ADVISORI

# Insights in Cyber Deception

## PROAKTIVE DETEKTIONSTECHNOLOGIEN IN MODERNEN CYBER SECURITY STRATEGIEN

06.Mai 2021

# Vorstellung des Vortragenden

## Marcel Rieger

27 Jahre alt

Senior Consultant Information Security

ADVISORI FTC GmbH

Frankfurt am Main

### Themen
Detektion-Technologien
SIEM ft. AI
Incident Response

### Projekte
Banken und Finanzbranche
Industrie-Konzerne
Mittelständische Industrie

### Kontakt
Marcel.Rieger@advisori.de
LinkedIn
XING

ADVISORI

**Unsere Vision**
Den digitalen Wandel am Puls der Zeit, gemeinsam gestalten.

**Unsere Kernbereiche:**
- Information Security
- Big Data
- Risk Management
- Regulatory Reporting
- Digital Process Management

Seit 2014

in Frankfurt am Main

Umsatz
+ 15 Mio. €

Erfolgreiche Projekte
+ 350

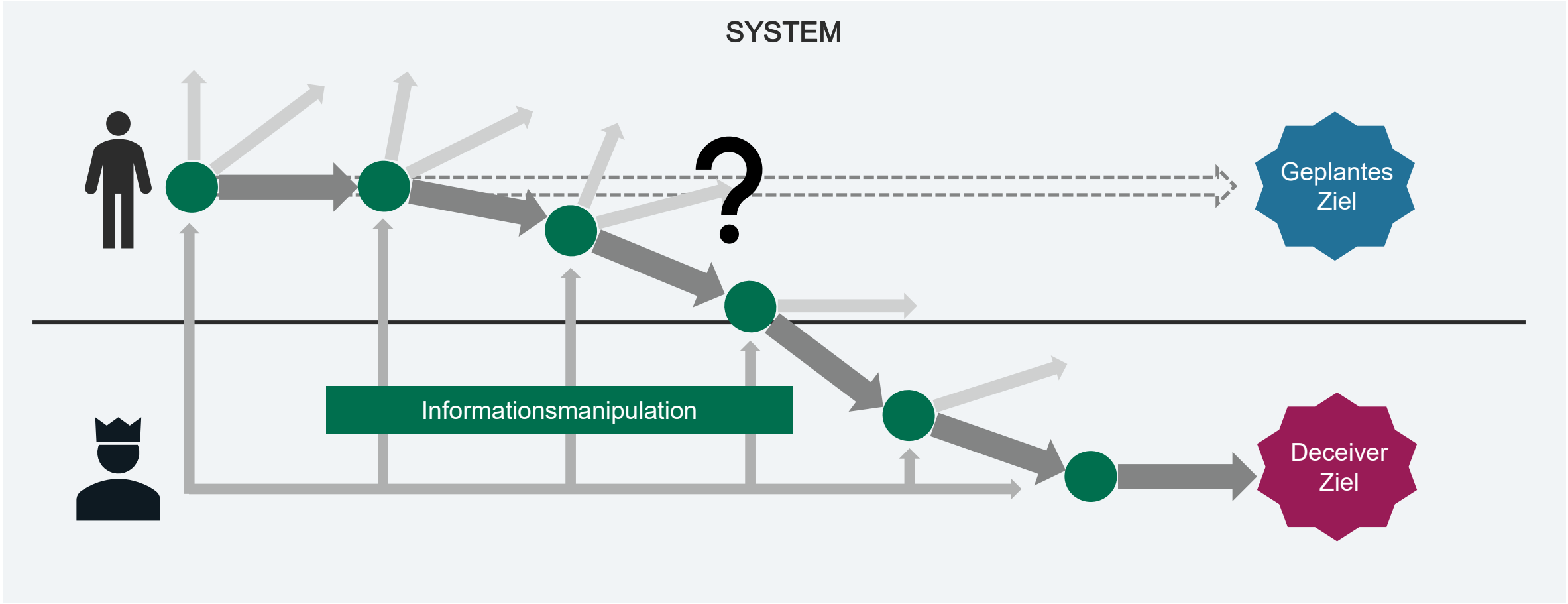
> 100 Mitarbeiter

# Agenda

1. Einleitung – Was ist Deception?
2. Hintergrund – Wie sind wir zum aktuellen Stand gekommen?
3. Problemstellung – Was sind die Grenzen der aktuellen Security Ansätze?
4. Lösung – Wie löst Cyber Deception diese Herausforderung?

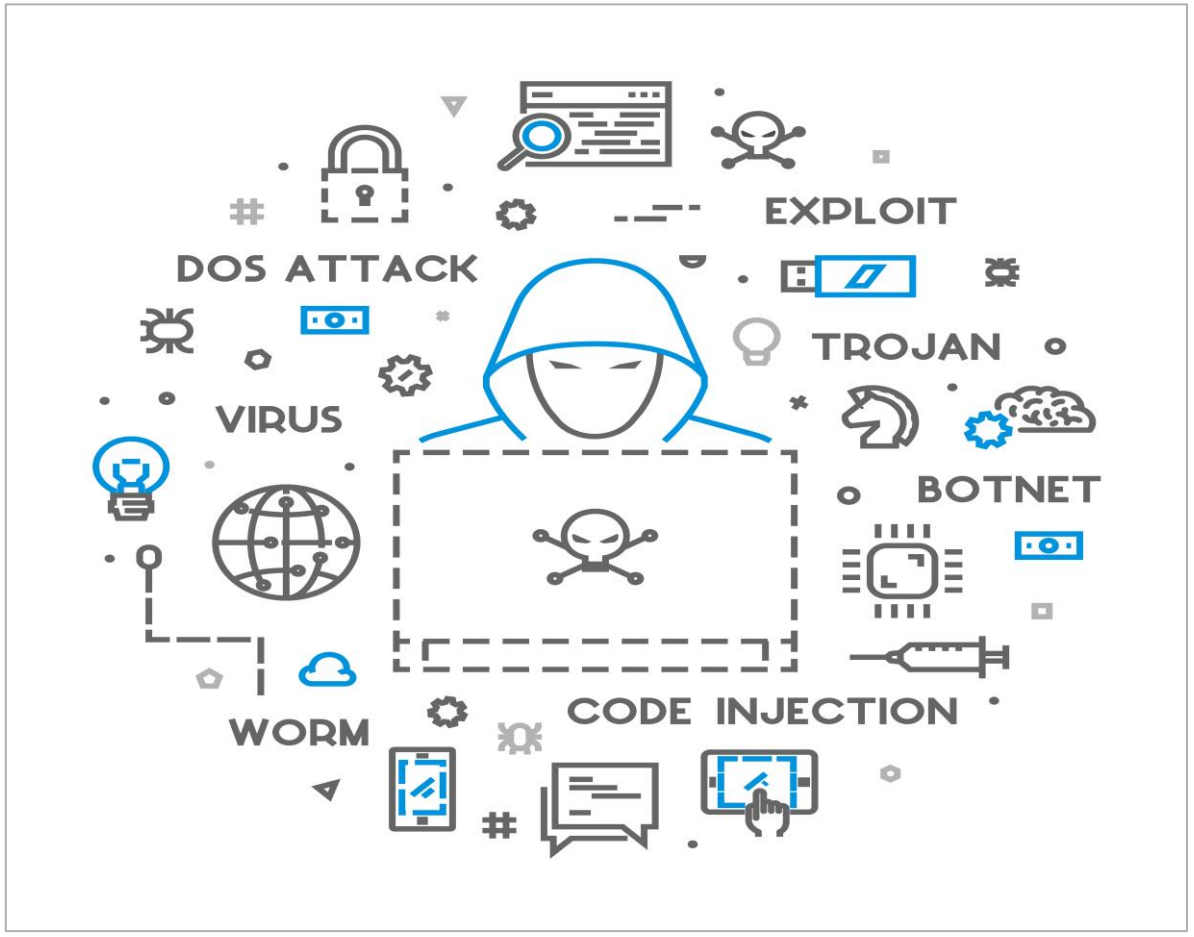
# Einleitung – Was ist Deception?

# Deception lenkt den Adressaten in eine Richtung entgegen der eigenen Intention



# Deception, so alt wie die Menschheitsgeschichte…

# Angreifer haben Deception längst in ihr Repertoire aufgenommen




Social Engineering

(Spear)-Phishing

Impersonation

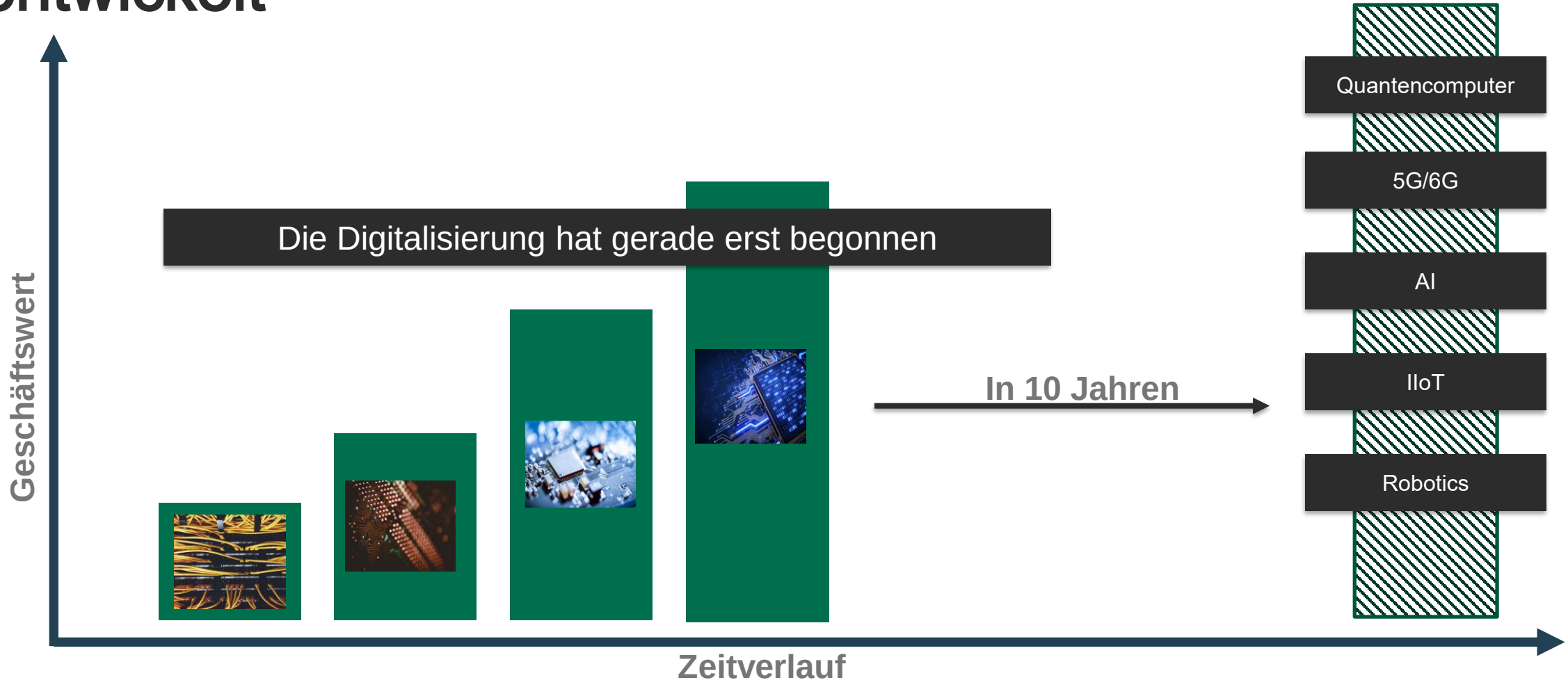
Es gibt zwei Arten von Unternehmen:

1. Die Unternehmen, die gehackt wurden

2. Die Unternehmen, die es noch nicht bemerkt haben

# Wie sind wir zum aktuellen Stand gekommen?

# Die IT hat sich zum wichtigsten Wachstumsfaktor entwickelt



# Mit steigendem Wert, werden auch mehr Kriminelle angezogen

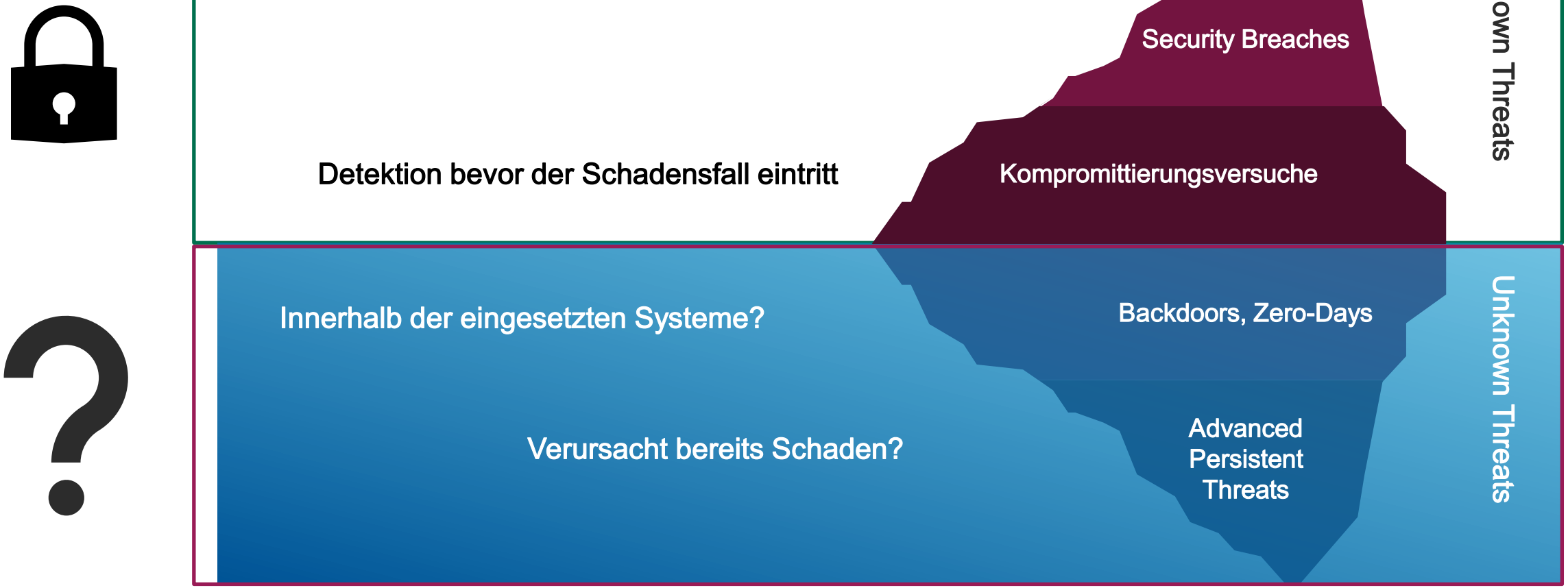

Wachsender Geschäftswert der IT

Kriminelles Interesse und Schadenspotenzial

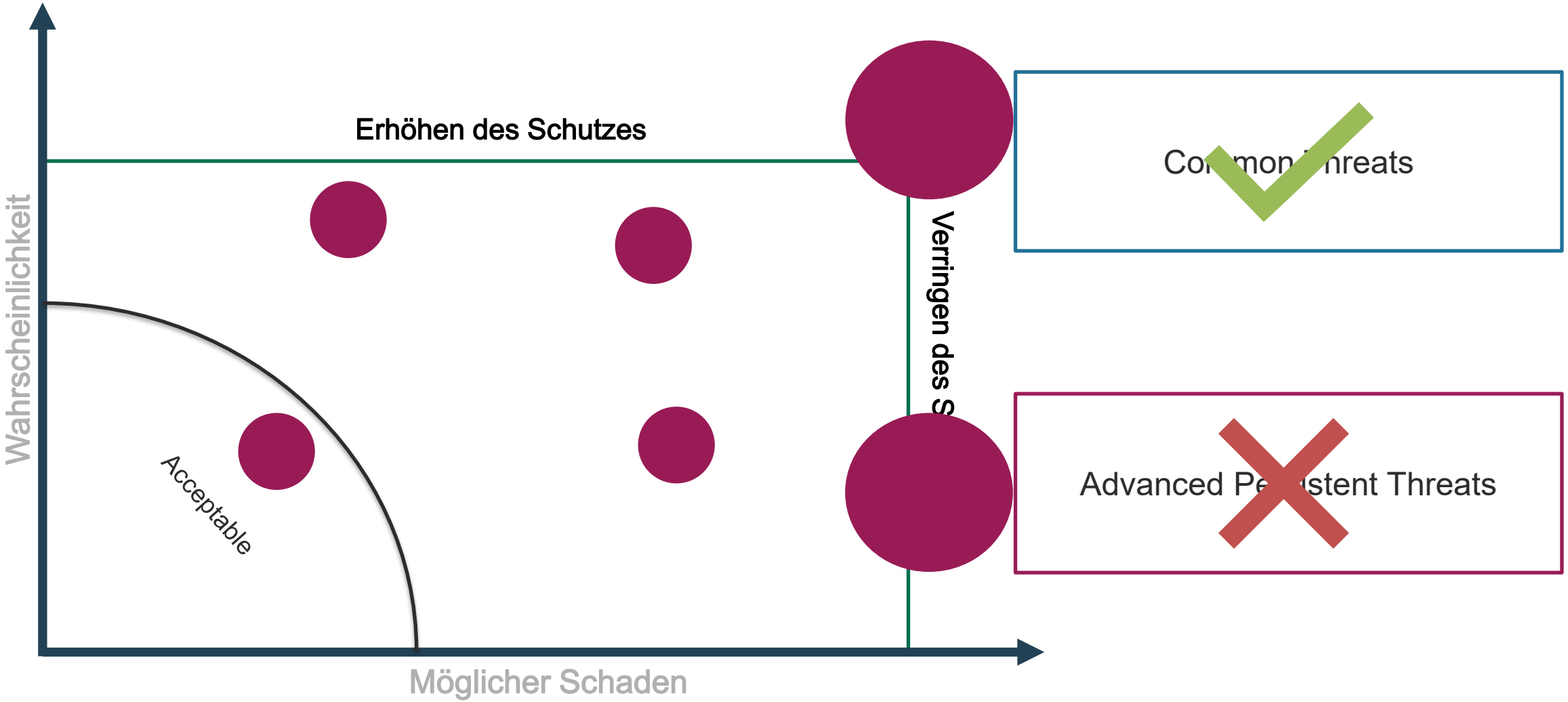
*Source: Statista

# Problemstellung – Was sind die Grenzen der aktuellen Security Ansätze

# Es gibt viele bekannte und unbekannte Angriffsvektoren



# Das Risiko einer Bedrohung ergibt sich aus Wahrscheinlichkeit und Schaden



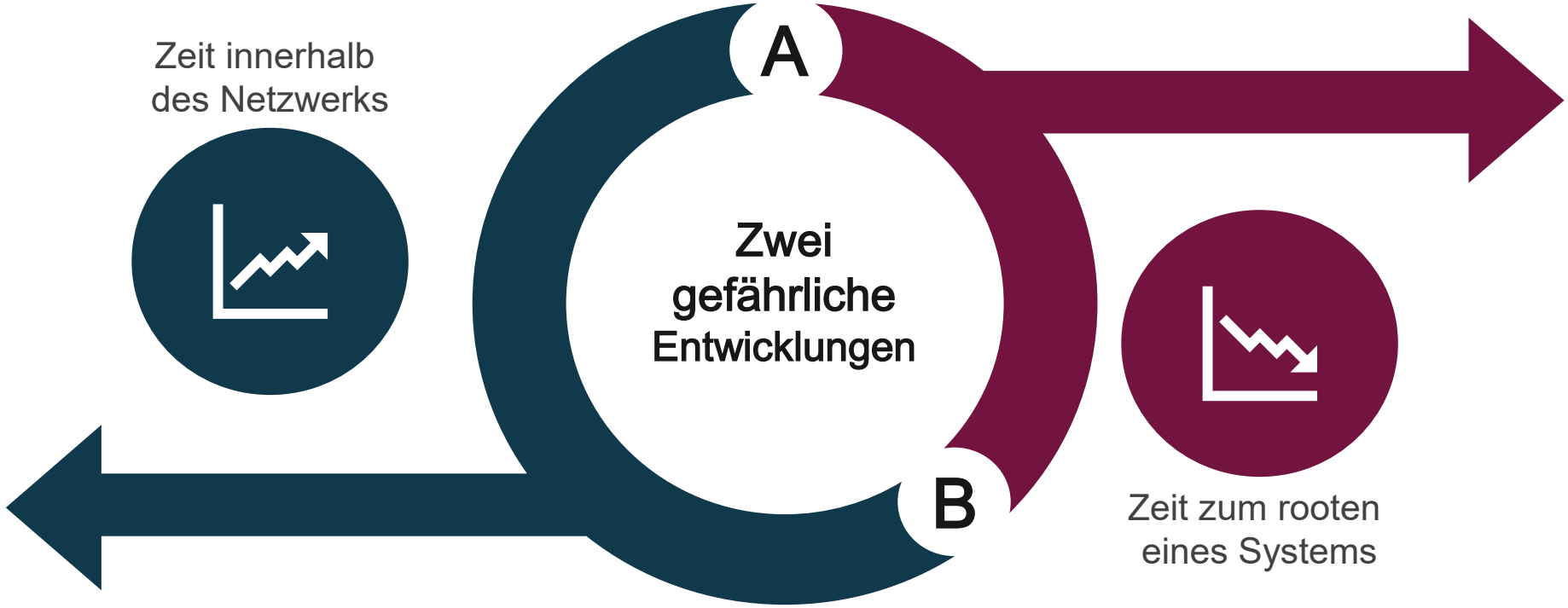
# Zwei Entwicklungen machen Advanced Persistent Threats enorm gefährlich

Advanced Persistent Threats

Darknet Aktivitäten

Automatisierte Angriffe

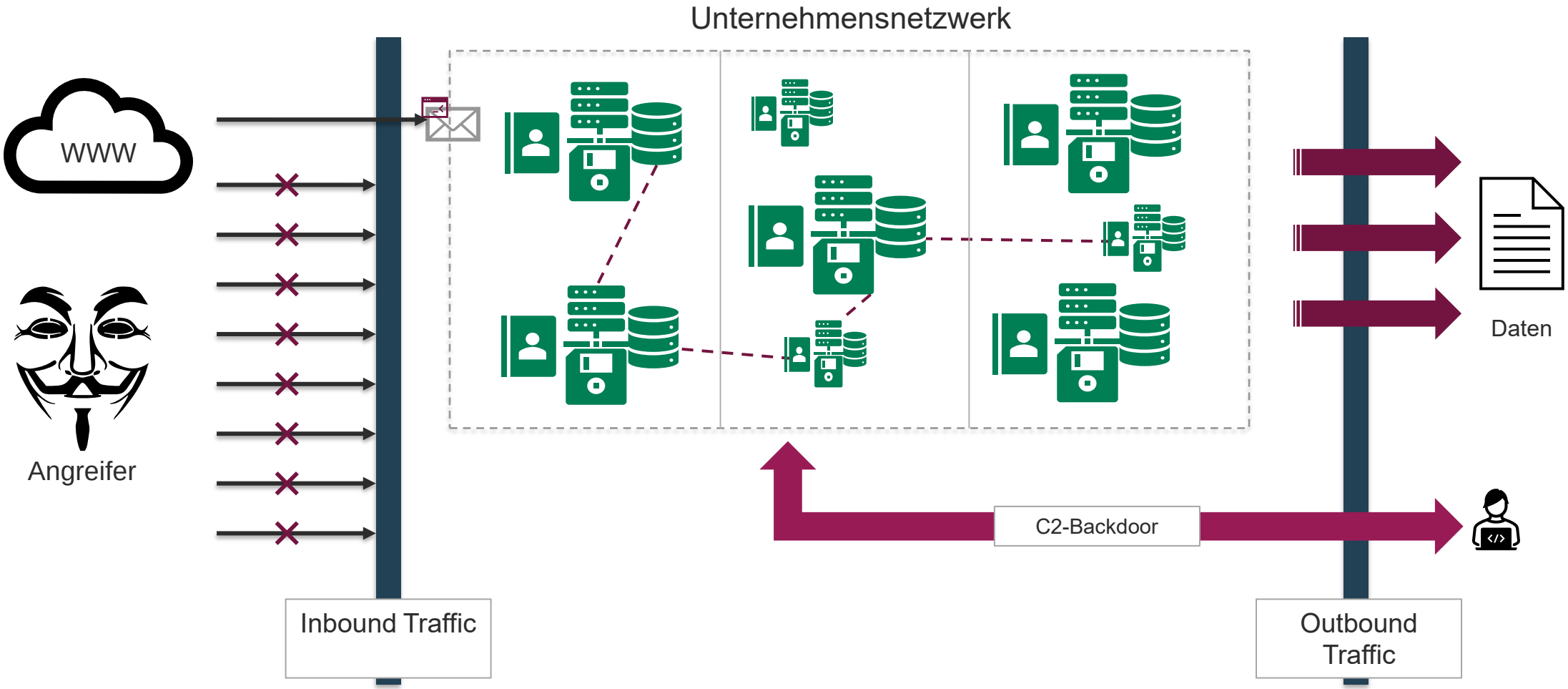
Drive-By + Waterholing



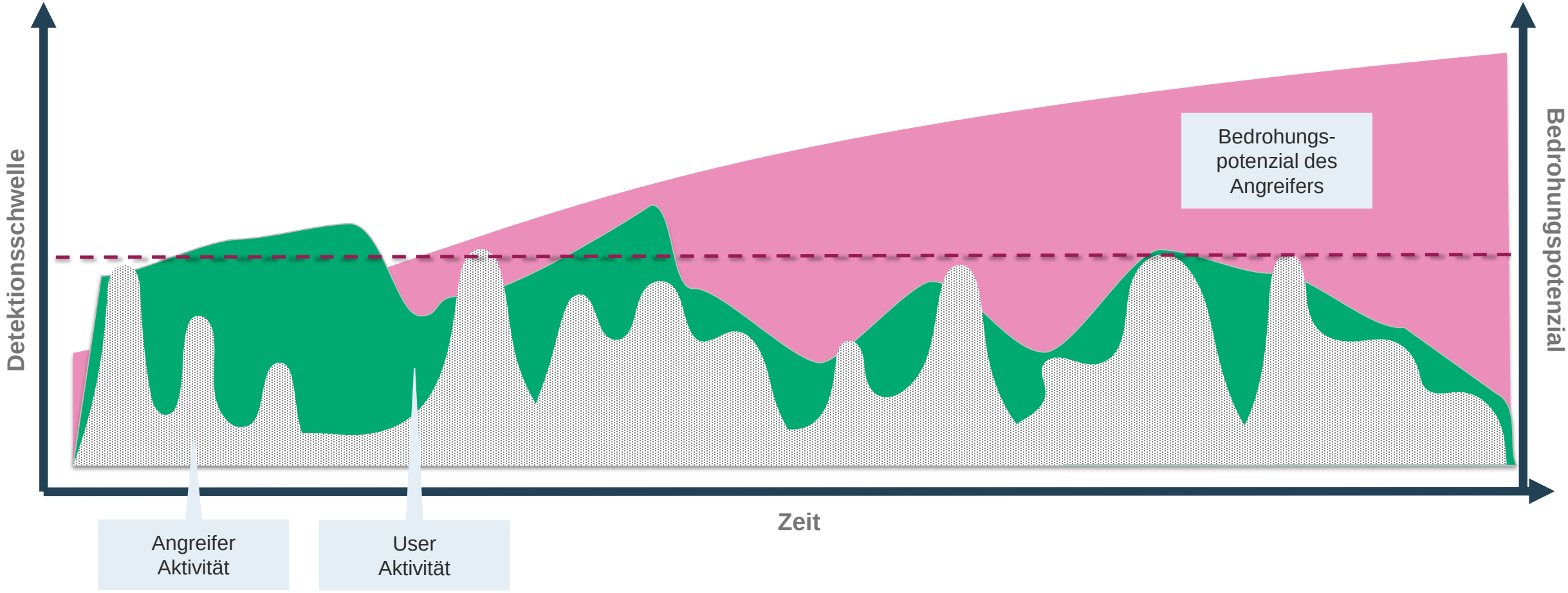

*Source: Counterhack Report

Bis Unternehmen erkennen, welche Möglichkeiten neue Technologien bieten, haben Angreifer diese längst perfektioniert

# Versierte Angreifer kompromittieren sukzessive alle Systeme innerhalb des Netzwerks



# Versierte Angreifer erhöhen sukzessive und unerkannt ihr Bedrohungspotenzial



# Lösung – Wie löst Cyber Deception diese Herausforderung?

Mit Hilfe von Deception kann ein Unternehmen Bedrohungen innerhalb des Netzwerks detektieren, die mit herkömmlichen Mitteln unerkannt bleiben

# Mit Deception wird ein Ansatz verfolgt der sich auf Advanced Persistent Threats fokussiert

- Unbekannte Angriffsvektoren identifzieren
- Wissen über Angriffstechniken ausbauen
- Relevante Ziele innerhalb des Netzwerks identifizieren
- Angriffe komplett am root cause stoppen

Lösung – Wie löst Cyber Deception diese Herausforderung?

# Deception wird als zusätzliche Schicht in die Security Strategie integriert

**Deception**

\+ Fokus – Detektion des Unbekannten bevor Schaden entsteht

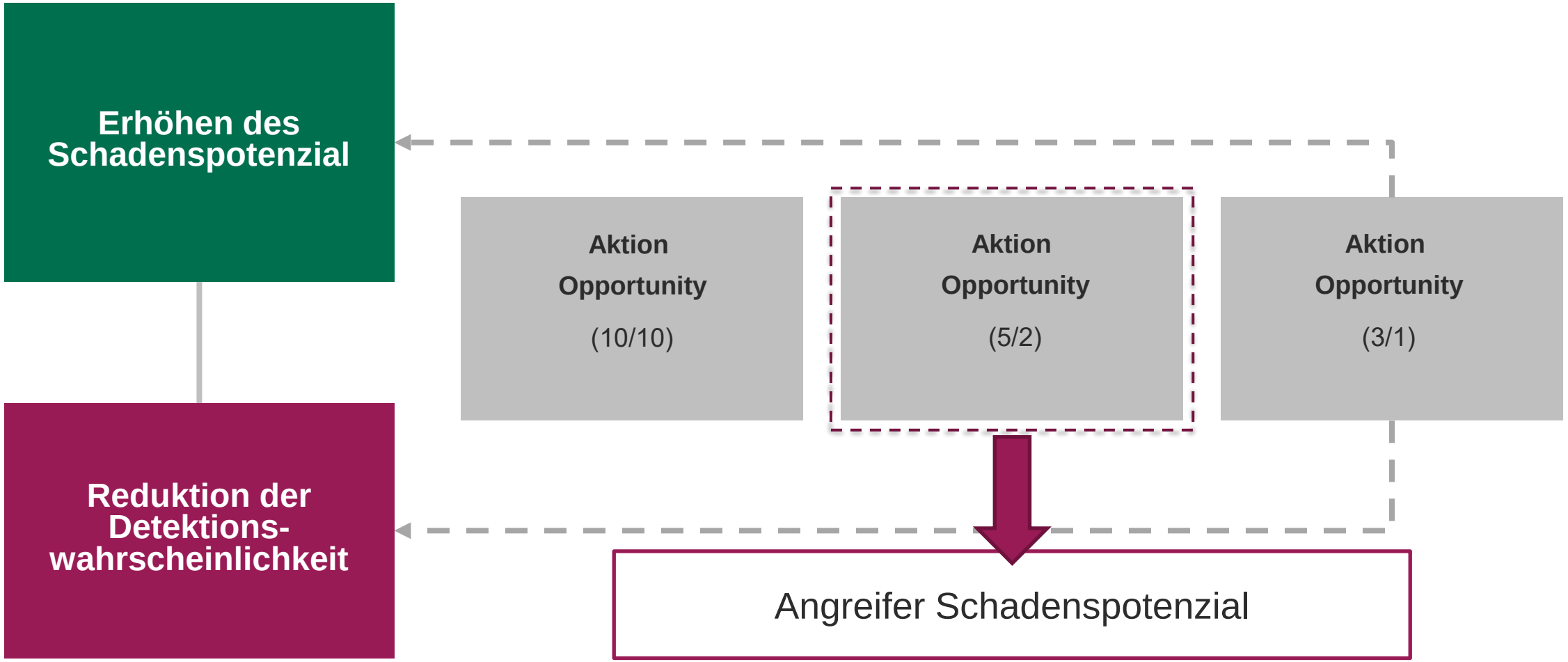
**Protection**

o Fokus – Schutz vor bekannten Bedrohungen

The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself – Sun Tzu

Lösung – Wie löst Cyber Deception diese Herausforderung?

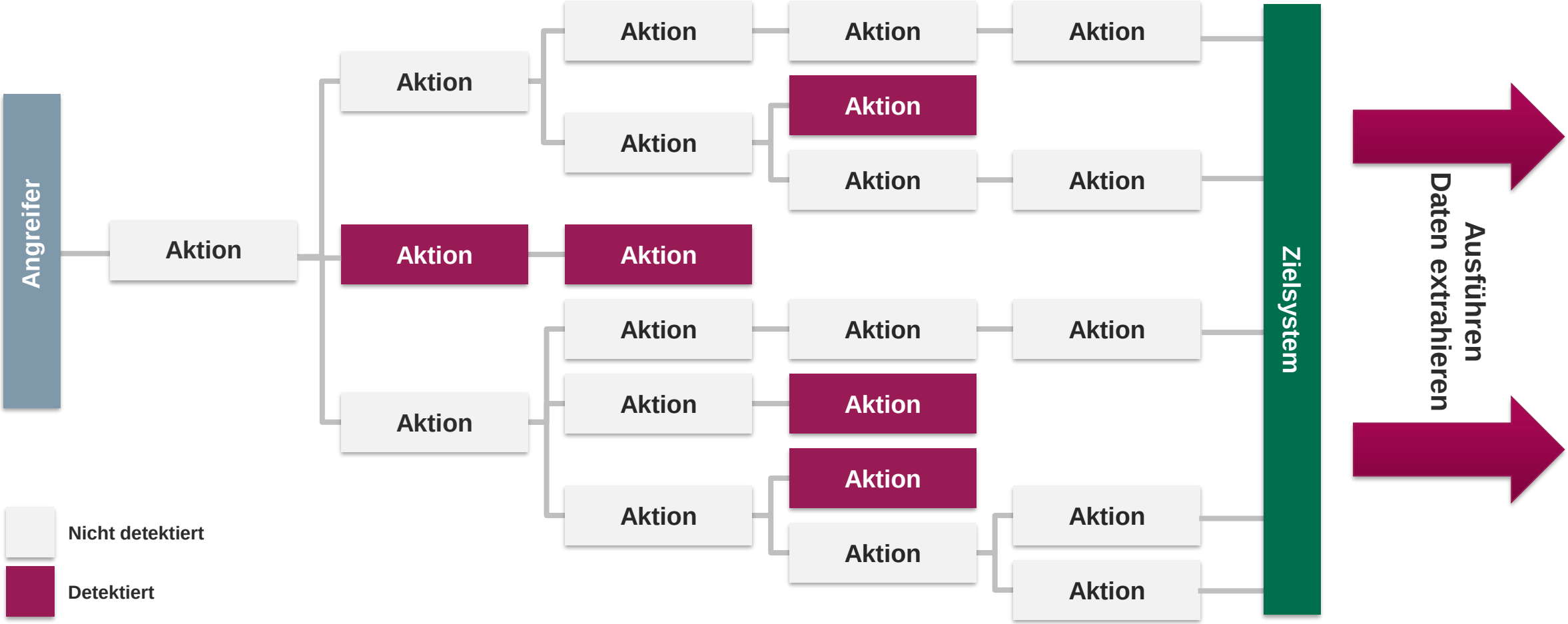
# Das Damage-Detection-Model* hilft potenzielle Aktionen eines Angreifers zu modellieren



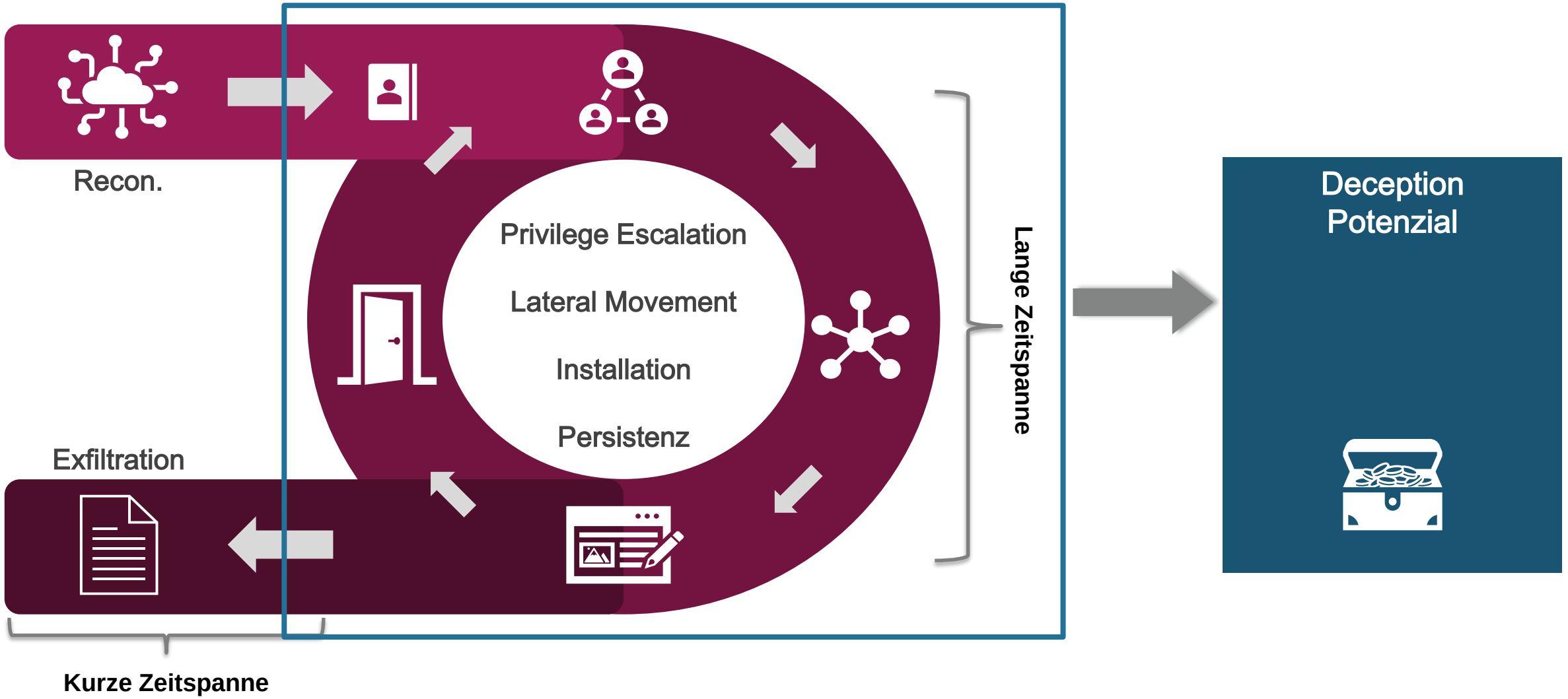

*Source: HUANG, ZHU (2018, NY)

Lösung – Wie löst Cyber Deception diese Herausforderung?

# Angreifer haben vielfältige Möglichkeiten, um jedes Zielsystem im Netzwerk zu erreichen



# Einige Angriffsphasen bieten Potenzial für das implementieren von Deception



Lösung – Wie löst Cyber Deception diese Herausforderung?

# Deception wird mit Hilfe von Decoys im Unternehmen implementiert

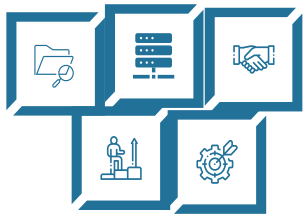
Deception ist nicht universell einsetzbar

Decoy Systeme | Decoy Accounts | Decoy Informationen | Decoy Vulnerabilities | Decoy Schnittstellen

Decoys werden individuell auf das Netzwerk des Unternehmens zugeschnitten

Lösung – Wie löst Cyber Deception diese Herausforderung?

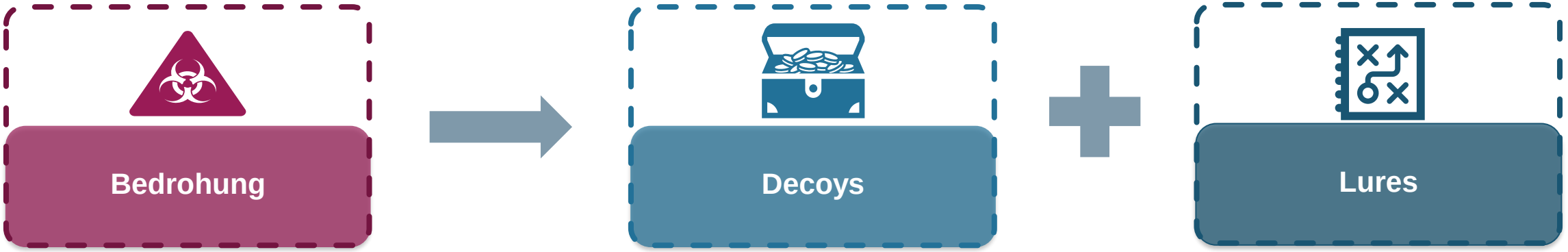
# Lures rücken die Decoys in das Blickfeld des Angreifers



Decoys

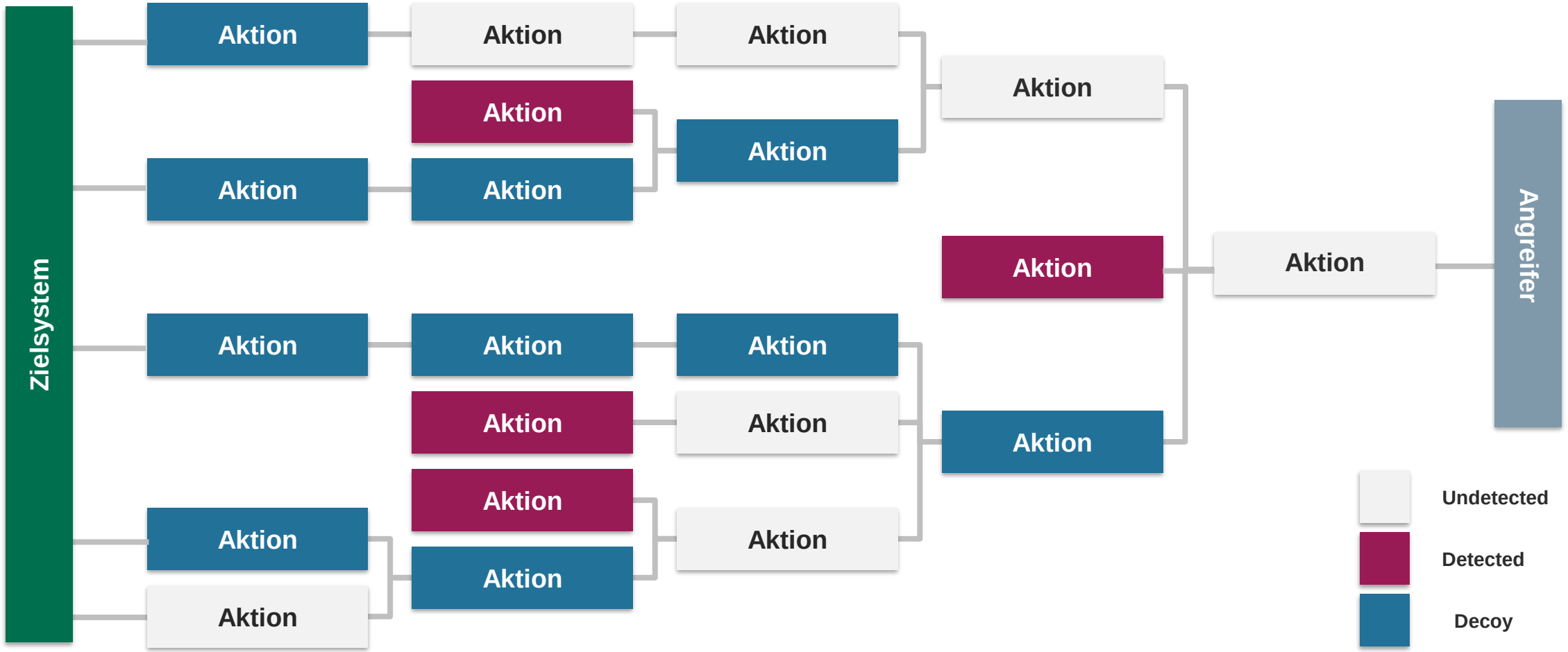
Decoys allein helfen noch nicht

Lures locken den Angreifer zu den Decoys anstatt der produktiven Systeme



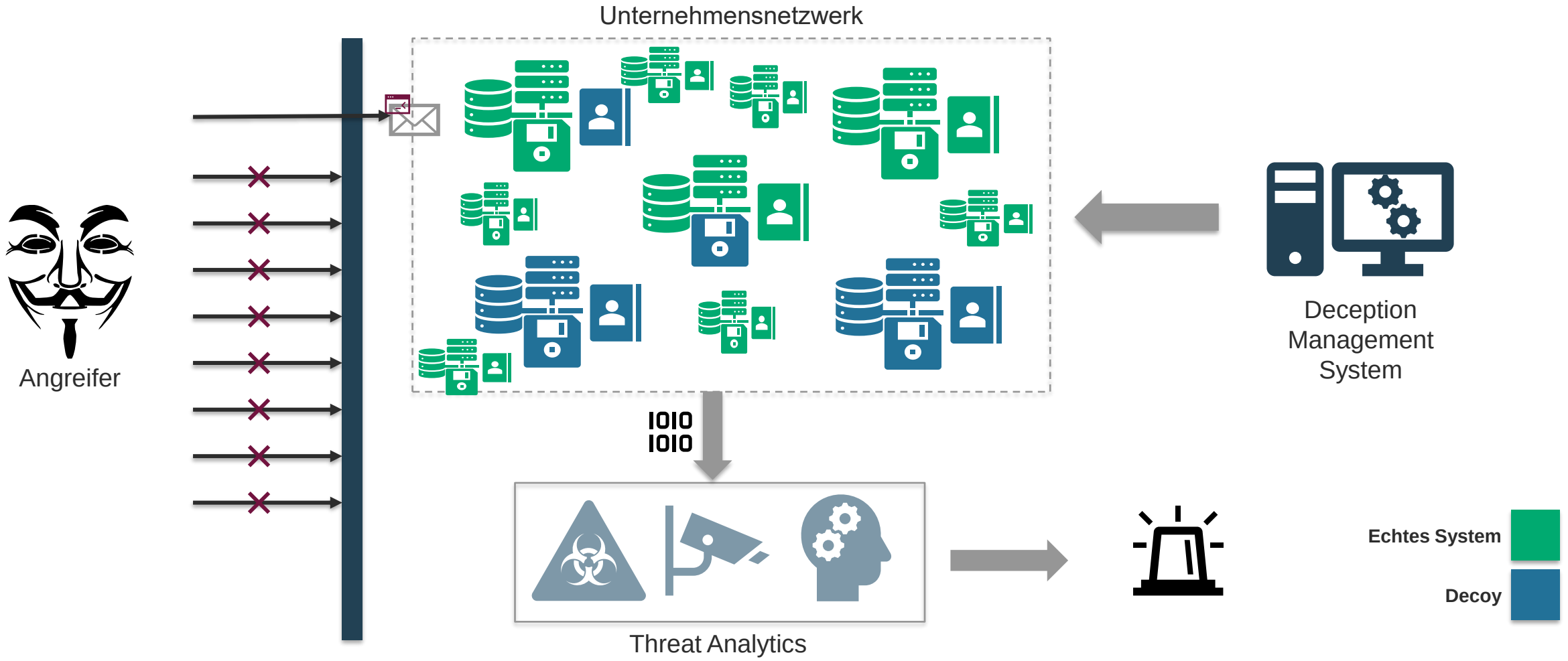
Lösung – Wie löst Cyber Deception diese Herausforderung?

# Deception legt einen Pfad aus Decoys auf den Weg des Angreifers



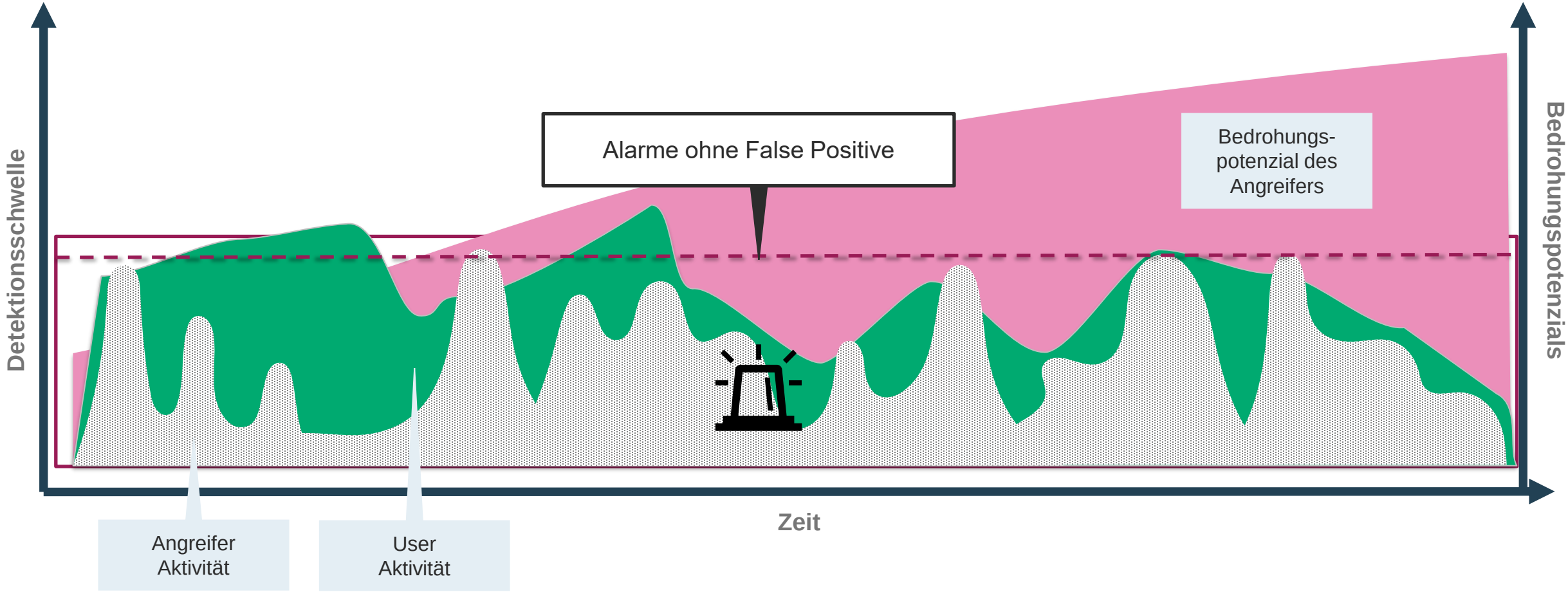
Versierte Angreifer müssen sich darauf verlassen, dass die Daten, die sie in einem Netzwerk sammeln real und zuverlässig sind

# Deception Technologien implementieren Decoys als Bestandteile des Netzwerks



Lösung – Wie löst Cyber Deception diese Herausforderung?

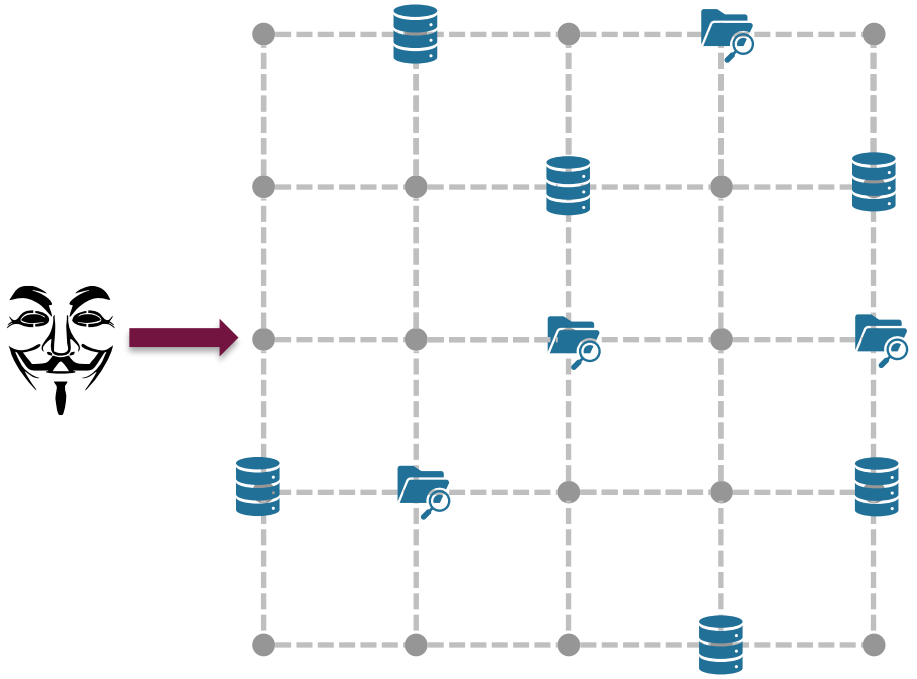
# Deception macht alle Angreifer Aktionen für das Unternehmen sichtbar



Deception hilft dabei bei der Suche nach der Nadel im Heuhaufen, den Heuhaufen aus der Gleichung zu streichen

Lösung – Wie löst Cyber Deception diese Herausforderung?

# Deception findet den Angreifer und ermöglicht es den Ausgangspunkt des Angriffs zu finden



Woher kommt der Angreifer?

Welche Tools werden verwendet?

Welche Systeme sind noch kompromittiert?

| Records Deceptions | | |
|---|---|---|
| 1 | 11/06/2020 22:53:12 | Entering System A with Decoy Account „Fake-Admin“ |
| 2 | 11/06/2020 23:54:17 | Execution of Mimikatz on System A |
| ……. | | |
| 3 | 22/06/2020 23:54:17 | RDP-Connection User A to System B |
| …… . | | |

| Post-Incident – Forensic Records | | |
|---|---|---|
| 1 | 07/04/2020 01:05:32 | Unblocked Mail to User X with Link to „Enter page“ |
| 2 | 11/06/2020 22:53:12 | Entering System Z with User Z via RDP |
| 3 | …… | …… |

# Deception kann für jegliche Security Maturity Level Mehrwerte liefern

| | Deception | Mehrwert |
|---|---|---|
| Low Maturity | Deception als Alternative bzw. Ergänzung von herkömmlichen Detektionsmitteln | Liefert im Vergleich zu „normalen“ Detektionssystemen keine False-Positive Alarme |
| Medium Maturity | Aufbau einer Deception Umgebung als proaktive Erweiterung des bestehenden Defensiven Spektrums | Ergänzend zu SIEM Systemen kann mithilfe von Deception die IR optimiert werden |
| High Maturity | Integration von Deception Technologien als Bestandteil einer holistischen Security Infrastruktur | Proaktive Verteidigung mit Threat Hunting und Incident Response in Form von Blue Teaming → TI |

# Deception Use Cases finden sich in allen Unternehmen

| | Bank | Industrie | Konsumgüterhersteller |
|---|---|---|---|
| **Systemlandschaft** | Große und unterschiedliche Applikations- und Datenbanksysteme | Applikationssysteme und zunehmende vernetzte ICS | Applikationssysteme und zunehmende vernetzte ICS und Produktdaten |
| **Bedrohungen** | Falsche Trading Informationen<br>Manipulation Zahlungsströme | Manipulation Industrieanlagen<br>Übernahme Produktionsdaten | Diebstahl Produktgeheimnisse<br>Manipulation Produktionsanlagen |
| **Deception Use Case** | Erweiterung des Netzwerks Decoy Accounts, Decoy Vulnerabilities, Decoy Systeme | Erweiterung des ICS<br>Decoy ICS, Decoy Files, Decoy Systeme und Schnittstellen | Applikationssysteme und zunehmende vernetzte ICS und Produktdaten |

Lösung – Wie löst Cyber Deception diese Herausforderung?

# In der Security-Welt ist Deception als Lösung bereits etabliert

Gartner listet Deception als vielversprechende Technologie

| ResearchAndMarkets.com | Growth rate<br>> 16% | 2.6 Bio. $<br>Until 2025 |
|---|---|---|

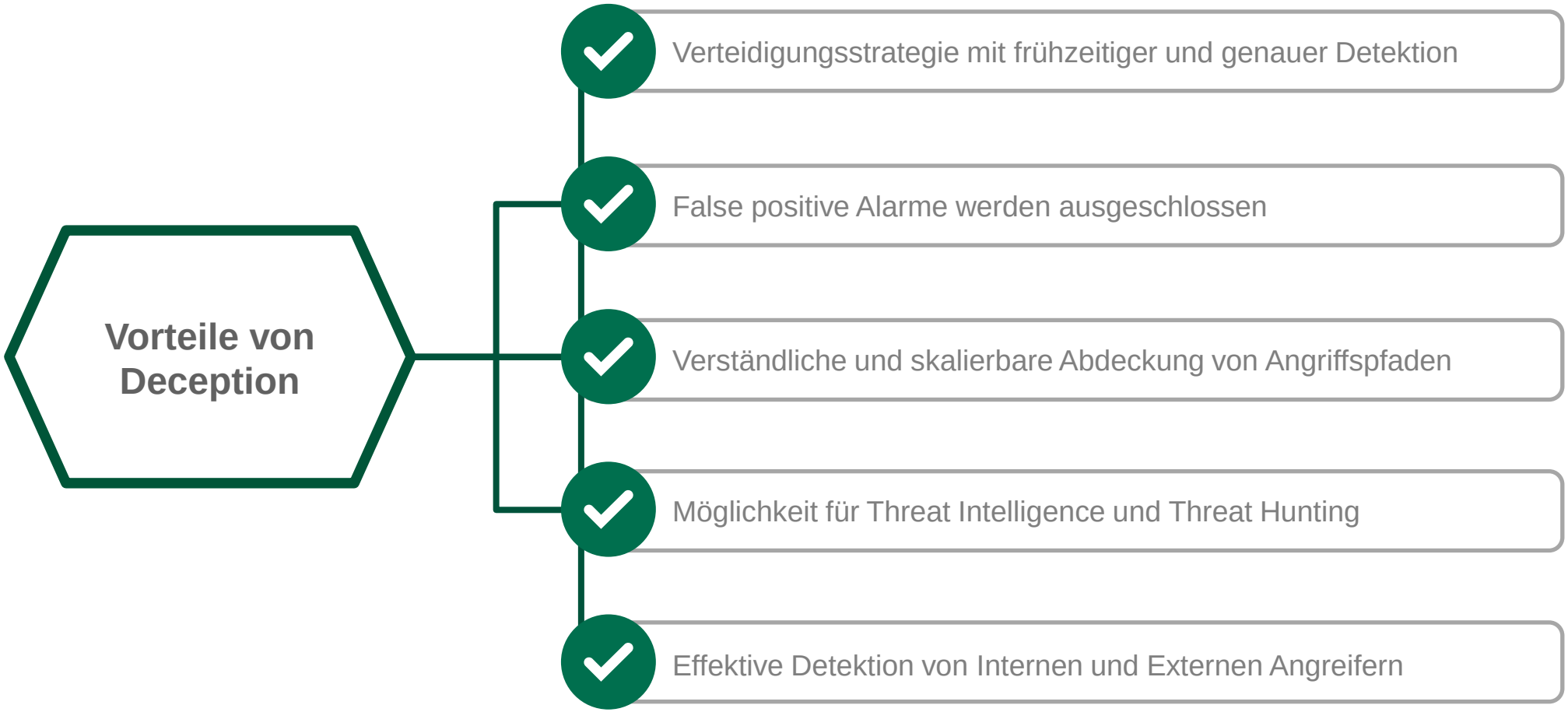
| Vendors | | |
|---|---|---|
| Illusive Networks | Rapid 7 | Attivo |
| SmokeScreen | TrapX | Ridgeback Network Defense |
| Countercraft | CyberTrap | Andere |

MITRE | Shield

| Channel | Collect | Contain | | | Facilitate | Legitimize | Test |
|---|---|---|---|---|---|---|---|
| Admin Access | API Monitoring | Admin Access | API Monitoring | Admin Access | Admin Access | Application Diversity | Admin Access |
| API Monitoring | Application Diversity | Baseline | Application Diversity | Application Diversity | Application Diversity | Burn-In | API Monitoring |
| Application Diversity | Backup and Recovery | Decoy Account | Baseline | Backup and Recovery | Behavioral Analytics | Decoy Account | Application Diversity |
| Decoy Account | Decoy Account | Decoy Network | Behavioral Analytics | Baseline | Burn-In | Decoy Content | Backup and Recovery |
| Decoy Content | Decoy Content | Detonate Malware | Decoy Account | Behavioral Analytics | Decoy Account | Decoy Credentials | Decoy Account |
| Decoy Credentials | Decoy Credentials | Hardware Manipulation | Decoy Content | Decoy Content | Decoy Content | Decoy Diversity | Decoy Content |
| Decoy Diversity | Decoy Network | Isolation | Decoy Credentials | Decoy Credentials | Decoy Credentials | Decoy Network | Decoy Credentials |
| Decoy Network | Decoy System | Migrate Attack Vector | Decoy Diversity | Decoy Network | Decoy Diversity | Decoy Persona | Decoy Diversity |
| Decoy Persona | Detonate Malware | Network Manipulation | Decoy Network | Email Manipulation | Decoy Persona | Decoy Process | Decoy Network |
| Decoy Process | Email Manipulation | Security Controls | Decoy Persona | Hardware Manipulation | Decoy System | Decoy System | Decoy Persona |
| Decoy System | Hunting | Software Manipulation | Decoy System | Isolation | Network Diversity | Network Diversity | Decoy System |
| Detonate Malware | Network Diversity | | Email Manipulation | Network Manipulation | Network Manipulation | Pocket Litter | Detonate Malware |

Lösung – Wie löst Cyber Deception diese Herausforderung?

# Fazit -Das Verwenden von Deception hat für Unternehmen viele Vorteile



Mit Deception könnte es gelingen, dass Unternehmen den Angreifern ausnahmsweise einen Schritt voraus sind