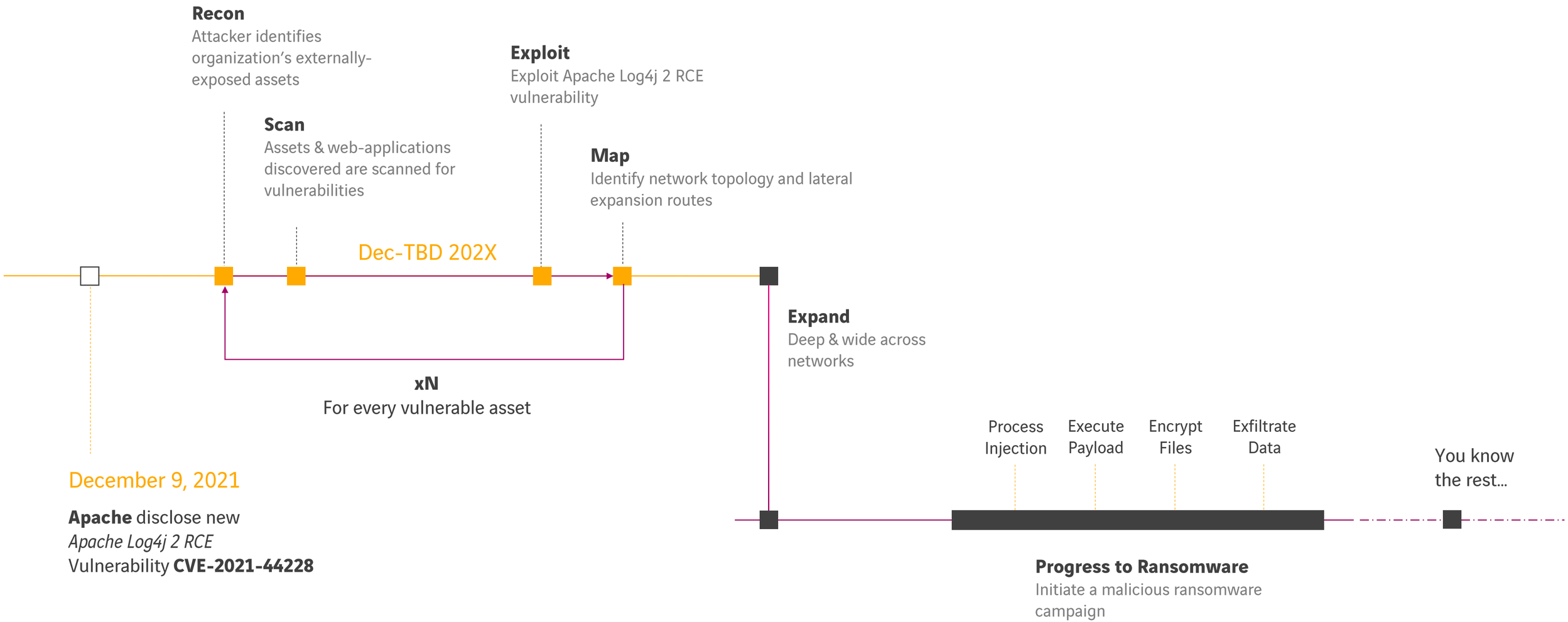
Ransomware Angriffe im Gesundheitswesen – Kennen Sie die Konsequenzen, bevor diese Realität werden

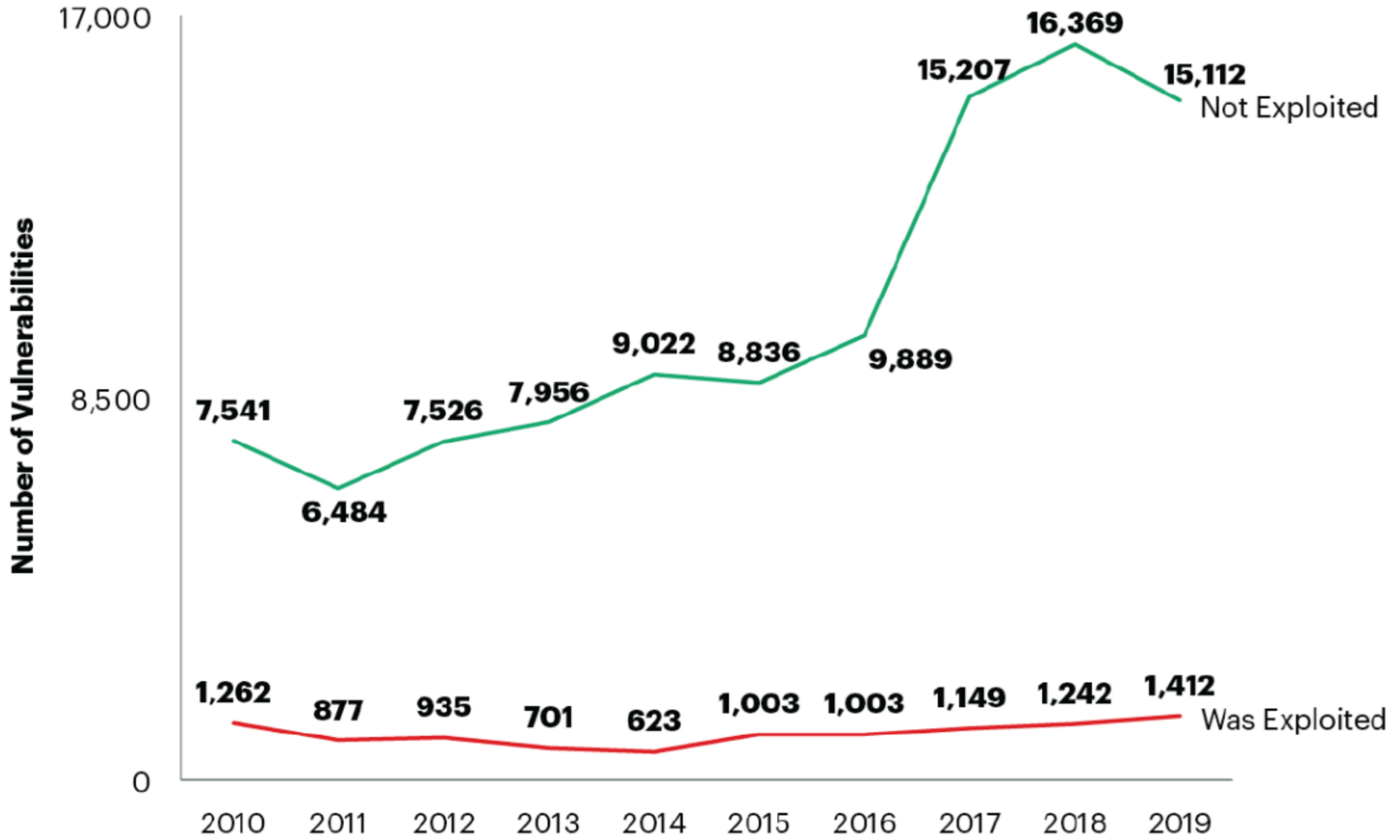
Renata Rekic, Presales & Security Consulting - renata.rekic@axians.com

Anatomie einer Attacke

Log4Shell & Ransomware Campaign



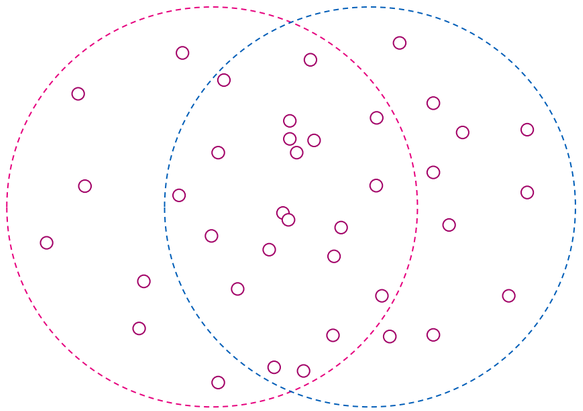
Vulnerabilities exploited by year



Key Challenges

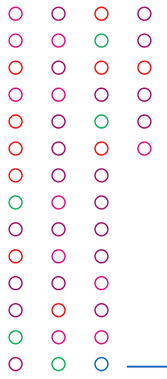
Where do you start? Which one do you focus first? Which impacts you the most?

What Organizations Know



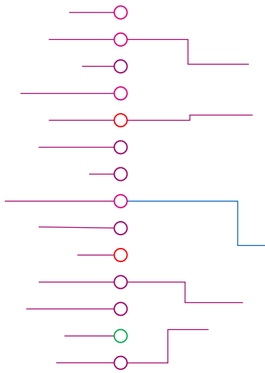
What Attackers See

False Remediation Prioritization (CVSS)



What Attackers Exploit

Vulnerability Confirmed



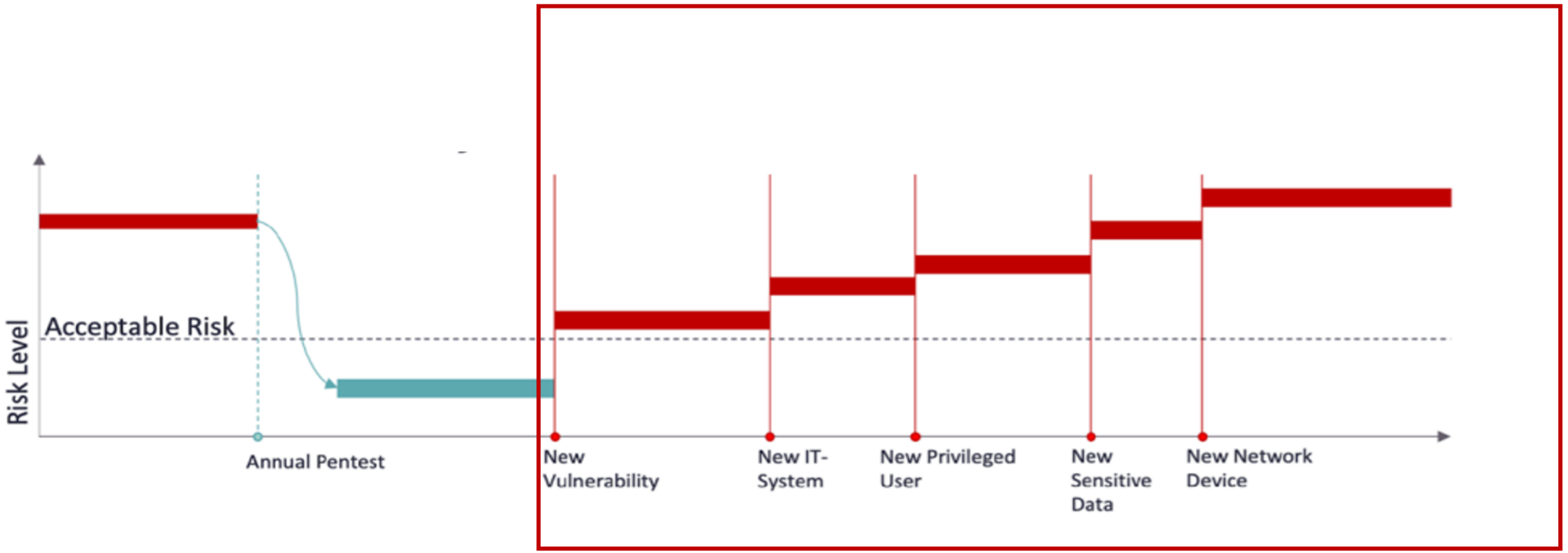
Impact Confirmed

Visibility
Gap

Prioritization
Gap

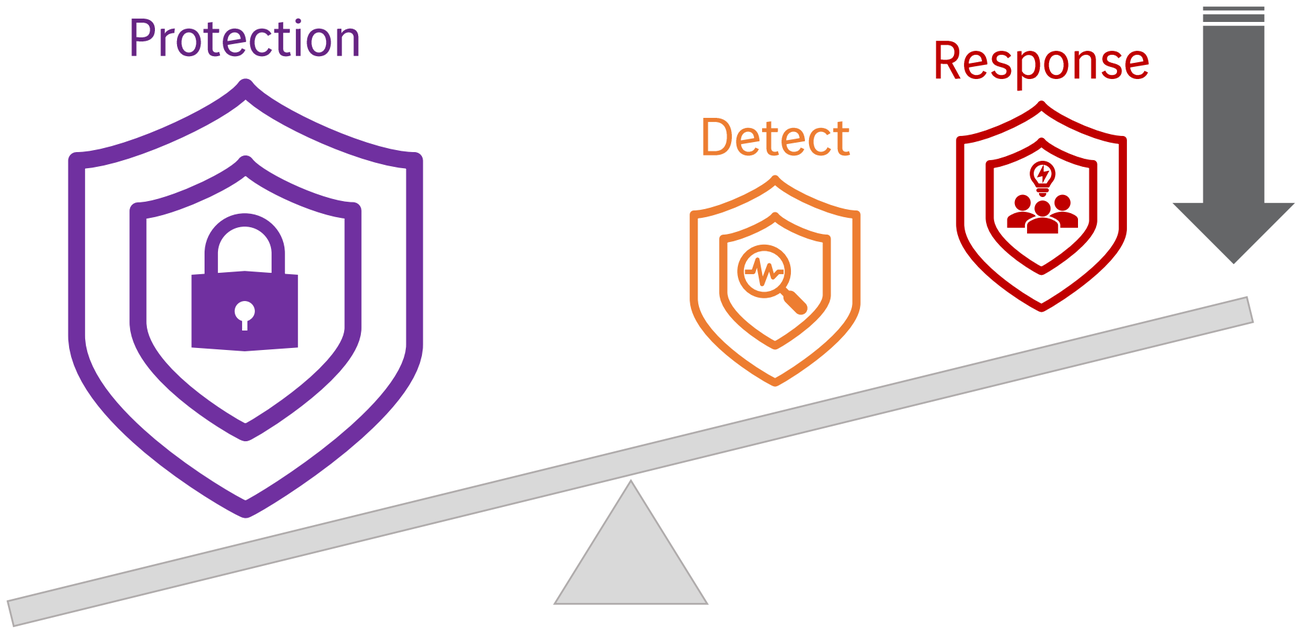
Validation
Gap

Massnahme 1 – Jährliches Penetration Testing



Massnahme 2 – Protection & Detection

- **Präventive Massnahmen -** Firewalls, AV, IPS, Zero Trust Konzepte, etc.
- **Detection Massnahmen -** SIEM, EDR, etc.

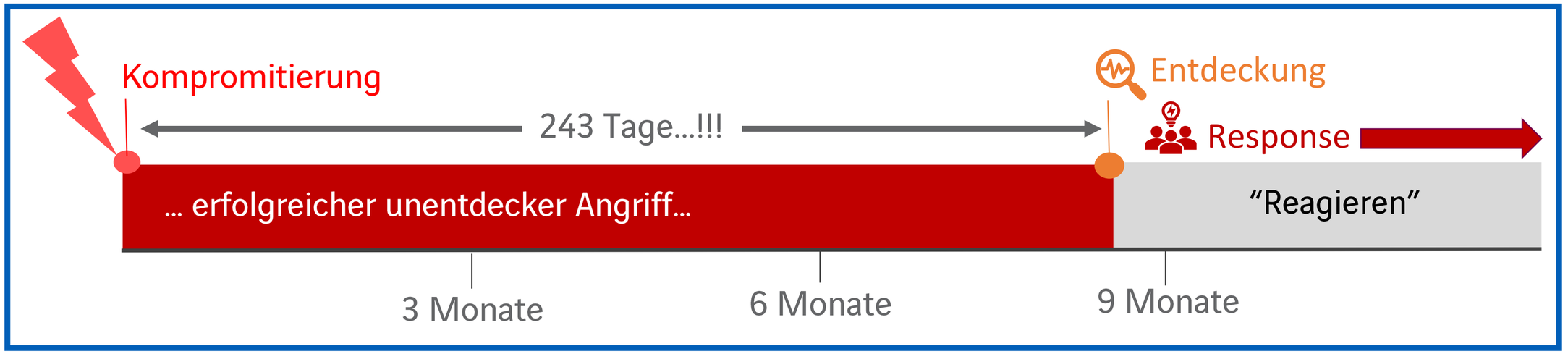


Der Realitäts-Check für Unternehmen

Viele Firmen erfahren von dritter Stelle über erfolgreiche Angriffe auf das eigene Unternehmen

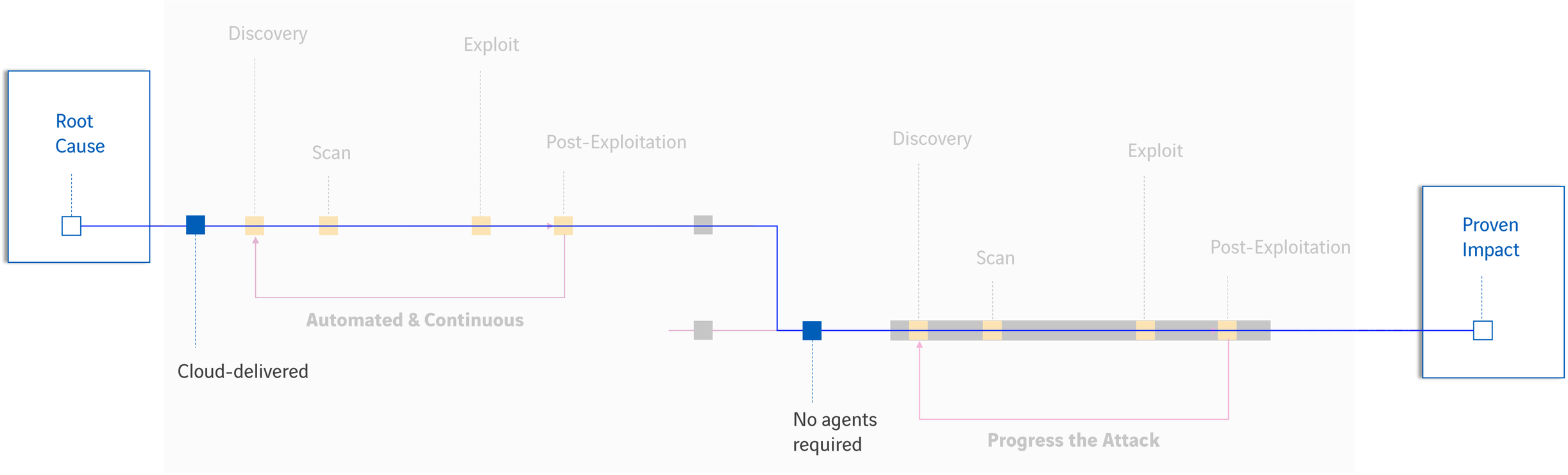
Die meisten Opfer hatten aktuelle (up-to-date) Präventivmassnahmen bzw. Schutzvorrichtungen

Es gibt keinen 100% Schutz. Die Frage ist nicht ob, sondern wann ein Angriff erfolgreich sein wird.



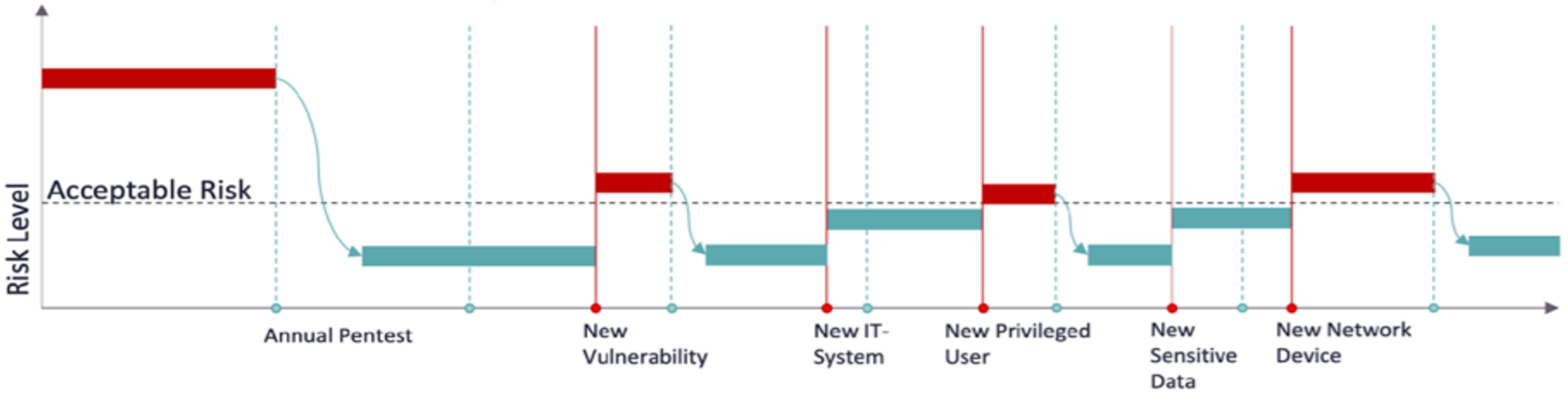
Massnahmen 1.1 – End-to-End Security Validation

Outside-in

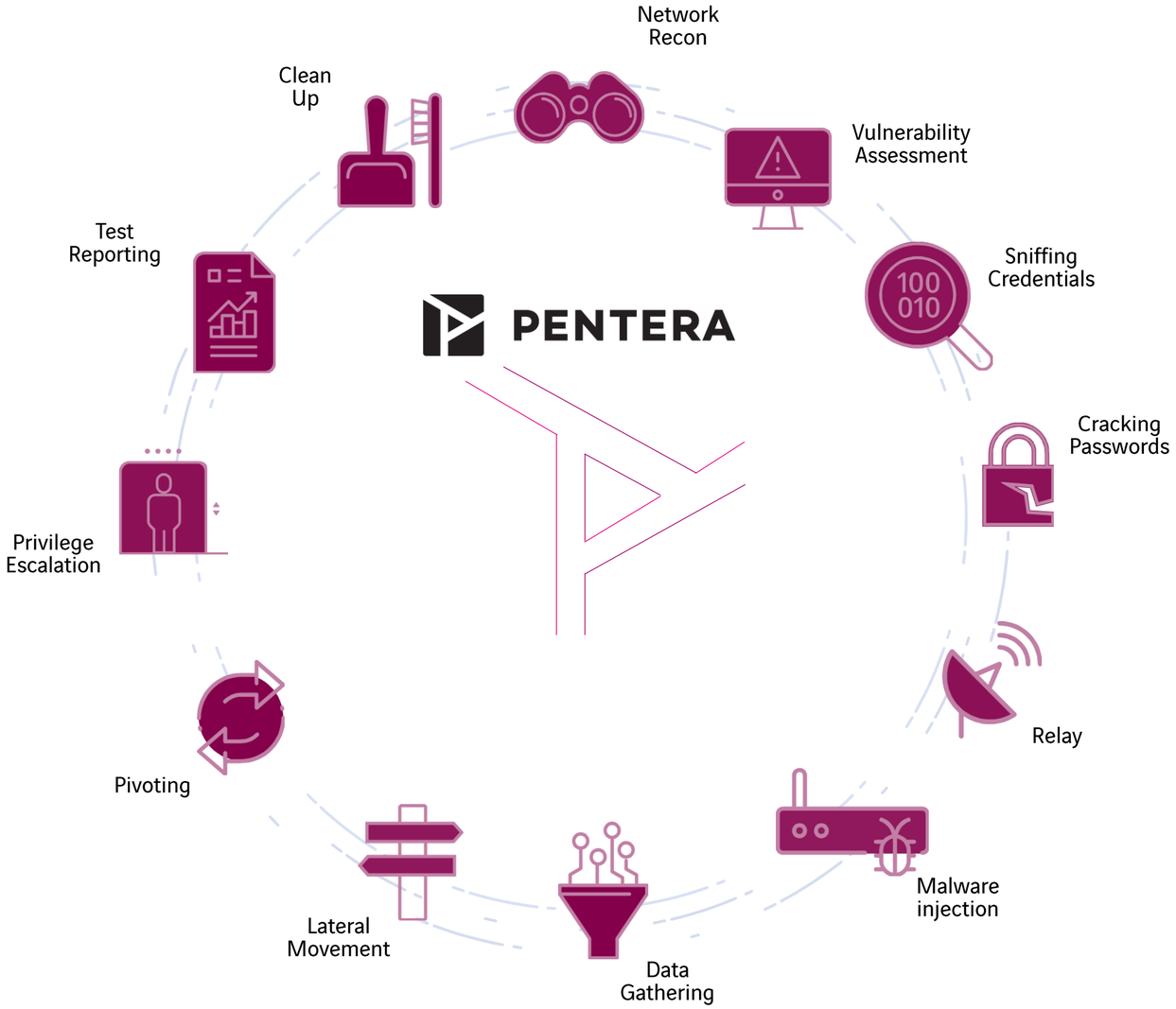


Inside-out

Massnahmen 1.1 – Continuous End-to-End Security Validation



Technology matters – Automatisiertes Pentesting



Keine Simulation.
Ethical exploits

sicher & kontrolliert
#Do-No-Harm

Agentless & Echtzeit
Vollständige Security Validierung

Unmittelbare Reaktionsfähigkeit

Technologie Fakten

- Keine Simulation (interner und externer Angriffsvektor)
  - Angriffe werden, dem MITRE Attack Framework und OWASP folgend, ethisch sauber und harmlos durchgeführt. Ergebnisse sind daher keine statistischen Modelle, die nur Rückschlüsse auf die tatsächlichen Sicherheitslücken in der produktiven Infrastruktur erlauben.
- Keine **statische** Security Priorisierung nach CVSS Punktekarte wie bei klassischem Vulnerability Management
  - Intelligente Schwachstellen Priorisierung erfolgt basierend auf „exploited" und damit angreifbarer Sicherheitslücken. Volle Visualisierung des gesamten Attack-Trees
- Ethisch saubere und harmlose Attacken
  - Penetration Tests finden laufend in der produktiven Umgebung und denselben Bedingungen statt, die auch Hacker vorfinden, daher darf kein Schaden angerichtet werden. Keine Penetration auf Kernelebene, Exploits aus Eigenentwicklung und Verzicht auf künstliche Intelligenz
- Unterschiedliche Targeted Testszenarien
  - Blackbox Test
  - Graybox Test (gezielte Security Validierung mit "What-if" Parametern)
  - RansomwareReady Überprüfung (vollständige Emulation eines Ransomware Angriffes)
  - Active Directory Security Assessment

Technologie Fakten

- Häufigkeit von Pentests kann massiv erhöht und jederzeit in der exakt gleichen Form wiederholt werden
  - Re-Validierung nach Behebung von Schwachstellen
  - Trotz grosser Anzahl von getesteten Systemen (Server, Clients, Firewalls, IPS, Router, Wlan APs,...) gleichbleibend hoher Qualitätsstandard und Detailtiefe der Resultate
- Remediation Wiki
  - Erklärung & Anleitung zur Bereinigung von Sicherheitslücken (integrierbar in Support Ticket System via API) für alle Findings und Resultate
- Technical Reporting
  - Live Dashboard und Live Attack Tree Visualisierung der vollständigen Angriffsoperationen (MITRE Framework, OWASP)
  - Auflistung aller durchgeführten / versuchten Attacken inklusive Dokumentation von allfälligen Systemeingriffen
  - Sämtliche Aktivitäten und Resultate sowohl als PDF als auch im Excel Format zur gezielten Nachbearbeitung
- Management Reporting
  - Bewertung des Security Zustandes wird C-Level tauglich auf einer Zeitachse dargestellt
  - Top Findings und Risikoanalyse
  - Dokumentation unterstützt Security Verantwortliche bei der Argumentation für zukünftige Investitionen (hohes Risiko in bestimmten Bereichen wird konstant nachgewiesen) und/oder bereits abgeschlossene IT Projekte (Security Posture hat sich verbessert)

Erweiterter Anwendungsbereich

- Einhaltung Compliance Richtlinien und Vorgaben
- Validierung von interne/externen IT Security Leistungen (z.B.: EDR-, SOC-, NBA- Services)
- Effizienzsteigerung von Red-Teams & Bug Bounties
- Überprüfung von Home Office-, Cloud- oder remote Infrastruktur (Azure Assets, Azure AD...)
- Quality / Security Assurance Unterstützung in der Applikationsentwicklung
- Unterstützung bei Produkt Evaluationen und IT Projekten
  - IT Security Protection Lösungen (EDR, Firewalls, IPS, Malware Protection, ...)
  - Netzwerk-, Server- und Infrastruktur Re-Design
  - Applikationsentwicklung

Live Demo

Renata Rekic
Axians IT Services AG
Riedstrasse 1
CH-6343 Rotkreuz
renata.rekic@axians.com