Stiftung Zentrale Stelle VERPACKUNGSREGISTER

Wie erreiche ich Cyber Resilience?

Mensch, Automation und Technologie im Management Dreiklang

Wolfram Nötzel

CIO

Wolfram Nötzel

2017 – heute	CIO **ZSVR** Stiftung Zentrale Stelle Verpackungsregister
2011 – 2017	Geschäftsführer **Microtec GmbH**
1997 – 2011	Business Manager IT Security & Datacenter **DTS Systeme Gmbh**
1994 – 1997	Systemingenieur **CE Computer**
1989 – 1994	Dipl. Ing. Nachrichtentechnik **TH OWL**

Aufgaben der Zentralen Stelle Verpackungsregister

- Aufbau und Betrieb eines Onlineregisters für die Hersteller laut VerpackG
- Aufbau und Betrieb einer Datenbank mit Datenmeldungen zu den Verpackungsmengen von Herstellern (950000) und Systemen (10): das Verpackungsregister LUCID
- Marktanteilsberechnung zur Aufteilung der Entsorgungskosten und -mengen der dualen Systeme
- Definition und Veröffentlichung eines Mindeststandards zum recyclinggerechten Design von Verpackungen (im Einvernehmen mit dem Umweltbundesamt)
- Prüfung der Mengenstromnachweise der Systeme und Branchenlösungen
- Einordnung von…
  - …Verpackungen als systembeteiligungspflichtig,
  - …Verpackungen als Mehrwegverpackungen,
  - …Getränkeverpackungen als pfandpflichtig,
  - …Anfallstelle von Abfällen als eine mit privaten Haushaltungen vergleichbare Anfallstelle

Entwicklung einer Cyber-Security Strategie

Voraussetzungen um Cyber Resilience zu erreichen!

1. Absicherung durch GF, Vorstand, da die Sicherheit höher priorisiert werden muss als Effizienz
2. Ausreichender Ressourcen, da Cyber Security kein „Beiwerk“ ist, sondern zentraler Punkt der IT Strategie sein muss

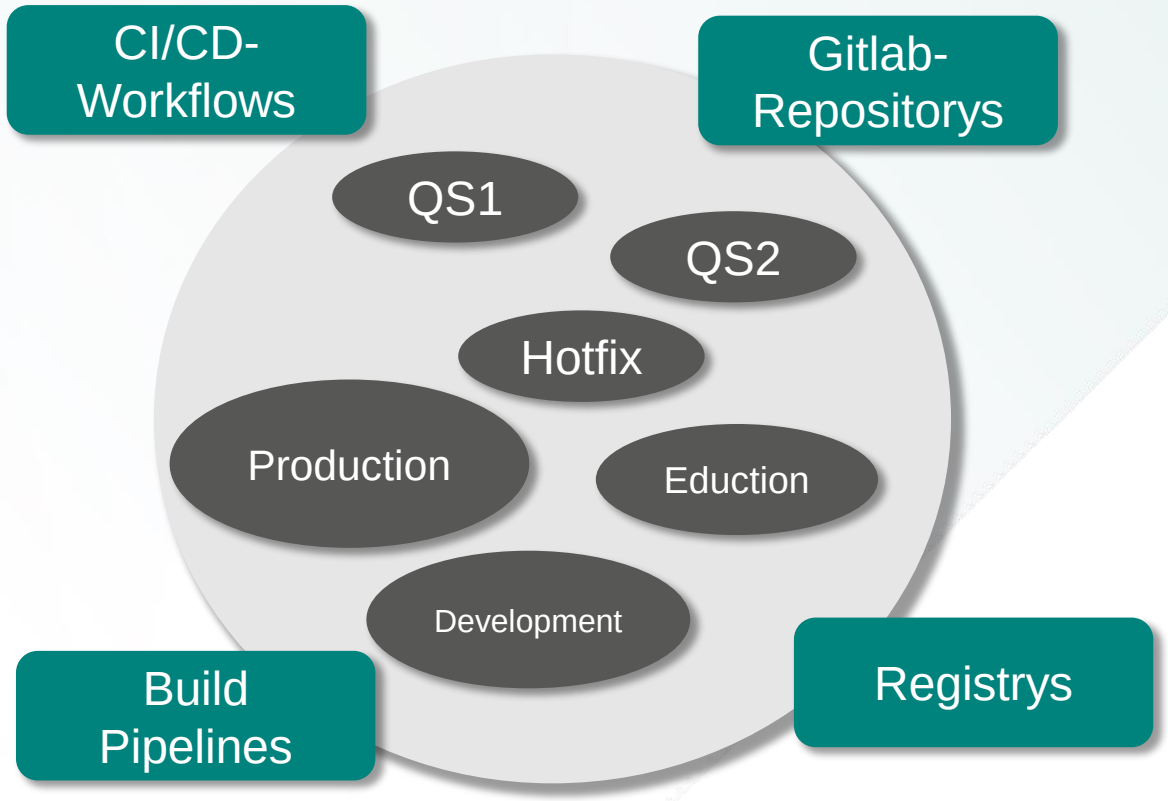
3. Situationsgerechtes Handeln durch vorabgestimmtes Playbook, mit den notwendigen Freiraum
4. Sicherheitsbewusstsein stärken durch wiederkehrende IT Sicherheitsschulungen mit aktuellen Bedrohungslagen (Ransomware, Phishing etc.).

5. Transparenz und Aufarbeitung von kritischen Situationen, um eine kontinuierliche Qualitätssteigerung zu erzielen (Lernkurve).

Prozess Automation

Prozess Automation

Es erfolgt eine vollständige Überwachung der Private Cloud Stages.



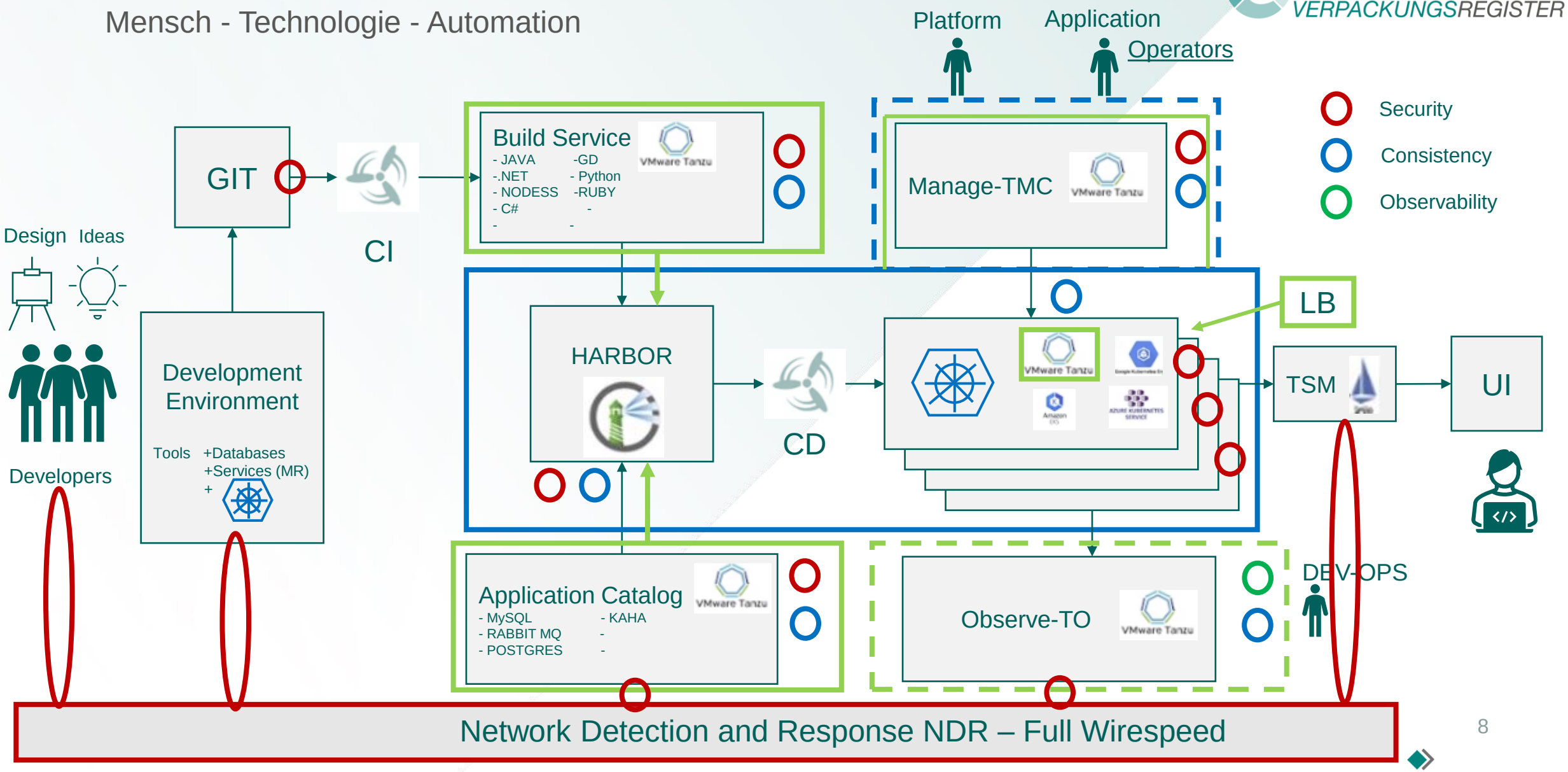
Zudem bieten die eingesetzten Sicherheitsmodule:

- Hostsicherheit
- Schwachstellenmanagement
- Laufzeitschutz
- Containersicherheit
- Compliance-Management

Die definierte Security Automation setzt dynamisch die Cyber Security Policies des K8 Stacks in Echtzeit um.

DevSecOps

Mensch - Technologie - Automation



Technologie

Technologie

Einsatz einer NDR Lösung (Network Detection & Response)

- Überwachung des gesamten Netzwerkes (innerhalb der Standorte der ZSVR und ausgelagerte private Clouds in den Rechenzentren)
- Echtzeitauswertung des Netzwerkverkehrs Agentless
- Terminierung einzelner schädlicher TCP Sessions
- Isolierung befallener Container und automatisierter neu deployment von Services im self healthy mode bei einem Infektionsfall

Für die sofortige Erkennung späterer Anomalien wird die AI & ML Funktionalität der NDR Appliance während der Entwicklung auf der QS1 und QS2 Stage antrainiert.

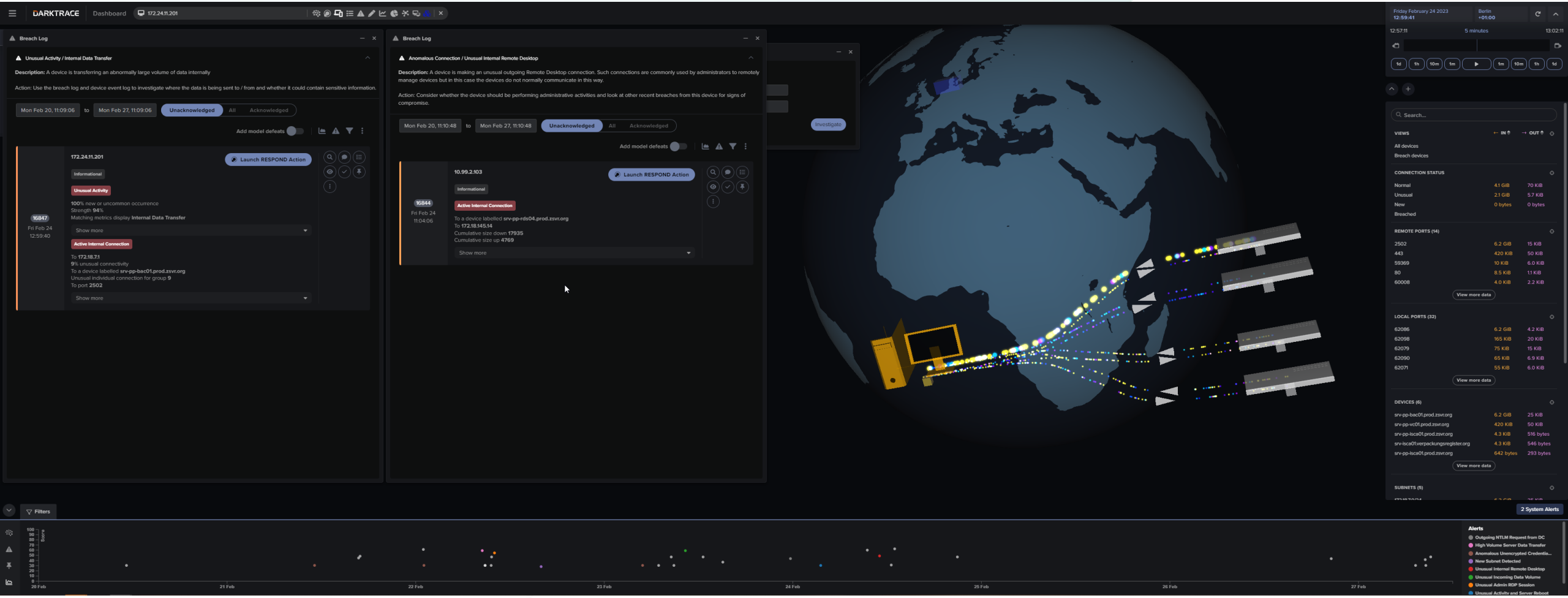
Erkennt und Terminiert werden u.a.

- Angriffe gegen Benutzerkonten
- unautorisierte Zugriffsversuche auf Systeme
- Versuche eines Angreifers, nach einem erfolgreichen Angriff einen Rückkanal zu seinem Server im Internet aufzubauen

Sichtbarkeit auf Anomalien durch FULL TRUST

NDR Technologie durch Darktrace

Dynamische Eventreaktion durch Antigina



Mensch

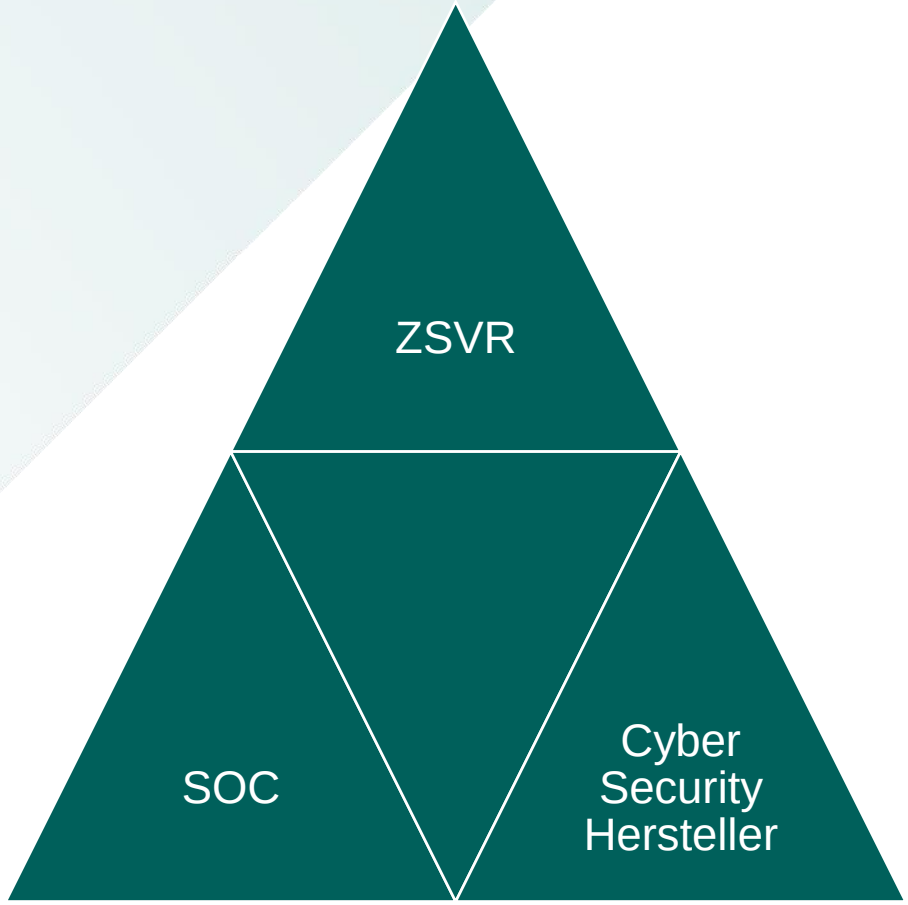
Its a people business….

Das Dreiklang-Vertragswerk zwischen

- ZSVR
- externem 24/7 SOC Service
- Cyber Security Herstellern

basiert auf einer RACI Matrix (Responsible, Accountable, Consulted, Informed).

Beschreibung und Abbildung dynamischer Anforderungen für alle internen und externen Mitarbeiter.



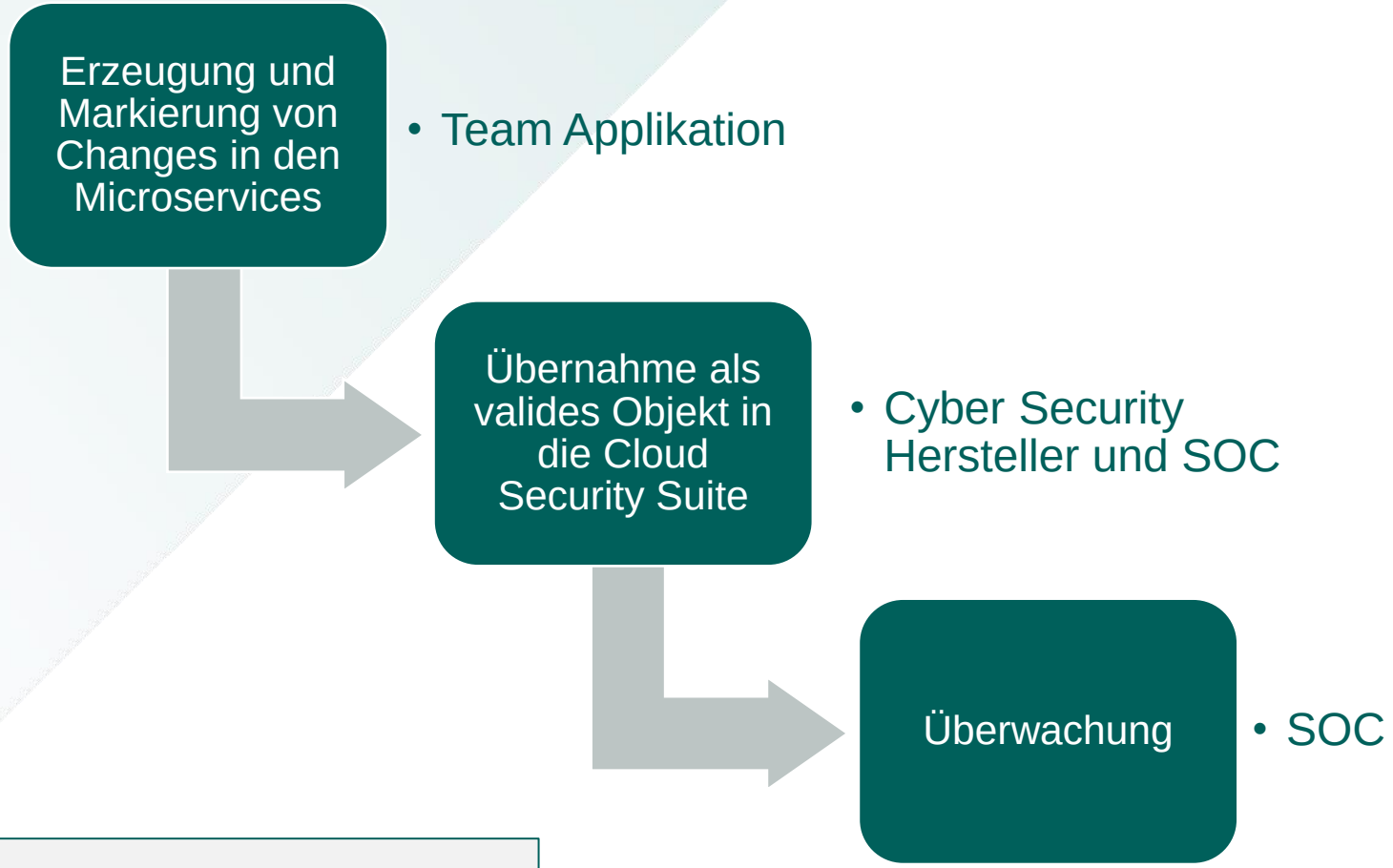
Zusammenspiel der Akteure

Die 100% Erreichung von Full Trust!

- 24/7 Überwachung ausschließlich durch die Beauftragung eines SOC Service Anbieters möglich
- Wahl eines Dreistufenmodells

<u>Vorteile</u>

- SOC Team stets auf dem aktuellsten Stand
- Ausschließen von Fehlalarme durch Fehlinterpretation
- Gegenseitige Absicherung und Qualitätskontrolle



Vertragsregelwerk in RACI Matrix definiert.
Anpassung und Optimierung durch Cyber Security Lenkungsausschuss.

SOC – Report - Monatlich

Stiftung Zentrale Stelle VERPACKUNGSREGISTER

dacoso | Ihre Aufgaben | Projekte | Filter | Dashboards | Personen | Pläne | Assets | Apps | Erstellen | Suchen

208 filtered issues (6234 hidden) — Statistics by **Priority** 3

Rich Filter Created vs Resolved Chart

208 filtered issues (6234 hidden) — Erstellt vs Erledigt **Issues** 31d

Rich Filter Flexi Charts

T	Schlüssel	P	Zusammenfassung	Status
	OPS-27986	=	ZSVR - NDR - AIA-Incident -New AI Analyst incident event created for 172.19.179.28: "New Credential Usage"	GESCHLOSSEN
	OPS-27985	^	ZSVR - NDR - MB-Antigena -172.19.179.28 breached "Antigena/Network/Insider Threat/Antigena Unusual Privileged User Activities Block"	GESCHLOSSEN
	OPS-27984	v	ZSVR - NDR - MB-Normal -172.19.179.28 breached "User/New Admin Credentials on Client"	CLASSIFICATION
	OPS-27983	=	ZSVR - NDR - AIA-Incident -New AI Analyst incident event created for Prod-Clair-DBserver: "Unusual WinRM Connections"	WAITING FOR CUSTOMER
	OPS-27979	^	ZSVR - NDR - MB-Antigena [redacted] breached "Antigena/Network/Insider Threat/Antigena Unusual Privileged User Activities Block"	WAITING FOR CUSTOMER
	OPS-27978	v	ZSVR - NDR - MB-Normal [redacted] breached "Anomalous Connection/Unusual Admin RDP Session"	WAITING FOR CUSTOMER
	OPS-27977	v	ZSVR - NDR - MB-Normal -Prod-Clair-DBserver breached "Anomalous Connection/Rare WinRM Outgoing"	CLASSIFICATION
	OPS-27970	=	ZSVR - NDR - AIA-Incident -New AI Analyst incident event created for christian.vogt: "Suspicious Remote Service Control Activity"	GESCHLOSSEN
	OPS-27966	=	ZSVR - NDR - MB-Normal -domaindnszones.prod.zsvr.org breached "Compliance/High Priority Compliance Model Breach"	GESCHLOSSEN
	OPS-27965	=	ZSVR - NDR - MB-Normal -domaindnszones.prod.zsvr.org breached "Compliance/Anomalous Vulnerable Service Ticket Request"	GESCHLOSSEN
	OPS-27964	^	ZSVR - NDR - MB-Antigena -172.17.162.6 breached "Antigena/Network/Insider Threat/Antigena Unusual Privileged User Activities Block"	GESCHLOSSEN
	OPS-27963	v	ZSVR - NDR - MB-Normal -172.17.162.6 breached "User/New Admin Credentials on Client"	GESCHLOSSEN
	OPS-27958	=	ZSVR - NDR - AIA-Incident -New AI Analyst incident event created for christian.vogt: "Suspicious Remote Service Control Activity"	GESCHLOSSEN

Vielen Dank für Ihre Aufmerksamkeit