DECEPTIONGRID™
Überblick

TRAPX SECURITY

Führender Anbieter im Bereich
Advanced Breach Detection

TrapX Security im Überblick

Gründung: 2012

Unterstützung durch Intel, BRM, Opus, Liberty und Strategic Cyber Ventures

Niederlassungen in den USA, Mexiko, Großbritannien und Israel

WELTWEIT VERTRAUEN MEHR ALS 300 KUNDEN UND PARTNER AUF TRAPX.

Führender Anbieter im Bereich
Advanced Breach Detection

Gartner 2015 Cool Vendor

„Sicherheitsverantwortliche auf der Suche nach einer Lösung, die vor modernen, gezielten Angriffen auf umfangreiche und komplexe Umgebungen schützt, sollten sich TrapX genauer ansehen.“

The New York Times

Web Defenders Detect Russian Hand in Iranians' Hacking Attempt

FROST & SULLIVAN

Technology Leadership Award

„Frost & Sullivan gratuliert TrapX – die Lösung des Anbieters informiert Kunden in Echtzeit über die Aktivitäten innerhalb ihrer Netzwerke und liefert direkt verwertbare Erkenntnisse.“

THE GOLDEN BRIDGE AWARDS BEST WORLDWIDE

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2017

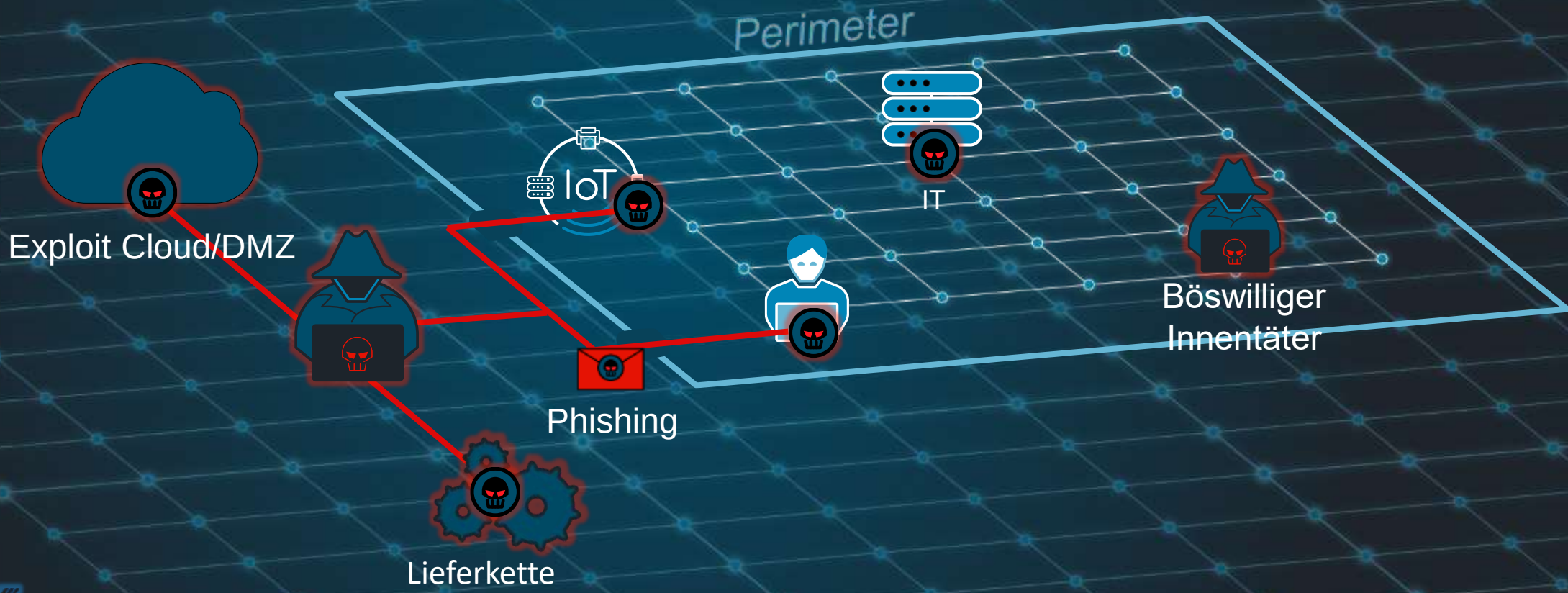
2015 Computing Security Awards WINNER

Beste APT-Lösung

SC 2017 awards Honored in the U.S.

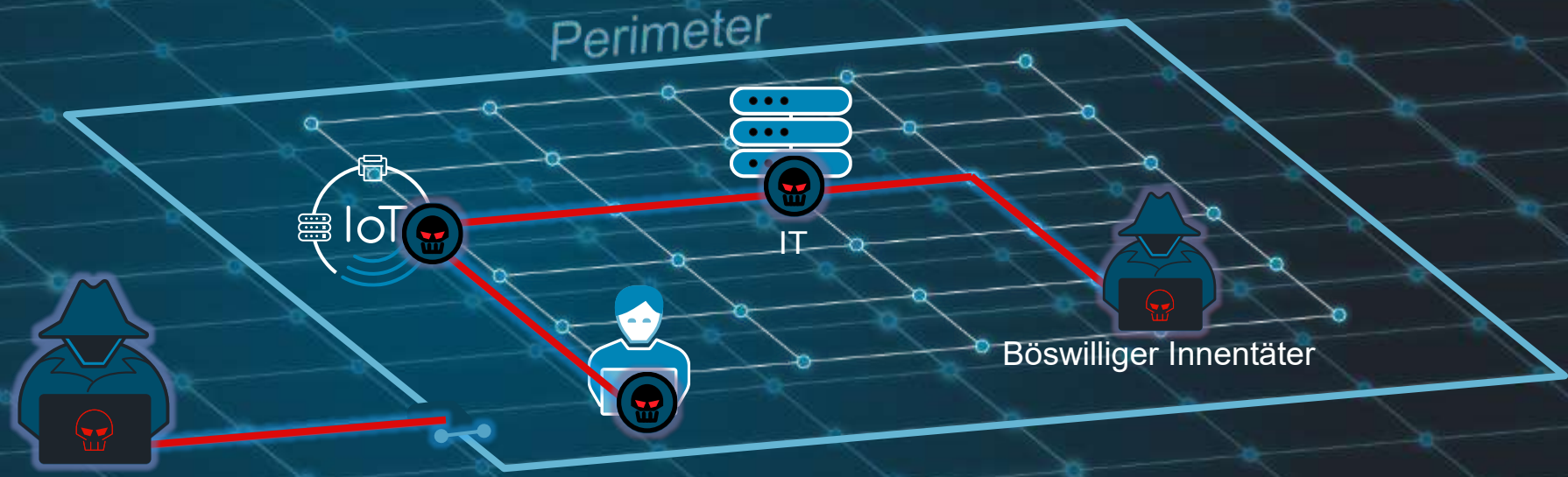
Verweildauer des Angreifers durch Sicherheitslücken

„Im Schnitt dauert es 191 Tage, bis eine Datenpanne entdeckt wird.
Wenn solche Datenpannen nicht schnell entdeckt werden, steigen die Kosten ins Unermessliche.“
„Cost of Data Breach“-Studie 2017, © Ponemon Institute



DeceptionGrid verhindert lange Verweildauer

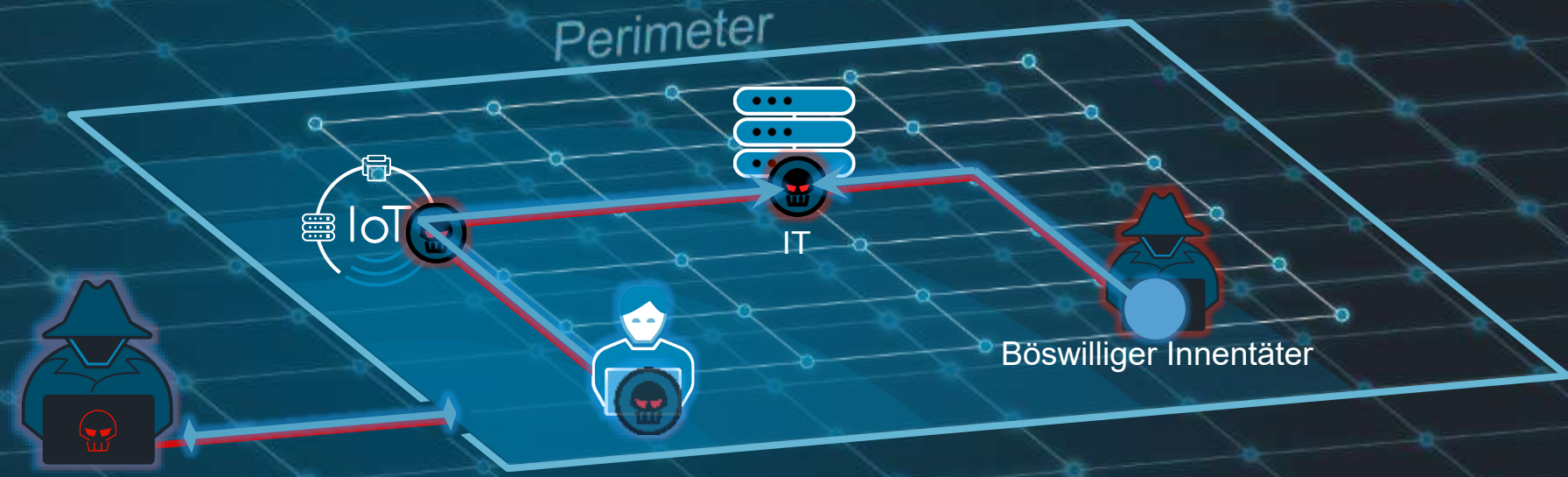
- Anlocken des Angreifers
- Präzise Erkennung von Sicherheitsverletzungen, fast keine False Positives
- Einleiten von Maßnahmen zur Mitigierung



TRAPX SECURITY

Umfassende Einblicke in das Netzwerk

- Einblicke hinsichtlich interner Reconnaissance (Informationsbeschaffung) auf Endgeräten
- Einblicke hinsichtlich Lateral Movement (Ausbreiten im internen Netzwerk)
- Einblicke hinsichtlich Netzwerk-Sniffing/Mapping-Aktivitäten
- Ermittlung von C&C-Kommunikation



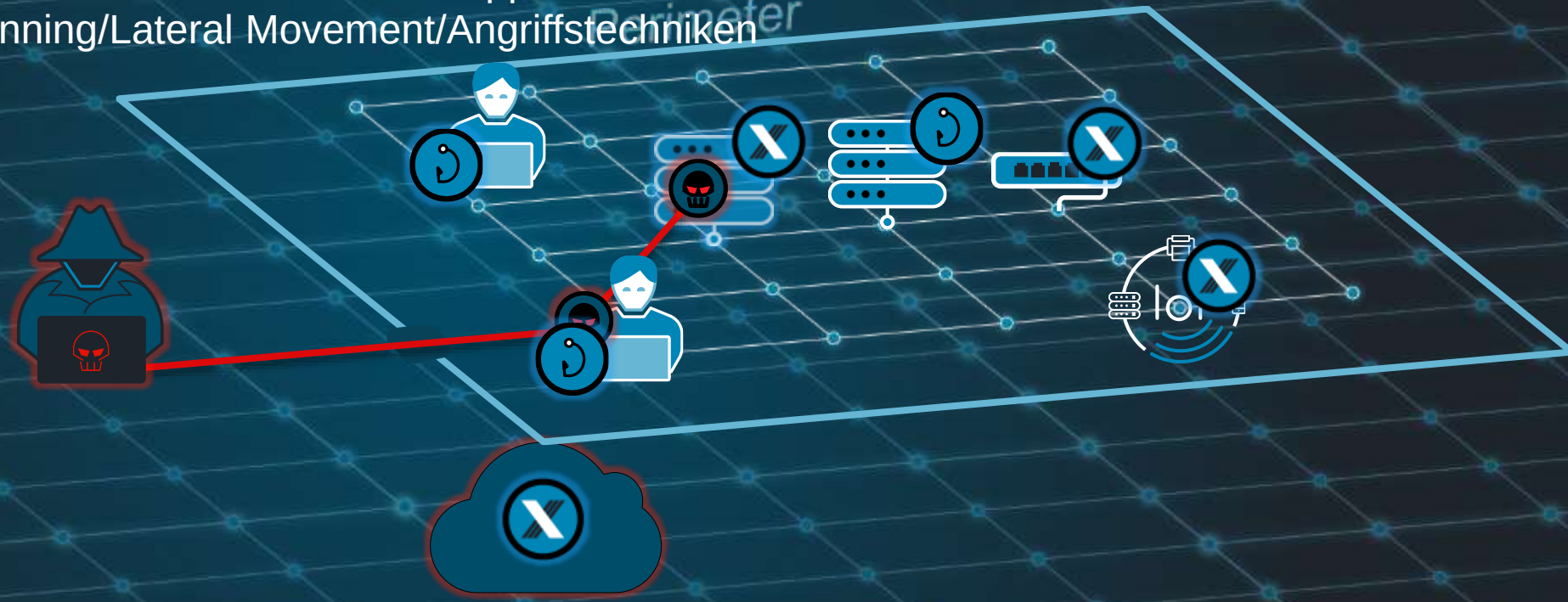
TRAPX SECURITY

Angreifer in die Falle locken

- Gefälschte Daten und Konfigurationen auf echten Endgeräten locken Angreifer in die Falle
- Einblicke hinsichtlich interner Reconnaissance auf Arbeitsplatzrechnern und Servern
- Simulierte Angriffspunkte, getarnt als mit dem Netzwerk verbundene Assets
- Glaubwürdige Reaktion auf diverse Protokolle und Applikationen
- Einblicke hinsichtlich Scanning/Lateral Movement/Angriffstechniken

Köder

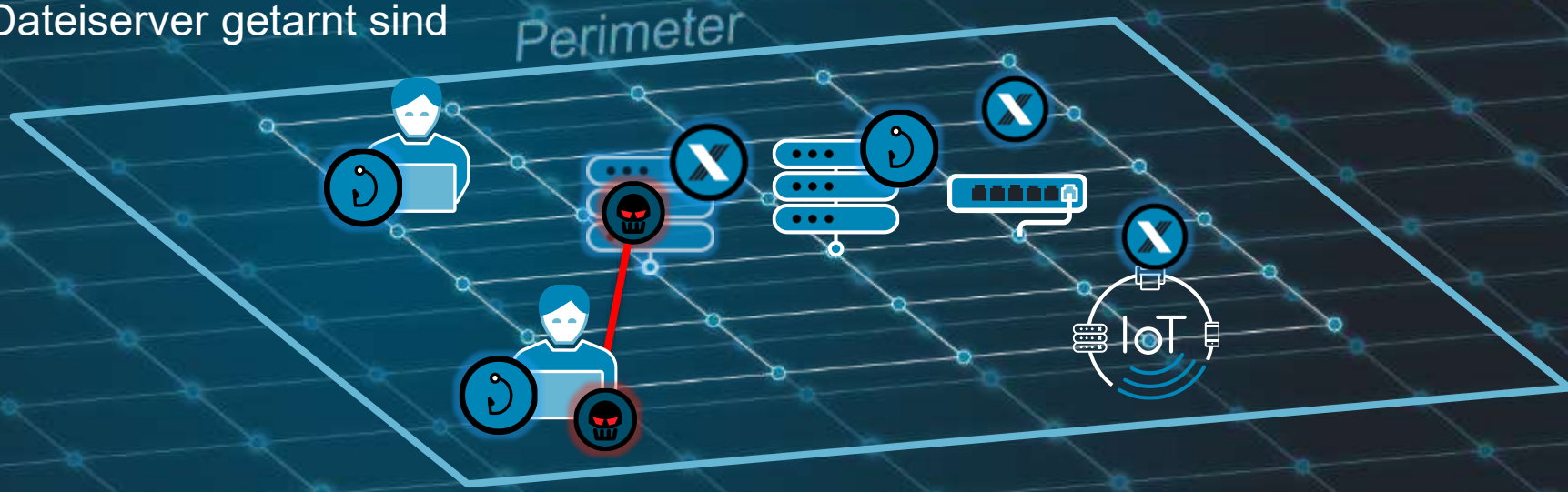
Fallen



TRAPX SECURITY

Exemplarische Use Cases

- Angreifer werden mithilfe von Fake-Passwörtern/simuliertem Netzwerkverkehr angelockt, um mit Fallen zu kommunizieren, die als wertvolle Assets getarnt sind
- Versuche, IoT-Schwachstellen auszunutzen, werden von Fallen abgefangen, die als IoT-Geräte getarnt sind
- Böswillige Mitarbeiter werden mithilfe von irreführenden Dateien angelockt („vergiftete Süßigkeiten“)
- Sich selbst verbreitende Malware/Ransomware wird durch simulierte Netzwerkfreigaben erfasst – diese führen zu Fallen, die als Dateiserver getarnt sind

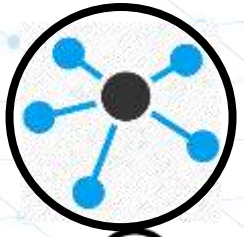


TRAPX SECURITY

DeceptionGrid – Mehrschichtenarchitektur

Nicht agentenbasiert, eingebrachte Zugangsdaten, SMB-Freigaben, irreführende Dateien etc.

Köder



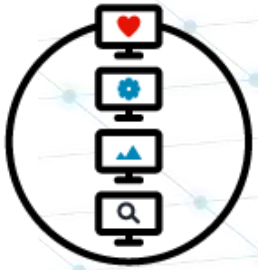
Zentrale Verteilung, SCCM, GPO etc.

Windows, Linux, Mac, Swift etc.

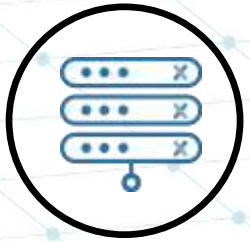
Fallen

SCADA, Netzwerkgeräte, VoIP, Drucker, POS, Geldautomaten, Kameras, Medizinprodukte etc.

Kein Risiko, dass Fallen als Ausgangspunkt genutzt werden
Keine Änderungen im Netzwerk erforderlich



FTP, SMB, SSH, HTTP, MS SQL, RDP, Broadcast



Leicht und hoch skalierbar, mehr als 500 Fallen pro Appliance

Golden Image und jede Anwendung

AWS, ESX, Hyper-V, KVM, ISO, Hardware, MSSP

TRAPX SECURITY

DeceptionGrid – sehr glaubwürdige Täuschung

TRAPX SECURITY

TRAP

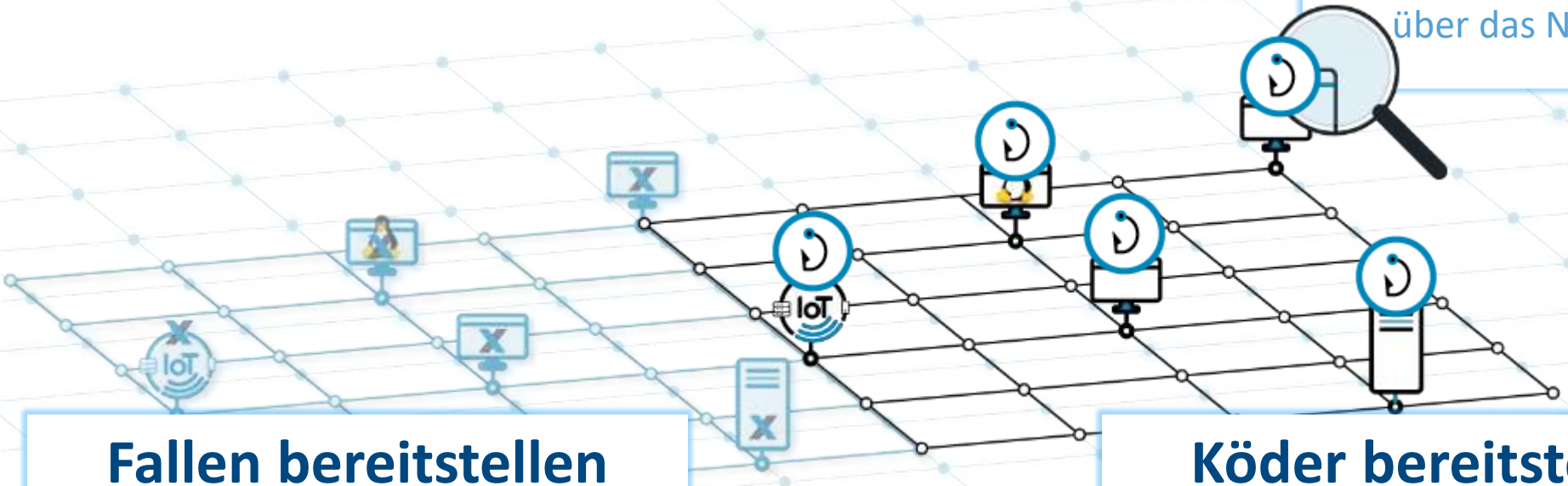
APPROVED PATENT APPROVED

Patent # US9516054 B2

Bereitstellung eines Schattennetzwerks innerhalb weniger Minuten

Entdecken

Automatische Sammlung von Informationen über das Netzwerk



Fallen bereitstellen

Automatische Bereitstellung von Fallen, die so getarnt sind, dass sie echten Assets entsprechen

Köder bereitstellen

Automatische Bereitstellung von Ködern, um Angreifer von echten Assets in die Falle zu locken

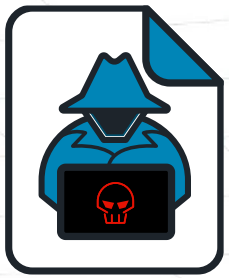
TRAPX SECURITY

Einleiten von Mitigierungsmaßnahmen

Einblick

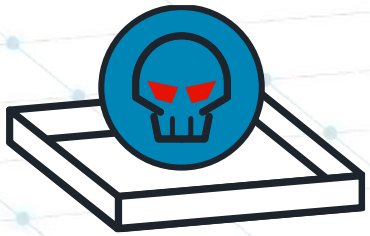
ArcSight An HP Company

splunk>



QRadar

Analyse



Mitigierung

ForeScout

portnox™
boundlessly smart

CISCO

TRAPX SECURITY

Bewährte Erkennung komplexer Angriffe

The New York Times

Web Defenders Detect Russian Hand in Iranians' Hacking Attempt

'Zombie Zero' Cyber-Attacks Hit Logistics, Robotic Firms for Months

eWeek - 21 Jul 2014

Zombie Zero is a suspected nation-state attack, which compromised at least eight companies beginning in May 2013, according to **TrapX's** ...

Iranian '**OilRig**' expands attacks, works with Russian hackers-for-hire

SC Magazine UK - 17 May 2017

Iranian '**OilRig**' expands attacks, works with Russian hackers-for-hire ... This hypothesis is countered by **TrapX** researchers, however, who ...

TrapX Labs Discovers New Medical Hijack Attacks Targeting Hospital Devices

MEDJACK 2 Report Reveals Attackers Are Disguising Sophisticated Attacks Within Old Malware Wrappers to Gain Entry to Hospital Networks and Steal Patient Data

SAN MATEO, CA (Marketwired - Jun 27, 2016) - TrapX™ Security, a global leader in deception-based cyber security, reported today that industry, leading to an influx of attacks against hospital networks that have successfully compromise medical devices, which are often vulnerable to attackers. TrapX today released the ttack - Medical Device Hijack 2" (MEDJACK 2). The report explains how attackers have evolved vices that use legacy operating systems that contain known vulnerabilities. By camouflaging old e able to successfully bypass traditional security mechanisms to gain entry into hospital networks

The WannaCrypt attack -- what we know and how to protect yourself

BetaNews - 15 May 2017

Infections by the **malware** known as WannaCrypt or WannaCry, began in ... co-founder and vice president of deception technology firm **TrapX** ...

Weitere Forschungsberichte finden sich unter: http://trapx.com/labs/

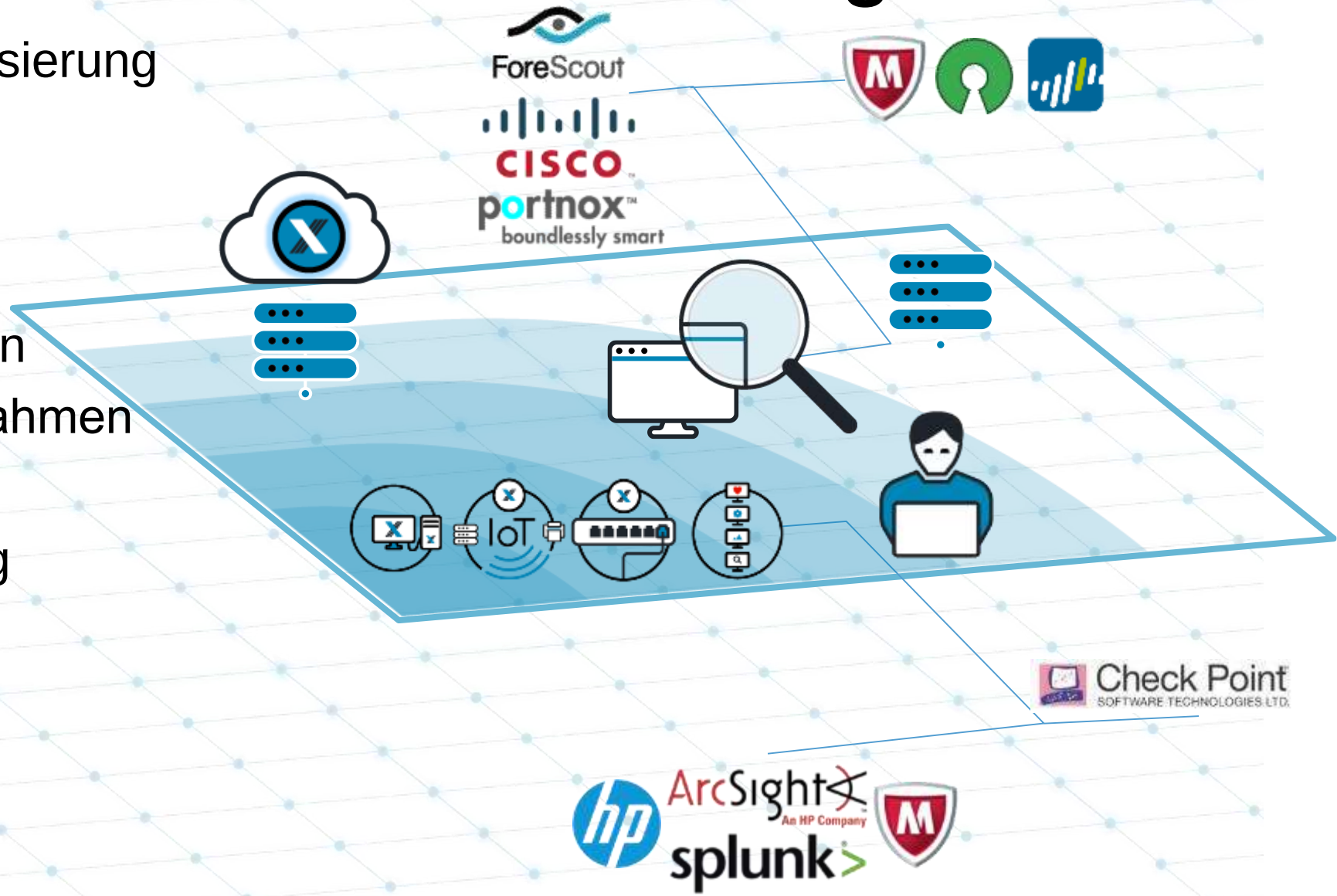
TrapX – Fallstudien

Demo

TRAPX SECURITY

TrapX – wesentliche Unterscheidungsmerkmale

- Weitgehende Automatisierung
- Skalierung
- Breite Abdeckung
  (On Premises/Cloud)
- Automatisches Einleiten
  von Mitigierungsmaßnahmen
- Signaturunabhängig
- Nachgewiesener Erfolg



TRAPX SECURITY

Weitere Schritte

„TrapX hat uns einen direkten Einblick in unsere Netzwerke ermöglicht, und wir mussten keine Änderungen an unserer Netzwerktopologie vornehmen.“
Tom August, CISO John Muir Health

„Als Finanzinstitut ist es unser oberstes Ziel, hinsichtlich IT-Sicherheitsbedrohungen immer auf dem Laufenden zu sein. TrapX DeceptionGrid hat uns Einblicke in die unberechtigte Ausbreitung von Angreifern im Netzwerk gewährt. Das und die Tatsache, dass sich dieses Tool sehr einfach implementieren und nahezu wartungsfrei betreiben lässt, hat uns dazu bewegt, TrapX DeceptionGrid für den Schutz unseres Netzwerks einzusetzen.“
Oren Zenescu, CISO Altshuler Shaham investment house

TRAPX SECURITY

Vielen Dank!

TRAPX
SECURITY