Controlware Security Day 2022

tenable

EXPOSURE-MANAGEMENT AUF DER GESAMTEN MODERNEN ANGRIFFSOBERFLÄCHE

DIE MODERNE ANGRIFFSOBERFLÄCHE

3 Attribute der modernen Angriffsoberfläche führen dazu, dass sie schwieriger denn je zu verteidigen ist:

1. RAPIDES **WACHSTUM**
2. HOHE **DYNAMIK**
3. ZUNEHMENDE **VERNETZUNG**

tenable

UMGANG MIT GEFÄHRDUNGEN AUF DER GESAMTEN MODERNEN ANGRIFFSOBERFLÄCHE

EXPOSURE-MANAGEMENT

Transparenz über die gesamte moderne Angriffsoberfläche – mit Informationen zur Priorisierung von vorbeugenden Maßnahmen und zur Kommunikation von Risiken an alle Unternehmensebenen

SOFTWARE-SCHWACHSTELLEN	EXTERNE ANGRIFFS-OBER-FLÄCHE	ANWENDUNGS-SCHWACHSTELLEN	PUBLIC CLOUD KONFIGURATION	OT-SCHWACHSTELLEN	ZUGRIFFS-RECHTE
On-Prem- & Remote-IT	Assets mit Internetan-bindung	Web-Apps/ APIs	Public Cloud	Industrielle (OT-) Infrastruktur	Identitäten

tenable

TENABLE-VORREITERSCHAFT: VON SCHWACHSTELLEN-MANAGEMENT HIN ZU EXPOSURE-MANAGEMENT

MARKT-FÜHRERSCHAFT

Platz 1

Marktanteil im Bereich Vulnerability Management

3 Jahre in Folge

IDC

FORSCHUNGS-TIEFE

„Tenable hat ein eigenes Forschungsteam und kann neue Erkennungen meist innerhalb von 24 Stunden nach dem Auftreten neuer Schwachstellen entwickeln."

IDC

WACHSENDES BETÄTIGUNGSFELD

Einstufung als Leader in „Forrester Wave for ICS Security Solutions"

FORRESTER®

Einstufung als CNAPP- und Active Directory Defense-Anbieter

Gartner

tenable

DAS TENABLE-PORTFOLIO

tenable

SCHWACHSTELLEN-MANAGEMENT

Die moderne Angriffsoberfläche wächst kontinuierlich – und mit ihr auch die Anzahl der Schwachstellen. Es wird für Unternehmen immer schwieriger, mit dieser zunehmenden Menge und Vielfalt Schritt zu halten, und Maßnahmen entsprechend korrekt zu priorisieren.

Nicht bewertete Assets und Schwachstellen erhöhen das Unternehmensrisiko und machen es anfällig für Angriffe. Parallel dazu führt eingeschränkte Priorisierung zu Ineffizienz in Sicherheitsprozessen.

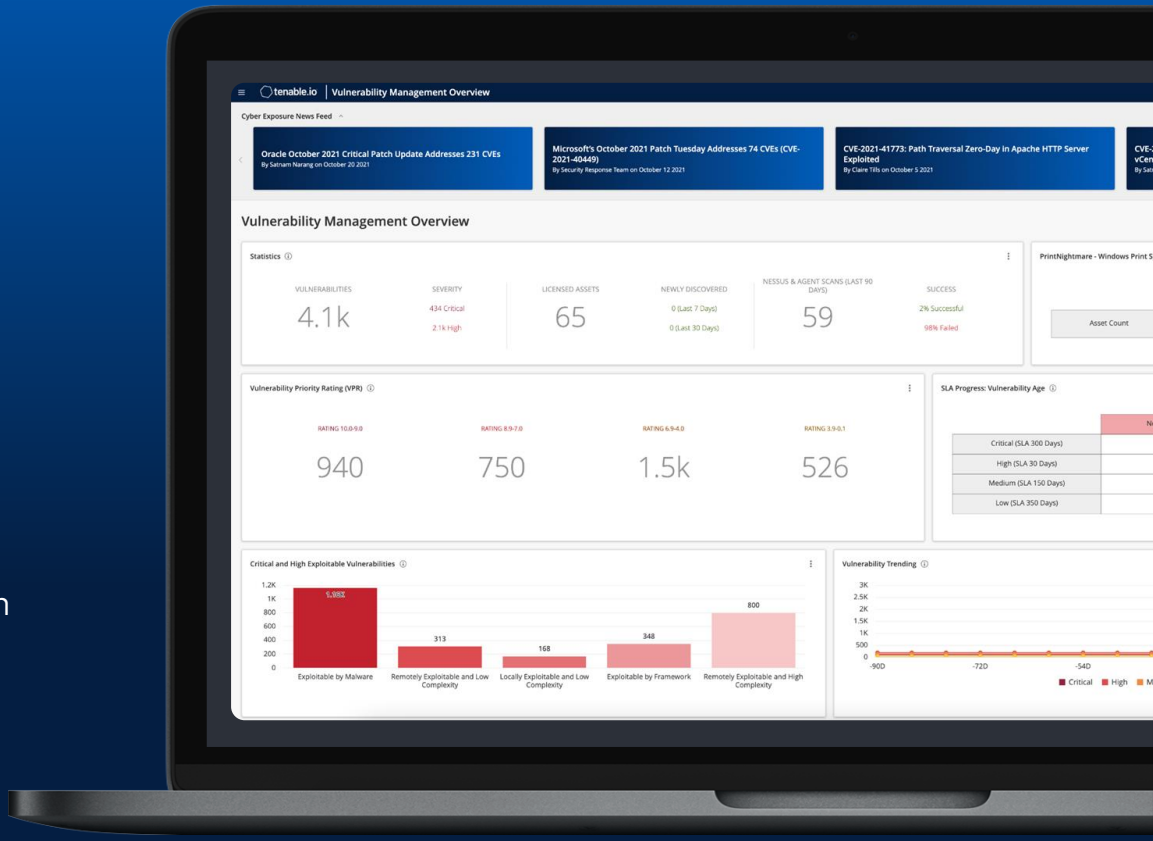
tenable

tenable.io
vulnerability management

Cloudbasiertes Schwachstellen-Management

WARUM TENABLE?

- Bessere Schwachstellen-Abdeckung und schnelle Unterstützung bei kritischen Sicherheitsvorfällen
- Multiple Sensortechnologien für einen tieferen Einblick in sämtliche Asset-Typen
- Risikobasierte Priorisierung, damit Sicherheitsteams sich auf diejenigen Schwachstellen konzentrieren, deren Ausnutzung am wahrscheinlichsten ist



tenable

ATTACK SURFACE MANAGEMENT

Da die moderne Angriffsoberfläche immer größer wird, verfügen die meisten Unternehmen heute über eine beträchtliche Anzahl von Assets mit Internetanbindung, von denen sie nicht einmal wissen, dass sie existieren – geschweige denn, ob sie für Angriffe anfällig sind.

Durch diese unbekannten oder unzureichend verstandenen Assets entsteht eine neue Risikodimension, denn sie sind leichte Ziele für Bedrohungsakteure und bieten ihnen die Möglichkeit, unbemerkt auf Assets zuzugreifen.

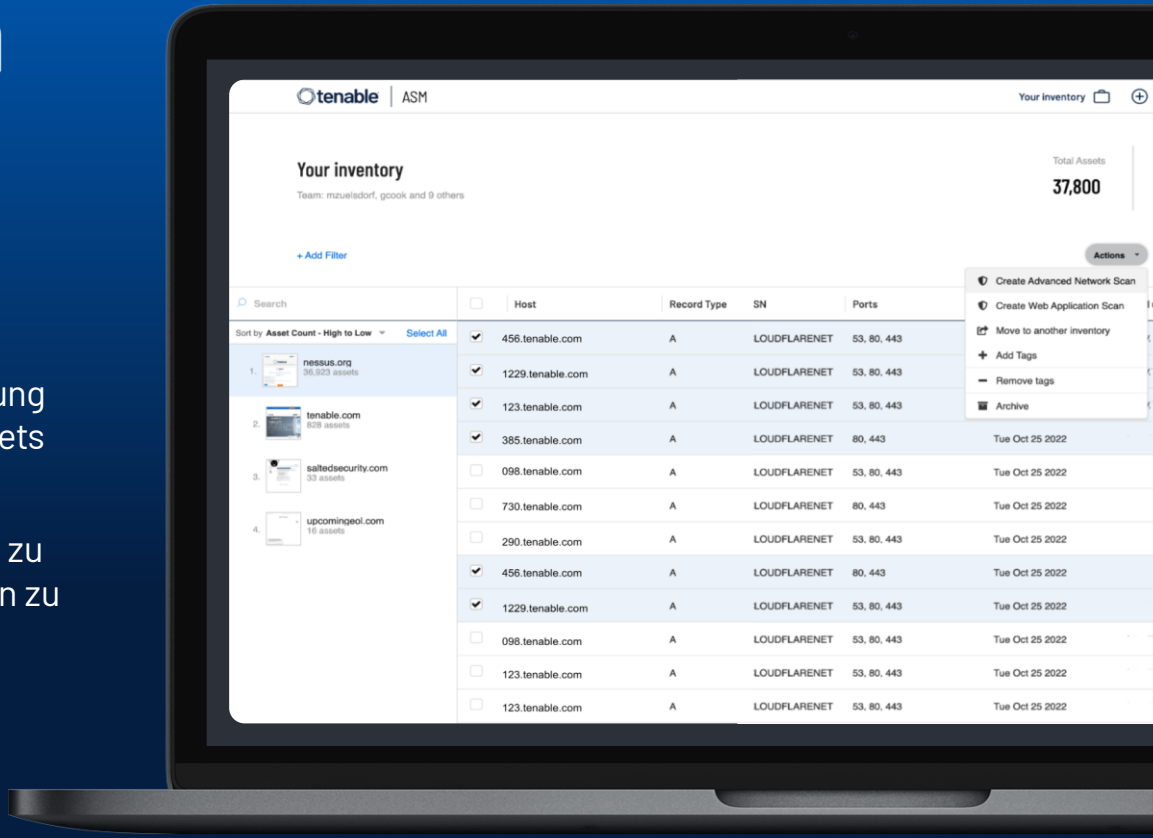
tenable

tenable.asm
attack surface management

Attack Surface Management

WARUM TENABLE?

- Präzise Sichtbarkeit und Inventarisierung der mit dem Internet verbundenen Assets eines Unternehmens
- Schnelle Erfassung, um blinde Flecken zu beseitigen und das Ausmaß von Risiken zu erkennen
- Integration in Tools und Prozesse des Schwachstellen-Managements



tenable

Die Sichtbarkeitslücke: Hintergründe

Sichtbarkeit ist für Cybersecurity von grundlegender Bedeutung

NIST Cybersecurity Framework

Grundlegende

1. Inventarisierung und Kontrolle von Hardware-Assets
2. Inventarisierung und Kontrolle von Software-Assets

CIS Controls, Version 8

Doch nur wenige Unternehmen haben dieses Problem im Griff

73 sind aufgrund ihrer wachsenden Angriffsoberfläche besorgt

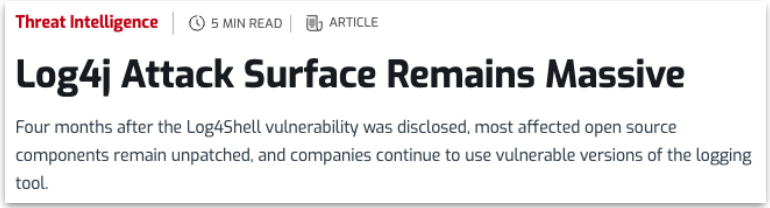
62 % der Angriffsoberfläche ist der Cybersecurity-Branche laut Schätzungen derzeit bekannt

62 % haben blinde Flecken, die Sicherheitsmaßnahmen beeinträchtigen

Quelle: Sapio Research & Trend Micro, April 2022

tenable

Außenstehende **wissen mehr über die Angriffsoberfläche eines Unternehmens** als dessen Mitarbeiter

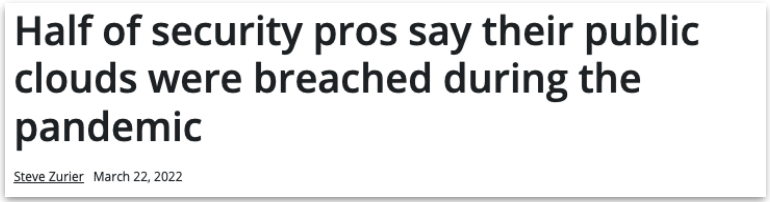


Link

Über 90.000 Server mit Internetanbindung sind weiterhin anfällig

Link

245.000 laufende Kubernetes-Cluster sind öffentlich zugänglich



Link

Unbekannte, nicht verwaltete Daten führen zu Cloud-Risiken durch Schatten-IT

tenable

Wir stellen vor: Tenable.asm

Sämtliche Assets erfassen

Verschaffen Sie sich einen gründlichen Überblick über alle Assets mit Internetanbindung – ob bekannt oder unbekannt.

Geschäftlichen Kontext verstehen

Kategorisieren Sie Assets mithilfe von umfassenden Metadaten und Filtermöglichkeiten.

Ganz einfach auf Cyberrisiken bewerten

Starten Sie neue Scans mit wenigen Klicks, um Gefährdungen nachzuvollziehen.

tenable

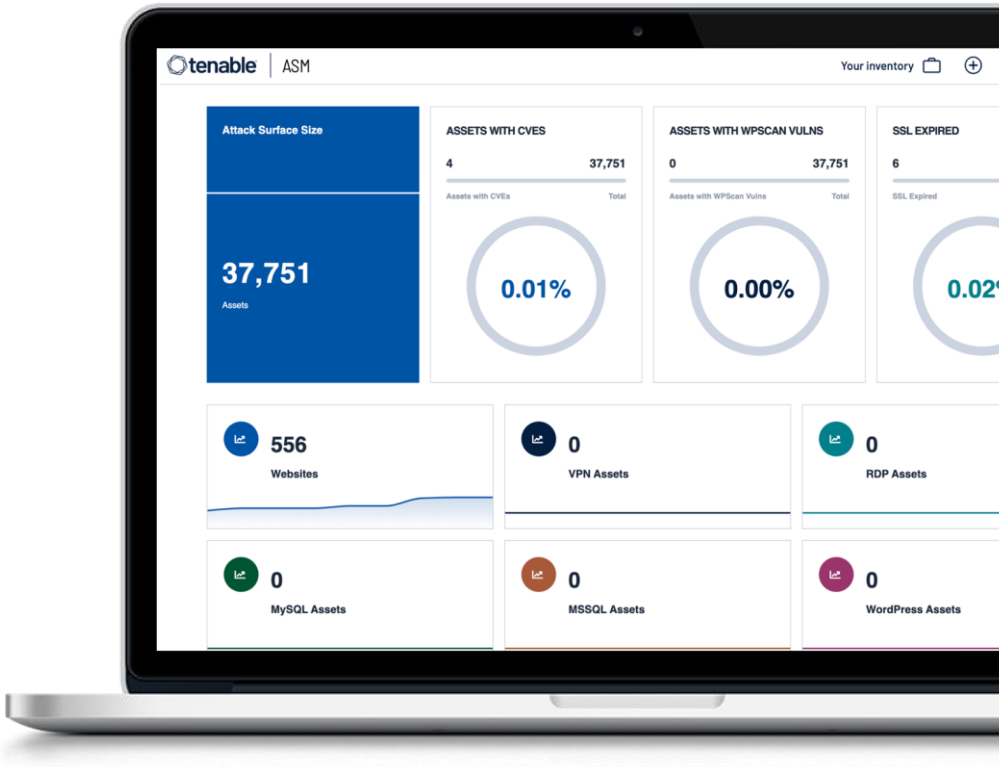
Sämtliche Assets erfassen

Greifen Sie auf eine Karte der Angriffsoberfläche mit mehr als 5 Milliarden Assets zu – bei einer unbegrenzten Anzahl von Top-Level-Domänen.

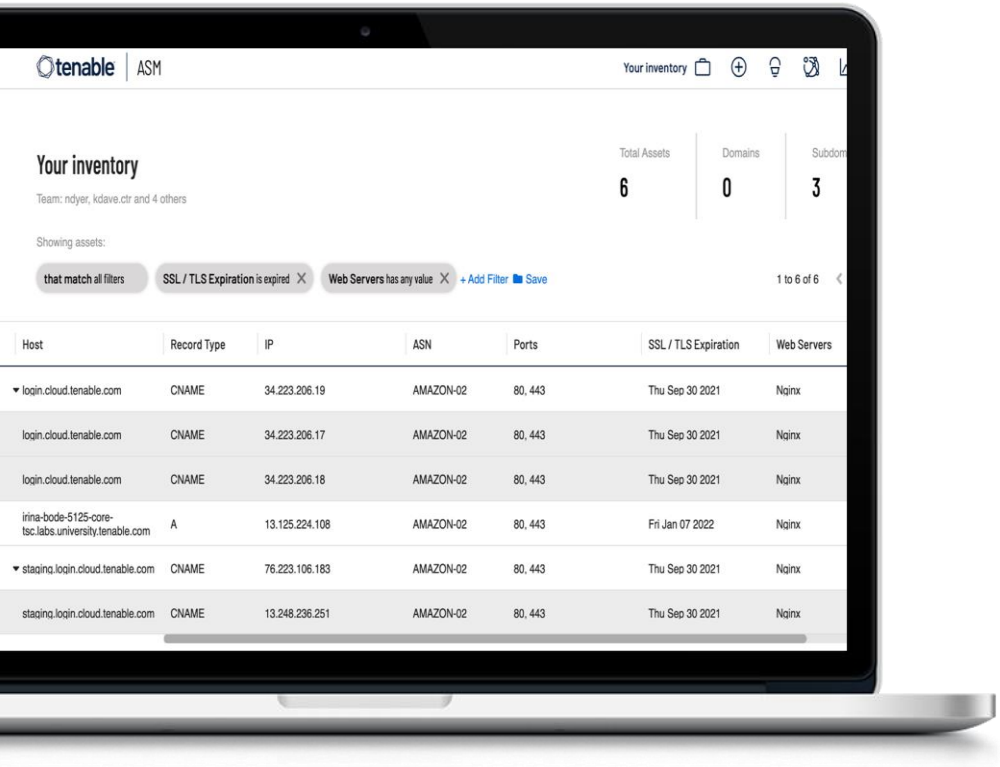
Nutzen Sie mehr als 500 Datenquellen und 200 Internet-Snapshots.

Erfassen Sie vorgeschlagene Domänen, die mit Assets aus Ihrem Bestand in Zusammenhang stehen.

Lassen Sie sich bei Änderungen an Ihrer Angriffsoberfläche benachrichtigen – durch kundenspezifische Subscriptions für kontinuierliches Monitoring.



Geschäftlichen Kontext verstehen



200 Felder mit Metadaten liefern detaillierte Asset-Informationen, mit deren Hilfe Sie fundiertere Entscheidungen treffen können.

Sortieren und filtern Sie Assets ganz einfach anhand von Filtern, Tags, Datentypen und vielem mehr.

Wenden Sie Tags basierend auf Asset-Informationen an, um das Asset-Management zu optimieren.

Machen Sie sich ein Bild von potenziellen Gefährdungen im Zusammenhang mit Technologie-Fingerprinting, Port-Scanning und vielem mehr.

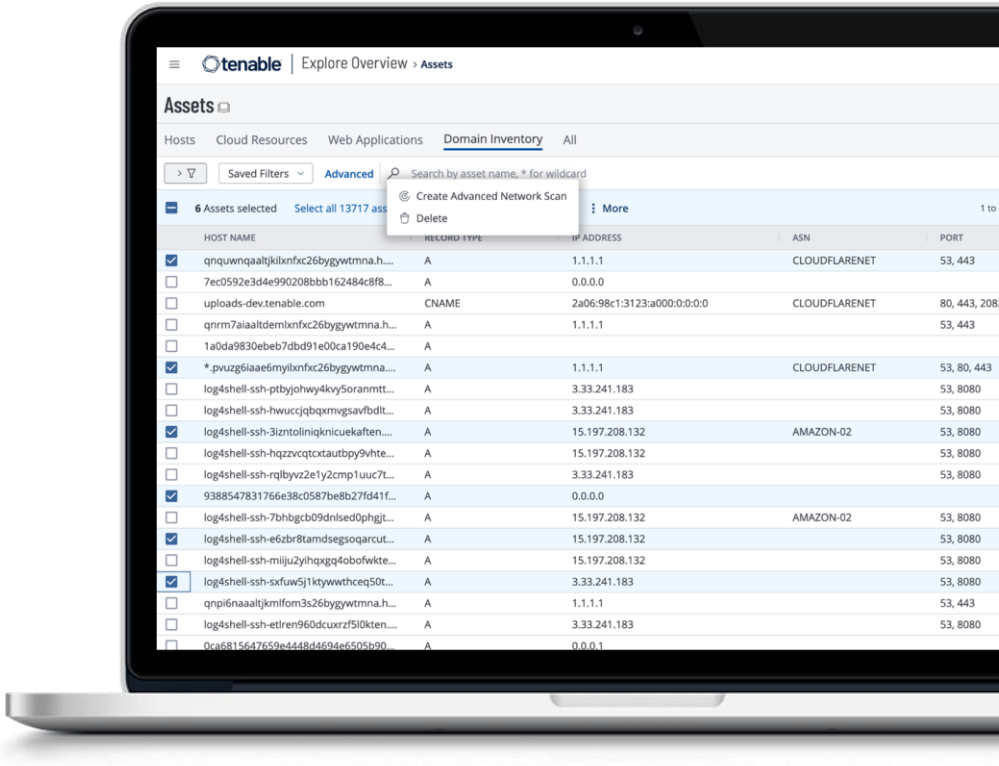
tenable

Ganz einfach auf Cyberrisiken bewerten

Asset- und Exposure-Daten der Angriffsoberfläche sind vollständig in Tenable.io, Tenable.sc und Tenable.ep integriert.

Starten Sie neue Scans von noch nicht bewerteten Assets mit nur wenigen Klicks, um blinde Flecken zu beseitigen.

Bewerten Sie Domänen und Subdomänen über Nessus oder Tenable.io Web Application Scanning und erzielen Sie umfassende Abdeckung.



tenable

Primäre Anwendungsfälle für Tenable.asm

Cybersecurity

Minimieren Sie Risiken und wehren Sie potenzielle Bedrohungen ab, indem Sie alle Ihre Assets genau kennen. Die Ermittlung der Angriffsoberfläche ist entscheidend für die Sicherheitsstrategie.

Schutz Ihrer Marke

Schützen Sie Ihre Marke, indem Sie bereits beendete Marketingkampagnen, Tippfehler, SEO-Gelegenheiten und Missbrauch erkennen.

Fusionen und Übernahmen

Überblicken Sie im Vorfeld einer Übernahme sofort sämtliche Assets mit Internetanbindung eines Zielunternehmens, um Risiken frühzeitig zu erkennen.

Compliance

Finden Sie heraus, wo personenbezogene Daten erfasst und gespeichert werden, um Branchenbestimmungen vollständig einzuhalten.

Wettbewerbsanalyse

Legen Sie die Angriffsoberfläche aktueller und potenzieller Mitbewerber offen, um strategische Chancen zu identifizieren.

Rechtliches

Machen Sie sich ein Bild davon, bei welchen Assets nicht konforme Technologien zum Einsatz kommen oder fehlende Haftungsausschlüsse und abgelaufene Copyright-Hinweise vorliegen.

tenable

ACTIVE DIRECTORY-SICHERHEIT

Für Angreifer ist Active Directory (AD) zum bevorzugten Ziel geworden, um durch Ausnutzung bekannter Schwachstellen und Fehlkonfigurationen Zugriffsrechte zu erwerben, um sich dann im Netzwerk ungehindert fortzubewegen.

In AD kommt es permanent zu Änderungen, Fehlkonfigurationen häufen sich und die Komplexität nimmt zu. Dadurch entstehen neue Angriffswege und Sicherheitsteams sind nicht mehr in der Lage, Schwachstellen aufzuspüren, zu priorisieren und zu beheben, bevor sich daraus geschäftsschädigende Probleme entwickeln.

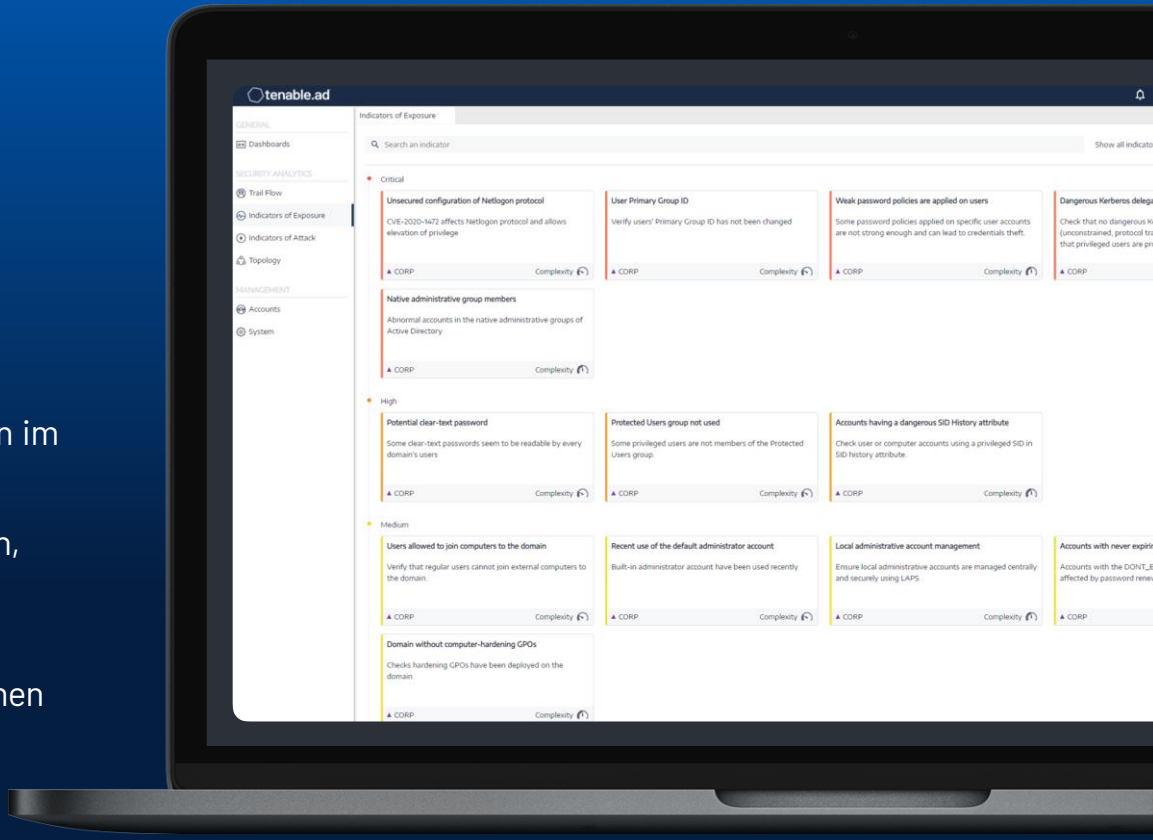
tenable

tenable.ad™
active directory

Active Directory-Sicherheit

WARUM TENABLE?

- Transparenz und Priorisierung für Schwachstellen und Fehlkonfigurationen im Zusammenhang mit AD-Identitäten
- Kontinuierliche Erkennung von Angriffen, um neue Angriffswege sofort zu identifizieren
- Funktionen zum fundierten Nachvollziehen von Aktivitäten in AD



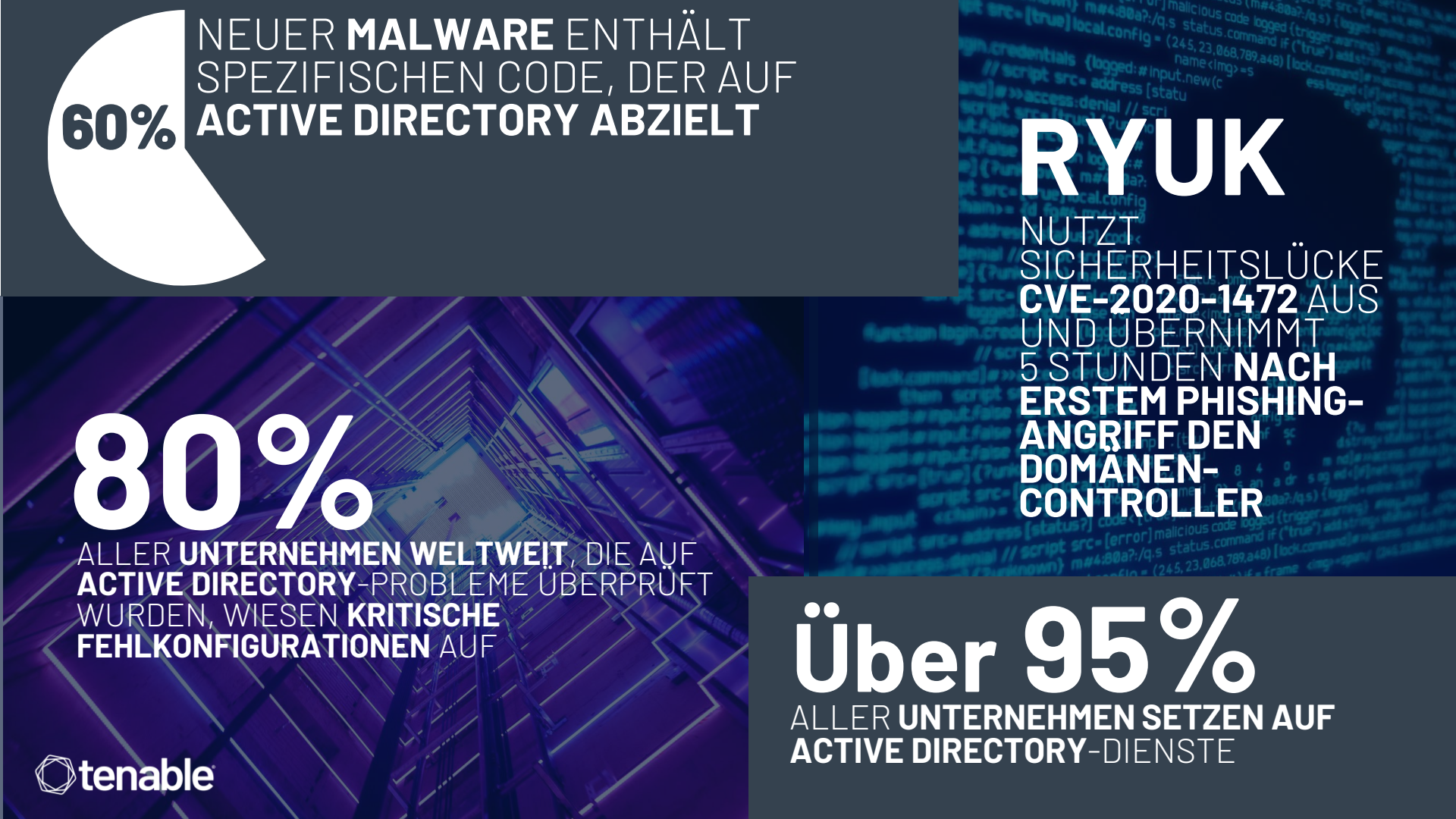
tenable

Active Directory:
Der Schlüssel zu Ihrer Umgebung

- Regelt die Authentifizierung, speichert alle Passwörter
- Verwaltet Zugriffsrechte auf alle wichtigen Assets
- Eine komplexe, sich weiterentwickelnde Architektur, die mit der Zeit unübersichtlich werden kann

HINTER NAHEZU JEDER **DATENPANNE** IN DEN SCHLAGZEILEN STECKT EIN **UNSICHERES ACTIVE DIRECTORY**

tenable

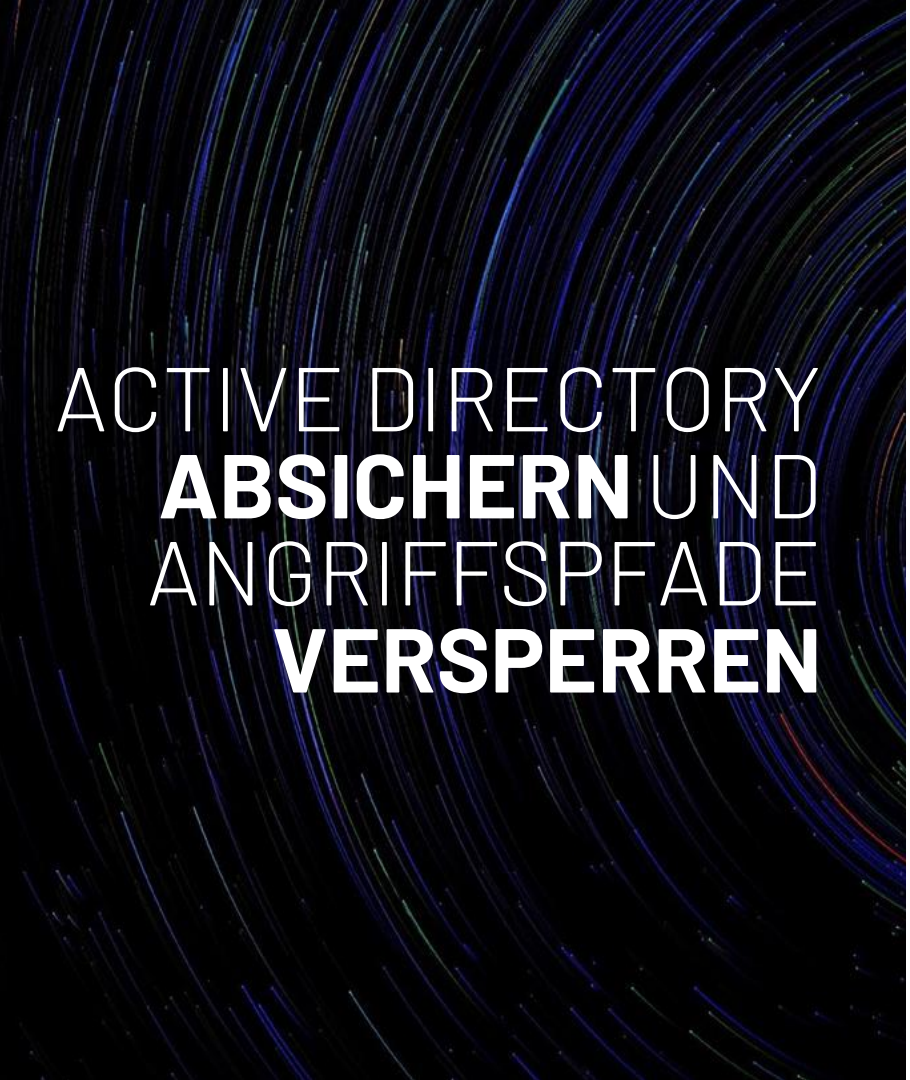

60%
NEUER MALWARE ENTHÄLT SPEZIFISCHEN CODE, DER AUF ACTIVE DIRECTORY ABZIELT
RYUK
NUTZT SICHERHEITSLÜCKE CVE-2020-1472 AUS UND ÜBERNIMMT 5 STUNDEN NACH ERSTEM PHISHING-ANGRIFF DEN DOMÄNEN-CONTROLLER
80%
ALLER UNTERNEHMEN WELTWEIT, DIE AUF ACTIVE DIRECTORY-PROBLEME ÜBERPRÜFT WURDEN, WIESEN KRITISCHE FEHLKONFIGURATIONEN AUF
Über 95%
ALLER UNTERNEHMEN SETZEN AUF ACTIVE DIRECTORY-DIENSTE
tenable

VERSPERREN VON ANGRIFFSPFADEN

Wissen, welche Fehlkonfigurationen und Schwachstellen zur Ausweitung von Rechten in Active Directory genutzt werden

Identifizieren von Indikatoren, die auf eine Rechteausweitung und laterale Bewegung hinweisen

tenable



1

VORHANDENE SCHWACHSTELLEN AUFSPÜREN UND BEHEBEN

- Vorhandene Schwachstellen umgehend erfassen, zuordnen und bewerten
- Schritt-für-Schritt-Taktiken zur Behebung befolgen und Angriffe verhindern

2

NEUE ANGRIFFSPFADE AUFDECKEN

- Neue Schwachstellen und Fehlkonfigurationen kontinuierlich identifizieren
- Übertragungswege von Angriffen unterbrechen und das Bedrohungsrisiko im Zaum halten

3

LAUFENDE ANGRIFFE IN ECHTZEIT ERKENNEN

- Warnmeldungen und umsetzbare Remediation-Pläne bei AD-Angriffen erhalten
- SIEM mit Informationen zu laufenden Angriffen ergänzen

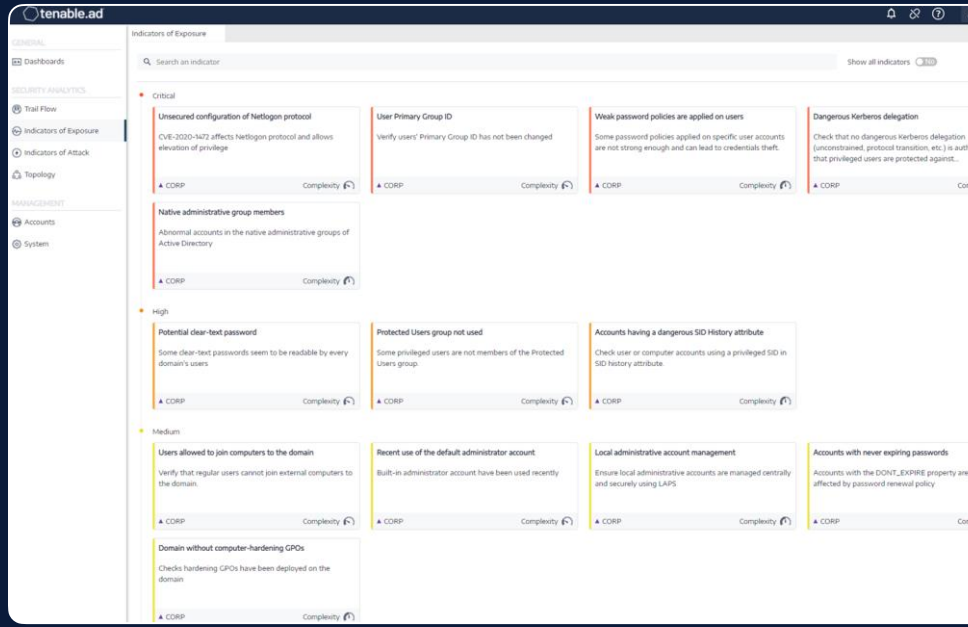
4

VORFÄLLE UNTERSUCHEN UND BEDROHUNGEN ERMITTELN

- AD-Änderungen auf Objekt- und Attributebene suchen und entsprechend korrelieren
- Playbooks mit Reaktionsmaßnahmen im Zuge von SOAR auslösen

tenable.ad

- Erfassen Sie die zugrunde liegenden Probleme, die Ihr Active Directory betreffen
- Identifizieren Sie gefährliche Vertrauensstellungen
- Erkennen Sie sämtliche Änderungen an Ihrem AD
- Durchschauen Sie den Zusammenhang zwischen AD-Änderungen und böswilligen Handlungen
- Analysieren Sie Angriffe bis ins kleinste Detail
- Rufen Sie MITRE ATT&CK-Beschreibungen direkt aus den Detailinformationen zu Vorfällen auf



KEINE AGENTS

KEINE BERECHTIGUNGEN

AD-NATIV

NAHEZU SOFORTIGER NUTZEN

DAS TENABLE-PORTFOLIO

EXPOSURE-MANAGEMENT VON TENABLE

Sichtbarkeit ausweiten | Maßnahmen priorisieren | Risiken kommunizieren

Analyse und Kommunikation von Gefährdungen

- Schwachstellen-Management
- External Attack Surface Management
- Web-App-Sicherheit
- Cloud-Sicherheit
- OT-Sicherheit
- AD-Identitäts-sicherheit

tenable

SCHÜTZEN SIE IHRE MODERNE ANGRIFFSOBERFLÄCHE

Transparenz über die gesamte moderne Angriffsoberfläche erzielen

Bedrohungen antizipieren und Maßnahmen priorisieren, um Angriffe zu verhindern

Expositionsrisiken kommunizieren, um bessere Entscheidungen zu treffen

Besuchen Sie uns an unserem Stand

tenable

tenable

VIELEN DANK!