Cyber Security Tool-Kit: Fight Todays Cyber Threats with MDR

Mit Vodafone
& Accenture

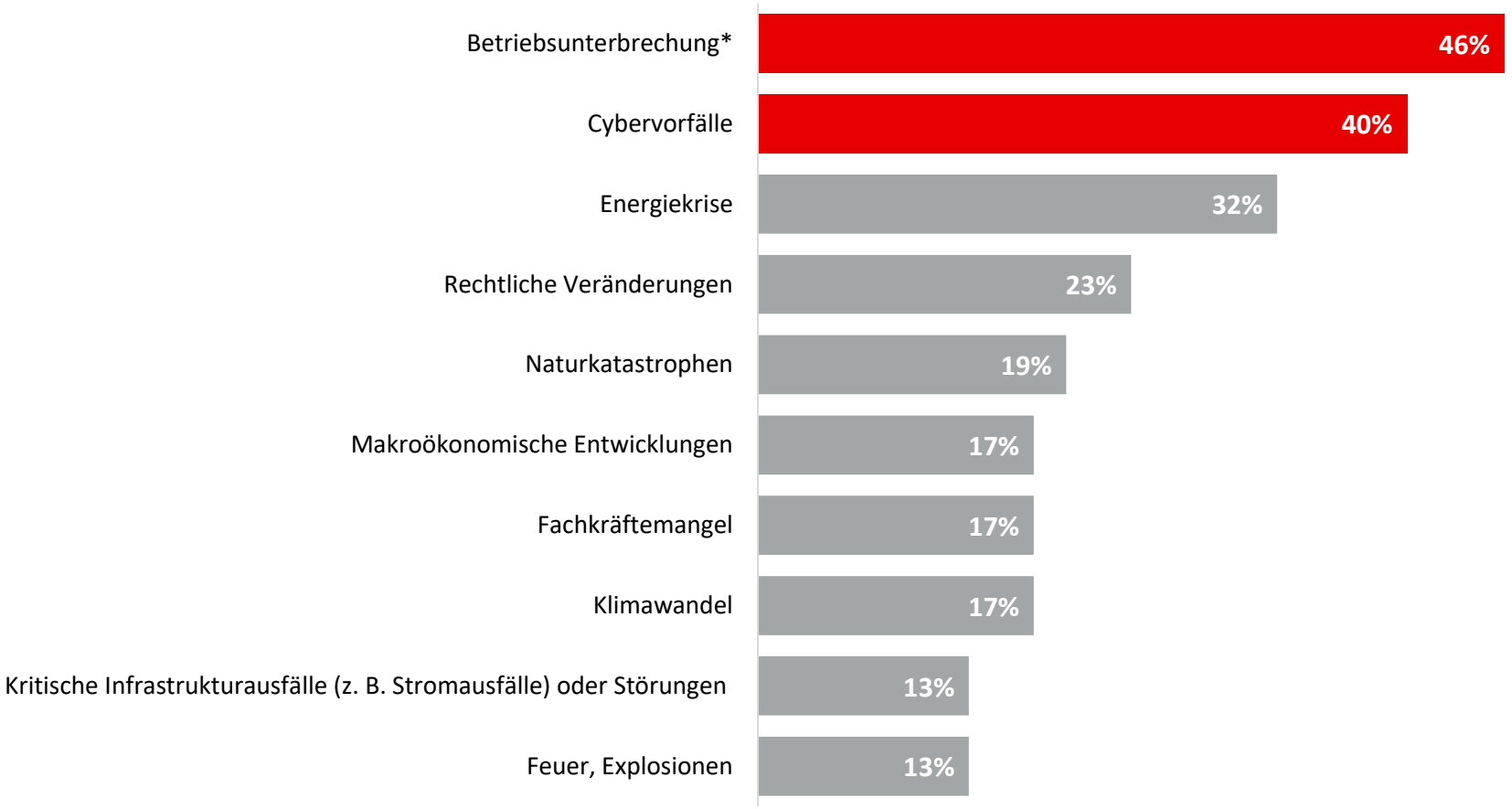
Lukas Garlik

vodafone business

In collaboration with accenture

Cyber Angriffe gehören zu den Top 2 Geschäftsrisiken weltweit

Top 10 Geschäftsrisiken in Deutschland in 2023

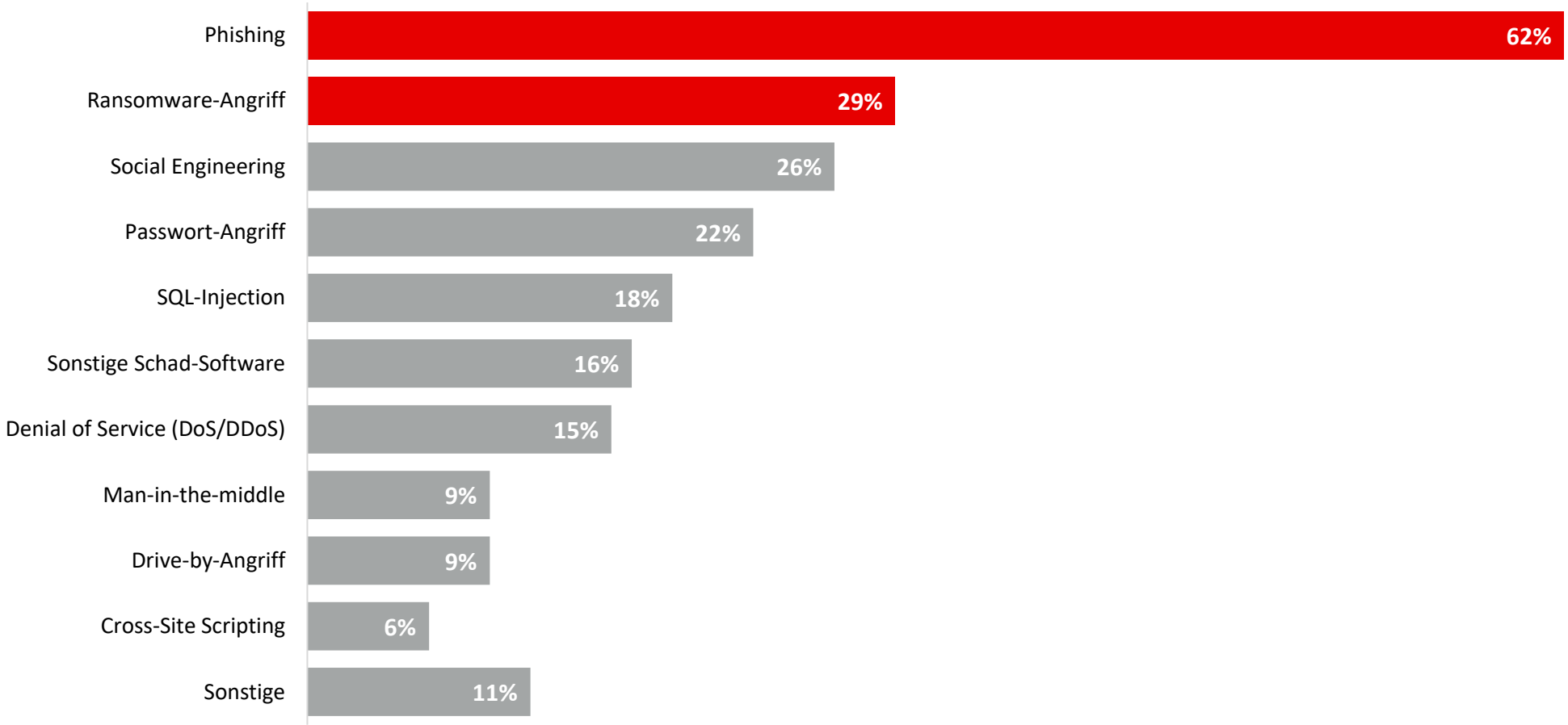


Quelle: Allianz Risk Barometer 2023

Die Zahlen stellen den Prozentsatz der Antworten aller Teilnehmer:innen dar, die geantwortet haben (925). Die Zahlen addieren sich nicht zu 100 %, da mehr als ein Risiko ausgewählt werden konnte.

* Meist durch Cybervorfälle ausgelöst.

Phishing und Ransomware bleiben die häufigsten Angriffsmethoden



Quelle: TÜV Cybersecurity Studie 2023

Identitäts- und Zugriffsmanagement

Cyber-Bedrohungen für den Mittelstand nehmen zu

15.08.2022 | Von Sandra Rios

Das Coronavirus hat eine „digitale Pandemie“ ausgelöst. Besonders der Mittelstand ist stärker in den Fokus von Cyberkriminellen gerückt, da die Sicherheitsmaßnahmen an vielen Stellen nicht ausreichen. Um Daten zu

Home » Nachrichten Sicherheit » Nachrichten Cyberkriminalität

Nürnberger Elektronikkonzern meldet Hackerangriff

Stefan Beiersmann, 3.8.2022, 11:44 Uhr

CYBERSECURITY

Hacker und Spione kosten Unternehmen 203 Milliarden Euro

VON STEPHAN FINSTERBUSCH UND MAXIMILIAN SACHSE - AKTUALISIERT AM 31.08.2022 - 16:57

Die deutsche Wirtschaft verzeichnet immer mehr Angriffe aus Russland und China. Cyberkriminelle werden immer professioneller – und verändern ihre Taktiken.

Einen Monat nach Cyberangriff Noch immer Einschränkungen

08.09.2022 | Stand 08.09.2022, 16:13 Uhr

Cyberangriffe auf den Mittelstand

Die Gefahr durch Cyberangriffe steigt und kleinere Unternehmen werden von den Hackern attackiert. Anzuraten ist externe Expertise.

von Dr. Jakob Jung am 14. September 2022 , 09:49 Uhr

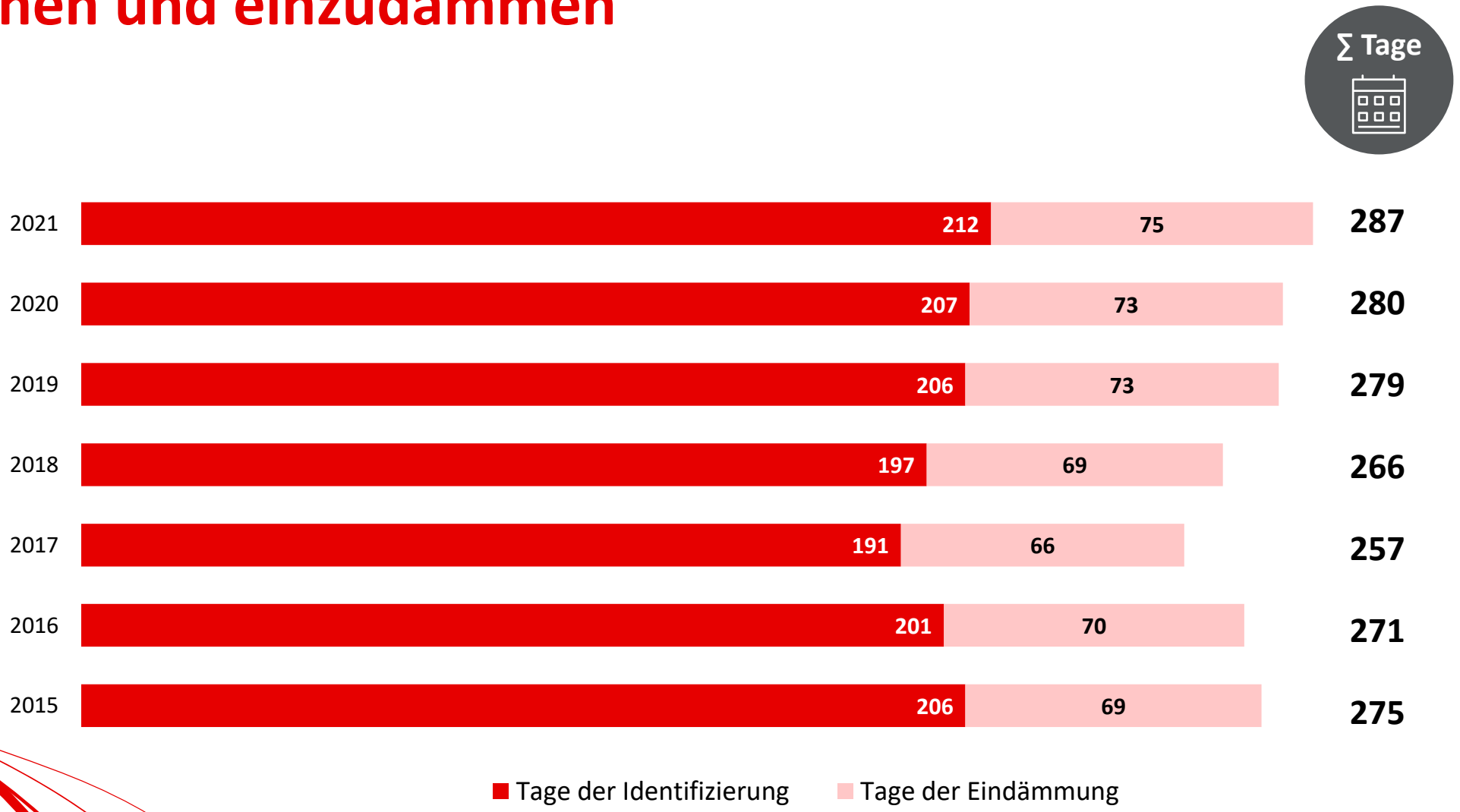
IM FOKUS

Cyberangriffe im Mittelstand: Jedes dritte Unternehmen schon betroffen

Alle News | NEWS DEUTSCHLAND

Mittelstand vermehrt von Cyberattacken betroffen

Durchschnittliche Zeit, um einen Einbruch zu erkennen und einzudämmen



Quelle: IBM (2022) “The cost of a data breach 2022”

Gründe für die Zunahme von Cyber-Angriffen

1. Umstellung auf Homeoffice und zunehmende Digitalisierung
2. Cyberattacken als Waffe in strategischen/politischen Konflikten
3. Der Faktor Mensch als Schwachstelle
4. Cybercrime-as-a-Service (CaaS) im Darknet angeboten

CISOs leben im Auge des Hurrikans

Würde uns ein Breach auf die Titelseite bringen?

- Wahrscheinlichster Angriffsvektor?
- Schwächste Verteidigungselemente?

Wie schnell würden wir uns erholen, wenn wir heute einen Breach haben würden?

- Von Ransomware?
- Von einem Phishing-Angriff?

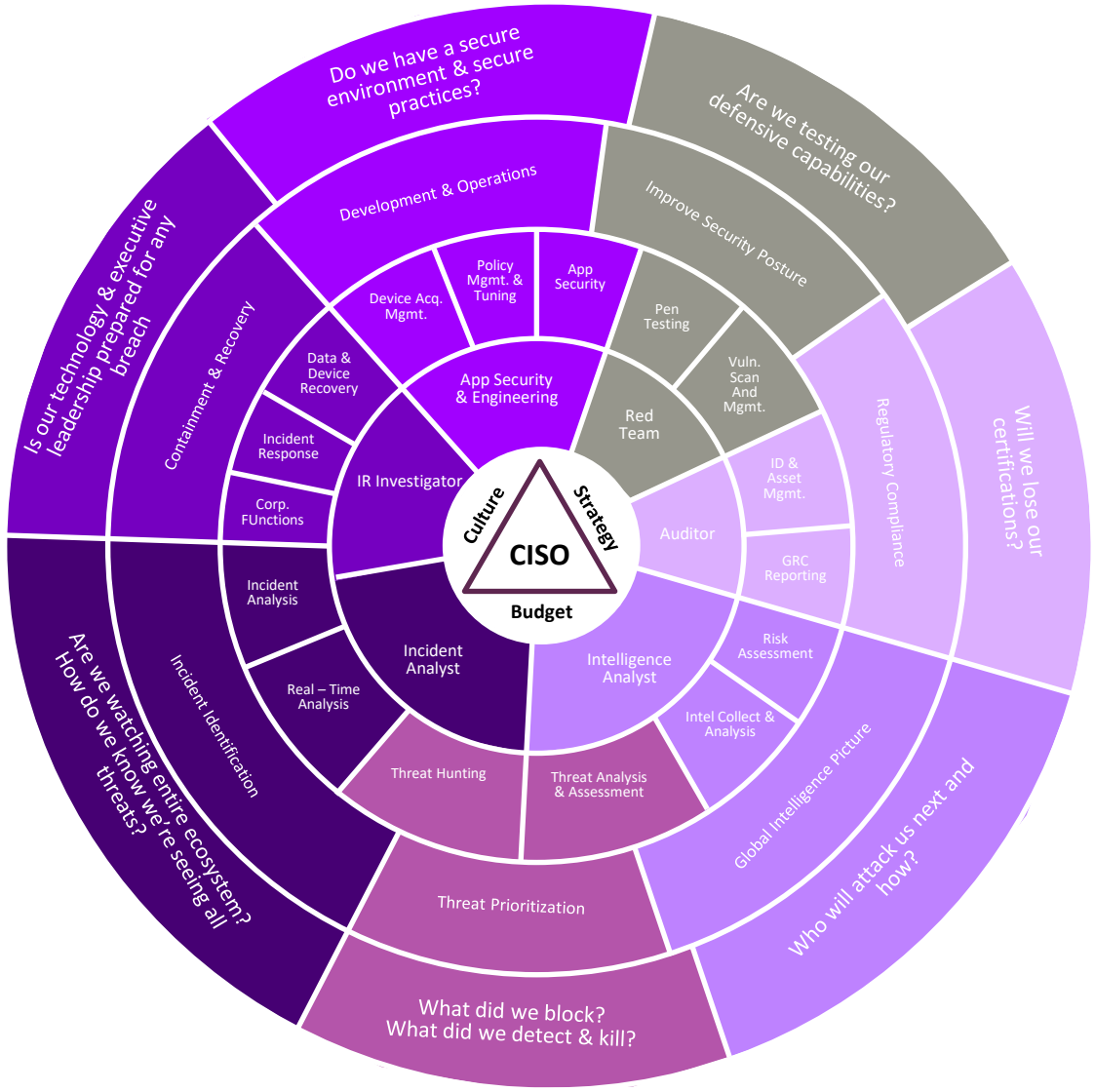
Sind wir sicher vor:

- Hacktivisten mit einer sozialen Agenda?
- Cyberkriminelle?
- Nationalstaatliche Angreifer?

Wer hat es auf unsere Kronjuwelen abgesehen?

- Insider
- Verbrecher
- Konkurrenten
- Nationalstaaten

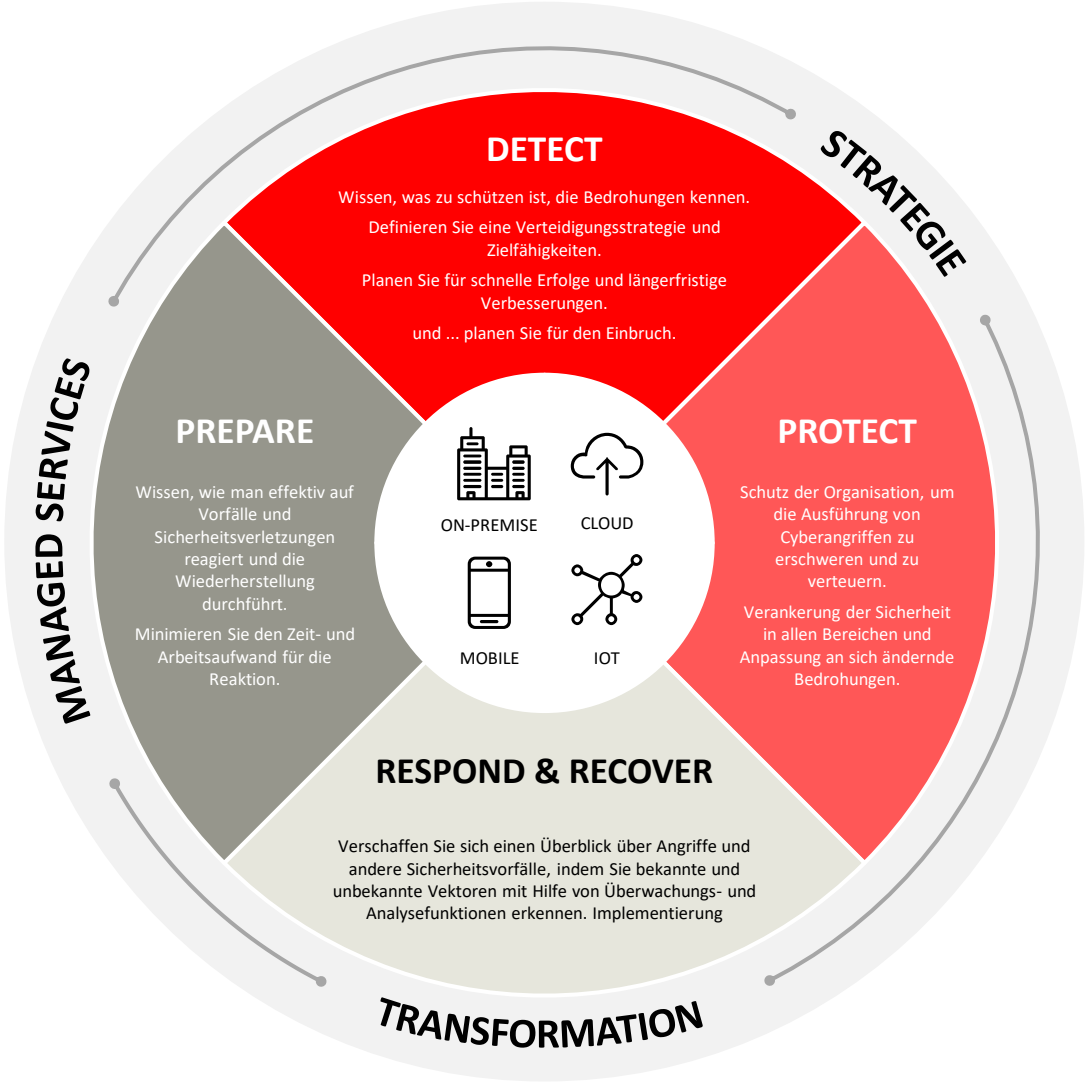
Wie effektiv ist Ihre Überwachung, Erkennung und Reaktion?



Personalaufstockung und Beratung

Seien Sie auf alles vorbereitet und schützen Sie Ihr Unternehmen!

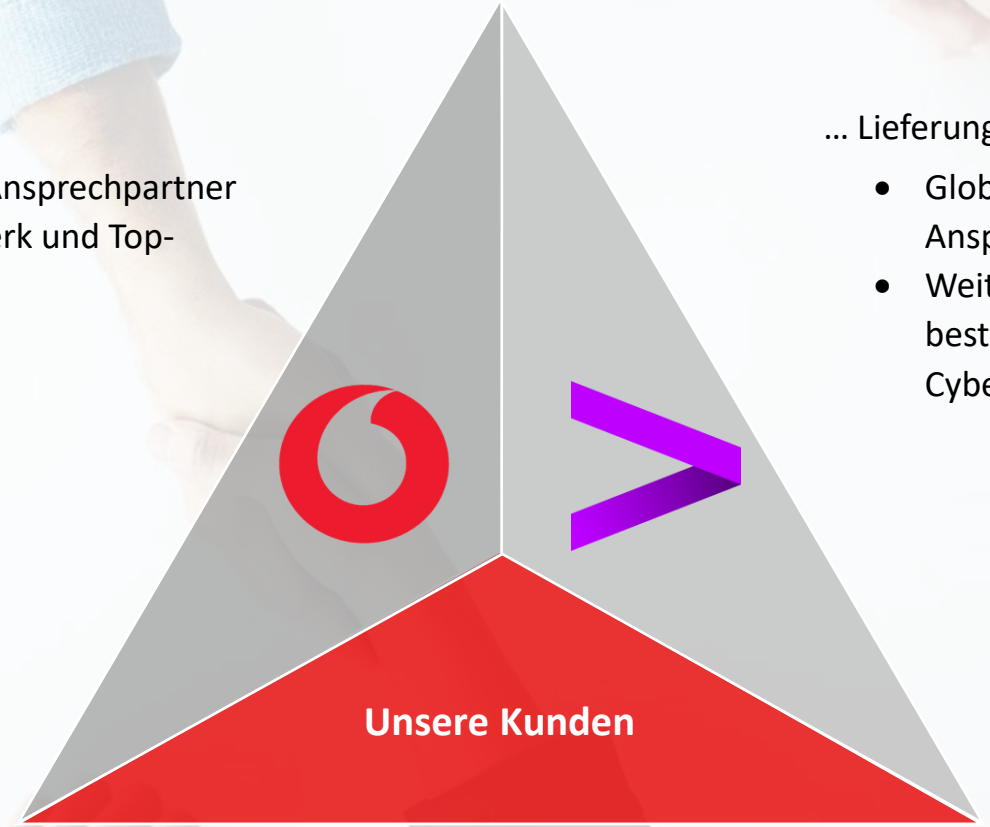
- Cyber-Awareness der Geschäftsführung & der Mitarbeiter herstellen
- Cyber-Strategie erstellen: Kronjuwelen identifizieren, die besonders geschützt werden müssen und Hürde für Angreifer hoch legen
- Stabilen Basis IT-Betrieb herstellen und überwachen (Abarbeitung bekannter Schwachstellen)
- Externe Informationen einholen, um ein realistisches Lagebild zu erhalten (z.B. Threat Intelligence, Darknet Analysen, Red-Teaming, etc.)
- Einbindung von CEO und Vorstand in die Prüfung und Validierung von Angriffsprävention



Cyber Security als win-win-win-Partnerschaft zwischen Vodafone und Accenture, gemeinsam für Sie

Vertrieb an Endkunden über **VODAFONE** …

- Existierende Beziehung und bekannte Ansprechpartner
- Zugriff auf weltweites Experten-Netzwerk und Top-Skills mit lokaler Präsenz



… Lieferung der Services über **ACCENTURE!**

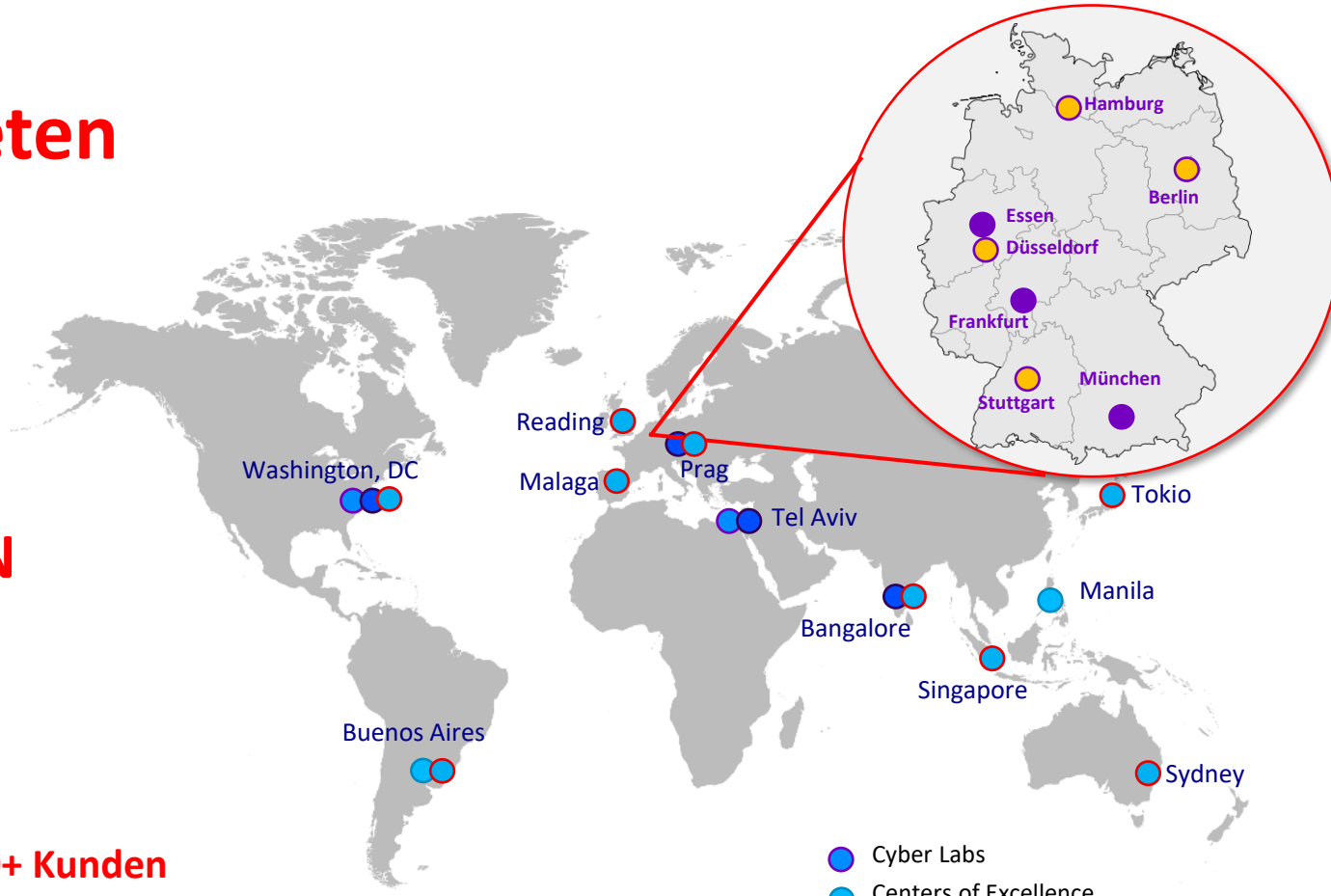
- Globale Expertise mit lokaler Präsenz und Ansprechpartner:innen
- Weitreichende Delivery Capabilities und bestehende Services der ACN-Akquisition Symantec Cyber Security

Sie erhalten **vordefinierte Security-Produkte und Services** – schnell einsetzbar und skalierbar – von **führenden Fachleuten und globalen Experten**, welche normalerweise nur große Konzerne erhalten, über

Vodafone, den Partner Ihres Vertrauens.

Accenture Security – Global vernetzt, Lokal vertreten

RUND UM DIE WELT & RUND UM DIE UHR BESCHLEUNIGEN WIR DAS TEMPO DER CYBER-SECURITY REISE UNSERER KUNDEN



16,000+
Professionelle Security Mitarbeiter

500+
innerhalb der DACH Region

25+ Jahre
Erfahrung, die Organisationen unserer Kunden sicherer zu machen

500+ PROJEKTE
mit Security Fokus jährlich

3100+ Kunden
in 67 Ländern

Zunehmende Komplexität durch unterschiedliche Konzepte von „Detection & Response“

Endpoint Detection & Response

Fokus auf Endpunkte und Hosts

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

Network Detection & Response

Netzwerk und Inter-Device Traffic in Scope

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

eXtended Detection & Response

Endpunkte, Server, Firewalls, UTM, Anwendungen etc.

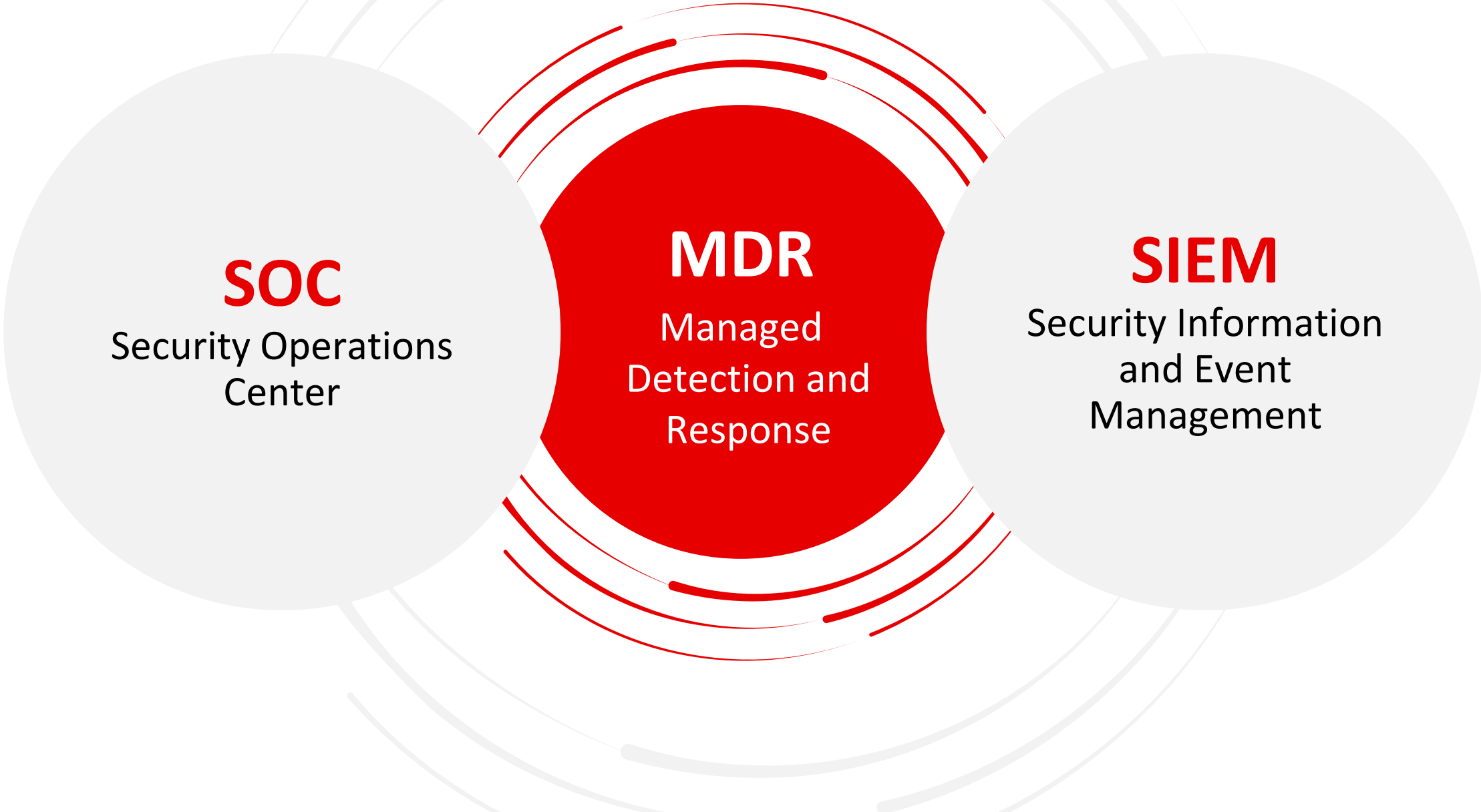
- Sichtbarkeit/Transparenz auf mehreren Sicherheitsebenen
- Überwachung und Analyse der Alarme kostet viel Zeit
- Ganzheitliches Monitoring & Mitigation

Managed eXtended Detection & Response

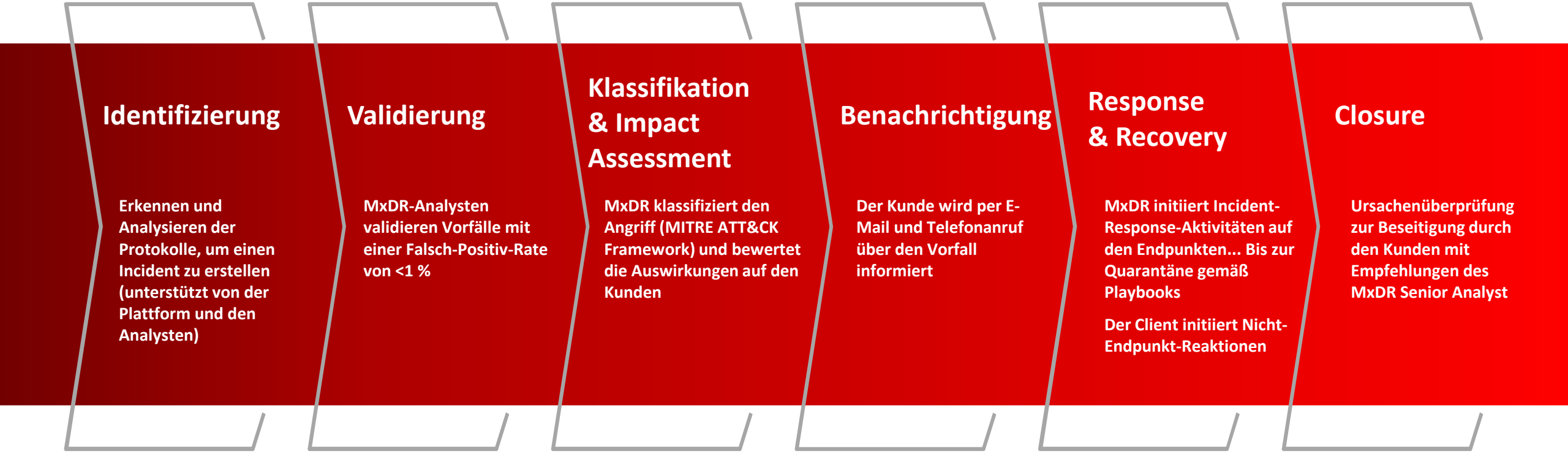
Ein XDR als managed Service

- Outsourcing der Security-Expertise
- Zentralisierung der Security-Informationen in einem Tool
- Hochqualitative Beratung durch ein externes Security Operation Center

Make or Buy


SOC
Security Operations Center
MDR
Managed Detection and Response
SIEM
Security Information and Event Management

Der Lebenszyklus eines Sicherheitsvorfalls



Für bekannte Bedrohungen:

MxDR bietet seinen Kunden detaillierte Berichte und Best-Practice-Gegenmaßnahmen

Für unbekannte Bedrohungen:

Fast-Track-Analysen, Beschreibungen und aktualisierte Signaturdefinitionen

- MxDR kann mit dem Kunden zusammenarbeiten, um benutzerdefinierte Verhaltensüberwachungs- und Gegenmaßnahmen zu entwickeln und bereitzustellen.

MDR mit Vodafone und Accenture

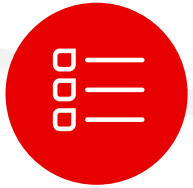
Der MDR-Service ist ein Managed Service, der mittels führenden Analysen und hochqualifizierten Analysten proaktiv Cyberangriffe aufspürt, vermeidet oder eindämmt, bevor sie wesentliche Auswirkungen auf das Geschäft haben.

Datenanalyse

24/7 Alert Monitoring

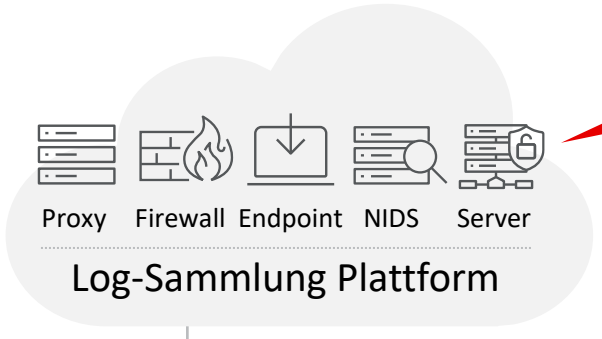
Hochqualifizierte Analysten (SOC)

Individuell anpassbarer Service



Erkennung von Anomalien

MDR Service für Sie – vom Logfile bis zur Benachrichtigung



Schritt 1: Log-Sammlung und Transport

Schritt 2: Analyse und Sicherheits-überwachung

Analytics Tier

Analyse-Engines und Module

Wandelt Protokolldaten in Sicherheitsvorfälle um

- Intelligence
- Geschäftskontext
- Maschinelles Lernen
- Customer rules

Schritt 3: Analyse von Sicherheitsereignissen und Antwort

Analyst Response Console

Behandlung von Sicherheitsvorfällen

Analyse-Team

Validieren, klassifizieren, priorisieren, eskalieren

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

Schritt 4: Präsentation von Sicherheitsereignissen

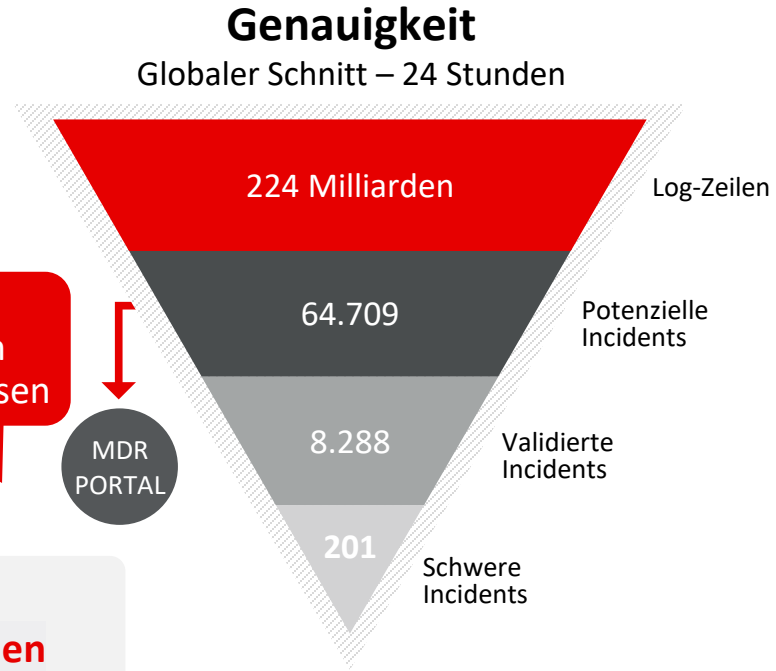
MDR PORTAL

Meldung von Sicherheitsvorfällen

- Notfall
- Informativ
- Kritisch
- Tägliche Übersicht
- Warnung

- Vollständiger Log-Abruf
- DeepSight
- Reports

Progressives Bedrohungs-modell



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 6 SOCs
- 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

MDR als Erweiterung Ihres Teams

Wir sind eine Erweiterung Ihres Teams!

Service Delivery Lead

- Erster Ansprechpartner für Problemlösung und Eskalation
- Entwirft einen Client-Escalation Tree für die richtige Incident-Eskalation
- Identifiziert Bereiche zur Serviceverbesserung
- Verwaltet Kundenanrufe - Service Kick-off, monatliche Serviceüberprüfungen, Briefings für Führungskräfte etc.

Senior Security Analyst

- Dedizierter, GIAC-zertifizierter Analyst
- Eskalationsstelle für Probleme und Anfragen von Sicherheitsanalysten
- Abstimmung und Neuklassifizierung von proprietären Signaturen und Fehlalarmen
- Bereitstellung von Security Incidents und Log-Reporting
- Arbeitet mit dem SOC-Analystenteam zusammen, um über die Bedrohungen der Branche informiert zu bleiben

Security Engineer Team

- Vervollständigung der Geräteeinbindung und Alarmoptimierung
- Unterstützung bei LCP-Design, Testen und Implementierung
- Aktiviert Geräte für die Log-Collection mit Zertifikaten oder Agenten
- Identifiziert potenzielle add-on Technologien/Monitoring
- Überwacht den Gerätezustand und optimiert die Protokollierung
- Verwaltet den LCP-Zustand

Security Analyst Team

- GCIA, GCIH, GCFA zertifiziert
- Überwacht den Network-Traffic
- Bewertet und untersucht potenzielle Sicherheitsvorfälle
- Eskaliert potenzielle Sicherheitsvorfälle und bietet Remediation Anleitung
- Isoliert und korrigiert Endpunkte
- Bearbeitet/behebt Probleme und Anfragen von Kundenanalysten

vodafone business

In collaboration with

accenture