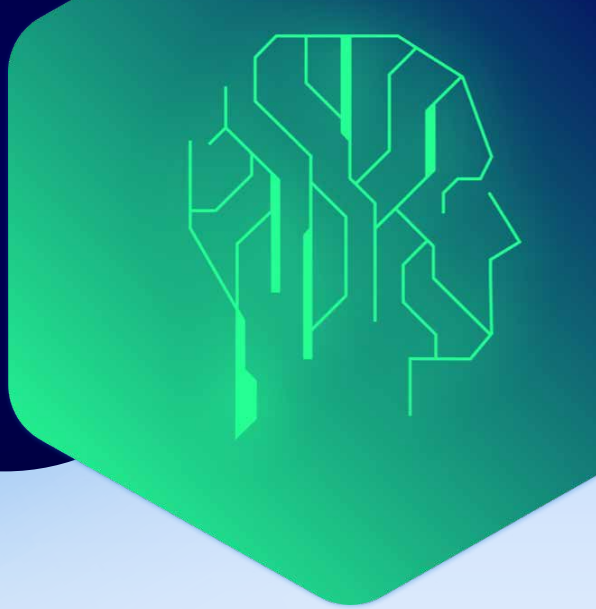
tenable | Datenblatt

Identity Exposure

Unverzichtbarer Schutz vor Identitätsrisiken



Identitäten sind der neue Perimeter – kompromittierte Identitäten stehen im Mittelpunkt fast jedes erfolgreichen Cybersecurity-Angriffs. Active Directory und Entra ID gehören zu den bevorzugten Zielen von Angreifern, die die komplexen Beziehungen zwischen Objekten, Berechtigungen und Entitäten mithilfe von handelsüblichen Tools – sogenannten Off-the-Shelf-Tools – ausnutzen und dadurch Domänendominanz erlangen können.

Die ständigen Veränderungen in Verzeichnisdiensten schränken zudem die Sichtbarkeit der gesamten Angriffsfläche ein und führen laufend zu neuen Einfallstoren für Angriffe. Nur wenige Sicherheitsteams verfügen über genügend Einblick und Kontext, um die große Angriffsfläche von Verzeichnisdiensten abzusichern. Die von ihnen häufig eingesetzten Tools liefern nur eine Momentaufnahme, wodurch Sicherheit zu einem beweglichen Ziel wird.

Noch schlimmer ist jedoch, dass sich die durchschnittliche Zeit bis zur Erkennung eines Übergriffs im Zusammenhang mit kompromittierten Zugangsdaten auf 243 Tage und die durchschnittliche Zeit bis zu dessen Eindämmung auf 84 Tage beläuft, wie aus dem Cost of a Data Breach Report 2022 von IBM hervorgeht. Das wiederum bedeutet, dass erfolgreiche Angreifer unter Umständen fast ein Jahr Zeit haben, um den wichtigsten Dienst in modernen Unternehmen zu beeinträchtigen.

Tenable Identity Exposure ist eine Sicherheitslösung ganz ohne Agents, die durchgängigen Schutz vor identitätsbasierten Angriffen bietet. Sie validiert die Sicherheitslage von Verzeichnisdiensten kontinuierlich und benachrichtigt Sie umgehend, wenn diese angegriffen werden. Darüber hinaus bietet Tenable Identity Exposure priorisierte Schritt-für-Schritt-Anleitungen zur Risikominderung, stuft Ihre risikoreichsten Identitäten anhand von Risiko-Scores ein und stellt Angriffspfad-Visualisierung bereit. Durch Isolation und Beseitigung der Sicherheitslücken bei Identitäten stärkt Tenable Identity Exposure Ihre allgemeine Sicherheitslage – für ein identitätsorientiertes Unternehmen.

Wichtige Vorteile

- **Vorhersagen und Priorisieren**
  Stufen Sie jede Identität anhand eines Risiko-Scores ein, um aufzudecken, wo sich Ihre risikoreichsten Identitäten befinden, und priorisieren Sie Behebungsmaßnahmen dort, wo es am wichtigsten ist.
- **Umfassende Sichtbarkeit**
  Verschaffen Sie sich tieferen Einblick, bewerten Sie sämtliche Personen- und Maschinenidentitäten und priorisieren Sie präventive Sicherheitsmaßnahmen mithilfe von Risikobewertungen, um aufzudecken, wo sich Ihre risikoreichsten Identitäten befinden. Visualisieren Sie komplexe Beziehungsgeflechte in Domänen und Gesamtstrukturen.
- **Visualisieren von Angriffspfaden**
  Beseitigen Sie Angriffspfade mithilfe einer Echtzeit-Darstellung von Pfaden, die zu Domänendominanz führen.
- **Keine Agents**
  Durch eine schnelle und reibungslose Bereitstellung, die weder Agents noch Administratorrechte erfordert, sind Ergebnisse umgehend verfügbar.
- **Sofortige Erkennung von Angriffen**
  Profitieren Sie von Angriffserkennung in Echtzeit inklusive Zuordnung zum MITRE ATT&CK-Framework sowie vollständiger SIEM- und SOAR-Integration.

Wichtige Funktionen

- **Identitätsvereinheitlichung und Risikopriorisierung**
  Bauen Sie Silos bei Unternehmensidentitäten ab und vereinheitlichen Sie sämtliche Identitäten in Active Directory-, Hybrid- und Entra ID-Umgebungen, um die tatsächlichen Gegebenheiten im Identitätsbereich ans Licht zu bringen. Gewinnen Sie an einem zentralen Ort die Kontrolle über Identitäten, die sich über mehrere Verzeichnisdienste, Domänen und Gesamtstrukturen verteilen. Priorisieren Sie Behebungsmaßnahmen anhand unseres datenwissenschaftlich untermauerten Identitätsrisiko-Score, der Identitäten nach dem Ausmaß des Risikos für die jeweilige Umgebung bewertet. Optimieren Sie die Effizienz Ihres Teams und konzentrieren Sie Ihre Maßnahmen auf die Minimierung von Geschäftsrisiken und Angriffsprävention.

- **Kontinuierliche Validierung der Sicherheit von Verzeichnisdiensten in Echtzeit**
  Bewerten Sie die Sicherheitslage Ihrer Verzeichnisdienste und decken Sie seit geraumer Zeit bestehende Probleme bei Konfigurationen und Berechtigungen auf, die Identitäten zu einem zentralen Bestandteil der meisten Angriffe machen. Tenable Identity Exposure stellt eine taktische Schritt-für-Schritt-Anleitung zur Verfügung, die betroffene Objekte identifiziert, sodass keine zeitaufwendigen manuellen Berichte oder Skripts notwendig sind.

- **Beseitigung von Angriffspfaden, die zu Domänendominanz führen**
  Gehen Sie den komplexen gegenseitigen Beziehungen zwischen Objekten, Dienstprinzipalen und Berechtigungen auf den Grund und beseitigen Sie Angriffspfade, die zu Domänendominanz führen. Die Angriffspfad-Analyse (Attack Path Analysis, APA) zeigt alle möglichen Schritte auf, mit denen sich Angreifer seitwärts fortbewegen, Zugriffsrechte erhöhen und die Verzeichnisdienste Ihres Unternehmens unter ihre Kontrolle bringen könnten.

- **Angriffserkennung in Echtzeit**
  Im Falle eines Angriffs werden Sie umgehend per Warnmeldung benachrichtigt, darunter bei Credential Dumping-, Kerberoasting-, DCSync-, ZeroLogon- und vielen weiteren Angriffen. Reagieren Sie in Echtzeit auf Angriffe, indem Sie Tenable Identity Exposure mit Ihren SIEM- und SOAR-Lösungen integrieren. Das Forschungsteam von Tenable nimmt regelmäßig Aktualisierungen an Angriffsindikatoren (Indicators of Attack, IoA) vor, sobald neue identitätsbasierte Exploits entdeckt werden.

- **Untersuchen und Informieren**
  Senken Sie den Zeitaufwand bei der Vorfallsreaktion und erfassen Sie alle Änderungen an Active Directory mithilfe des Trail Flow. Informieren Sie Ihre Incident Response-Teams und optimieren Sie Ihre Sicherheitsprozesse mit Echtzeit-Priorisierung und detaillierten Behebungsmaßnahmen.

- **Erhöhen der Passwortsicherheit**
  Verbessern Sie die Passworthygiene in Ihrem Unternehmen und verringern Sie das Risiko von Angriffen im Zusammenhang mit Passwörtern. Prüfen Sie auf Passwörter, die kompromittiert oder an Dritte weitergegeben wurden oder die nicht den Komplexitätsanforderungen entsprechen.

- **Tenable One: Korrelation von Identitätsrisiken in Ihrer Umgebung**
  Dank der Leistungsstärke von Tenable Identity Exposure bietet Tenable One entscheidende Kontextinformationen, die aus Identitäten entlang der gesamten Angriffsfläche von Unternehmen stammen. Dies hilft bei der Priorisierung von präventiven Sicherheitsmaßnahmen, die das Angriffsrisiko senken. Reduzieren Sie den notwendigen Zeit- und Arbeitsaufwand für das Patch-Management, gewinnen Sie ein besseres Verständnis der gesamten Angriffsfläche, beseitigen Sie blinde Flecken und erstellen Sie eine Baseline für effektives Exposure Management.

- **Unterstützt von Tenable Research**
  Unser weltweit anerkanntes Forschungsteam ergänzt Tenable Identity Exposure regelmäßig um neue Angriffserkennungen und Gefährdungsindikatoren (Indicators of Exposure, IoE). Das Team deckt Zero-Day-Schwachstellen auf, erarbeitet Sicherheitsempfehlungen und Behebungsmaßnahmen und veröffentlicht Kurzinformationen und Erkenntnisse.

Über Tenable

Tenable®, das Unternehmen für Exposure Management, identifiziert und schließt Sicherheitslücken, die den Wert, die Reputation und die Vertrauenswürdigkeit von Unternehmen gefährden. Die KI-gestützte Exposure Management-Plattform von Tenable bietet umfassende Sichtbarkeit und handlungsrelevante Erkenntnisse entlang der gesamten Angriffsfläche und ermöglicht es Unternehmen, sich vor Cyberangriffen zu schützen – von IT-Infrastrukturen über Cloud-Umgebungen bis hin zu kritischen Infrastrukturen und allen dazwischen liegenden Bereichen. Mehr als 44.000 Kunden weltweit verlassen sich auf Tenable, wenn es darum geht, Sicherheits- und Geschäftsrisiken zu minimieren. Weitere Informationen finden Sie auf de.tenable.com.

Kontakt:

Bitte senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact.

073024