Detektion von und Reaktion auf IT-Angriffe

Red Teaming – IT-Security im Stresstest

HiSolutions Know-how to go

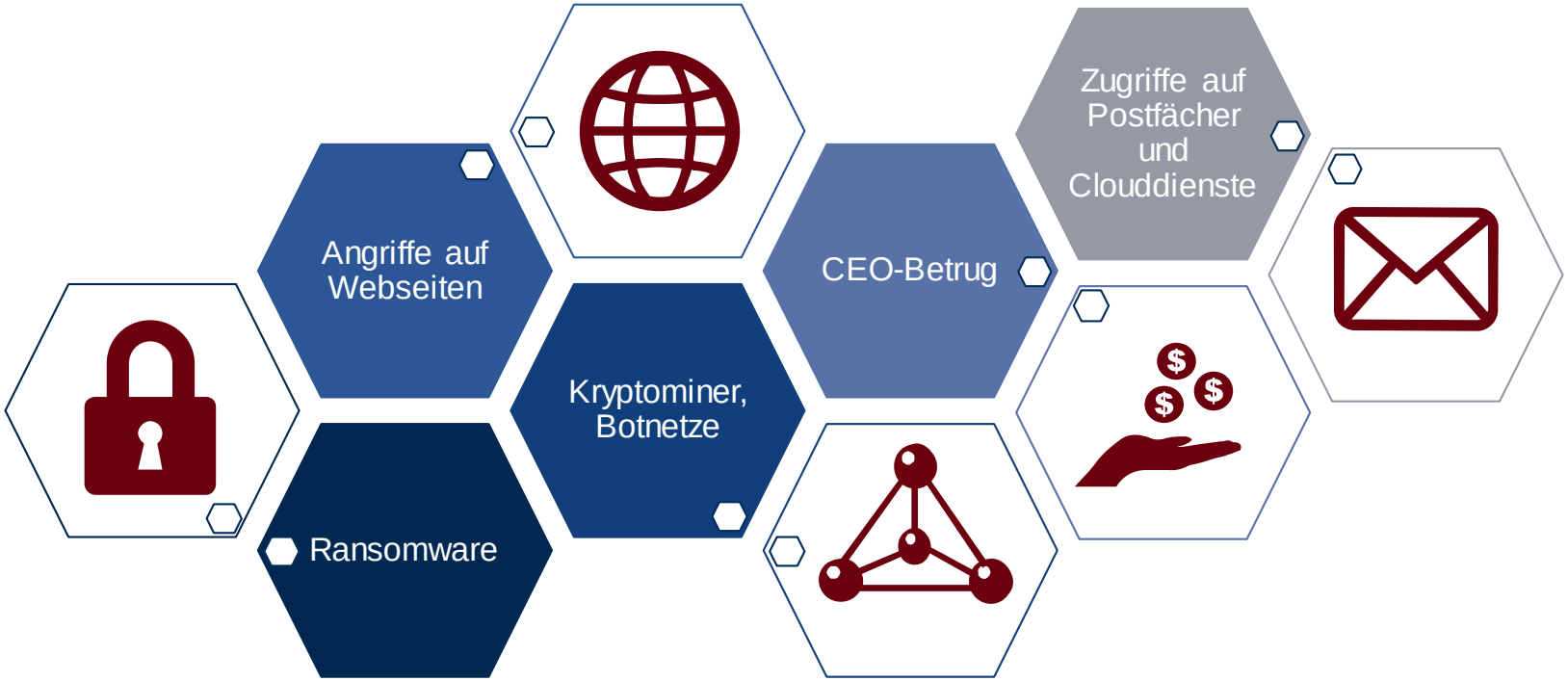
Lena Morgenroth

Agenda

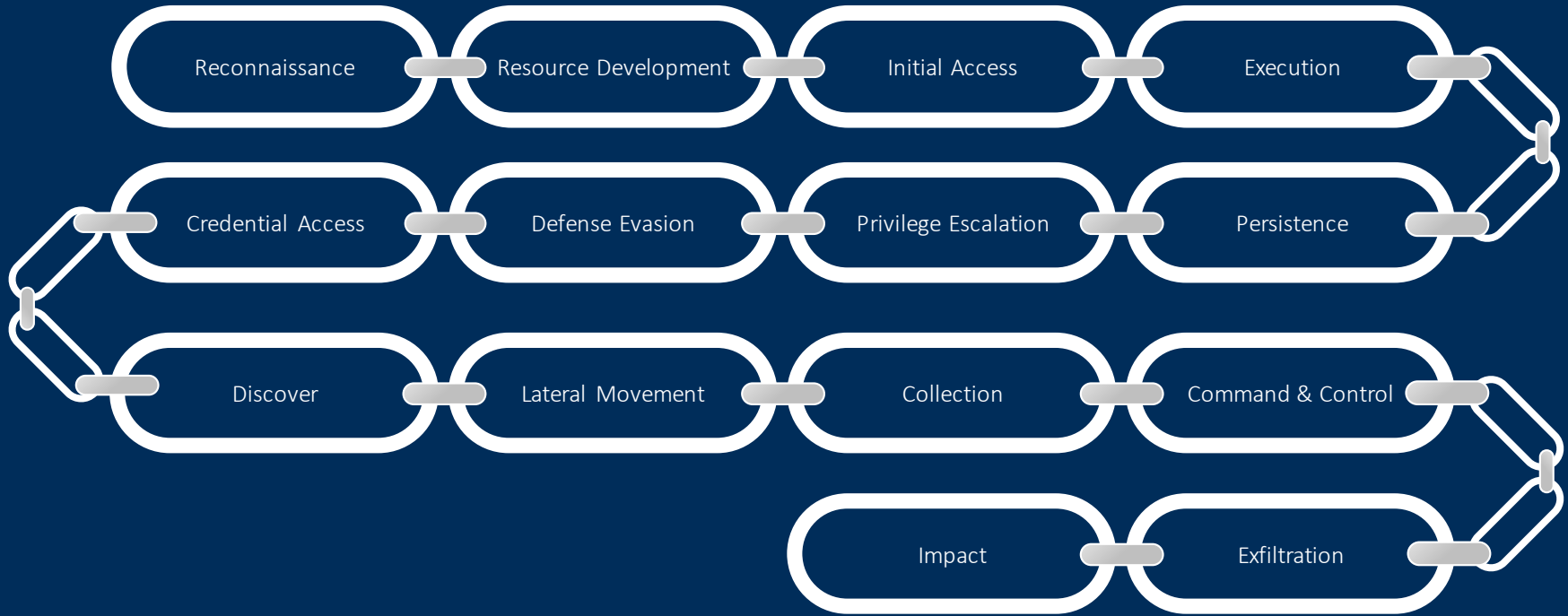
1. Ablauf von IT-Angriffen und Detektionsmöglichkeiten
2. Beispiel-Szenarien
3. Drei Botschaften zum Mitnehmen

1. Ablauf von IT-Angriffen und Detektionsmöglichkeiten

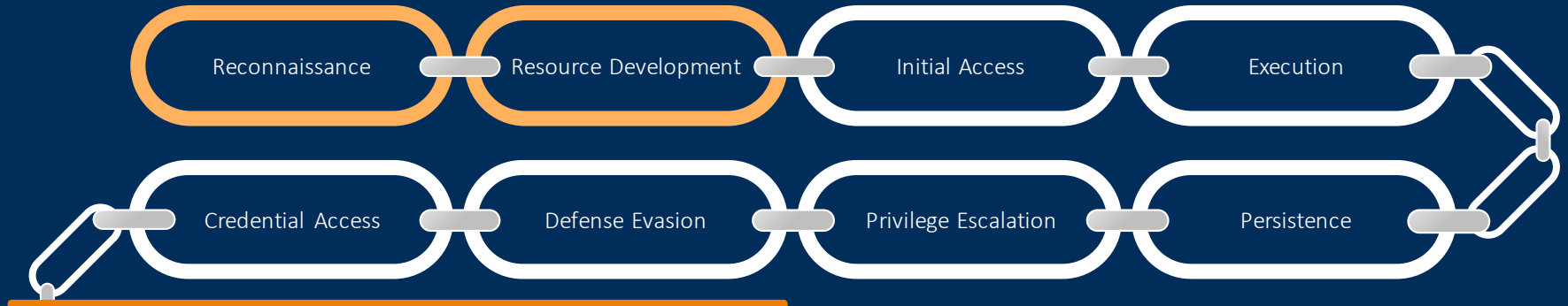
Typische IT-Angriffe in der Incident Response



Ablauf eines IT-Angriffs nach MITRE ATT&CK

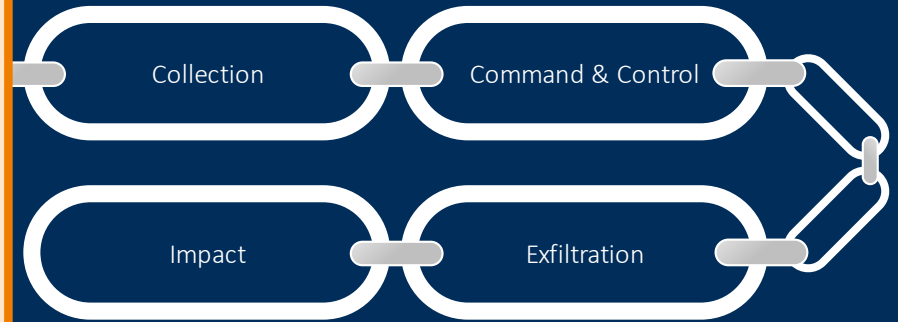


Ablauf eines IT-Angriffs nach MITRE ATT&CK

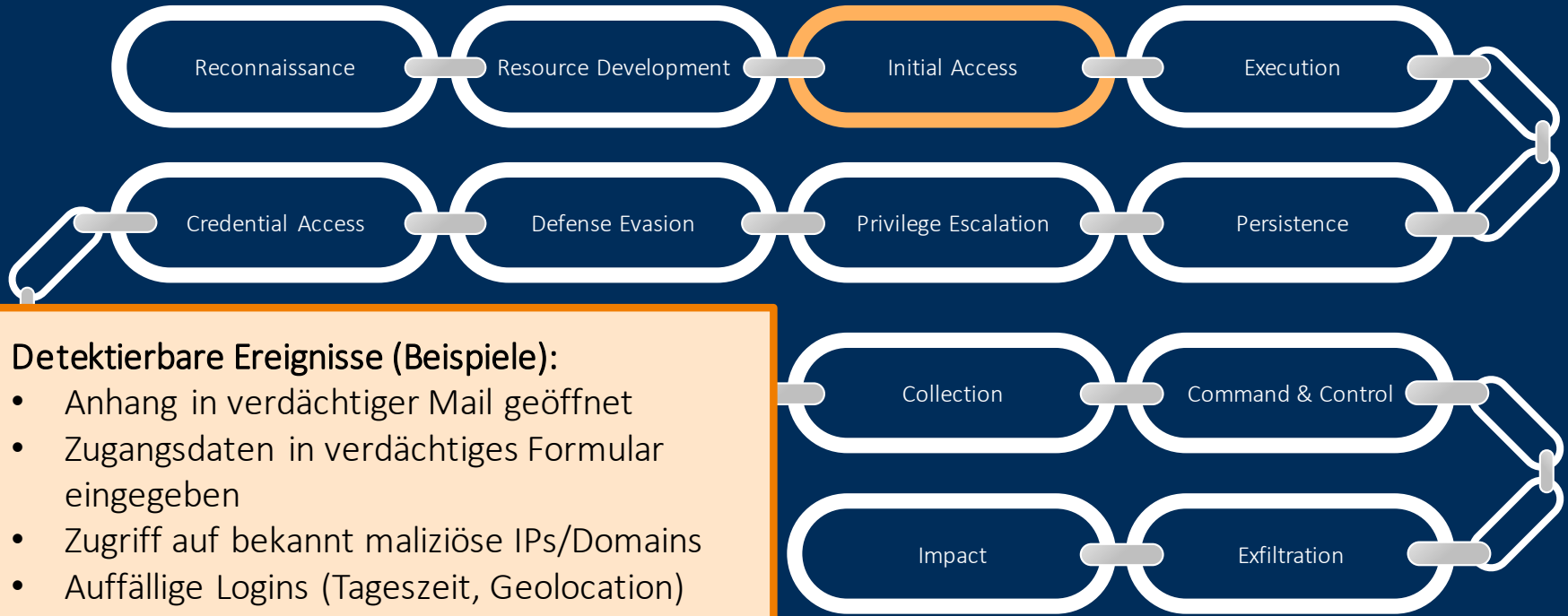


Detektierbare Ereignisse:

- keine



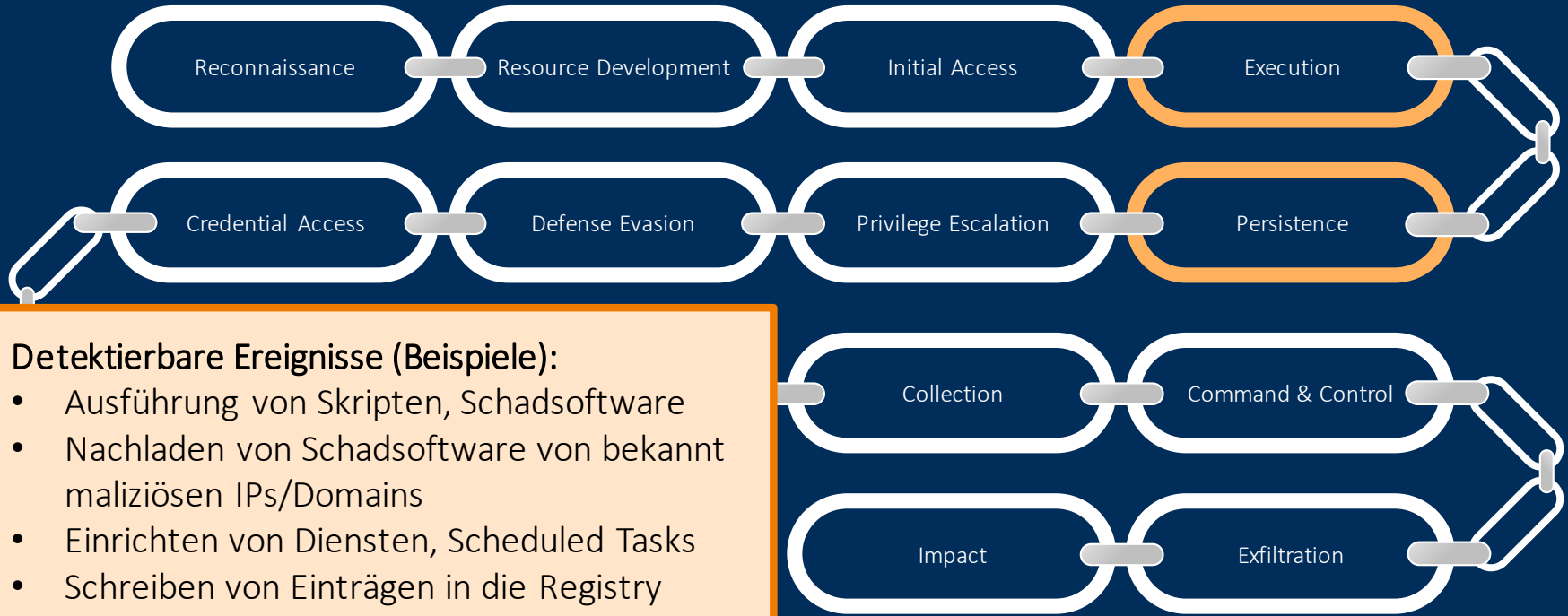
Ablauf eines IT-Angriffs nach MITRE ATT&CK



Detektierbare Ereignisse (Beispiele):

- Anhang in verdächtiger Mail geöffnet
- Zugangsdaten in verdächtiges Formular eingegeben
- Zugriff auf bekannt maliziöse IPs/Domains
- Auffällige Logins (Tageszeit, Geolocation)
- Erfolgreiche Brute-Force-Angriffe

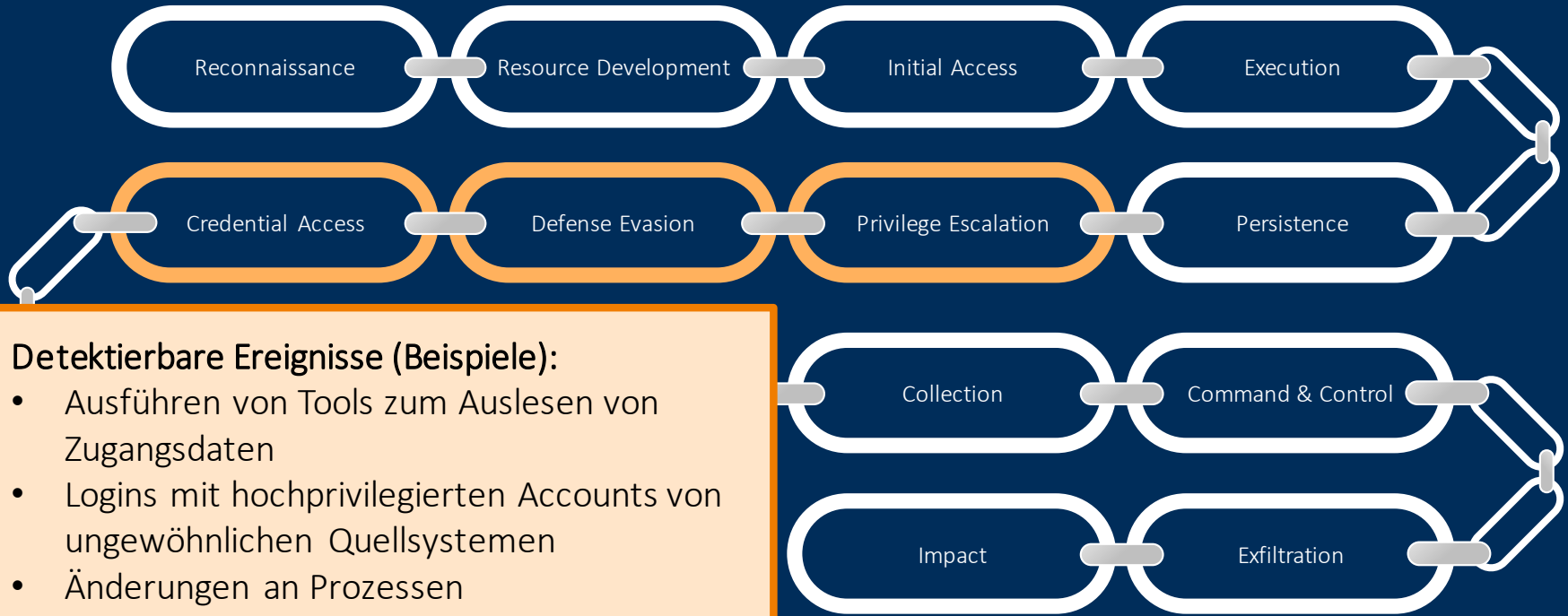
Ablauf eines IT-Angriffs nach MITRE ATT&CK



Detektierbare Ereignisse (Beispiele):

- Ausführung von Skripten, Schadsoftware
- Nachladen von Schadsoftware von bekannt maliziösen IPs/Domains
- Einrichten von Diensten, Scheduled Tasks
- Schreiben von Einträgen in die Registry
- Anlegen von Nutzerkonten

Ablauf eines IT-Angriffs nach MITRE ATT&CK



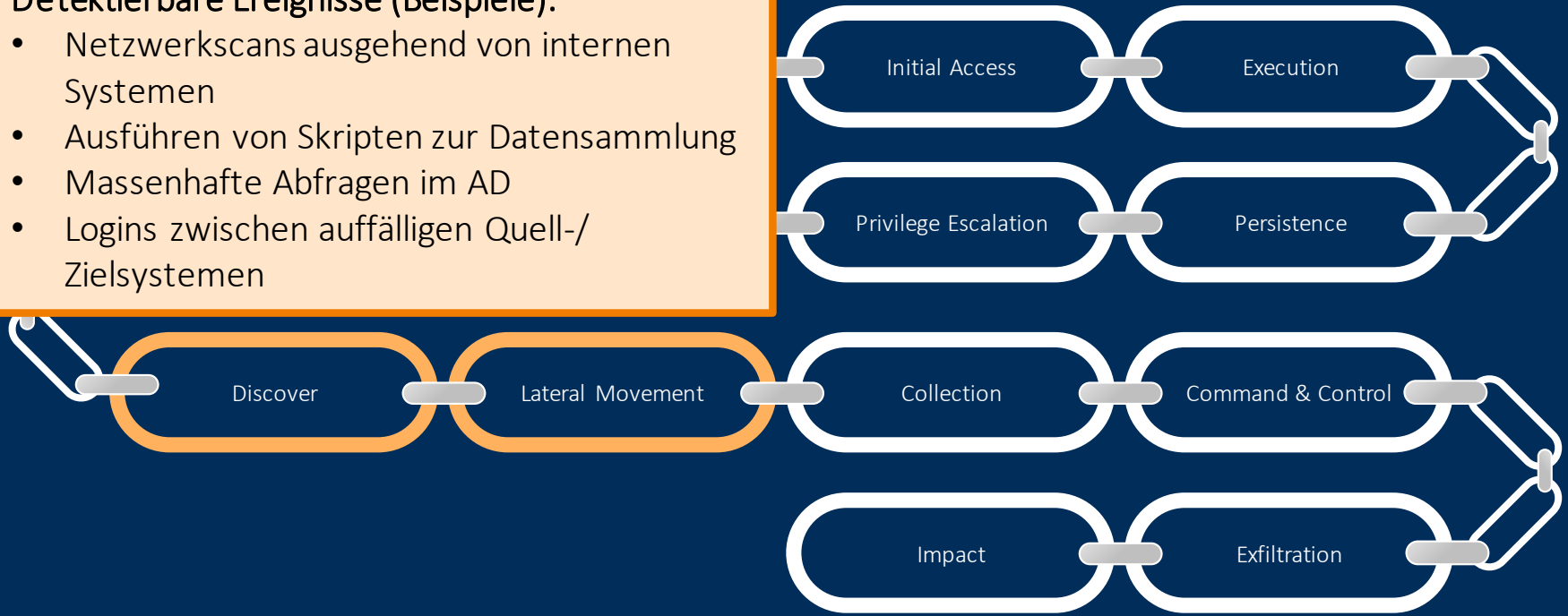
Detektierbare Ereignisse (Beispiele):

- Ausführen von Tools zum Auslesen von Zugangsdaten
- Logins mit hochprivilegierten Accounts von ungewöhnlichen Quellsystemen
- Änderungen an Prozessen

Ablauf eines IT-Angriffs nach MITRE ATT&CK

Detektierbare Ereignisse (Beispiele):

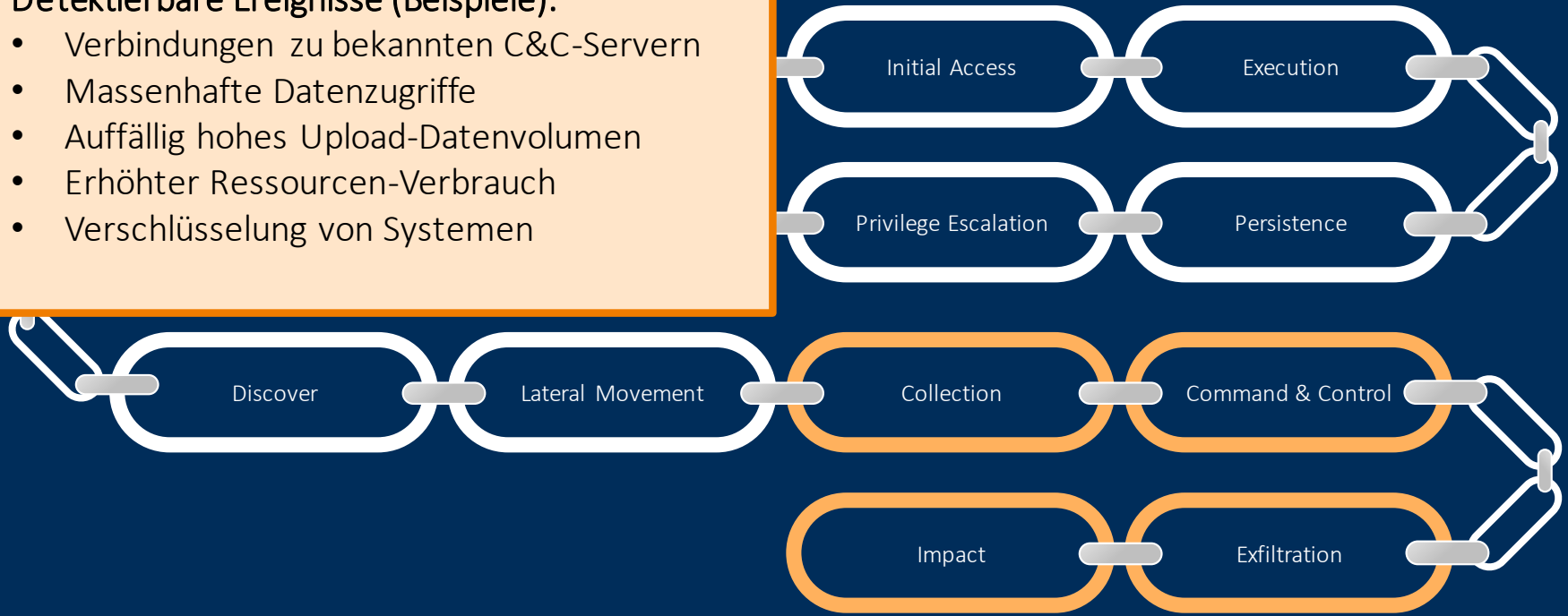
- Netzwerkscans ausgehend von internen Systemen
- Ausführen von Skripten zur Datensammlung
- Massenhafte Abfragen im AD
- Logins zwischen auffälligen Quell-/ Zielsystemen



Ablauf eines IT-Angriffs nach MITRE ATT&CK

Detektierbare Ereignisse (Beispiele):

- Verbindungen zu bekannten C&C-Servern
- Massenhafte Datenzugriffe
- Auffällig hohes Upload-Datenvolumen
- Erhöhter Ressourcen-Verbrauch
- Verschlüsselung von Systemen



2. Beispiel-Szenarien

Szenario 1: Kleine Organisation ohne professionelle IT

- keine eigene IT-Abteilung
- IT wird selbst verwaltet oder Unterstützung durch kleinen Dienstleister bei Bedarf

Vorhandene Detektionsmaßnahmen:

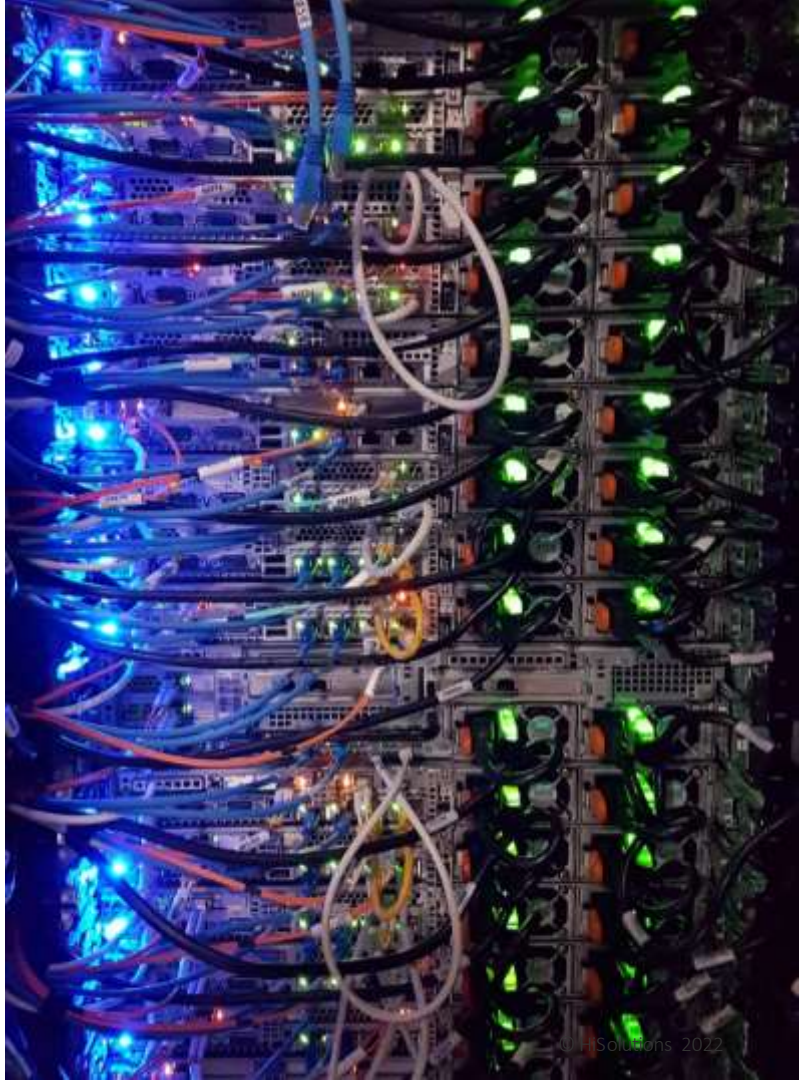
- Aufmerksamkeit der Mitarbeitenden

Szenario 2: Mittlere oder große Organisation mit professioneller IT

- eigene IT-Abteilung oder Systemhaus

Vorhandene Detektionsmaßnahmen:

- Aufmerksamkeit der Mitarbeitenden
- Überwachung der Systemauslastung und Verfügbarkeit
- zentrale Virenscanner-Konsole
- ggf. Überwachung einzelner Ereignisse z. B. Webseitenlogs, Fehllogins
- ggf. Security Dashboard der Cloud-Umgebung



Szenario 3: Organisation mit professioneller Informationssicherheit

- eigene IT-Abteilung oder Systemhaus
- 1-2 zuständige Mitarbeitende für Informationssicherheit
- interne Prozesse für Sicherheitsvorfälle

Vorhandene Detektionsmaßnahmen:

- Aufmerksamkeit der Mitarbeitenden
- Überwachung von Systemauslastung und Verfügbarkeit
- zentral betriebene Endpoint Protection
- eigenes SIEM
- ggf. IDS/IPS

3. Drei Botschaften zum Mitnehmen

Drei Botschaften zum Mitnehmen

1. • **Personelle Kapazitäten für grundlegende Detektion und Reaktion schaffen**
   Alarme müssen von qualifiziertem Personal gesichtet werden
   Reaktionsweisen müssen festgelegt werden

2. • **Prävention ausbauen**
   Eine gut abgesicherte Umgebung zwingt Angreifende, mehr Spuren zu hinterlassen, um ihr Ziel zu erreichen, und vergrößert das Zeitfenster für die Reaktion

3. • **Prävention, Detektion und Reaktion schrittweise ausbauen**
   …und dabei vorhandene Maßnahmen zielgerichtet prüfen

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com