

Cybersecurity die nie schläft

Smarte Antworten auf Fachkräftemangel & NIS2

Michael Schröder
ESET Deutschland GmbH

Selbstdiagnose IT-Sicherheit 2025

Fazit: Vor 20 Jahren war alles besser 😊

Bundeslagebild Cybercrime

Berichtsjahr 2024

DIE LAGE

Die Bedrohungslage im Cyberraum ist anhaltend hoch.

Die Anzahl polizeilich bekannt gewordener Cyberdelikte steigt - maßgeblich hierfür sind vor allem Fälle, bei denen der Handlungsort des Täters unbekannt oder im Ausland ist.



rund **90%**
Dunkelfeld



Täter im Ausland/
unbekannt¹
201.877
Fälle

Täter in
Deutschland
131.391
Fälle

Gründe für die Nicht-Anzeige sind oft Scham, Angst vor Reputationsverlust oder der Angriff wurde gar nicht bemerkt.

¹Straftaten, die aus dem Ausland oder von einem unbekanntem Ort aus verübt werden und zu Schäden in Deutschland führen.

Wirtschaftlicher Schaden durch Cyberattacken



Quelle: Bitcom e.V.

höchste je gemessene Schadenssumme



Underground Economy

Cyberkriminelle agieren hochprofessionell und arbeits- teilig. Sie bieten in industriellem Maßstab kriminelle Dienstleistungen zur Begehung von Cyberstraftaten an.



TRENDS UND ENTWICKLUNGEN



Phishing

400.000

vgl. zu 2023:
Anstieg um fast
70%

Phishing-E-Mails wurden 2024 der Verbraucherzentrale Nordrhein-Westfalen gemeldet

Anzahl der weitergeleiteten Phishing-Mails 2024



Wie in den Vorjahren beziehen sich die häufigsten Narrative auf den Finanzsektor, der eine hohe Bedeutung für Staat und Bevölkerung hat.

Ransomware



950

Ransomware-Angriffe wurden zur Anzeige gebracht

 ≈ 10 Millionen \$

Erpressungsziele



der Angriffe richteten sich gegen Unternehmen, Organisationen und Institutionen.



der Angriffe richteten sich gegen kleine und mittelständische Unternehmen.

Nur die ca. 10% die wir sehen!

umgerechnet rund

800 Mio US-Dollar

Festgestellte Lösegelder auf Kryptowallets von Ransomware-Akteuren weltweit Quelle: Analysis



Manche Dinge ändern sich nie, oder?

Top 5 Angriffsvektoren	Methodik	Relative Häufigkeit
1. Ransomware	Phishing, Remote Desktop	30%
2. Exploits & Schwachstellen	Sicherheitslücken, ZeroDays	25%
3. Phishing & Social Engineering	SpearPhishing, Mails, CEO-Fraud	20%
4. Supply-Chain-Angriffe	Software-Updates, kompromittierte Dienstleister	15%
5. Cloud-Sicherheitslücken & Fehlkonfigurationen	Fehlende MFA, Lücken in Konfiguration	10%

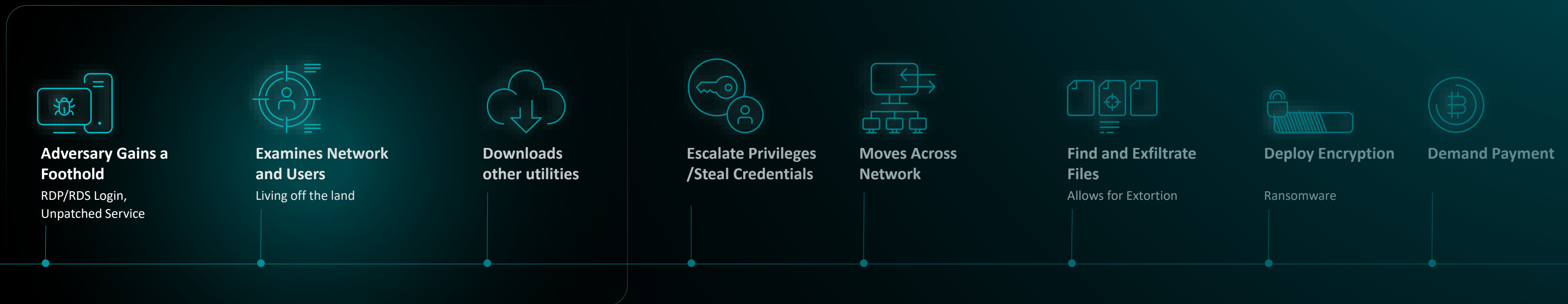
Quellen: BSI Lagebild, Enisa Threat Landscape, Deloitte Cyber Threats, Swiss National Cyber Security Center, Microsoft Digital Defense Report

anomalie erkannt!

Anomalie erkannt!

Neue Regeln, alte Strukturen!

Spotting the Breach



58% können das technologisch nicht leisten!

Jäger der ungenutzten Potentiale

5 klassische Warnsignale das Sie MDR brauchen!

Und warum NIS2 als Weckruf überfällig ist!



1. Blinde Flecken

A man in a light blue shirt is sleeping at a desk in a dimly lit room. The desk has a large monitor displaying a hacker in a hoodie, a keyboard, and a mouse. A desk lamp is on, casting a soft glow. In the background, another monitor shows a world map. A teal banner is overlaid on the right side of the image.

2. Standby-Modus



3. Ressourcen auf Kante



4. Hightech im Leerlauf

COMPLIANCE









5. Compliance als Showact



Cybersecurity
Progress. Protected.

Wir können uns diesen „Luxus“ nicht mehr leisten!

Welche Dinge wirklich zählen

Oktober 2024 Krankenhaus Bayern Mai 2024 Behörde Mecklenburg-Vorpommern
April 2025 Wohnungsbaugesellschaft Baden-Württemberg
Mai 2025 Kulturverein Bayern
April 2025 Brauerei Bayern
Januar 2025 Ministerium Bremen

Mehr als 2 öffentliche Incidents pro Tag!

Januar 2025 Elektronische Signaturen Berlin April 2025 Logistikunternehmen Nordrhein-Westfalen Mai 2025 Nahverkehrsgesellschaft Berlin
Februar 2025 Stadtverwaltung Bayern Juni 2024 Krankenhaus Bayern
Mai 2025 Autohändler Nordrhein-Westfalen
April 2025 Stadtverwaltung Sachsen
September 2024 Fußballverein Nordrhein-Westfalen Mai 2025 Molkereigenossenschaft Nordrhein-Westfalen Februar 2025 Reiseveranstalter Nordrhein-Westfalen
August 2024 Flugsicherungsunternehmen Hessen
November 2024 Arztpraxis Bayern
November 2024 Stadtverwaltung Bayern
Januar 2025 Eisenbahngesellschaft Schleswig-Holstein Februar 2025 Gemeinnütziger Verein Nordrhein-Westfalen Mai 2024 Landmaschinenhersteller Nordrhein-Westfalen März 2025 Gemeinde Saarland September 2024 Radiostation Bayern
März 2025 Arbeitsagentur Bayern
Dezember 2024 Stiftung Nordrhein-Westfalen
Oktober 2024 Anbieter von Reisebuchungs-Software Berlin
September 2024 Industrieunternehmen Nordrhein-Westfalen März 2025 Stadtmarketing-Gesellschaft Baden-Württemberg April 2025 Entsorgungsunternehmen Rheinland-Pfalz
Juli 2024 Notarkammer Rheinland-Pfalz
Oktober 2024 Schulen Bayern
Februar 2025 Landratsamt Bayern
März 2025 Versorgungsunternehmen Nordrhein-Westfalen
August 2024 Jugendherbergen Nordrhein-Westfalen
Januar 2025 Galerieshops Rheinland-Pfalz

Ca. 50% davon KRITIS oder Verwaltung

Januar 2025 Medizinisches Zentrum Hamburg
April 2025 Stadtverwaltung Baden-Württemberg
Oktober 2024 Pharmagroßhändler Bayern
Januar 2025 IT-Dienstleister Bremen
Mai 2025 Berufsschule Nordrhein-Westfalen
Mai 2025 Zeitung Baden-Württemberg

Cybersecurity braucht ein sicheres Fundament

Das ist die Basis für ein erfolgreiches Projekt. Ein solches Fundament ist die Sicherheit der Daten. Nur wenn die Daten sicher sind, kann die Cybersecurity erfolgreich sein. Ein solches Fundament ist die Sicherheit der Daten. Nur wenn die Daten sicher sind, kann die Cybersecurity erfolgreich sein.

Vertrauen ist kein Add-On !



>70% wollen zukünftig auf EU-Anbieter wechseln!

Das „Unsichtbare“ sichtbar machen!

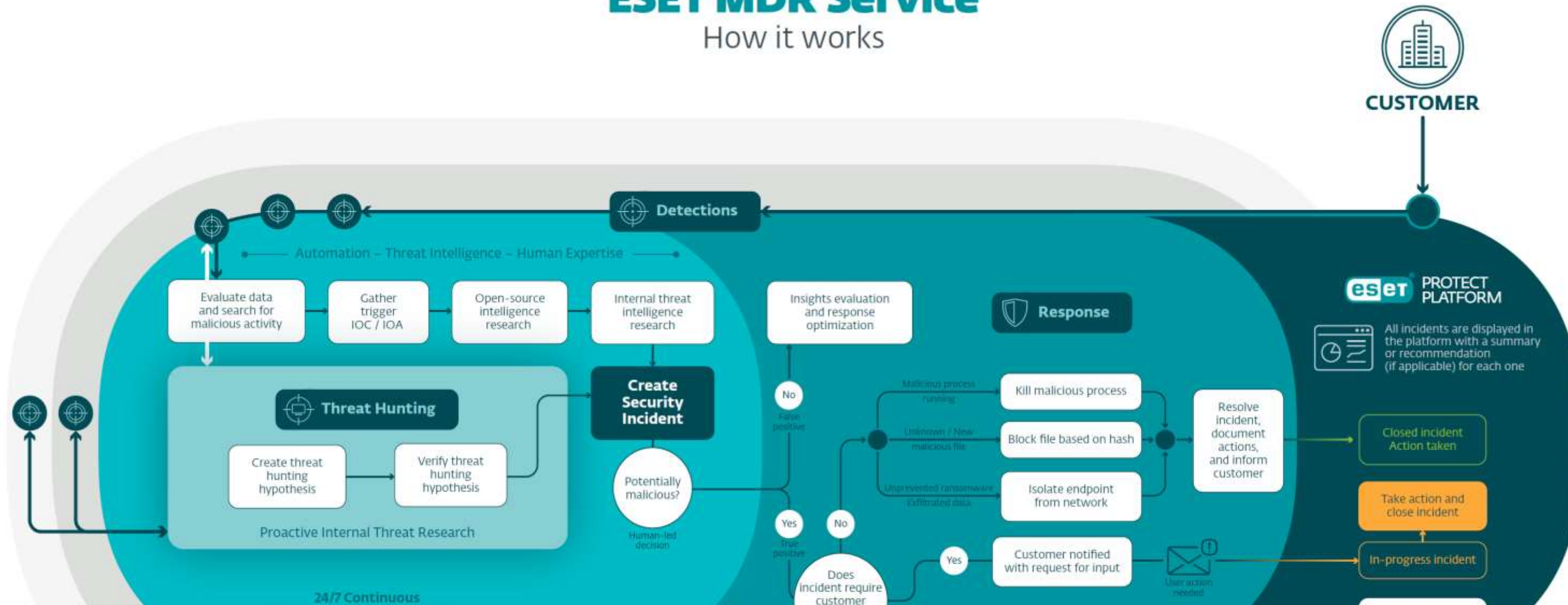
MDR ohne Kontrollverlust und bei voller Integrität



De belangrijkste trends in de wereld van de klantreis

ESET MDR Service

How it works



Komplexität reduzieren & Sicherheit maximieren

Von Prävention zu Reaktion, mit Wirkung!

6 Minuten (MTTR) bis zur finalen Response!

MITARBEITER DES JAHRES

eset[®]

MDR



24/7 „Stundenlohn“ 0,54 EUR (KI + menschliche Expertise im SOC / bei 100 Mitarbeitern)

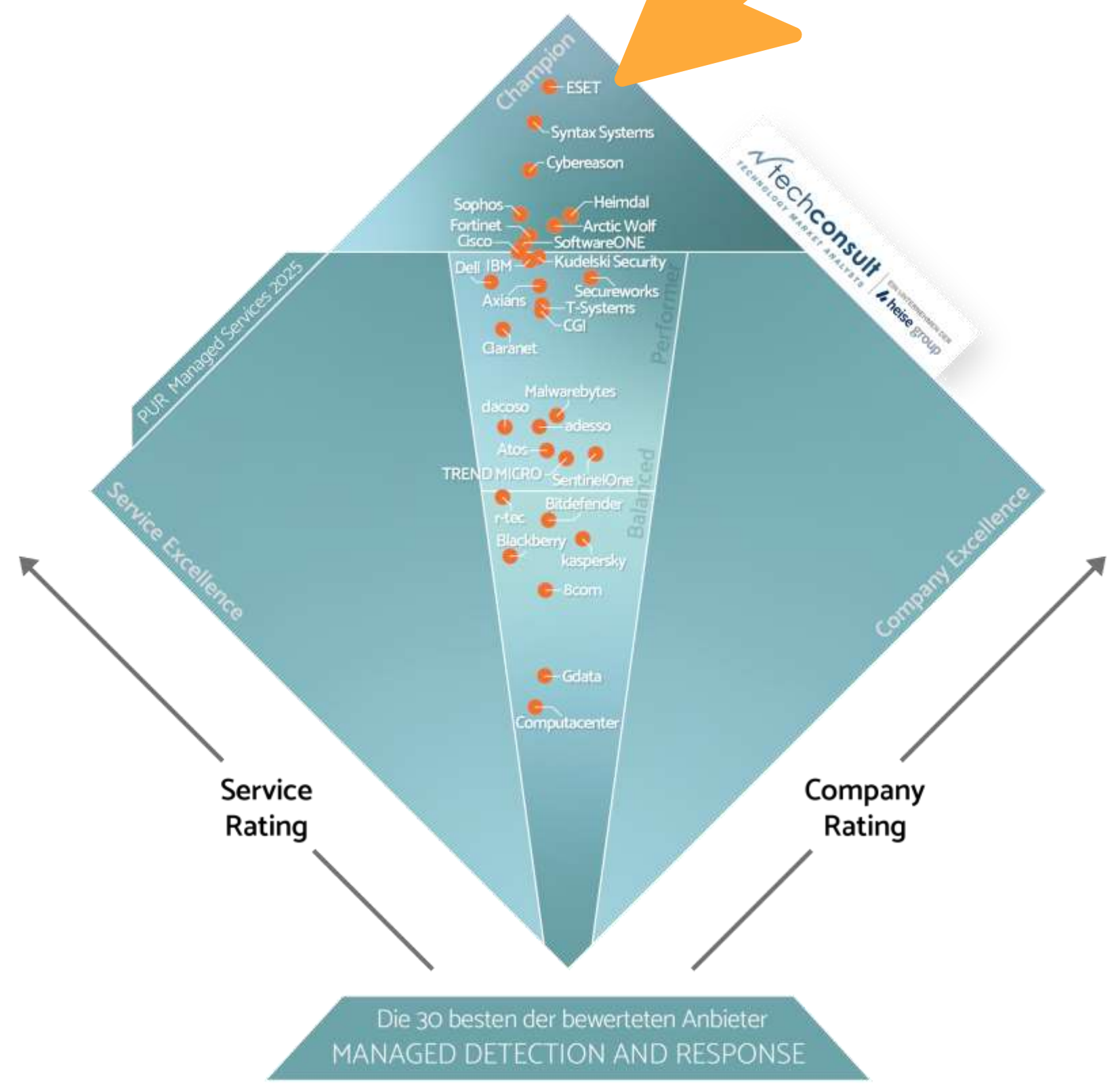


CHAMPION
IN DER KATEGORIE
MANAGED DETECTION AND RESPONSE



Diese Auszeichnung steht für das hervorragende Ergebnis des Anbieters von Managed Services im Rahmen der Kundenbewertungen. Der Erfüllungsgrad von mehr als 67 Einzelkriterien auf Unternehmens- und Serviceebene wurde ausschließlich von den Kunden der Anbieter beurteilt.

Peter Burghardt
Peter Burghardt
- Managing Director -



“

Sicherheit beginnt mit der Entscheidung,
nicht alles selbst machen zu müssen!

Michael Schröder

ESET Business-Lösungen

ESET PORTFOLIO

Data Feeds + APT-Reports
ESET Threat Intelligence

Endpoint Detection and Response
Cloud: ESET Inspect® / **
On-Premises: ESET Inspect On-Prem®

Managed Detection and Response Services
ESET MDR Ultimate
ESET MDR

Detection and Response Service
ESET Detection and Response Advanced

Cloud Sandboxing
ESET LiveGuard® Advanced

Schutz von Cloud-Anwendungen
ESET Cloud Office Security® / **

Verschlüsselung
ESET Endpoint Encryption®
ESET Full Disk Encryption

Multi-Faktor-Authentifizierung
ESET Secure Authentication®

Schutz von Clients und Mobilgeräten
ESET Endpoint Security
ESET Endpoint Antivirus

Schutz von Fileservern
ESET Server Security

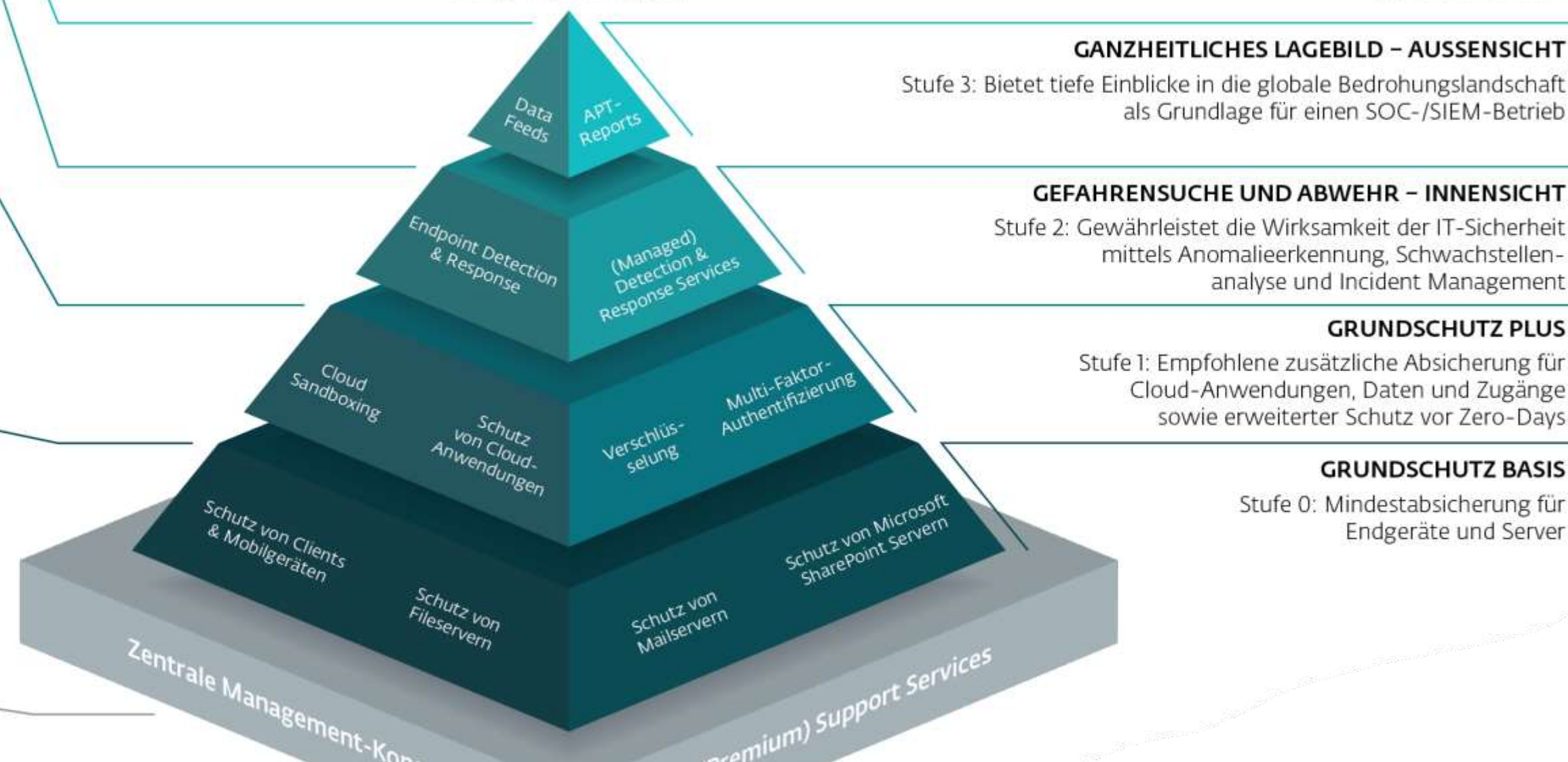
Schutz von Mailservern
ESET Mail Security

Schutz von Microsoft SharePoint Servern
ESET Security for Microsoft SharePoint Server

Zentrale Management-Konsole
Cloud: ESET PROTECT**, inkl.:

EINSATZBEREICH

SCHUTZLEVEL



Cybersecurity zuende gedacht / On-Prem & Cloud

* Verwaltung über separate Management-Konsole
** Unterstützung von ESET Connect (REST-API)

Let's talk!



Halle 9
Stand 9-434