
15. BECHTLE IT-FORUM
THÜRINGEN
2024
BECHTLE
15. Mai 2024 • STEIGERWALD Stadion Erfurt
Hewlett Packard Enterprise
cisco Partner
HUAWEI
intel.

Von Angriff bis Verteidigung: Das Bechtle Cyber Defense Center im Kampf gegen Hacker

05.2024 | Patrick Sommer | Bechtle Cyber Defense Technical

Agenda.

1 Einleitung.
2 Unsere Leistungen.
3 Aktuelle Bedrohungslandschaft.
4 Schlussfolgerung.
5 Q&A.

Einleitung.

Wer bin ich?

Patrick Sommer

IT Solutions Architekt Security

CompTIA+

Netzwerk
Secruity

ISC2

CISSP

Projektmanagement

Prince2

Hersteller

Sophos
Macmon
Trellix (McAfee)
Crowdstrike
Cybereason
Cisco
Darktrace

Wer bin ich?

Patrick Sommer

IT Solutions Architekt Security

CompTIA+

Netzwerk
Secruity

ISC2

CISSP

Projektmanagement

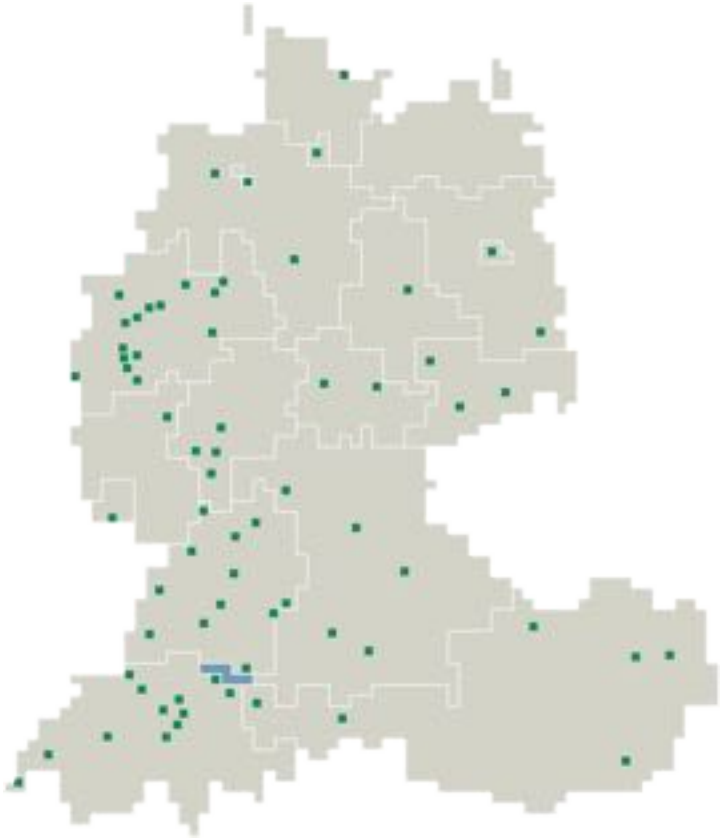
Prince2

Hersteller

Sophos
Macmon
Trellix (McAfee)
Crowdstrike
Cybereason
Cisco
Darktrace

Wer sind wir im CDC?

- Cyber Defense Center Plattform
  - Wien
- Forensic Labors
  - Wien
  - Dresden
  - Chemnitz
  - Neckarsulm
  - Bodensee
  - Dortmund



Cyber Defense Center Personal

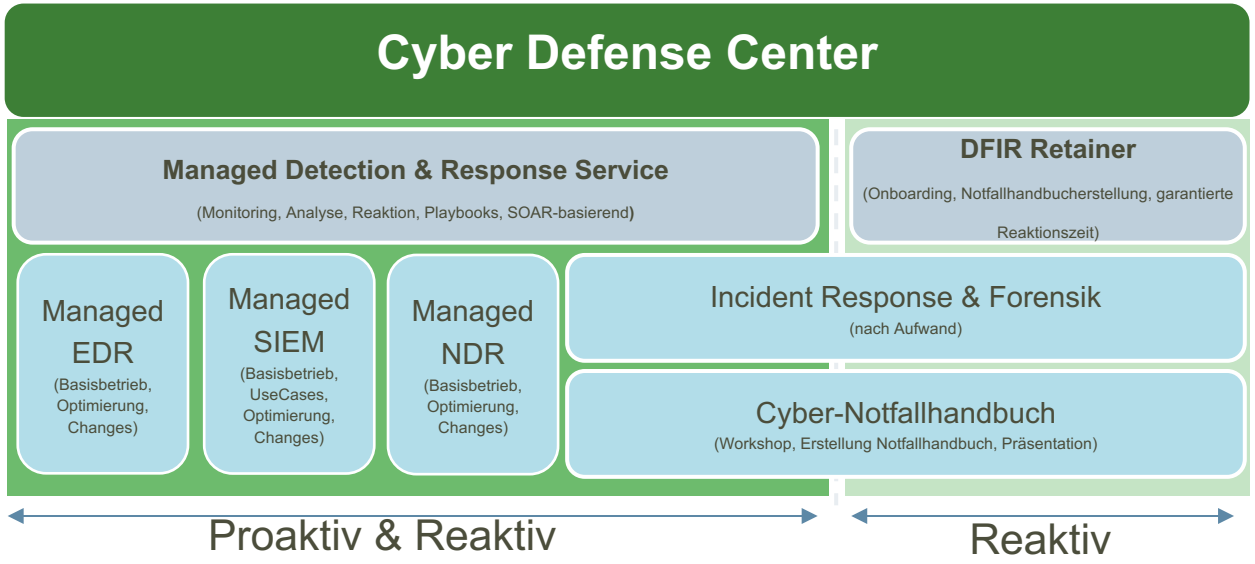
- Wien
- Dresden
- Chemnitz
- Neckarsulm
- Bremen
- Hille
- Bielefeld
- Dortmund

Vorgehensweise in der Krisenbewältigung

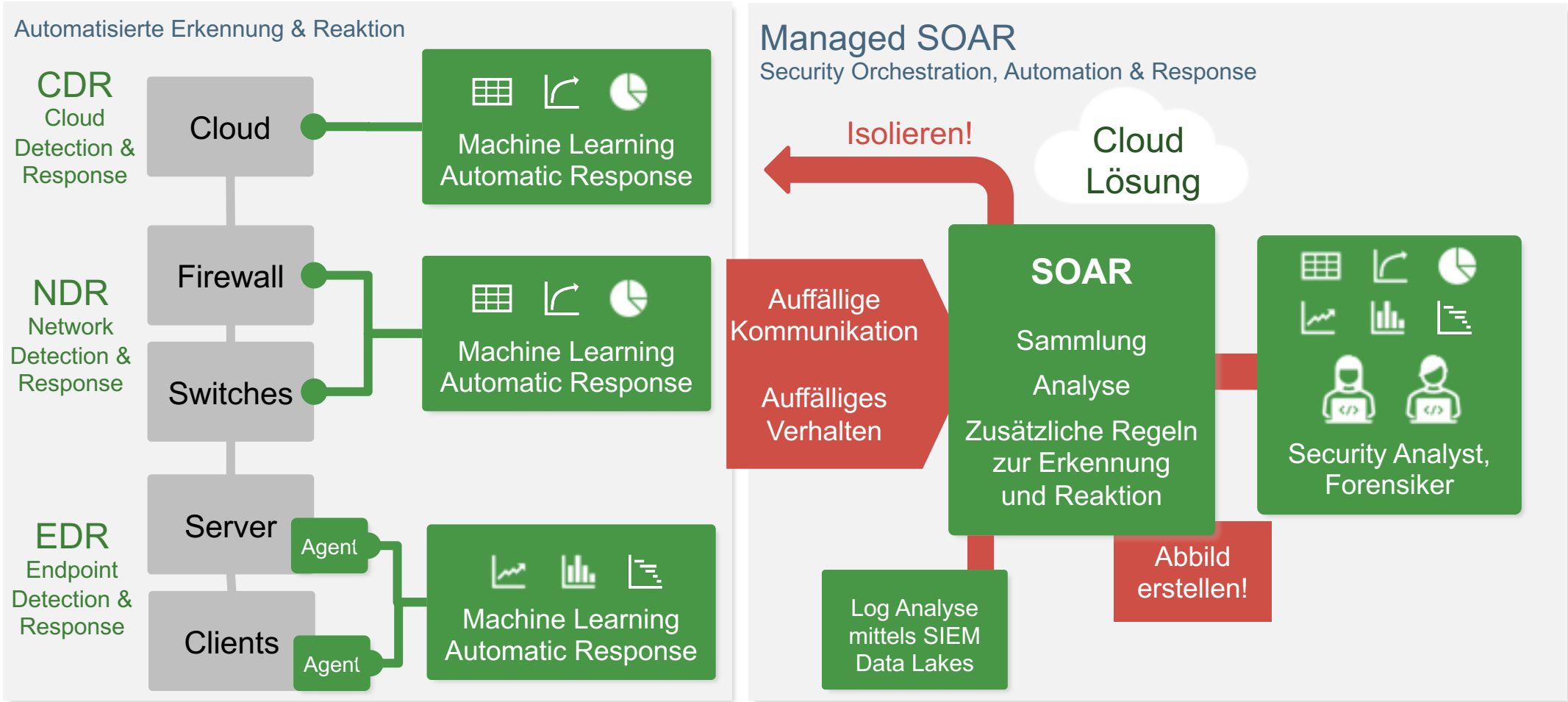
Unsere Leistungen.

Managed Security Services
CDC-Portfolio

- Modular aufgebaut
- Kunden-individuell
- Wächst mit den Anforderungen



Next Generation Cyber Defense
Bechtle SOC Plattform



Incident Response
Wenn dennoch was passiert ist…

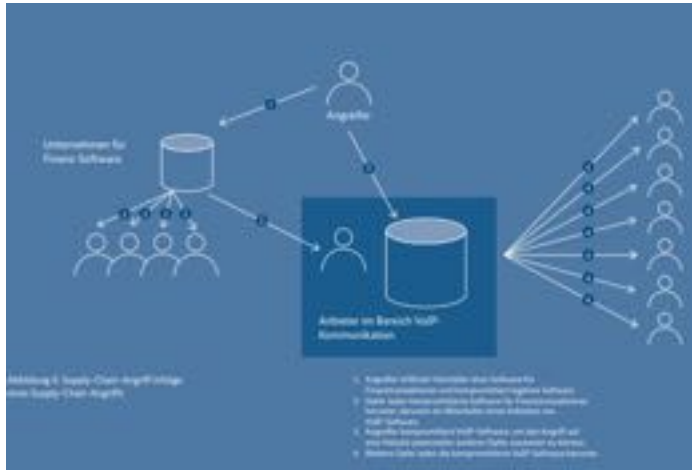
- Krisenmanagement, Planung und Koordination erforderlicher Maßnahmen
- Gegebenenfalls Aufbau, Installation und Konfiguration der Analyseplattform
- Sammlung und Sicherung wichtiger Informationen beispielsweise von Windows- (Logs, Events, Images), Firewall-, NDR- oder EDR-Systemen
- Analyse der gesicherten Daten, Forenische Analyse und Verhaltensanalyse des Netzwerkverkehrs sowie der Aktivitäten auf den Endgeräten
- Entwicklung einer Kommunikations- und Response-Matrix
- Einsatz von geprüften Security-Tools
- 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

Bechtle Kontaktdaten
Telefonnummer:
+49 7132 981 2783
E-Mail-Adresse:
help.sirt@bechtle.com

Bundesamt für Sicherheit in der Informationstechnik

Aktuelle Bedrohungslandschaft.

BSI-Lagebericht



CDC-Lagebericht

Häufigsten Angriffssektoren

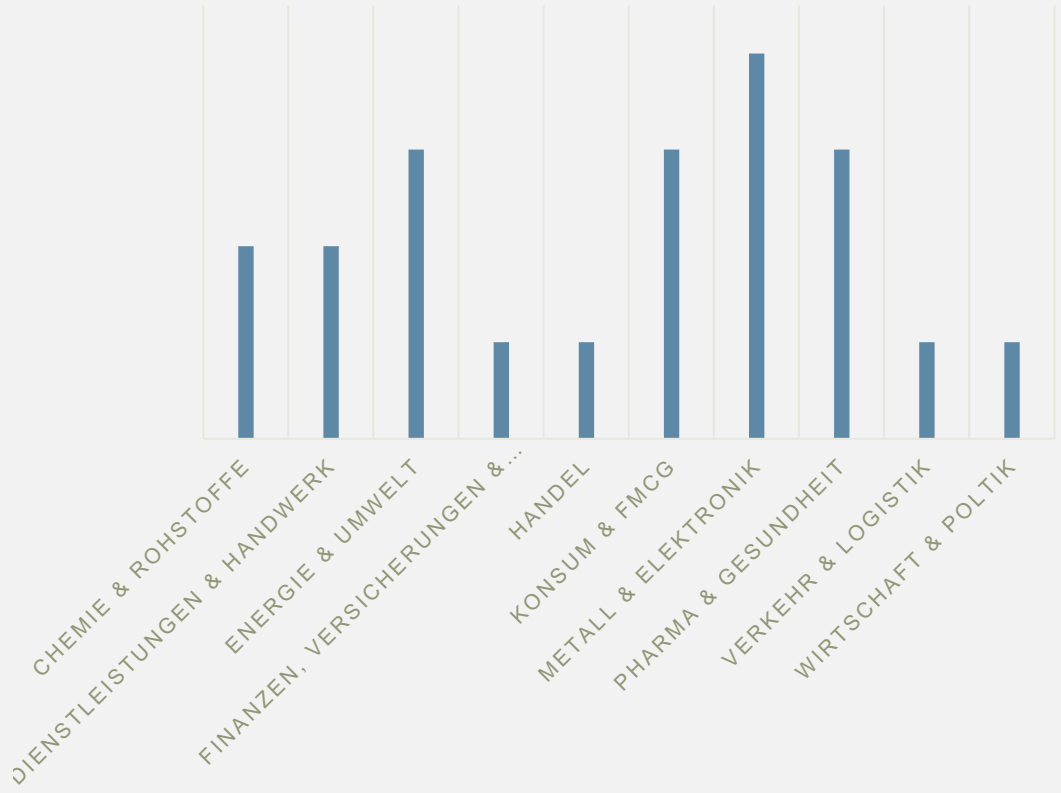
- Exploits/Zero Day Lücken
- Malware/Ransomware

- E-Mail/Phishing
- Insider Bedrohungen/Supply Chain Attacken
- E-Mail/Fraud

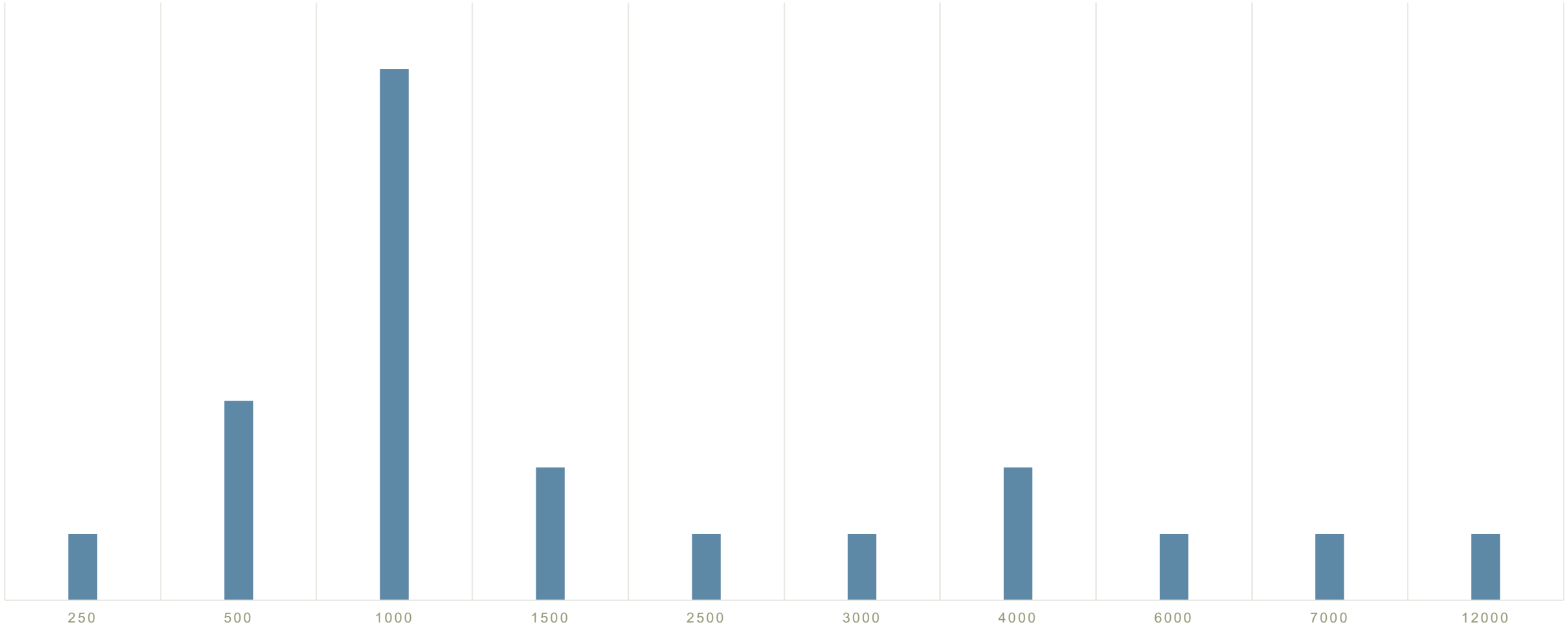
Häufigsten Erkennungstool

- EDR
- Mailsecurity
- SIEM
  - Firewall
  - IDS
- AV-Software
- Vulnerability Management
- NTA

Häufigste Angriffe

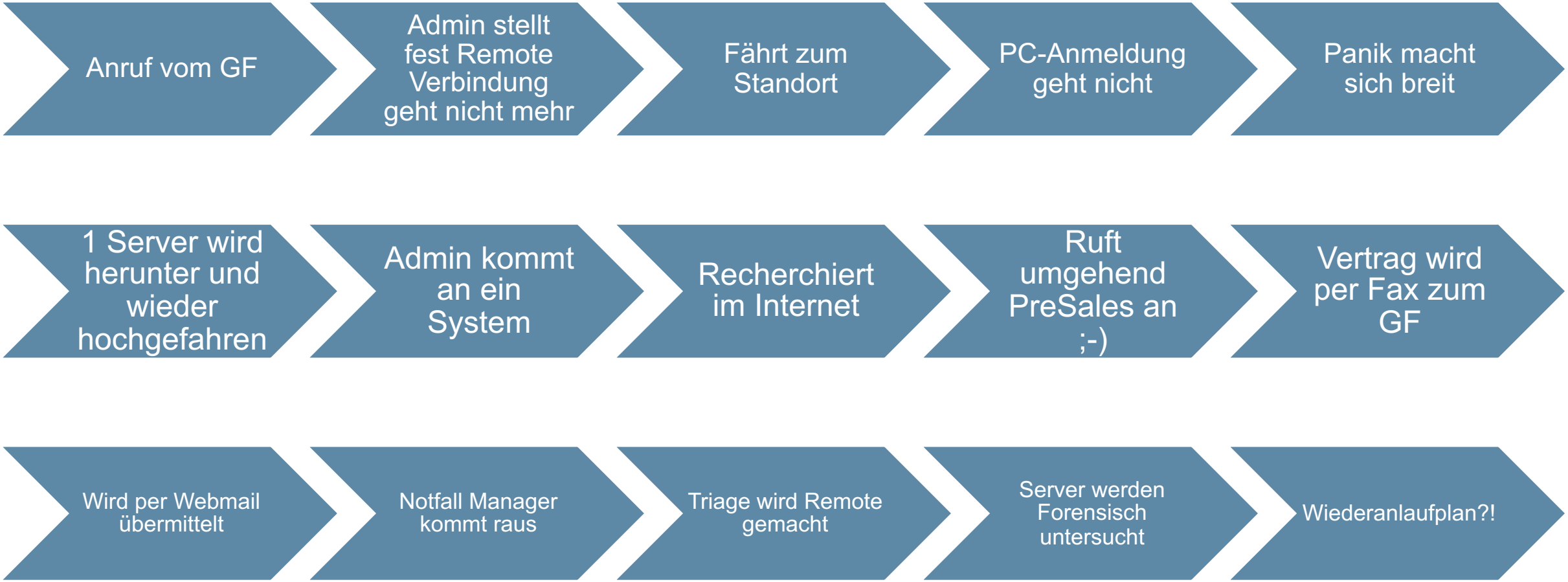


CDC-Lagebericht



CDC - Angriffsbericht

Kunde im September CDC 24*7 Angriffserkennung vorgestellt > Projekt auf 2024/2025 verschoben



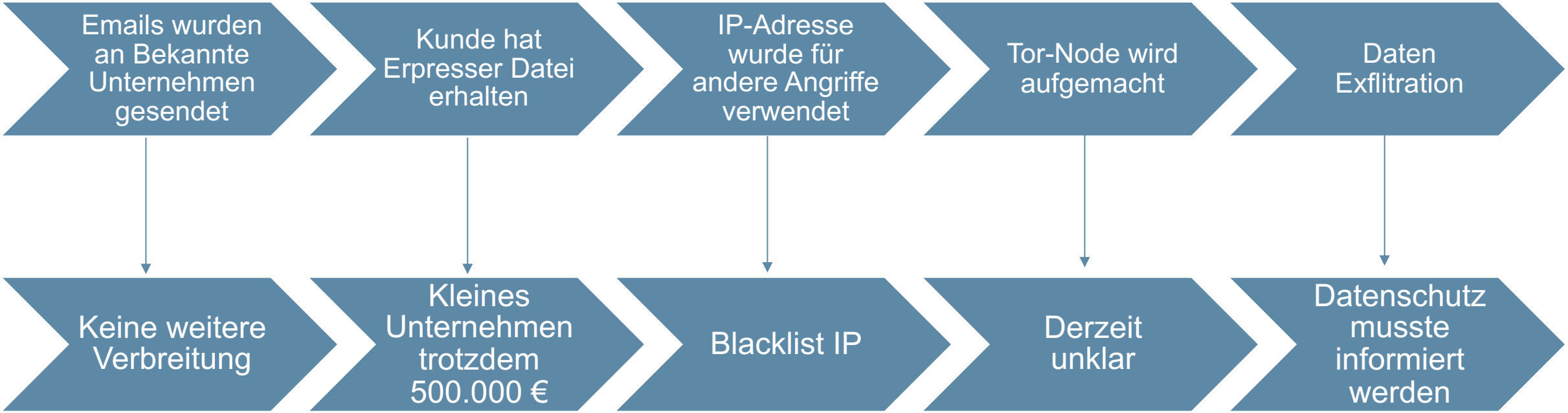
IT-Forensik

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 – Bericht danach

Was war parallel passiert



Schlussfolgerung.

Was ist zu tun wenn es passiert ist ?
Incident Bearbeitung

Lockdown
- Kein Internet-Zugriff (in/out)
- Firewall oder ReverseProxy
- IIS-Dienste beenden
- Server isolieren

Analyse
- Bin ich betroffen?
- Malware- & IoC-Scan
- Malware removal
- Risiko-bewertung

Reparieren
- Aktuelle CUs installieren
- Security Update installieren

ODER:
- Neuaufbau

Auswertung
- Forensische Sicherung
- Risiko-/ Sicherheits-bewertung
- Meldung nach DSGVO?

Incident Response

Wenn dennoch was passiert ist…

- Krisenmanagement, Planung und Koordination erforderlicher Maßnahmen
- 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
- Entwicklung einer Kommunikations- und Response-Matrix
- Einsatz von geprüften Security-Tools
- 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

Vorgehensweise in der Krisenbewältigung

Q&A.