

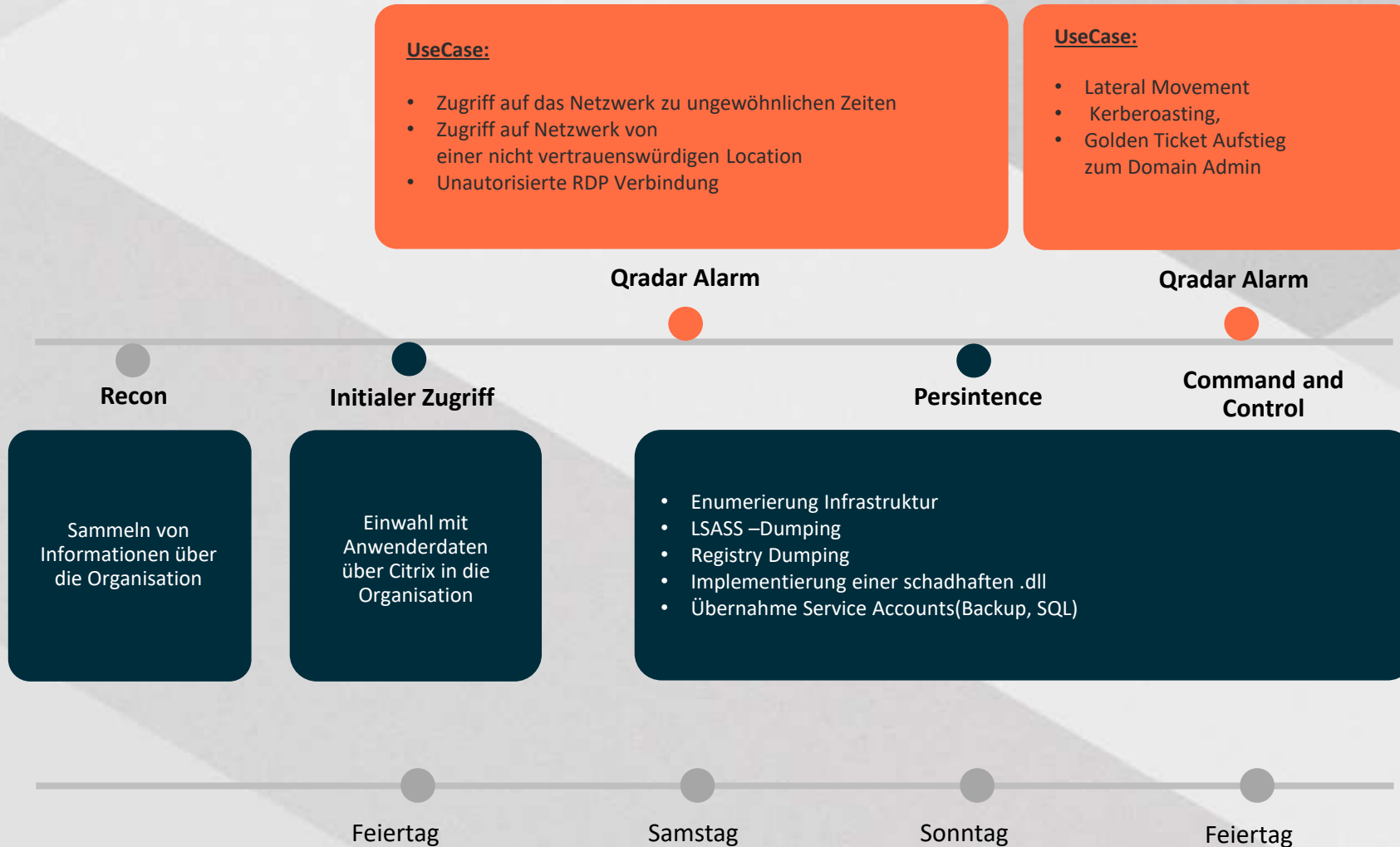
EVIDEN

SOC Alarm: Und was jetzt? (Realer UseCase)

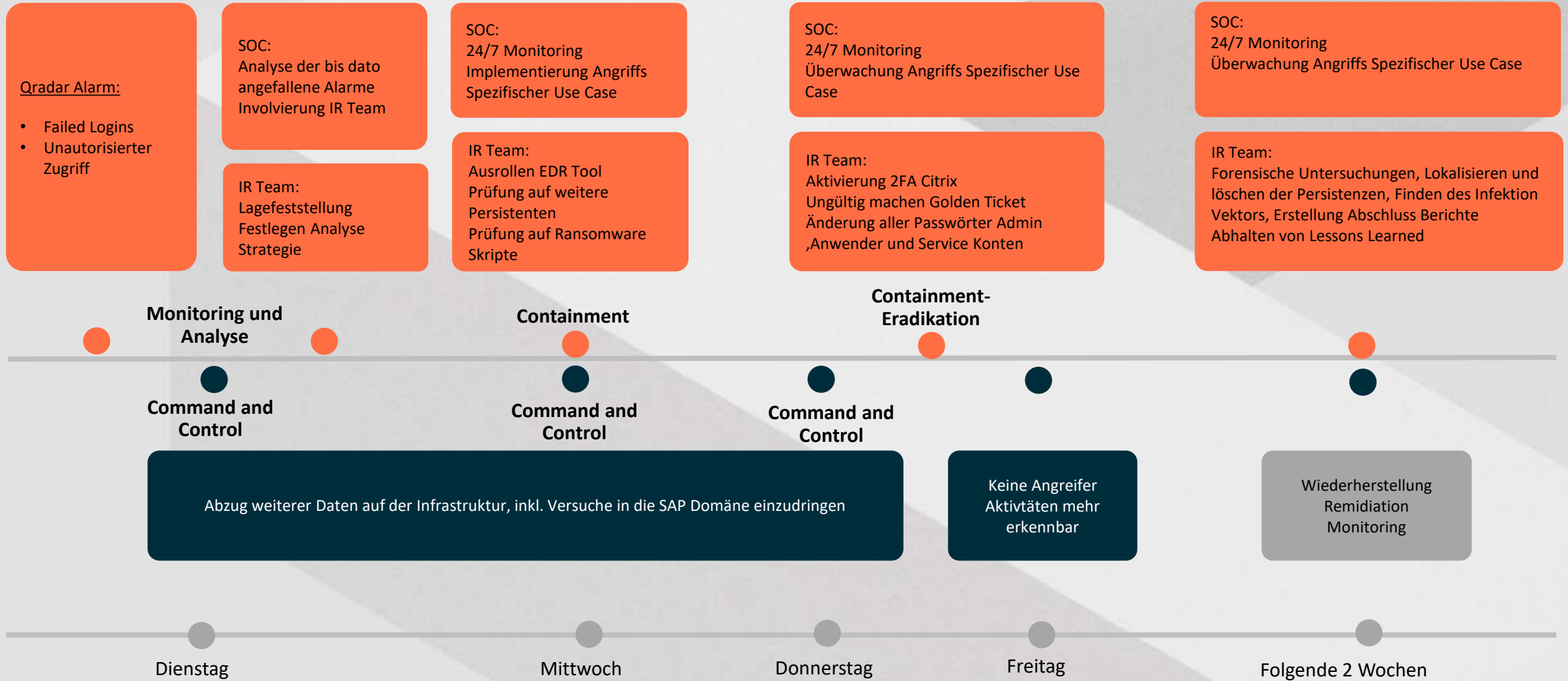
Vom Mobiltelefon
zum Domain-Admin
in 3...2...1...

Christian Rau
Senior Security Consultant
10/10/2023

Angriffsverlauf ohne Live Monitoring des SIEMs



Angriffsverlauf mit Live Monitoring des SIEMs



Lessons Learned des Kunden

2-Faktor Authentifizierung

**Einführung
SSO**

**Microsoft PAM
Tier Modell**

**EDR/EPP
Plattform**

**Use Case
Anpassungen**

**24/7 SIEM Monitoring inkl.
Rufbereitschaft**

Vom Mobiltelefon zum Domain-Admin in 3...2...1

Wie können wir Ihnen Helfen



Incident Response

Managed Incident Response

- Garantierte Reaktionszeit 24x7
- Hilfe im Ernstfall
- Incident Manager und digitale Forensiker
- Direkter Support - kein Call-Center



EDR-Assessment

Prüfung von:

- Konfiguration und Implementierung
- Erkennung und Antwort
- Strategie und Prozesse
- Performance und Systembelastung
- Reporting und Analyse



Analyse der SOC-Prozesse

Optimierungs-Assessment

- Assessment-Bericht
- Optimierungs-Vorschläge
- Workshop um den Bericht zu besprechen
- Use Case Analyse



DDoS Protection

„DDoS Mitigation“-Assessment

- Analyse des bestehenden DDoS-Schutzes
- Optimierungs-Vorschläge
- Management Summary
- Ergebnis-Meeting: OnPrem & Hybrid



Rule Analyse

Regelauswertung und Finetuning Analyse

- Auswertung in Anlehnung an das MITRE ATT&CK Framework
- Finetuning und Anpassung der bestehenden Regeln auf Basis von Best Practises und Erfahrung
- Management Summary



Zero Trust Network Access

„ZTNA 2.0“-Assessment

- Analyse der bestehenden ZTNA(RAS)-Umgebung
- Optimierungs-Vorschläge
- Begleitung eines PoCs
- Management Summary

EVIDEN

Vielen Dank für Ihre Aufmerksamkeit

Für weitere Fragen stehen wir Ihnen Gerne zur Verfügung:

Christian Rau

Eviden Germany GmbH

Halle 7A IBM Stand 510

christian.rau@atos.net