Always a good security decision

We are security architects and take responsibility from strategy and vendor selection to implementation and interim management

Projekt management

1 Strategy, gap assessments, architectures and roadmaps

2 Bid comparisons + tenders

3 Implimentation, Compliance, Transition

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

CyberCompare
Always a good decision

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

CyberCompare
Always a good decision

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
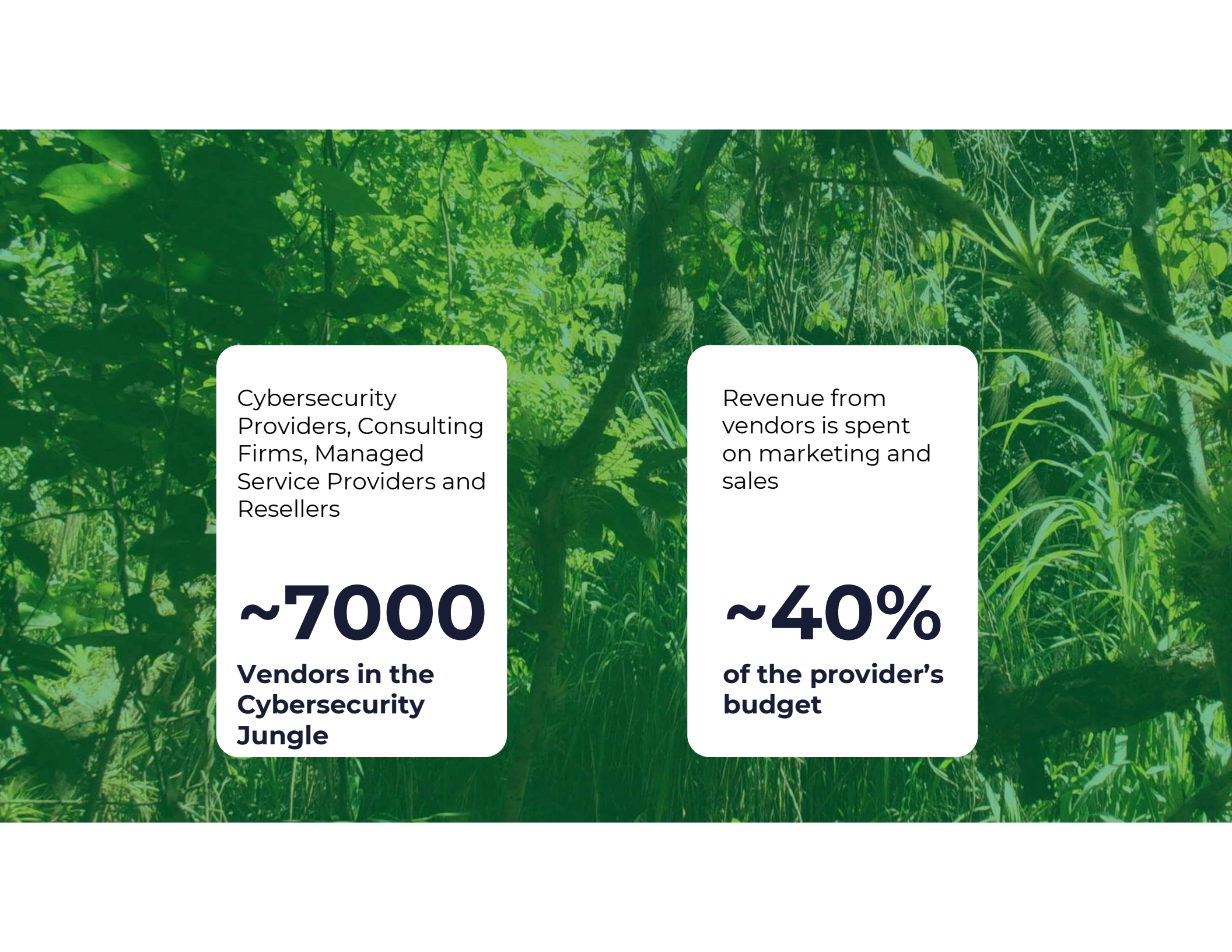Chief Cybersecurity Officer,
Robert Bosch GmbH

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

CyberCompare
Always a good decision

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:

BlueVoyant · orange · nicos cyber defense · kyndryl · T Systems · SVA · NVISO · SOPHOS · NTT Data · OBRELA · SOC dhpg & TÜV AUSTRIA Group · ARCTIC WOLF · G DATA · arvato BERTELSMANN Arvato Systems · Ontinue AI-Powered MXDR · telent service · commitment · value · EVIDEN · 8COM CYBER SECURITY · DXC TECHNOLOGY · accenture · CANCOM · controlware · THALES Building a future we can all trust · SCALTEL · glueck·kanja · Ovens Security for the greater good · vodafone · bechtle · KUDELSKI SECURITY · r tec cyber security · infoGuard SWISS CYBER SECURITY · EnBW Cyber Security · Deloitte · claranet cyber security

Selection of SIEM/XDR platforms:

elastic · paloalto NETWORKS · exabeam · RAPID7 · Trellix · Microsoft · splunk> · securonix · Hunters. · Google · wazuh. · CROWDSTRIKE · LOGPOINT · IBM · LogRhythm · SentinelOne

...List not exhaustive

Over 60 customer projects. Typical examples:

KRITIS Company: **Combined SIEM/SOC** project including connection of oerations 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 **cource 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**

CyberCompare
Always a good decision

Example: Managed SOC RfP

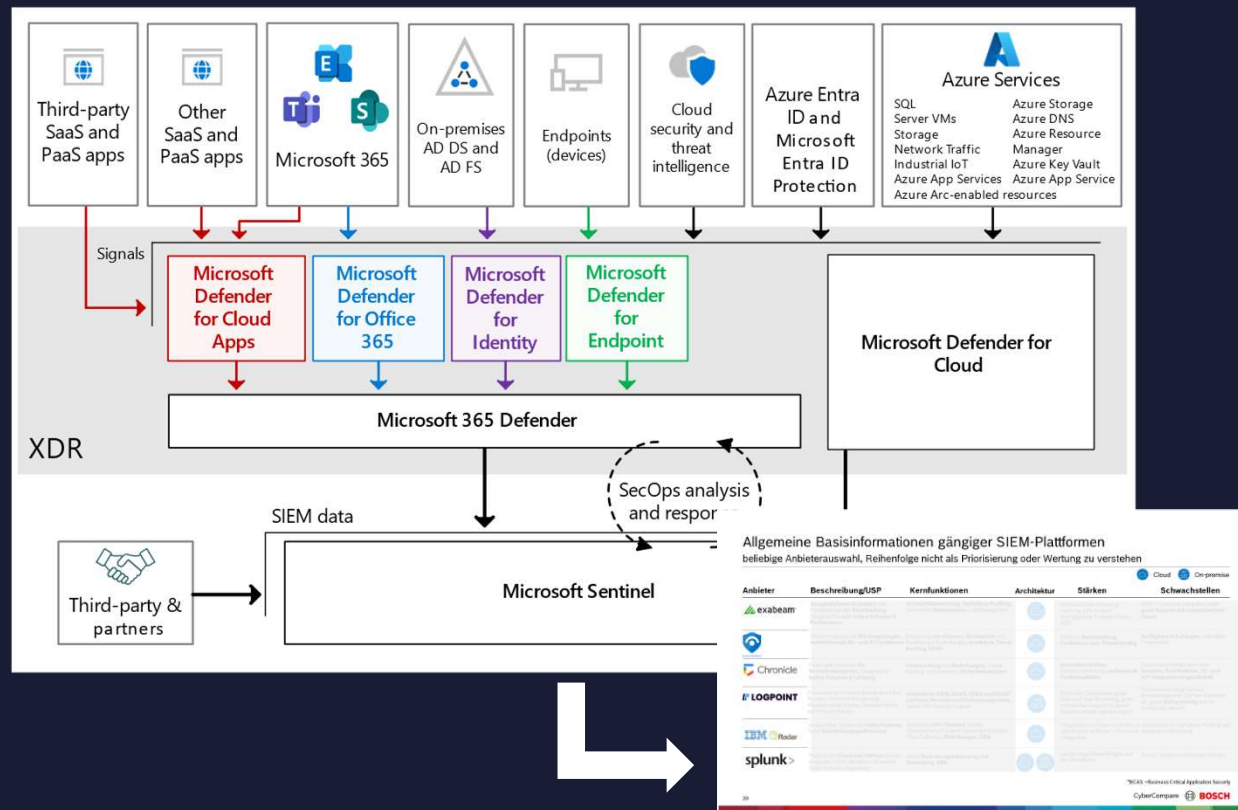| Criteria	MSSP A	MSSP B	MSSP C	MSSP D	MSSP E	MSSP F
SOC analyst locations	EU country 1	EU country 2	EU country 3	Germany	Germany	Germany
# MSOC customers globally	200	200	400	350	50	Unclear
# MSOC customers in Germany	10	6	20	50	40	Unclear
Reaction time 365/24/7 for critical security incidents (start of L1 triage)	15 min	15 min	30 min	30 min	30 min	45 min
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...

CyberCompare
Always a good decision

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

CyberCompare
Always a good decision

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

9

CyberCompare
Always a good decision

Recommendations are based on content-related, technical and commercial evaluations to enable optimal decision-making

Management Summary

Fulfilment of requirements/ service description

Commercial Scenarios / TCO

Technical Reviews / CompareDays

CyberCompare
Always a good decision

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

- Answering **bidders' questions professionally**
- Coordination with the awarding authority

- **Evaluation of the application for participation** with attachments and references in coordination with the awarding authority

- **Preparation and moderation** (if desired) of bidder discussions

- If required: **Project management of implementation**, PoCs or other downstream stages

CyberCompare
Always a good decision

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

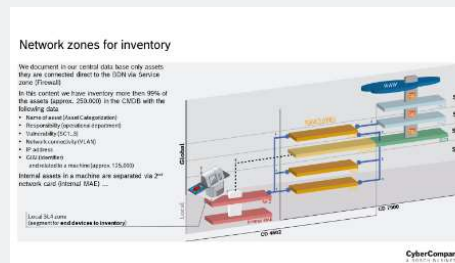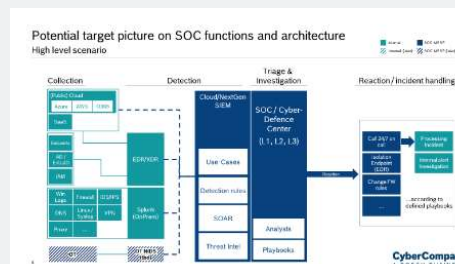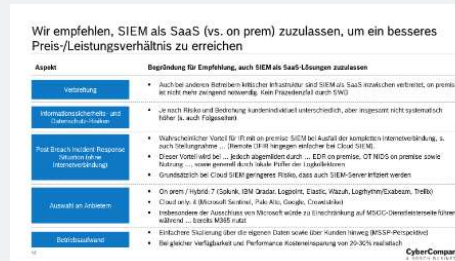**CyberCompare**
Always a good decision

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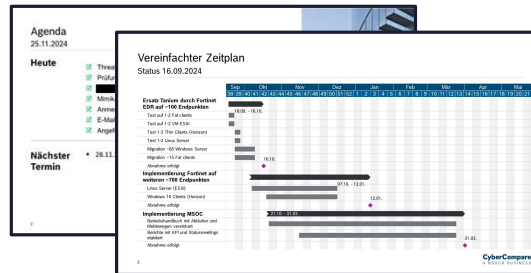
- **Project management on the customer side**
- Organization of **rule meetings and updates for the governing body**
- **Tracking** of actions
- **Invoice and performance audit**
- **Decision templates,** e.g. in the case of problems such as incompatibilities**, based on customary market procedures**

3

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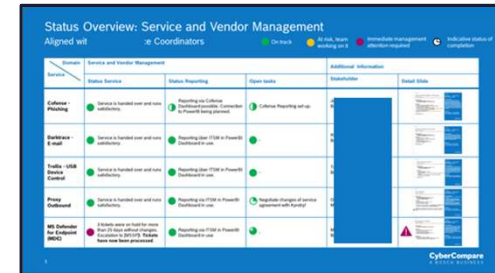
- **Coordination of transition and new introduction of managed services**
- Review of contracts and **performance certificates (SLA)**
- Development of **KPI-based service Mgmt.**
- **Negotiation of changes** (e.g. number of tickets) that are necessary after the conclusion of the contract
- Establishment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

CyberCompare

Good security decisions

🌐 www.cybercompare.com

✉ jannis.stemmann@bosch.com

CyberCompare
Always a good decision