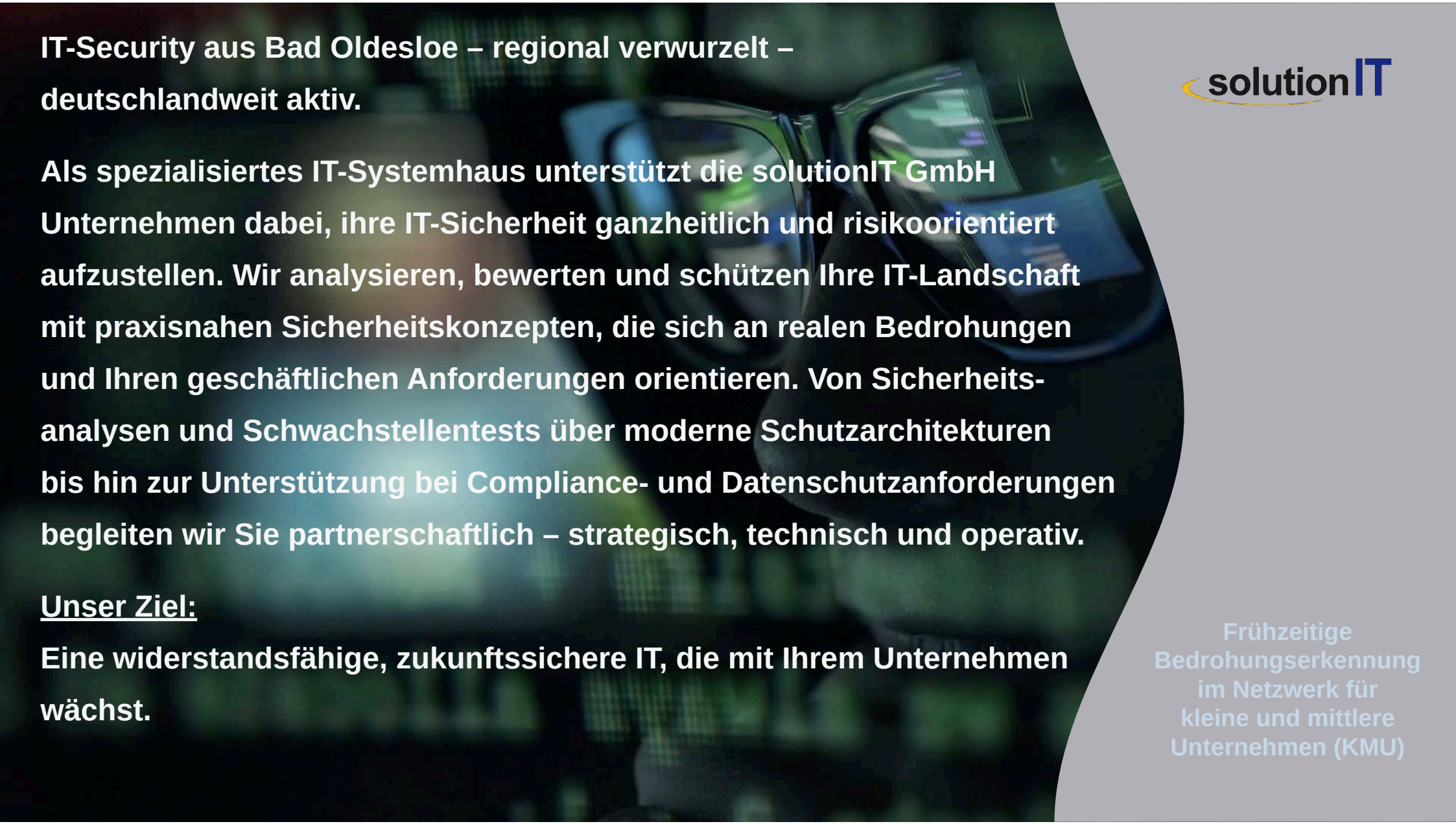
Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU)

IT4B Digital Summit 2026
24.06.2026 – 14:00 Uhr – Red Stage

Olaf Otahal – solutionIT GmbH



IT-Security aus Bad Oldesloe – regional verwurzelt – deutschlandweit aktiv.

Als spezialisiertes IT-Systemhaus unterstützt die solutionIT GmbH Unternehmen dabei, ihre IT-Sicherheit ganzheitlich und risikoorientiert aufzustellen. Wir analysieren, bewerten und schützen Ihre IT-Landschaft mit praxisnahen Sicherheitskonzepten, die sich an realen Bedrohungen und Ihren geschäftlichen Anforderungen orientieren. Von Sicherheits-analysen und Schwachstellentests über moderne Schutzarchitekturen bis hin zur Unterstützung bei Compliance- und Datenschutzanforderungen begleiten wir Sie partnerschaftlich – strategisch, technisch und operativ.

<u>Unser Ziel:</u>
Eine widerstandsfähige, zukunftssichere IT, die mit Ihrem Unternehmen wächst.

solutionIT

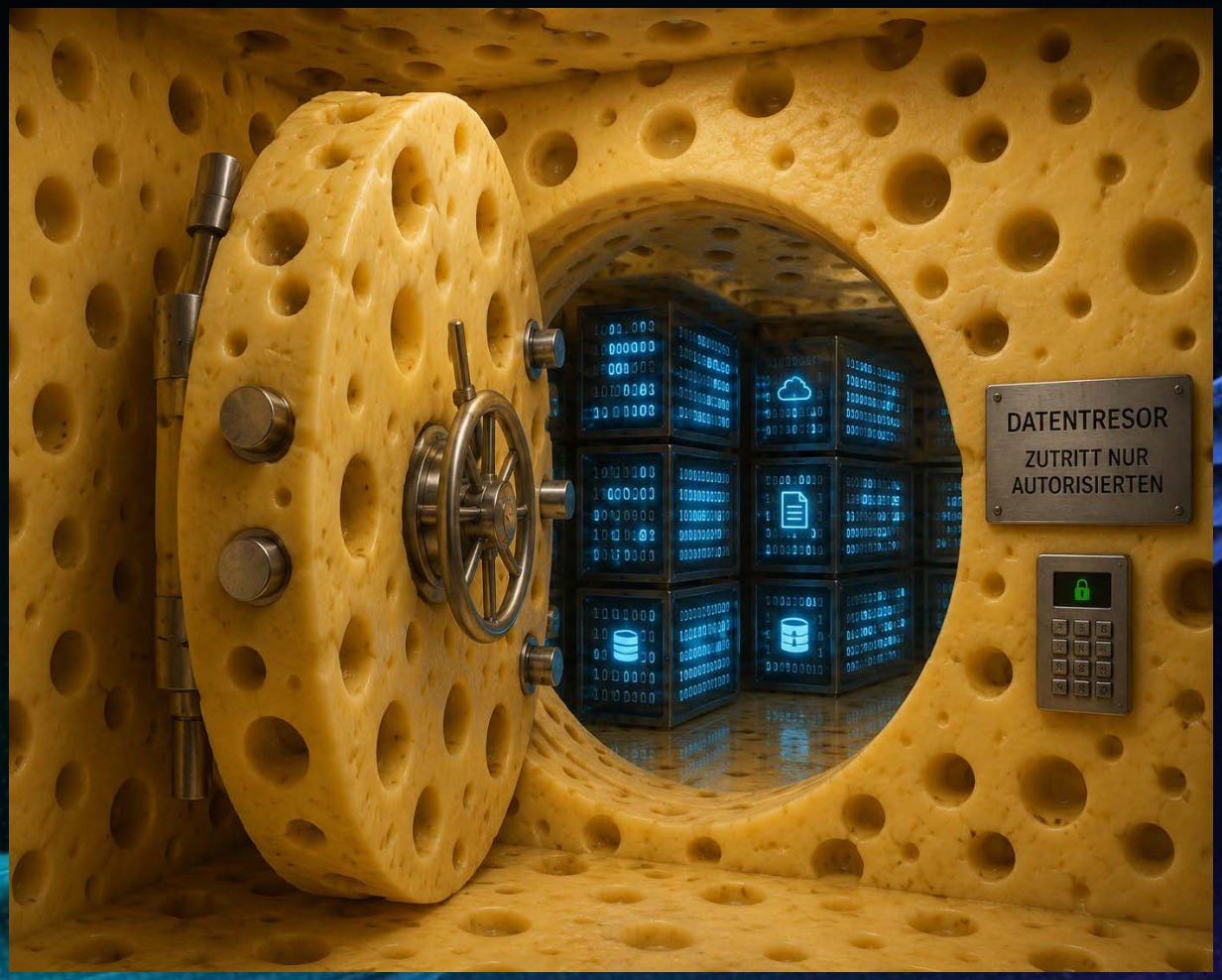
Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU)

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU)

WIE?

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Ziele

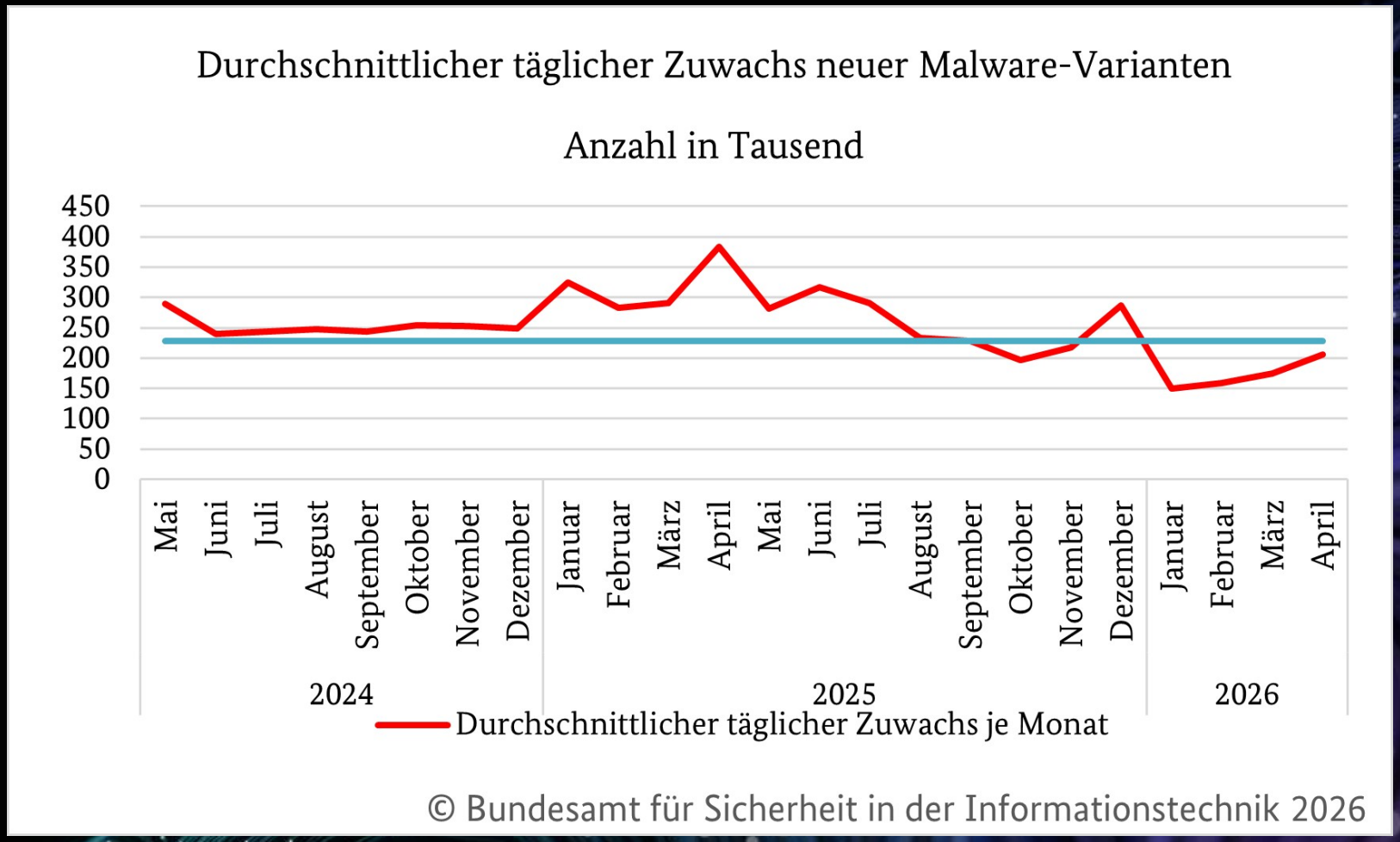


solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Ziele

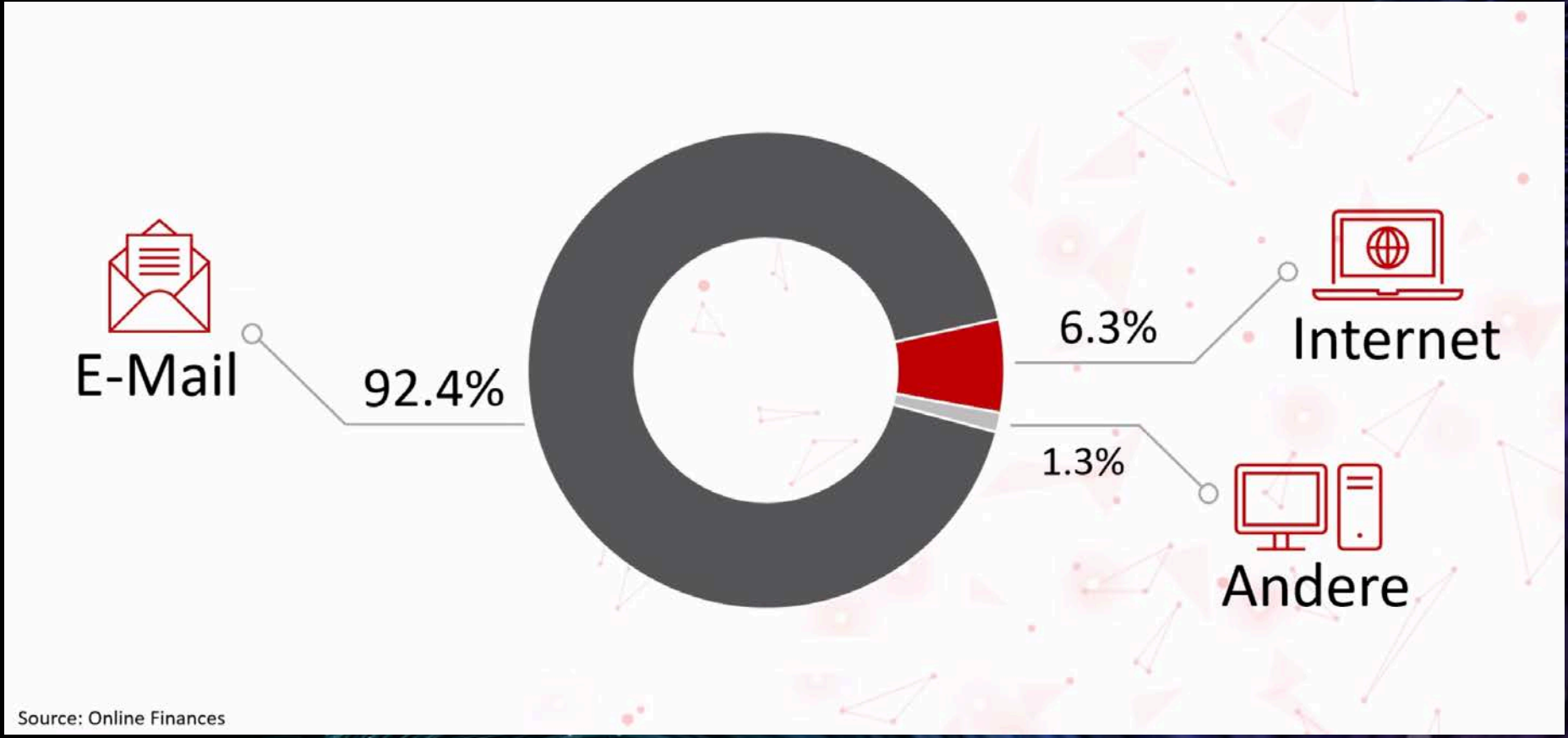
solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum



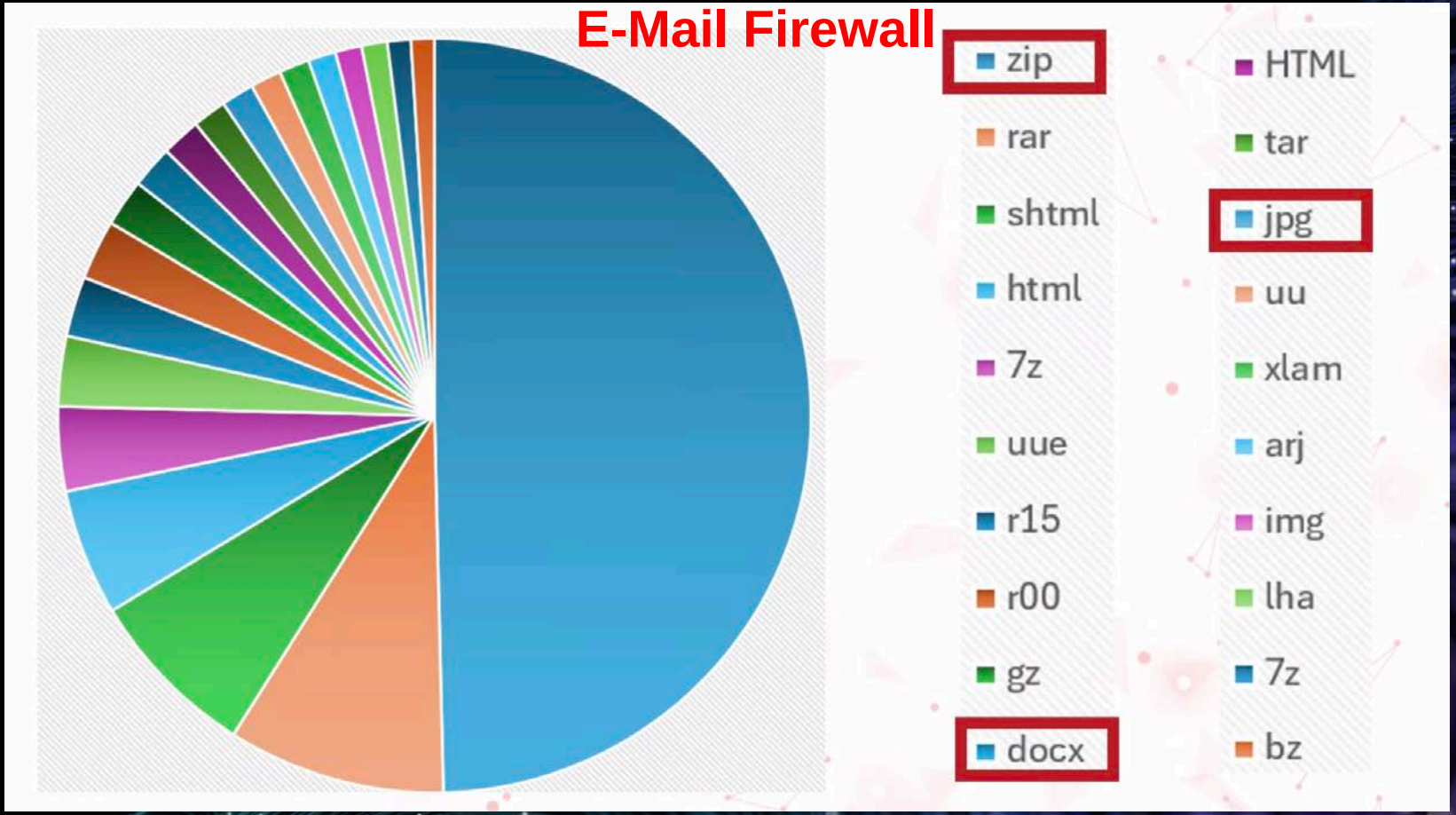
solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum



solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum



solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

- Vom Einzeltäter zur organisierten Cyberökonomie
- Cybercrime als digitaler Dienstleistungsmarkt
- Von Einzelangriffen zu arbeitsteiligen Lieferketten
- Daten, Zugänge und Automation als Kernressourcen

Warum gerade jetzt?

Aktuelle Kennzahlen zur Untergrundökonomie

- Ransomware-Angriffe + 25%
- 43% mehr Breach-Diskussionen in Untergrundforen
- 2,9 Mrd. kompromittierte Credentials auf illegalen Märkten

Quelle: bitsight.com

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Von der Statistik zur Realität

- Leaks werden zum Startpunkt, nicht zum Endpunkt
- Daten wandern durch mehrere Hände und Geschäftsmodelle
- Ein Vorfall kann mehrfach monetarisiert werden

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Die Underground Cyber-Economy als vernetztes Ökosystem

- Verdecktes Ökosystem rund um Daten und Zugänge
- Zusammenspiel von Foren, Marktplätzen und Leak-Sites
- Fokus: Handel, Vermittlung, Service

solutionIT

Digitale „Warenkörbe“

Welche Güter im Untergrund gehandelt werden

Element	Typischer Preis	Warum es wertvoll ist	Bittere Wahrheit
Kreditkarte (basic)	5 $ – 20 $	Sofortiges Betrugspotenzial	Günstiger als dein Netflix-Abo
Kreditkarte mit CVV	30 $ – 150 $	Identitätsdiebstahl, größerer Betrug	Preis variiert je nach Kreditlimit
Sozialversicherungsnummer	1 $ – 10 $	Identitätserstellung / Kredite	Deine Identität kostet weniger als ein Burger 🍔
E-Mail- und Passwort-Kombi	0,001 $	Credential-Stuffing-Angriffe	Milliardfach verkauft. 1.000 Logins für 2 $.
Unternehmens-VPN-Zugangsdaten	500 $ – 5.000 $	Netzwerkzugang für Ransomware	„Initial Access Brokers“ sind darauf spezialisiert

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Warum Identitäten zur Hauptwährung werden

Zugang schlägt Schadcode

- Zugang wirkt oft leiser und glaubwürdiger
- Sessions umgehen technische Schutzmechanismen
- Identität als wichtigste Angriffsfläche

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Business-Logik im Untergrund

Spezialisierung, Skalierung, Risikoteilung

- Spezialisierung statt Alleskönner
- Wiederverwendung von Daten über mehrere Kampagnen
- Risikoteilung und Affiliate-Modelle

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Die Rollen im Schattenmarkt

Wer welche Aufgabe übernimmt

- Initial Access Broker
- Malware-Entwickler und Exploit-Anbieter
- Phisher, Datenhändler, Ransomware-Affiliates

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Infrastruktur der Underground-Märkte

Wohin die Daten wandern

- Untergrundforen und geschlossene Communities
- Darknet-Marktplätze und Leak-Sites
- Broker-Plattformen für Zugänge und Datensätze

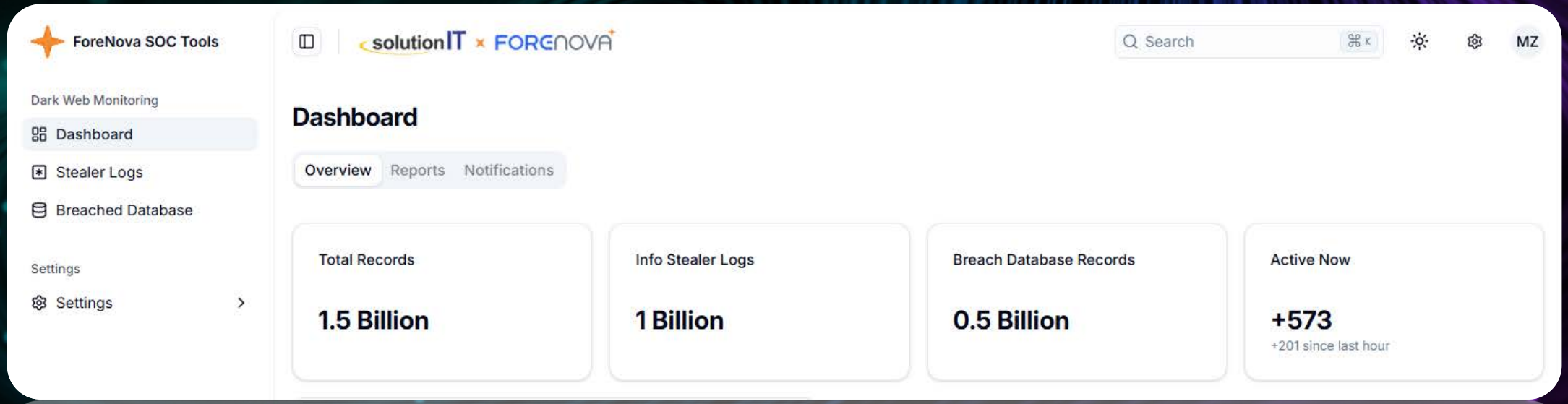
solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Dark-Web-Scans als Schaufenster der Schattenökonomie

- Sichtbar: Domains, Nutzer, Services, Zeitpunkte
- Häufig Kombination aus alten und neuen Leaks
- Relevanz für Exposure- und Risikoanalyse

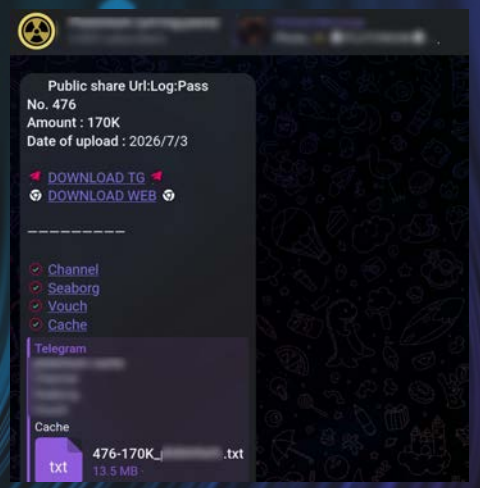
solutionIT

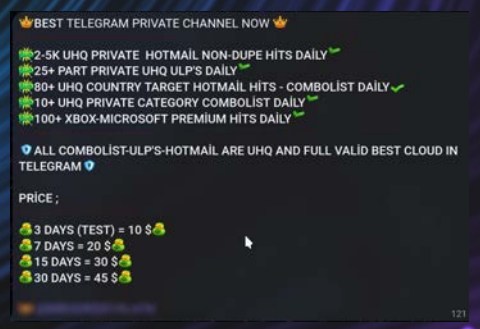


Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Cybercrime-Marktplätze

Wie professionelle Plattformen im Verborgenen funktionieren





solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Cybercrime-as-a-Service

Wenn kriminelle Fähigkeiten zum Service werden

- Fähigkeiten werden als Services angeboten
- Angriffe werden modular und skalierbar
- Einstiegshürden sinken deutlich

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Malware- und Ransomware-as-a-Service

- Bereitgestellte Builder, Panels und Infrastruktur
- Affiliate-Programme mit Umsatzbeteiligungen
- Ständige Updates und neue Versionen

Angriffe im Abo-Modell

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Typische Angriffsabläufe in der Schattenökonomie

- Einstieg: Phishing, Stealer oder gekaufter Zugang
- Ausweitung und Datensammlung im Ziel
- Monetarisierung: Verkauf, Betrug, Erpressung

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Supply-Chain-Angriffe

Wenn Vertrauen zur Angriffsoberfläche wird

- Angriff über Dienstleister, Software oder Integrationen
- Missbrauch von Update-Mechanismen und Zugriffe
- Schwierige Abgrenzung, weil Vertrauen ausgenutzt wird

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Warum insbesondere Mid-Sized-Unternehmen ins Fadenkreuz geraten

- Attraktive Zielgröße bei moderater Verteidigung
- Viele Integrationen und Dienstleister
- Oft keine 24/7-Security-Kapazität

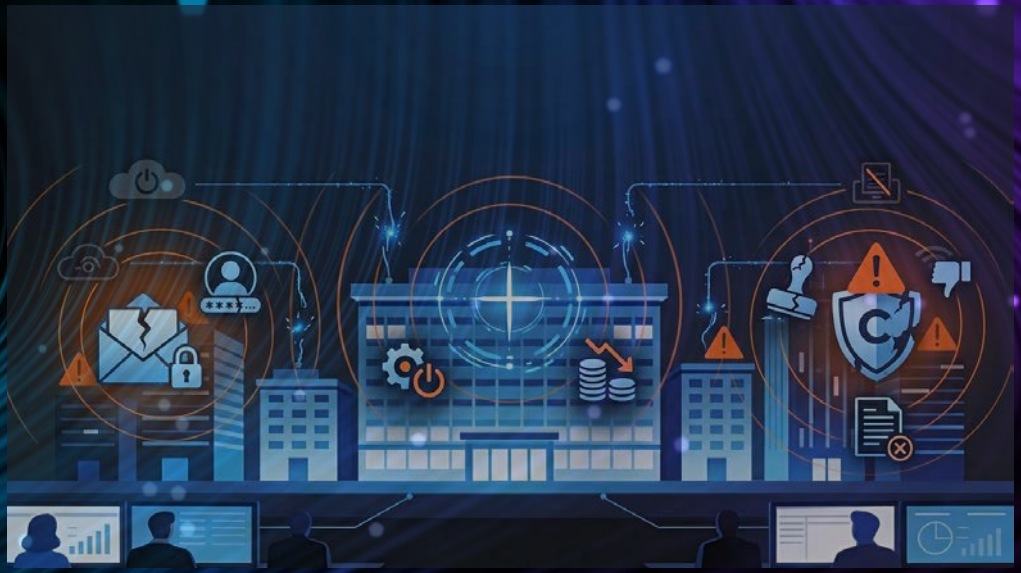
solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Auswirkungen auf Unternehmen

Von BEC bis Betriebsunterbrechung

- Kontoübernahmen und Business Email Compromise
- Betriebsunterbrechungen und Incident-Kosten
- Reputations- und Compliance-Risiken



solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Auswirkungen auf Privatpersonen

Identitätsdiebstahl als Dauerproblem

- Identitätsdiebstahl und Finanzbetrug
- Missbrauch von Accounts und persönlichen Beziehungen
- Langfristige Risiken durch Datenpersistenz

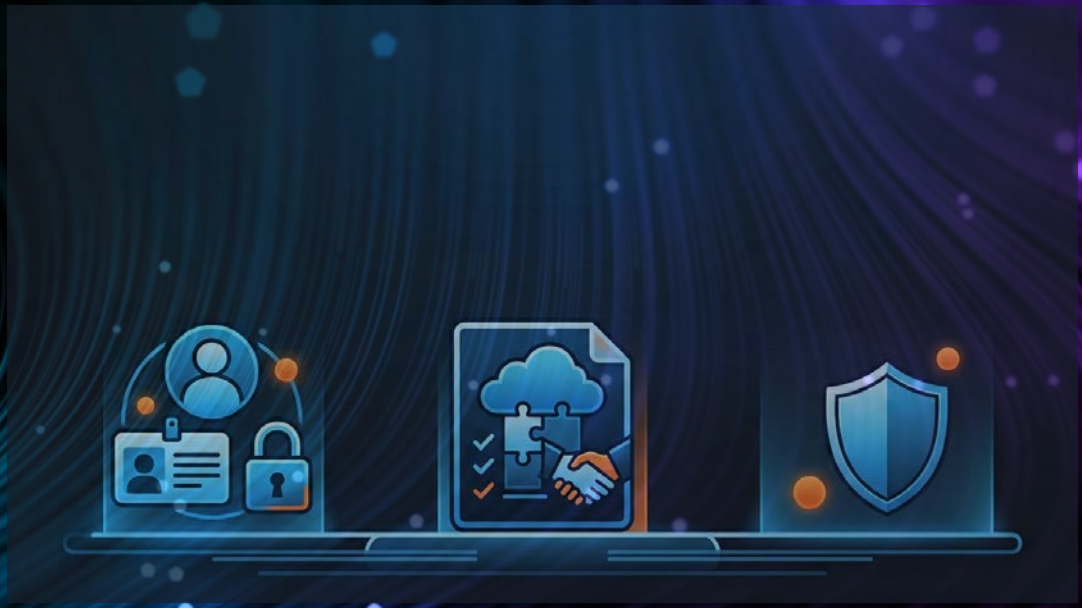
solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Warum

Regeln als Sicherheitsfaktor

- Klare Regeln für Zugriff und Identitäten
- Richtlinien für Drittanbieter und Tool-Nutzung
- Regeln für Umgang mit sensiblen Daten

Die Rolle von Policies



solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU)

Warum

- Bedrohungen nehmen zu
- Daten sind wertvoll
- Gesetze & Compliance werden strenger
- Ausfälle kosten Zeit und Geld

Ziele

- Daten & Systeme sicher schützen
- Verfügbarkeit & Stabilität gewährleisten
- Effizienz steigern & Kosten senken
- Vertrauen schaffen & Wettbewerbsvorteile sichern
- Zukunftsfähig & skalierbar wachsen

Wie

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Wie

Technische Schutzmaßnahmen gegen die Schattenökonomie

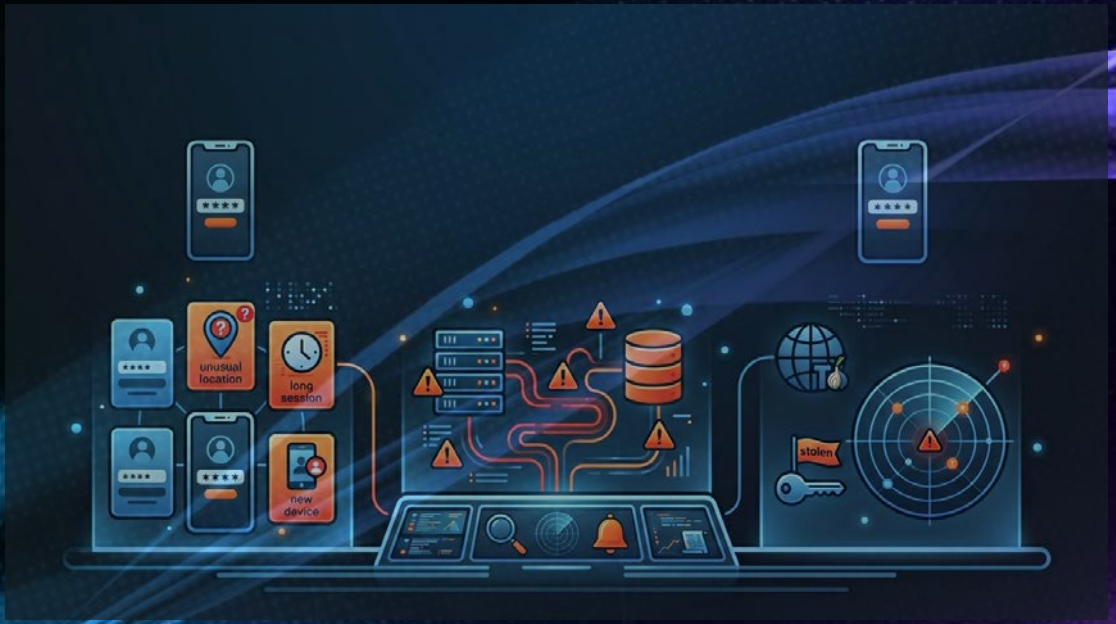
- Phishing-resistente MFA und Zero-Trust
- Monitoring für geleakte Credentials und Dark-Web-Exposure
- Session- und Access-Hygiene plus schnelle Response

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Wie

Welche Anomalien moderne Detection idealerweise erkennt

- Ungewöhnliche Logins und Session-Muster
- Verdächtige Bewegungen in sensiblen Systemen
- Korrelation mit Leak- und Exposure-Signalen



solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Wie

Wie ein modernes MDR Angriffe und Exposure in Kontext setzt

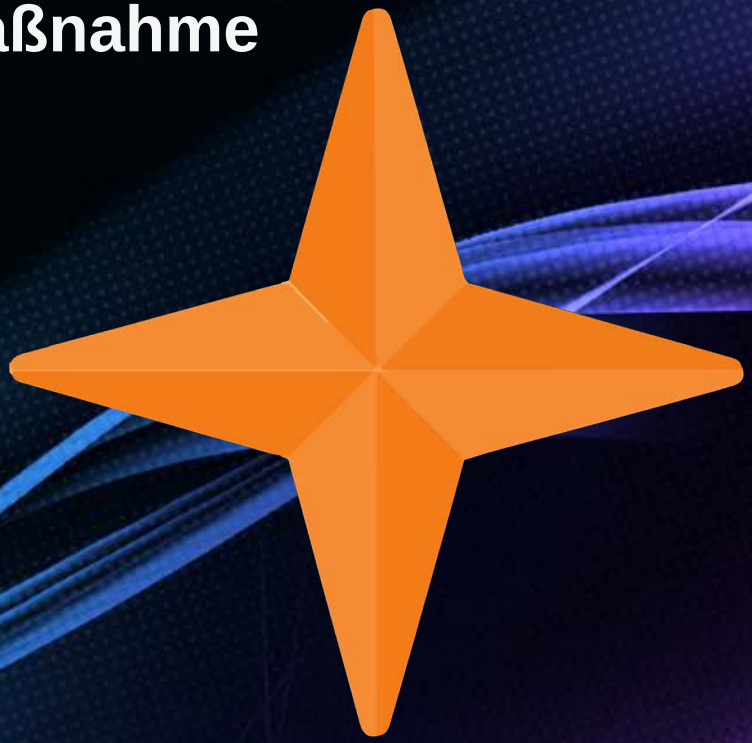
- Sichtbarkeit auf Exposure, Anomalien und Angriffe
- Kontextbildung rund um Identitäten und Systeme
- Ableitung konkreter Maßnahmen in Echtzeit

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Wie

Vom Leak-Signal zur konkreten Gegenmaßnahme

- Leak-/Exposure-Signal erkennen
- Betroffene Konten, Systeme und Drittparteien priorisieren
- Sessions, Credentials und Rechte bearbeiten, Monitoring verstärken



solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Wie

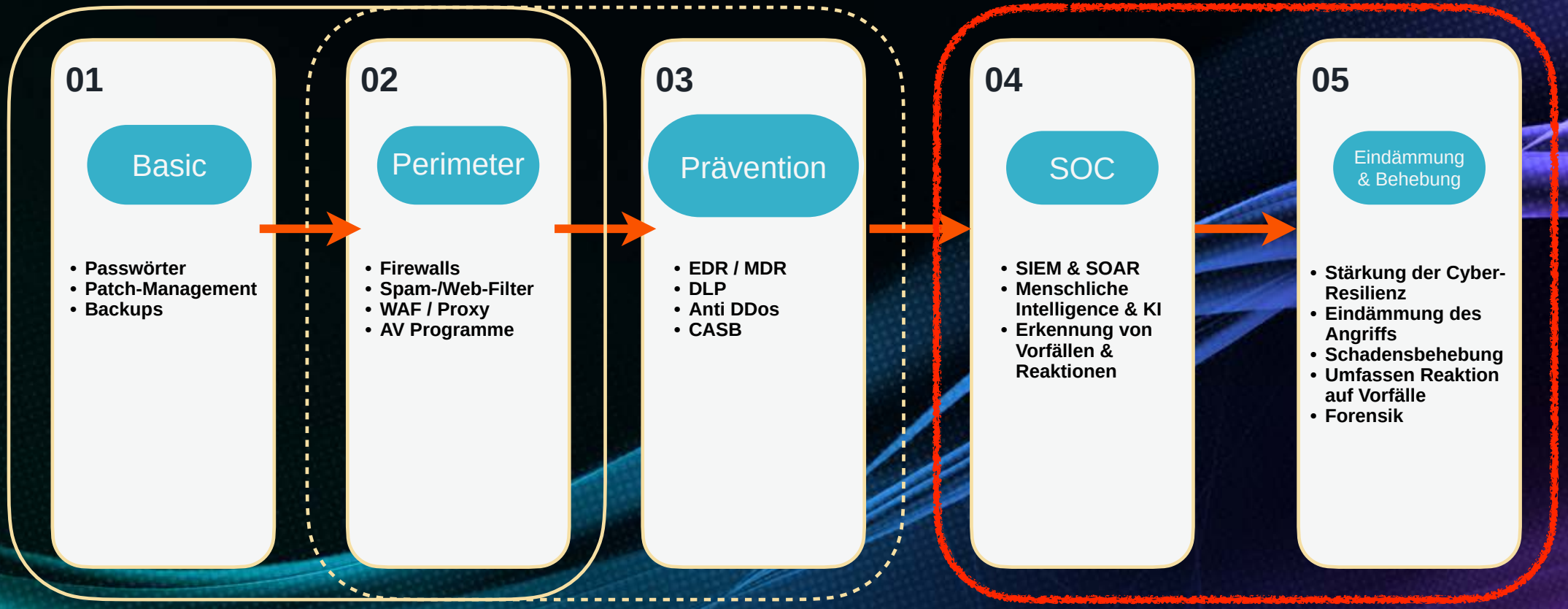
Drei Kernbotschaften für den sicheren Umgang mit der Schattenökonomie

- Cybercrime ist ein Markt, kein Chaos
- Daten = Rohstoff, Zugang = Währung, Automation = Skalierung
- Sichtbarkeit, Regeln und schnelle Reaktion sind entscheidend

solutionIT

Frühzeitige Bedrohungserkennung im Netzwerk für kleine und mittlere Unternehmen (KMU) - Wie

Wie gut sind Sie auf Cyberbedrohungen vorbereitet?



solutionIT

Wo die meisten Unternehmen sind

Wo die meisten Unternehmen sein wollen/sollten

MINIMIERE DEINE ANGRIFFSFLÄCHE

STELLE EINE STARKE DEFENSE AUF

IDENTITÄT
Schütze den Zugang

ZUGRIFF
Nur wer muss, hat Zugang

PRIVILEGIEN
Mit minimalen Rechten arbeiten

ÜBERWACHUNG
Erkennen. Reagieren. Verteidigen.

SYSTEME
Härten & aktuell halten

DATEN
Verschlüsseln & sichern

RESPONSE
Vorbereitet sein. Schnell handeln.

VERTEIDIGUNGSPRINZIPIEN

- ✕ Angriffsfläche verkleinern
- ✕ Schwachstellen schließen
- ✕ Kontrolle behalten
- ✕ Früh erkennen
- ✕ Schnell reagieren

ZIEL: KEIN RAUM FÜR ANGRIFFER

MINIMIERE DEINE ANGRIFFSFLÄCHE

solutionIT

DEINE DEFENSSIVE ERGEBNISSE

WENIGER RISIKEN
Weniger Einfallstore für Angreifer

MEHR SICHERHEIT
Schütze was zählt: Daten, Systeme, Menschen

MEHR EFFIZIENZ
Weniger Vorfälle. Weniger Unterbrechungen.

MEHR ERFOLG
Sichere Basis für nachhaltiges Wachstum


Wenn Sie Fragen haben...
solutionIT
Kommen Sie zu uns auf den Stand
2+3
und informieren sich über erstklassige Mail-Security und Managed Detection & Response Lösungen und testen Sie Ihre Domain in unserem kostenlosen Dark-Web-Scan


solutionIT
Vielen Dank für Ihre Aufmerksamkeit