

Defender for Identity: das Active Directory im Blick

Es gibt diesen einen Moment in jedem Sicherheitsvorfall, den niemand gern erzählt. Der Moment, in dem jemand fragt: „Wann genau hat der Angreifer eigentlich Domänenadministrator bekommen?“ — und im Raum wird es still. Nicht weil die Antwort unangenehm wäre. Sondern weil es keine gibt. Die Sicherheitsereignisprotokolle der Domänencontroller sind nach vier Tagen umgelaufen, das SIEM zieht nur die Firewall, und die letzte Person, die das Active Directory wirklich verstanden hat, ist 2019 in Rente gegangen.

Genau in diese Lücke zielt Microsoft Defender for Identity. Das Produkt hieß früher Azure Advanced Threat Protection, davor Advanced Threat Analytics, und der Dienst heißt auf dem Domänencontroller bis heute „Azure Advanced Threat Protection Sensor“ — Microsoft-Marketing ist ein Fluss, in den du nie zweimal steigst. Die Idee dahinter ist seit einem Jahrzehnt dieselbe und immer noch richtig: Setz einen Sensor genau dort hin, wo Angreifer am Ende hinwollen, nämlich auf den Domänencontroller. Lies mit, was an Kerberos-, NTLM-, LDAP- und DNS-Verkehr durchgeht. Bau daraus Verhaltensprofile. Und schlag an, wenn jemand anfängt, sich im Verzeichnis umzusehen, als hätte er es nicht selbst gebaut.

Dieser Beitrag gehört zum Handlungsfeld „Erkennen und Reagieren“ unserer Serie [Microsoft 365 Security](#). Er ist bewusst die Brücke in die Hybrid-Welt: Wer heute über Identitätssicherheit spricht, meint meistens Entra ID, Conditional Access und MFA. Aber der Kerberos-Kram im Keller läuft weiter. Er synchronisiert Konten in die Cloud, er stellt Zertifikate aus, er fördert Anmeldungen — und er ist in den meisten Sicherheitsvorfällen der letzten Jahre der Ort gewesen, an dem der Angriff seine Flughöhe gewonnen hat.

FAKTEN · Was du hier bekommst

Sensor-Topologie inklusive AD FS, AD CS und Entra Connect, die Wahrheit über gMSA und Sensor v3.x, die Audit-Policy-Anforderungen im Detail, Honeytoken-Konten, Sensitive-Tags und ein Fahrplan, der in vier bis fünf Wochen passt.

- › Voraussetzung ist eine E5- oder E5-Security-Lizenzierung. Ohne die wird das hier eine reine Lesestunde.

Wofür Defender for Identity gebaut ist — und wofür nicht

Defender for Identity ist kein Virens scanner, kein Firewall-Ersatz und keine Här tungsmaßnahme. Es ist ein Erkennungswerkzeug für identitätsbasierte Angriffe auf dein lokales Verzeichnis. Der Unterschied ist wichtig, weil er die Erwartungshaltung sortiert: Das Produkt verhindert nichts, es sieht. Und was es sieht, ist erstaunlich viel — vorausgesetzt, du hast es korrekt verkabelt.

Drei Dinge, die es sehr gut kann

- Angriffserkennung entlang der Kette: Aufklärung, Diebstahl von Zugangsdaten, Seitwärtsbewegung, Domänenherrschaft. Von der LDAP-Aufzählung bis zum Golden Ticket.

- Identitätsbezogene Sicherheitsbewertung: stehengebliebene Konten, Dienstkonten in privilegierten Gruppen, schwache Verschlüsselungstypen, unsichere Kerberos-Delegierungen, riskante AD-CS-Vorlagen. Das fließt in den Microsoft Secure Score ein.
- Kontext für die Ermittlung: Wenn ein Konto in Exchange Online auffällig wird, siehst du im selben Vorfall, was dasselbe Konto im lokalen Verzeichnis getan hat. Genau das ist der Sinn von Defender XDR.

Drei Dinge, die es nicht tut

- Es härtet nichts. Wenn dein KRBGT-Passwort seit 2014 unverändert ist, sagt dir das Produkt Bescheid — geändert hat es sich davon nicht.
- Es ersetzt keine Protokollarchivierung. Die Rohdaten bleiben begrenzt vorgehalten; wer forensische Tiefe über Monate braucht, hängt Microsoft Sentinel dran.
- Es sieht nur, was der Sensor sieht. Ein Domänencontroller ohne Sensor ist kein Randfall, sondern ein Loch in der Erkennung. Dazu gleich mehr, denn das ist der häufigste Fehler überhaupt.

Die Lizenzfrage: E5 oder gar nicht

Hier gibt es wenig zu verhandeln. Defender for Identity steckt in den großen Paketen, und der Mittelstand mit Business-Premium-Plänen schaut in die Röhre. Das ist ärgerlich, aber es ist die Realität, und es lohnt sich, sie am Anfang eines Projekts auszusprechen statt in Woche drei.

Lizenz	Enthalten?	Anmerkung
Microsoft 365 E5 / A5 / G5	Ja	Der Standardweg. Enthält auch Defender for Endpoint, das der Sensor v3.x zwingend braucht.
Microsoft 365 E5/A5/G5/F5 Security	Ja	Das Security-Add-on ohne den Rest von E5. Für viele Häuser der günstigere Weg.
Enterprise Mobility + Security E5 / A5	Ja	Der klassische EMS-Weg, historisch weit verbreitet.
Microsoft 365 F5 Security + Compliance	Ja	Für Frontline-Szenarien, mit den genannten Zusatzvoraussetzungen.
Eigenständige Defender-for-Identity-Lizenz	Ja	Existiert, wird aber selten separat gekauft.
Microsoft 365 Business Premium	Nein	Enthält Defender for Office 365 P1 und Defender for Business — aber kein Defender for Identity.
Microsoft 365 E3	Nein	Auch nicht mit Entra ID P2. Der Sprung auf E5 Security ist die einzige Abkürzung.

Lizenzwege zu Defender for Identity. Die F5-Pläne setzen zusätzlich Microsoft 365 F1/F3 oder Office 365 F3 sowie Enterprise Mobility + Security E3 voraus.

WICHTIG · Lizenzieren musst du nur die überwachten Identitäten

Gezählt werden die Benutzer, nicht die Server. Ein Sensor auf einem Domänencontroller kostet keine Zusatzlizenz — du brauchst schlicht genügend berechnete Konten im Tenant. In der Praxis heißt das: Wenn ohnehin alle auf E5 Security sitzen, ist der Sensor-Rollout lizenzrechtlich ein Nullsummenspiel.

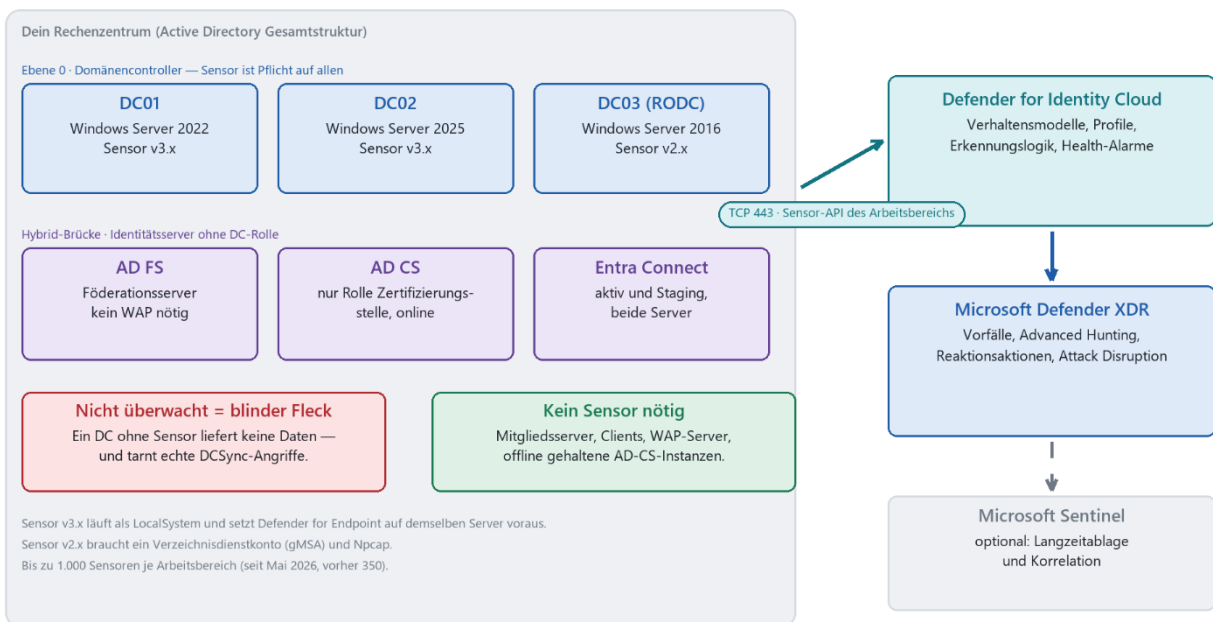
Wenn du gerade dabei bist, das Gesamtbild zu sortieren, hilft ein Blick auf [Secure Score: sinnvoll nutzen statt Punktejagd](#) — die Identitätsbewertungen von Defender for Identity landen dort und verschieben deinen Punktestand spürbar. Und wer noch am Fundament arbeitet, findet in [Tenant-Härtung: die 20 wichtigsten Schrauben](#) die Reihenfolge, in der man die Schrauben anzieht.

Sensor-Topologie: wohin die Fühler gehören

Die Architektur ist erfreulich langweilig. Ein leichtgewichtiger Sensor läuft auf jedem Server mit Identitätsrolle, liest lokal mit und schickt aufbereitete Telemetrie über TCP 443 an den Cloud-Dienst. Kein Span-Port, kein Netzwerk-Tap, keine Appliance. Eingehend braucht der Sensor gar nichts — was die Diskussion mit dem Netzwerkteam angenehm kurz hält.

Sensor-Topologie: wo die Fühler sitzen

Jeder Domänencontroller, dazu die Hybrid-Brücken AD FS, AD CS und Entra Connect



Ausgehend genügt Port 443. Eingehend braucht der Sensor nichts — nur DNS und für v2.x die Namensauflösung.

Skizze 1: Sensor-Topologie. Alle Domänencontroller plus die Hybrid-Brücken. Ausgehend genügt Port 443.

Alle Domänencontroller. Wirklich alle.

Das ist die eine Regel, an der die meisten Einführungen scheitern — und zwar nicht aus Bosheit, sondern aus Buchhaltung. Der Test-Domänencontroller im alten Rechenzentrum. Der schreibgeschützte DC in der Filiale. Der frisch heraufgestufte Server, der letzte Woche dazukam. Jeder einzelne davon ist ein Ort, an dem eine Replikationsanfrage stattfinden kann, ohne dass irgendjemand sie sieht.

Microsoft schreibt das in der Dokumentation zum DCSync-Alarm ungewöhnlich deutlich hin: Domänencontroller ohne Sensor werden von Defender for Identity nicht abgedeckt, und ein neu heraufgestufter Domänencontroller wird nicht sofort als solcher erkannt. Übersetzt: Der beste Ort für eine DCSync-Attacke ist der Domänencontroller, den dein Erkennungswerkzeug für einen gewöhnlichen Mitgliedsserver hält. Schreibgeschützte Domänencontroller werden übrigens unterstützt, Server Core auch, Nano Server nicht.

WARNUNG · Der Klassiker im Betrieb

Ein neuer Domänencontroller wird ausgerollt, der Sensor aber nicht mitinstalliert, weil er nicht im Basis-Image steckt. Vier Monate später fällt es niemandem auf, weil die Konsole nur meldet, was da ist — nicht, was fehlt.

- › Nimm den Sensor ins DC-Basis-Image oder in die Heraufstufungs-Automatisierung auf.
- › Setz einen wiederkehrenden Abgleich auf: Anzahl Domänencontroller im Verzeichnis gegen Anzahl Sensoren im Portal.
- › Die Domänenermittlungsseite im Defender-Portal (seit Juli 2026 allgemein verfügbar) zeigt dir Bereitstellungszustand und Vertrauensstellungen je Domäne auf einen Blick.

Die Hybrid-Brücke: AD FS, AD CS und Entra Connect

Hier wird es interessant, und hier hört bei den meisten Einführungen die Sorgfalt auf. Ein Domänencontroller ist offensichtlich schützenswert. Aber der Entra-Connect-Server ist ein Mitgliedsserver, der aussieht wie jeder andere — und im Bauch ein Konto trägt, das Passwort-Hashes aus dem gesamten Verzeichnis liest. Der AD-FS-Server ist ein Webserver mit einem Token-Signaturschlüssel, mit dem sich Anmeldungen für die halbe Cloud fälschen lassen. Und die Zertifizierungsstelle stellt Zertifikate aus, die als Kerberos-Anmeldeinformation taugen.

Wer nur die Domänencontroller überwacht, hat genau die drei Systeme ausgelassen, über die der Weg von lokal nach Cloud führt.

Rolle	Wohin der Sensor kommt	Was er dort liefert
AD FS	Auf die Föderationsserver. Web Application Proxy braucht keinen Sensor.	Anmeldeereignisse 1202/1203 und 4624/4625, Lesezugriffe auf den DKM-Schlüssel, Änderungen an Vertrauensstellungen. Der Alarm „Verdächtiger Lesevorgang des AD-FS-DKM-Schlüssels“ ist einer der wenigen, die praktisch nie harmlos sind.
AD CS	Nur auf Server mit der Rolle Zertifizierungsstelle. Offline gehaltene Instanzen brauchen keinen Sensor.	Ereignisse 4870, 4882, 4885, 4887, 4888, 4890, 4896. Erkennt ESC8-Anfragen, verdächtige Änderungen an AD-CS-Berechtigungen, Abschalten der Überwachungsfilter, Löschen von Datenbankeinträgen.
Entra Connect	Auf den aktiven Server und auf den Staging-Server. Beide, nicht nur einen.	Ereignis 4624, dazu Lesezugriff auf die ADSync-Datenbank. Seit Juni 2026 gibt es den eigenen Alarm „Verdächtige Authentifizierung des Entra-Connect-Kontos“ — genau für den Missbrauch des Synchronisationskontos.

Was der Sensor auf den Hybrid-Rollen zusätzlich beisteuert.

Sensor v2.x oder v3.x: die Gretchenfrage 2026

2025 und 2026 hat Microsoft den Sensor umgebaut, und zwar grundlegend. Der neue Sensor v3.x — vermarktet als „unified identity and endpoint sensor“ — ist kein separates Produkt mehr, sondern reitet auf dem Defender-for-Endpoint-Sensor mit. Das hat spürbare Folgen für die Voraussetzungen, und zwar in beide Richtungen.

Punkt	Sensor v2.x	Sensor v3.x
Betriebssystem	Windows Server 2016 bis 2025	Windows Server 2019 oder neuer, mit kumulativem

		Update von Juli 2026 oder später
Defender for Endpoint	Nicht erforderlich	Zwingend, und zwar als vollständig integrierter Server — reines Endpoint-Onboarding genügt nicht
Identität gegenüber AD	Verzeichnisdienstkonto: gMSA oder AD-Benutzer	LocalSystem, ausschließlich. Kein DSA, kein gMSA
Aktionskonto	Separates gMSA für Reaktionsaktionen	LocalSystem. Bleibt gMSA eingestellt, funktionieren Reaktionsaktionen und Attack Disruption nicht
Paketmitschnitt	Npcap wird installiert	Kein Npcap. Nach der Migration darf es weg
Ressourcendeckel	Zwei Kerne, 6 GB RAM, 6 bis 10 GB Plattenplatz	Harte Grenzen: 30 % CPU, 1,5 GB Arbeitsspeicher
Windows-Überwachung	Manuell per GPO oder PowerShell	Automatische Konfiguration, prüft alle 24 Stunden nach
Aktualisierung	Eigener Updater-Dienst, verzögerbar je Sensor	Über Windows Update mit dem Betriebssystem. Die Option „verzögertes Update“ entfällt
Bekannte Grenzen	—	Keine VPN-Integration, keine Syslog-Benachrichtigungen, Einschränkungen bei Azure ExpressRoute

Sensor v2.x und v3.x im Vergleich. Stand September 2026.

Die Migration aus dem Defender-Portal ist seit Juli 2026 allgemein verfügbar und angenehm unspektakulär: Server, die alle Voraussetzungen erfüllen, erscheinen auf der Sensorensseite als „Ready for migration“, du markierst sie und drückst auf Migrieren. Der v2.x-Sensor läuft weiter, bis der v3.x-Sensor bereit ist — es gibt also kein Erkennungsloch. In der Regel dauert das bis zu zwanzig Minuten je Server. Seit Juli 2026 lassen sich auch Domänencontroller unter Windows Server 2025 migrieren, was vorher ausdrücklich nicht ging.

TIPP • Nach der Migration bitte aufräumen

Die Migration deaktiviert den v2.x-Dienst, deinstalliert die Software aber nicht. Was übrig bleibt, ist Altlast mit Angriffsfläche.

- › Sensor v2.x deinstallieren — kann einen Neustart verlangen.
- › Npcap entfernen, sofern es nichts anderes auf dem Server nutzt.
- › Aktionskonten im Portal auf „Automatisch das lokale Systemkonto des Sensors verwenden“ umstellen. Vergisst du das, laufen Reaktionsaktionen ins Leere.
- › Erst wenn wirklich kein v2.x-Sensor mehr existiert: DSA und gMSA im Arbeitsbereich entfernen. Vorher nicht, sonst brechen die verbliebenen v2.x-Sensoren weg.

WARNUNG • Der Sensor v3.x auf Nicht-Domänencontrollern ist noch Vorschau

Auf AD-FS-, AD-CS- und Entra-Connect-Servern, die keine Domänencontroller sind, befindet sich der v3.x-Sensor in der Vorschau: manuelle Aktivierung ja, automatische Aktivierung und In-Place-Migration nein. Und wenn du v3.x ausschließlich auf diesen Servern betreiben willst, brauchst du trotzdem mindestens einen v3.x-Sensor auf einem Domänencontroller. Für Server unter Windows Server 2016 oder älter bleibt es beim v2.x-Sensor.

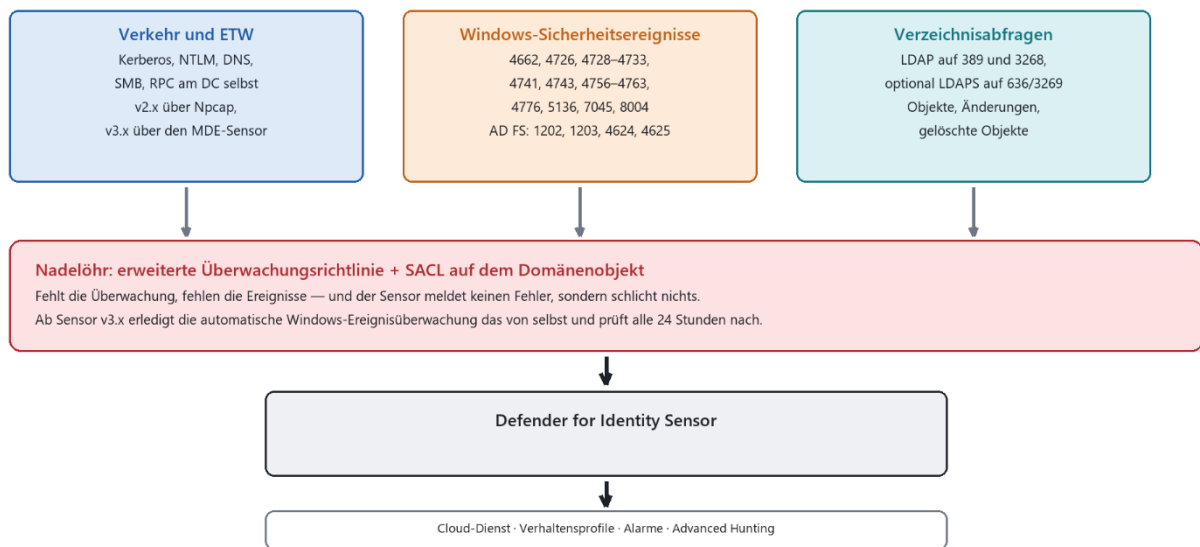
Weil v3.x ohne Defender for Endpoint schlicht nicht startet, wird das Endpoint-Onboarding auf Servern plötzlich zum kritischen Pfad. Wie das ohne Reibung läuft, steht in [Defender for Endpoint: Onboarding ohne Drama](#).

Das Kleingedruckte: gMSA, Audit-Policy und Ports

Jetzt kommt der Teil, den in Projektplänen niemand einplant und der trotzdem drei Viertel der Zeit frisst. Der Sensor ist in zehn Minuten installiert. Dass er anschließend auch etwas sieht, ist eine ganz andere Baustelle.

Woraus der Sensor seine Erkennungen baut

Drei Quellen, ein Nadelöhr: ohne Audit-Policy bleibt die mittlere Spalte leer



Skizze 2: Drei Datenquellen, ein Nadelöhr. Ohne Überwachungsrichtlinie bleibt die mittlere Spalte leer — geräuschlos.

Das Verzeichnisdienstkonto: gMSA statt Passwortzettel

Für alle v2.x-Sensoren brauchst du ein Verzeichnisdienstkonto, mit dem der Sensor das Verzeichnis abfragt. Technisch ginge ein gewöhnlicher AD-Benutzer mit Lesezugriff. Nimm ihn nicht. Ein gruppenverwaltetes Dienstkonto — gMSA — hat ein 240 Zeichen langes Passwort, das Windows alle 30 Tage selbst rotiert und das nirgendwo in einem Kennwortsafe liegt, weil es niemand kennt. Das ist der seltene Fall, in dem der sichere Weg auch der bequemere ist.

Wenn in deiner Gesamtstruktur noch nie ein gMSA im Einsatz war, fehlt der KDS-Stammschlüssel. Der wird einmal je Gesamtstruktur erzeugt:

```

# Einmal je Gesamtstruktur. Danach 10 Stunden Replikation abwarten.
Add-KdsRootKey -EffectiveImmediately

# Gruppe anlegen, die das gMSA-Passwort abrufen darf
$gMSA_AccountName = 'mdiSvc01'
$gMSA_HostsGroupName = 'mdiSvc01Group'
$gMSA_HostNames = 'DC1','DC2','DC3','ADFS1','AADC1'

Import-Module ActiveDirectory
$grp = New-ADGroup -Name $gMSA_HostsGroupName -GroupScope DomainLocal -PassThru
$gMSA_HostNames | ForEach-Object { Get-ADComputer -Identity $_ } |
    ForEach-Object { Add-ADGroupMember -Identity $gMSA_HostsGroupName -Members $_ }

New-ADServiceAccount -Name $gMSA_AccountName `
    -DNSHostName "$gMSA_AccountName.$env:USERDNSDOMAIN" `
    -PrincipalsAllowedToRetrieveManagedPassword $grp `
  
```

-KerberosEncryptionType AES128,AES256

Der Befehlsname suggeriert, der Schlüssel sei sofort wirksam. Ist er nicht — plane zehn Stunden Replikationszeit ein. In Testumgebungen mit einem einzigen Domänencontroller kann man den Wirksamkeitszeitpunkt zehn Stunden zurückdatieren; in Produktion macht man das nicht.

WICHTIG · Drei Stolpersteine beim gMSA, in der Reihenfolge ihrer Häufigkeit

Alle drei erzeugen denselben Gesundheitsalarm — „Anmeldeinformationen des Verzeichnisdienstbenutzers sind falsch“ — und alle drei haben verschiedene Ursachen.

- › Das Kerberos-Ticket des Computerkontos ist älter als die neue Gruppenmitgliedschaft. Server neu starten oder auf dem Domänencontroller die Tickets verwerfen: `klist purge -li ox3e7`.
- › Die Richtlinie „Anmelden als Dienst“ ist per GPO gesetzt, das gMSA steht aber nicht drin. Wenn du sie per Gruppenrichtlinie konfigurierst, müssen sowohl NT Service\All Services als auch das gMSA-Konto in der Liste stehen.
- › Die Leserechte auf den Container „Deleted Objects“ fehlen. Ohne sie erkennt der Sensor keine Kontolöschungen. Vergeben wird das über eine Sicherheitsgruppe mit dem gMSA als Mitglied, per dscls mit LCRP auf CN=Deleted Objects.

Und dann ist da noch die Eigenheit, die in gemischten Umgebungen für Verwirrung sorgt: Solange im Arbeitsbereich überhaupt ein DSA oder gMSA hinterlegt ist, werden dessen Anmeldeinformationen auf allen Sensoren geprüft — auch auf den v3.x-Sensoren, die sie gar nicht benutzen. Das ist so gewollt. Der Gesundheitsalarm verschwindet erst, wenn du das Konto nach vollständiger Migration aus dem Arbeitsbereich entfernst.

Audit-Policy: ohne Ereignisse keine Erkennung

Der Sensor liest Netzwerkverkehr mit, aber ein erheblicher Teil der Erkennungslogik hängt an Windows-Sicherheitsereignissen. Und die entstehen nur, wenn die erweiterte Überwachungsrichtlinie sie erzeugt. Das ist der unangenehmste Fehlermodus des ganzen Produkts: Es kracht nicht, es meldet nichts, es erkennt einfach weniger.

Kategorie	Unterkategorie	Ereignis-IDs
Anmeldeversuche	Überprüfung der Anmeldeinformationen	4776
Kontenverwaltung	Computerkontenverwaltung	4741, 4743
Kontenverwaltung	Verteilergruppenverwaltung	4753, 4763
Kontenverwaltung	Sicherheitsgruppenverwaltung	4728, 4729, 4730, 4732, 4733, 4756, 4757, 4758
Kontenverwaltung	Benutzerkontenverwaltung	4726
DS-Zugriff	Verzeichnisdienständerungen	5136
DS-Zugriff	Verzeichnisdienstzugriff	4662 — funktioniert nur mit Objektüberwachung auf dem Domänenobjekt
System	Sicherheitssystemerweiterung	7045
Sicherheitsoptionen	NTLM-Überwachung (drei Richtlinien)	8004

Erweiterte Überwachungsrichtlinie auf Domänencontrollern. Alle Unterkategorien für Erfolg und Fehler konfigurieren.

Ereignis 4662 ist der wichtigste und zugleich der fummeligste Posten. Die Unterkategorie allein reicht nicht — du musst zusätzlich auf dem Domänenobjekt eine Überwachungsliste setzen, und zwar für „Everyone“, Typ Erfolg, und getrennt für jeden nachfolgenden Objekttyp: Benutzer, Gruppen, Computer, msDS-GroupManagedServiceAccount, msDS-ManagedServiceAccount und — sobald mindestens ein Domänencontroller unter Windows Server 2025 läuft — msDS-DelegatedManagedServiceAccount. Nur Benutzerobjekte zu überwachen ergibt eine unvollständige Erkennung, und zwar eine unvollständige, die aussieht wie eine vollständige.

FAKTEN · Die Ausnahme, die man kennen sollte

Die Überwachung des Konfigurationscontainers brauchst du nur, wenn in der Gesamtstruktur jemals Exchange installiert war. Der Konfigurationscontainer wird gesamtstrukturweit repliziert — du konfigurierst ihn also einmal, auch wenn der Gesundheitsalarm für mehrere Domänen erscheint.

- › Ereignis 1644 wird nicht mehr benötigt. Wenn du früher „15 Field Engineering“ oder die Suchschwellenwerte in der NTDS-Registrierung gesetzt hast, dürfen die Werte weg.

Der schnelle Weg: Skripte statt Klickstrecke

Die gute Nachricht: Du musst das nicht von Hand klicken. Es gibt drei Werkzeuge, und in dieser Reihenfolge setzt man sie ein.

```
# 1) Bereitschaft prüfen - findet fehlende Voraussetzungen auf allen DCs
#   Verfügbar im Defender-Portal unter Identitäten > Tools
.\Test-MdiReadiness.ps1

# 2) Ist-Zustand der Überwachung als HTML-Bericht
New-MDIConfigurationReport -Path 'C:\Reports' -Mode Domain `
    -Identity 'CONTOSO\svc-mdi' -OpenHtmlReport

# 3) Alles Nötige per GPO setzen und verknüpfen
Set-MDIConfiguration -Mode Domain -Configuration All

# Kontrolle auf dem DC
auditpol.exe /get /category:*
```

Ab Sensor v3.x geht es noch bequemer: Im Defender-Portal unter Einstellungen > Identitäten > Erweiterte Funktionen schaltest du „Automatische Windows-Überwachungskonfiguration“ ein. Der Sensor prüft dann alle 24 Stunden den Ist-Zustand, erkennt Lücken und korrigiert sie selbst — inklusive der SACL auf dem Domänenobjekt, der NTLM-Registrierungswerte und der Konfigurationspartition. Seit August 2026 gilt das auch für AD-FS-, AD-CS- und Entra-Connect-Server. Die Funktion ist seit April 2026 allgemein verfügbar und die einzige Antwort auf die Frage, wer die Überwachung eigentlich nachhält, wenn jemand die GPO überschreibt.

WARNUNG · Gruppenrichtlinie und lokale Einstellung können sich beißen

Die automatische Überwachung schreibt in die lokale Sicherheitsrichtlinie des Servers. Eine GPO, die dieselben Einstellungen anders setzt, gewinnt beim nächsten Aktualisieren — und dann korrigiert der Sensor wieder zurück. Entscheide dich für einen Weg, nicht für beide.

- › Bekanntes Verhalten: In manchen v3.x-Umgebungen bleiben Gesundheitsalarme zur Ereignisüberwachung stehen, obwohl alles korrekt eingestellt ist. Das passiert vor allem bei manueller Konfiguration über GPO oder PowerShell. Die Erkennung ist davon nicht betroffen; die Lösung ist, auf die automatische Konfiguration umzustellen.

Ports und Netzwerk

Ausgehend braucht der Sensor genau eine Verbindung: HTTPS auf 443 zur Sensor-API-Adresse deines Arbeitsbereichs — die setzt sich aus dem Arbeitsbereichsnamen und der Dienstdomäne zusammen und steht im Portal. SSL-Inspektion wird nicht unterstützt — das ist der Punkt, an dem viele Bereitstellungen an einer Proxy-Richtlinie hängenbleiben. Wer keinen Proxy hat, arbeitet mit dem Dienstag AzureAdvancedThreatProtection in der Azure-IP-Liste; ExpressRoute geht über Microsoft-Peering mit der BGP-Community 12076:5220.

Zweck	Protokoll und Port	Anmerkung
Cloud-Anbindung	TCP 443 ausgehend	Einzige zwingende Internetverbindung
Namensauflösung	TCP und UDP 53	Zum DNS-Server
Sensor-Updater	TCP 444 auf localhost	Nur relevant, wenn eine lokale Firewall Loopback blockt
Netzwerknamensauflösung	TCP 135, UDP 137, TCP 3389	Zur Auflösung von IP zu Computernamen. Einer der drei genügt, empfohlen sind alle
RADIUS-Buchhaltung	UDP 1813 eingehend	Nur bei VPN-Integration — die es beim v3.x-Sensor nicht mehr gibt
Mehrere Gesamtstrukturen	TCP/UDP 389, TCP 636, 3268, 3269	LDAP und Global Catalog. Umstellung auf LDAPS erfordert einen Supportfall

Interne Ports für den Sensor v2.x. Der v3.x-Sensor nutzt dieselben URLs wie Defender for Endpoint.

Köder auslegen: Honeytoken-Konten und Sensitive-Tags

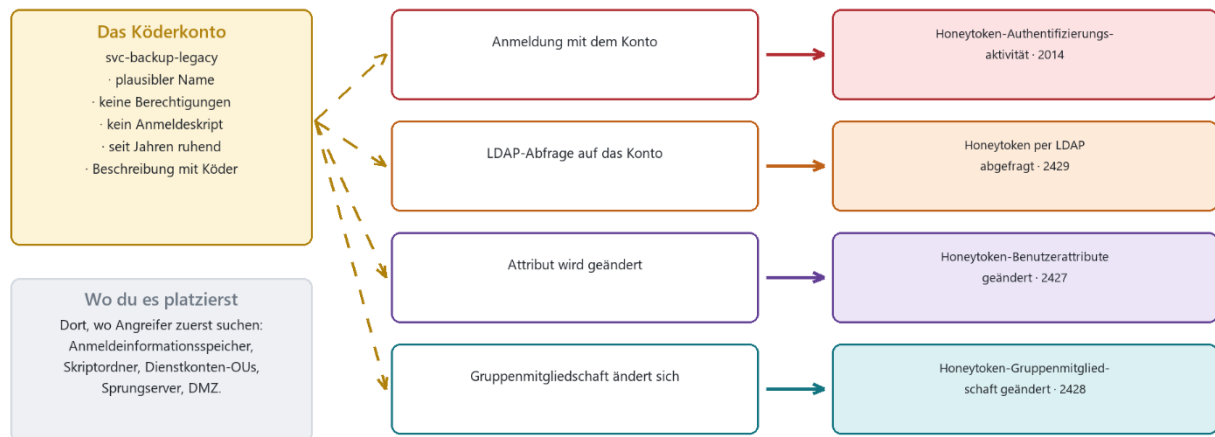
Zwei Werkzeuge, fünf Minuten Aufwand, und beide werden konsequent ignoriert. Das ist bemerkenswert, weil sie zu den wenigen Stellschrauben gehören, an denen du die Erkennungsqualität ohne Lizenzaufschlag und ohne Serverneustart deutlich verbesserst.

Honeytoken: das Konto, das niemand anfassen darf

Ein Honeytoken ist ein Köderkonto ohne Geschäftszweck. Es tut nichts, es meldet sich nirgends an, es steht in keinem Skript. Genau deshalb ist jede Aktivität darauf per Definition verdächtig: Es gibt keinen legitimen Grund, warum irgendjemand sich damit anmelden, es per LDAP abfragen oder seine Gruppenmitgliedschaft ändern sollte. Falsch-positive Meldungen gehen gegen null — der seltene Fall eines Alarms, den du nicht triagieren, sondern nur bearbeiten musst.

Die Honeytoken-Falle: ein Konto, das niemand benutzen darf

Vier Wege, wie ein Angreifer hineintappt — und was dabei ausgelöst wird



Getaggt wird im Defender-Portal unter Einstellungen > Identitäten > Honeytoken. Das Tag gilt für Benutzer und Geräte.

Skizze 3: Vier Wege in die Honeytoken-Falle und die zugehörigen Alarme mit externer ID.

Alarm	Externe ID	Wird ausgelöst durch
Honeytoken-Authentifizierungsaktivität	2014	Irgendeine Anmeldung mit dem Köderkonto. Der lauteste und eindeutigste der vier.
Honeytoken wurde per LDAP abgefragt	2429	Gezielte LDAP-Abfrage auf das Konto — typisch für Aufklärungswerkzeuge, die Dienstkonten einsammeln.
Honeytoken-Benutzerattribute geändert	2427	Änderung an Attributen des Köderkontos, etwa Setzen eines SPN oder Manipulation von Delegierungsattributen.
Honeytoken-Gruppenmitgliedschaft geändert	2428	Jemand nimmt das Köderkonto in eine Gruppe auf — meistens in eine privilegierte.

Die vier Honeytoken-Alarme. Alle setzen voraus, dass das Konto im Defender-Portal als Honeytoken markiert ist.

TIPP • So baust du ein Köderkonto, das auch als Köder taugt

Ein Konto namens „honeypot-test“ in der OU „Testkonten“ fängt niemanden. Ein Köder muss aussehen wie Beute.

- › Plausibler Name aus deiner eigenen Namenskonvention: svc-sql-legacy, svc-backup-alt, adm-migration.
- › Beschreibungsfeld füllen — Angreifer lesen Beschreibungen und Kommentarfelder. „Dienstkonto Altsystem, Passwort siehe Wiki“ wirkt Wunder.
- › Keinerlei echte Berechtigungen. Das Konto muss wertlos aussehen und wertlos sein.
- › Anmeldeinformationen bewusst dort ablegen, wo gesucht wird: Skriptordner, Anmeldeinformationsspeicher auf Sprungservern, DMZ-Systeme.
- › Ein paar Stück streuen, nicht eins. Und dann dokumentieren, damit in zwei Jahren niemand aufräumt und das Konto „endlich mal sinnvoll benutzt“.

Ein hübscher Nebeneffekt: Ein Honeytoken ist der einfachste Funktionstest für die gesamte Kette. Melde dich einmal absichtlich damit an und schau, ob der Alarm im Portal landet, ob die

Benachrichtigung ankommt und ob die Bereitschaft reagiert. Das ist billiger als eine Übung und ehrlicher als eine Statusfolie.

Sensitive-Tags: wer automatisch als wertvoll gilt

Defender for Identity markiert bestimmte Konten und Systeme automatisch als sensibel, und manche Erkennungen hängen direkt an diesem Tag — die Erkennung „Verdächtige Ergänzungen zu sensiblen Gruppen“ etwa funktioniert ohne die Markierung nicht sinnvoll. Automatisch sensibel sind alle Mitglieder der klassischen privilegierten AD-Gruppen, einschließlich verschachtelter Mitgliedschaften:

- Domänen-Admins, Organisations-Admins, Schema-Admins, Domänencontroller, schreibgeschützte Domänencontroller und deren Organisationsvariante
- Administratoren, Hauptbenutzer, Konten-Operatoren, Server-Operatoren, Druck-Operatoren, Sicherungs-Operatoren, Replikations-Operator, Netzwerkkonfigurations-Operatoren
- Ersteller-Besitzer von Gruppenrichtlinien, Eingehende Gesamtstruktur-Vertrauensersteller, Microsoft Exchange Server
- Zusätzlich automatisch als hochwertig eingestuft: Zertifizierungsstellen, DHCP-Server, DNS-Server, Exchange-Server und alles, was das Recht „Verzeichnisänderungen replizieren“ trägt

Bemerkenswert ist, was fehlt: Remotedesktopbenutzer wurden bis September 2018 automatisch als sensibel geführt, seither nicht mehr. Wer eine alte Umgebung übernimmt, findet dort also manchmal Altbestände mit Markierung und daneben identische Gruppen ohne. Das ist kein Fehler, das ist Geschichte.

WICHTIG · Was du manuell markieren solltest

Die Automatik kennt die Windows-Standardgruppen. Sie kennt nicht deine Organisation.

- › Konten mit Zugriff auf Kronjuwelen, die technisch nicht privilegiert sind: Finanzbuchhaltung, Konstruktion, Personalabteilung, Forschung.
- › Eigene Tier-o-Gruppen mit Fantasienamen, die nicht in der Standardliste stehen.
- › Sprungserver und Verwaltungsarbeitsplätze — das Sensitive-Tag gibt es auch für Geräte.
- › Dienstkonto mit weitreichenden Rechten: Sicherungssoftware, Überwachungssysteme, Softwareverteilung. Das sind statistisch die interessantesten Ziele überhaupt.

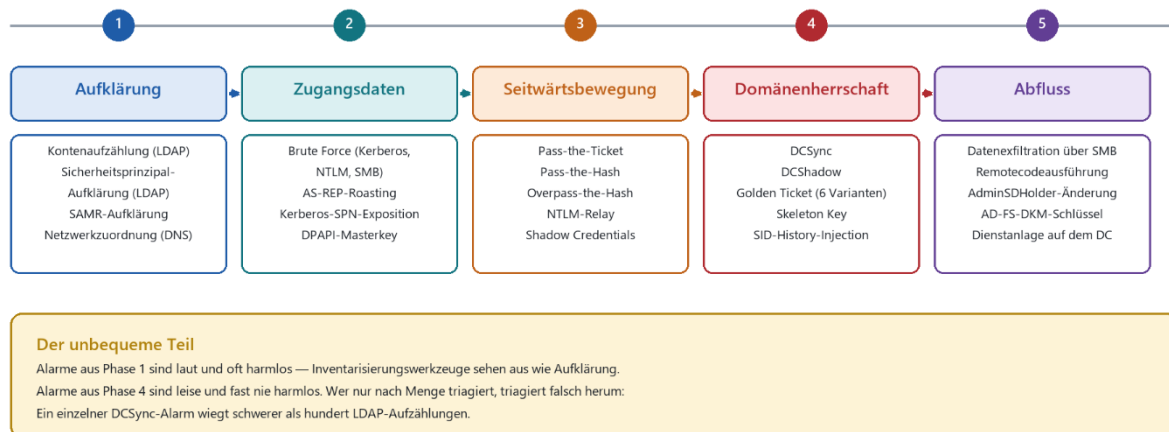
Wer Konten und Rechte grundsätzlich aufräumen will, findet den passenden Rahmen in [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#). Und für die andere Seite der Medaille — Notfallkonten, die bewusst außerhalb der normalen Regeln stehen und deshalb besonders sorgfältig überwacht gehören — lohnt [Break-Glass-Konten anlegen und überwachen](#).

Was der Sensor erkennt — und was du damit anfängst

Kommen wir zum eigentlichen Punkt. Defender for Identity kennt inzwischen über hundert Erkennungen, und die Liste wächst in praktisch jedem Monat. Interessant sind nicht alle. Interessant sind die, die einen Angriff in einer Phase erwischen, in der man ihn noch abbrechen kann.

Die Angriffskette im Verzeichnis — und wo der Sensor anschlägt

Von der ersten LDAP-Abfrage bis zum gefälschten Ticket



Alarmnamen gekürzt. Jeder Alarm trägt eine externe ID (z. B. 2006 für DCSync) — die bleibt stabil, der Anzeigename nicht.

Skizze 4: Die Angriffskette im Verzeichnis und die Alarme, die in jeder Phase greifen.

Aufklärung: das laute Vorspiel

Jeder Angreifer, der im Netz landet, macht zuerst dasselbe wie du an deinem ersten Arbeitstag: Er schaut sich um. Wer ist Admin? Welche Server gibt es? Welche Konten haben Dienstprinzipalnamen und lassen sich damit rösten? Defender for Identity erkennt die Kontenaufzählung per LDAP (2437), die Sicherheitsprinzipal-Aufklärung per LDAP (2038), die Benutzer- und Gruppenmitgliedschaftsaufklärung per SAMR (2021) und die Netzwerkzuordnung über DNS (2007).

Seit Januar 2026 sind Erkennungen dazugekommen, die genau auf die leiseren Varianten zielen: die Aufzählung des Verzeichnisses über Active Directory Web Services statt über klassisches LDAP, die Aufzählung von AD-CS-Zertifikatvorlagen und ein Kerberoasting-Versuch, der sich hinter einer unauffälligen LDAP-Suche versteckt. Das ist die richtige Antwort auf Werkzeuge, die inzwischen ausdrücklich damit werben, klassische Erkennungen zu umgehen.

Der Haken: Aufklärungsalarme sind laut. Dein Inventarisierungssystem, deine Softwareverteilung und dein Schwachstellenscanner tun ungefähr dasselbe wie ein Angreifer, nur mit besserem Gewissen. Wer hier keine Ausnahmen pflegt, hat nach zwei Wochen eine Konsole voller Meldungen und ein Team, das nicht mehr hinschaut. Wie so ein Vorlauf in der Realität aussieht — inklusive der Frage, warum niemand die Aufklärungsphase bemerkt hat — steht in Schritt 6 des Dokuments [TerminalFix und der Berlin-Hack](#).

Pass-the-Ticket, Overpass-the-Hash und der Kerberos-Zoo

Wenn Zugangsdaten erst einmal gestohlen sind, beginnt die Seitwärtsbewegung — und die läuft in Windows-Netzen fast immer über Kerberos. Beim Pass-the-Ticket klaut der Angreifer ein Kerberos-Ticket von einem Rechner und legt es auf einem anderen vor. Defender for Identity erkennt das daran, dass dasselbe Ticket auf zwei verschiedenen Computern auftaucht (Alarm 2018) — eine erfreulich physikalische Beweisführung. Beim Overpass-the-Hash wird ein gestohlener NTLM-Hash benutzt, um ein legitimes Kerberos-Ticket zu beantragen (2002), und in der Variante

mit erzwungenem Verschlüsselungstyp fällt zusätzlich auf, dass jemand künstlich auf schwaches RC4 heruntergehandelt hat (2008).

Seit Januar 2026 gibt es zusätzlich Erkennungen für eine TGT-Anforderung, die als TGS-REQ getarnt daherkommt, und für Kerberos-Key-List-Angriffe. Beides Techniken, die vor drei Jahren noch Konferenzvorträge waren und heute in Werkzeugkästen stecken.

Dieser Artikel bleibt bei der Erkennung. Wenn du verstehen willst, warum ein Ticket überhaupt auf einem zweiten Rechner funktioniert, was in einem TGT eigentlich drinsteht, wie das PAC-Feld missbraucht wird und wo die Delegierungsvarianten ihre Sollbruchstellen haben, liegt die Tiefe im [Kompetenzbereich Microsoft Kerberos](#). Ohne dieses Grundverständnis triagierst du Kerberos-Alarme wie Wetterberichte: Man liest sie, aber man weiß nicht, was zu tun ist.

DCSync: die Replikationsanfrage, die keine sein sollte

DCSync ist elegant und deshalb gefährlich. Der Angreifer greift nicht die Datenbank an, er fragt höflich nach. Active Directory repliziert Änderungen zwischen Domänencontrollern, und wer die Rechte „Verzeichnisänderungen replizieren“ und „Verzeichnisänderungen alle replizieren“ besitzt, darf eine Replikation anstoßen — und bekommt dabei Passwort-Hashes geliefert. Inklusive dem des KRBTGT-Kontos. Ab da ist die Domäne vorbei.

Der Alarm (2006, hoch) feuert, wenn eine Replikationsanfrage von einem Rechner kommt, der kein Domänencontroller ist. Die Logik wurde inzwischen erweitert und deckt auch Fälle ab, in denen die Quell-IP hinter einem NAT-Gerät liegt. Seit Juni 2026 gibt es zusätzlich eine XDR-seitige DCSync-Erkennung.

WARNUNG · Warum ein DCSync-Alarm anders behandelt gehört als alle anderen

Es gibt legitime DCSync-Vorgänge — Entra Connect mit Passwort-Hash-Synchronisierung macht genau das, und manche Sicherungs- oder Migrationswerkzeuge auch. Aber die Liste der legitimen Quellen ist kurz, endlich und dir bekannt. Alles, was nicht darauf steht, ist ein Notfall.

- › Leg diese Liste vorab an, nicht im Vorfall. Wer um drei Uhr morgens erst recherchieren muss, ob dieser eine Server das darf, verliert eine Stunde.
- › Prüfe regelmäßig, wer die Replikationsrechte überhaupt hat. Die Sicherheitsbewertung in Defender for Identity listet das aus.
- › Ein Domänencontroller ohne Sensor ist bei DCSync besonders bitter: Von dort aus sieht die Anfrage aus wie legitime Replikation.

Golden Ticket und die KRBTGT-Frage

Wer den KRBTGT-Hash hat, kann sich selbst Kerberos-Tickets ausstellen — mit beliebigen Gruppenmitgliedschaften und beliebiger Laufzeit. Das ist Persistenz in Reinform, und sie überlebt Passwortänderungen, Kontosperrungen und meistens auch die Neuinstallation der betroffenen Server. Defender for Identity erkennt Golden Tickets nicht an einem Merkmal, sondern an mehreren Ungereimtheiten in gefälschten Tickets.

Alarm	ID	Auffälligkeit
Nicht existierendes Konto	2027	Das Ticket gehört zu einem Konto, das es im Verzeichnis nicht (mehr) gibt.

Ticketanomalie	2032	Struktur oder Felder des Tickets passen nicht zu dem, was ein echter Domänencontroller ausstellen würde.
Ticketanomalie über RBCD	2040	Variante, die ressourcenbasierte eingeschränkte Delegation als Tarnung nutzt.
Zeitanomalie	2022	Die Gültigkeitsdauer ist länger, als die Kerberos-Richtlinie der Domäne zulässt.
Verschlüsselungsherabstufung	2009	Das Ticket verwendet schwaches RC4, wo AES erwartet würde.
Gefälschte Autorisierungsdaten	2013	Das PAC-Feld behauptet Gruppenmitgliedschaften, die das Konto nicht hat.

Die Golden-Ticket-Erkennungen und woran sie jeweils festmachen.

Die praktische Konsequenz ist unbequem: Wenn ein Golden Ticket bestätigt ist, hilft nur die zweifache Zurücksetzung des KRBTGT-Passworts, mit ausreichendem Abstand zwischen den beiden Durchgängen, damit die Replikation nachkommt. Wer das zu schnell hintereinander macht, kippt die eigene Kerberos-Infrastruktur. Wer es gar nicht macht, hat den Angreifer weiterhin im Haus. Und wer das erste Mal im Ernstfall darüber nachdenkt, hat schon verloren.

Genau deshalb gehört diese Prozedur getestet und dokumentiert in den [Incident-Response-Plan für Microsoft 365](#) und einmal jährlich in eine [Feuerwehübung: Security-Notfälle im Team trainieren](#). Wer wissen will, ob die Erkennungen tatsächlich greifen, statt es nur zu hoffen, findet die härtere Variante in [Red-Team-Übung: der kontrollierte Angriff](#).

NTLM: der Altlastenkanal

Ein erheblicher Teil der Erkennungen hängt an NTLM — Pass-the-Hash (2017), NTLM-Relay über Exchange-Konten (2037), Manipulation der NTLM-Authentifizierung entlang CVE-2019-1040 (2039), DFSCoerce, erzwungene Authentifizierung über den Druckwarteschlangendienst. Der gemeinsame Nenner: NTLM ist ein Protokoll aus einer Zeit, in der Netzwerke vertrauenswürdig waren.

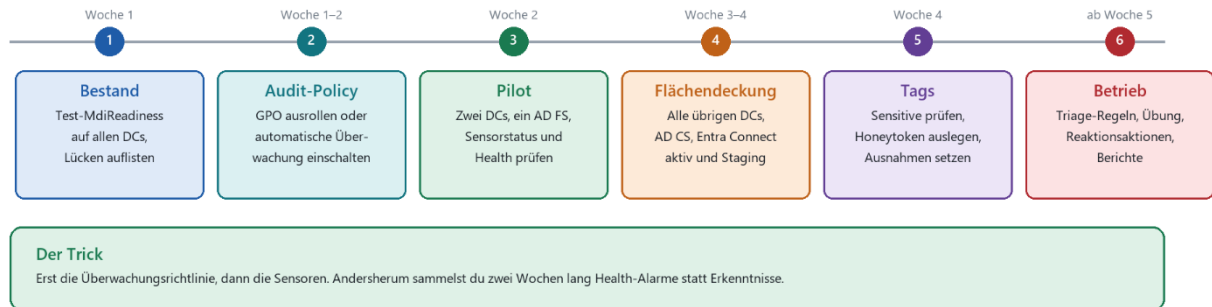
Die NTLM-Überwachung ist deshalb kein Selbstzweck. Sie ist die Vorstufe zum Abschalten — erst siehst du, wer noch NTLM spricht, dann drehst du den Hahn zu. Der Weg dorthin steht in [Legacy Authentication endgültig abschalten](#), und wer die Anmeldung insgesamt auf ein anderes Fundament stellen will, findet in [Passwordless: FIDO2 und Passkeys in der Praxis](#) die Zielrichtung.

Vom Alarm zur Handlung: Betrieb statt Konsole

Erkennung ohne Reaktion ist ein teures Hobby. Defender for Identity kann inzwischen selbst eingreifen: Konten deaktivieren, Passwörter zurücksetzen, Benutzer als kompromittiert markieren. Beim v3.x-Sensor läuft das über das lokale Systemkonto, autorisiert über Entra-ID-Rollen und protokolliert dort — ein deutlicher Fortschritt gegenüber dem gMSA-Konstrukt. Achte nur darauf, dass du die Aktionskonten nach der Migration tatsächlich umgestellt hast, sonst passiert schlicht nichts.

Ein Fahrplan, der ohne Nachtschichten auskommt

Sechs Schritte vom leeren Arbeitsbereich zum belastbaren Betrieb



Skizze 5: Ein Einführungsfahrplan, der in vier bis fünf Wochen passt.

Für den laufenden Betrieb brauchst du drei Dinge, die technisch nichts mit dem Sensor zu tun haben: einen Weg, wie Alarme zu Menschen kommen (siehe [Alert Policies und Benachrichtigungen richtig aufsetzen](#)), eine Vorgehensweise für den Fall, dass ein Konto tatsächlich übernommen wurde (siehe [Kompromittiertes Konto erkennen und aufräumen](#)), und eine Entscheidung darüber, ob die Daten zusätzlich in ein SIEM sollen (siehe [Microsoft Sentinel anbinden: wann es sich lohnt](#)).

WICHTIG · Bevor der erste Sensor läuft: die Mitbestimmung

Defender for Identity erzeugt personenbezogene Auswertungen über das Anmeldeverhalten der Belegschaft. Das ist mitbestimmungspflichtig, und der Betriebsrat erfährt es besser vorher als aus dem ersten Alarm.

- › Die Bewertung, was genau darunterfällt und wie man eine belastbare Vereinbarung formuliert, steht in „Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist“.
- › Praktisch hilfreich: Der Zugriff im Defender-Portal lässt sich auf Domänen (allgemein verfügbar) und seit Kurzem auf Organisationseinheiten (Vorschau) eingrenzen. Damit kannst du zusagen, wer welche Identitäten überhaupt sehen darf.

Der vollständige Beitrag dazu: [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#). Und wenn der Anlass für das ganze Vorhaben regulatorisch ist, ordnet [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) die Erkennung von Identitätsangriffen in den Pflichtenkatalog ein.

Häufige Fragen

Brauche ich wirklich auf jedem Domänencontroller einen Sensor?

Ja. Nicht als Empfehlung, sondern als Funktionsvoraussetzung. Ein Domänencontroller ohne Sensor liefert keine Daten, und Microsoft weist ausdrücklich darauf hin, dass solche Systeme nicht abgedeckt sind. Bei DCSync kommt hinzu, dass ein nicht registrierter Domänencontroller die Erkennung sogar aktiv untergräbt — die Replikationsanfrage sieht dann legitim aus. Schreibgeschützte Domänencontroller werden unterstützt und gehören ebenfalls dazu.

Wir haben noch Windows Server 2016 als Domänencontroller. Und jetzt?

Dann bleibt es dort beim Sensor v2.x, inklusive Verzeichnisdienstkonto, manueller Überwachungskonfiguration und Npcap. Der v3.x-Sensor setzt Windows Server 2019 oder neuer voraus, dazu ein kumulatives Update von Juli 2026 oder später. Gemischter Betrieb ist ausdrücklich vorgesehen — du kannst also die neueren Domänencontroller migrieren und die alten weiterlaufen lassen. Denk nur daran, dass die gMSA-Prüfung dann weiter auf allen Sensoren stattfindet und du das Konto erst entfernen darfst, wenn wirklich kein v2.x-Sensor mehr existiert.

Ersetzt Defender for Identity unser SIEM?

Nein, und es will es auch nicht. Es liefert Erkennungen und Vorfälle für die Identitätsschicht, mit begrenzter Datenvorhaltung. Wer Protokolle über Monate braucht, wer Daten aus Firewalls, Nicht-Microsoft-Systemen und OT korrelieren will oder wer regulatorische Aufbewahrungsfristen erfüllen muss, hängt Microsoft Sentinel dran. Umgekehrt ist Sentinel ohne die Erkennungslogik von Defender for Identity ein leeres Fass: Die Verhaltensmodelle für Kerberos-Angriffe bekommst du dort nicht geschenkt.

Wie laut wird das in den ersten Wochen?

Lauter, als dir lieb ist, und leiser, als du befürchtest. Es gibt eine Lernphase, in der der Dienst Verhaltensprofile aufbaut — bei manchen Erkennungen 30 Tage, bei anderen gar keine. Die Aufklärungsalarme aus Phase eins produzieren am Anfang den meisten Lärm, weil legitime Werkzeuge dasselbe tun wie Angreifer. Plane zwei bis drei Wochen ein, in denen ihr Ausnahmen für Inventarisierung, Schwachstellenscanner und Softwareverteilung pflegt. Danach wird es ruhig — und wenn es dann laut wird, hört man hin.

Was ist mit reinen Cloud-Umgebungen ohne lokales AD?

Dann brauchst du keinen Sensor, aber Defender for Identity ist trotzdem nicht wertlos: Ein wachsender Teil der Erkennungen bezieht sich inzwischen auf Microsoft Entra ID selbst — verdächtige Anmeldungen, Missbrauch von Dienstprinzipalen, auffällige Aktivitäten nach einer Rollenerhöhung, gestohlene Sitzungscookies. Der Schwerpunkt dieses Artikels liegt bewusst auf der lokalen Seite, weil dort die Sensor-Arbeit anfällt. Für den Cloud-Anteil ist die entscheidende Ergänzung eine saubere Richtlinienbasis, wie sie in „Conditional Access: Baselines, die nicht nerven“ beschrieben ist.

Der Sensor läuft, aber die Konsole meldet fehlende Überwachung. Warum?

Drei übliche Verdächtige. Erstens: Die erweiterte Überwachungsrichtlinie ist gesetzt, aber die Objektüberwachung auf dem Domänenobjekt fehlt — dann kommt Ereignis 4662 nicht zustande. Zweitens: Die Überwachung ist nur für Benutzerobjekte konfiguriert statt für alle geforderten Objekttypen. Drittens, und speziell bei v3.x: Es gibt ein bekanntes Verhalten, bei dem Gesundheitsalarme trotz korrekter manueller Konfiguration stehenbleiben. Die Erkennung ist

davon nicht betroffen; die Lösung ist, auf die automatische Windows-Überwachungskonfiguration umzustellen.

Lohnt sich externe Unterstützung bei der Einführung?

Die Sensorinstallation schafft jedes Team allein. Wo es sich regelmäßig lohnt, ist die Ecke davor und danach: die vollständige Inventur der Identitätsserver, die Audit-Policy im Zusammenspiel mit vorhandenen Gruppenrichtlinien, die Triage-Regeln und die Frage, welche Alarmer welche Reaktion auslösen. Wir machen das im Rahmen der [Microsoft-365-Security-Beratung](#); wenn das Team den Betrieb selbst übernehmen soll, ist die [Schulung Microsoft 365 Security](#) der direktere Weg. Und wer der Geschäftsführung erklären muss, warum ein E5-Security-Upgrade nötig ist, findet die Argumentationslinie in [Security-Reporting für die Geschäftsführung](#).

Fazit

Defender for Identity ist eines der wenigen Sicherheitsprodukte, bei denen der Nutzen nicht an der Konfigurationstiefe hängt, sondern an der Vollständigkeit. Ein perfekt eingestellter Sensor auf achtzig Prozent der Domänencontroller ist schlechter als ein Standardsensor auf allen. Die Erkennungslogik kommt aus der Cloud, die Verhaltensmodelle baut Microsoft, die Alarmer sind erstaunlich treffsicher. Deine Aufgabe reduziert sich auf drei Dinge: alle Identitätsserver erwischen, die Überwachung korrekt einstellen und die Alarmer zu jemandem bringen, der sie liest.

2026 ist dabei ein gutes Jahr für den Einstieg. Der v3.x-Sensor hat das nervigste Stück Handarbeit beseitigt — kein Verzeichnisdienstkonto, keine gMSA-Rechtevergabe, kein Npcap, keine manuelle Audit-Policy, dafür automatische Konfiguration mit täglicher Nachkontrolle. Der Preis dafür ist eine harte Kopplung an Defender for Endpoint und an aktuelle Betriebssystemstände. Das ist ein fairer Handel, solange man ihn vorher kennt und nicht in Woche drei entdeckt.

Und dann sind da die zwei Dinge, die fünf Minuten kosten und trotzdem fast nie gemacht werden: ein paar Honeytoken-Konten auslegen und die Sensitive-Markierungen an die eigene Organisation anpassen. Wenn du nach diesem Artikel nur zwei Sachen umsetzt, dann diese. Ein Köderkonto, das nach drei Monaten anschlägt, ist die billigste Frühwarnung, die du bekommen kannst — und der einzige Alarm, bei dem niemand fragen muss, ob er wohl echt ist.

Weiter im Handlungsfeld

- › [Microsoft 365 Security](#) — die Übersicht über alle Handlungsfelder
- › [Kompetenzbereich Microsoft Kerberos](#) — die Tiefe zu Tickets, Delegation und den Angriffen darauf
- › [TerminalFix und der Berlin-Hack](#) — der komplette Angriffsverlauf, Schritt 6 ist die AD-Aufklärung
- › [Defender for Endpoint: Onboarding ohne Drama](#) — Voraussetzung für den Sensor v3.x
- › [Ransomware-Vorsorge in Microsoft 365](#) — warum Domänenherrschaft und Verschlüsselung zusammengehören
- › [Conditional Access: Baselines, die nicht nerven](#) — die Cloud-Seite derselben Identität
- › [Microsoft-365-Security-Beratung](#) — Unterstützung bei Inventur, Audit-Policy und Triage