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/die Moderator:in bringt Ihre Fragen entsprechend ein.

Session wird aufgezeichnet

Educational Month |

Cyber Security

Online-Session

Live Hacking:

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

25.09.2024

Herzlich willkommen!

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/die Moderator:in bringt Ihre Fragen entsprechend ein.

Session wird aufgezeichnet

Heute für Sie in der Online-Session:

Lukas Garlik
Security Manager
Accenture

Emil Stahr
Security Consultant
Accenture

Agenda

01 Introduction

02 Live Hack

03 Ransomware

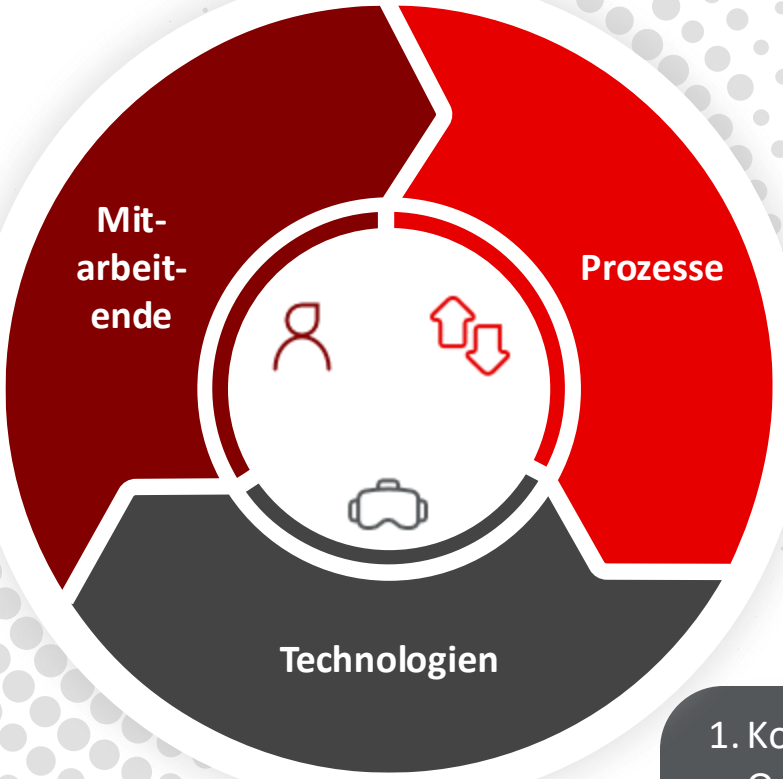
04 Detection & Response

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)

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 um 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

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?

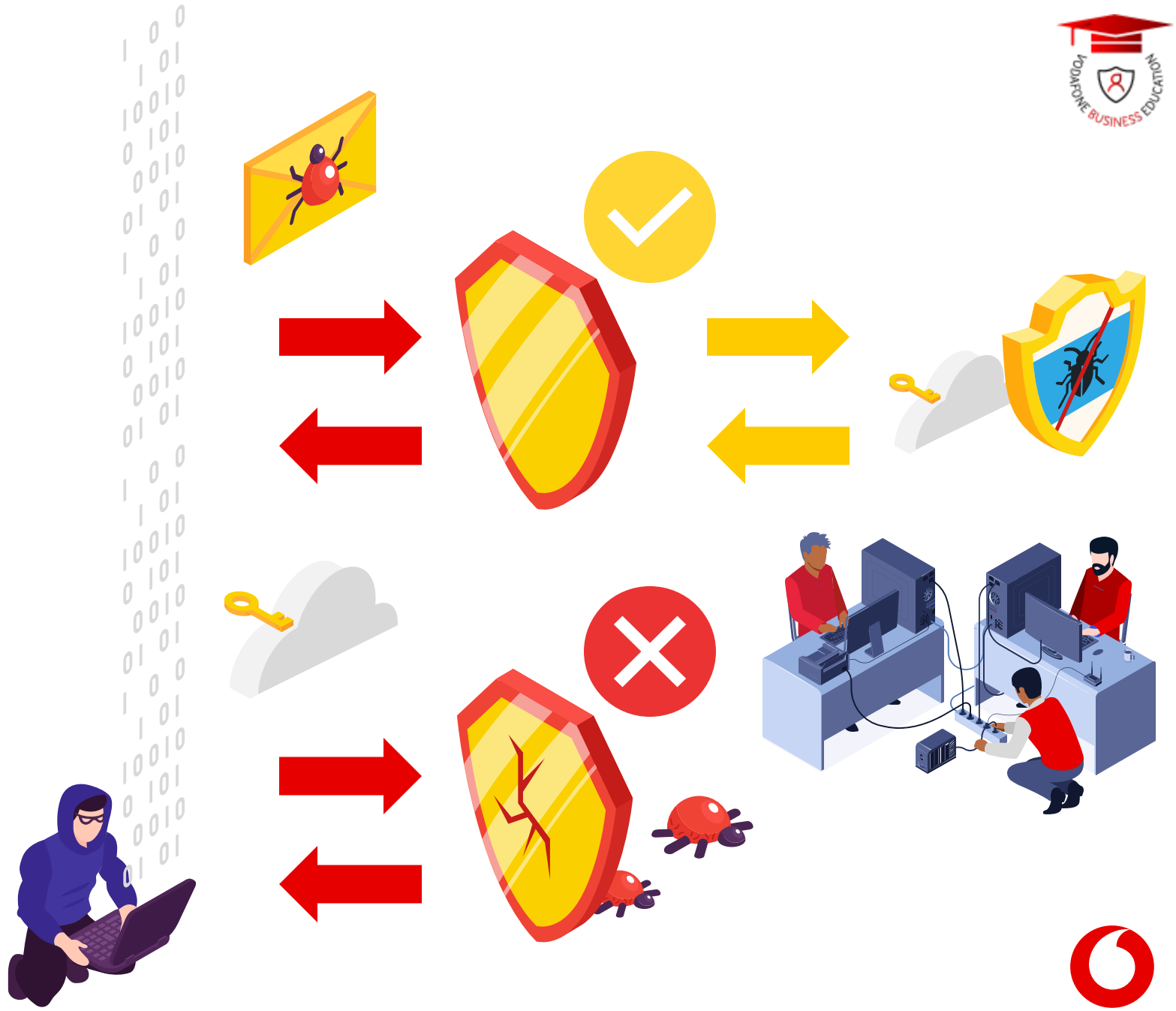
- Diebstahl vertraulicher Daten
- Credentials sammeln
- Manipulation der IT-Infrastruktur
- Weitere Zielgeräte infizieren

Aus der Perspektive eines Hackers ...

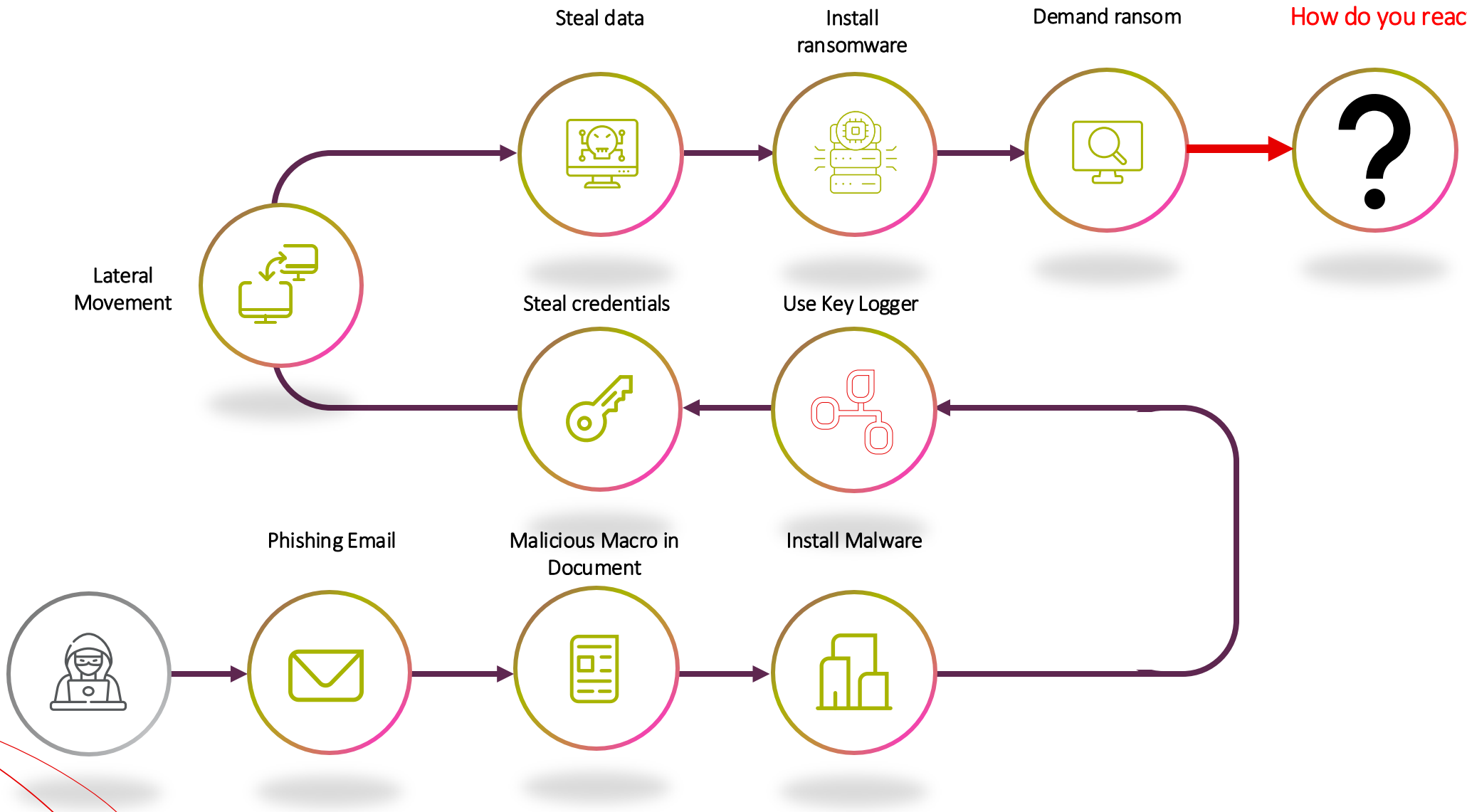
Die Firewall blockiert den gesamten eingehenden Datenverkehr.

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

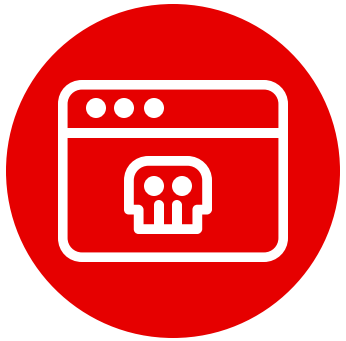
03

Ergebnis einer Ransomware Attacke

Ransomware ist eine wachsende Bedrohung

59 %

der Unternehmen waren 2024 von Ransomware betroffen:



76 %

sind die Angriffe mit Ransomware seit der Einführung von ChatGPT gestiegen.

49%

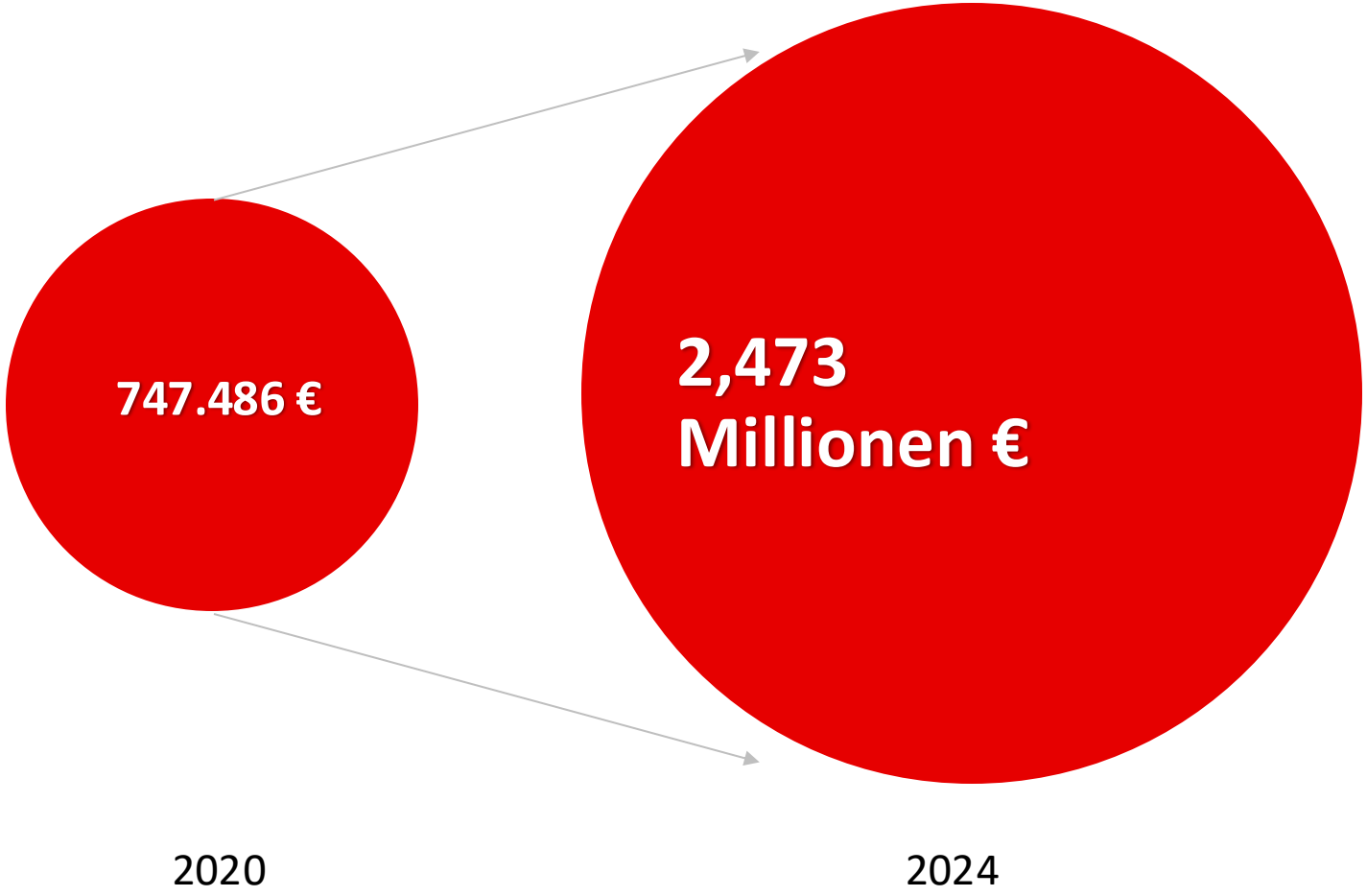
der Computer eines Unternehmens waren bei Ransomware Angriffen im Durchschnitt verschlüsselt.

5 x

mehr Lösegeld wurde durchschnittlich pro Ransomware Angriff gezahlt im Vergleich zu 2023.

Quellen: Sophos – Ransomware-Report 2024; https://www.csoonline.com/de/a/5-tipps-fuer-mehr-sicherheit-im-ki-zeitalter,3693467

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



Quellen: Sophos – Ransomware-Report 2024

1.800.000 €

Durchschnittliche Lösegeld-Summe

- Die Kosten der Wiederherstellung des operativen Betriebs sind um den **Faktor 1,4 höher** als die Lösegeld-Summe
- Betriebsunterbrechung und Wiederherstellungskosten sind die Hauptkostentreiber nach einer Ransomware-Attacke
- **Downtime**: durchschnittlich **21 Tage**

Generative künstliche Intelligenz wird genutzt um die Angriffsvektoren zu optimieren

Erweiterung und Optimierung durch GenAI

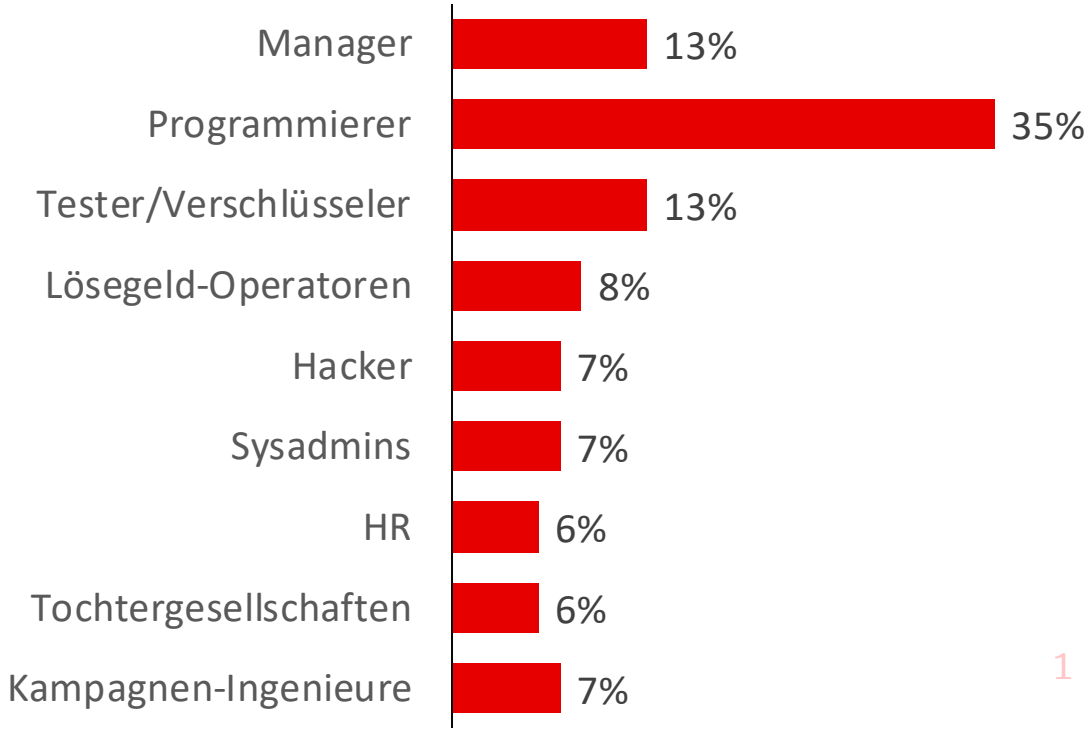
- Passwörter schneller zu knacken
- Personalisierte Phishing-Kampagnen die kaum zu erkennen sind
- Polymorphe Malware einfach zu entwickeln
- Gezielt Desinformation zu verbreiten

Neue Angriffsvektoren durch GenAI

- Deepfakes - täuschend echte Video- oder Audiomanipulation
- Promt Injection – Manipulation von KI Systemen
- Hacker nutzen AI zur Automatisierung der Ransomware Angriffe
- AI kann helfen Data Leak Prevention (DLP) zu umgehen
- Data Poisoning – der AI zu Grunde liegende Daten werden verfälscht.

Die Angreifer sind oft Teil großer organisierter Verbrecherbanden

Mitglieder von Cyber-Gangs nach Berufsgruppen[1]

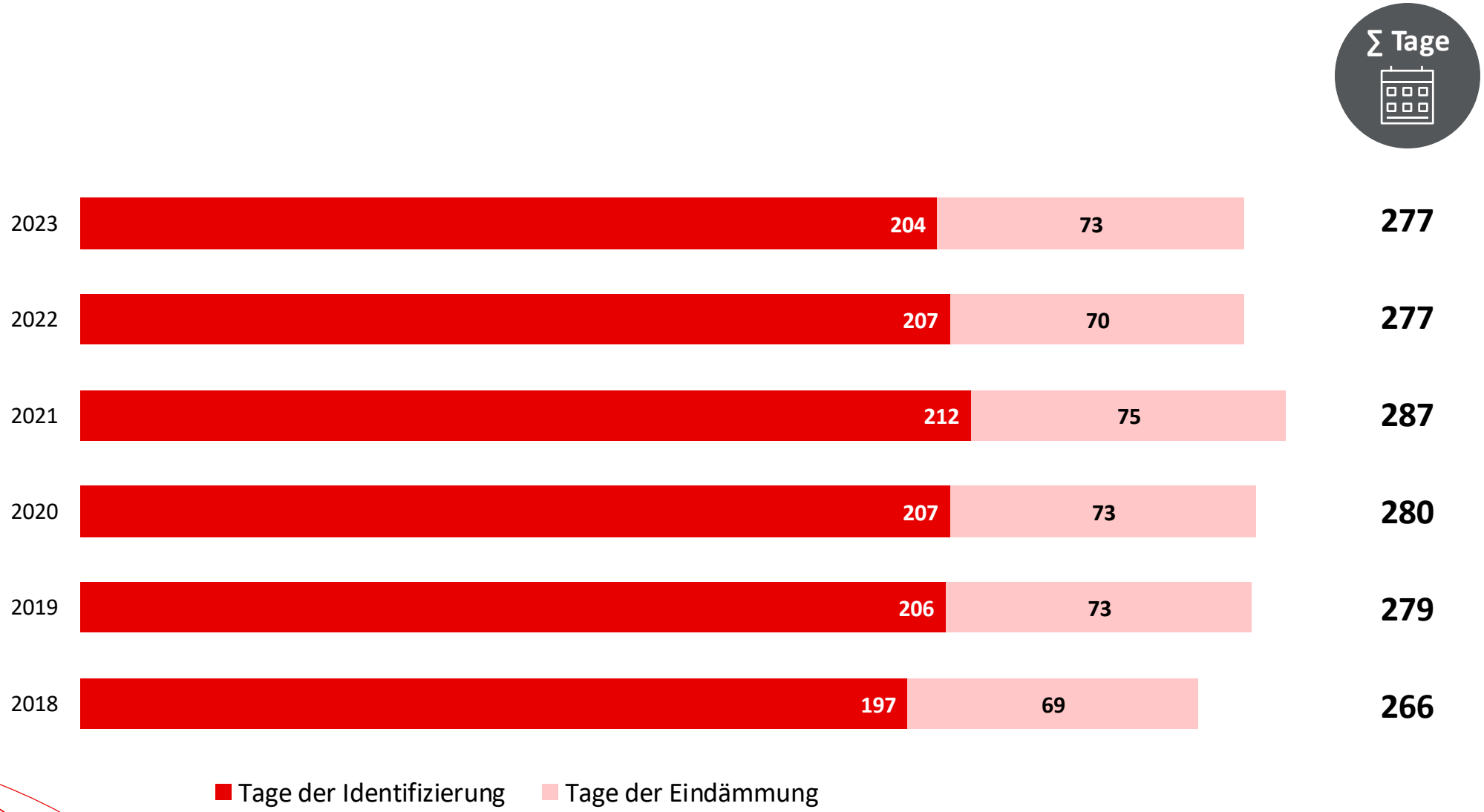


Quelle: atlasVPN (2022) “Role Structure Conti Cybercrime Group”

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

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



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

Detection & Response

04

Detection ist ein entscheidender Aspekt der Cybersicherheit

1. **Früherkennung von Angriffen:** Die Erkennung ermöglicht es, Cyberangriffe frühzeitig zu identifizieren, bevor sie Schäden verursachen können.

2. **Minimierung von Schäden:** Je schneller ein Sicherheitsvorfall erkannt wird, desto effektiver können Maßnahmen ergriffen werden

3. **Verbesserung der Reaktionsfähigkeit**: Die Erkennung ist der erste Schritt in einem effektiven Incident-Response-Plan.

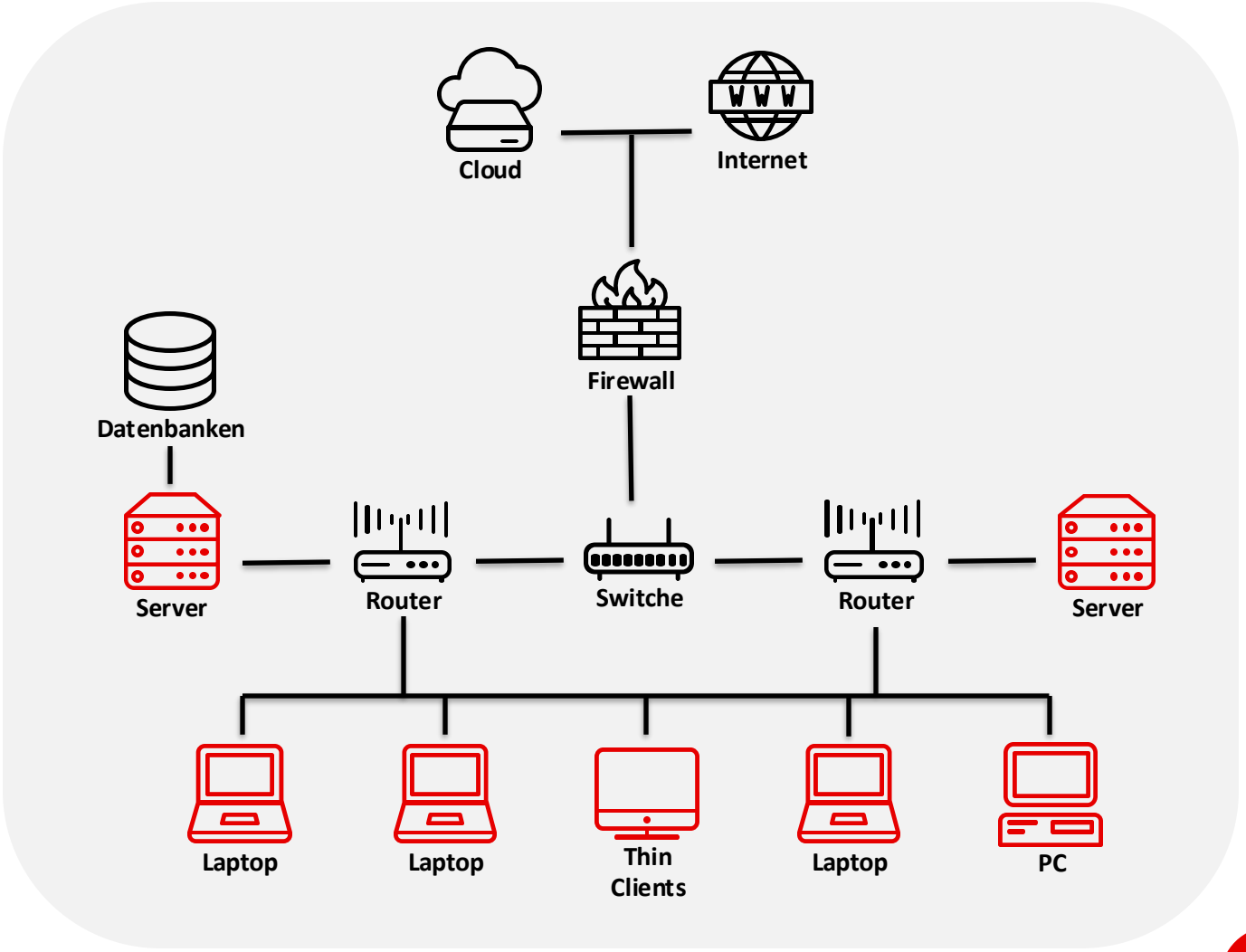
4. **Abwehr fortschrittlicher Bedrohungen:** Die Erkennung ist entscheidend, um auch gegenüber fortschrittlichen Bedrohungen auf dem neuesten Stand zu bleiben.

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

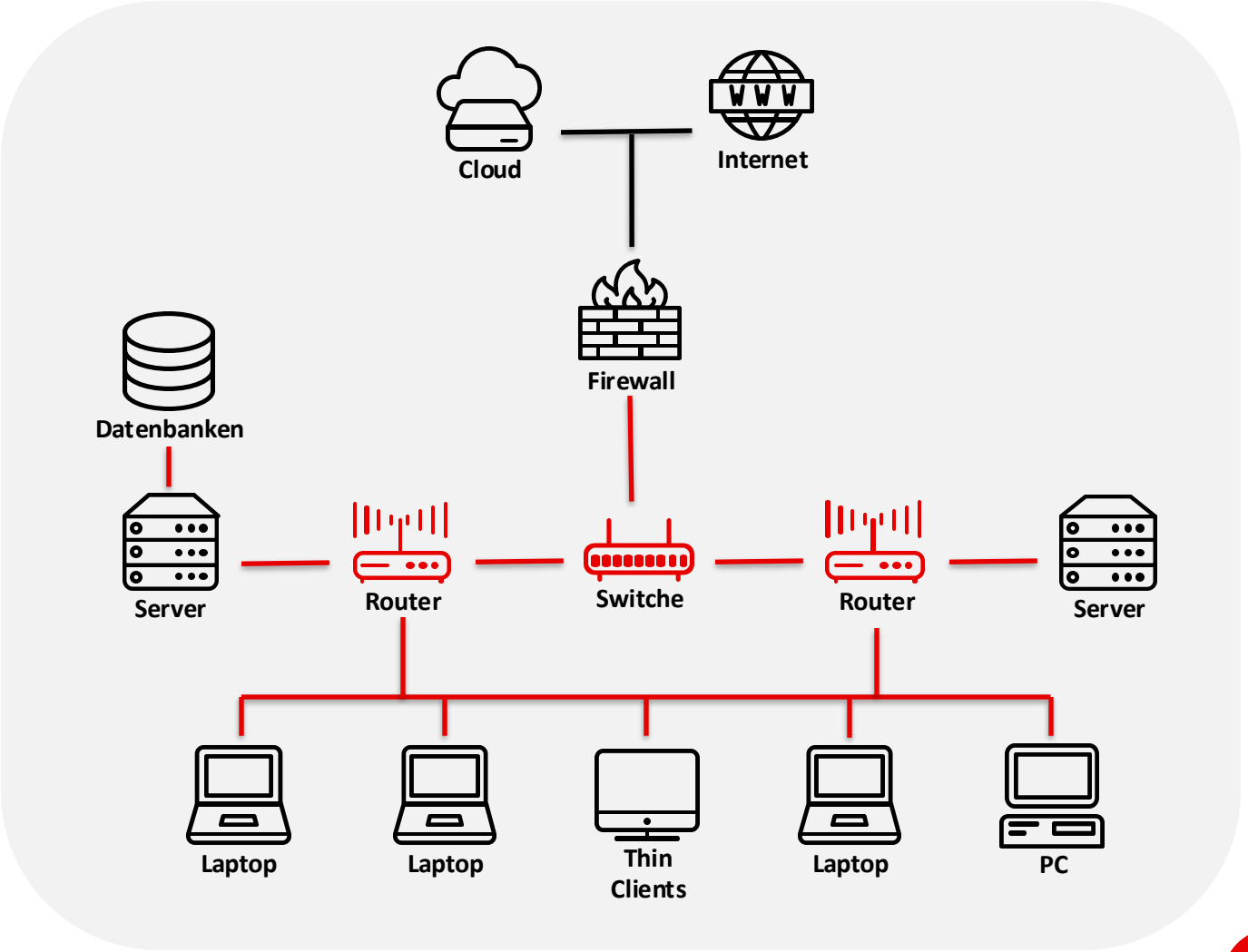


Zunehmende Komplexität durch unterschiedliche Konzepte von „Detection & Response“

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

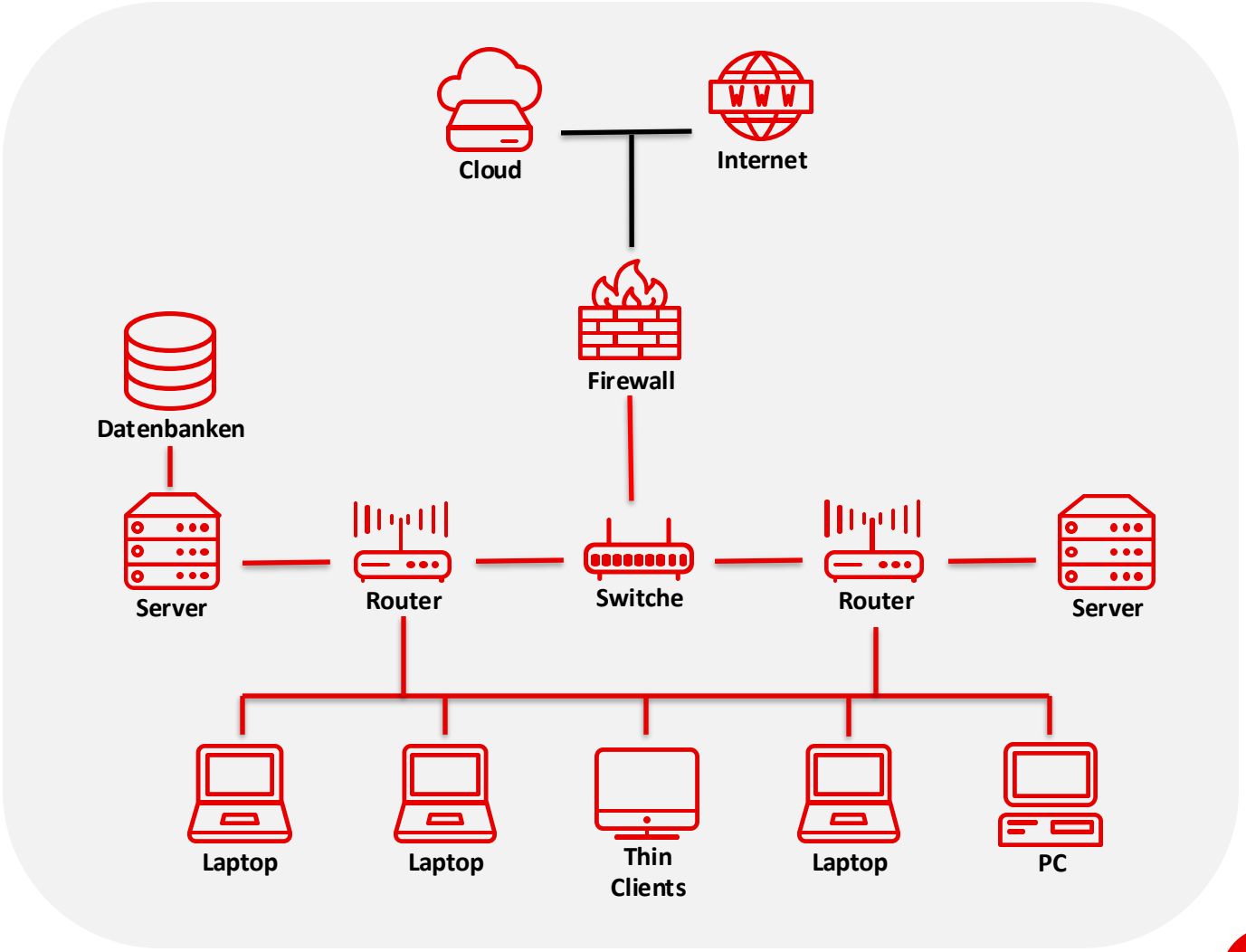


Zunehmende Komplexität durch unterschiedliche Konzepte von „Detection & Response“

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



Der Lebenszyklus eines Sicherheitsvorfalls mit Detection & Response Serivce

Identifizierung

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

Validierung

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

Klassifikation & Impact Assessment

MDR 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

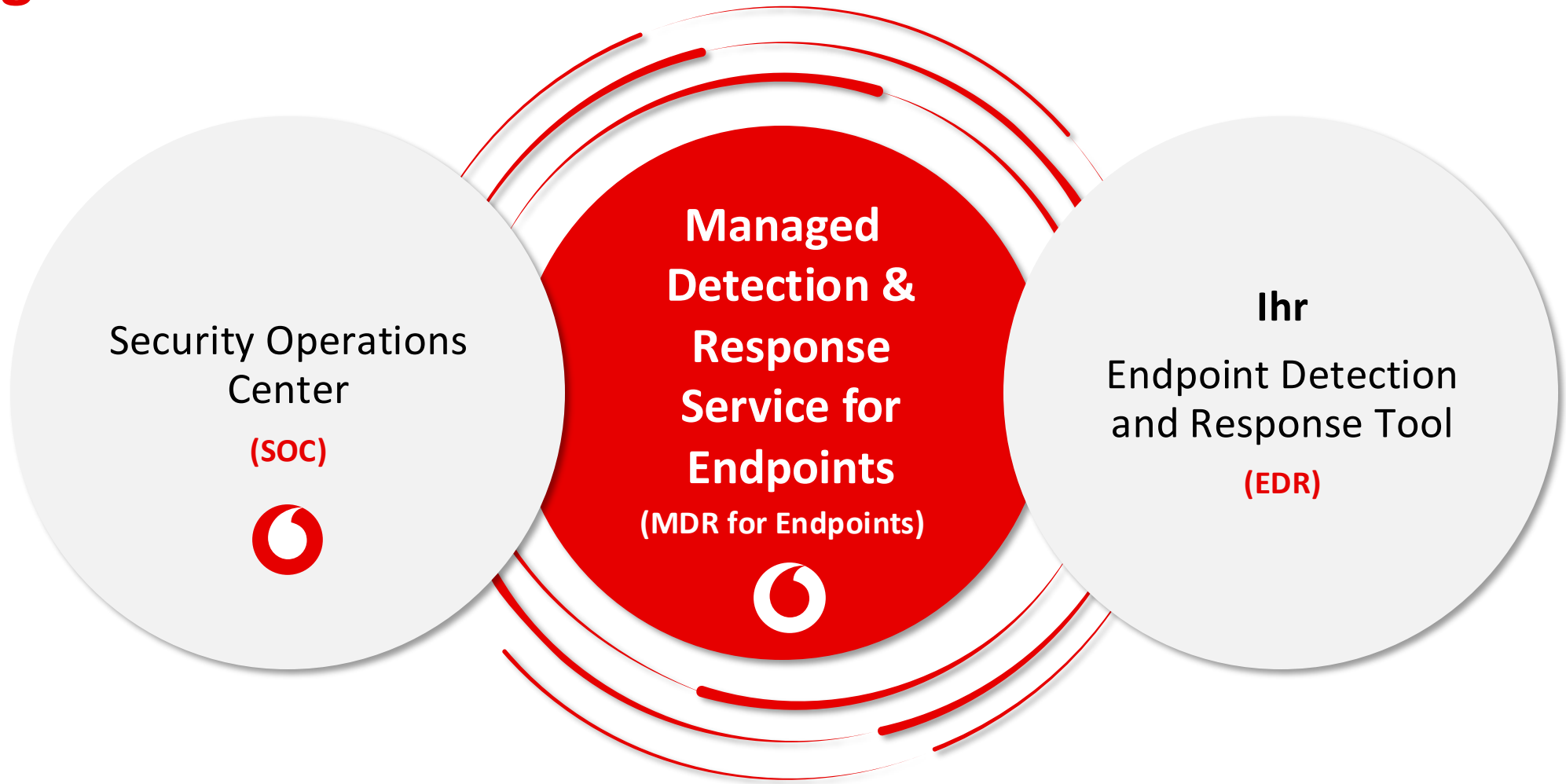
MDR initiiert Incident-Response-Aktivitäten auf den Endpunkten... Bis zur Quarantäne gemäß Playbooks

Der Client initiiert Nicht-Endpunkt-Reaktionen

Closure

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

Im Zusammenspiel mit Ihrem EDR Tool rundet das VF Managed Detection & Response Service for Endpoints Ihre Security Strategie ab



Über das MDR for Endpoints werden vorher definierte Reaktionen ausgelöst

Endpoints

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

Threat Hunting

Analyst führt Bedrohungsjagd auf neue IOCs, IOAs & TTPs durch

01

Investigation

SOC-Analyst untersucht verdächtige Aktivitäten und sammelt kritische forensische Daten

02

Reaktion

SOC-Analyst führt vorautorisierte Behebung durch

03

Benachrichtigung

Kunden werden per Portal und E-Mail benachrichtigt

Durchführen von Behebungen/Isolierungen über das kundeneigene EDR-Tool

elastic

paloalto NETWORKS

Microsoft Defender for Endpoint

vmware Carbon Black

CROWDSTRIKE

SentinelOne

Notfall

Fragen beantworten die Incident Response-Expert:innen

Wir managen aktiv die Bedrohungslage für Sie – mit MDR for Endpoints

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

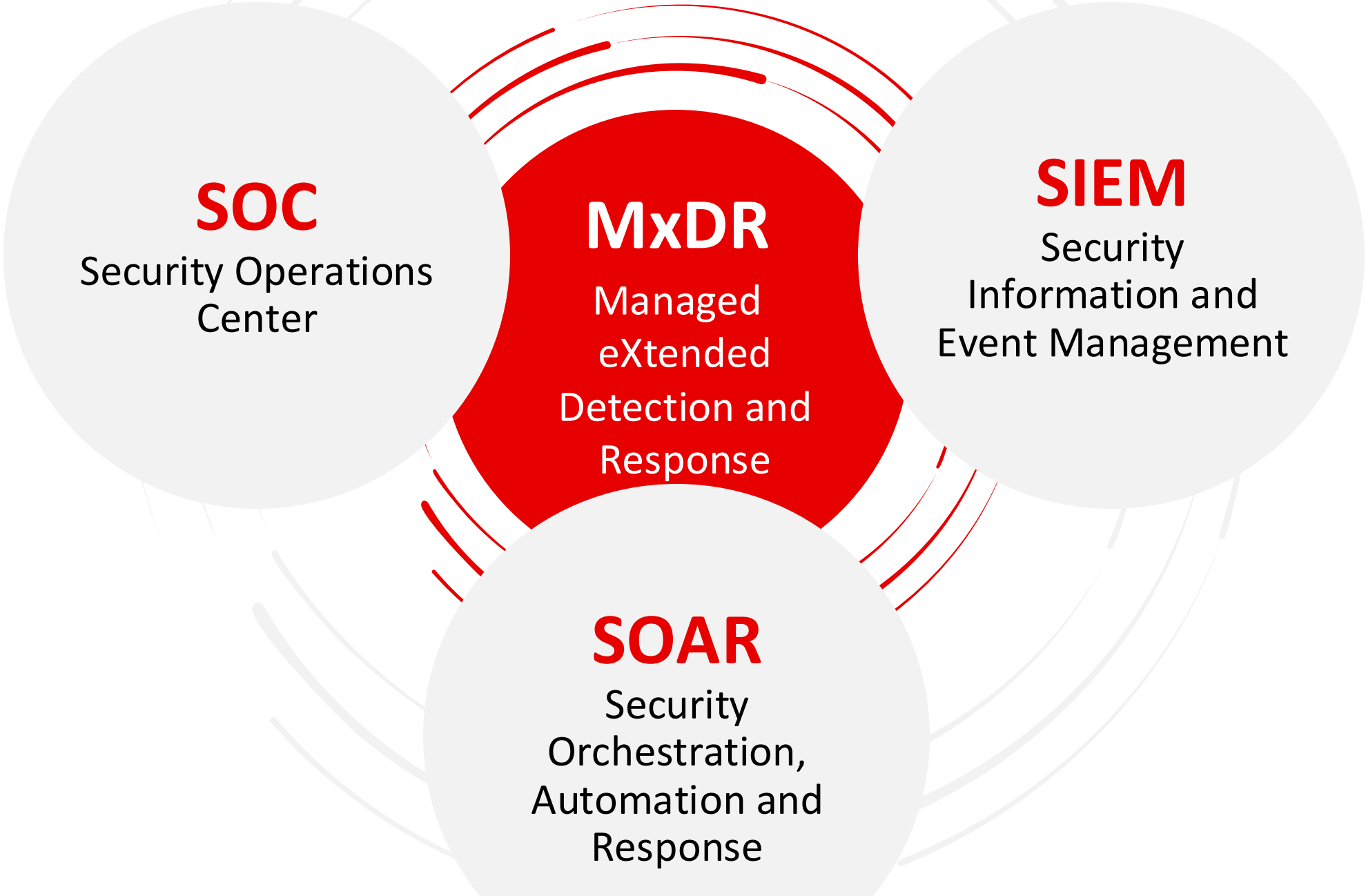
- Zugang zu zertifizierten, geschulten Expert:innen – 24/7 rund um die Uhr
- Engagiertes SOC-Team in Malaga
- Erweiterung Ihres Teams
- Verwaltete Bedrohungssuche, -untersuchung und -behebung
- Branchen- und kundenorientierte Sicherheitsexpert:innen

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 MxDR-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)

Automatisierte Reaktion 24/7

Individuell anpassbarer Service

Erkennung von Anomalien

Gemanagter Service für Sie – vom Logfile bis zur Benachrichtigung

1: Log-Sammlung und Transport

4: Automatisierte Reaktionen über vordefinierte Playbooks mittels SOAR

Endpoints Cloud Email Identität Netzwerk

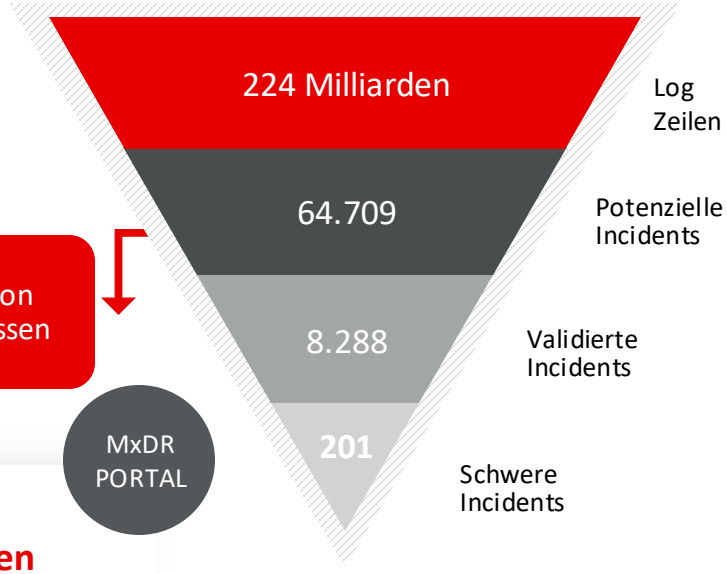
Log-Sammlung Plattform

3: Analyse von Sicherheitsereignissen und Reaktion

5: Präsentation von Sicherheitsereignissen

Genauigkeit

Globaler Schnitt – 24 Stunden



Analytics Tier

Analyse-Engines und Module

Wandelt Protokolldaten in Sicherheitsvorfälle um

2: Analyse & Sicherheits-überwachung

- Eigener SIEM Tennent
- Cyber Threat Intelligence
- Customer rules
- AI unterstützte Analyse
- Vordefinierte Detection Use Cases

Analyst Response Console

Behandlung von Sicherheitsvorfällen

Analyse-Team
Validieren, klassifizieren, priorisieren, eskalieren und reagieren

- Validierung der Vorfälle durch L1, L2 und L3 Analysten
- Reaktion auf den Endpunkten (EDR) mittels SOAR
- Vordefinierte Playbooks für die Reaktion

MxDR PORTAL

Meldung von Sicherheitsvorfällen

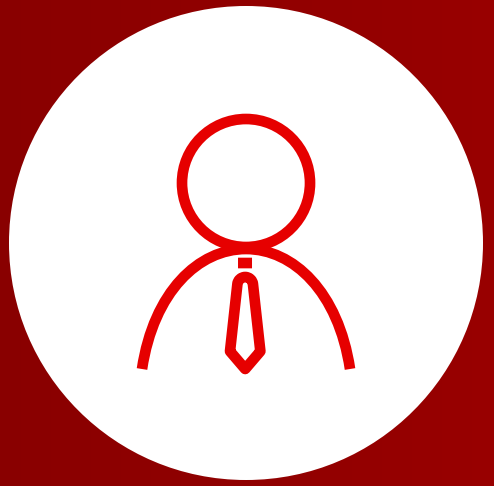
- Notfall
- Informativ
- Kritisch
- Tägliche Übersicht
- Warnung

- Modernes MxDR Portal
- Vollständiger Log-Abruf
- Große Anzahl vordefinierter Reports

Progressives Bedrohungsmodell

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.

Die Aufzeichnungen und
Unterlagen aller Sessions
finden Sie hier.

TIMETABLE 2024

Educational Month Cyber Security

VODAFONE BUSINESS EDUCATION

KW 38

19.09. | 10:00 IT-Sicherheit ist Chefsache: Schützen Sie Ihre Unternehmenswerte und minimieren Sie die (persönliche) Haftung
Dr. Hauke Hansen (FPS Law)

20.09. | 10:00 KI-gesteuerte Security: Ende-zu-Ende-Sicherheit mit Microsoft
Andreas Wach (Microsoft)
Thomas Schmidt (PCG)

KW 39

24.09. | 10:00 Human Firewall – aus Sicht eines White-Hat-Hackers
Immanuel Bär (Prosec Networks)

25.09. | 10:00 Live Hacking: Die Methoden der Hacker und wie Sie sich gegen Ransomware Attacken schützen können
Lukas Garlik (Accenture)
Emil Stahr (Accenture)

26.09. | 10:00 Cyber Security im Zeitalter der KI: Strategien und Best Practices
Fabian Flanhardt (PCG)
Thomas Schmidt (PCG)

KW 40

30.09. | 10:00 Kampf der Ransomware! Wie Sie sich mit Zero Trust richtig schützen
Thanh Trieu (Zscaler)

Together we can

vodafone business