Bechtle Security – Cyber Defense Center DOK FORUM 2024

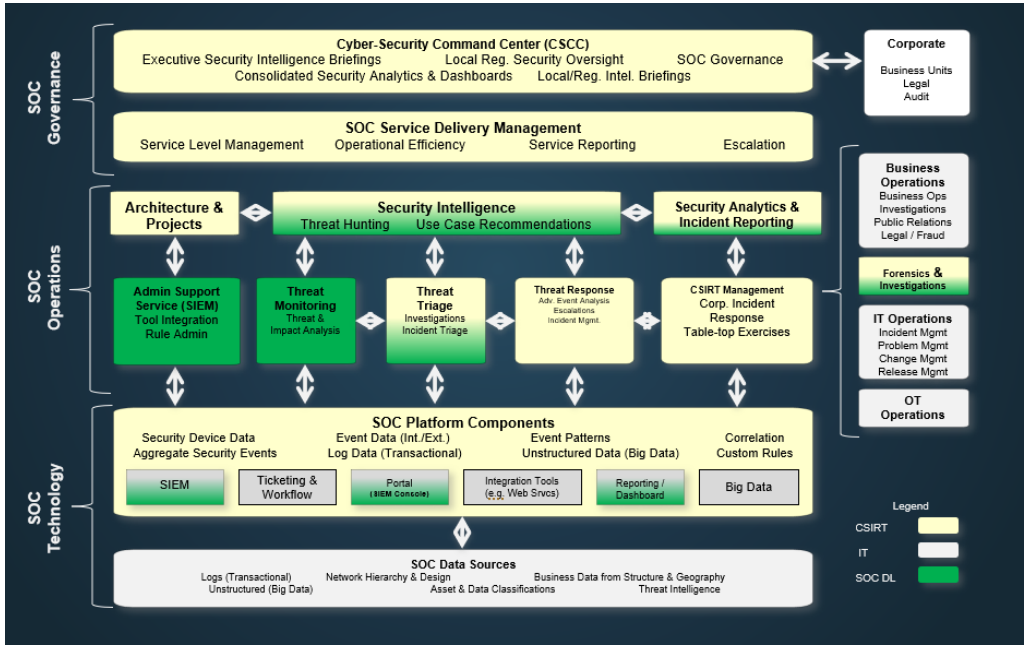
27.11.2024

Georgios Salustros
Bechtle CDC Presales

Next Generation SOC?

SOC Blueprints und Services sind designed für Großkunden:

- Der Kunde ist 24/7 erreichbar mit fachlicher Expertise
- Der Kunde kann die Triage finalisieren und im CERT die Bearbeitung der Incidents übernehmen bzw. orchestrieren
- Tayloristische Arbeitsweise bzw. Zusammenspiel zwischen Kunde und Dienstleister



Aber was ist, wenn der Kunde diese Voraussetzungen nicht erfüllt?

Wer stellt den Boom überhaupt fest?

Wer stellt den Boom überhaupt fest?

Kunde aktiviert den APT-Service

SOC-Dienstleister

APT-Response-Dienstleister + Kunde

Prävention | Detektion | Reaktion

Welche SLOs hat der Kunde selbst?

Die Schlüsselfragen für viele Kunden sind:

1. Ist in den Randzeiten ein Kundenmitarbeiter zeitnah verfügbar, der bei einem entdeckten (durch den Dienstleister) und eskalierten Angriff qualifiziert reagieren kann?

2. Ist die Einleitung einer Reaktion durch den Kunden in jeder Situation der richtige Weg?

Bechtle CDC Integrierter Service mit Detektion und Reaktion

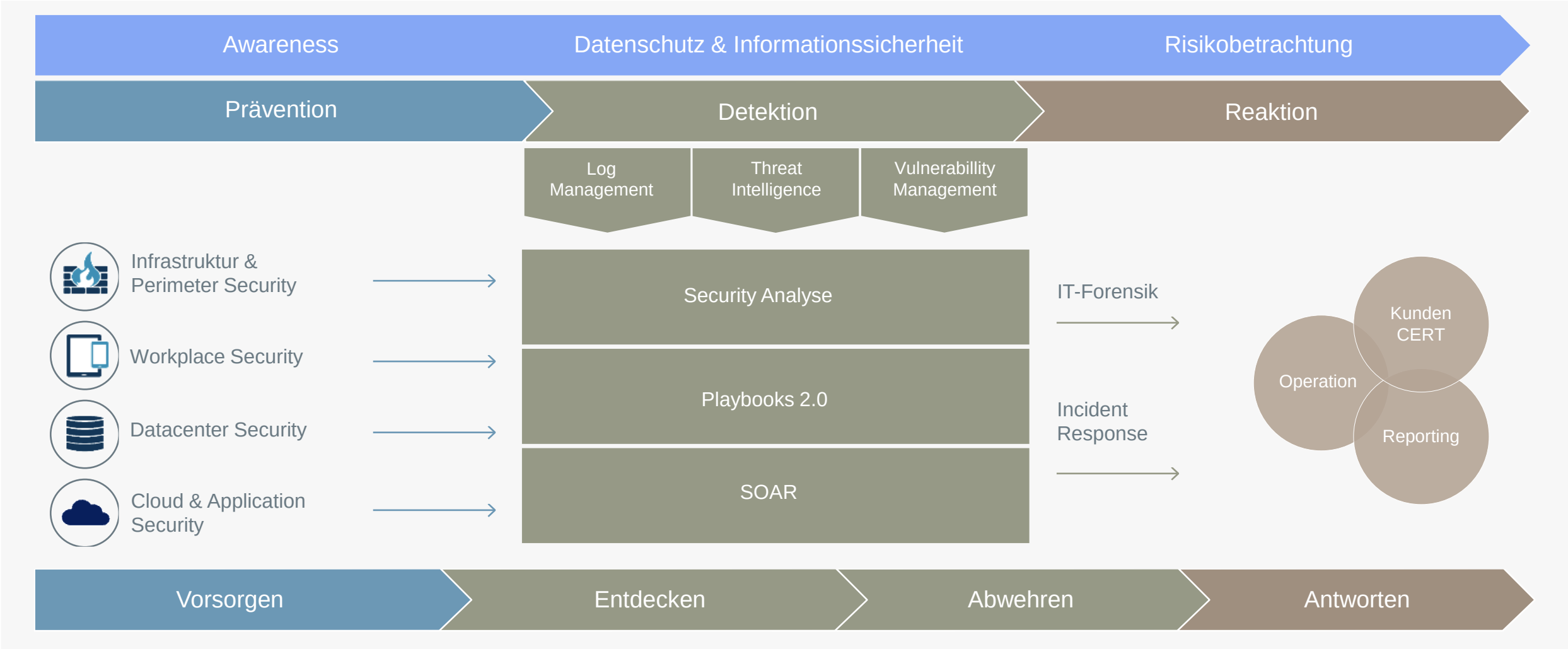
Wer stellt den Boom überhaupt fest?

Damit das Notfallkonzept anlaufen kann, muss der Notfall erst entdeckt werden
Hacker nutzen die Randzeiten für die Angriffe

- **Wirksamkeit des Bechtle CDC**

Prävention → Detektion → Reaktion

Cyber Defense Konzept



Philosophie Bechtle SOC - „Feuermelder + Sprinkleranlage“

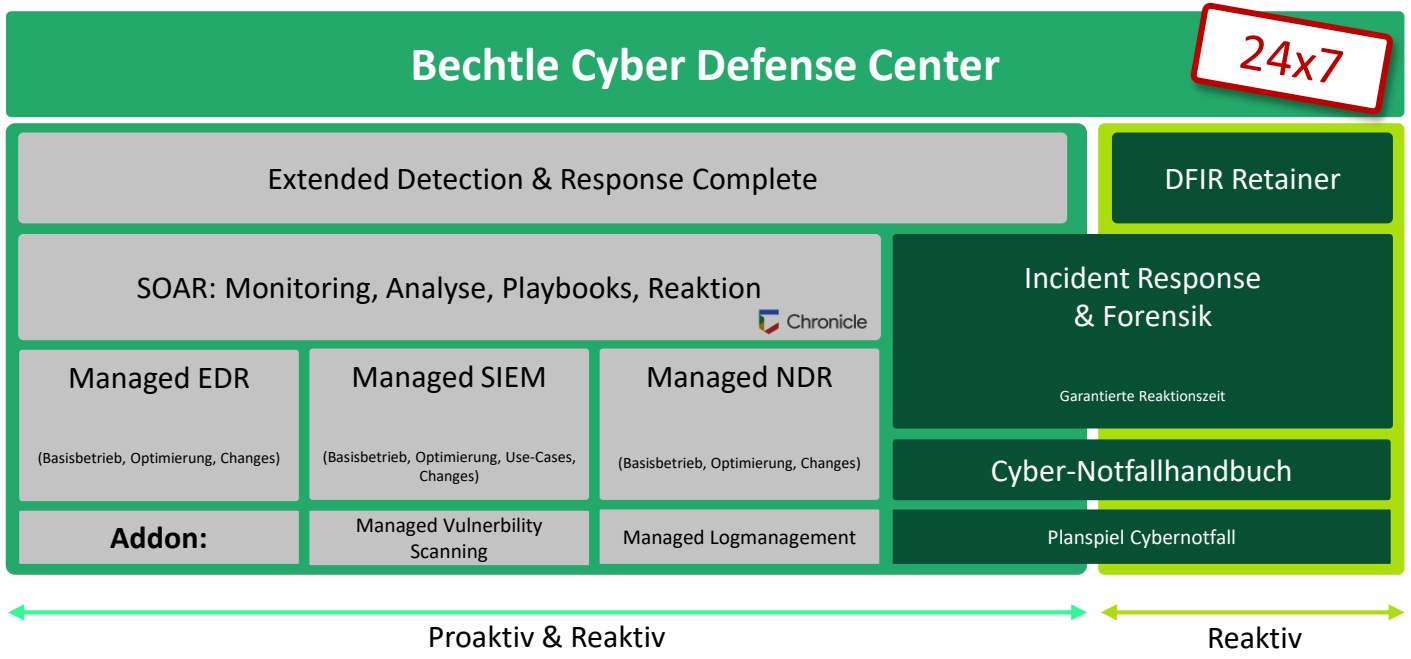
Automatisierung und Verkürzung der sogenannten „Mean Time To Respond“:

- Erfolgreiche Abwehr von bereits laufenden Angriffen und das bestmögliche Unterbinden von Schäden
- Automatisierte Playbooks 2.0 – mit Reichweite bis in IT-Ops

Erfahrene SOC-Analysten mit übergreifendem Know-how in IR, IT-Forensik und Monitoring

Bechtle CDC – Modulares Konzept mit „Best of Breed“ Technologien

- **24x7** Überwachung
- **Betrieb** der eingesetzten Security-Werkzeuge
- Einheitliche **Governance-Struktur**
- **Volle Transparenz**



Bechtle CDC - Arbeitsweise

Personal

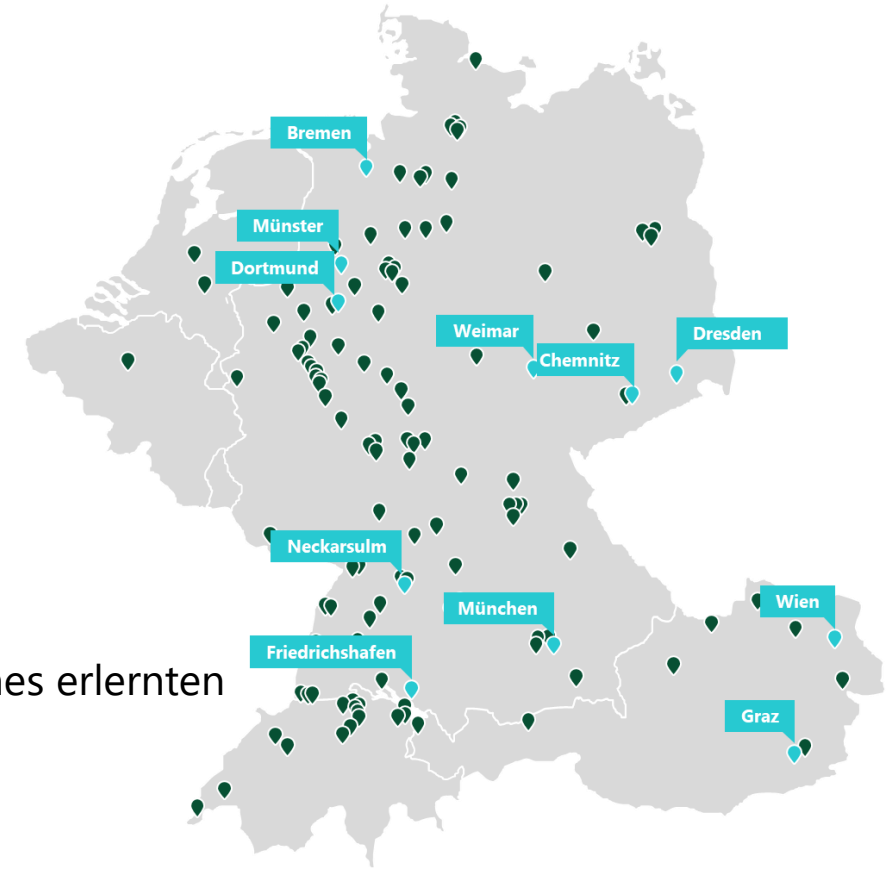
- Analyse und Forensik in Personalunion
- 1st Level durch SOAR, 2nd Level durch SOAR/Analysten
- Deutlich weniger Personalbedarf und günstigere Produktion

Effektivität

- Technologien, Prozesse und Skills sind auf Reaktion ausgerichtet
- Schnellere Eindämmung von Angriffen

KI-Unterstützung / Automatisierung

- Behavioral Analysis basierende Systeme erkennen Anomalien auf Basis eines erlernten Normalzustandes
- Fokus liegt auf Playbooks mit Schnittstelle zu IT-OPS
- Incident Automatisierung und Effizienz in der Bearbeitung von Standard-Situationen



Wenn doch etwas passiert ist…

- Krisenmanagement, Planung und Koordination erforderlicher Maßnahmen (+ Vor-Ort Unterstützung)
- Forensik:
  - Gegebenenfalls Aufbau, Installation und Konfiguration der Analyseplattform
  - Sammlung und Sicherung wichtiger Informationen beispielsweise von Windows- (Logs, Events, Images), Firewall-, NDR- oder EDR-Systemen
  - Analyse der gesicherten Daten, Forensische Analyse und Verhaltensanalyse des Netzwerkverkehrs sowie der Aktivitäten auf den Endgeräten
  - Einsatz von geprüften Security-Tools
  - Entwicklung einer Kommunikations- und Response-Matrix
- Recovery:
  - Entwicklung kurzfristiger und langfristiger Lösungsansätze
  - Entfernen von Schadsoftware, Aufzeigen von Sicherheitslücken, Unterstützung bei der
  - Behebung entstandener Schäden bis hin zur Beratung bei Neuanschaffungen von Hard- und Softwarelösungen
- Dokumentation der durchgeführten Maßnahmen
- Präsentation und Übermittlung der Ergebnisse

Zusammenspiel CDC mit lokalen Systemhäusern

Symbiose von Zentralkompetenz mit Kundennähe

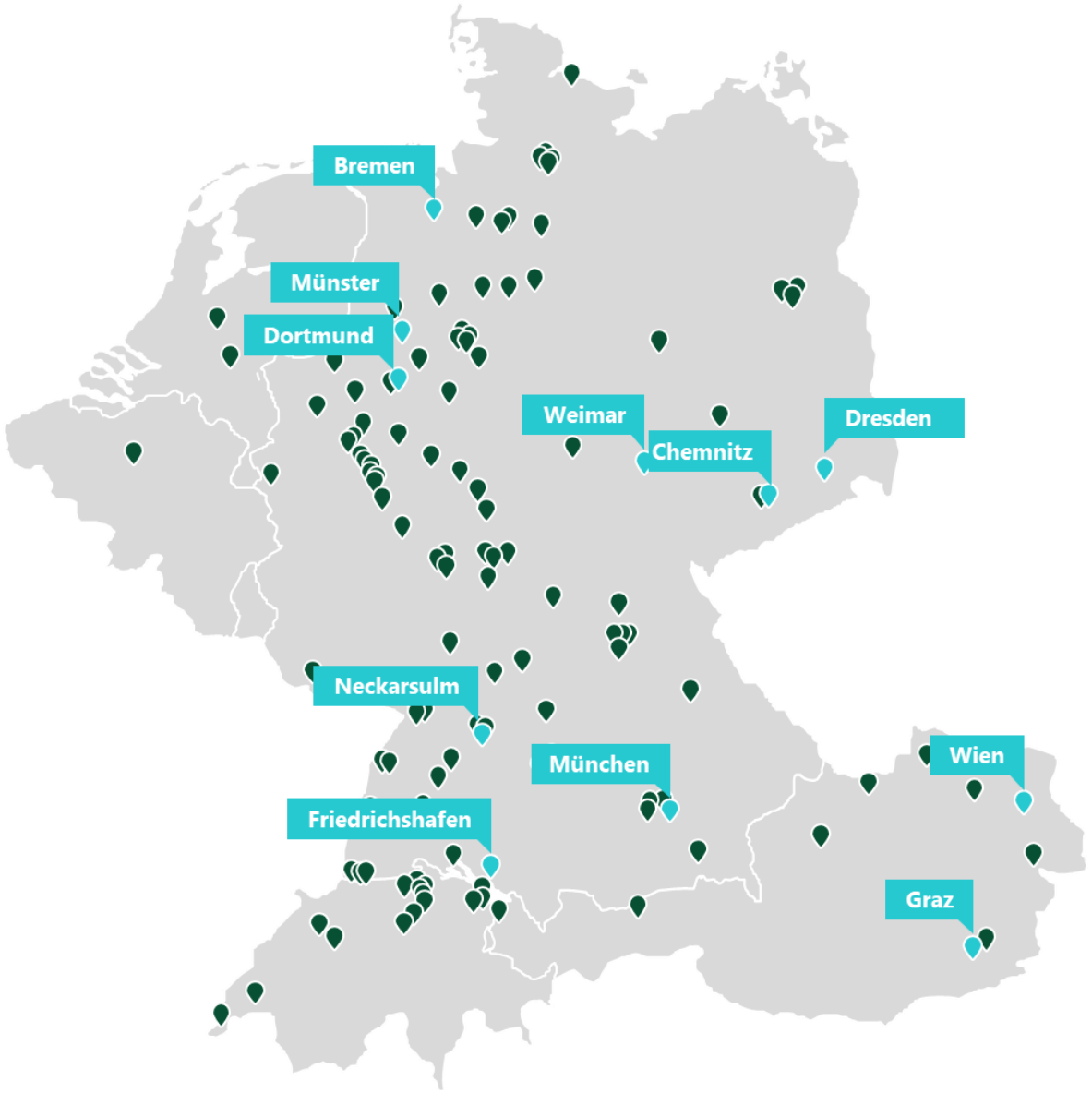
Zur Spurensicherung und ggf. Strafverfolgung

- Forensische Sicherung von Datenträgern
- Unterstützung bei der Ermittlung des Täters
- Aufrechterhaltung der Beweiskette (Chain of Custody)
- Einsatz von bewährten Methoden und Technologien zur forensischen Analyse digitaler Spuren
- Dokumentation der Ergebnisse als forensisches Gutachten

CDC Kennzahlen und Lokationen

Zahlen aus 2024:

- 30 CDC Mitarbeitende
- 60 DFIR Incidents (bis zur Jahresmitte)
- 236 Playbooks
- 1700 Alarme je Tag
- 56.413 Cases im letzten Jahr
- >70 Kunden



Bechtle CDC – wofür wir stehen

1. Sprache
   - Alle Mitarbeiter im CDC sprechen Deutsch und auch die Response ist **deutschsprachig**
2. **EU-Lösung** – gilt für Technologie und Mitarbeiter
3. **Transparenz** – der Kunde hat vollen Einblick ins Geschehen
4. **Co-Managed** als Option
   - Viele Hersteller fordern eine sehr strikte Trennung zwischen Managed Service sowie Eigenleistung des Kunden ein. Beispiele sind der Betrieb der Plattform durch den Hersteller oder Usecaseentwicklung. Einige Kunden wollen teils einen gesharten Ansatz mit Unterstützung in den Randzeiten – Bechtle macht dies möglich
5. Remediation Support
   - Bechtle ist nah am Kunden – kann also bei einer schweren Attacke auch **bei der Recovery unterstützen** (Aufsetzen Server/Endpoints, Daten-Wiederherstellung etc.)
6. Preismodell
   - Das CDC Preismodell basiert auf der Mitarbeiteranzahl des Kunden, ist also **denkbar einfach und planbar**
7. Bechtle - **ein starker Partner**
   - Das Managen unterschiedlicher Partner stellt für viele Kunden eine Herausforderung dar. Mit Bechtle haben sie einen starken Partner, der von Awareness bis Incident Response unterstützen kann.

bechtle