

Defender for Identity



Prevent



Detect



Investigate

Microsoft Defender for Identity

Dein Ultimativer Guide

- Defender for Identity Installation & Architektur
- Sensoren- & Domänen-Integration
- Sicherheitswarnungen & Cloud-Anbindung



Über den Autor


Aaron Siller


Als ich 2014 als IT-Dienstleister startete, stand ich vor denselben Herausforderungen, mit denen heute viele meiner Kunden zu mir kommen: Komplexe Microsoft-Systeme, ständig neue Security-Anforderungen und nie genug Zeit, um alles richtig zu konfigurieren.

Was als klassische IT-Beratung begann, entwickelte sich schnell zu einer klaren Mission: **Microsoft 365 Umgebungen sicherer machen, ohne dass Admins dafür Wochenenden opfern müssen.**



Heute werde ich von führenden Instituten wie der Heise Academy und Golem Karrierewelt als Trainer für Microsoft 365 Security eingesetzt. Meine Expertise bestätigt sich in der Zusammenarbeit mit Unternehmen vom handwerklichen Mittelstand bis hin zu internationalen Konzernen. Schau Dir gerne meine Referenzen auf meiner Website an.

 E-MAIL aaron@siller.consulting

 WEBSITE siller.consulting

 LINKEDIN [Aaron-Siller](https://www.linkedin.com/in/Aaron-Siller)

 YOUTUBE [Aaron-Siller-YT](https://www.youtube.com/Aaron-Siller-YT)

Inhaltsverzeichnis

Microsoft Defender for Identity	4
Einführung.....	4
Was ist Microsoft Defender for Identity?.....	4
Architektur	5
Microsoft Defender for Identity bereitstellen.....	6
Den richtigen Sensortyp auswählen	7
Die Umgebung vorbereiten.....	8
Das lokale Verzeichnis vorbereiten	9
Bereitstellen von Sensoren auf Domänencontrollern	19
Microsoft Defender for Identity optimieren	22
Hinzufügen von Active Directory-Domänen	24
Lernphase.....	24
Überprüfen von Warnungen	25
Sicherheitswarnungs-Leitfäden.....	28
Pfade für seitliche Bewegung	28
Integration mit anderen Produkten	29
Microsoft Defender for Cloud Apps	29
Microsoft Sentinel	30
Microsoft 365 Defender	30
Verwaltung der Sicherheitslage	30
Endpunkte sichern	31

Microsoft Defender for Identity

Einführung

Sicherheitsvorfälle, die in Cloud-Umgebungen passieren, haben ihren Ursprung oft vor Ort. Die Komplexität, Größe und oft veraltete Natur einiger Systeme schaffen eine herausfordernde Umgebung für Sicherheitsexperten: Sie müssen verschiedene Systeme, Updates, (Inter-)Konnektivität, Authentifizierung und so weiter im Auge behalten. Je größer eine Umgebung wird, desto mehr Aufwand ist nötig, um sie sicher zu halten. Angesichts der hybriden Konnektivität zwischen der Cloud und lokalen Systemen, aber auch der Transformation der IT-Umgebung durch die COVID-19-Pandemie, ist die Sicherheit der lokalen Systeme wichtiger denn je geworden.

Eines dieser lokalen "Legacy"-Systeme ist Windows Server Active Directory. Nach mehr als zwei Jahrzehnten aktiven Dienstes ist und bleibt Active Directory für lange Zeit das vorherrschende Identitätssystem, das weltweit in digitalen Umgebungen eingesetzt wird. Allein diese Tatsache macht es zu einem interessanten Ziel für Angreifer; Auch sie hatten über zwei Jahrzehnte Zeit, ihre Fähigkeiten zum Hacken in Active Directory zu perfektionieren, was es für uns Verteidiger nicht gerade einfacher macht...

Was ist Microsoft Defender for Identity?

Microsoft Defender for Identity ist der Nachfolger des lokalen Advanced Threat Analytics (ATA). Dies hatte seit März 2019 keine signifikanten Updates mehr erhalten und der Mainstream-Support endete offiziell im Januar 2021. Microsoft Defender for Identity, das im Gegensatz zu Advanced Threat Analytics vollständig cloudbasiert ist, ist eine Sicherheitslösung, die hilft, dein lokales Active Directory zu sichern. Basierend auf einer Vielzahl von Signalen wie Protokolldateien, Windows-Ereignissen und Netzwerkverkehrserfassungen kann Microsoft Defender for Identity Bedrohungen und verdächtige Aktivitäten im Zusammenhang mit lokalen Identitäten erkennen, aufspüren und untersuchen, die in und durch Active Directory stattfinden.

Microsoft Defender for Identity hilft bei der Erkennung verschiedener Angriffe wie Pass-the-Hash-, Print Nightmare- und Petit Potam-Schwachstellen, Golden-Ticket-Angriffen, verschiedener Aufklärungsaktivitäten wie der Aufzählung von Domänen-Admins und vielem mehr. Es überwacht und analysiert Benutzer, Gruppenmitgliedschaften, Entitätsverhalten und -aktivitäten. Wenn verdächtige Benutzeraktivitäten erkannt werden, identifiziert und untersucht Microsoft Defender for Identity die vollständige Angriffskette, indem es klare Vorfallsinformationen auf einer einfachen Zeitachse darstellt, die wiederum für eine schnelle Ereignis-Triage und -Analyse verwendet werden kann.

Zum Zeitpunkt des Schreibens unterstützt Microsoft Defender for Identity die Überwachung von drei (3) verzeichnisbezogenen Diensten:

- **Domänencontroller:** Hier passiert der Großteil. Informationen von Domänencontrollern werden genutzt, um eine Vielzahl potenziell bössartiger Aktivitäten zu erkennen.
- **Active Directory-Verbunddienste-Server:** Durch die Fähigkeit, Verbunddienste-Server zu überwachen, verbessert die Plattform bestehende Erkennungen, die vor der Unterstützung für AD FS-Server ausschließlich auf Informationen von Domänencontrollern basierten. Beispiele dafür sind Brute-Force-Angriffe und Konto-Enumerationen.
- **Active Directory-Zertifikatdienste (AD CS):** Der neueste Zugang zu Microsoft Defender for Identity. Dieser Detektor ist für Server vorgesehen, die AD-Zertifikatdiensten gewidmet sind. ADCS auf Domänencontrollern (die nur in einer Testumgebung existieren sollten!) nutzen den bestehenden DC-Sensor. Mit der Einführung des Detektors werden nun auch die Abläufe und die Sicherheitslage von AD-Zertifikatdiensten überwacht.

Active Directory-Verbunddienste (AD FS): Die Unterstützung für AD FS-Server war dringend erforderlich, da viele Organisationen weiterhin auf Verbundlösungen setzen, um die Authentifizierung für zahlreiche Anwendungen – häufig auch Microsoft 365 – bereitzustellen. Obwohl das Konzept grundsätzlich funktioniert, stellt die Unterstützung für AD FS-Server keineswegs eine Empfehlung dar, AD FS weiter zu betreiben oder dessen Einsatz auszubauen. Wenn möglich, sollte AD FS durch cloudbasierte Authentifizierungsmethoden ersetzt werden. Dadurch lässt sich die Sicherheitslage der Umgebung deutlich verbessern, insbesondere durch die Reduzierung der Angriffsfläche.

Architektur

Die Architektur von Microsoft Defender for Identity ist einfach aufgebaut: Sie besteht aus dem Microsoft Defender for Identity-Clouddienst und lokalen Sensoren. Letztere erfassen Informationen wie Ereignisprotokolle und Netzwerkverkehr von Domänencontrollern und senden diese zur weiteren Analyse an den Clouddienst.

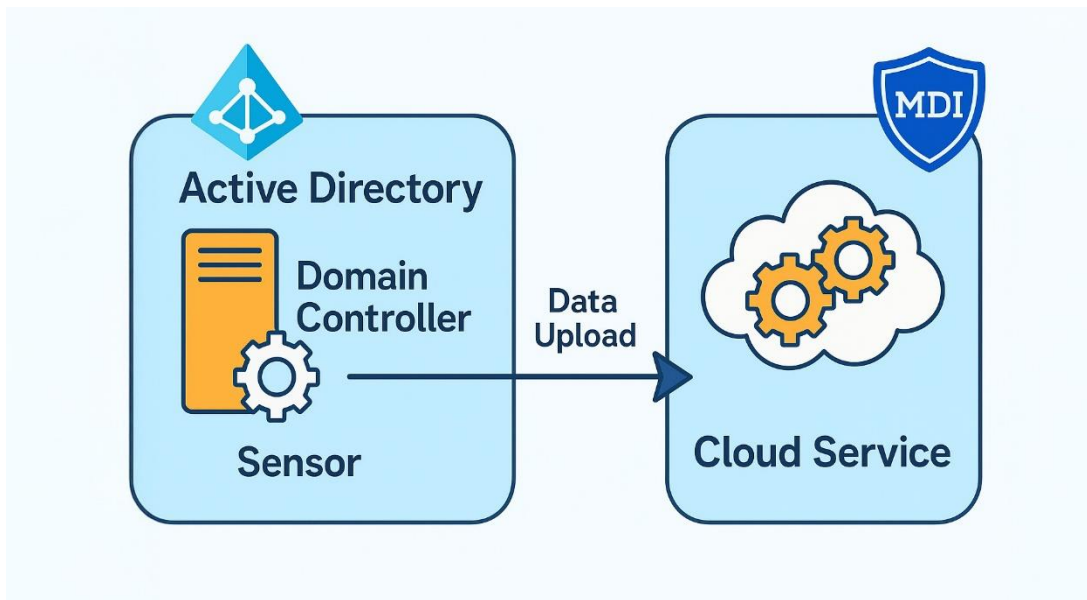


Abbildung 3-1: Microsoft Defender for Identity-Architektur.

Der Microsoft Defender for Identity-Sensor ist ein Agent, der Aktivitäten auf Domänencontrollern sowie auf Verbunddienste-Servern überwacht. Er ist dafür verantwortlich, Netzwerkverkehr zu erfassen, relevante Windows-Ereignisse zu sammeln, RADIUS-Kontoinformationen zusammenzustellen, verschiedene Netzwerkentitäten wie IP-Adressen, Benutzernamen und Gruppen aufzulösen und all diese Daten an den Clouddienst zu übermitteln. Weitere Informationen zu den Sensorarten findest du später in diesem Kapitel.

Der Microsoft Defender for Identity-Clouddienst läuft auf der Azure-Infrastruktur und ist mit dem **Microsoft Intelligent Security Graph (ISG)** verbunden. Er interpretiert die von den Sensoren gesendeten Informationen. Wie andere Sicherheitslösungen von Microsoft nutzt Defender for Identity eine Vielzahl von Techniken, darunter auch maschinelles Lernen, um Anomalien in den erfassten Daten zu erkennen. Diese Anomalien basieren auf bekannten Bedrohungen und Angriffstechniken, die typischerweise in Active-Directory-Umgebungen vorkommen – etwa laterale Bewegungen, Aufklärungsaktivitäten, Exfiltrationsversuche und mehr.

Im Gegensatz zum früheren Advanced Threat Analytics (ATA), das ein vollständig lokaler Dienst war, werden alle Daten bei Microsoft Defender for Identity in der Cloud gespeichert und verarbeitet.

Microsoft Defender for Identity bereitstellen

Die folgenden Schritte zeigen, wie du Microsoft Defender for Identity über das Microsoft 365 Security Center konfigurierst. Obwohl zum Zeitpunkt des Schreibens noch das klassische

Legacy-Portal verwendet werden konnte, ist dies inzwischen nicht mehr die bevorzugte Methode.

Zur Konfiguration von Microsoft Defender for Identity sind folgende Schritte erforderlich:

1. Falls noch nicht geschehen, initialisiere den Mandanten für Microsoft Defender for Identity..
2. Richte geeignete Konten ein, die von den Sensoren verwendet werden können, um eine Verbindung zum lokalen Active Directory herzustellen. Seit Kurzem gehört dazu auch das sogenannte „**Aktionskonto verwalten**“, das bestimmte Aktionen im lokalen Active Directory durchführen kann – beispielsweise das Zurücksetzen von Benutzerkennwörtern oder das Deaktivieren von Benutzerkonten.
3. Die Konfiguration von Überwachungs-, Protokollierungs- und Berechtigungseinstellungen stellt sicher, dass die Sensoren und Konten über die erforderlichen Berechtigungen verfügen, um ihre Aufgaben ausführen zu können.
4. Lade den passenden Sensortyp herunter und installiere ihn auf geeigneten Systemen innerhalb der lokalen Organisation.
5. Konfiguriere zusätzliche Optionen wie vertrauliche Konten, Honeypoken-Konten, Ausschlüsse und weitere sicherheitsrelevante Einstellungen.

Den richtigen Sensortyp auswählen

Bevor du mit der Konfiguration von Microsoft Defender for Identity beginnst, solltest du überlegen, wie du die Sensoren bereitstellen möchtest. Grundsätzlich gibt es zwei Möglichkeiten:

- **Regulärer Sensor:** Dies ist die Standardmethode, bei der der Sensor-Agent direkt auf einem Domänencontroller oder einem AD FS-Server installiert wird.
- **Eigenständiger Sensor:** Dabei wird der Sensor-Agent auf einem separaten Server installiert, der eine Kopie des Netzwerkverkehrs von Domänencontrollern oder AD FS-Servern über Port Mirroring erhält. Port Mirroring ist eine Funktion, die von den meisten Switches in Unternehmensnetzwerken unterstützt wird. Sie spiegelt den Datenverkehr eines bestimmten Ports und leitet ihn an einen anderen Port weiter – daher der Begriff *Mirroring*.

Der einfachste und empfohlene Weg besteht darin, den Sensor direkt auf den Servern zu installieren, die überwacht werden sollen. Dafür ist es notwendig, dass diese Server in der Lage sind, Daten an die Cloud-Plattform von Microsoft Defender for Identity zu senden. Da es sich hierbei um Domänencontroller handelt, ist ein direkter Internetzugang möglicherweise nicht standardmäßig vorhanden. Das stellt jedoch kein grundsätzliches Problem dar: Du musst lediglich den Zugriff auf bestimmte vertrauenswürdige Microsoft-Endpunkte zulassen.

Bis vor Kurzem lautete Microsofts Empfehlung, Domänencontrollern keinen Internetzugang zu gewähren. Diese Richtlinie wurde inzwischen überarbeitet. Um Microsoft Defender for Identity – das auch vom Incident Response Team (DART) von Microsoft eingesetzt wird – vollständig nutzen zu können, empfiehlt Microsoft nun, den Zugriff auf die eigenen Cloud-Plattformen zu ermöglichen. Dies erleichtert die Implementierung erheblich, insbesondere für Unternehmen, die sich eng an Microsofts Sicherheitsvorgaben orientieren.

In vielen Organisationen ist es zudem üblich, den Internetzugang über einen Proxyserver bzw. ein sicheres Web-Gateway abzusichern. Auch hierfür bietet Microsoft Defender for Identity Konfigurationsmöglichkeiten. Der Sensor kann so eingerichtet werden, dass er mit einem Proxyserver zusammenarbeitet. Die Details zur Konfiguration werden hier beschrieben.

Leistung ist wichtig. Viele Unternehmen befürchten, dass der Sensor die Ressourcen der überwachten Server stark beansprucht. Zwar benötigt der Sensor einige Ressourcen, er ist jedoch so konzipiert, dass die Überwachungsfunktionen niemals die Primärfunktionen des Servers beeinträchtigen. Sollte ein Server über unzureichende Ressourcen verfügen, weist dich das Portal entsprechend mit Warnmeldungen darauf hin.

Wenn Leistungsbedenken oder netzwerktechnische Einschränkungen bestehen kann der Einsatz eines **eigenständigen Sensors** sinnvoll sein. In diesem Fall muss kein Agent auf dem Zielsystem installiert werden, und dieser benötigt auch keinen Internetzugang. Allerdings ist diese Variante mit deutlich höherem Konfigurationsaufwand verbunden. Du musst sicherstellen, dass Port Mirroring korrekt eingerichtet ist. Du musst die Ereignissammlung und -weiterleitung von Windows konfigurieren, damit auch diese Daten dem Sensor zur Verfügung stehen. Wenn keine Einschränkungen bestehen, installiere den Sensor direkt auf dem zu überwachenden Server. Der Einsatz eines eigenständigen Sensors sollte nur dann erfolgen, wenn eine direkte Installation nicht möglich oder nicht erwünscht ist.

Virtuelle Maschinen. Wenn du einen regulären Sensor auf einer virtuellen Maschine installierst - insbesondere VMware – kann es notwendig sein, bestimmte Netzwerkeinstellungen anzupassen, um Performanceprobleme zu vermeiden. Weitere Informationen dazu findest du [hier](#).

Die Umgebung vorbereiten

Wenn du Microsoft Defender for Identity zum ersten Mal konfigurierst, wird dir beim Aufrufen der Plattformeinstellungen ein entsprechender Bildschirm angezeigt. Dieser weist darauf hin, dass eine neue MDI-Instanz vorbereitet wird. In diesem Zuge werden automatisch die erforderlichen Gruppen in Microsoft Entra ID erstellt, um den Zugriff auf die Funktionen von Microsoft Defender for Identity zu ermöglichen.



Hang on! We're preparing your Microsoft defender for identity workspace



This may takes a few minutes. When this process is completed, you can start monitoring your on-premises active directory environment with Microsoft defender for Identity. [Learn more](#)

Abbildung 3-2: Erstellen einer neuen MDI-Instanz.

Vorsicht bei Testversionen. Falls du Microsoft Defender for Identity bereits zuvor getestet hast, wurden möglicherweise die in Microsoft Entra ID erstellten Gruppen, die als Teil der MDI-Instanz erstellt wurden nicht vollständig entfernt. In diesem Fall kann es zu einer Fehlermeldung kommen, auf die bereits vorhandenen Gruppen hinweist. Entferne in diesem Fall manuell die folgenden Gruppen aus Microsoft Entra ID und starte den Vorgang anschließend erneut: "Azure ATP tenant Administrators", "Azure ATP tenant Users" und "Azure ATP tenant Viewers".

Das lokale Verzeichnis vorbereiten

In den folgenden Abschnitten behandeln wir die Konfiguration der lokalen Konten sowie die Berechtigungen, die erforderlich sind, damit Microsoft Defender for Identity die notwendigen Informationen aus der Umgebung sammeln kann.

Directory Services Account (DSA)

Directory Services Accounts sind die Dienstkonten, die Microsoft Defender for Identity verwendet, um eine Verbindung zum lokalen Active Directory herzustellen. Diese Konten dienen dazu, Informationen aus dem Verzeichnis auszulesen und – sofern entsprechend konfiguriert – bestimmte Aufgaben auszuführen, etwa das Zurücksetzen von Benutzerkennwörtern.

Dabei können zwei Arten von Directory Services Accounts verwendet werden:

- Ein reguläres Benutzerkonto, das mit den erforderlichen Berechtigungen ausgestattet ist, um eine Verbindung zu Active Directory herzustellen und Daten auszulesen
- Ein gruppengesteuertes Dienstkonto (gMSA), das dieselben Aufgaben übernimmt, aber ohne die Notwendigkeit, ein Kennwort manuell zu konfigurieren oder zu verwalten.

Die Verwendung eines gMSA ist grundsätzlich vorzuziehen, da hier keine Anmeldeinformationen manuell gepflegt werden müssen. Stattdessen übernimmt das Windows-Betriebssystem die sichere Verwaltung dieser Daten, was gMSAs zu einer sichereren Option macht. Eine detaillierte Erklärung der Funktionsweise gruppengesteuerter Dienstkonten würde den Rahmen dieses Buches sprengen.

Ein Directory Services Account erstellen

Es gibt verschiedene Möglichkeiten, ein gMSA zu erstellen und zu konfigurieren. Speziell für Microsoft Defender for Identity verwenden wir eine Reihe von PowerShell-Skripten, um diesen Prozess zu vereinfachen. Zunächst muss das gMSA erstellt werden – dies geschieht mit dem folgenden Skript:

```
# Configure the variables which will be used later in the script
$gMSA_Name = 'svc_MDI'
$gMSA_GroupName = 'grp_MDI'
$gMSA_Hosts = 'DomainController1', 'DomainController2'

# Install the required PowerShell module if not already present on the system
Install-Module ActiveDirectory

# Create the group and add the members
$gMSA_HostsGroup = New-ADGroup -Name $gMSA_GroupName -GroupScope Global -PassThru
$gMSA_Hosts | ForEach-Object { Get-ADComputer -Identity $_ } |
    ForEach-Object { Add-ADGroupMember -Identity $gMSA_GroupName -Members $_ }
# Create the gMSA:
New-ADServiceAccount -Name $gMSA_Name -DNSHostName "$gMSA_Name.$env:USERDNSDOMAIN" `
-PrincipalsAllowedToRetrieveManagedPassword $gMSA_HostsGroup.Name
```

Bitte beachte, dass du, wenn du zum ersten Mal ein gMSA einsetzt, möglicherweise etwa zehn Stunden warten musst, nachdem der KDS-Stammschlüssel erstellt wurde, bevor du das Skript ausführen kannst. Der Grund dafür ist, dass alle Domänencontroller zunächst den Stammschlüssel benötigen, um gMSA-Kennwörter generieren zu können. Weitere Informationen dazu findest du [hier](#).

Scoping. Das Skript erfordert, dass du eine Liste aller Domänencontroller angibst, auf denen ein Sensor installiert werden soll. Um sicherzustellen, dass keine sicherheitsrelevanten Ereignisse übersehen werden und Microsoft Defender for Identity effizient arbeiten kann, sollten alle Domänencontroller innerhalb einer Domäne erfasst werden. Stelle also sicher, dass du

entweder alle relevanten Systeme in die Liste aufnimmst oder das Skript so anpasst, dass es automatisch alle Domänencontroller abfragt.

Wenn neue Domänencontroller zur Umgebung hinzugefügt oder bestehende ersetzt werden, muss das gMSA entsprechend aktualisiert werden. Verwende dafür den Parameter - *PrincipalsAllowedToRetrieveManagedPassword*, um die betroffenen Systeme hinzuzufügen oder zu entfernen.

Nach der Erstellung muss das gMSA auf allen Systemen installiert werden, auf denen ein Sensor vorgesehen ist. Diese Systeme sollten mit den im Skript unter \$gMSA_Hosts aufgeführten Servern übereinstimmen. Wenn später zusätzliche Domänencontroller hinzukommen, musst du das gMSA auch auf diesen Systemen installieren.

```
# Install the required PowerShell module if not already present on the system Install-Module ActiveDirectory
```

```
# Install the gMSA Account on the server  
Install-ADServiceAccount -Identity svc_MDI
```

Achte darauf, dass der Kontoname, den du im gMSA definiert hast, mit der tatsächlichen Identität des gMSA übereinstimmt.

Nachdem das gMSA installiert wurde, kannst du mit dem folgenden Befehl auf allen entsprechenden Servern testen, ob das Konto korrekt verwendet werden kann:

```
# Test the gMSA account  
Test-ADServiceAccount -Identity svc_MDI
```

Leseberechtigungen für den Papierkorb

Um die für Defender for Identity relevanten Informationen abrufen zu können, muss das Directory Services Account (DSA) in der Lage sein, alle Objekte in der Umgebung zu lesen – einschließlich versteckter Container wie dem Papierkorb. Das ist erforderlich, damit Microsoft Defender for Identity z. B. gelöschte Objekte zuverlässig erkennt. Zwar lassen sich die benötigten Berechtigungen auch über die Benutzeroberfläche zuweisen, doch bietet das folgende Skript eine einfachere und schnellere Möglichkeit, dies umzusetzen. Es verwendet das zuvor erstellte gMSA. Wichtig: Die Berechtigungen werden nicht direkt dem gMSA zugewiesen. Stattdessen wird das gMSA einer Sicherheitsgruppe hinzugefügt, der anschließend die benötigten Rechte erteilt werden.

```
#Declaring the identity to give permissions to  
$DSAIdentity = '<domain>\SecurityGroup'  
  
# Get the deleted objects container's distinguished name:  
$distinguishedName = ([adsi]'' ).distinguishedName.Value
```

```
$deletedObjectsDN = 'CN=Deleted Objects,{0}' -f $distinguishedName
# Take ownership on the deleted objects container:
$params = @("$deletedObjectsDN", '/takeOwnership')
C:\Windows\System32\dsacsls.exe $params

# Grant the 'List Contents' and 'Read Property' permissions to the user or group:
$params = @("$deletedObjectsDN", '/G', "$($DSAIdentity):LCRP")
C:\Windows\System32\dsacsls.exe $params
```

Ein 'Aktionskonto verwalten' konfigurieren

Microsoft Defender for Identity ermöglicht es Administratoren, bestimmte Aktionen im lokalen Verzeichnis direkt über die Aktionen in einem Vorfall auszuführen, beispielsweise das Deaktivieren eines Benutzerkontos oder das Zurücksetzen eines Kennworts. Standardmäßig verwendet Microsoft Defender for Identity hierfür das LocalSystem-Konto auf den Domänencontrollern, sodass keine zusätzliche Konfiguration erforderlich ist, damit diese Funktion funktioniert.

Wenn du jedoch ein dediziertes Konto verwenden möchtest – etwa zu Überwachungszwecken –, kannst du ein benutzerdefiniertes Konto einrichten. Im Gegensatz zum Directory Services Account kann als Aktionskonto ausschließlich ein gruppengesteuertes Dienstkonto (gMSA) verwendet werden. Technisch wäre es zwar möglich, das DSA-Konto auch für Aktionen zu verwenden, empfohlen wird jedoch, ein separates Konto anzulegen. Dadurch wird der Lesezugriff vom Ausführen privilegierter Aktionen wie dem Zurücksetzen von Kennwörtern sauber getrennt.

Zur Erstellung des gMSA verwendest du das gleiche Skript wie zuvor. Nachdem das Konto angelegt wurde, stelle sicher, dass es über die Berechtigung „Als Dienst anmelden“ auf allen Servern verfügt, auf denen ein Sensor installiert ist. Anschließend müssen dem Konto die erforderlichen Berechtigungen im Active Directory erteilt werden. Öffne hierzu die **Active Directory-Benutzer und -Computer-Konsole** und klicke mit der rechten Maustaste auf den Domänenknoten. Falls du zuvor nur bestimmte Organisationseinheiten (OUs) für die Überwachung ausgewählt hast, verwende stattdessen die entsprechende OU. Wähle „Eigenschaften“ und navigiere zu „Sicherheit > Erweitert“. Gehe auf die Registerkarte „Berechtigungen“ und klicke dort auf „Hinzufügen“. Beachte, dass sich dieses Vorgehen von der vorherigen Konfiguration unterscheidet, bei der du die Überwachung statt der Berechtigungen eingestellt hast.

Wähle als Prinzipal das gMSA des Aktionskontos aus. Damit du es auswählen kannst, musst du zuvor unter „**Objekttypen**“ die Option „**Dienstkonten**“ aktivieren.

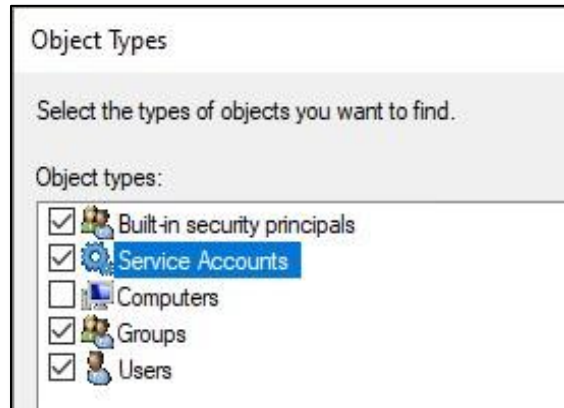


Abbildung 3-3: Auswählen von Dienstkonten

Wähle anschließend „**Zulassen**“ als Typ und „**Untergeordnete Benutzerobjekte**“ im Feld „**Gilt für**“. Konfiguriere dann die folgenden Berechtigungen:

Aktion	Zustimmung
Benutzer deaktivieren	Eigenschaften: Read userAccountControl Eigenschaften: Write userAccountControl
Passwort zurücksetzen	Berechtigungen: Reset password Eigenschaften: Read pwdLastSet Eigenschaften: Write pwdLastSet

Tabelle 3-1: Konfigurieren der Einstellungen für das Aktionskonto

Wiederhole diesen Schritt, wähle diesmal jedoch „**Untergeordnete Gruppenobjekte**“ im Feld „**Gilt für**“ aus und konfiguriere erneut die Berechtigungen:

- Mitglieder lesen
- Mitglieder schreiben

Automatische Angriffsunterbrechung

Die automatische Angriffsunterbrechung in Microsoft 365 Defender kann ein Benutzerkonto deaktivieren, wenn festgestellt wird, dass dieses Konto eine Gefahr für den restlichen Teil der Umgebung darstellt. Diese Maßnahme basiert auf den im Zusammenhang mit dem Vorfall erfassten Signalen und erfolgt über Microsoft Defender for Identity. Um sicherzustellen, dass bestimmte Benutzerkonten – wie beispielsweise Dienstkonten – von dieser Maßnahme ausgenommen bleiben, solltest du entsprechende Ausschlüsse unter **Einstellungen > Identitäten > Ausschlüsse für automatische Reaktionen** konfigurieren.

Sicherstellen, dass das DSA über 'Als Dienst anmelden'-Rechte verfügt

Das Dienstkonto, das du für Defender for Identity verwendest, sollte über die Berechtigung verfügen, sich lokal auf den Domänencontrollern und auf den Servern anzumelden, auf denen ein Sensor installiert wird. Der Grund dafür ist, dass der Sensor als LocalService ausgeführt wird und dabei das Dienstkonto imitiert. Um dies zu ermöglichen, aktualisiere die Standarddomänencontroller-Richtlinie entsprechend. Navigiere dazu zu **Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten**. Wähle dort den Eintrag **Als Dienst anmelden** aus und stelle sicher, dass das gMSA-Konto eingetragen ist.

GPO Durcheinander. Behalte dabei den Überblick über die GPOs, die bereits angewendet werden. Es ist leicht, den Überblick zu verlieren, wenn mehrere GPOs miteinander in Konflikt stehen, was dazu führen kann, dass deine Einstellungen nicht wie erwartet wirksam werden. Wenn du keine Richtlinie definiert hast, die regeln, welche Konten sich als Dienst anmelden dürfen, oder wenn du generell keine Einschränkungen festgelegt hast, kannst du diesen Schritt überspringen. Trotzdem ist es immer empfehlenswert, den Zugriff auf dieses Recht gezielt zu beschränken - insbesondere auf einem Domänencontroller!

Sammeln der notwendigen Informationen

Damit Informationen aus der lokalen Umgebung gesammelt werden können, benötigt der Directory Services Account entsprechenden Zugriff auf relevante Bereiche der Umgebung. Im Folgenden findest du eine Übersicht darüber, welche Berechtigungen erforderlich sind und wie du sie konfigurierst.

Konfigurieren der Windows-Ereignissammlung

Der Sensor stützt sich unter anderem auf bestimmte Einträge im Windows-Ereignisprotokoll, um Bedrohungen zu erkennen und weiterführende Informationen über sicherheitsrelevante Ereignisse bereitzustellen, wie etwa Kontoinformationen oder Änderungen an Sicherheitsgruppen. Damit dies zuverlässig funktioniert, sollten die Domänencontroller mit spezifischen erweiterten Überwachungsrichtlinieneinstellungen konfiguriert sein. Wenn diese Richtlinien nicht korrekt angewendet werden, kann Defender for Identity die betreffenden Ereignisse nicht erfassen, was die Effektivität der Lösung deutlich einschränkt.

Es wird empfohlen, die Standarddomänencontroller-Richtlinie für diese Konfiguration zu verwenden, da sie automatisch auf alle Domänencontroller in der Domäne angewendet wird. Alternativ kannst du auch eigene Richtlinien definieren, solange du sicherstellst, dass sie auf alle Systeme angewendet werden, die mit Defender for Identity arbeiten.

Öffne auf einem Domänencontroller die **Gruppenrichtlinienverwaltung**, navigiere zur **Standarddomänencontroller-Richtlinie**, klicke mit der rechten Maustaste darauf und wähle dann **Bearbeiten...** aus, wie unten dargestellt:

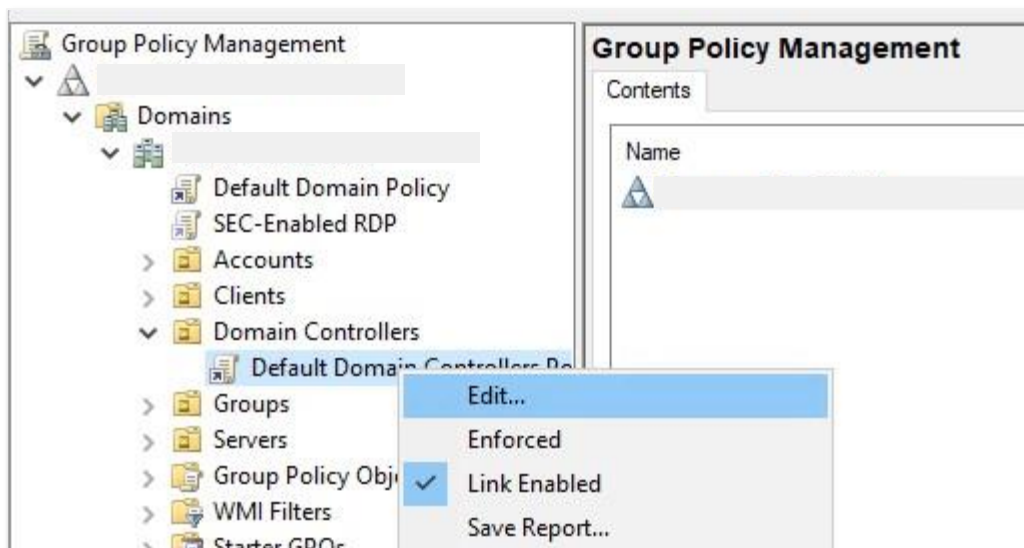


Abbildung 3-4: Bearbeiten der Standarddomänencontroller-Richtlinie

Navigiere als Nächstes zu **Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Erweiterte Überwachungsrichtlinienkonfiguration > Überwachungsrichtlinien** und konfiguriere die folgenden Einstellungen so, dass sowohl *Erfolgs-* als auch *Fehlerereignisse* protokolliert werden.

Richtlinie	Kategorie
Kontenanmeldung	Überwachung der Anmeldeinformationen
Kontoverwaltung	Überwachung der Computerkontenverwaltung
Kontoverwaltung	Überwachung der Verteilung Gruppenverwaltung
Kontoverwaltung	Überwachung der Sicherheitsgruppenverwaltung
Kontoverwaltung	Überwachung der Benutzerkontenverwaltung
DS-Zugriff	Überwachung des Zugriffs auf Verzeichnisdienste

DS-Zugriff	Überwachung von Verzeichnisdienständerungen
System	Überwachung der Sicherheitssystemerweiterung

Tabelle 3-2: Konfigurieren von Erweiterten Überwachungsrichtlinieneinstellungen

Der nächste Schritt ist erforderlich, um die Protokollierung von Aktivitäten im Zusammenhang mit NTLM zu aktivieren, beispielsweise Ereignis-ID 8004. Bleibe innerhalb der Standarddomänencontroller-Richtlinie (oder innerhalb der Richtlinie, die du manuell erstellt hast), und gehe zu **Lokale Richtlinien > Sicherheitsoptionen**. Stelle dort sicher, dass die Einstellungen wie in der untenstehenden Tabelle konfiguriert sind:

Einstellung	Wert
Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Verkehr zu Remote-Servern	Alle überwachen
Netzwerksicherheit: NTLM einschränken: NTLM-Authentifizierung in dieser Domäne überwachen	Alles aktivieren
Netzwerksicherheit: NTLM einschränken: Eingehender NTLM-Verkehr überwachen	Überwachung für alle Konten aktivieren

Tabelle 3-3: Konfigurieren von NTLM-Ereignissen

Konfigurieren der Objektüberwachung

Zusätzlich zu den oben beschriebenen Konfigurationsschritten solltest du auch die Objektüberwachung innerhalb der Domäne aktivieren. Dadurch wird sichergestellt, dass unter anderem die Windows-Ereignis-ID 4662 generiert wird. Öffne dazu die Konsole **Active Directory-Benutzer und -Computer**, klicke mit der rechten Maustaste auf den Domänenknoten und wähle **Eigenschaften**. Beachte, dass du alternativ auch bestimmte OUs auswählen kannst – in diesem Fall musst du die Konfiguration jedoch für jede OU separat vornehmen, die du überwachen möchtest.

Navigiere im Eigenschaftenfenster zur Registerkarte **Sicherheit** und klicke anschließend auf **Erweitert**. Wähle dort den Reiter **Überwachung** aus.

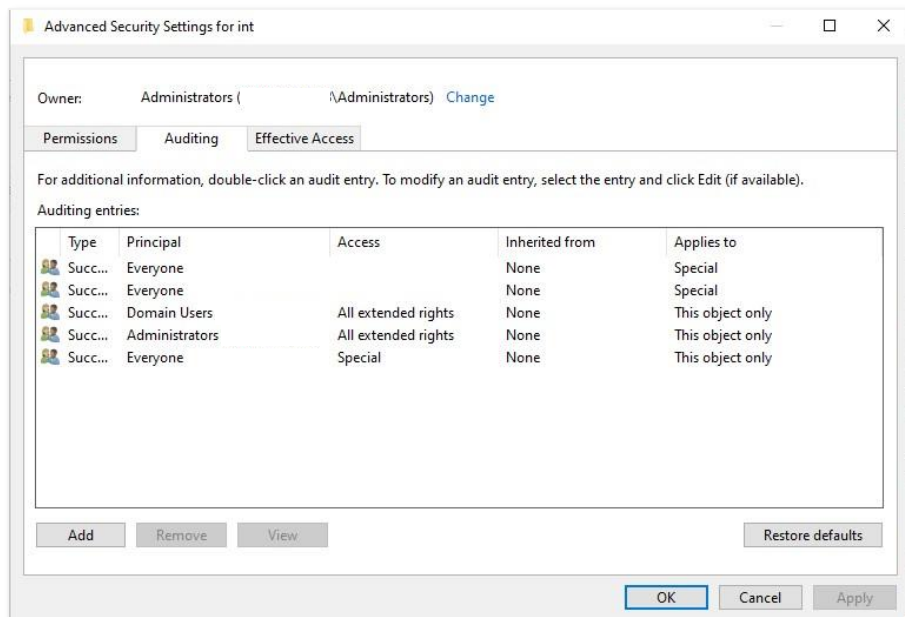


Abbildung 3-5: Aktivieren der Objektüberwachung.

Klicke auf der Registerkarte “Überwachung” auf **Hinzufügen** und anschließend auf **Benutzer, Computer oder Gruppe auswählen**. Stelle im Popup-Fenster sicher, dass du “Jeder” auswählst, wie im folgenden Bild dargestellt.

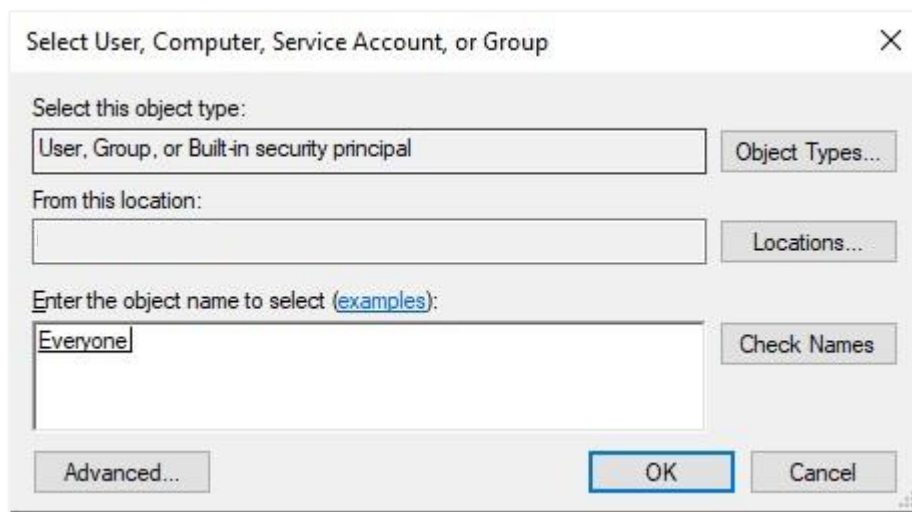


Abbildung 3-6: Auswählen des Sicherheitsprinzips, für den die Objektüberwachung konfiguriert werden soll.

Wähle bei **Gilt für** die Option **Untergeordnete Benutzerobjekte**. Stelle dann in der Liste der Berechtigungen sicher, dass alle Optionen aktiviert sind – mit Ausnahme der folgenden Berechtigungen. Auf diese Weise wird sichergestellt, dass Ereignisse ausgelöst werden, wenn Änderungen an Verzeichnisobjekten im Geltungsbereich vorgenommen werden:

- Inhalte auflisten
- Berechtigungen lesen
- Alle Eigenschaften lesen

Wiederhole abschließend die oben beschriebenen Schritte für die folgenden Elemente im Feld **Gilt für**:

- **Untergeordnete Gruppenobjekte**
- **Untergeordnete Computerobjekte**
- **Untergeordnete msDS-GroupManagedServiceAccount-Objekte**
- **Untergeordnete msDS-ManagedServiceAccount-Objekte**

Objektüberwachung für AD FS und Microsoft Exchange

Wenn du Active Directory-Verbinddienste überwachst oder wenn Exchange in deiner lokalen Organisation installiert ist, sind einige zusätzliche Schritte erforderlich. Für AD FS gehe wie folgt vor: Öffne zunächst „Active Directory-Benutzer und -Computer“ und navigiere zu **Domäne > Programmdateien > Microsoft > ADFS**. Beachte, dass dieser Container nur sichtbar ist, wenn AD FS in der Organisation bereitgestellt wurde.

Klicke mit der rechten Maustaste auf den Container und öffne die Registerkarte **Sicherheit**. Klicke auf **Erweitert** und wechsle zur Registerkarte **Überwachung**. Ähnlich wie in den vorherigen Schritten klickst du auf **Hinzufügen** und wählst **Jeder** als Sicherheitsprinzipal. Belasse den Typ auf **Alle** und „Gilt für“ auf **Dieses Objekt und alle untergeordneten Objekte**. Stelle sicher, dass **Alle Eigenschaften lesen** und **Alle Eigenschaften schreiben** in der Liste der Berechtigungen aktiviert sind.

Für die Überwachung von Exchange-Objekten musst du stattdessen **ADSI Edit** verwenden. Öffne dazu *ADSIEdit.msc*, klicke auf **Aktion** und anschließend auf **Verbinden**. Wähle im Dialogfeld **Verbindungseinstellungen** unter **Bekannten Namenskontext auswählen** die Option **Konfigurations-** aus.

Erweitere den Konfigurationscontainer und klicke mit der rechten Maustaste auf den Knoten, der mit **CN=Configuration,DC=...** beginnt. Navigiere zur Registerkarte **Sicherheit**, klicke auf **Erweitert**, dann auf **Überwachung** und anschließend auf **Hinzufügen**. Wähle erneut **Jeder** als Sicherheitsprinzipal, setze den Typ auf **Alle** und „Gilt für“ auf **Dieses Objekt und alle untergeordneten Objekte**. Stelle sicher, dass nur **Alle Eigenschaften schreiben** ausgewählt ist.

Überwachung und Ereignisprotokollüberwachung für AD CS

Wie bei AD FS und Microsoft Exchange sind auch für AD CS zusätzliche Konfigurationsschritte notwendig, damit die relevanten Informationen erfasst werden. Zunächst muss die Objektüberwachung angepasst werden, um zusätzliche Ereignisse einzuschließen. Ähnlich wie bei der Konfiguration anderer Servertypen aktualisierst du dazu die **Erweiterte**

Überwachungsrichtlinienkonfiguration für deine Active Directory-Zertifikatdienste, sodass Objektzugriffe auf die Zertifizierungsstelle sowohl für erfolgreiche als auch für fehlgeschlagene Zugriffe protokolliert werden. Verwende dafür eine Gruppenrichtlinie anstelle der lokalen Richtlinie auf dem/den Server(n). Falls du mit einem Server arbeitest, der nicht in die Domäne eingebunden ist, verwende die lokale Richtlinie.

Konfiguriere anschließend die Überwachung direkt auf der Zertifizierungsstelle (CA). Führe dazu den entsprechenden Befehl an der Eingabeaufforderung auf dem Server selbst aus:

```
certutil -setreg CA\AuditFilter 127 net
stop certsvc && net start certsvc
```

Sobald du diese Schritte – zusätzlich zu den allgemeinen Überwachungseinstellungen – abgeschlossen hast, kannst du den Sensor auf den entsprechenden Servern bereitstellen.

Registrieren des DSA im Portal

Nachdem du das gMSA erstellt hast, öffne das Microsoft 365 Security Center und navigiere zu **Einstellungen > Identitäten**. Klicke auf **Verzeichnisdienstkonten** und anschließend auf **Anmeldeinformationen hinzufügen**. Gib die Kontodaten so ein, wie du sie zuvor erstellt hast. In unserem Beispiel würdest du **svc_MDI** als Kontonamen verwenden. Klicke abschließend auf **Speichern**. Vergiss nicht, auch das Aktionskonto hinzuzufügen, falls du ein benutzerdefiniertes Konto erstellt hast.

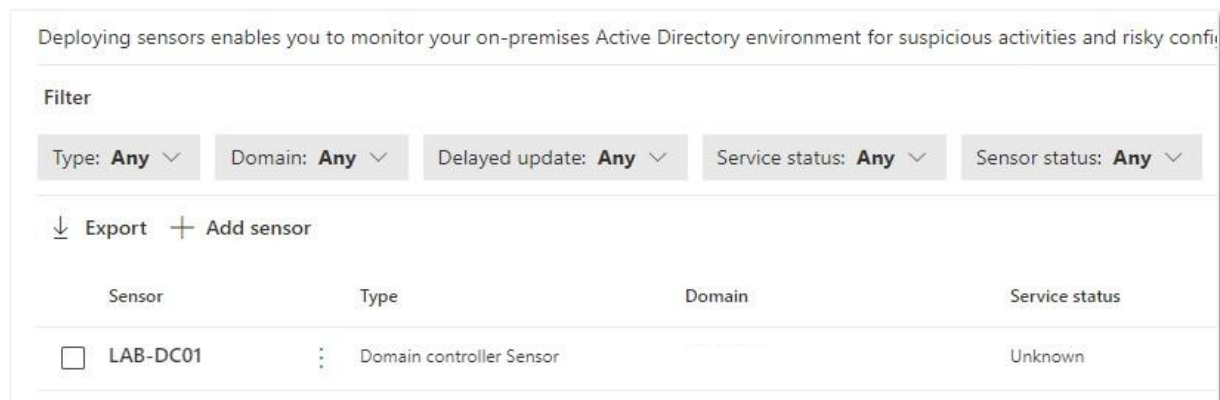


Abbildung 3-7: Konfigurieren des DSA im Portal.

Beachte, dass das Verzeichnisdienstkonto (DSA) automatisch erkannt wird, sobald du einen Sensor auf deinem Server oder deinen Servern installiert hast, nachdem du es dem Portal hinzugefügt hast.

Bereitstellen von Sensoren auf Domänencontrollern

Herunterladen und Installieren des Sensor-Setup-Pakets

Um den Sensor zu installieren, musst du zunächst die aktuelle Version herunterladen. Öffne dazu das Microsoft 365 Security Center und navigiere zu **Einstellungen > Identitäten**. Klicke auf **Sensoren** und anschließend auf **Sensor hinzufügen**. Es öffnet sich eine neue Slideout-Ansicht mit dem Download-Link für das Installationsprogramm sowie einem Zugriffsschlüssel. Kopiere diesen Zugriffsschlüssel, da du ihn später während der Installation des Sensors benötigen wirst.

Nach dem Herunterladen des Sensor-Setup-Pakets entpackst du es und öffnest die Datei **Azure ATP Sensor Setup.exe**. Während des Installationsassistenten wirst du aufgefordert, den zuvor kopierten Zugriffsschlüssel einzugeben. Dieser Schlüssel ermöglicht es dem Sensor, sich mit der richtigen Microsoft Defender for Identity-Cloud-Instanz zu verbinden und Daten dorthin zu übertragen. Der Zugriffsschlüssel wird beim Herunterladen des Sensor-Setups angezeigt, wie in Abbildung 3-8 dargestellt:

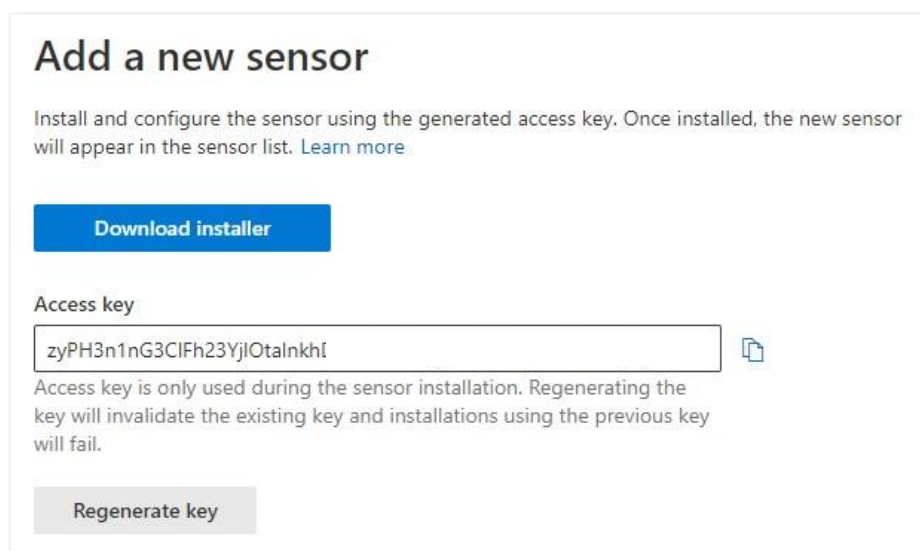


Abbildung 3-8: Herunterladen der Sensor-Setup-Datei

Nach einiger Zeit wird der Status des Sensors aktualisiert, und er beginnt damit, Domänencontroller-Daten und Netzwerkverkehr an den Microsoft Defender for Identity-Clouddienst zu übermitteln.

Verbunddienste-Server. Bei der Installation eines Sensors auf einem Verbunddienste-Server ist nach dem Setup eine zusätzliche Konfiguration erforderlich: Öffne die Sensorliste klicke auf den entsprechenden Verbunddienste-Server und gib den FQDN des Resolver-Domänencontrollers ein. Nach der Eingabe dieser Information kann es ein paar Minuten dauern, bis der Sensor-Status auf *Wird ausgeführt* wechselt.

Der letzte Schritt besteht darin, das gMSA in die Konfiguration von Microsoft Defender for Identity aufzunehmen. Öffne erneut das Microsoft 365 Security Center, navigiere zu **Einstellungen > Identitäten** und klicke auf **Aktionskonten verwalten**. Klicke auf **Anmeldeinformationen hinzufügen** und gib die entsprechenden Informationen ein.

Umgang mit Sensor-Updates

Als Cloud-Dienst erhält Microsoft Defender for Identity regelmäßige Updates. Diese beinhalten gelegentlich auch Aktualisierungen für die auf den Servern installierten Sensoren. Microsoft unterscheidet dabei zwischen zwei Arten von Updates:

- **Kleinere Updates** erfolgen relativ häufig, haben jedoch nur geringe oder keine Auswirkungen auf den Domänencontroller. Sie werden automatisch installiert und erfordern lediglich einen Neustart des Defender for Identity-Sensors.
- **Größere Updates** treten seltener auf, können jedoch einen Neustart des gesamten Servers erfordern. In diesem Fall sollte ein entsprechendes Wartungsfenster eingeplant werden, um potenzielle Auswirkungen auf den Betrieb zu minimieren.

Sensor-Updates werden automatisch ausgeliefert, sobald der Defender for Identity-Dienst aktualisiert wird. Standardmäßig werden Server nicht ohne Zustimmung eines Administrators neu gestartet. Du kannst jedoch automatische Serverneustarts aktivieren, indem du zur Einstellungsseite von Microsoft Defender for Identity gehst, unter **System** auf **Updates** klickst und den Schalter für **Domänencontroller und ADFS-Server während Updates neu starten** aktivierst.

Auf derselben Seite findest du auch eine Übersicht über alle aktiven Sensoren. Jeder Sensor verfügt dort über zwei zusätzliche Schalter:

- **Automatischer Neustart**, der steuert, ob der Sensor nach einem Update automatisch neu gestartet werden kann.
- **Verzögertes Update**, verzögert die Aktualisierung eines Sensors um 72 Stunden nach einem Dienst-Update.

Update-Ringe. Durch die Nutzung der Option "Verzögertes Update" kannst du einen virtuellen Update-Ring für deine Umgebung einrichten. Beispielsweise kannst du einige Server im regulären Update-Zyklus belassen und alle übrigen Sensoren auf verzögertes Update konfigurieren. So erhalten bestimmte Server die Aktualisierung früher, wodurch du die Auswirkungen prüfen kannst, bevor das Update in der gesamten Umgebung ausgerollt wird.

Überwachung der Sensor-Integrität

Um eine vollständige Abdeckung und damit Zuverlässigkeit der Lösung zu gewährleisten, ist es wichtig, die Integrität der bereitgestellten Sensoren im Blick zu behalten. Obwohl Sensoren im Allgemeinen stabil arbeiten, gibt es verschiedene Faktoren, die ihre Fähigkeit zur Datenübertragung beeinträchtigen können – beispielsweise fehlende Systemressourcen oder entfernte Berechtigungen.

In den Einstellungen von Microsoft Defender for Identity gibt es einen eigenen Bereich, der sich mit der Sensor-Integrität befasst. Du findest ihn, indem du das Microsoft 365 Security Center öffnest und zu **Einstellungen > Identitäten > Allgemein > Integritätsprobleme** navigierst.

Um zu vermeiden, dass du diese Seite regelmäßig manuell prüfen musst, empfiehlt es sich, Benachrichtigungen zu Integritätsproblemen zu konfigurieren. Das kannst du tun, indem du im Abschnitt **Benachrichtigungen** eine oder mehrere E-Mail-Adressen hinterlegst.

Microsoft Defender for Identity optimieren

Konfigurieren vertraulicher Konten

Es ist sehr wichtig, vertrauliche Active Directory-Konten, -Gruppen, -Server und -Computer in Microsoft Defender for Identity zu identifizieren. Einige Erkennungsmechanismen, wie etwa die Erkennung von Änderungen an vertraulichen Gruppen oder lateralen Bewegungen, basieren auf dem Vertraulichkeitsstatus der jeweiligen Entität.

Vertrauliche Konten müssen bestimmten Rollen oder Kategorien zugeordnet sein. Konten, die Mitglied einer der in Tabelle 3-4 aufgeführten Active Directory-Gruppen sind, werden automatisch als vertraulich gekennzeichnet.

Administratoren	Domänen-Administratoren
Power User	Domänencontroller
Kontenoperatoren	Gruppenrichtlinien-Ersteller-Eigentümer
Serveroperatoren	Schreibgeschützte Domänencontroller
Druckoperatoren	Unternehmensweit schreibgeschützte Domänencontroller
Backup-Operatoren	Schema-Administratoren

Replikatoren	Unternehmensadministratoren
Netzwerkkonfigurationsoperatoren	Microsoft Exchange-Server
Eingehende Forest-Trust-Ersteller	

Tabelle 3-4: Active Directory-Gruppen, die automatisch als vertraulich markiert werden.

Neben den oben genannten Rollen werden auch Systeme in den folgenden Kategorien automatisch als vertraulich erkannt:

- Zertifizierungsstellenserver
- DHCP-Server
- DNS-Server
- Microsoft Exchange-Server

Entitäten können auch manuell als vertraulich markiert werden. Öffne dazu im Microsoft 365 Security Center den Bereich **Einstellungen > Identitäten** und klicke unter **Entitäts-Tags** auf **Vertraulich**. Wähle anschließend aus, ob du Benutzer, Geräte oder Gruppen kennzeichnen möchtest. Typischerweise würdest du hier hochsensible Konten, Geräte oder Gruppen auswählen, etwa Unternehmens- oder Domänen-Administratoren, Exchange-Server oder Dateiserver mit vertraulichen Informationen.

Konfigurieren von Honeytoken-Konten

Honeytoken-Konten sind speziell eingerichtete Konten, die dazu dienen, böswillige Akteure in die Irre zu führen. Sie sollen den Eindruck erwecken, es handle sich um reguläre, nutzbare Konten, obwohl sie in Wahrheit unbenutzt sind und ausschließlich zu Überwachungszwecken existieren. Ziel ist es, Angreifer zu täuschen und deren böswillige Absichten frühzeitig zu erkennen. Wird ein solches Konto in irgendeiner Form verwendet, missbraucht oder manipuliert, löst dies unmittelbar eine Sicherheitswarnung aus.

Die manuelle Kennzeichnung von Benutzern oder Clients als Honeytoken erfolgt ebenfalls über das Microsoft 365 Security Center. Öffne **Einstellungen > Identitäten**, klicke unter **Entitäts-Tags** auf **Honeytoken** und anschließend auf **Benutzer kennzeichnen**, um die gewünschten Benutzer auszuwählen. Dasselbe Verfahren gilt auch für Geräte.

Achte bei der Auswahl eines Honeytoken-Kontos darauf, einen realistisch wirkenden Namen zu wählen, um die Glaubwürdigkeit des Lockvogel-Kontos zu erhöhen. Wird ein solcher Benutzer oder ein entsprechendes Gerät zur Authentifizierung verwendet, erscheint ein Ereignis in der

Zeitachse des Microsoft Defender for Identity-Portals. Du kannst auf das Ereignis klicken, um zu analysieren, was genau mit dem Honeytoken-Konto passiert ist.

Wichtig. Um die Anzahl falsch-positiver Sicherheitswarnungen zu minimieren, können Ausschlüsse konfiguriert werden. Dies ist entweder über eine geöffnete Sicherheitswarnung möglich – klicke dazu auf die drei Punkte und wähle **Schließen und ausschließen..** -, oder zentral über die Verwaltung von Ausschlüssen auf Basis des Bedrohungstypen. Letzteres ist insbesondere hilfreich, wenn du Systeme betreibst, die automatisierte Tests durchführen (wie Breach and Attack Simulation-Clients), oder wenn eine Anwendung Aktivitäten legitime, aber sicherheitskritisch wirkende Aktivitäten erzeugt. Öffnen dazu das **Zahnrad-Symbol** und navigiere zu **Ausschlüsse** unter **Erkennungen**. Weitere Informationen zu den Bedrohungen findest du [hier](#).

Hinzufügen von Active Directory-Domänen

Bei Bedarf können zusätzliche Domänen innerhalb einer Active Directory-Gesamtstruktur hinzugefügt werden, um sie mit Microsoft Defender for Identity zu schützen. Dies ermöglicht eine einheitliche Sichtweise bei der Überwachung des Netzwerks und bei der Untersuchung potenzieller Vorfälle, die durch Defender for Identity erkannt wurden.

Microsoft Defender for Identity unterstützt sowohl Gesamtstrukturen mit als auch ohne Vertrauensstellungen. Eine einzelne Instanz kann bis zu 30 Active Directory-Gesamtstrukturen verwalten, unabhängig davon, ob eine Vertrauensstellung besteht. Um zusätzliche Gesamtstrukturen einzubinden, muss der Sensor auf einem Domänencontroller der jeweiligen Gesamtstruktur installiert werden. In jeder Gesamtstruktur werden zudem Directory Services-Konten mit den erforderlichen Berechtigungen benötigt!

Das Hinzufügen weiterer Domänen erfolgt über die Einstellungen im Defender for Identity-Portal. Navigiere dazu zum *Zahnrad-Symbol*, gehe im Abschnitt „**Datenquellen**“ auf „**Verzeichnisdienste**“ und klicke anschließend auf „**Anmeldeinformationen hinzufügen**“. Folge dann den zuvor beschriebenen Schritten.

Lernphase

Nach der Erstinstallation von Microsoft Defender for Identity werden möglicherweise nicht sofort Warnungen angezeigt. Grund dafür ist eine initiale Lernphase von etwa 30 Tagen, in der Defender for Identity das normale Verhalten innerhalb der Umgebung analysiert. Diese Phase hilft dabei, Anomalien später besser zu erkennen und die Anzahl falsch positiver Meldungen zu reduzieren. Es gibt jedoch Szenarien, in denen diese Lernphase nicht erwünscht ist, zum Beispiel:

- Beim Testen der Lösung vor einer flächendeckenden Bereitstellung.

- Bei der Bereitstellung von MDI im Rahmen eines laufenden Vorfalls, bei dem sofortige Einblicke notwendig sind.

Auch wenn sich die Lernphase deaktivieren lässt, sollte dabei beachtet werden, dass dies zu einer höheren Anzahl falsch positiver Warnungen führen kann. Um die Lernphase zu deaktivieren, öffne das Microsoft 365 Security Portal und navigiere zu **Einstellungen > Identitäten > Erweiterte Einstellungen**. Aktiviere dort die Option „**Lernphase entfernen**“, um sofort Warnmeldungen zu erhalten.

Nicht alle Warnungen sind von der Lernphase betroffen. Binäre Warnungen, wie beispielsweise Honeytoken-Aktivitäten, werden unabhängig davon ausgelöst. Andere Warnungen, die auf Verhaltensanalysen basieren, erfordern jedoch die Lernphase.

Bei neuen Defender for Identity-Instanzen wird die Lernphase automatisch deaktiviert sein, bis die erste Lernperiode abgeschlossen ist. Danach wird die Option automatisch deaktiviert.

Sobald die Lernphase deaktiviert ist, kann für bestimmte Warnungstypen eine Empfindlichkeitsstufe konfiguriert werden – vorausgesetzt, der jeweilige Warnungstyp unterstützt die Lernphase. Hierfür stehen drei Optionen zur Verfügung:

- **Normal.** Es erfolgt keine Änderung der Standardeinstellungen.
- **Mittel.** Die Empfindlichkeit wird erhöht, was zu mehr falsch positive Meldungen führen kann.
- **Hoch.** Die Empfindlichkeit wird noch weiter erhöht, was zu einer deutlich höheren Anzahl an Warnungen führt..

Diese Einstellungen sollten mit Bedacht gewählt werden, um eine Überlastung des Security Operations Center (SOC) zu vermeiden. In manchen Fällen kann eine Erhöhung der Empfindlichkeit jedoch sinnvoll sein, etwa in Umgebungen mit spezifischen Abfrageverhalten, das die Erkennung echter Bedrohungen erschwert. Zwar steigt die Anzahl der Warnungen bei erhöhter Empfindlichkeit, gleichzeitig sinkt aber das Risiko, dass schädliche Aktivitäten fälschlich als unauffällig eingestuft werden.

Überprüfen von Warnungen

Das Überwachen von Warnungen ist eine zentrale Aufgabe beim Schutz von Identitäten und deiner gesamten Umgebung. Durch die Konsolidierung aller Sicherheitslösungen im Microsoft 365 Security Center kannst du dich gezielt auf Warnungen aus Microsoft Defender for Identity konzentrieren, indem du die Vorfälle nach der jeweiligen Servicequelle filterst:

Incidents

Most recent incidents and alerts

↓ Export

Filters: Status: New +1 X Service sources: Microsoft Defender for Identity X

<input type="checkbox"/>	Incident name	Incident Id	Tags	Severity	Investigation state	Categories
<input type="checkbox"/>	> Discovery incident on one endpoint			Medium	1 investigation states	Discovery
<input type="checkbox"/>	> User and IP address reconnaissance (SMB) on o...			Medium	1 investigation states	Discovery

Abbildung 3-9: Überprüfen von Warnungen und Vorfällen innerhalb des Microsoft 365 Security Center.

Der Schweregrad verdächtiger Aktivitäten wird in drei Stufen unterteilt. Diese Einstufung erfolgt auf Grundlage der folgenden Kriterien:

- **Niedrig** -- Aktivitäten mit niedrigem Schweregrad sind häufig Teil von Angriffen, die darauf abzielen, dass böswillige Benutzer oder Schadsoftware allgemeinen Zugriff auf Organisationsdaten erhalten.
- **Mittel** -- Aktivitäten mit mittlerem Schweregrad deuten oft auf Versuche hin, bestimmte Identitäten zukompromittieren. Dies kann zu Identitätsdiebstahl oder einer Eskalation von Berechtigungen führen.
- **Hoch** -- Aktivitäten mit hohem Schweregrad weisen in der Regel auf gezielte Angriffe hin, die sich auf Identitätsdiebstahl, privilegierte Eskalation oder andere sicherheitskritische Virfälle mit potenziell erheblicher Auswirkung richten.

Wenn ein Vorfall oder eine Warnung ausgelöst wird, kann der Administrator das Ereignis zur weiteren Untersuchung öffnen. Jede Vorfalls- oder Warnungsseite enthält zusätzliche Informationen über die zugrunde liegenden Aktivitäten, wie in Abbildung 3-10 veranschaulicht. Auf der Seite findest du:

- Eine grafische Darstellung der Aktivität oder Aktivität(en), die dabei hilft, die Beziehung zwischen beteiligten Entitäten wie Geräte, Benutzer oder IP-Adressen zu verstehen.
- Eine Übersicht über die relevanten Aktivitäten (Beweise), die zur Auslösung der Warnung geführt haben.

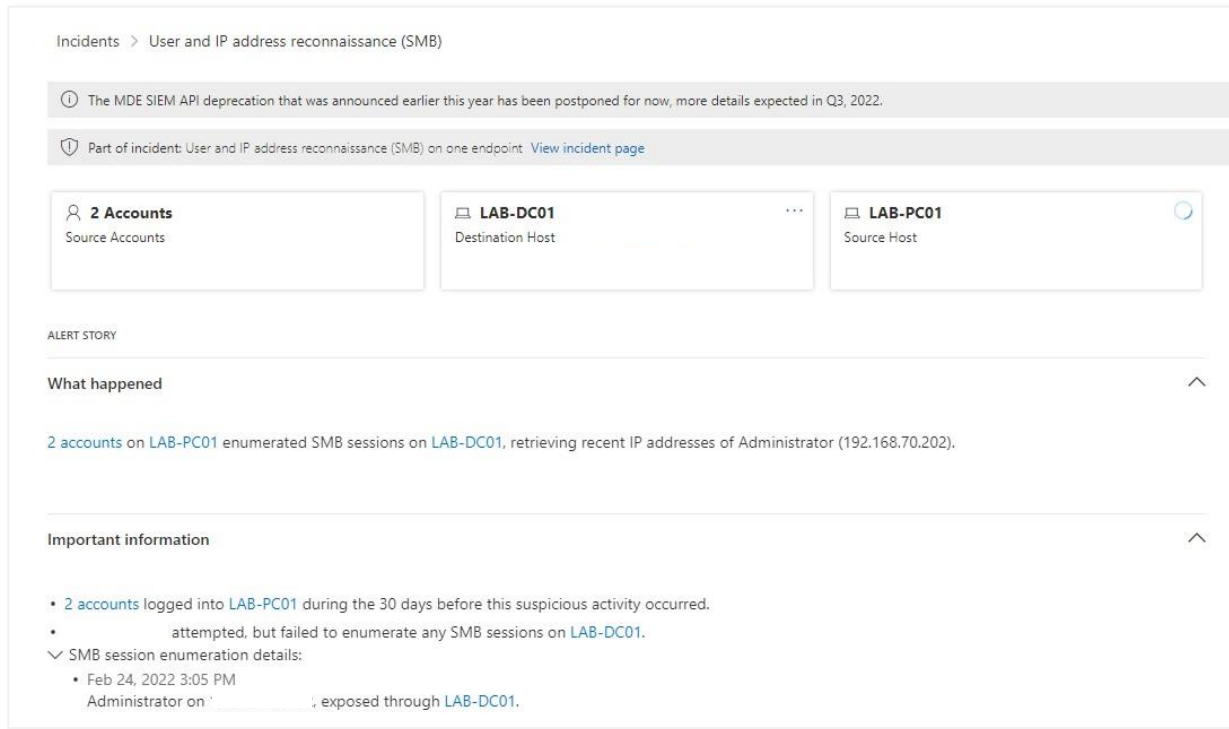


Abbildung 3-10: Seite mit Defender for Identity-Warnungen

Jeder Vorfall oder jede Warnung ermöglicht es dir, bestimmte Aktionen durchzuführen. Die verfügbaren Maßnahmen hängen von der Art des Ereignisses ab und davon, ob du beispielsweise ein Aktionskonto konfiguriert hast.

Schnellere Reaktion. Für schnelle Reaktionen auf einen Vorfall stehen dir mehrere Optionen zur Verfügung. Besonders im Hinblick auf Benutzeridentitäten hat Microsoft eine positive Änderung vorgenommen, um sicherzustellen, dass Maßnahmen schneller greifen. Mit der Option *Benutzer deaktivieren* kannst du den Benutzer sofort im lokalen Active Directory deaktivieren. Bei der nächsten Synchronisierung wird der Benutzer dann auch in Microsoft Entra ID deaktiviert. Mit *Benutzer sperren* wird der Benutzer hingegen sofort in Microsoft Entra ID gesperrt. So musst du nicht auf den nächsten Synchronisierungszyklus warten, um zu verhindern, dass der Benutzer weiterhin auf Dienste zugreift. Beachte jedoch, dass ein Benutzer bei der nächsten Synchronisierung wieder in Microsoft Entra ID aktiviert wird, wenn er dort deaktiviert wurde, aber im lokalen Active Directory noch aktiv ist. Behalte dies im Auge, wenn du auf einen Vorfall reagierst - du willst nicht riskieren, dass ein Benutzer kurz nach der Deaktivierung erneut Zugriff auf Ressourcen erhält!

Obwohl das Microsoft 365 Security Center verschiedene Tools zur Untersuchung von Warnungen und Vorfällen bereitstellt – einschließlich der erweiterten Suchoberfläche – kannst du zusätzlich einen Excel-Bericht herunterladen, der detaillierte Informationen über die Aktivitäten im Rahmen des Ereignisses enthält. Um diese Datei zu exportieren, klicke in der Warnungsansicht auf das Slideout-Menü und dann auf „**Exportieren**“.

Der Excel-Bericht liefert umfangreiche Informationen zum Sicherheitsereignis, unter anderem:

- Eine Zusammenfassung mit Details zur Warnung (Problem, Beschreibung, Zeitpunkt, Schweregrad, Status, Links zu den Warnungen in Microsoft Defender for Identity und Microsoft 365 Defender).
- Angaben zu den Quellcomputer sowie – falls zutreffend - zu Honeypot-Konten
- Informationen zu den Zielressourcen (z.B. DNS-Server, Domänencontroller, Computer, Benutzer, Dienste)
- Netzwerkaktivitäten, d.h. von welchen Quellen auf welche Ressourcen und Ports zugegriffen wurde, sowie die dabei verwendeten Protokolle.

Sicherheitswarnungs-Leitfäden

Die Warnungen in Microsoft Defender for Identity beschreiben verdächtige Aktivitäten, die von Sensoren im lokalen Netzwerk erkannt wurden. Diese Sensoren identifizieren die beteiligten Akteure und Computer. Um die Untersuchung zu erleichtern, sind die relevanten Beweisinformationen in der Warnung enthalten, sodass die betroffenen Benutzer und Geräte leicht identifiziert werden können.

Wie bei jeder typischen Cyberangriffskette besteht auch hier ein Angriff aus mehreren Phasen oder Kategorien. Microsoft Defender for Identity ordnet jede Warnung einer Phase oder Kategorie zu, sodass alle Phasen der Angriffskette abgedeckt werden. Microsoft führt eine [Liste der Ereignisse](#), zudem die beobachteten Ereignisse, ihren Schweregrad und ihre Zuordnung zu Angriffstypen in der MITRE ATT&CK-Matrix.

Pfade für seitliche Bewegung

Wenn ein Angreifer von einem Konto auf ein anderes übergeht – also ein Konto kompromittiert, um Zugriff auf ein weiteres zu erhalten – verfolgt er das Ziel, seine Berechtigungen in der Umgebung zu erweitern. Üblicherweise wird zunächst ein nicht sensibles Konto kompromittiert, um anschließend auf privilegiere, sensiblere Konten überzugehen. Diese Technik wird als seitliche Bewegung bezeichnet und ist eine verbreitete Methode, mit der sich Angreifer innerhalb eines Netzwerks fortbewegen. Wird sie frühzeitig erkannt und gestoppt, kann verhindert werden, dass privilegierte Konten kompromittiert werden. Daher ist die Erkennung und Meldung seitlicher Bewegungen eine zentrale Funktion von Defender for Identity.

Neben der Erkennung seitlicher Bewegungen liefert Defender for Identity auch Informationen, um das Risiko solcher Aktivitäten zu minimieren:

- Die Pfade für seitliche Bewegungen zu sensiblen Konten geben einen Überblick über potenziell kritische Angriffswege.

- Eine visuelle Darstellung dieser Pfade findest du auf der Benutzerentitätsseite, die über einen Klick auf den Benutzernamen innerhalb einer Warnungszeitachse erreichbar ist.

Seitliche Bewegung ist eine reale Bedrohung, die jede Organisation betrifft. Wie bereits erläutert, ist diese Technik oft unerlässlich, wenn Angreifer – mit Ausnahme direkter Kompromittierung eines hochprivilegierten Kontos – ihre Position innerhalb der Umgebung ausbauen wollen. Solche Pfade entstehen durch eine Vielzahl von Faktoren, häufig jedoch aufgrund schlechter Sicherheitspraktiken, nicht geschlossener Schwachstellen und ähnlicher Versäumnisse.

Um potenzielle Angriffswege zu reduzieren, sollten bestimmte Grundsätze beachtet werden:

- Halte dich strikt an das Prinzip der minimalen Rechtevergabe. Je mehr Berechtigungen ein Konto hat, desto mehr Möglichkeiten bestehen für seitliche Bewegungen.
- Trenne strikt zwischen regulären Benutzerkonten und Administratorkonten. Auch verschiedenen Ebenen von Administratorkonten sollten getrennt verwaltet werden. Ein Mitglied der Gruppe "Domänen-Admins" sollte sich beispielsweise niemals an regulären Arbeitsstationen anmelden können – andernfalls werden seine Anmeldeinformationen auf potenziell unsicheren Geräten gespeichert, was ein erhebliches Risiko darstellt.
- Führe Remote-Administration nur von speziell gehärteten Admin-Arbeitsstationen aus – sogenannten Privileged Access Workstations. Dadurch reduzierst du ebenfalls das Risiko einer Kompromittierung. Funktionen wie Credential Guard und Attack Surface Reduction, beide später in diesem Buch behandelt werden, tragen zusätzlich zur Risikominderung bei.

Fehlende Pfade für seitliche Bewegungen? Wenn in deiner Umgebung keine Pfade für seitliche Bewegungen angezeigt werden, ist dies meist ein Hinweis auf eine unvollständige Konfiguration. Damit die Plattform diese Pfade erkennen und darstellen kann, muss sie Informationen über das SAM-R-Protokoll abrufen können. Da dies standardmäßig nicht aktiviert ist, sind [zusätzliche Konfiguration erforderlich](#).

Integration mit anderen Produkten

Obwohl Microsoft Defender for Identity ein eigenständiges Produkt ist, sind es vor allem seine zahlreichen Integrationen, die es zu einem leistungsstarken Verbündeten im Bereich der Sicherheitsuntersuchungen machen. Die von der Plattform bereitgestellten Informationen lassen sich mit anderen Sicherheitslösungen wie Microsoft Defender for Cloud Apps und Microsoft Defender for Endpoint teilen, um einen ganzheitlichen Überblick über deine Bedrohungslandschaft zu erhalten. Für beide Lösungen ist die Integration mit Microsoft Defender for Identity nur einen Klick entfernt. Weitere Informationen zur Integration und den

jeweiligen Funktionen findest du in den entsprechenden Kapiteln zu Microsoft Defender for Cloud Apps, Microsoft 365 Defender und Microsoft Defender for Endpoint.

Microsoft Defender for Cloud Apps

Es ist wichtig, dass die Defender for Identity-Warnungen zentral erfasst und mit allen anderen Diensten kombiniert werden, um die Sicherheitslage ganzheitlich zu betrachten. In Kapitel 11 wird die Integration mit Microsoft Defender for Cloud Apps ausführlich erklärt.

Microsoft Sentinel

Auch Microsoft Sentinel, das in Kapitel 13 behandelt wird, kann alle Microsoft Defender for Identity-Ereignisse und -Warnungen erfassen, sodass sämtliche sicherheitsrelevanten Vorkommnisse zentral protokolliert werden.

Microsoft 365 Defender

Natürlich ist Microsoft Defender for Identity – wie die anderen hier erwähnten Produkte – ein integraler Bestandteil von Microsoft 365 Defender. Das bedeutet nicht nur, dass die Warnungen und die oben genannten Integrationen im Microsoft 365 Security Center angezeigt werden, sondern auch, dass die Funktion für die erweiterte Suche Tabellen mit Informationen enthält, die direkt von Microsoft Defender for Identity stammen.

Verwaltung der Sicherheitslage

Die Bewertung der allgemeinen Cybersicherheitsstärke und -widerstandsfähigkeit in Bezug auf die Bedrohungslage deiner Organisation – auch bekannt als Sicherheitslage – ist eine kontinuierlich notwendige Aufgabe. Deine lokale Identitätssicherheitslage wird von Microsoft automatisch bewertet und lässt sich über den Microsoft Secure Score einsehen. Dort findest du unter anderem Empfehlungen zur Optimierung von Microsoft Defender for Identity.

Im Rahmen dieser Bewertung überprüft Defender for Identity verschiedene Elemente, darunter:

- Domänencontroller mit aktiviertem Druckwarteschlangendienst
- Verwendung schwacher Verschlüsselungsverfahren
- Unsichere SID-Verlaufsattribute, Kerberos-Delegierung, Domänenkonfiguration, Kontoattribute
- Nicht überwachte Domänencontroller
- Verwendung veralteter Protokolle

- Verwendung von Microsoft LAPS
- Speicherung von Kennwörter im Klartext
- Inaktive Entitäten (Benutzer) in sensiblen Gruppen
- Riskante Pfade für seitliche Bewegung

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

ⓘ SaaS Security Posture Management for non-Microsoft applications is currently in public preview for every customer with Defender for Cloud Apps. At General Availability the licensing of this capability may be changed.

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

↓ Export 14 items

Filters: Product: Defender for Identity X

Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
<input type="checkbox"/> 1	Resolve unsecure domain configurations	+0.41%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/> 2	Set a honeytoken account	+0.08%	0/1	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/> 3	Stop clear text credentials exposure	+0.41%	5/5	<input checked="" type="radio"/> Completed	No	Yes	Identity	Defender for Identity
<input type="checkbox"/> 4	Stop legacy protocols communication	+0.41%	5/5	<input checked="" type="radio"/> Completed	No	Yes	Identity	Defender for Identity
<input type="checkbox"/> 5	Stop weak cipher usage	+0.41%	5/5	<input checked="" type="radio"/> Completed	No	Yes	Identity	Defender for Identity
<input type="checkbox"/> 6	Remove dormant accounts from sensitive groups	+0.41%	5/5	<input checked="" type="radio"/> Completed	No	Yes	Identity	Defender for Identity

Abbildung 3-11: Überprüfen von Microsoft Defender for Identity-Empfehlungen in Microsoft Secure Score.

Für jede von Microsoft identifizierte Schwachstelle wird eine konkrete Verbesserungsmaßnahme inklusive detaillierter Bewertung und Implementierungsplan bereitgestellt, damit du sie möglichst effizient in deiner Umgebung umsetzen kannst. Es empfiehlt sich, diese Maßnahmen regelmäßig zu prüfen, insbesondere wenn deine Identitätssicherheitslage offene Punkte aufweist.

Interpretation der Ergebnisse. Was die Interpretation der Ergebnisse betrifft, so müssen die Empfehlungen des Identity Secure Score manchmal eingeordnet werden. Nehmen wir die "Microsoft LAPS-Nutzung" als Beispiel: LAPS - die Local Admin Password Solution - wurde entwickelt, um sicherzustellen, dass jedes Gerät in deiner Umgebung ein individuelles lokales Administratorkennwort verwendet. Das verringert erheblich das Risiko seitlicher Bewegung, da ein kompromittiertes Passwort nicht für den Zugriff auf andere Geräte verwendet werden kann. Auch wenn LAPS eine effective und von Microsoft bereitgestellte Lösung ist, existieren gleichwertige Alternativen von Drittanbietern, etwa BeyondTrust. Nur weil Microsofts Plattform diese Lösung bevorzugt, heißt das nicht, dass sie alternativlos ist.

Endpunkte sichern

Du hast nun vieles über Identitäten und die Schutzmechanismen erfahren, die Microsoft dafür bereitstellt. Dabei darfst du jedoch nicht vergessen, dass auch die Endgeräte, über die auf

Microsofts Dienste zugegriffen wird, eine zentrale Rolle spielen. Wie bereits in Kapitel 1 erwähnt, beinhalten viele Angriffe die Kompromittierung eines Endpunkts, um Zugriff zu erlangen oder weitere Angriffe innerhalb der Umgebung zu starten.

Die Sicherheitslage eines Geräts hängt maßgeblich von dessen Konfiguration und dem Grad seiner Verwaltung ab. Im nächsten Kapitel widmen wir uns daher Microsoft Intune und zeigen, wie es zur Absicherung von Endpunkten und zur Aufrechterhaltung einer stabilen Sicherheitslage beitragen kann.