Educational Month
Cyber Security

Live Hacking: Die Methoden der Hacker und wie Sie sich gegen Ransomware Attacken schützen können

Presented by
Martin Mausner, Lukas Garlik und Emil Stahr

8. November 2023

Herzlich willkommen! Ihre Online-Session startet gleich.

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der Moderator bringt Ihre Fragen entsprechend ein.

Heute für Sie in der Online-Session:

Martin Mausner
Cyber Security Sales Specialist
Vodafone

Lukas Garlik
Security Consultant
Accenture

Emil Stahr
Security Consultant
Accenture

Agenda

01 Introduction

02 Live Hack

03 Ransomware

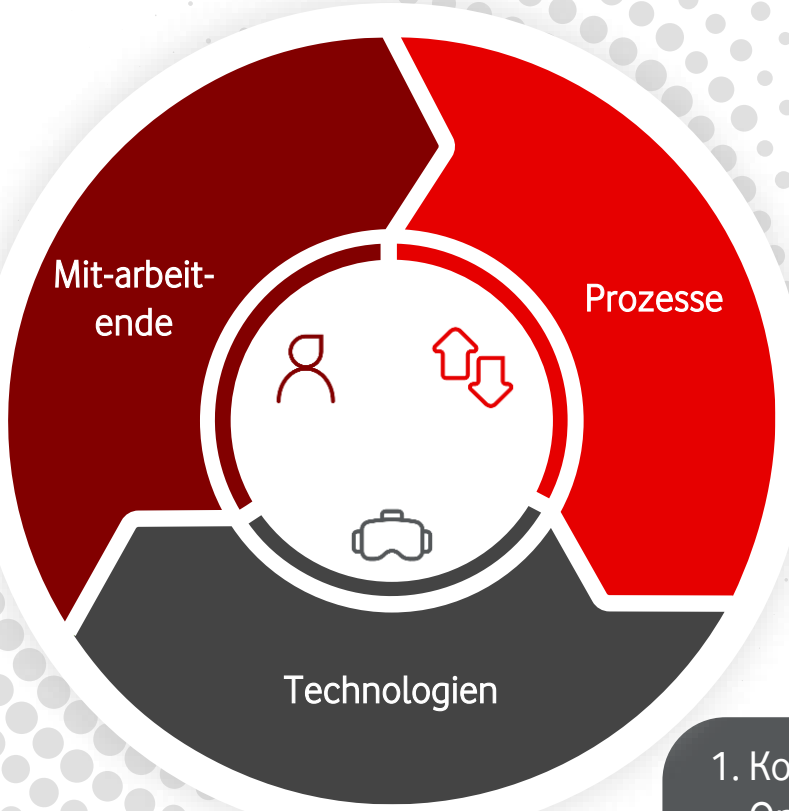
04 Detection & Response

Introduction

01

Kundenfeedback zeigt: Schwachstellen bei Mitarbeitenden, Prozessen und Technologien

1. Security Awareness
2. Security vs. User Experience
3. Rekrutierung und stetige Weiterbildung von Cyber Security Spezialisten



1. Risk Assessment
2. Lücken in Prozessen
3. Notfall Planung

1. Komplexe IT-Umgebung
   On-Prem / Cloud / Remote / IoT
2. Schwachstellen in Software
3. Ständig sich weiter entwickelnde Bedrohungslandschaft (RaaS / KI)

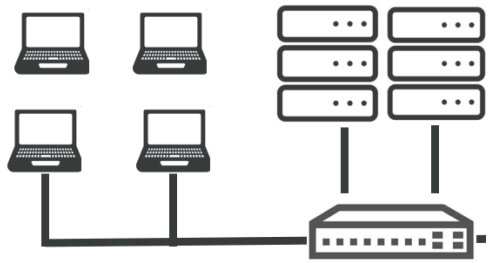
Komplexe IT-Umgebung

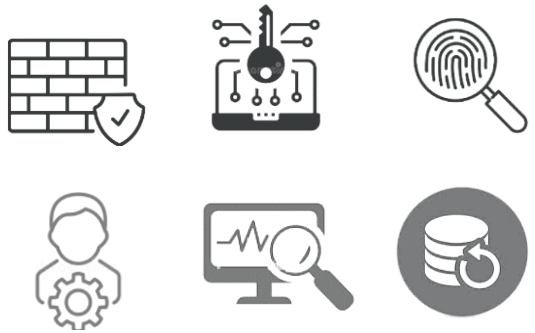
Basis beschaffen

Security selbst beschaffen und einrichten

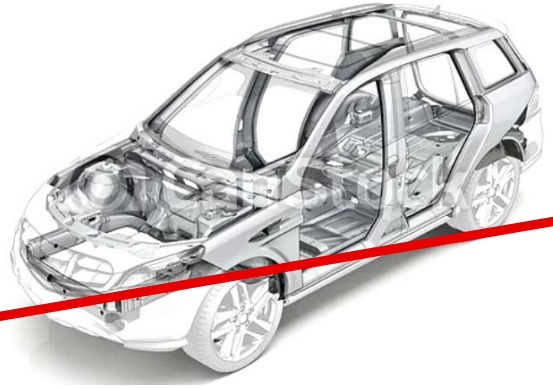
eigene Wartung

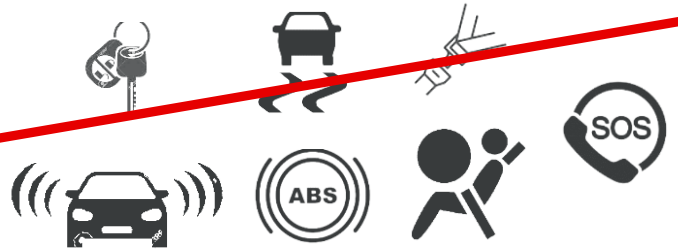
IT-Hersteller Ist-Situation





Bei einem Autohersteller undenkbar





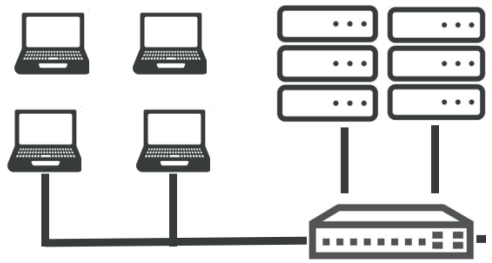
Komplexe IT-Umgebung

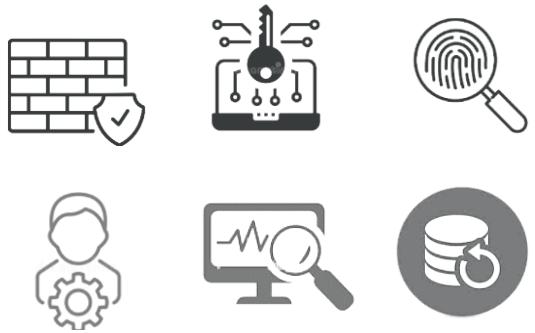
Basis beschaffen

Security selbst beschaffen und einrichten

eigene Wartung

IT-Hersteller
Ist-Situation





Komplett-System
Auto

Cyber Security gehört zu den 4 Top IT-Themen / TC(I)P

Transform

- XaaS
- Multi Cloud
- O/M 365
- UCC
- IoT / MEC

Endpoints jederzeit und überall

Connect

- Glass fiber
- 5G
- Company Net
- SD-WAN

Inform

Vodafone V-Hub

- IoT
- KI Chatbox
- SAP S/4 HANA Cloud
- Business Anwendungen z.B. Predictive Analytics

Protect

Sichern Sie die Zukunftsfähigkeit Ihres Unternehmens

Vodafone Security entlang des NIST Cyber Security Frameworks

Bewerten

Vulnerability Test
Auflistung von Schwachstellen

Penetration Test
Ausnutzen von Schwachstellen

Cyber Exposure Diagnose
Betrachtung des Netzwerks und der Endgeräte

Entdecken

Managed Detection and Response

SIEM - Security Incident und Event Management

SOC - Security Operation Center

Erfassung und Analyse von Vorfällen

Frühwarnsystem vor Schäden

Schützen

Phishing Awareness Workshop

Managed Firewall

Zero Trust Zugang zu Applikationen

DDoS Mitigation

Mobile Device Security

Reagieren

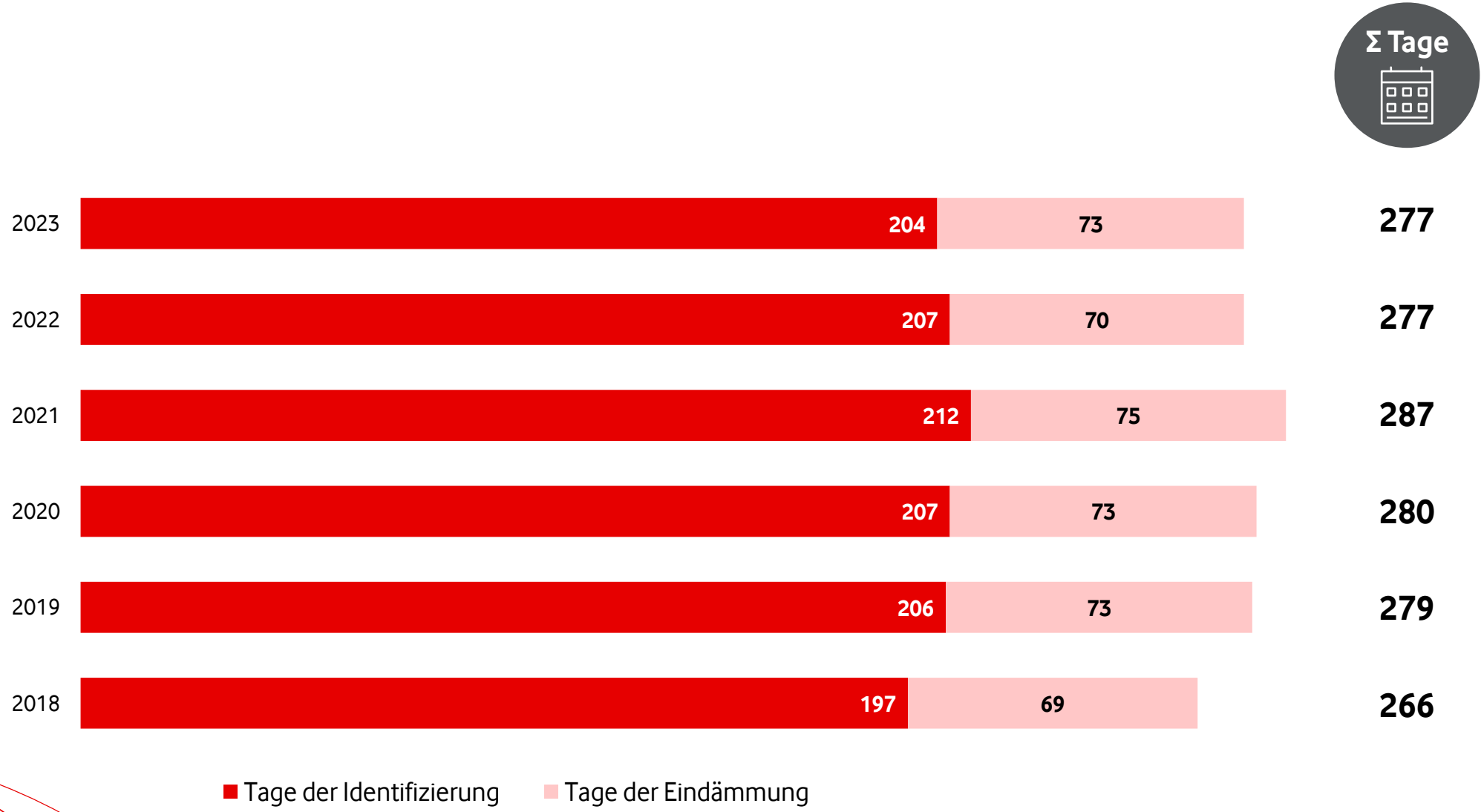
Breach Response and Forensics

Schnelles Eingreifen bei einem Vorfall

Analyse des Vorfalls

Datenrettung

Bis zu 277 Tage dauertes es 2023 eine Cyber Attacke zu erkennen und einzudämmen



Quelle: IBM "The cost of a data breach 2023"

Live Hack

02

Die Hauptcharaktere

Paul Schneider

- Arbeitet in der HR-Abteilung eines KMU
- Zu seinen Aufgaben gehören die Personalbesetzung, die Beantwortung von Anträgen, die Verwaltung der Gehaltsabrechnung usw.
- Er hat keine ausgeprägten technischen Kenntnisse

Killnet

- Hacker-Gruppe
- Ihre Ziele sind kleine und mittelgroße Unternehmen
- Sie suchen nach vertraulichen Daten und erpressen ihre Opfer mit den erbeuteten Informationen

Aus der Perspektive eines Hackers ...

Was will der Hacker?

- Er will das Opfer dazu bringen, seinen Code auszuführen

Wie schafft er es trotzdem?

- Er erstellt eine Phishing-E-Mail, die auf sein Opfer zugeschnitten ist
- Er bettet schadhaften Code in ein Dokument ein. Beim Öffnen wird der Code ausgeführt und stellt eine Verbindung zum Hacker her.

Warum ist das nicht so einfach?

- Technische Beschränkungen (Firewalls, Endpoint protection, SEGs etc.)
- Sensibilisierung des Opfers für die Risiken

Was ist für ihn drin?

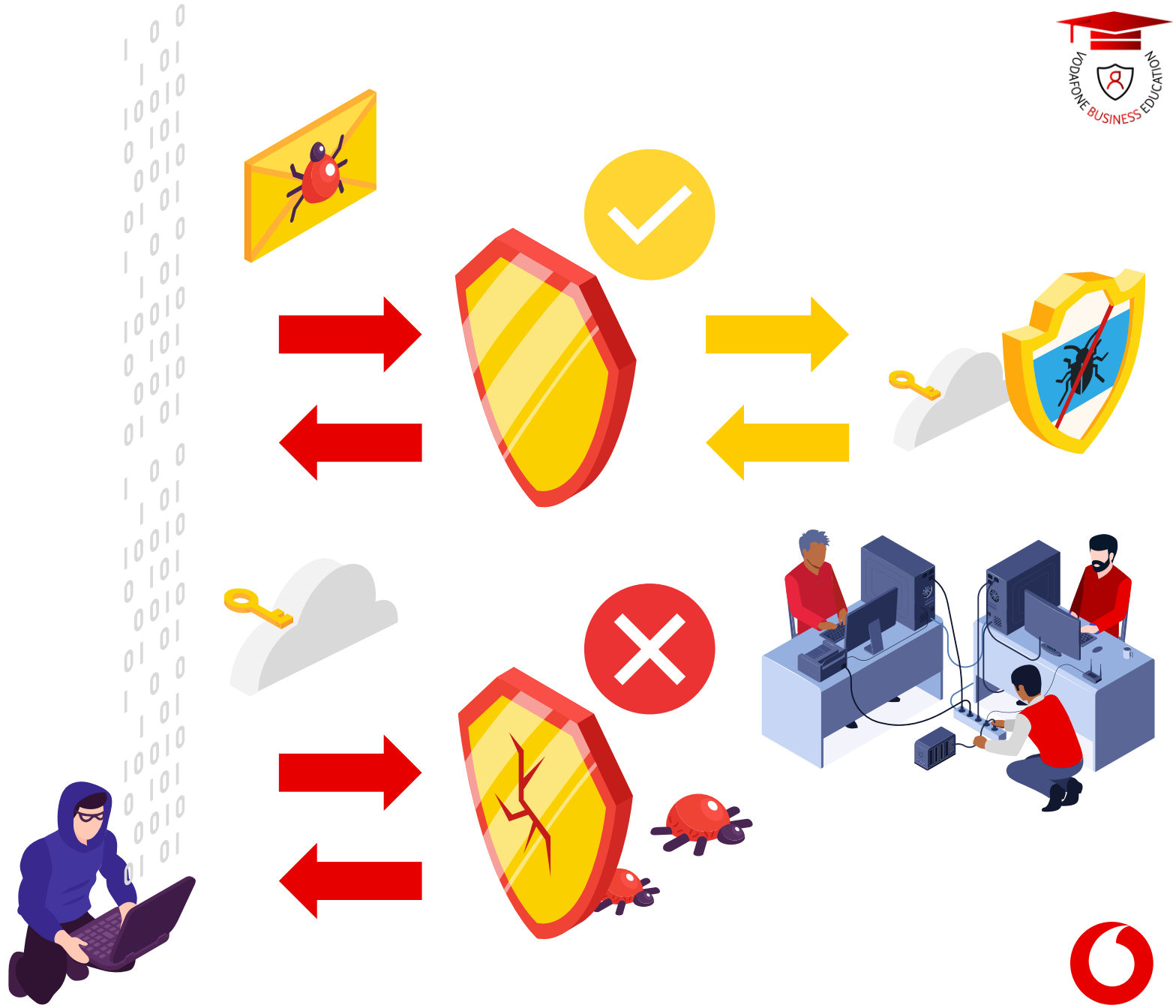
- Diebstahl vertraulicher Daten
- Credentials sammeln
- Manipulation der IT-Infrastruktur
- Weitere Zielgeräte infizieren

Aus der Perspektive eines Hackers ...

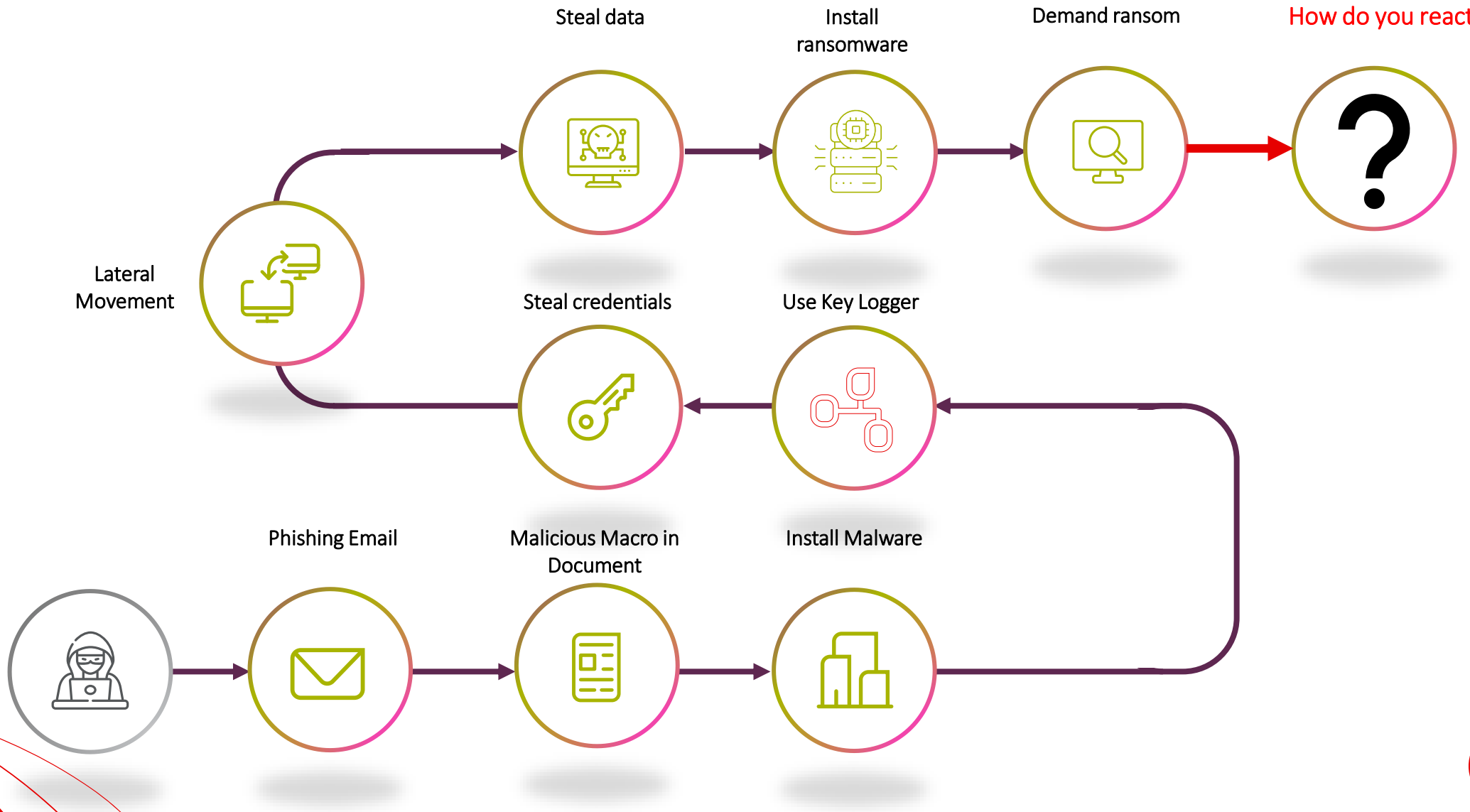
Die Firewall blockiert den gesamten eingehenden Datenverkehr.

Er stellt eine umgekehrte Verbindung her, indem er ein bösartiges Dokument per E-Mail an einen Mitarbeiter schickt.

Nachdem die erste Verbindung hergestellt ist, beginnt er mit der Suche nach vertraulichen Daten.



Die Art und Weise, wie Angreifer Ihre Daten verschlüsseln und stehlen



Ransomware

03

Ergebnis einer Ransomware Attacke

Ransomware ist eine wachsende Bedrohung

84%

der Unternehmen beobachten im Vergleich zu 2022 einen **Anstieg der Bedrohungslage**

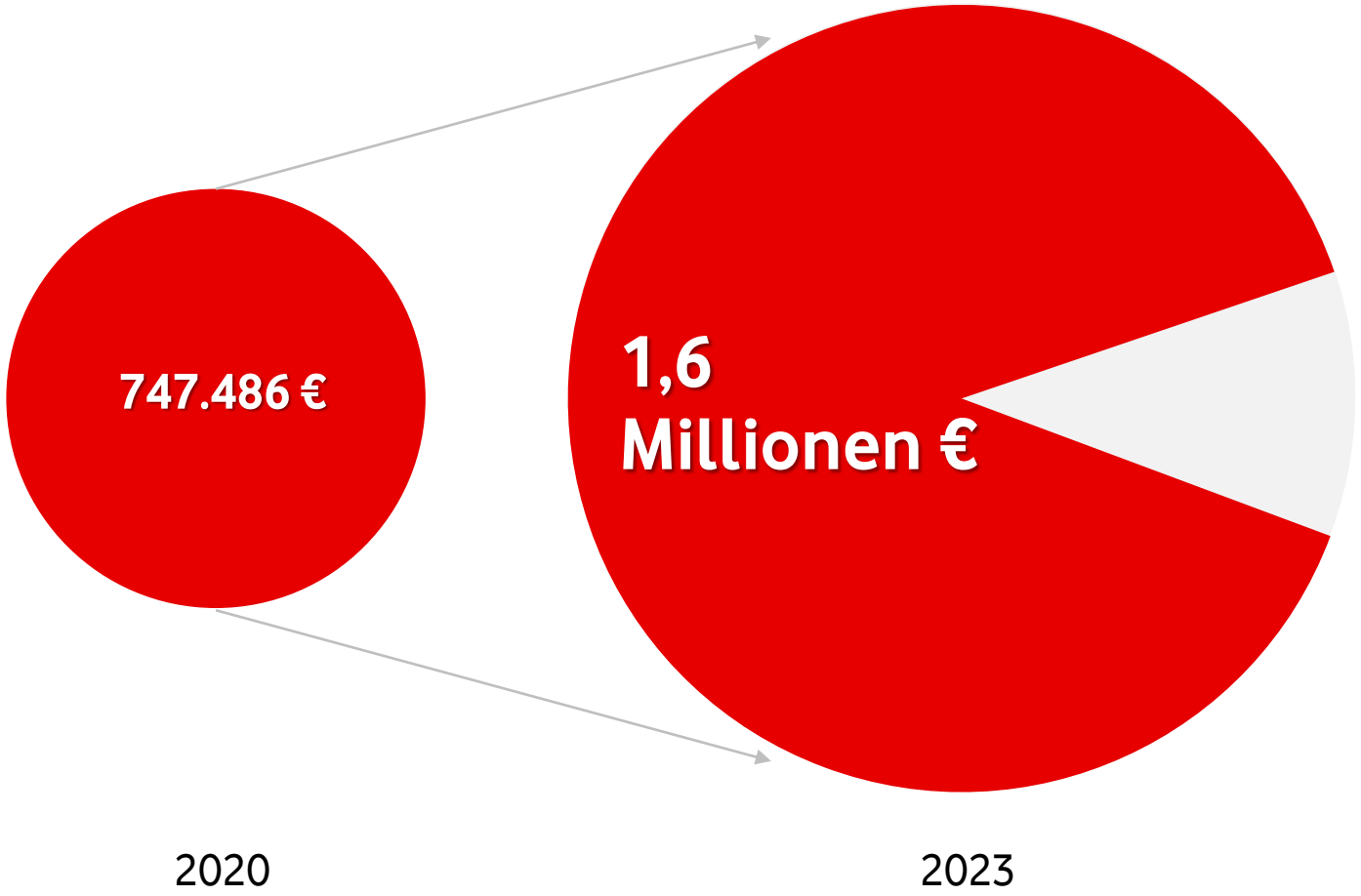
35%

des Angriffsvolumens sind Ransomware- und Erpressungsvorfälle

203

Milliarden EUR Schaden pro Jahr durch Angriffe auf deutsche Unternehmen

Cyber.Crime.Cash.
Lösegeld-Zahlung nur Bruchteil der Kosten



Quellen: Sophos - The State of Ransomware 2021; Coverware 2023

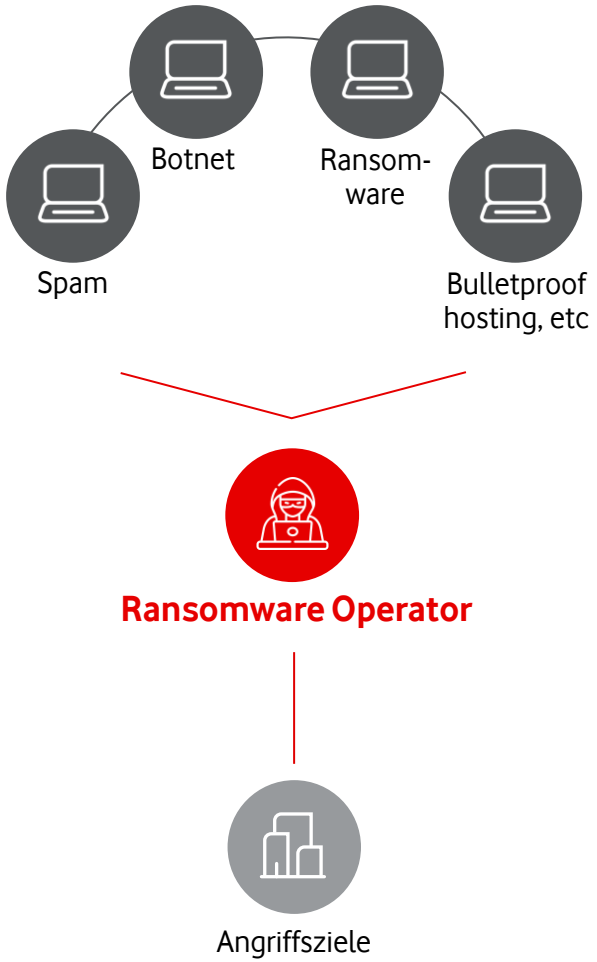
VODAFONE BUSINESS EDUCATION

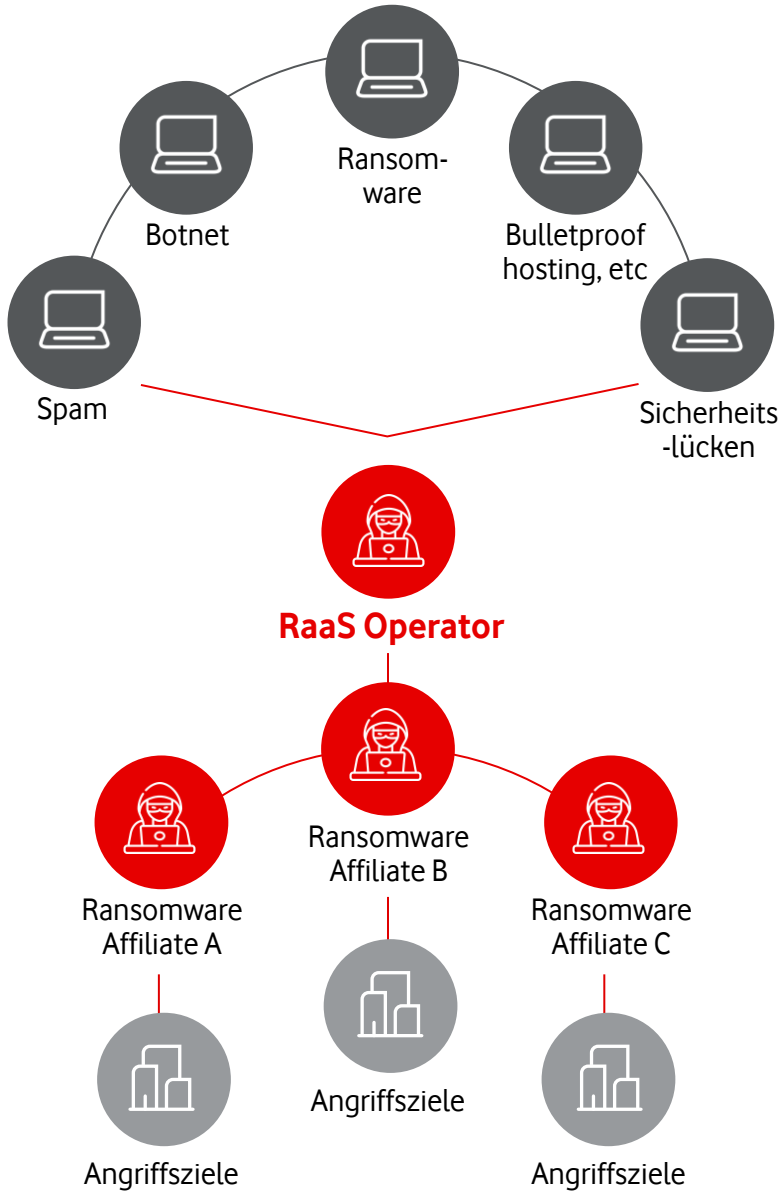
361.000 €

Durchschnittliche Lösegeld-Summe

- Die Kosten der Wiederherstellung des operativen Betriebs sind um den **Faktor 4,4 höher** als die Lösegeld-Summe
- Betriebsunterbrechung und Wiederherstellungskosten sind die Hauptkostentreiber nach einer Ransomware-Attacke
- **Downtime**: durchschnittlich **21 Tage**

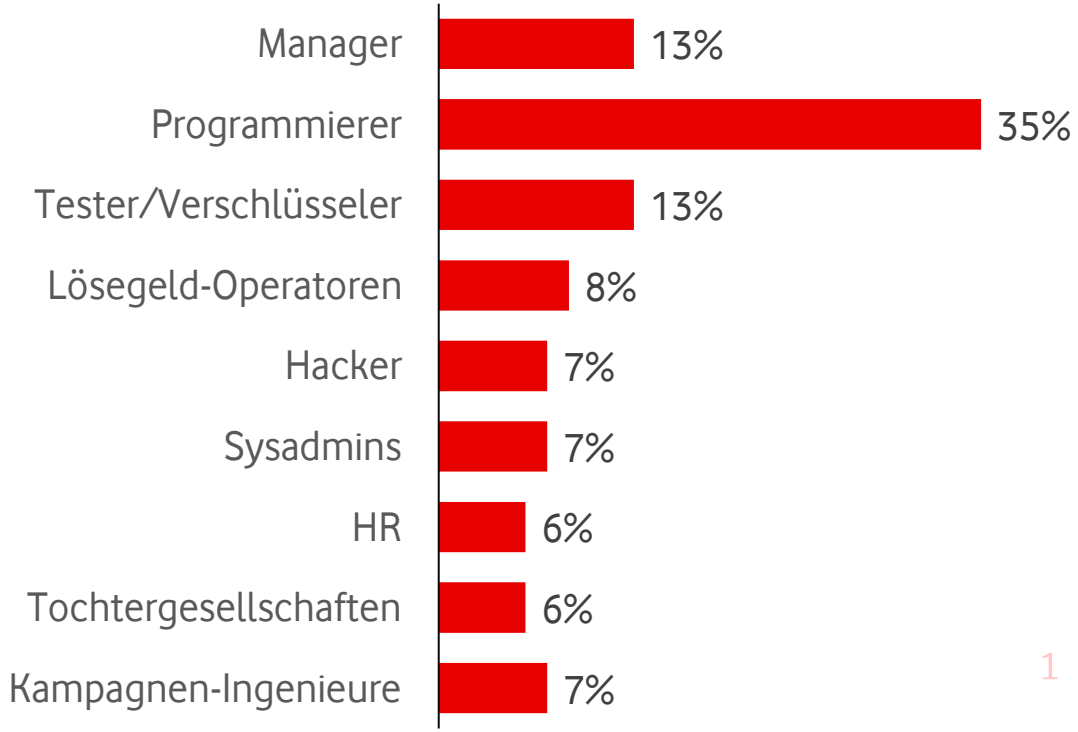
Ransomware as a Service – RaaS





Die Angreifer sind oft Teil großer organisierter Verbrecherbanden

Mitglieder von Cyber-Gangs nach Berufsgruppen[1]



Quelle: atlasVPN (2022) “Role Structure Conti Cybercrime Group”

Im Inneren der Hackergruppen

- Professionelle kriminelle Organisationen ähneln von ihrer Struktur her großen Unternehmen
- Einige große Hackergruppen bilden Kartelle zum Austausch von Daten und "bewährten Verfahren", z. B. Wizard Spider, Twisted Spider, Viking Spider und LockBit
- Hacker bieten "Kundendienst"-Chatrooms an
- Hacker-Websites haben FAQs, in denen z. B. erklärt wird, wie man Krypto-Wallets einrichtet

Detection & Response

04

Detection ist ein entscheidender Aspekt der Cybersicherheit

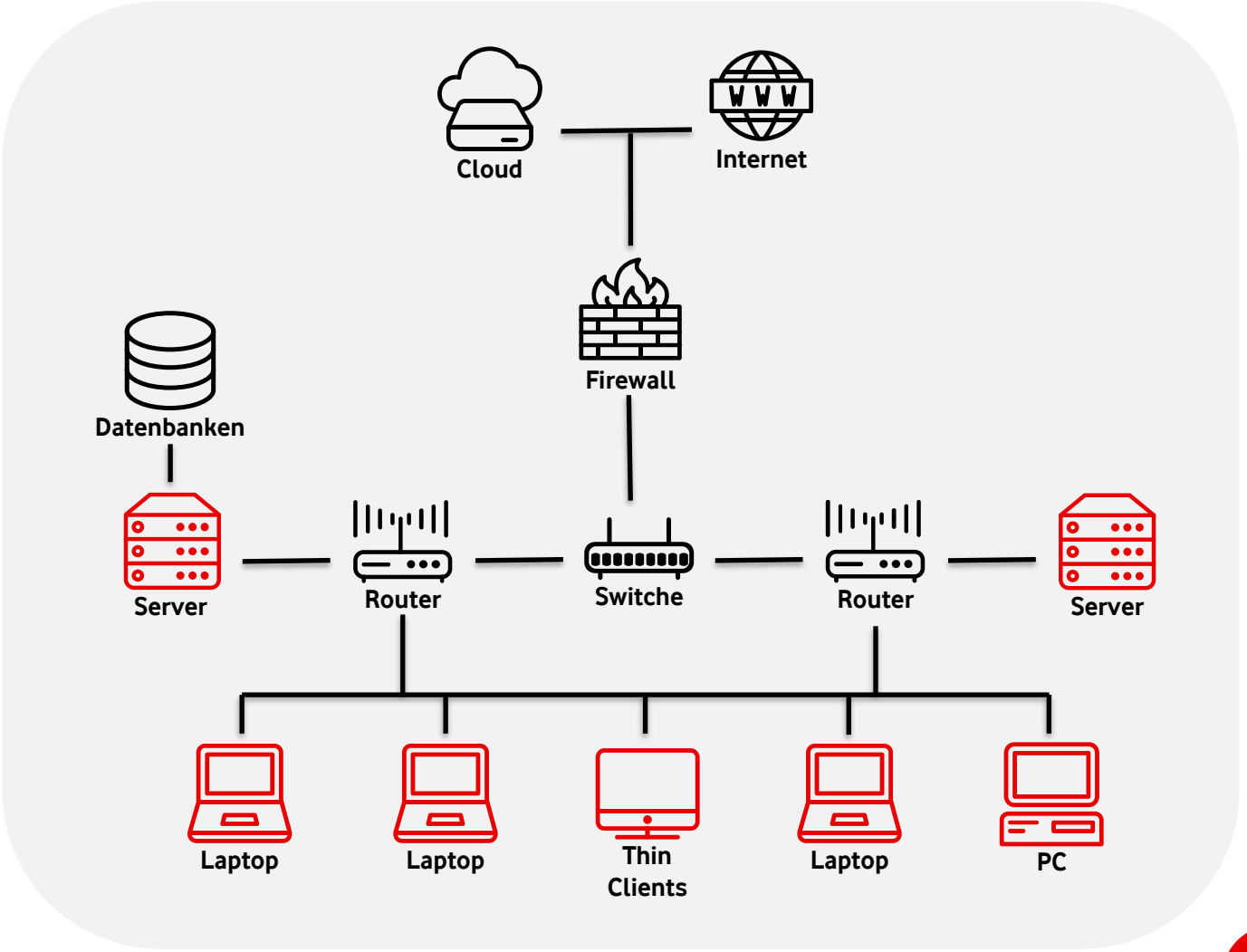
1. Früherkennung von Angriffen
2. Minimierung von Schäden
3. Verbesserung der Reaktionsfähigkeit
4. Abwehr fortschrittlicher Bedrohungen

Zunehmende Komplexität durch unterschiedliche Konzepte von „Detection & Response“

Endpoint Detection & Response

Fokus auf Endpunkte und Hosts

- Kontinuierliche proaktive Überwachung der Endpunkte
- Schutz des Endpoint-/Access-Bereichs vor Infiltration, Monitoring & Mitigation, Bewertung von Vulnerabilität, Alerting & Response
- Hoher Ressourcenbedarf auch durch Analyse von Fehlalarmen
- Stand Alone Sicherheitslösung

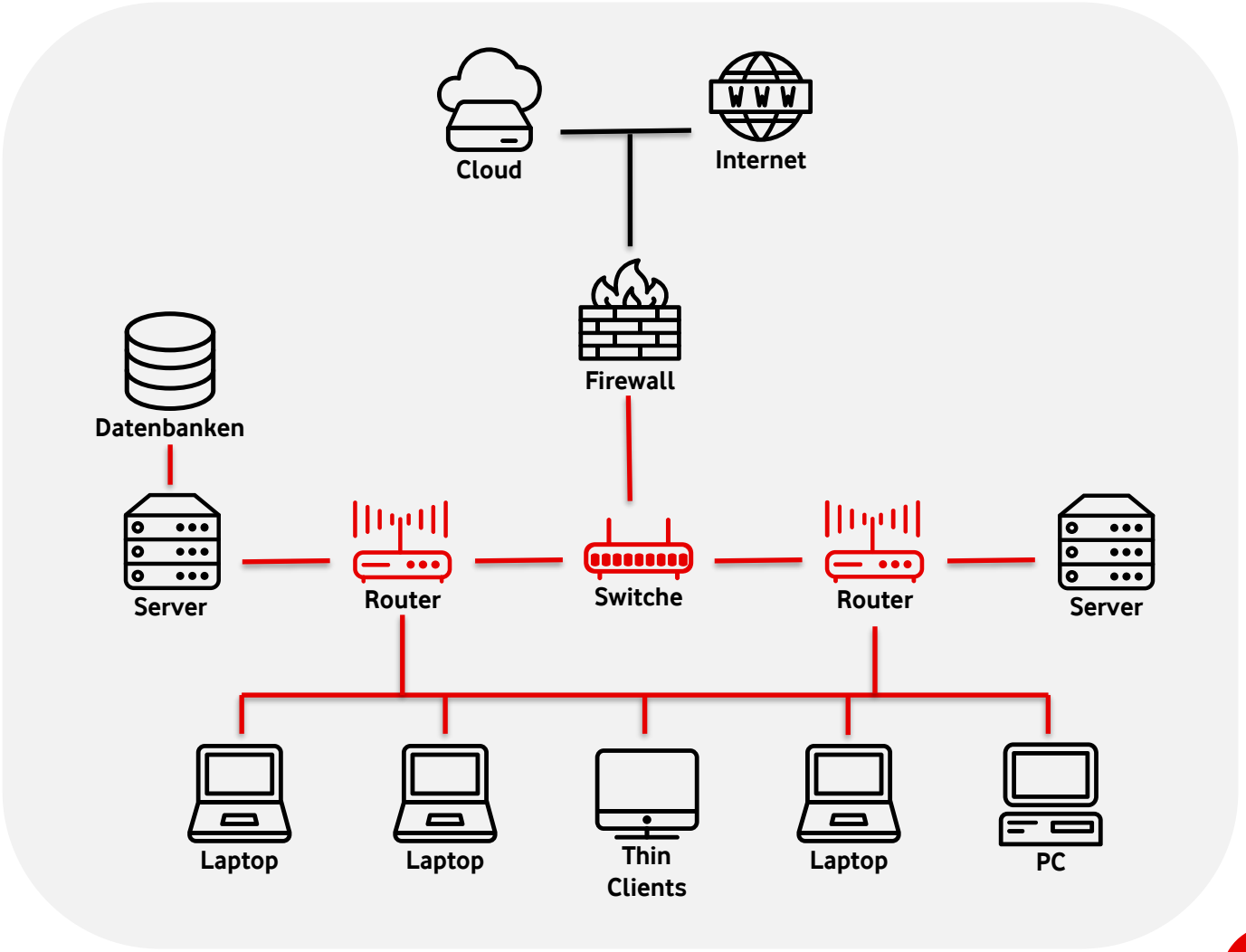


Zunehmende Komplexität durch unterschiedliche Konzepte von „Detection & Response“

Network Detection & Response

Netzwerk und Inter-Device Traffic in Scope

- Kontinuierliche Analyse des Netzwerkdatenverkehr
- Sichtbarkeit/Tranzparenz des Netzwerk-Traffics, Detektion bekannter und unbekannter Threats sowie Lateral Movements, Alerting & Response
- Hoher Ressourcenbedarf bei Implementierung und Betrieb
- Stand Alone Sicherheitslösung

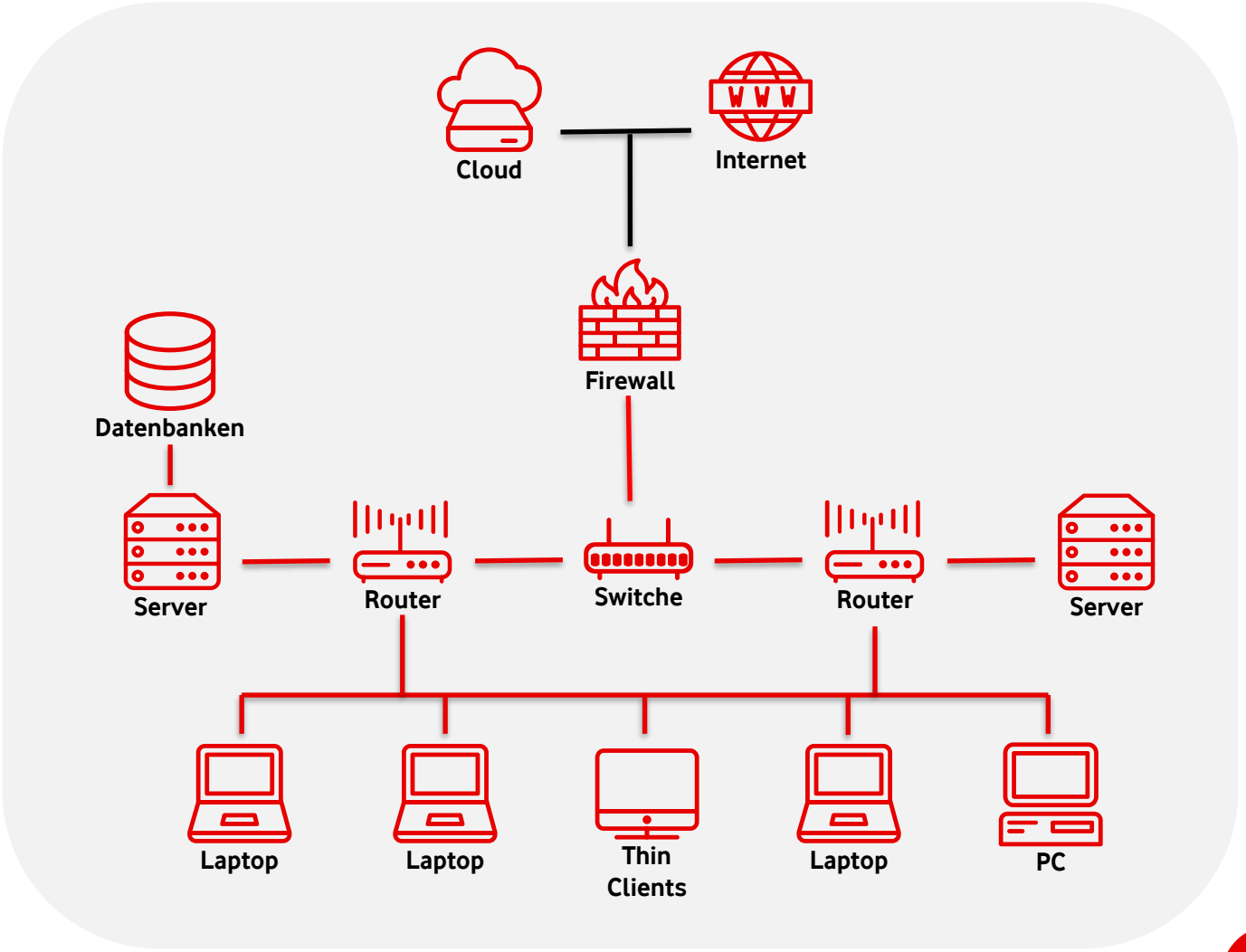


Zunehmende Komplexität durch unterschiedliche Konzepte von „Detection & Response“

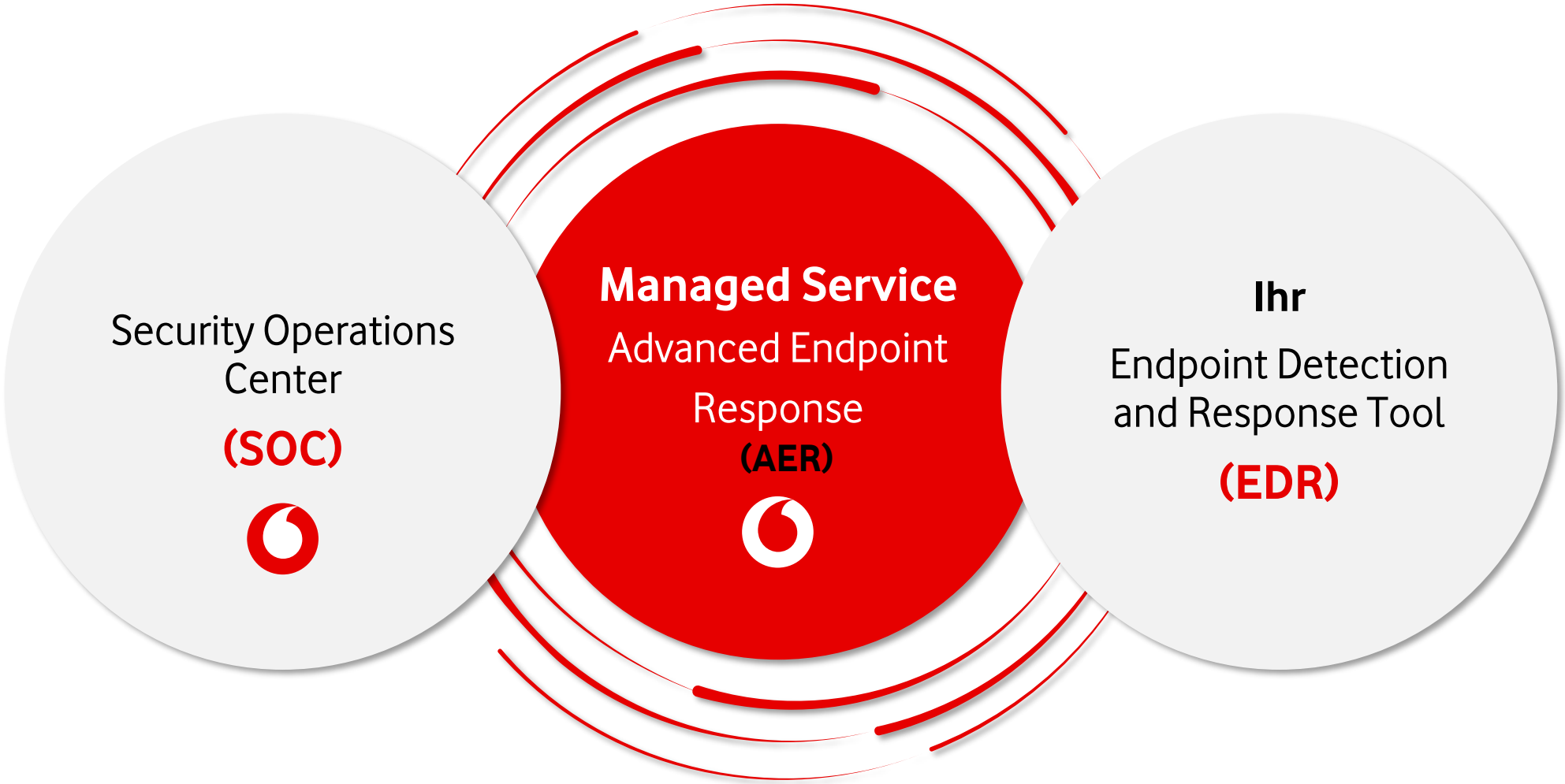
eXtended Detection & Response

Endpunkte, Server, Firewalls, UTM, Anwendungen etc.

- Erhöht Sichtbarkeit, Transparenz und Kontext auf mehreren Sicherheitsebenen
- XDR erfasst und korreliert Daten über E-Mails, Endpunkte, Server, Cloud-Workloads und Netzwerke hinweg
- Überwachung und Analyse der Alarme kostet viel Zeit
- Ganzheitliches Monitoring & Mitigation von Angriffsbedrohungen



Im Zusammenspiel mit Ihrem Endpoint Detection and Response Tool rundet das AER Ihre Security Strategie ab



Über das AER werden vorher definierte Reaktionen ausgelöst

Endpoint

Server

Log-Sammlung Plattform

Analyse-Engines und Module

Wandelt Protokolldaten in Sicherheitsvorfälle um

Start

Bekannte IOC/IOA/TTP

Korrelierte Vorfälle, die an das SOC-Analystenteam <gesendet werden

01

Investigation

SOC-Analyst untersucht verdächtige Aktivitäten und sammelt kritische forensische Daten

02

Response

SOC-Analyst führt vorautorisierte Behebung durch

03

Notification

Kunden werden per Portal und E-Mail benachrichtigt

Threat hunting

Analyst führt Bedrohungsjagd auf neue IOCs, IOAs & TTPs durch

Durchführen von Behebungen/Isolierungen über das kundeneigene EDR-Tool

Microsoft Defender for Endpoint

CROWDSTRIKE

CORTEX XDR

vmware Carbon Black

SentinelOne

Emergency Response

Fragen beantworten die Incident Response-Expert:innen

Wir managen aktiv die Bedrohungslage für Sie – mit Advanced Endpoint Response (AER)

Überflutung mit Warnungen

Fokus auf relevante Warnungen

- Überwachung und Untersuchung durch Sicherheitsexpert:innen
- Transparenz über Hunderte von Sicherheitstools und Protokollquellen: vor Ort, in der Cloud, hybrid ...
- Big-Data-Analyse und hochmoderne Korrelation von Bedrohungsinformationen

Kompetenz- und Ressourcenlücken

Globales Team erfahrener Sicherheitsexpert:innen

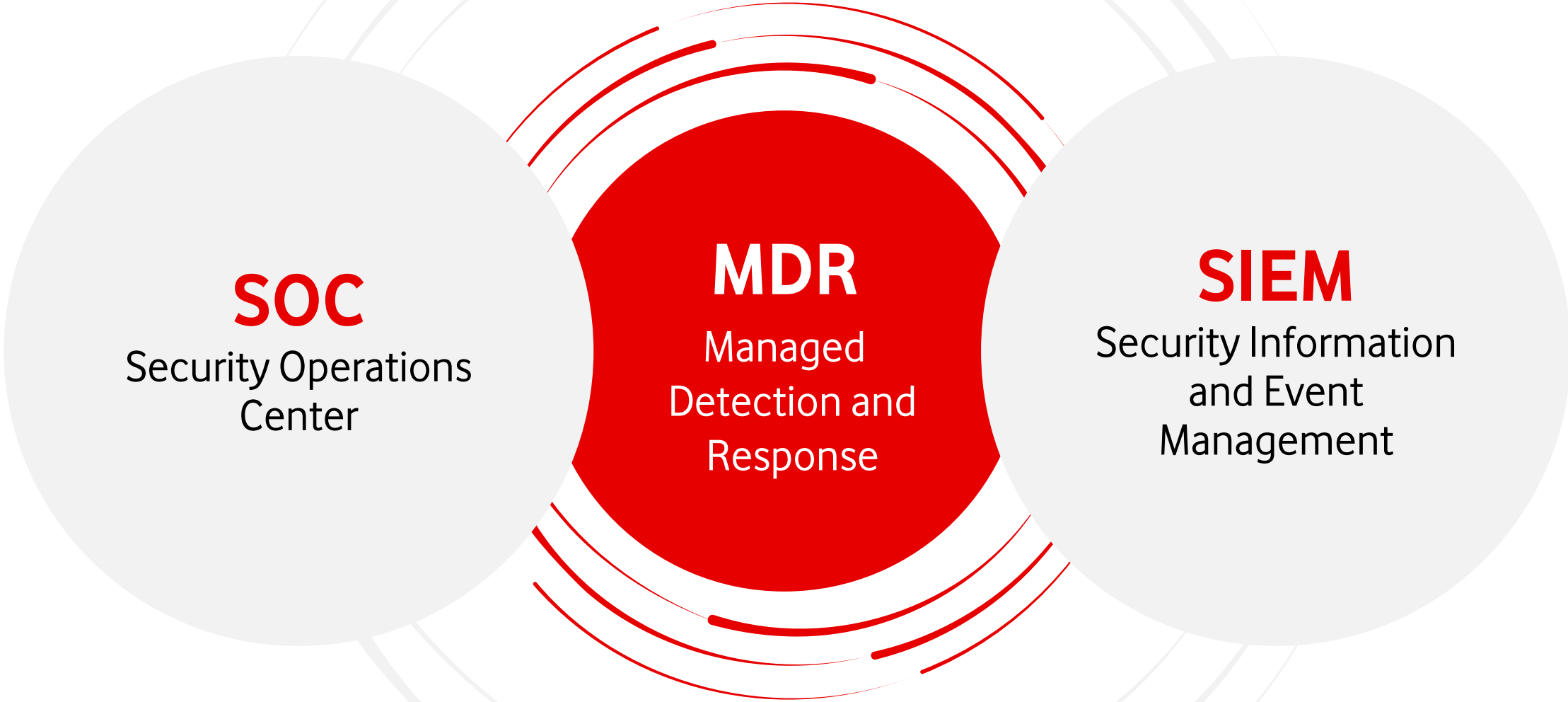
- Zugang zu zertifizierten, geschulten Expert:innen – 24/7 rund um die Uhr
- Engagiertes SOC-Team in Malaga
- Erweiterung Ihres Teams
- Verwaltete Bedrohungssuche, -untersuchung und -behebung
- Branchen- und kundenorientierte Sicherheitsexpert:innen

Dynamische Bedrohungslage

Reagieren auf Änderungen und die ständig neue Bedrohungslage

- Integrierte globale Bedrohungsinformationen
- Korrelation von Big-Data-Analysen
- Proaktive Bedrohungssuche
- Bewährte Cyber-Abwehrtechniken
- Regelmäßige Besprechungen und Berichte über neue Bedrohungen

Security Monitoring als Managed Service



MDR mit Vodafone und Accenture

Der MDR-Service ist ein Managed Service, der mittels führenden Analysen und hochqualifizierten Analysten proaktiv Cyberangriffe aufspürt, vermeidet oder eindämmt, bevor sie wesentliche Auswirkungen auf das Geschäft haben.

Datenanalyse

24/7 Alert Monitoring

Hochqualifizierte Analysten (SOC)

Individuell anpassbarer Service

Erkennung von Anomalien

Der Lebenszyklus eines Sicherheitsvorfalls

Identifizierung

Erkennen und Analysieren der Protokolle, um einen Incident zu erstellen (unterstützt von der Plattform und den Analysten)

Validierung

MxDR-Analysten validieren Vorfälle mit einer Falsch-Positiv-Rate von <1 %

Klassifikation & Impact Assessment

MxDR klassifiziert den Angriff (MITRE ATT&CK Framework) und bewertet die Auswirkungen auf den Kunden

Benachrichtigung

Der Kunde wird per E-Mail und Telefonanruf über den Vorfall informiert

Response & Recovery

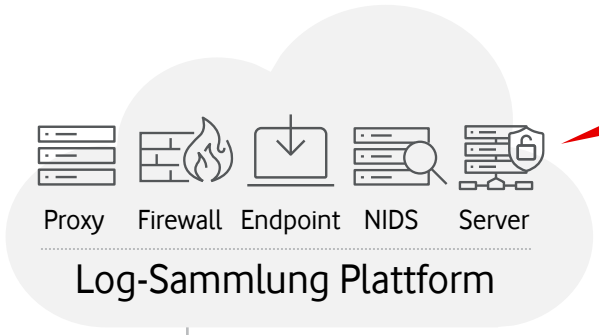
MxDR initiiert Incident-Response-Aktivitäten auf den Endpunkten... Bis zur Quarantäne gemäß Playbooks

Der Client initiiert Nicht-Endpunkt-Reaktionen

Closure

Ursachenüberprüfung zur Beseitigung durch den Kunden mit Empfehlungen des MxDR Senior Analyst

MxDR Service für Sie – vom Logfile bis zur Benachrichtigung



Schritt 1: Log-Sammlung und Transport

Schritt 2: Analyse und Sicherheits-überwachung

Schritt 3: Analyse von Sicherheitsereignissen und Antwort

Schritt 4: Präsentation von Sicherheitsereignissen

Analytics Tier

Analyst Response Console

MDR PORTAL

Analyse-Engines und Module

Wandelt Protokolldaten in Sicherheitsvorfälle um

- Intelligence
- Geschäftskontext
- Maschinelles Lernen
- Customer rules

Behandlung von Sicherheitsvorfällen

Analyse-Team

Validieren, klassifizieren, priorisieren, eskalieren

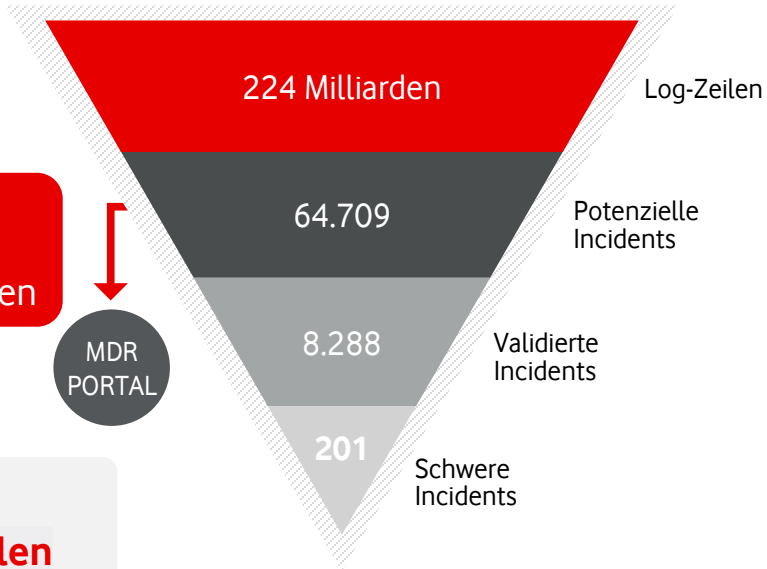
- Sicherheitsanalytik
- DeepSight
- GIN-Analyse-Tool
- Reaktion auf den Endpunkten (AER)

Meldung von Sicherheitsvorfällen

- Notfall
- Kritisch
- Warnung
- Informativ
- Tägliche Übersicht

- Vollständiger Log-Abruf
- DeepSight
- Reports

Progressives Bedrohungs-modell



IHRE FRAGEN.

Vielen Dank für Ihre Teilnahme!

Bei Fragen
melden Sie sich gern
bei Ihrem:r Vodafone-
Ansprechpartner:in.

Sie sind neu bei uns?
Schreiben Sie uns an
online.sessions@vodafone.com
eine E-Mail.

Weitere Online-Sessions
aus unserem Educational
Month Cyber Security
finden Sie hier.

TIMETABLE 2023

VODAFONE BUSINESS EDUCATION

Cyber Security Educational Month

KW 42

17.10. | 10:00 **Cyber Security**
Jessica Schäfer (Accenture)
Martin Mausner (Vodafone)

18.10. | 10:00 **Cyberversicherungen**
Sönke Glanz (HDI Versicherung)
Matthias Magnus (Vodafone)

19.10. | 10:00 **Deepfakes**
Dominik Wojcik

KW 43

23.10. | 14:00 **Schutz vor Cyberkriminalität**
Sarah Elßer (Tech Well Told)
Alexander Pessler (Tech Well Told)
Patrick Sulewski (Vodafone)

KW 45

06.11. | 10:00 **KRITIS & NIS 2.0**
Robert Steffen (Vodafone)
Matthias Magnus (Vodafone)

08.11. | 10:00 **Live Hacking**
Lukas Garlik (Accenture) | Emil Stahr (Accenture)
Martin Mausner (Vodafone)

10.11. | 10:00 **Gehacktes Unternehmen**
Stefan Würtemberger (Marabu) | Carsten Wallmann (Vodafone)
Matthias Magnus (Vodafone)

KW 46

16.11. | 10:00 **Cyber-Angriffe abwehren**
Franz Finke (Lookout) | Jasin Mehovic (Lookout)
Mario Bohum (Vodafone)


Together we can
vodafone
business