Integrierte Sicherheitsarchitektur im Cyber-Raum…
…aber bitte sicher
statt einfach nur teuer

Impulse + Diskussion

CyberCompare
A BOSCH BUSINESS

Jannis Stemmann

Public-IT-Security (PITS), Berlin, 12./13. Juni 2024

1. **Wie sieht eine gute integrierte Sicherheitsarchitektur im landesweiten Cyber-Raum überhaupt aus?**

2. **Teuer ≠ sicher**

3. **Öffentliche Stellen managen Cyberrisiken häufig gut**

Wie sieht eine gute integrierte Sicherheitsarchitektur im landesweiten Cyber-Raum überhaupt aus?

- Es ist kein anerkanntes „Vorbild“ oder eine Blaupause bekannt, die als Referenzarchitektur dienen könnte. Wer ist eigentlich der Architekt?

- „How does good look like?“: Nach welchen Kriterien kann man das beurteilen?

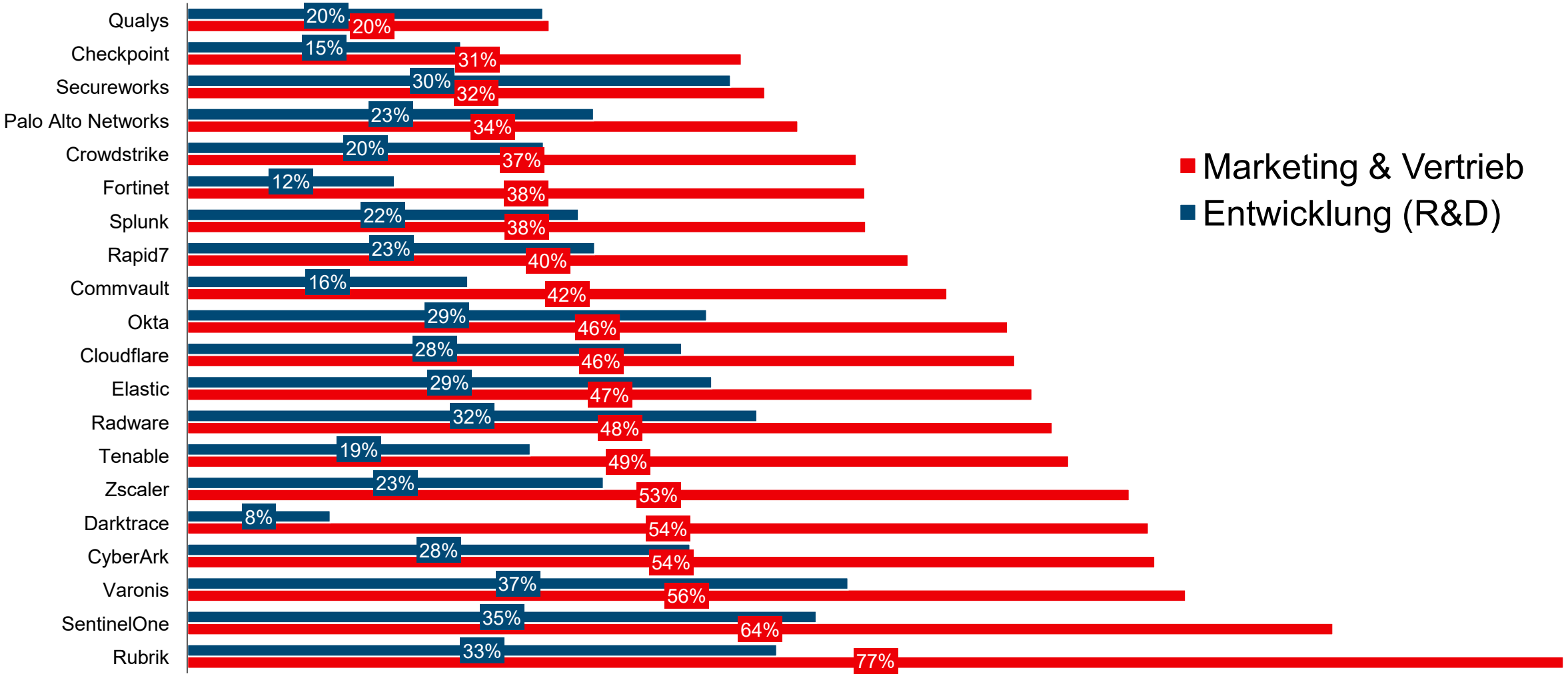
- Wichtig: Effektivität in der Cyber-Abwehr. Auch wichtig: Effizienz und Angemessenheit

1. Wie sieht eine gute integrierte Sicherheitsarchitektur im landesweiten Cyber-Raum überhaupt aus?

2. **Teuer ≠ sicher**

3. Öffentliche Stellen managen Cyberrisiken häufig gut

Teuer ≠ Sicher: Der größte Kostentreiber von Security ist Marketing + Vertrieb, pro Jahr Ausgaben von mehr als 50 Mrd. EUR



 Ausgaben als % des Umsatzes; Quelle: 10K / 10Q / S1 reports 2023 / 2024

CyberCompare
A BOSCH BUSINESS

Fallbeispiel: System zur Angriffserkennung (OT NIDS mit Monitoring-Service), Einsparung von ~30% bei höchster Erfüllung der funktionalen Kriterien erreicht

Lösungen / Anbieter	Anbieter A	Anbieter B	Anbieter C	Anbieter D	Anbieter E	Anbieter F	Anbieter G	Anbieter H
Konzept	NIDS	NIDS	NIDS	NIDS	NIDS	NIDS	NIDS (Logdaten management noch in Entwicklung)	SIEM mit Endpoint Agents, NIDS auf …, … server
Gesamterfüllung inhaltliche Anforderungen	**92%**	**91%**	**84%**	**83%**	**70%**	**65%**	**63%**	**61%**
Bereits bei Netzbetreibern eingesetzt	✓	✓	✓	✓ (… Kunden, davon … Netzbetreiber)	✓	- (… Kunden, davon … Netzbetreiber)	✓	✓ (Ca. … Kunden, davon … Energieversorger)
Bereits erfolgreich gem. IT-Sig. 2.0 geprüft	✓	✓		-	-	-	✓	-
Schriftlich bestätigt: System erfüllt alle technischen MUSS-Kriterien der OH des BSI zum Einsatz von SzA	✓	✓	✓	✓	✓	✓	Teilweise (abhängig von Prüfer)	✓
Sonstiges	Auszeichnungen durch …	Auszeichnungen durch …	Kooperation mit XYZ	Optimert auf … Ökosystem (Integrationen). Auszeichnung durch …	Noch in Entwicklung/ Testphase, z.B. noch kein MFA; Potenzial für schnelle Erweiterung Funktionalität	…	Alles Open Source, Ca. … MA	Alles Open Source, ca. … MA
Abschätzung Kosten 3 Jahre (Minimalpaket, ohne zusätzliche Beratung nach Einführung), TEUR	**70**	**100**	**90**	**220**	**60**	**50**	**70**	**70**
Abschätzung Kosten 3 Jahre (Minimal paket + 12 PT/Jahr Beratung), TEUR	**120**	**160**	**180**	**250**	**80**	**70**	**80**	**90**
Gesamteinschätzung: Eignung, Preis/Leistung	★★★★★	★★★★★	★★★★☆	★★★★☆	★★★☆☆	★★★☆☆	★★☆☆☆	★★☆☆☆
Kommentare	Erprobt, starker Partner, höchster Funktionsumfang (zukunftssicher, z.B. Prozessdaten-überwachung)	Erprobt, starker Partner, hoher Funktionsumfang (zukunftssicher)	Erprobt, Marktführer in … Energieversorgung	… erprobt, aber in D bei KRITIS nicht stark verbreitet. … keine/geringe Erfahrung mit … in OT	Funktionsumfang minimal/noch in Entwicklung, noch keine Partner für Managed Services	Funktionsumfang minimal/noch in Entwicklung, noch keine Partner für Managed Services	Bisher noch kein SIEM/Logdatenmanagement, Informationen mündlich	Kleiner Anbieter, geringer Funktionsumfang mit Einschränkungen hinsichtlich OT

CyberCompare
A BOSCH BUSINESS

Fallbeispiel: Mehrstufige Evaluierung (ähnlich Verhandlungsverfahren mit Teststellungen) von > 20 MSSPs für Managed Services

Einsparung > 1 Mio. EUR auf 5-Jahreszeitraum trotz Priorisierung Security-Qualifizierung

Possible MSSP																												
Estimated size (FTE)		1000	4000	75	150	150	300	1500	110	1000	40 / 250	50	570	2800	60	3500	660	330	(security	500	2000	2800	800	4000		6000	> 1000 (250	2000	>10000	5500
Locations		Germany, France, UK	Europe, US	Germany	Germany, Austria	Germany	Germany, Austria	Europe, US	Germany	Germany	Germany, Austria	UK, Greece	Global with HQ	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	0,5	1	0,5	1	1	0,5	1	1	1	1	1	1
Customer focus/flexibility	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
	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
Reference VS-NfD / NATO restricted customers	1	1	0	0	0	0	0	0	0	1	0	0	0	1	0,5	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0
OT security managed services	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	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
	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
	1	0	0	0	0	0	0	0	0	0	0	0,5	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
	1	0	0	0	0	0	0,5	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
	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	2	0,5	0	0	0,5	0	1	0,5	1	0,5	0,5	0,5	1
	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	1	0	1
	1	0	0	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	1	0	1
	1	0	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	2	0
	1	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
	1	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	1
	1	0	1	0	0	0	0	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
	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
	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
	1	0	0	0	0	1	0	0	0	1	0	0,5	0,5	0	1	0	0	0	0	0	0	0,5	1	1	1	1	0,5	1	1	1
	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
	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 guidance		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 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 Microsoft, but also other vendors	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

CyberCompare
A BOSCH BUSINESS

1. Wie sieht eine gute integrierte Sicherheitsarchitektur im landesweiten Cyber-Raum überhaupt aus?
2. Teuer ≠ sicher
3. **Öffentliche Stellen managen Cyberrisiken häufig gut**

Öffentliche Stellen managen Cyberrisiken häufig gut

- Gleiche Nöte wie Privatwirtschaft: **Zuwenig Budget, mangelnde Personalkapazitäten, steigende Anforderungen**

- Fokus auf das Wesentliche: **Was bringt viel Security und kostet wenig?** => Oft ähnlich **pragmatisches Mindset** wie im klassischen deutschen Mittelstand

- **Transparente Ausschreibungen** mit **präzisen, durchdachten Formulierungen** in Leistungsverzeichnissen => Oft besser als bei privaten Unternehmen

Danke!

Vielen Dank für Ihre Aufmerksamkeit!

Diskussion:

- Katharina Sook Hee Koch, BSI
- Volker Presse, Auswärtiges Amt
- Jannis Stemmann, CyberCompare