Deutsche Telekom Security GmbH

Sicherheit durch Sichtbarkeit – Cyber Defense Center der Telekom

TELEKOM SOLUTION X

27. April 2023 | Frankfurt am Main

Deutsche Telekom Security GmbH
„Auf einen Blick“

> 25 Jahre Security KnowHow

Reselling / Best of Breed

Cyber Defense Center

> 1.600 Security-Spezialisten

Managed Services

Analyse und Consulting

Bedrohungslage

- Verschlüsselung von Daten
- Manipulation der Daten
- Diebstahl von Daten

Stillstand / Zerstörung von:

- E-Mail System
- Datenbanken
- Warenwirtschaft
- Webauftritt / Webshop
- uvam.

Produktionsausfälle

Image- / Reputations-Verlust

Verstöße gegen Regularien (DSGVO, BaFin, KRITIS...)

Tip: 14.45 – 15.45 Uhr IT Security – aktuelle Lage – Dr. Rüdiger Peusquens – Raum B.00.22

Lösungsansatz

Die Folgen

- KnowHow Verlust
- Veröffentlichung von:
  - Betriebsgeheimnissen
  - Patenten
  - Personenbezogenen Daten (Mitarbeiter / Kunden / Lieferanten)
- Verbraucherschutz
- Plagiate
- Haftung

Wir orientieren uns am NIST-Standard.

(National Institute of Standards and Technology, US-Bundesbehörde)

Best Practises sind somit:

- Identify
- Protect
- Detect
- Respond
- Recover

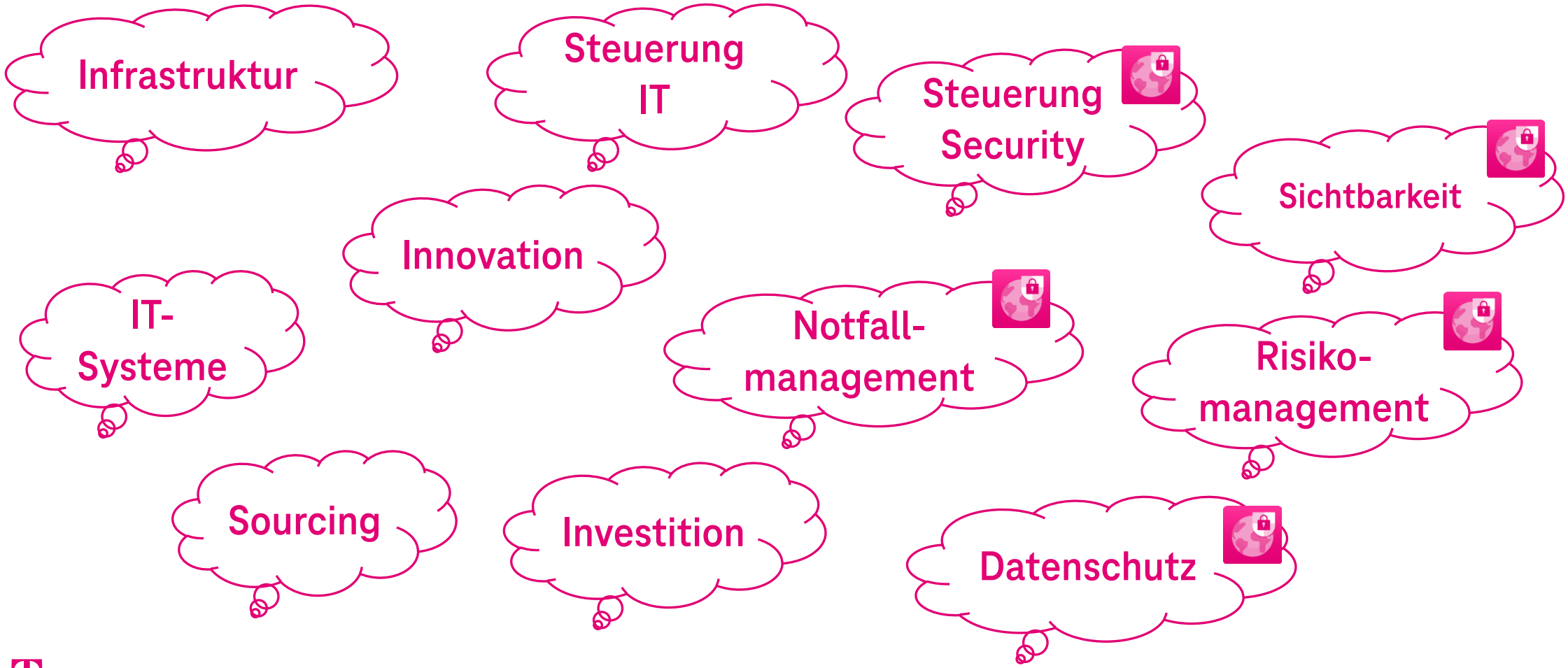
Security @ Telekom

Telekom-Services basierend auf dem NIST-Standard:

(NIST = National Institute of Standards and Technology)

- **Identify:** **ISMS-/Risiko-Beratung, Prozess-Beratung, Best-Practise-Workshops**
  Identifikation von business-kritischen Systemen, Daten, Funktionen und Prozessen
- **Protect:** **Design-Beratung, Vorschläge & Implementierung**
  Implementierung geeigneter Schutzmaßnahmen, techn. Voraussetzungen schaffen
- **Detect / Respond:** **Managed Cyber Defense Service (SOC)**
  Erkennen eines Vorfalls und Reaktion zur Gefahrenabwehr
- **Recover:** **Incident Response Service**
  Bereinigung betroffener Systeme

Kombination von IT-Strategie und Security-Strategie



Prävention alleine reicht nicht länger aus...

DETECT

RESPOND

Managed Cyber Defense

SOC

PREVENT

DETECT

RESPOND

Was ist Managed Cyber Defense?

ERKENNEN

VON INFILTRATIONEN, ANGRIFFEN, DATENVERLUST UND ANDEREN CYBERSECURITY INCIDENTS

IN EINER FRÜHEN PHASE

UM SIE ZU STOPPEN

BEVOR SCHÄDEN ENTSTEHEN.

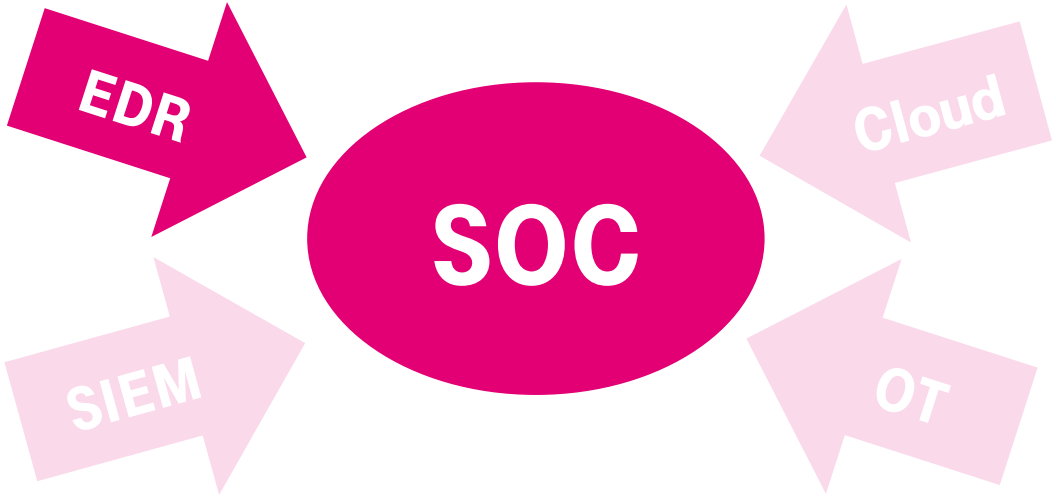
Wie wir vernetzte IT- und OT-Systeme ganzheitlich schützen:
Sicherheit aus integriertem IT-/OT-Security-Operations-Center

Wie wir vernetzte IT- und OT-Systeme ganzheitlich schützen:
Sicherheit aus integriertem IT-/OT-Security-Operations-Center

Security Operations Center:

- **24x7 Alarm-Monitoring**
- **Strukturierte Event-Analyse und Alarm-Handling**
- **Einleitung von Gegenmaßnahmen und Angriffsabwehr**
- **Betrieb der Monitoringsysteme**
- **Entwicklung von Run-/Playbooks und Detektionsszenarien**
- **Bereitstellung von Ticketsystem und Reporting**
- **Incident Reponse Services**
- **Threat Intelligence:**
  - Honey Pots
  - Foren/MISP
  - Netzbeobachtung
  - Fortlaufende Analyse aller im SOC auflaufenden Informationen

Wie wir vernetzte IT- und OT-Systeme ganzheitlich schützen:
Sicherheit aus integriertem IT-/OT-Security-Operations-Center



Endpoint Detection & Response:

- Monitoring des Endpunkts mittels Endpunktagenten
- Transparenz & Sichtbarkeit der IT-Umgebung
- Risikobewertung
- NextGen Antivirus
- Automatische Alarmerzeugung
- Verhaltensanalyse (Prozesse/Nutzer)
- Netzwerkanalyse am Endpunkt
- Erkennung unbekannter Malware
- Manuelle Gegenmaßnahmen
- Automatische Gegenmaßnahmen
- Effiziente Untersuchung von Bedrohungslagen

Wie wir vernetzte IT- und OT-Systeme ganzheitlich schützen:
Sicherheit aus integriertem IT-/OT-Security-Operations-Center

Security **I**nformation and **E**vent **M**anagement:

- **Monitoring und Echtzeitanalyse umfangreicher Logquellen:**
  - Firewall
  - AD-Informationen
  - Syslogs
  - DNS, IDS, IPS,...
  - etc.
- **Korrellation der Rohdaten im SIEM-System**
- **Automatische Filterung und Sortierung der Events**
- **Umfassende „Security Visibility“ zur Abwehr aktueller und potentieller Bedrohungsszenarien**

Wie wir vernetzte IT- und OT-Systeme ganzheitlich schützen:
Sicherheit aus integriertem IT-/OT-Security-Operations-Center

OT-Security:

- **Schutz der Produktionsanlagen vor Angriffen, Spionage und Sabotage**
- **Überwachung der Steuerungs- und Automatisierungs-systeme mit i.d.R. passiven Sensoren**
- **Anomalieerkennung auf Basis selbstlernender Überwachungssysteme (Machine Learning)**
- **Deep Packet Interpretation der produktionstypischen Protokolle**
  - SCADA
  - Siemens S7
  - Modbus
  - etc.

Tip: 13.30 – 14.30 Uhr OT Security – Bernd Jäger – Raum D.00.22

Wir betreiben Europas größtes integriertes Cyber Defense- und Security Operation Center in Bonn

1. **MASTER CDC + SOC**
2. **MAGENTA HERZSCHLAG FÜR CYBER SECURITY “MADE IN GERMANY”**
   Central Incident Coordination, Threat-Intelligence, Forensic
3. **ZUSAMMENARBEIT ALLER SOCS**
   (Bonn, Wien, Budapest,...)
4. **> 240 CYBER SECURITY PROFESSIONALS**
5. **MANAGEMENT FÜR KUNDEN JEDER GRÖSSE UND AUS JEDER INDUSTRIE**

Incident Response Service

„Im Falle eines Falles“

Onboarding Workshop

- Assesment von ICT Security Infrastruktur, Reaktionsplänen und Prozessen
- Erfahrene Forensiker führen das Onboarding onsite oder offsite durch

Hotline

- 24/7-Support bei Security-relevanten Fragen
- Erste Erfassung der Situation und schnelle Bewertung der Situation
- Festlegung der next steps
- Durchführung erster technischer Analysen

Request for Information

- Beantwortung spezieller Fragen im Kontext Threat Intelligence
- Analyse einer speziellen Bedrohung; Verfolgung einer Bedrohungs-kampagne oder Zusammenfassung von Ransomware

Incident Koordination

- 24x7 Projekt-management durch spezialisiertes Team
- Unterstützung der Kundenorganisation bei Koordination, Nach-haltung von Aktivitäten für Bearbeitung von Incidents
- Erstellung einer gemein-samen Eskalations-matrix als Grundlage

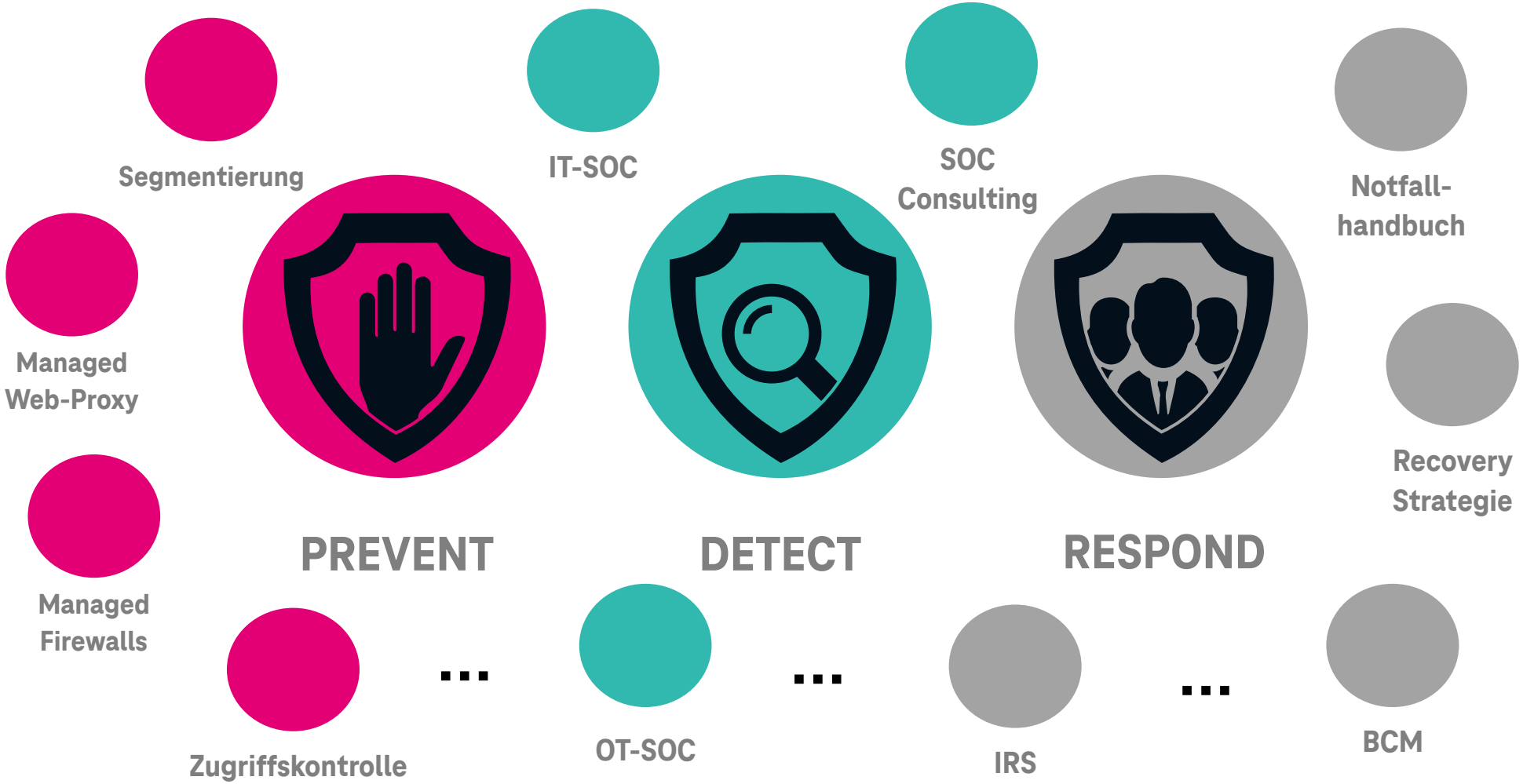
Incident Handling (Forensik)

- Abruf erfahrener Krisen-Spezialisten in den Phasen Planning, Investigation – Control – Elimination – Recovery & Post-Incident Analysis
- Onsite- oder offsite-Einsätze
- Durchführung von Digital Forensik- und/oder Malware-Analysen

Incident Retainer

- Bereitstellung eines vereinbarten Stundenkontingent
- Abruf der Teilleistungen durch den Kunden
- Nicht benötigte Stunden können bis zu 50% für Sicherheitsberatung, Penetrationstest oder weitergehende TI-Services genutzt werden

Managed Cyber Defense @ Telekom
Unsere Services



DANKE

ANDREAS VELTEN

- DIPL.-ING., SOLUTION SALES DESIGNER -

MOBIL: 0151 64840401

MAIL: A.VELTEN@TELEKOM.DE

LIFE IS FOR SHARING.