Modularer OT-Leitstand für KRITIS

Herstellerunabhängige Betriebs- und Sicherheitskonzepte neu gedacht

ExperTalk OT-Energiewirtschaft

Matthias Knauth – Senior Project Manager OT & ICS

Dietzenbach, 02.07.2025

www.controlware.de

Agenda

1. Einstieg und Zielbild eines OT-Betriebsmodells
2. Lösungsansatz & Betriebsstruktur
3. Bausteine für einen individuellen Servicekatalog
4. Rollen, Verantwortlichkeiten und Abläufe im OT-Betrieb
5. Der Blick nach vorn: Nutzung von KI in einem OT-Betrieb

Zwischen Standard und Fragment – Die Herausforderung im OT-Betrieb

Der Status Quo:

- In der IT sind NOC- und SOC-Services weitgehend standardisiert – Tools, Schnittstellen und Prozesse sind etabliert
- Für IT-Infrastrukturen bietet CW bereits vollumfängliche Managed Services, die sich wirtschaftlich gut skalieren lassen

In der OT-Welt ist das anders:

- Heterogene Systemlandschaften & herstellerabhängige Speziallösungen
- Viele System nicht für zentrale Services ausgelegt (Stichwort „Air-gapped“)
- Hersteller-Services sind meist nur sinnvoll bei vollständiger Vendor-Bindung – was in der Praxis oft nicht gegeben ist
- Dennoch: Viele Anfragen unserer TSO / DSO Kunden zu Service-Verträgen

Unser Ziel:
Ein modulares, KRITIS-taugliches Betriebsmodell für OT-Umgebungen, das sowohl wirtschaftlich als auch technisch tragfähig ist – unabhängig vom Hersteller

Agenda

1. Einstieg und Zielbild eines OT-Betriebsmodells
2. Lösungsansatz & Betriebsstruktur
3. Bausteine für einen individuellen Servicekatalog
4. Rollen, Verantwortlichkeiten und Abläufe im OT-Betrieb
5. Der Blick nach vorn: Nutzung von KI in einem OT-Betrieb

Gemeinsame Entwicklung eines OT-Betriebsmodells

- Betriebsunterstützung der OT-Infrastruktur durch CW Managed Services
- Kombination aus Betriebs- und Sicherheitsmonitoring (NOC/SOC)
- Modularer Aufbau für Service- und Kostentransparenz
- Klare Strukturierung in
  - Einmalige Setup & Auditmaßnahmen
  - operativen / zyklischen Tätigkeiten
  - On-Demand-Requests (Incidents, Changes)

Zu validieren im Rahmen mit dem Kunden:

- Welche Systeme verursachen aktuell den größten Betriebsaufwand?
- Wo ist aktivere Unterstützung notwendig: bei Störungen oder im Regelbetrieb?
- Welche Komponenten sind besonders relevant (technisch kritisch oder regulatorisch relevant)?

Von individueller OT-Systemlandschaft zu strukturiertem Servicekatalog

controlware

Konzept der Modularisierung	Dienstleistungen & Services	Adaptionsphase
Jedes Modul bildet einen abgrenzbaren, funktionalen Block in der OT-Infrastruktur (z. B. Backup, AD, Firewalls) Übersetzbarkeit in einen Managed Service mit definierten Aufgaben, Zuständigkeiten und Betriebsparametern	**Einmalige Tätigkeiten** • Infrastrukturaufnahme, Systemhärtung, Patch-Level-Audit, Basisdokumentation • „Betriebsreife“ herstellen **Zyklische / operative Tätigkeiten** • Patchmanagement, Housekeeping, Backupkontrolle, Log-Review, Schwachstellenscans • Frequenz: 1× monatlich / quartalsweise / halbjährlich **On-Demand Service** • Konfigurationsanpassungen und -erweiterungen • Troubleshooting & Fehlerbehebung (SLA-basiert)	Wir befinden uns noch in der Adaptionsphase Ziel: Verstehen, welche Module & Services sind relevant (technisch & organisatorisch) Frage der Realisierbarkeit: Was können wir wie schnell und verlässlich übernehmen?

Agenda

1. Einstieg und Zielbild eines OT-Betriebsmodells
2. Lösungsansatz & Betriebsstruktur
3. **Bausteine für einen individuellen Servicekatalog**
4. Rollen, Verantwortlichkeiten und Abläufe im OT-Betrieb
5. Der Blick nach vorn: Nutzung von KI in einem OT-Betrieb

Dreistufiges Service-Modell für den OT-Leitstand

controlware

Betriebsmodule

Klare technische Funktionsblöcke wie z. B. Backup, Netzwerk, Remote Access

Je Modul: eigenständig überwachbar, dokumentierbar und betrieblich betreubar

Grundlage für strukturierte Übergabe, Monitoring und Zuständigkeiten

Servicemodule

Standardisierte Betriebsprozesse wie Incident Management, Reporting, Schwachstellenbewertung

Unterstützen die Betriebsführung methodisch, effizient und nachvollziehbar

Bauen auf bewährten ITIL-nahen Abläufen auf (z. B. Ticketfluss, Analysepfade)

OT-Maintenance (On-Demand)

Regelmäßige, separat beauftragte Maßnahmen zur Systempflege und -härtung

Schwachstellenmanagement (VMS), Firewallregel-Review, Benchmarking nach CIS, regulatorische Updates,…

Ziel: langfristige Betriebssicherheit, Compliance und technische Aktualität

Beispielhafte Übersicht der Betriebsmodule innerhalb eines Servicekatalogs

controlware

Modul 1: Infrastruktur
- AD (on-prem)
- DNS
- Zertifkatsstelle
- GPO Verwaltung
- File Service /DFS
- MFA

Modul 2: Netzwerk & Firewall
- Cisco Switches & Router
- Dell Server
- Fortinet Firewalls
- SSL VPN

Modul 3: SzA
- Rhebo (CSIRT – CW Security Incident Response Team)
- Tenable (Vulnerability Check)
- SIEM (perspektivisch)
- Syslog-Server
- Endpoint Security (XDR/EDR)

Modul 4: Hypervisor (Virtualisierung)
- Verwaltung der Hosts vCenter
- Patch- und Update-Management
- ESXi vSphere 8 Enterprise Plus mit vSAN Add-on

Modul 5: Backup & Restore
- Veeam Backup & Replication (inkl. Tape Loader)

Modul 6: Überwachung & Monitoring
- Dezentrale Überwachung über CheckMK / Zabbix
- Managed Engine OpManager für zentrale Visualisierung
- Alamierungskonzept

Modul 7: Managed Remote Access
- Wallix
- Genua

Ziel: Jedes Modul in einen dokumentierten, überwachbaren und betreibbaren Zustand zu überführen, der einen standardisierten Managed Service durch CW ermöglicht

Marcom V2.0 2025

Beispielhafte Übersicht der Servicemodule innerhalb eines Servicekatalogs

Prozess-Steuerung
- Steuerung der Service-Prozesse
- Ticket-Koordination
- Überwachung der SLAs

Customer Service Center
- Call-Annahme (24/7)
- Single Point of Contact
- Ticketerstellung und- routing

Incident Management
- Analyse der Störung
- Behebung der Störung
- Dokumentation der Lösung
- Ticketbearbeitung

Problem Management
- Weitergehende Störungsqualifizierung
- Erarbeitung von Lösungswegen, u.U. zusammen mit dem Hersteller
- Dokumentation der Fehlerursachen

Change Management
- Konfigurationsanpassungen, Änderungen und Systemerweiterungen
- Softwarepflege und Umsetzung von Release Management-Vorgaben

Reporting
- Ticket Reporting nach Kategorie
- Infrastruktur Reporting (Verfügbarkeit, Auslastung, etc.)
- Kundenindividuelle Reports zu KPIs

Service-Level Management
- Service Manager als dedizierter AP
- SLA-Überwachung & Service Reviews

Ziel: Prozesse zur effizienten, regelbasierten Unterstützung und Steuerung der OT-Betriebsleistungen bereitzustellen.

Marcom V2.0 2025

Beispielhafte Übersicht der On-demand Leistungen i.S.v. OT-Maintenance

Configuration Management
- Regelmäßige Sicherung der Configs
- Widerherstellung der Konfiguration bei Gerätetausch oder System-Wiederherstellung

Release Management
- Aufrechterhaltung des vereinbarten Betriebszustands
- Überprüfung und Evaluierung von Herstellerempfehlungen
- Durchführung von Releases

VMS
- Durchführung von Schwachstellen-Scans
- Signatur- & Software-Updates für die Scan-Engines
- Bewertung von Findings (CVSS)

Log- und Eventfile Review
- Auswertung und Korrelation von Logs & Events
- Handlungsempfehlungen zur Anpassung der Alarmierungslogik
- Optimierung von Schwellwerten und Event-Filtern

Firewall-Regelüberprüfung
- Review und Bewertung bestehender Regeln
- Erarbeitung von Änderungs- und Löschvorschlägen

OT-Härtung
- Abgleich der System-Config gegen CIS-Benchmarks o.Ä.
- Ableitung und Umsetzung konkreter Härtungsmaßnahmen

Bulletin-Service
- Bereitstellung kundenspezifischer Sicherheitsmeldungen
- Formulierung kontextbezogener Handlungsempfehlungen

Ziel: Spezialisierte, bedarfsgesteuerte Leistungen situativ bereitstellen, zur Pflege, Härtung und Aktualität der eingesetzten OT-Systeme

Marcom V2.0 2025

Agenda

controlware

1 Einstieg und Zielbild eines OT-Betriebsmodells

2 Lösungsansatz & Betriebsstruktur

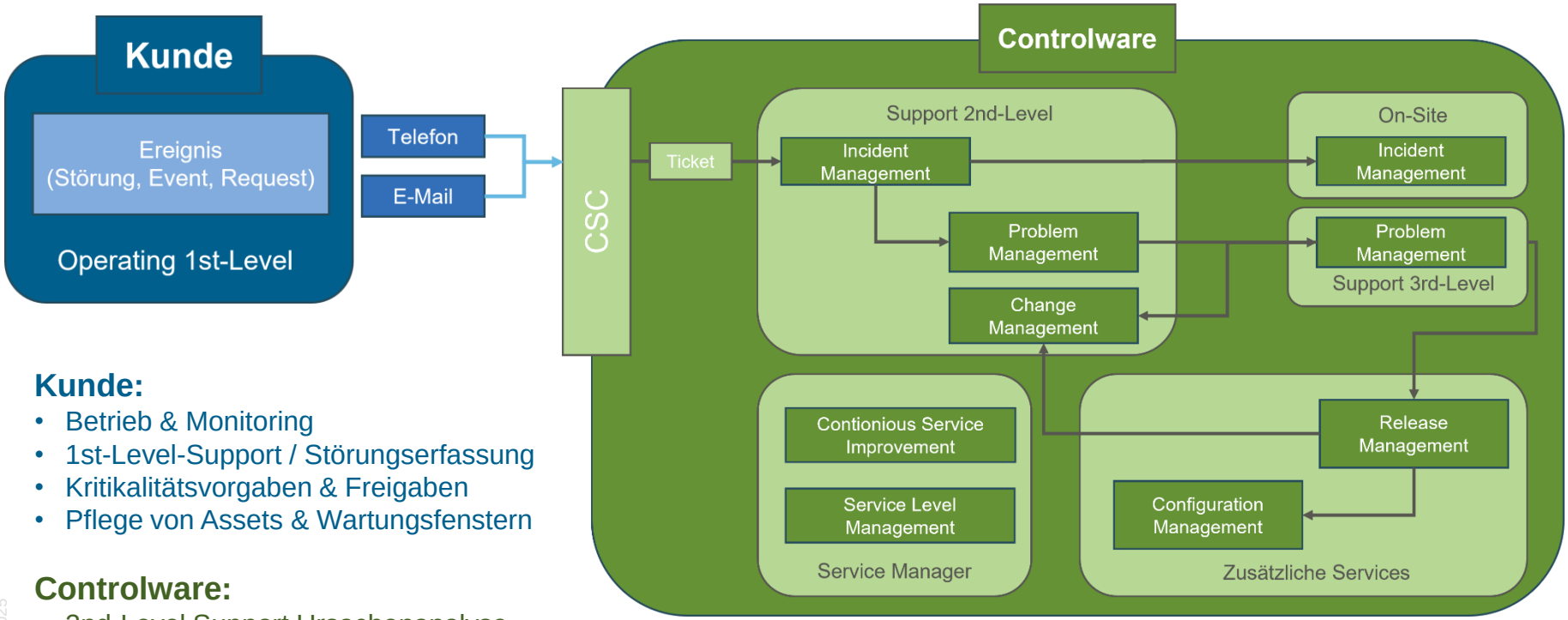
3 Bausteine für einen individuellen Servicekatalog

4 Rollen, Verantwortlichkeiten und Abläufe im OT-Betrieb

5 Der Blick nach vorn: Nutzung von KI in einem OT-Betrieb

Marcom V2.0 2025

Kontrollierter Betrieb mit klaren Zuständigkeiten & Prozessen



Kunde:

- Betrieb & Monitoring
- 1st-Level-Support / Störungserfassung
- Kritikalitätsvorgaben & Freigaben
- Pflege von Assets & Wartungsfenstern

Controlware:

- 2nd-Level Support Ursachenanalyse
- Schwachstellen- und Eventbewertung
- Dokumentation

Marcom V2.0 2025

Rollen & Aufgaben in einem kombinierten NOC/SOC-Betriebsmodell

Rolle	Aufgabe im NOC-Kontext	Aufgabe im SOC-Kontext
L1 Operator (Kunde) / 24/7 Monitoring	• Erkennen technischer Störungen (z. B. Link-Down, CPU-Auslastung, Backup-Fehler) • Validieren gegen Wartungspläne • Ticket-Erstellung bei Regelverstößen oder Schwellenwertüberschreitung	• Automatische oder manuelle Vorbewertung sicherheitsrelevanter Events (z. B. Login-Fails, Policy-Verletzungen) • Klassifizierung (False Positive / Weiterleitung an L2)
L2 Analyst (SOC/NOC)	• Root-Cause-Analyse technischer Störungen (vSphere, Backup, Netzwerk) • Korrelation über mehrere Systeme hinweg • Ableitung konkreter Handlungsempfehlungen für Betrieb	• Bewertung sicherheitsrelevanter Muster (z. B. ICS-Anomalien, Bruteforce) • Mapping auf Schwachstellen / CVEs • Entscheidung: Maßnahmen, Eskalation, Watchlist
Service Manager	• Organisation Wartungsfenster, Patch-Zyklen, Betriebs-KPIs • Kommunikation bei Systemausfällen / Störungen	• SOC-Reportings (monatlich) • Überblick über Eventlage, Ticketlage, Eskalationen • Koordination von Schwachstellenmaßnahmen
L3 Techniker / Spezialist (Optional bei Bedarf)	• Umsetzung komplexer Änderungen: Firmware-Updates, Cluster-Rekonfiguration, vSAN-Wartung • Troubleshooting tiefer technischer Probleme	• Analyse und Umsetzung bei sicherheitskritischen Incidents (z. B. Incident Response) • Durchführung von Isolierung / Recovery / Forensik
Architekt (optional)	• Definition technischer Schwellenwerte & Betriebsrichtlinien • Aufbau von Playbooks für Systemverfügbarkeit	• Definition sicherheitsrelevanter Use Cases (z. B. MITRE ATT&CK Mapping) • Risikoanalyse & Schwachstellenmanagement-Strategie

Fokus auf Relevanz statt Lizenzumfang

Problem: Hersteller-Services erfordern meist komplette Paketkäufe, obwohl nur ein Teil der Infrastruktur (z. B. nur Firewall oder nur ein Switch-Stack) genutzt wird -> hohe kumulierte Kosten und keine wirtschaftliche Effizienz.

Faktor	Beschreibung	Annahme (zu validieren)
Assets / Nodes	Basispreis je überwachtem System oder Modul	Kunde akzeptiert Asset-basiertes Preismodell
Use Case Komplexität	Bewertung nach Tiefe der Analysen (z. B. Logkorrelation, Schwachstellenbezug)	Aufwand pro Incident ist erfassbar und kalkulierbar
Ticketvolumen	Paketpreise für Incidents / Changes ab 2nd-Level	Erwartetes Volumen pro Jahr kann geschätzt werden
SLAs	Zuschläge für Reaktionszeiten / Eskalationspriorität	SLA-Level und Kritikalitätsklassen vertraglich abstimmbar
Remote Access	Zuschlag für Fernzugriff je Standort / Zugangsart (z. B. Wallix)	Remote-Zugriff dauerhaft und sicher möglich
Onboarding-Pauschale	Einmalige Setupkosten für Systemaufnahme, Baseline-Monitoring, Dokumentation	Umfang initialer Tätigkeiten gemeinsam abstimmbar
Dokumentation	Optional: Pflege der Asset-/Änderungsdokumentation (z. B. i-doit)	Zugriff auf Doku-System oder Standardvorlage vorhanden
Reporting	Optionales monatliches oder quartalsweises Reporting zu KPIs und Maßnahmen	Reporting-Frequenz & Format werden definiert
NOC-Funktion	Betriebs-Monitoring: Verfügbarkeit, Ressourcen, Backup-Status	Monitoringzugang über SNMP / Agent / API möglich
SOC-Funktion	Security-Monitoring: Logbewertung, Schwachstellenkorrelation, Eskalation	Logzugang + Eskalationsprozesse werden definiert

Agenda

controlware

1 Einstieg und Zielbild eines OT-Betriebsmodells

2 Lösungsansatz & Betriebsstruktur

3 Bausteine für einen individuellen Servicekatalog

4 Rollen, Verantwortlichkeiten und Abläufe im OT-Betrieb

5 Der Blick nach vorn: Nutzung von KI in einem OT-Betrieb

Marcom V2.0 2025

Exkurs: KI im OT-Leitstand: Zukunft oder schon heute?

Zielsetzung:

- Unterstützung des OT-Betriebs durch automatisierte Erstbewertung von Events und Störungen
- Entlastung interner Ressourcen im 1st-Level-Support / Tagesgeschäft

Mögliche Funktionsweise (MVP-Idee):

- Interaktive Nutzung durch Mitarbeiter („ChatBot“) auf Basis eines lokalen LLM
- Ausgabe von Lösungsvorschlägen auf Basis interner Trainingsdokumente
- Hosting on-prem (z.B. CW AI-Pod)

Perspektive (Soll-Zustand / Zielbild):

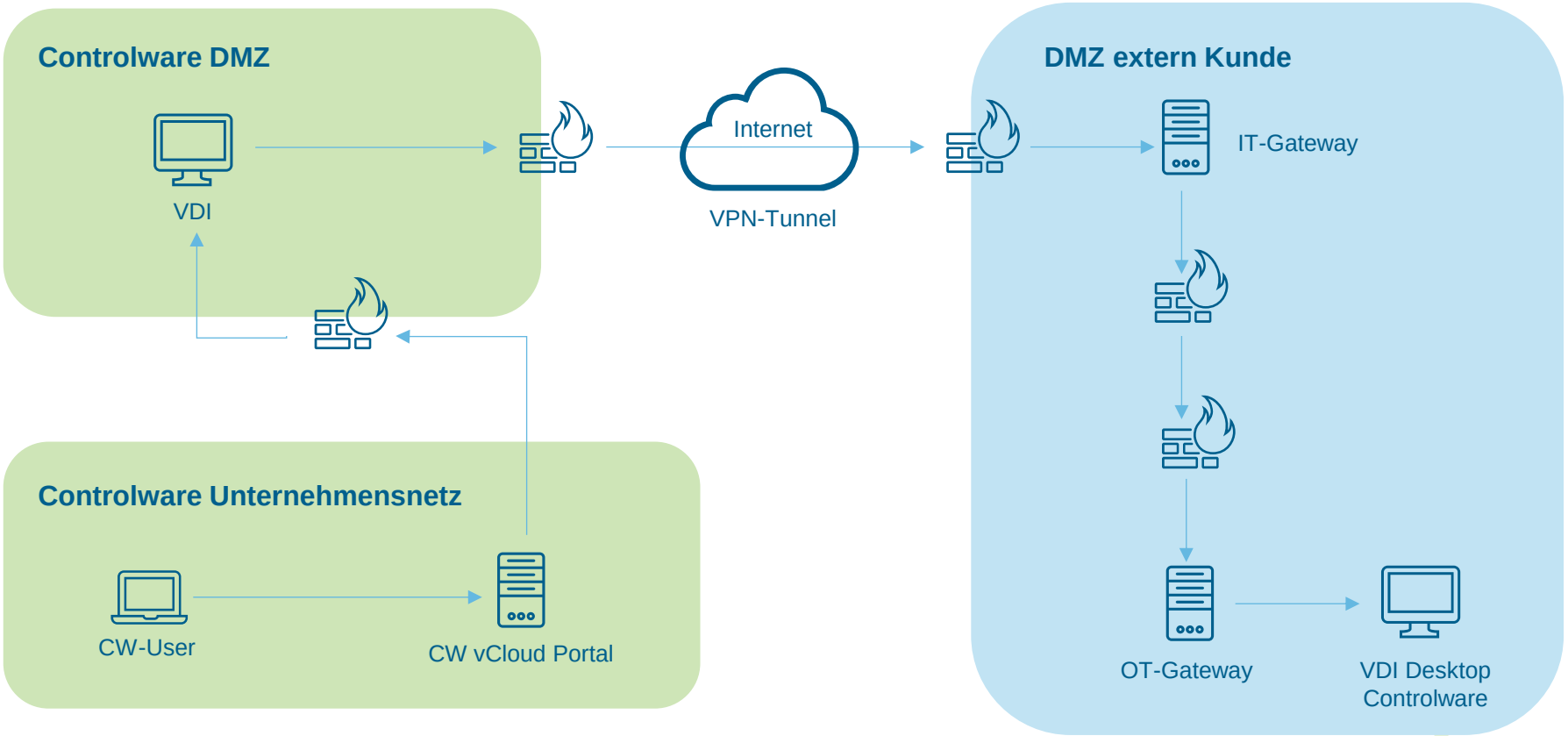
- Direkte Erfassung von Logs und Events aus relevanten OT-Systemen (FW, AD, Backup, vSphere, SzA, etc.)
- Bewertung nach Kritikalität, Wiederholungsfrequenz und Kontextbezug
- Automatische Generierung eines Tickets mit Handlungsempfehlung zur Übergabe an L2-Support

controlware

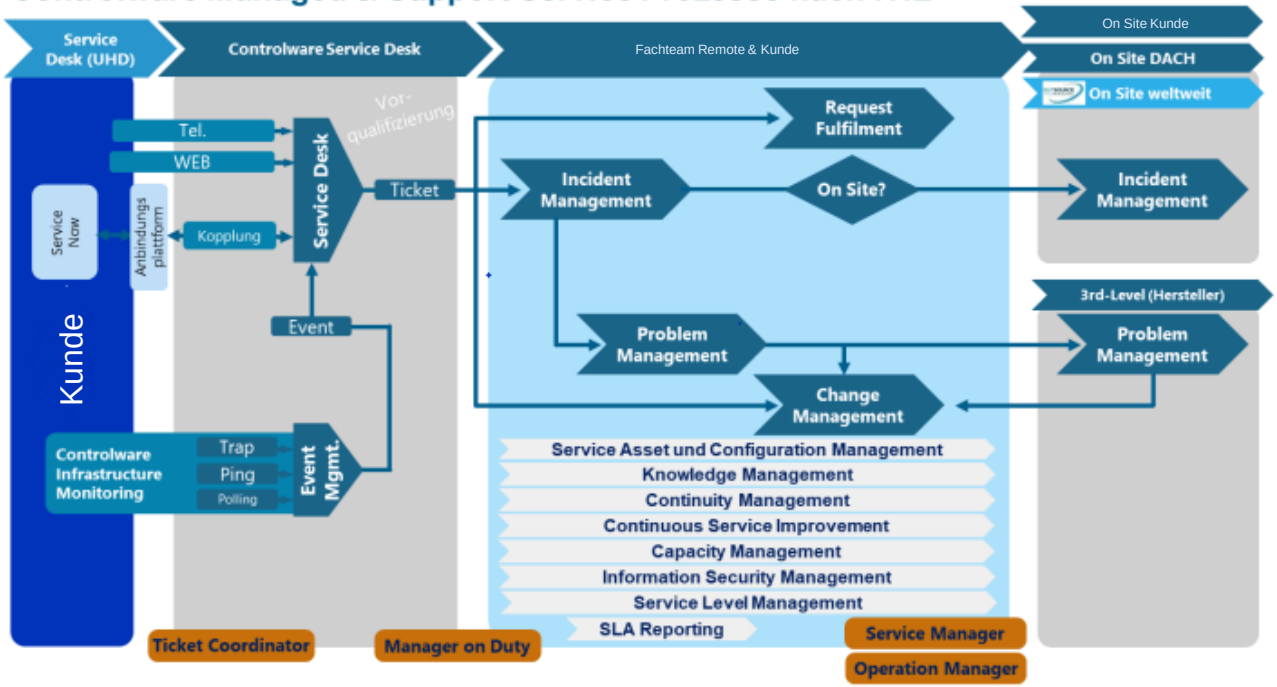
Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!

Anlagen

Remote-Zugriff



Controlware Managed & Support Service Prozesse nach ITIL



Datenquellen für NOC/SOC Betrieb

Datenquelle	Herkunft beim Kunden	Verwendung im NOC/SOC	Notwendig / Optional
Firewall-Logs (z. B. WatchGuard)	Cluster-Logs, Syslog, API-Export	Security Event Detection, Traffic Pattern, Regelverstoß, IPS	Notwendig
Switch-Status / SNMP-Traps (z. B. Aruba)	SNMPv2/3, Syslog, CLI-Abfragen	Link-State, Port-Ausfälle, Flapping Detection	Notwendig
Domain Controller / AD Logs	Windows Eventlog (z. B. via WMI, Winlogbeat)	Login-Fehler, Gruppenänderungen, Kontoänderungen, Bruteforce	Notwendig
Zertifikatdienste / PKI Logs	Windows CA Logs	Ablaufwarnungen, neue Zertifikate, Missbrauchserkennung	Optional
Backup-System (z. B. Veeam)	Veeam REST API, E-Mail Alerts, Syslog	Backup-Fehler, Tape-Probleme, Wiederherstellungstests	Notwendig
Hypervisor / vSphere	vCenter Events via API / Syslog	Host-Status, Snapshots, CPU/Memory-Load, HA-Failover	Notwendig
System Monitoring (CheckMK / Zabbix)	Agent oder SNMP auf Servern / VMs	CPU, RAM, Disk, Prozesse, Auslastungskurven	Notwendig
SzA / Anomalieerkennung (z. B. Rhebo)	ICS-Mirror-Traffic / Sensorboxen	Protokollabweichung, ICS-spezifische Muster, Netzwerkanomalien	Notwendig
Asset- & Konfig-Daten (i-doit CMDB)	Manuell gepflegt oder API-Sync	Kontext für Events, Zuordnung zu Standort / Kritikalität	Notwendig
Patch-/Vulnerability-Daten	WSUS, SCCM , manuelle Listen, CVE-Feeds	Priorisierung von Events, Sicherheitslagebewertung	Optional im MVP, notwendig bei späterem SOC-Ausbau
Pleasant Password Server / PAM Logs	Zugriffshistorie aus dem Vault	Detektion privilegierter Zugriffe außerhalb SLA-Zeiten	Optional
Wartungs-/Betriebspläne	Kalender oder Excel-Dateien aus Betrieb	Kontextabgleich bei Events: „Wartung oder Incident?“	Notwendig
Netzwerkübersicht / Segmentierungsplan	Visio, Netzplandokumentation, ggf. aus i-doit	Impact-Analyse, lateral movement detection	Notwendig
ITSM / Ticketsystem	Service-Ticketsystem	Rückmeldung zu Events, Feedback für KI-Agent, Historie	Notwendig