tenable.ad

Absichern von Active Directory und Versperren von Angriffspfaden

Hinter jeder Datenpanne in den Schlagzeilen steckt eine unsichere Bereitstellung von Active Directory (AD). 80 % der Angriffe nutzen AD für Lateral Movement und Rechteausweitung und 60 % der neuen Malware enthält Code, der auf AD-Fehlkonfigurationen abzielt. AD ist zum bevorzugten Ziel für Angreifer geworden, um durch die Ausnutzung bekannter Schwachstellen und Fehlkonfigurationen ihre Zugriffsrechte zu erhöhen und sich lateral im Netzwerk auszubreiten. Leider stellt Active Directory-Sicherheit die meisten Unternehmen vor Schwierigkeiten, da sich mit zunehmender Komplexität von Domänen auch die Zahl der Fehlkonfigurationen häuft. Sicherheitsteams sind dadurch nicht in der Lage, Schwachstellen aufzuspüren und zu beheben, bevor sich daraus geschäftsschädigende Probleme entwickeln.
Mit Tenable.ad können Sie sämtliche Änderungen an Ihrem Active Directory überblicken, vorhersagen, von welchen Anomalien oder Schwachstellen das größte Risiko ausgeht, und handeln, um kritische Angriffspfade zu versperren, bevor diese von Angreifern ausgenutzt werden.

Herausforderungen bei der Absicherung von Active Directory

Die ständigen Veränderungen in Active Directory (AD), die in jedem Unternehmen auftreten, schränken die Sichtbarkeit der AD-Angriffsoberfläche ein und führen häufig zu neuen Einfallstoren für Angriffe. Nur wenige Sicherheitsteams haben genügend Einblick und Kontext, um AD-Fehlkonfigurationen und -Schwachstellen zu finden und zu beheben.

Intensivierte Bemühungen helfen nicht weiter: Aufgrund der Größe und Komplexität der meisten AD-Implementierungen ist eine manuelle Überwachung nicht durchführbar und eine Erkennung von Angriffen in Echtzeit unmöglich. Incident Response und Threat-Hunting werden erschwert, da Teams nicht alle versteckten Fehlkonfigurationen und Beziehungsgeflechte erkennen können.

Folgen von schwacher Active Directory-Sicherheit

Auf erfolgreiche Eindringversuche folgen in der Regel Angriffe auf Active Directory, um Rechte auszuweiten, sich lateral fortzubewegen, Malware zu installieren und Daten zu exfiltrieren. Angreifer können diese Vorstöße erfolgreich vor Protokollen und anderen Überwachungstools verbergen, da ihre Aktivitäten innerhalb von Active Directory im Rahmen der bestehenden Sicherheitsrichtlinien konform erscheinen. Der hohe Preis von schwacher AD-Sicherheit wird spürbar, wenn Angreifer erfolgreich Payloads verteilen, die Datenverlust, Lösegeldforderungen, den Wiederaufbau der Umgebung oder Markenschäden zur Folge haben.

ACTIVE DIRECTORY-ANGRIFFE KONTINUIERLICH ERKENNEN UND VERHINDERN MIT TENABLE.AD

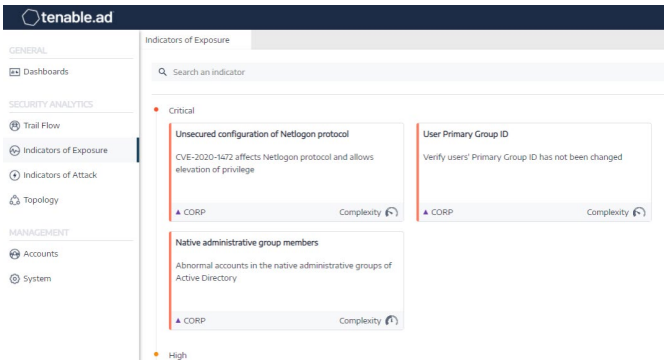
- Decken Sie versteckte Schwachstellen innerhalb Ihrer Active Directory-Konfigurationen auf.
- Erfassen Sie die zugrunde liegenden Probleme, die Ihre AD-Sicherheit bedrohen.
- Gehen Sie jeder Fehlkonfiguration im Detail – und in verständlicher Sprache – auf den Grund.
- Erhalten Sie empfohlene Fixes für jedes Problem.
- Erstellen Sie benutzerdefinierte Dashboards zur Verwaltung Ihrer AD-Sicherheit, um die Risikominderung voranzutreiben.
- Decken Sie gefährliche Vertrauensstellungen auf.
- Erfassen Sie sämtliche Änderungen an Ihrem AD.
- Decken Sie Angriffe innerhalb Ihres AD auf.
- Visualisieren Sie jede Bedrohung anhand des genauen zeitlichen Verlaufs von Angriffen.
- Konsolidieren Sie Angriffsdaten in einer zentralen Ansicht.
- Erkennen Sie den Zusammenhang zwischen AD-Änderungen und böswilligen Handlungen.
- Analysieren Sie einen AD-Angriff bis ins kleinste Detail.
- Rufen Sie MITRE ATT&CK® Beschreibungen direkt aus dem Vorfall heraus auf.

Tenable.ad sichert Active Directory ab und versperrt Angriffspfade

Mit dem proaktiven, risikobasierten Ansatz von Tenable.ad für Active Directory-Sicherheit können Sie alle Ihre Schwachstellen überblicken, vorhersagen, auf welche Übertragungswege Angreifer es abgesehen haben könnten, und handeln, um Angriffe zu erkennen, zu unterbinden und zu verhindern.

Active Directory-Schwachstellen aufspüren und beheben, bevor es zu Angriffen kommt

Entdecken und priorisieren Sie Schwachstellen in Ihren bestehenden Active Directory-Domänen proaktiv und reduzieren Sie Ihre Gefährdung, indem Sie die schrittweisen Behebungsempfehlungen von Tenable.ad befolgen.
Durch Hardening Ihres Active Directory können Sie Angreifer aufhalten, ihre potenziellen Aktivitäten unterbinden und sicherstellen, dass weniger Sicherheitsverletzungen zu einer Ausweitung von Rechten, Lateral Movement oder der Ausführung von Malware führen.

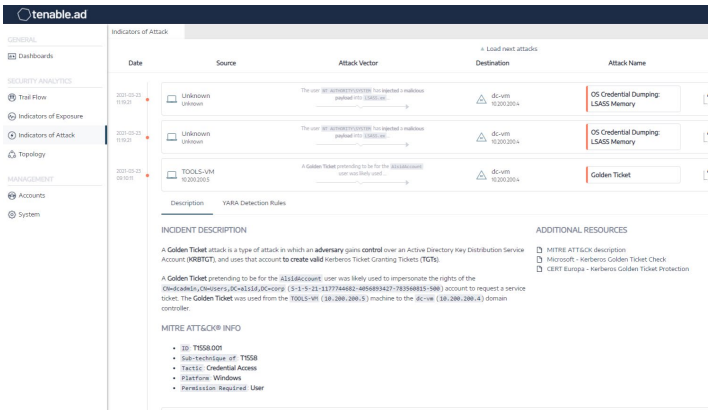


Angriffe auf Active Directory in Echtzeit erkennen und sofort darauf reagieren

Profitieren Sie von einer lückenlosen Überwachung und erkennen Sie gegen Active Directory gerichtete Angriffe wie Golden Ticket, DCShadow, Brute Force, Password Spraying, DCSync usw. Tenable.ad ergänzt Ihr SIEM, SOC oder SOAR durch Informationen zu Angriffen, damit Sie schnell reagieren und Angriffe aufhalten können. Die automatisierte Erkennung von AD-Angriffen entlastet Sicherheitsteams bei der Überwachung, sodass sie mehr Zeit für andere Prioritäten haben.

Die flexible, schlanke Bereitstellung sichert Ihr Active Directory in seinem ganzen Ausmaß ab – von On-Prem bis zur Cloud.

- **Keine Agents. Keine Berechtigungen. Keine Verzögerungen.**
  Ausgefeilte Angriffe auf Active Directory lassen sich ganz ohne Agents und Berechtigungen verhindern und aufspüren.
- **Schutz in der Cloud**
  Überprüfen Sie in Echtzeit die Sicherheit von Azure Active Directory Domain Services, AWS Directory Service oder Google Managed Service for Active Directory.
- **Überall einsetzbar**
  Tenable.ad bietet die Flexibilität von zwei Architekturkonzepten: On-Prem, damit Ihre Daten vor Ort und unter Ihrer Kontrolle bleiben, und SaaS, damit Sie die Cloud nutzen können.



Über Tenable

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Über 30.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen mehr als die Hälfte der Fortune 500-Unternehmen, mehr als 30 Prozent der Global 2000 sowie große Regierungsbehörden. Erfahren Sie mehr über uns auf de.tenable.com.

Weitere Informationen: Besuchen Sie **de.tenable.com**
Kontakt: Bitte senden Sie eine E-Mail an **sales@de.tenable.com** oder besuchen Sie **de.tenable.com/contact**