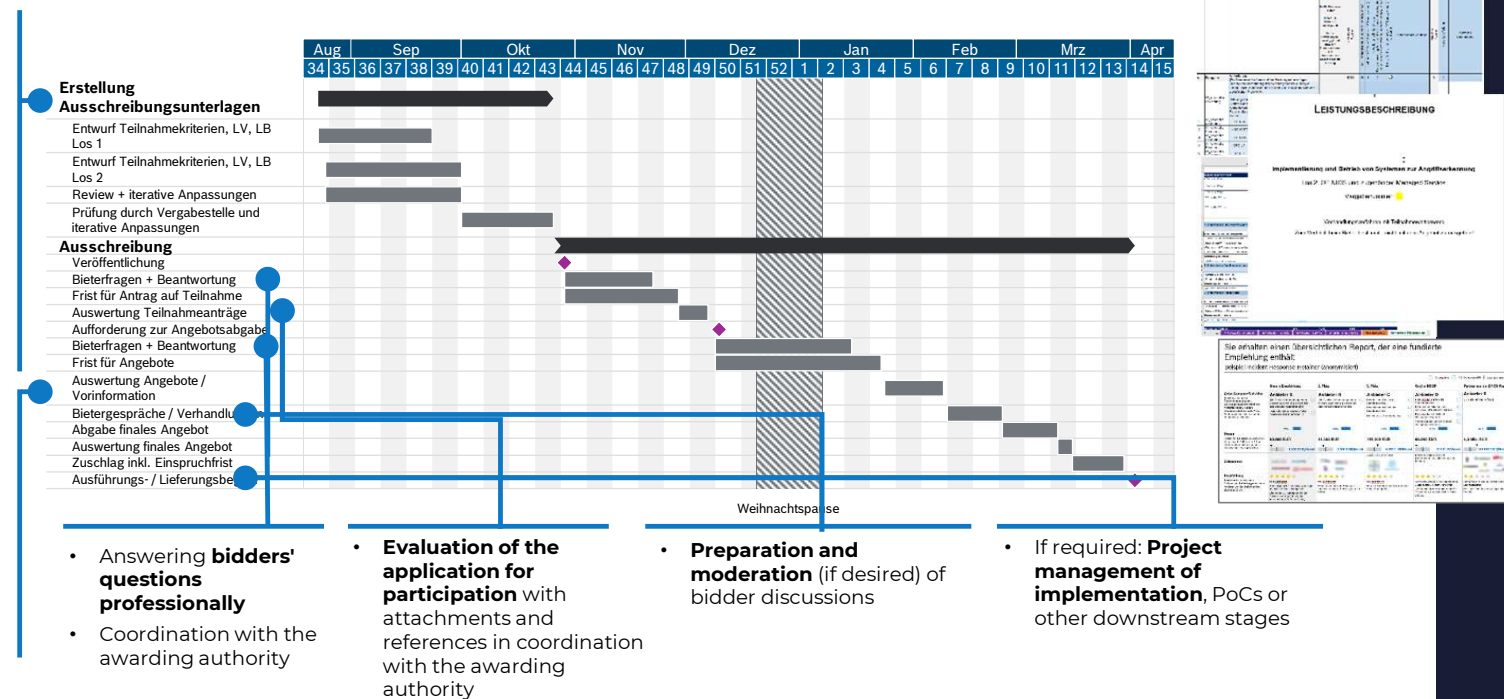
## Technical Reviews / CompareDays

[illegible]

# We support public authorities in the preparation of tender documents, evaluation of bids and tender management

- **Target Concept**
- **Specification, evaluation matrix, minimum requirements** for a **negotiated procedure** or public tender
- **Eligibility Criteria** and **Evaluation Criteria** for **Participation Competitions**
- Further tender documents
- **Coordination** with purchasing, awarding authority and specialist departments
- **Evaluation of bids** with evaluation matrix, bid documents and review of attachments
- **Transparent preparation** of critical points
- **Preparation of bidder meetings** and negotiations

> 50 reference projects with public clients



## Typical questions – a few examples

## SIEM on premise vs. Cloud bei KRITIS

## XDR vs. SIEM (MDR vs. MSOC)

## Operating concepts

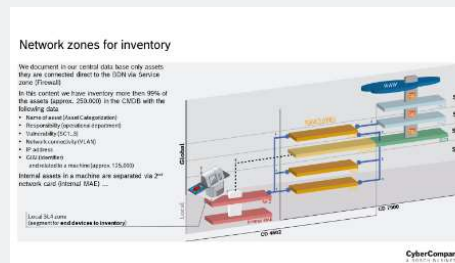
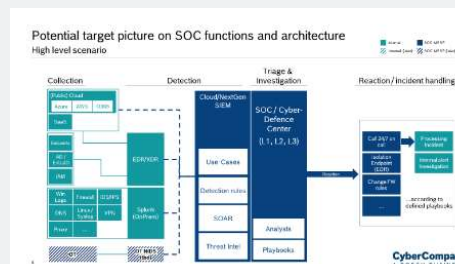
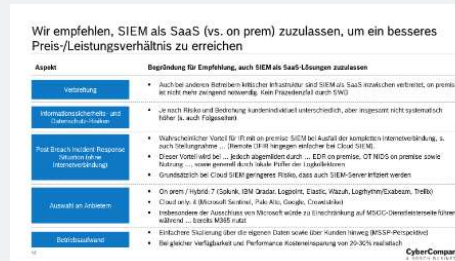
## Scalable segmentation (SASE/ZTNA vs. firewalling, NAC etc.) in IT/OT

## Vulnerability Management: Processes + Orga

## Comparison of MDR "Breach Warranties"

## Incident Response Service Level

## Comparison of AI assistants in SIEM/SOAR





# IT, Infosec and Compliance Project Management: Customer Projects (Examples)

1

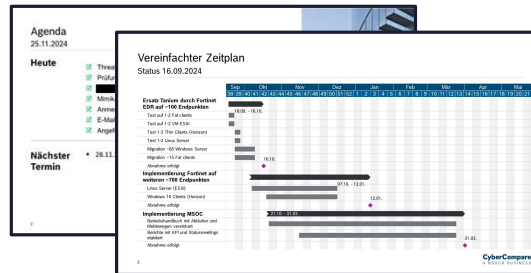
## Compliance Onboarding of suppliers and service providers



- **Coordination** between specialist department, purchasing, DPO, IT security, external service provider, etc.
- **Technical review of security and compliance requirements** (e.g. Transfer Impact Assessment, AVV, certifications) and proven checklists where helpful
- **Suggestions for a pragmatic solution** in the event of non-compliance with requirements
- **Audit-proof documentation**
- **Stakeholder-oriented documents**, e.g. for works councils

2

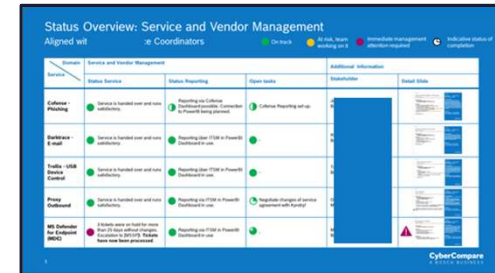
## Introduction of new security tools and processes (e.g. managed SOC)



- **Project management on the customer side**
- Organization of **rule meetings and updates for the governing body**
- **Tracking** of actions
- **Invoice and performance audit**
- **Decision templates**, e.g. in the case of problems such as incompatibilities, **based on customary market procedures**

3

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



- **Coordination of transition and new introduction of managed services**
- Review of contracts and **performance certificates (SLA)**
- Development of **KPI-based service Mgmt.**
- **Negotiation of changes** (e.g. number of tickets) that are necessary after the conclusion of the contract
- Establishment of **3rd Party Risk Management**

# CyberCompare

Good security decisions



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



[jannis.stemmann@bosch.com](mailto:jannis.stemmann@bosch.com)

**CyberCompare**

Always a good decision