Von der ersten Spur zur vollständigen Kartierung

Eine Incident-Response-Chronik

Dr. Simon Weber, Philipp Rehs, Frank Hommes, Heinrich-Heine-Universität Düsseldorf
Sebastian Struwe, Cybersense GmbH

28. Januar 2026

Philipp Rehs

Frank Hommes

Simon Weber

Die Mitglieder des HHU-CERT zum Vorfallszeitpunkt

Sebastian Struwe

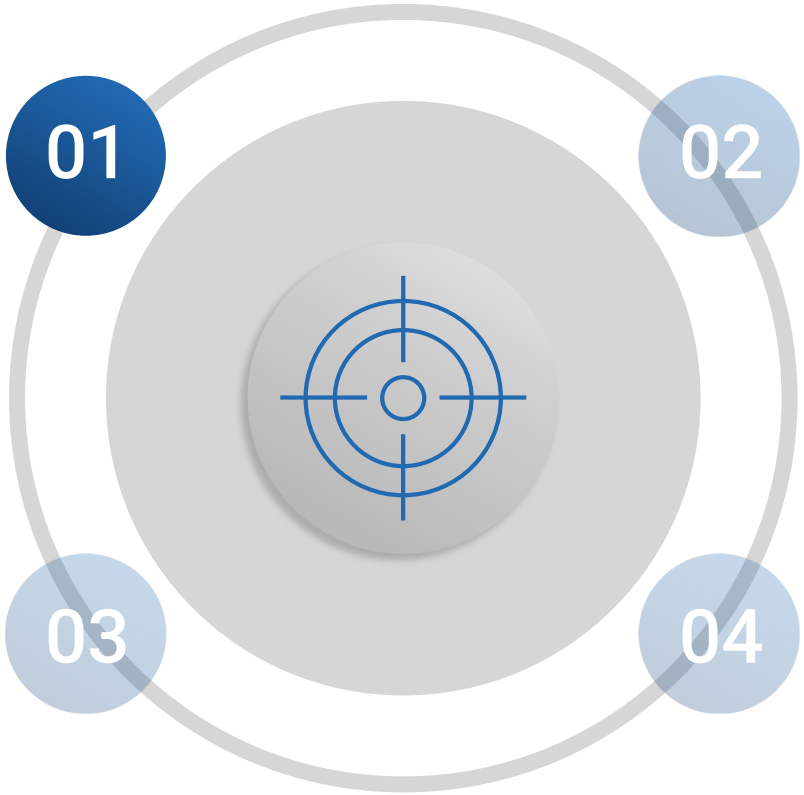
- Master Informatik TU Dortmund
- Security Dienstleister (Aufbau SOC und SIEM)
- Gründer & Geschäftsführer Cybersense GmbH

Systematische Aufarbeitung des mehrstufigen Angriffs

Temporale Dimension – Zeitliche Rekonstruktion

Wann geschah was?
Übersicht der Ereignisse und ihrer Abfolge über den gesamten Vorfallszeitraum.

Retrospektive & Forensik – Erkenntnisse im Rückblick



Visualisierte Angriffsschritte im Systemkontext

Taktische Dimension – Angreifer & Verteidiger

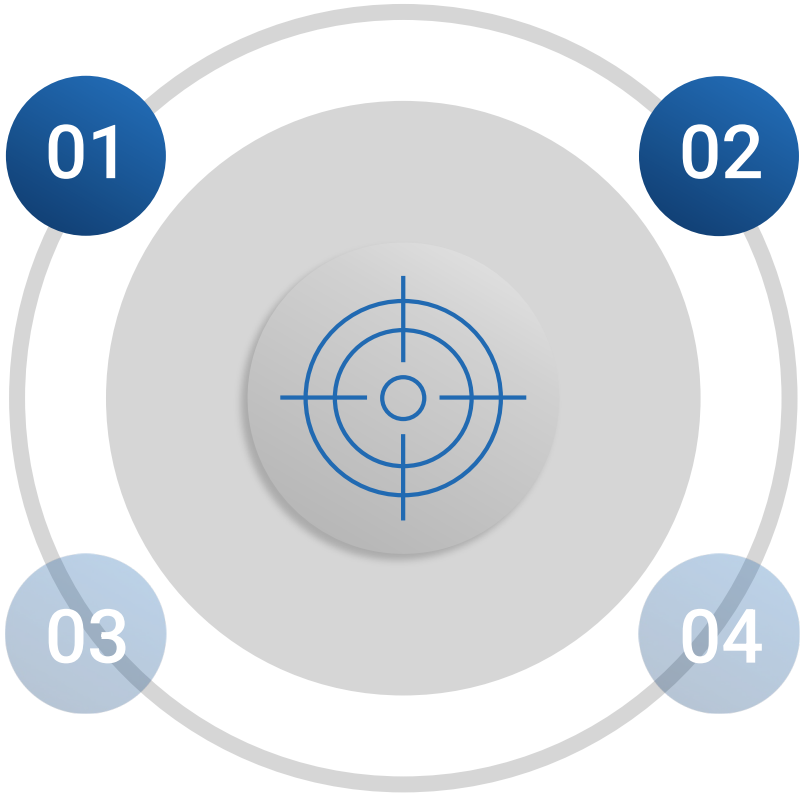
Systematische Aufarbeitung des mehrstufigen Angriffs

Temporale Dimension – Zeitliche Rekonstruktion

Wann geschah was?
Übersicht der Ereignisse und ihrer Abfolge über den gesamten Vorfallszeitraum.

Retrospektive & Forensik – Erkenntnisse im Rückblick

Nachträgliche Einordnung früher Hinweise durch Logauswertung und forensische Rückschlüsse.



Visualisierte Angriffsschritte im Systemkontext

Taktische Dimension – Angreifer & Verteidiger

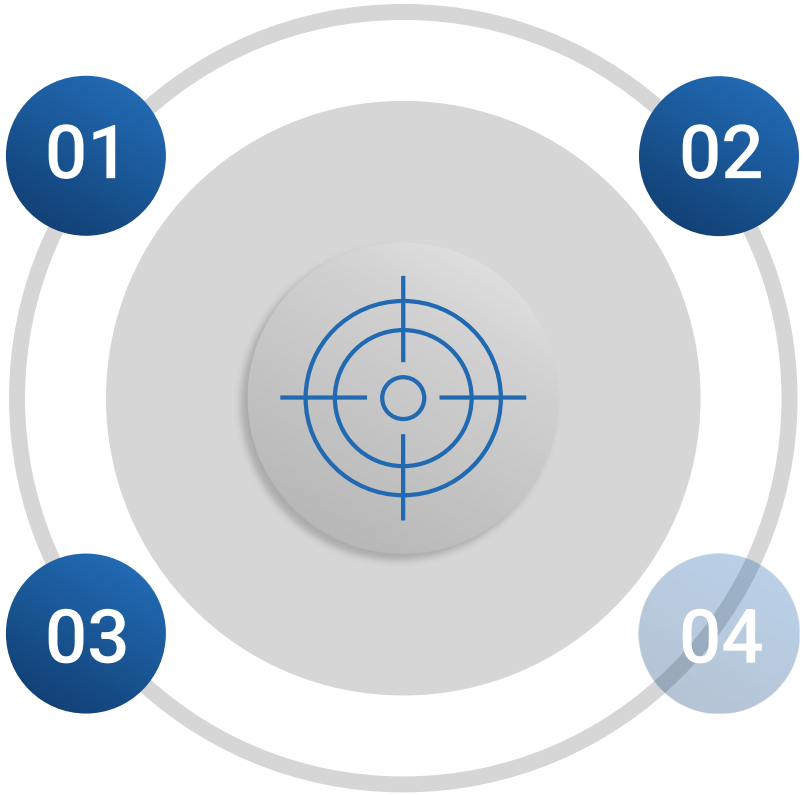
Systematische Aufarbeitung des mehrstufigen Angriffs

Temporale Dimension – Zeitliche Rekonstruktion

Wann geschah was?
Übersicht der Ereignisse und ihrer Abfolge über den gesamten Vorfallszeitraum.

Retrospektive & Forensik – Erkenntnisse im Rückblick

Nachträgliche Einordnung früher Hinweise durch Logauswertung und forensische Rückschlüsse.



Visualisierung der Angriffsbewegungen innerhalb der IT-Struktur mit Zeitbezug und Systembeteiligung.

Visualisierte Angriffsschritte im Systemkontext

Taktische Dimension – Angreifer & Verteidiger

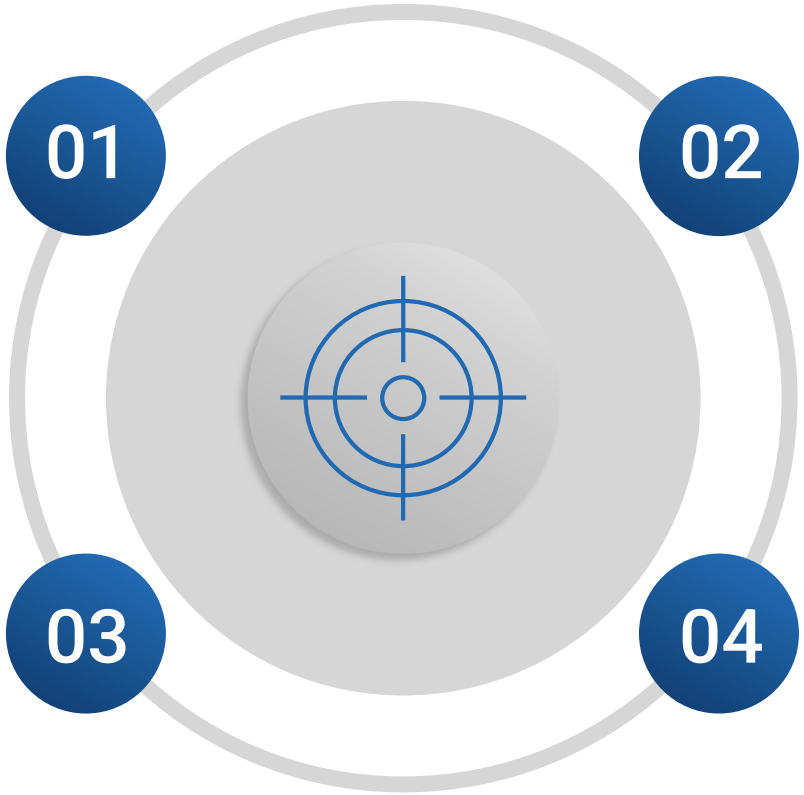
Systematische Aufarbeitung des mehrstufigen Angriffs

Temporale Dimension – Zeitliche Rekonstruktion

Wann geschah was?
Übersicht der Ereignisse und ihrer Abfolge über den gesamten Vorfallszeitraum.

Retrospektive & Forensik – Erkenntnisse im Rückblick

Nachträgliche Einordnung früher Hinweise durch Logauswertung und forensische Rückschlüsse.



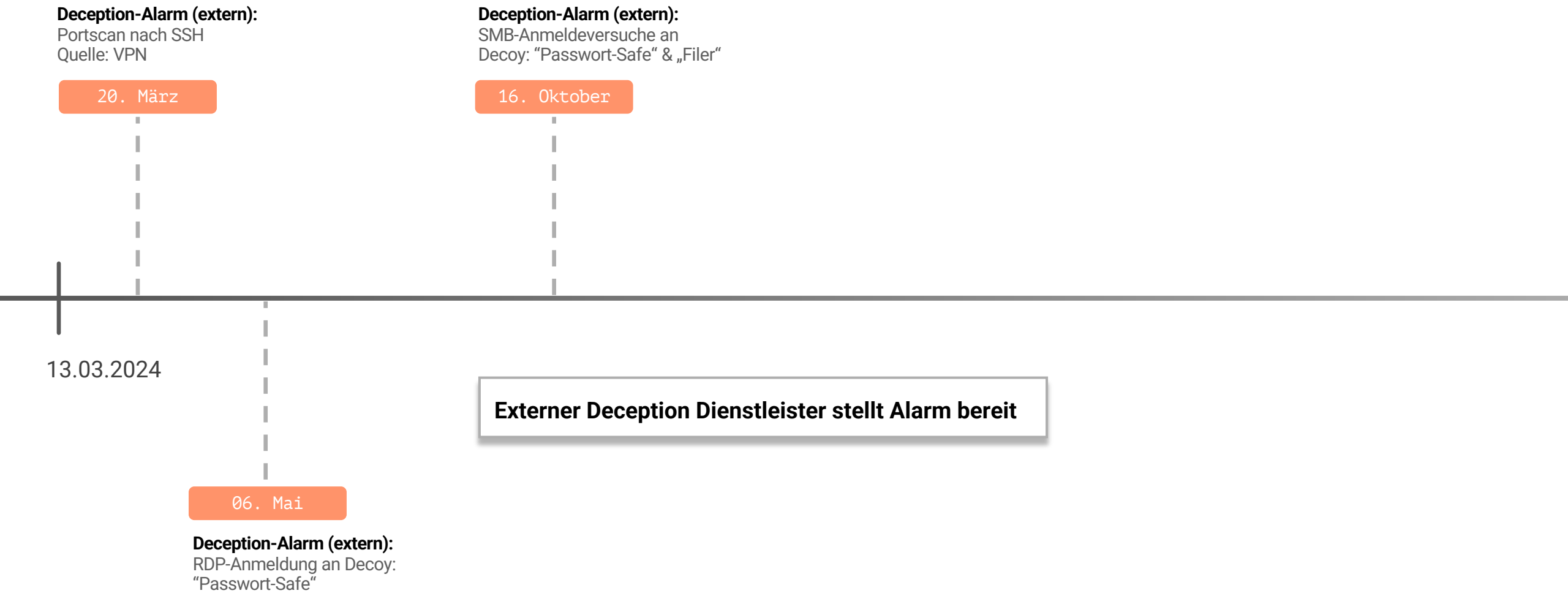
Visualisierte Angriffsschritte im Systemkontext

Visualisierung der Angriffsbewegungen innerhalb der IT-Struktur mit Zeitbezug und Systembeteiligung.

Taktische Dimension – Angreifer & Verteidiger

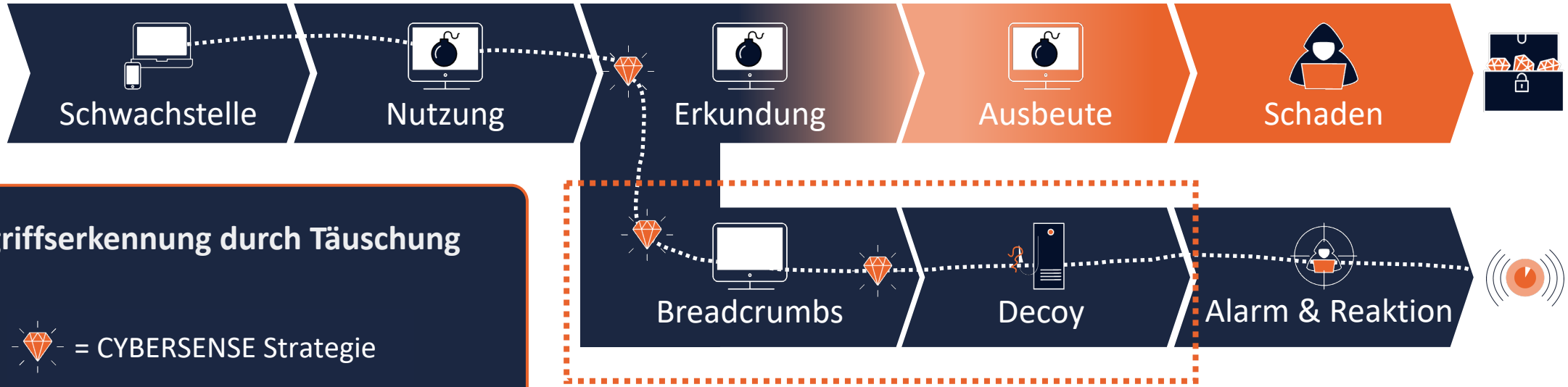
Analyse der Angriffswege und unserer Reaktionen auf taktischer und technischer Ebene.

Angriffszeitachse im Überblick



Unsere Deception-Strategie werden Angriffe erfolgreich erkannt

Deception-Technologie – Angriffsvektoren
Erfolgreiche Angriffserkennung



Angriffserkennung durch Täuschung

= CYBERSENSE Strategie

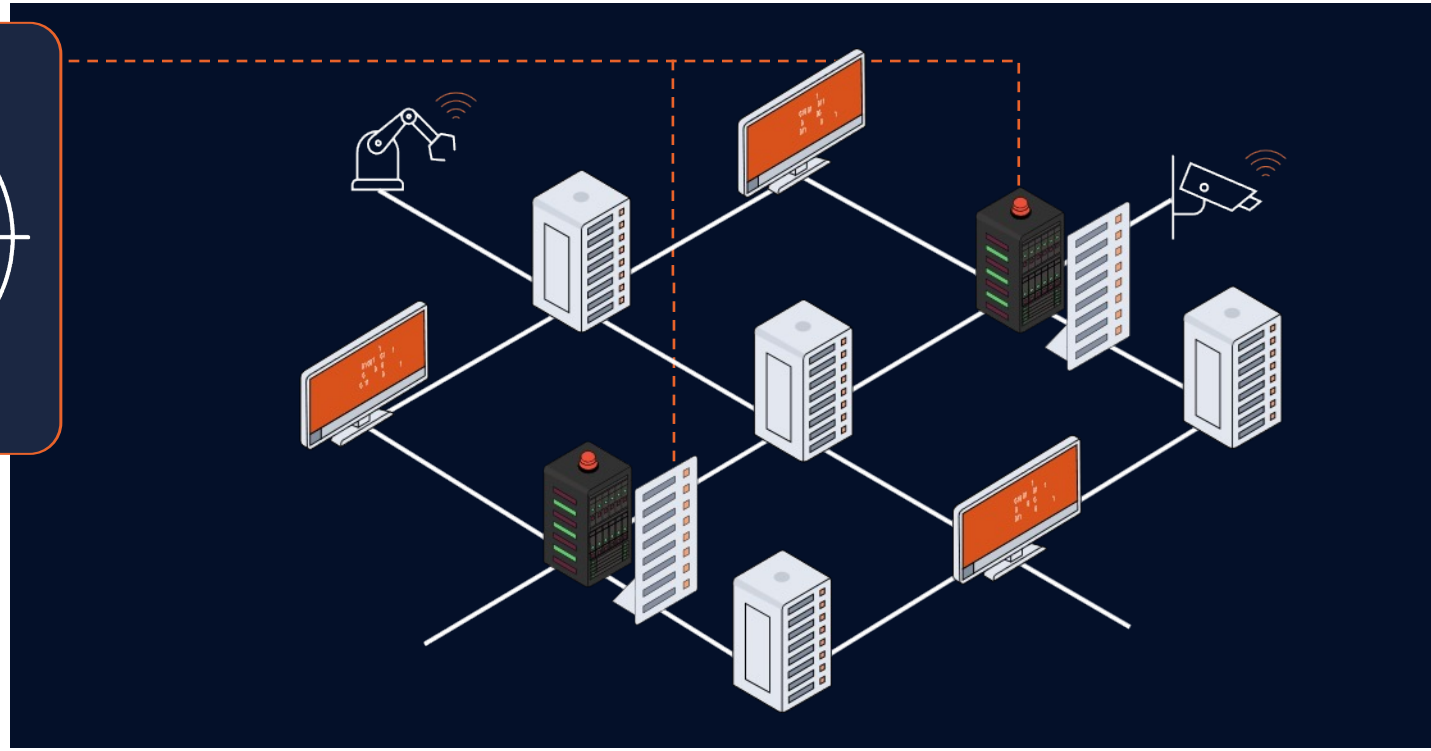
Unsere Elemente schaffen Sichtbarkeit

Sensoren – ganzheitliche Sichtbarkeit

Erkennen, wo andere Ansätze schwächeln

Sensoren & Fallen

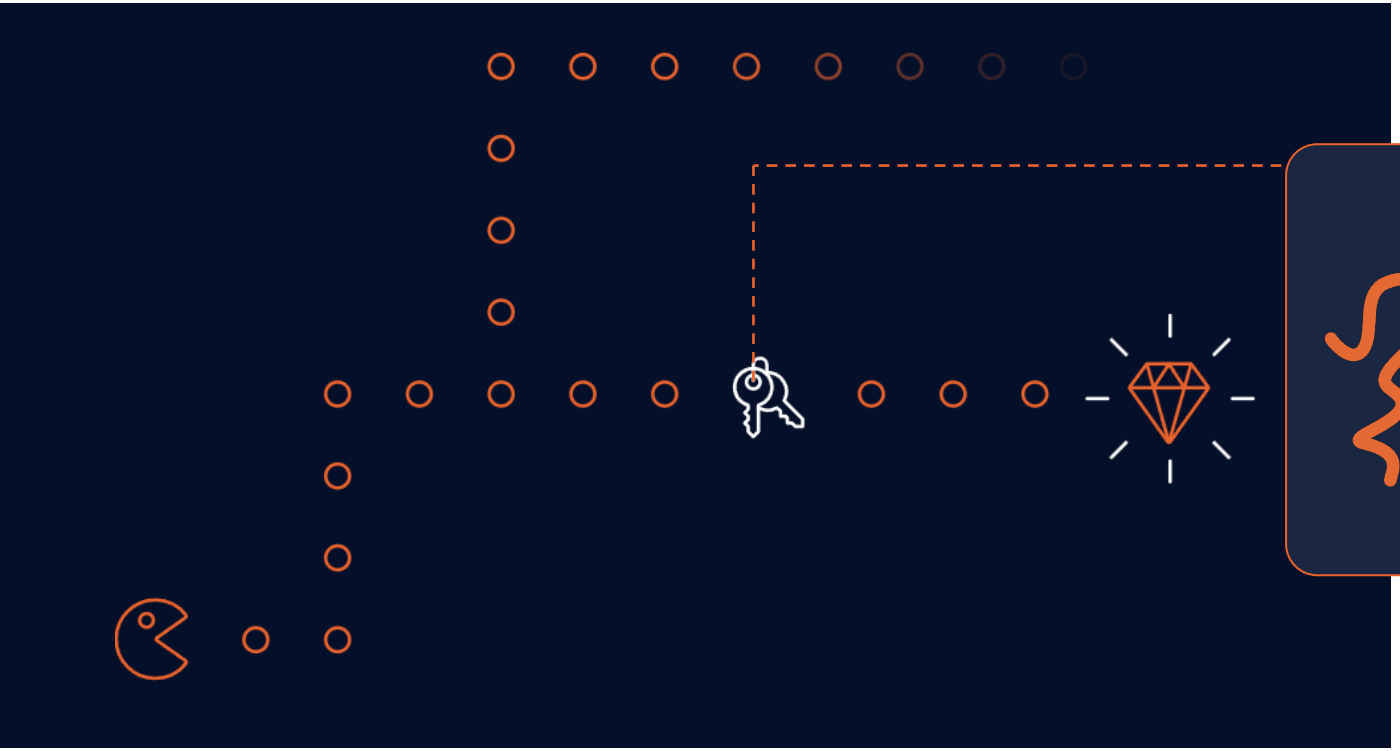
Alle Decoys, Breadcrumbs und Lures dienen nicht nur als Falle, sondern auch als Sensoren. Somit schaffen wir Transparenz, auch an Stellen, die andere Lösungen nicht erreichen.

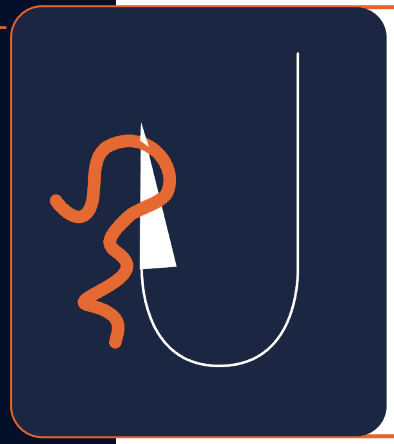


Gefälschte Schlüssel führen Angreifer auf eine falsche Fährte

Breadcrumbs – Gefälschte Informationen

Führen den Angreifer zu Decoy-Systemen





Falsche Informationen zum Erfolg

Der Angreifer sucht nach Zugangsdaten oder Schwachstellen. Die Breadcrumbs machen sich dabei sichtbar und führen den Angreifer auf eine falsche Fährte –
die Decoys.

Unsere Strategie arbeitet hochgradig effizient

Frühzeitige Erkennung

Sichtbarkeit auf Erkundungsversuche, Lateral Movement und versuchte Rechte-erhöhung im Netz, bei Diensten und im AD

Top Erkennungsraten

- Patentiertes Optimierungsverfahren
- Kein erfolgreicher Angriff in unseren geschützten Umgebungen

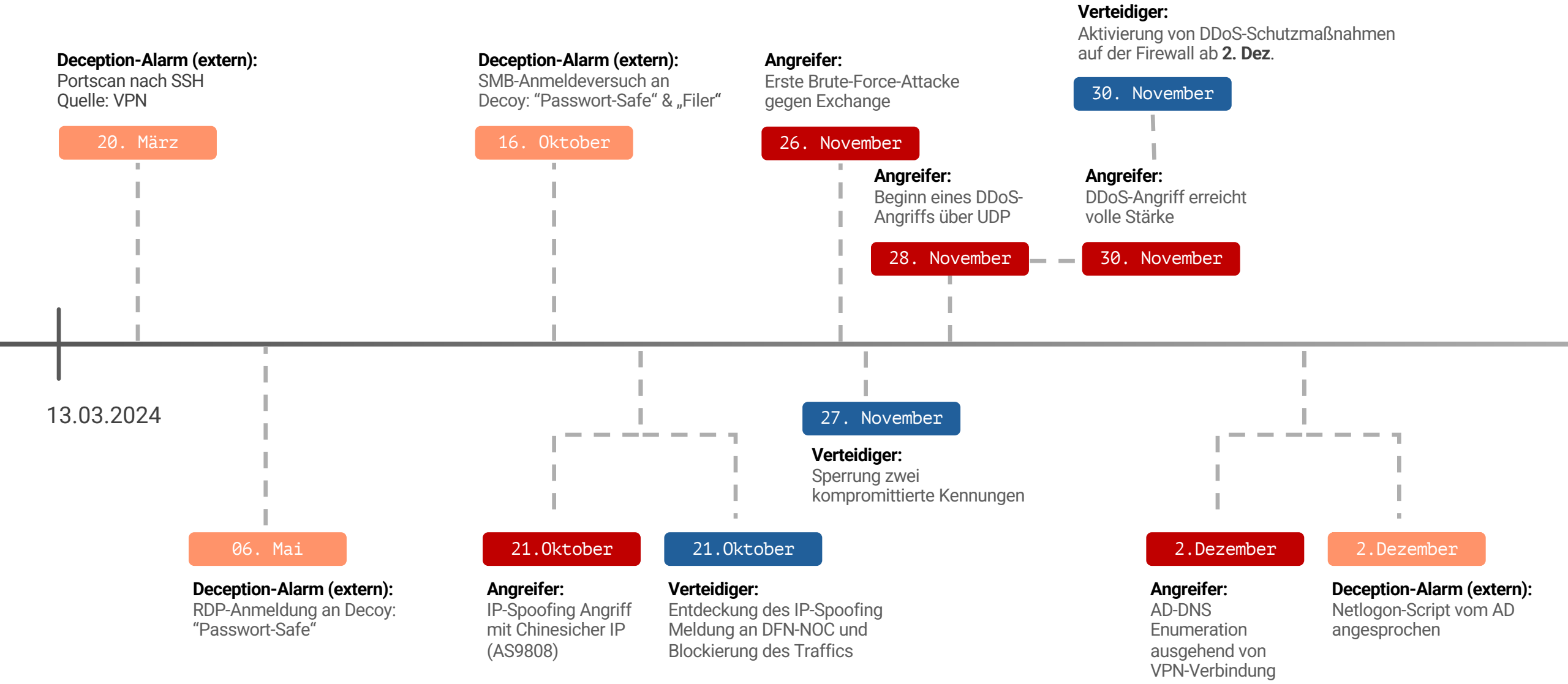
(fast) 0% False Positive

- Top Signal-zu-Rausch-Verhältnis
- Alarmmeldungen im Abstand von Tagen/ Wochen und nicht Minuten/ Stunden

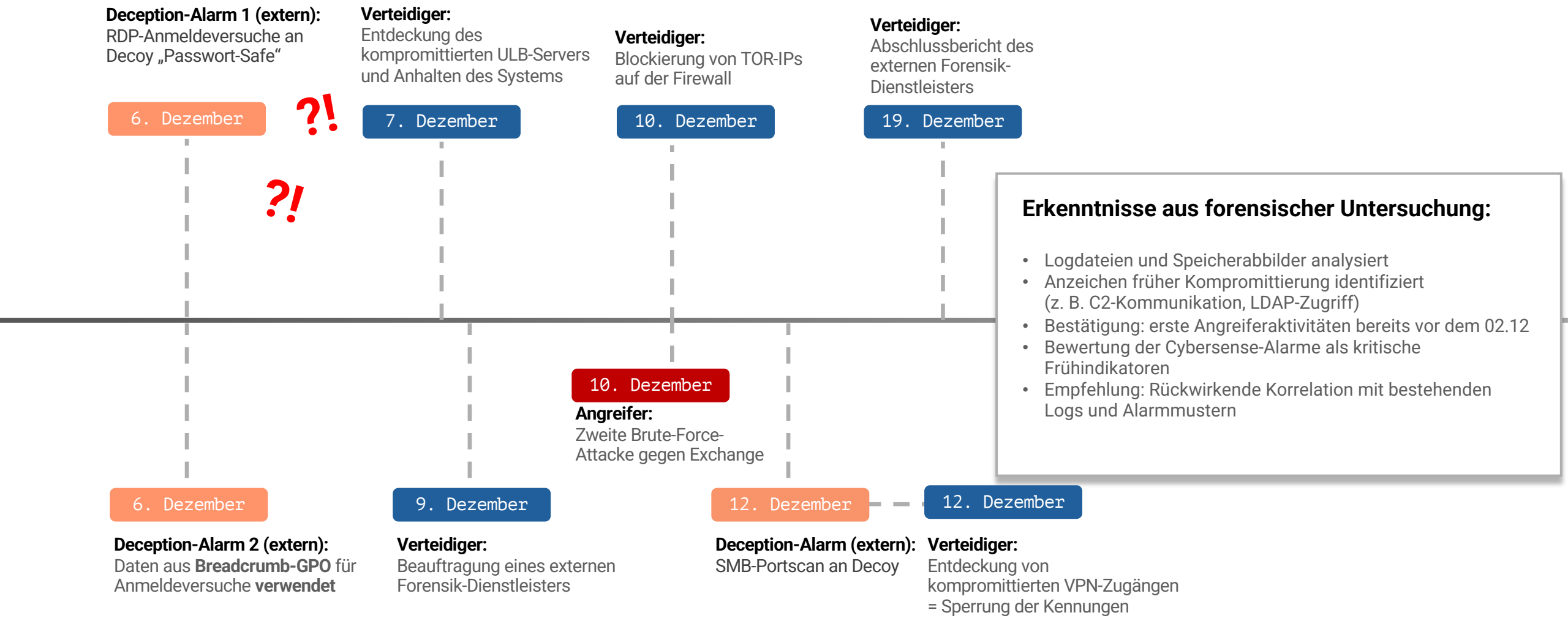
Betriebssicher

- On-Premise
- Agentenlos, komplementär
- Keine Veränderungen an produktiven Systemen notwendig

Angriffszeitachse im Überblick



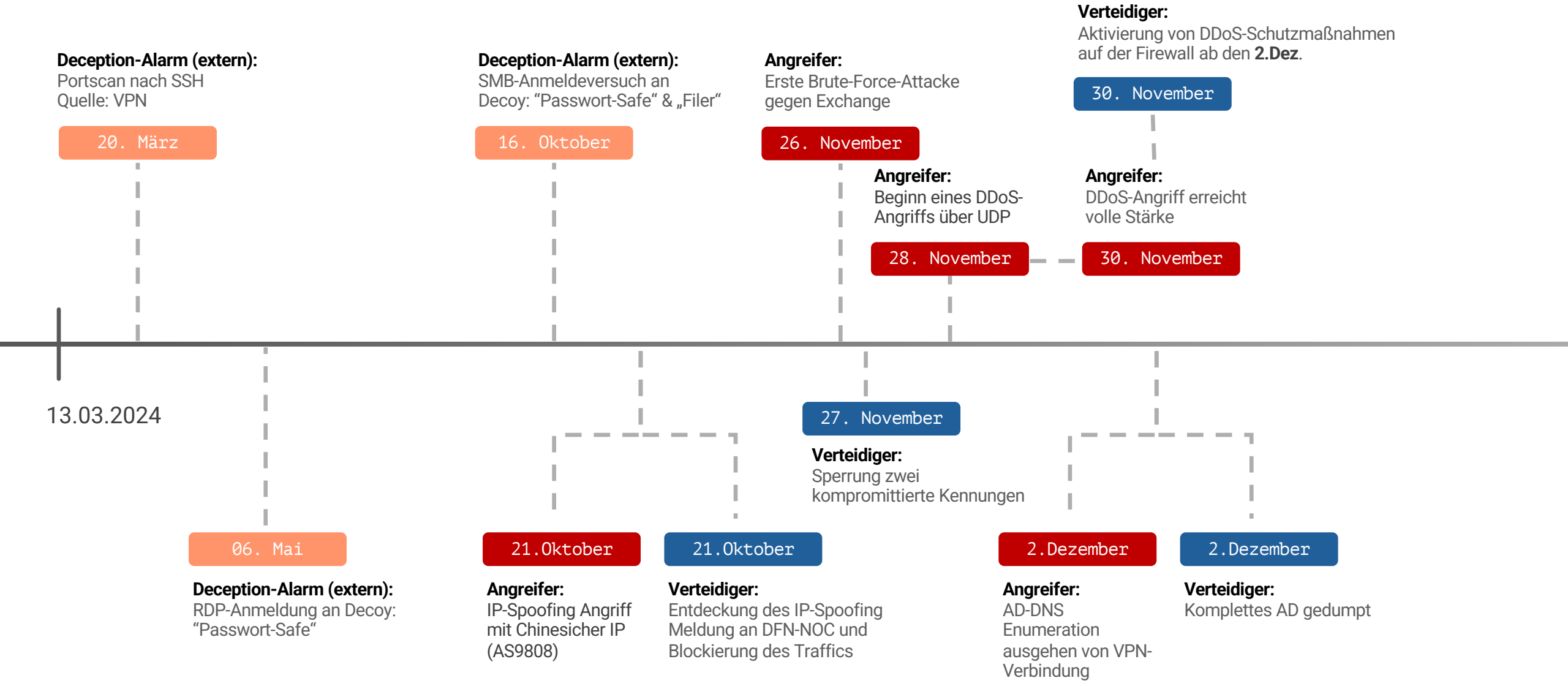
Angriffszeitachse im Überblick



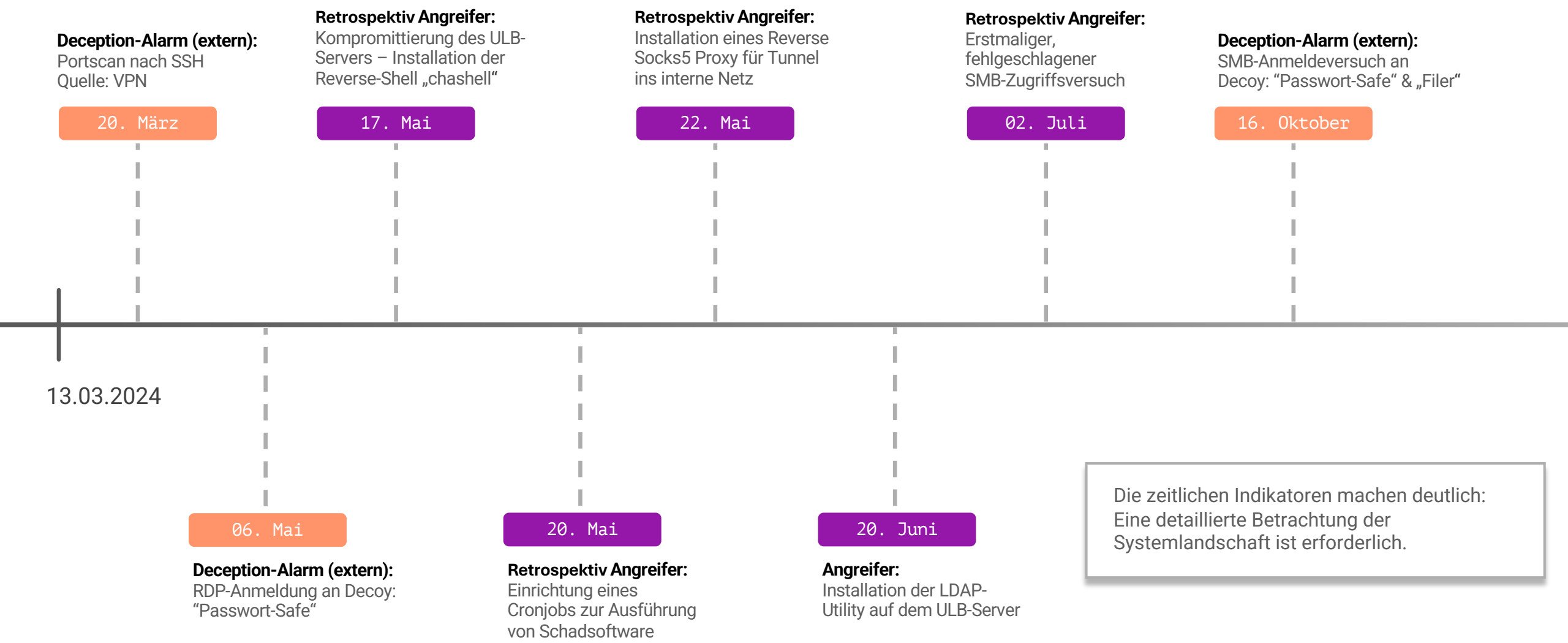
Erkenntnisse aus forensischer Untersuchung:

- Logdateien und Speicherabbilder analysiert
- Anzeichen früher Kompromittierung identifiziert (z. B. C2-Kommunikation, LDAP-Zugriff)
- Bestätigung: erste Angreiferaktivitäten bereits vor dem 02.12
- Bewertung der Cybersense-Alarme als kritische Frühindikatoren
- Empfehlung: Rückwirkende Korrelation mit bestehenden Logs und Alarmmustern

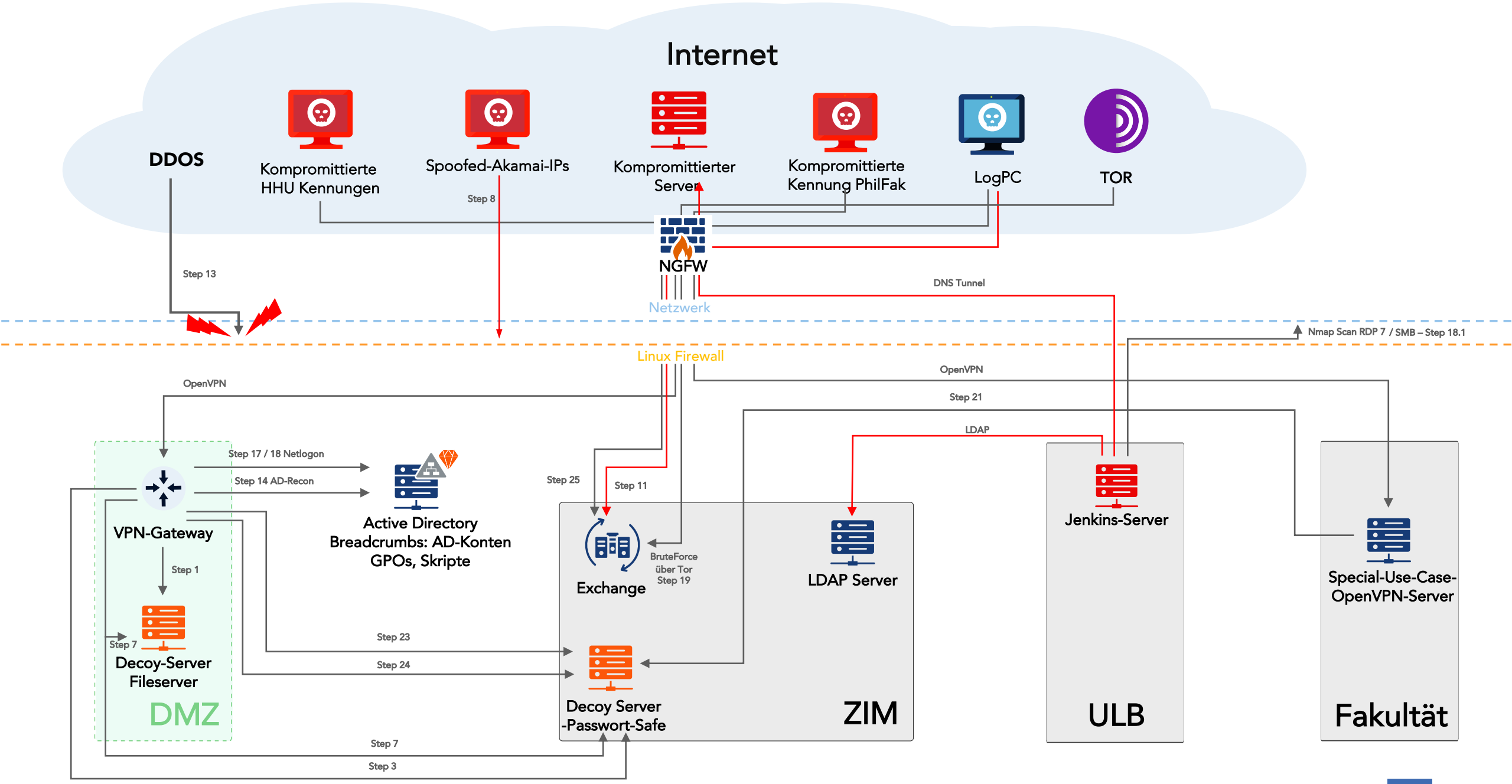
Angriffszeitachse: Retrospektive Korrelation



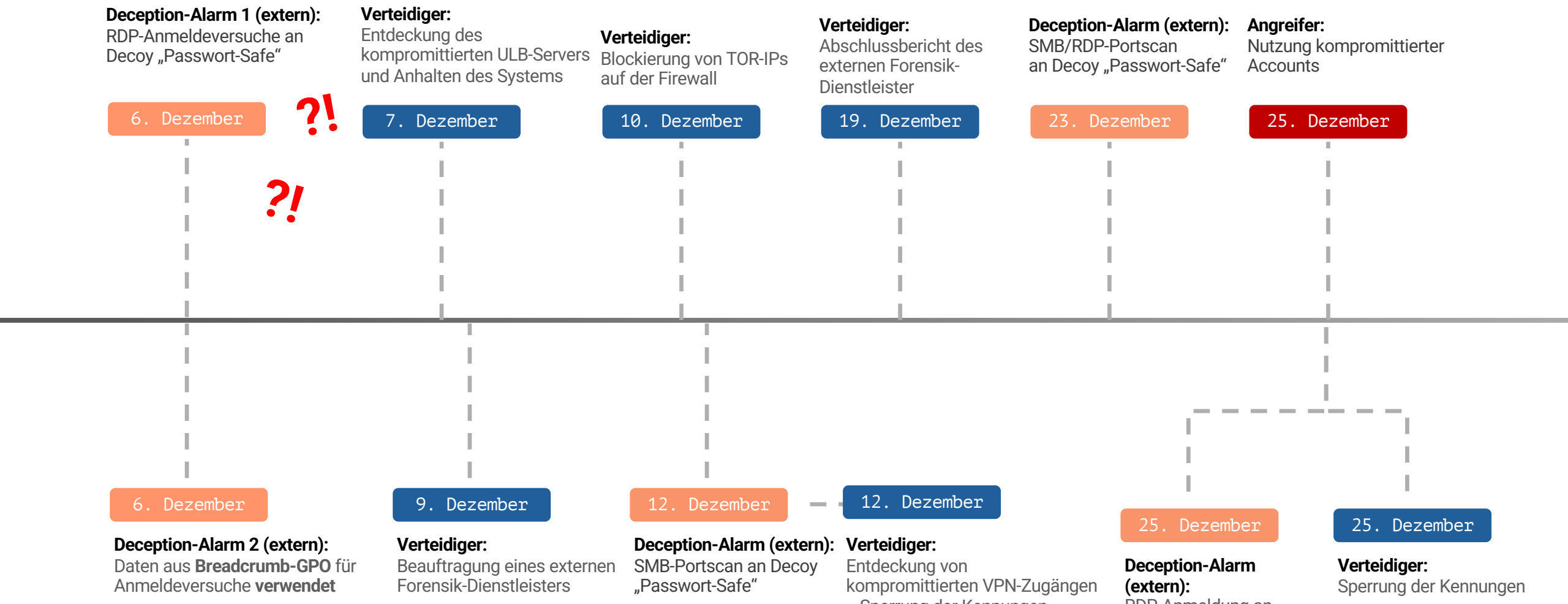
Angriffszeitachse: Retrospektive Korrelation



Die zeitlichen Indikatoren machen deutlich: Eine detaillierte Betrachtung der Systemlandschaft ist erforderlich.


Internet
DDOS
Kompromittierte HHU Kennungen
Spoofed-Akamai-IPs
Kompromittierter Server
Kompromittierte Kennung PhilFak
LogPC
TOR
Step 8
NGFW
Step 13
DNS Tunnel
Netzwerk
Nmap Scan RDP 7 / SMB – Step 18.1
Linux Firewall
OpenVPN
OpenVPN
Step 21
LDAP
Step 17 / 18 Netlogon
Step 14 AD-Recon
Step 25
Step 11
VPN-Gateway
Step 1
Active Directory
Breadcrumbs: AD-Konten
GPOs, Skripte
Exchange
BruteForce über Tor Step 19
LDAP Server
Jenkins-Server
Special-Use-Case-OpenVPN-Server
Step 7
Decoy-Server Fileserver
DMZ
Step 23
Step 24
Decoy Server -Passwort-Safe
ZIM
ULB
Fakultät
Step 7
Step 3

Angriffszeitachse im Überblick



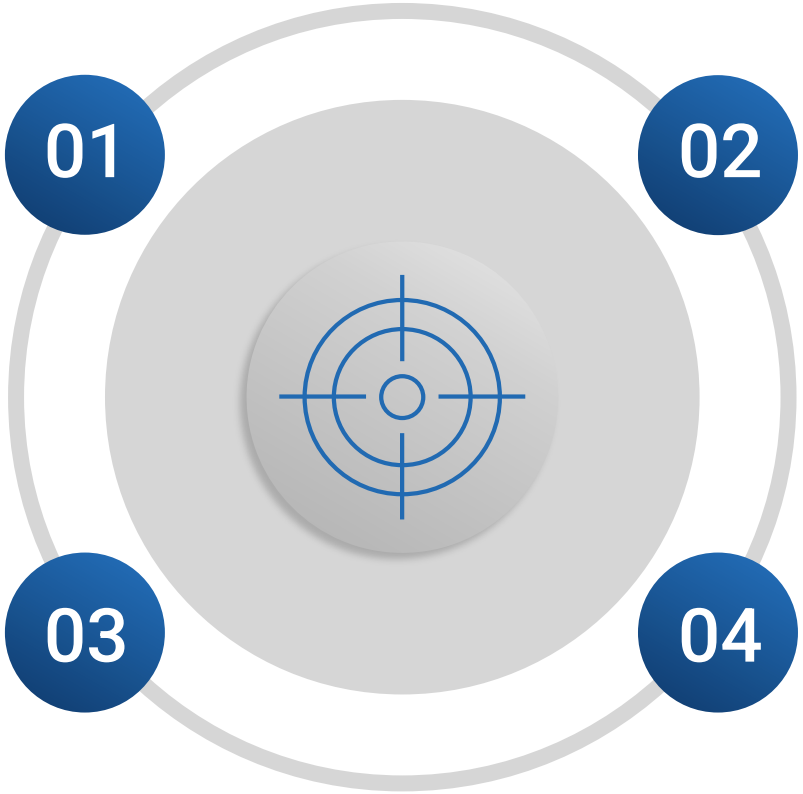
Systematische Aufarbeitung des mehrstufigen Angriffs

Temporale Dimension – Zeitliche Rekonstruktion

- Reihenfolge der Erkennung gibt nur einen groben Überblick

Retrospektive & Forensik – Erkenntnisse im Rückblick

- Neue Erkenntnisse aus der Analyse ändern die Einschätzung vergangener Events



- Übersichtsgrafik, um Zusammenhänge verständlich zu machen

Visualisierte Angriffsschritte im Systemkontext

- Was wird angegriffen?
- Was soll verteidigt werden?
- Versuch der Vorhersage was als Nächstes passiert

Taktische Dimension – Angreifer & Verteidiger

Resultat – Lessons Learned 1/2

- **MFA am VPN** verpflichtend
  - >35k aktive Accounts → irgendwer verliert Zugangsdaten immer!

- Striktes und **restriktives Netzkonzept** hat es dem Angreifer ungemein schwer gemacht
  - Über Monate hinweg keinen Weg für Lateral Movement gefunden
  - Legitime Wege wurden allerdings für weitere Ausbreitung genutzt

  → „**Defense-in-Depth**“ notwendig: Application Layer muss ebenfalls gehärtet werden

- **Abschlagen von „alten“ Zöpfen** doch möglich
  - AD muss nicht Campusweit erreichbar sein
  - Exchange und SharePoint nur noch aus VPN erreichbar gemacht
    - *Wurde allerdings nach 2 Wochen wieder vor das VPN gezogen...*

Resultat – Lessons Learned 2/2

- Entdeckte **Schatten-IT**:
  - Mehrere unbekannte Internet Breakouts beauftragt durch Gebäudedezernat
  - Mehrere dezentrale VPN Dienste durch Institute

- **CERT benötigt Mandat** & **Vertrauen**, akute Sicherheitsmaßnahmen in allen administrativen Bereichen und Fakultäten durchsetzen zu können.

- Zentrale Anlaufstelle für IT-Administratoren nötig, die übergreifende Sicherheitsmaßnahmen und –lage im Blick behält.

- Zusammenspiel von **verschiedenen Sicherheitslösungen** ist von Vorteil
  - Lösungen haben unterschiedliche Ansätze
    - Und damit unterschiedliche Stärken (und Schwächen)
  - Aber: Alarme und Incidents müssen korrekt bewertet werden

- Proaktives **„Assume Breach“ Mindset** für die Absicherung einer so komplexen Infrastruktur empfehlenswert

Fazit

- **Angriff wurde mehrfach abgewehrt**
- **Angriff war insgesamt nicht erfolgreich**

- Angreifer hat es trotzdem immer wieder ins Netz geschafft
- Verwendete Angriffstechniken deuten auf professionellen & zielstrebigen Angreifer hin
  - Ziel des Angreifers ist weiterhin nicht bekannt
  - Wir gehen von **gezielter**, mehrere Monate andauernder **Angriffskampagne auf HHU** aus

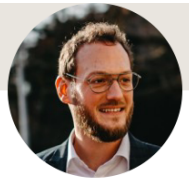
  → **Educational Sector** ist kein Beifang mehr, sondern **im Fadenkreuz** von Angreifern!

- Gesamtes Sicherheitskonzept hat gegriffen
- Entscheidender Vorteil durch Einsatz von verschiedenen Arten der Angriffserkennung
- Persönlicher Einsatz einzelner war entscheidend → Es gibt noch viel zu tun!

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Simon Weber

Referent des Prorektors für Digitalisierung @ HHU |
IT Security Consulting & Pentesting @ Machine Spirits



Sebastian Struwe

Angriffserkennung – einfach und wirksam |
Geschäftsführer bei Cybersense GmbH