telent

Security Operation Center

Angriffserkennung leicht gemacht

Digitalisierung

erfolgreich gestalten.

Daniel Weber

telent | Netzwerktag - 21.06.2023

telent

service • commitment • value

Housekeeping

Daniel Weber – (telentsche‘ Staatsangehörigkeit seit 2016)

- 2016 - 2019 | Security Solutions Consultant
- 2019 - 2021 | Senior Security Solutions Consultant
- Seit Mitte 2021 | Teamleiter Security Solutions – TCSL

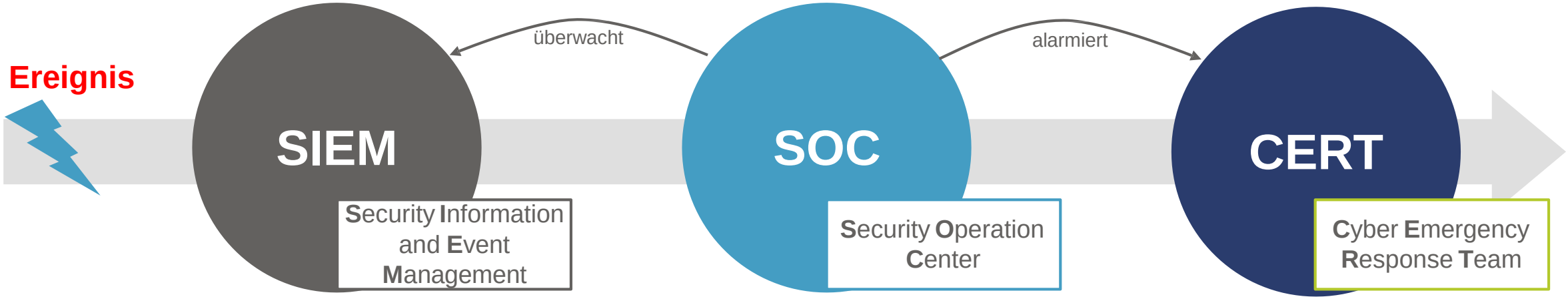
- Fragen bitte am Ende der Session und gerne beim Get Together.

Agenda

- Terminologie
- Vorstellung telent - Security Operation Center
- Projektablauf SOC Projekt

Terminologie

SIEM ≠ SOC ≠ CERT



Ist ein Werkzeug UND Prozess

- Ziel des SIEM ist die Erkennung und Analyse von sicherheitsrelevanten Vorgängen (in Echtzeit).
- Eine SIEM-Lösung sammelt, aggregiert, korreliert und visualisiert verschiedene Informationsquellen (z. B. Logdaten).

Ist eine Organisationseinheit

- Ein SOC besteht aus einem Expertenteam welches definierten Prozessen und Vorgehensweisen folgt, um Bedrohungen für IT-Systeme und Informationen zu entdecken und auf diese schnell und effektiv zu reagieren.

Ist eine (ad-hoc) Formation

Ein CERT ist eine Gruppe von (Sicherheits-) Fachleuten, die auf konkrete IT-Sicherheitsvorfälle reagiert.

Ein SOC ist mehr als nur ein Tool zum Monitoring des Netzwerks!

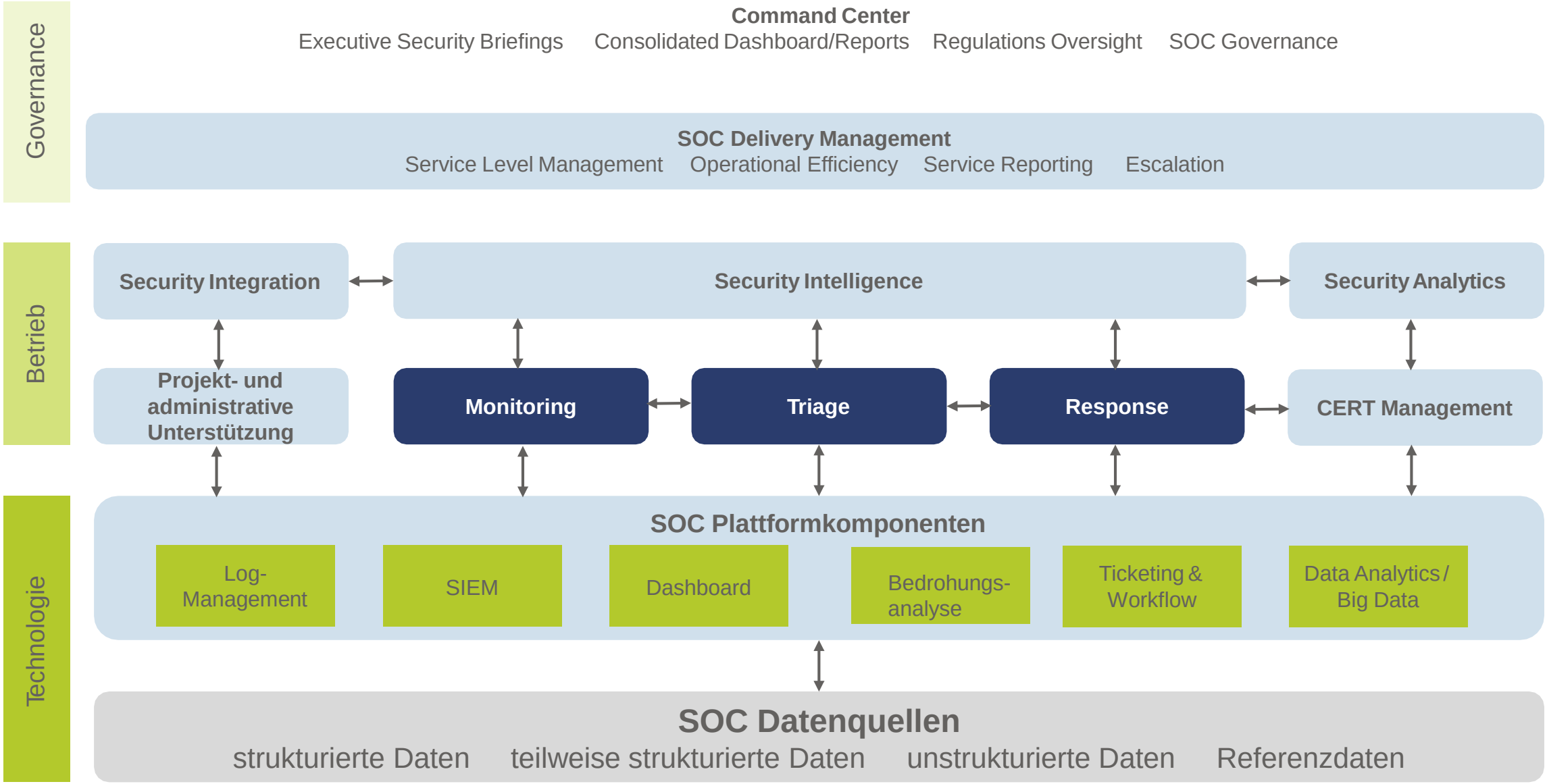
Systeme zur Angriffserkennung

Der Begriff „Systeme zur Angriffserkennung“ (SzA) bezieht sich auf eine große Bandbreite an technischen und organisatorischen Maßnahmen, die zur Angriffserkennung dienen. Diese überwachen die informationstechnischen Systeme des laufenden Betriebs, um jegliche Auffälligkeiten, die auf Cyber-Angriffe hindeuten, schnellstmöglich identifizieren zu können.

- BSIG § 8a (1a)

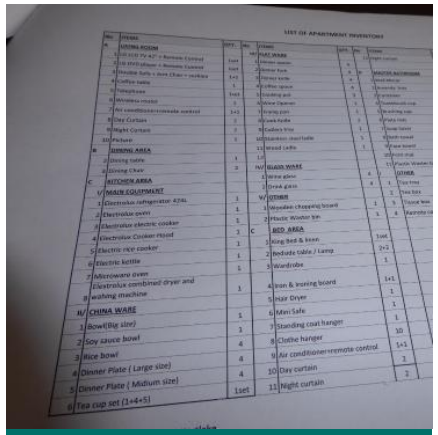
„Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung.
Die eingesetzten Systeme zur Angriffserkennung *müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten*.
Sie sollten dazu in der Lage sein, *fortwährend Bedrohungen zu identifizieren* und *zu vermeiden* sowie für eingetretene Störungen *geeignete Beseitigungsmaßnahmen* vorzusehen“

Referenzmodell – Security Operation Center



telent
service • commitment • value

Bausteine der Informationssicherheit (NIST Framework)



Identifizieren

Was muss geschützt werden?

- Inventar der Werte
- Geschäftsumfeld
- Vorgaben
- Risikomanagement

Schützen

Wie wird der Schutz umgesetzt?

- Zugriffsmanagement und - steuerung
- Sensibilisierung und Ausbildung
- Datensicherheit
- Informationsschutzrichtlinien
- Schutztechnologie

Detektieren

Wie werden Angriffe erkannt?

- Auffälligkeiten und Vorfälle
- Überwachung
- Detektionsprozess

Reagieren

Wie sieht die Reaktion aus?

- Reaktionsplanung
- Kommunikation
- Analyse
- Schadensminderung
- Verbesserungen

Wiederherstellen

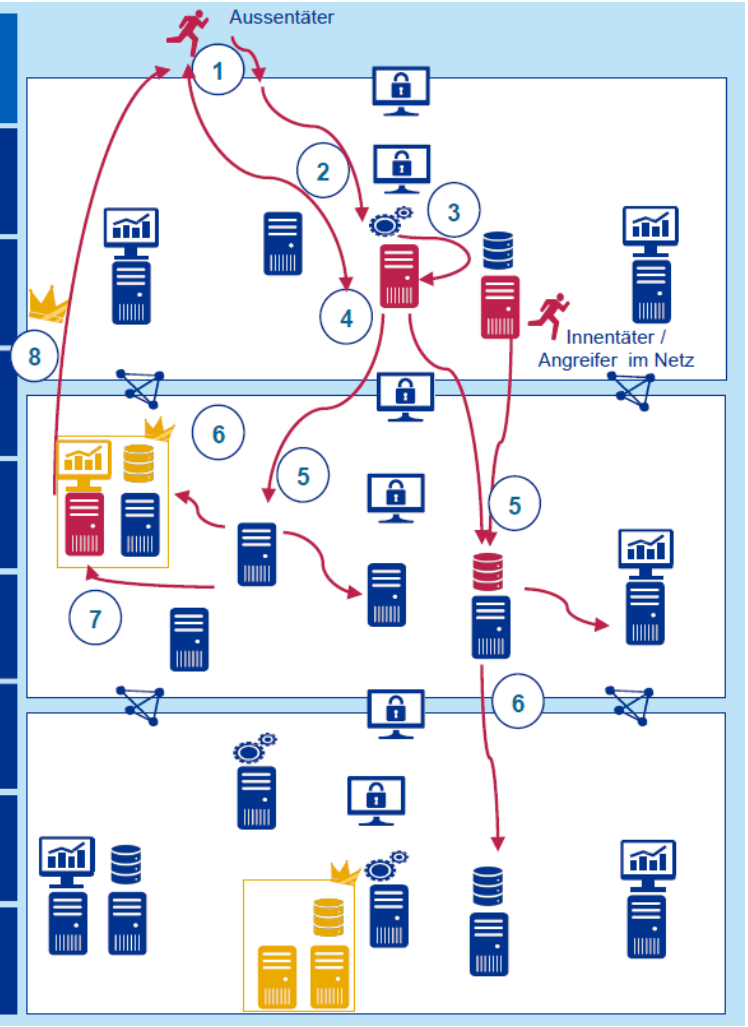
Wie werden Systeme wiederhergestellt?

- Wiederherstellungsplanung
- Kommunikation

Security Operation Center (SOC)

Ablauf eines Cyberangriffs

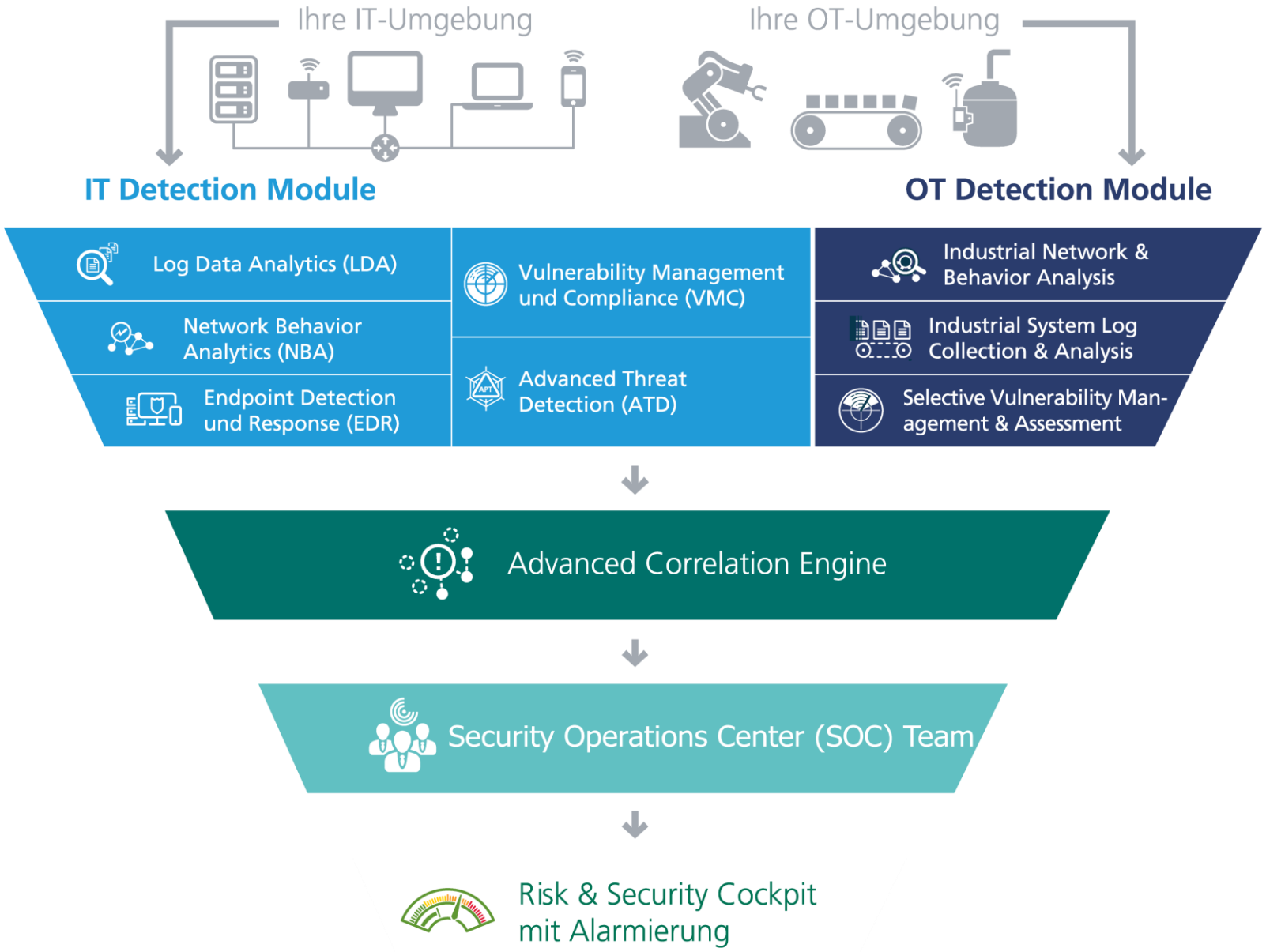
		Exemplarische Darstellung Detektionsszenarien
1	External Reconnaissance	Port Scans from External Source Scan Detected by IDS …
2	Attack Delivery	Attacks against Webservices Mail related Attack Delivery …
3	Exploit & Installation	Malware Detection Remote Code Execution …
4	Command & Control	Suspicious Outbound Traffic Command and Control Traffic …
5	Local Compromise	Suspicious Activity on Windows Suspicious Activity on Linux …
6	Internal Recon	Internal SNMP Scans Internal TCP Scans …
7	Lateral Movement	Suspicious Remote Logins Unusual Login Attempts & Account activity …
8	Exfiltration/Manipulation	Suspicious Outbound Data Transfer …



telent

Security Operations Center

Konsolidierte IT- und OT-Security



Log Data Analytics (LDA)

Logdatenanalyse mit Machine Learning und Use-Case-Forschung

Die Sammlung, Analyse und Korrelation von Logdaten aus verschiedensten Quellen ist die Kerndisziplin der IT-Sicherheit. Diese Art der Erkennungsleistung wird oftmals über ein SIEM verwirklicht. Das Resultat: Sicherheitsrelevante Informationen und Indicators of Comprise in Echtzeit, die schnellstmögliche Maßnahmen bei einem Sicherheitsvorfall erlauben.

- Unterstützung gängiger Log-Formate
- Aggregation von Events und Informationen aus allen Bereichen
- Identifizierung potentieller Risiken durch die Correlation Engine mit kontinuierlich erweiterten und maßgeschneiderten Regeln und Policies

Network Behavior Analytics (NBA)

Erkennung von gefährlicher Malware, Anomalien und anderen Risiken im Netzwerkverkehr auf Basis von signatur- und verhaltensbasierten Detection Engines.

- Mehr als 19.000 kontinuierlich erweiterte, mit IP-Reputationsdaten verglichene, Signaturen und Regeln
- Verhaltensbasierte Analysen für Zero-Day-Exploits und andere noch nicht bekannte Angriffsarten, Erkennung von Protokollen und Ports
- Identifizierung verschiedener Dateitypen anhand der MD5-Prüfsummen und weitergehen der Dateiextraktion, um Dokumente gegebenenfalls nicht in oder aus dem Netzwerk transferieren zu lassen

Vulnerability Management & Compliance (VMC)

Kontinuierliche, interne und externe Schwachstellen-Scans mit umfassender Erkennung,

- Kontinuierliche interne und externe Schwachstellen-Scans für einen 360-Grad-Überblick
- Authentifizierte oder nicht-authentifizierte Schwachstellen-Scans
- Erkennung von offenen Ports und der Nutzung von potentiell unsicheren oder überflüssigen Services auf diesen Ports
- Compliance- und Passwort-Checks zur Erkennung von Konfigurationsproblemen in Bezug auf Anwendungen und Passwörter- sowie Benutzerrichtlinien
- Empfehlungen zur Schwachstellen-Kategorisierung in hohes, mittleres und geringes Risiko und die Möglichkeit ihrer Ausnutzung

Industrielle Netzwerkverhaltensanalyse

- Erkennung aus Protokoll- und Flow-Daten
- Metadaten-Extraktion aus industriellen Protokollen
- Automatische Analyse durch Machine Learching

Industrielle System-Protokollsammlung und Analyse

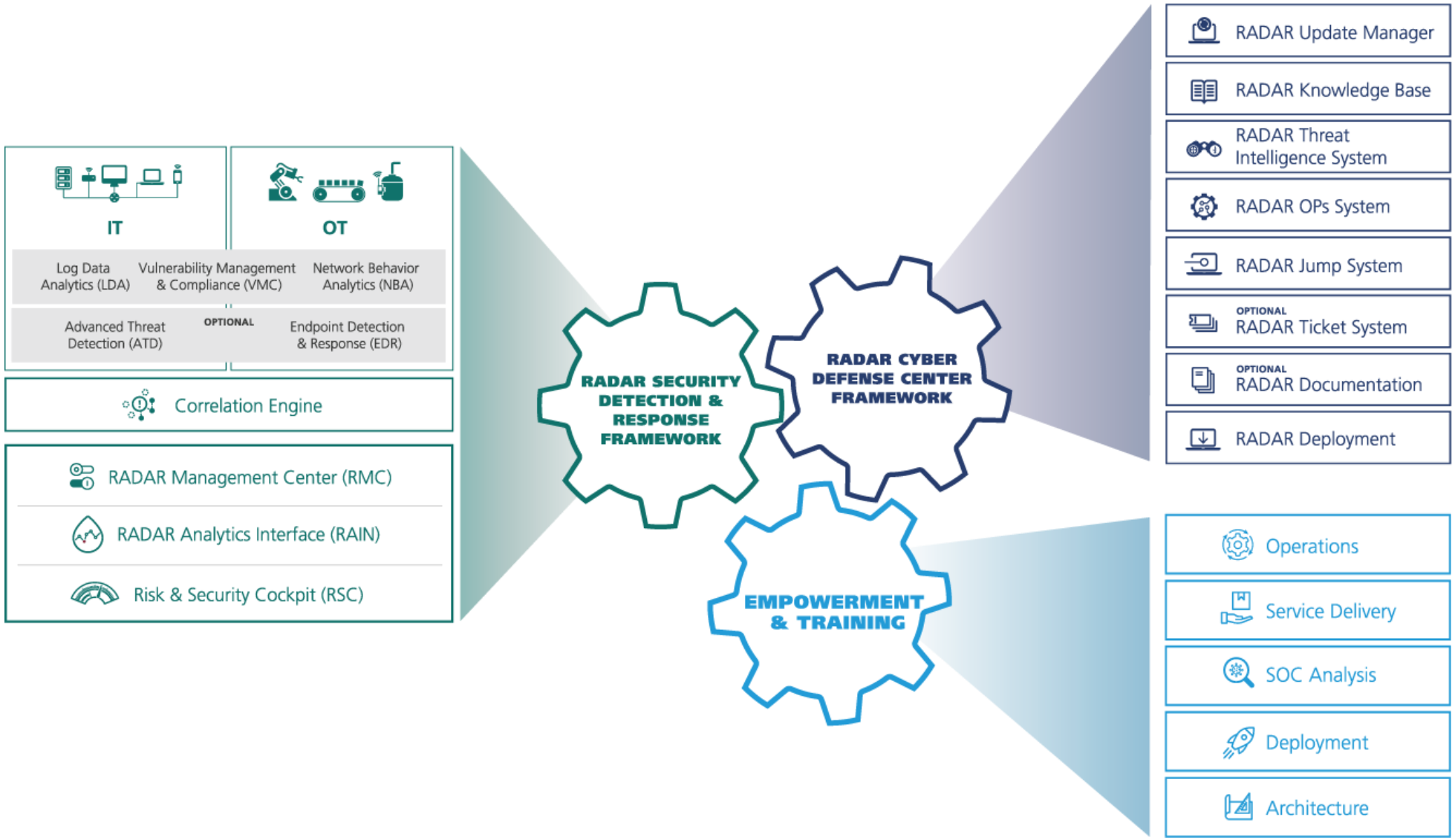
- Erkennung von sicherheitskritischen Vorgängen und Anomalien auf der Grundlage von definierten Use Cases
- Sammlung, Normalisierung und Korrelation von OT-Logs
- Erweiterte Korrelation mit integrierter IT- und OT-Protokolldatenanalyse

Advanced Correlation Engine

Die Korrelation innerhalb eines Moduls und die Cross-Korrelation von Informationen aus verschiedenen Modulen führen zu einer hochqualitativen Erkennung von Risiken und Sicherheitsproblemen. Dies ermöglicht einen umfassenden Blick auf die sicherheitsrelevanten Vorkommnisse innerhalb eines Unternehmens.

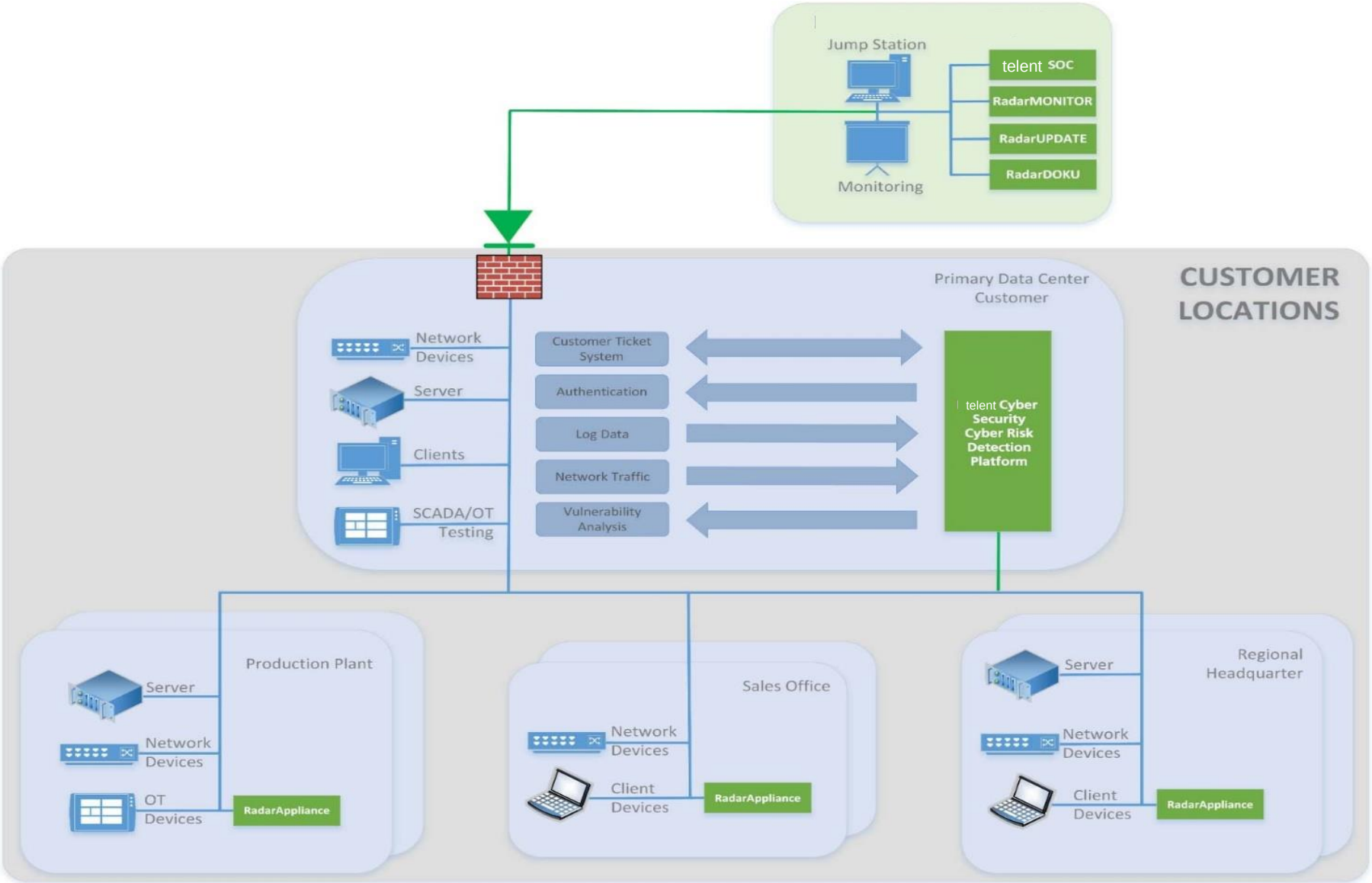
- Gesamtüberblick über sicherheitsrelevante Daten
- Miteinbeziehung von Logs, Schwachstellen, Anomalien, Asset-Informationen
- und vielem mehr
- Korrelation und Cross-Korrelation basieren auf Regeln, Policies
- und selbstlernenden Algorithmen
- Unterscheidung zwischen normalem und abnormalem Verhalten in der IT- und OT-Infrastruktur
- Alarmierung in kritischen Situationen

Technik des telent SOC im Detail



telent
service • commitment • value

Architektur - Aufbau



telent
service • commitment • value

Architektur - Systeme

- **Radar Core - Presentation Layer**
  - Management Center
  - Risk and Security Cockpit
- **Radar Worker - Orchestration Layer**
  - Log Collector
  - Parsing and Normalization
  - Correlation
- **Radar Data - Orchestration Layer**
  - ElasticSearch Database
- **VMC - Network Layer**
  - Scan Networks and Assets
- **NBA - Network Layer**
  - Collect and analyze network traffic

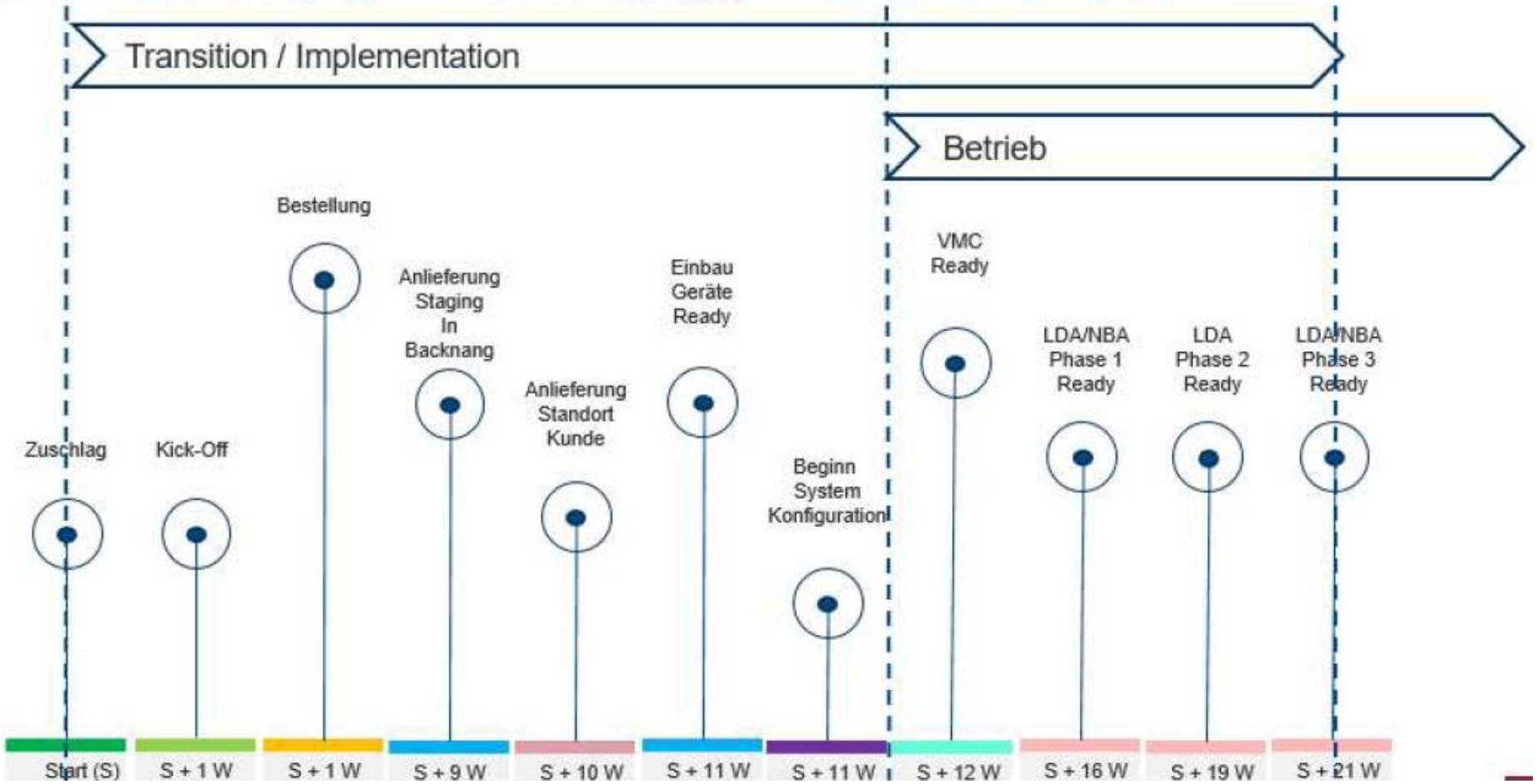
Projektablauf SOC Projekt

Beispiel SOC Projekt - Leistungsumfang

- Leistungsumfang
  - Log Data Analytics/LDA
  - Network Behaviour Analytics/NBA
  - Vulnerability Management/VMC
  - 350 Assets

- Hardware Radar Appliances
  - 1 x Radar Core 2000
  - 1 x Radar Data 2000
  - 1 x Radar Appliance NBA1G

Technische Implementierung - Meilensteinplan



telent
service • commitment • value

Beispiel SOC Projekt - Implementierung

Die Implementierung des SDRF nimmt üblicherweise mehrere Monate in Anspruch und beinhaltet folgende Punkte:

- Die Bereitstellung der RCS Hardware Appliance
- Die Aufnahme der Netzwerk Infrastruktur
- Die Anpassung an die IT-Infrastruktur
- Die Konfiguration der Schwachstellenanlyse –Umgebung
- Die Einbindung der Log-Devices und Log-Quellen
- Die Implementierung der Parser und Korrelationsregeln
- Die Dokumentation und Einrichtung des Fernzugriffs

Die Implementierung inkludiert die Konfiguration der Installation auf Basis vordefinierter Korrelations- und Alert-Einstellungen sowie die Anbindung der definierten Log Quellen.

Vielen Dank für Ihre Aufmerksamkeit!

Daniel Weber
Senior Manager Security Solutions
Mobil: 0151-16714394
E-Mail: daniel.weber@telent.de

Digitalisierung

erfolgreich gestalten.

telent
service • commitment • value