

Securing the hybrid identity infrastructure



Martin Schwartzman

Senior Product Manager @ Microsoft Defender for Identity

@martin77s



Threats related to identities



Benjamin Delpy @gentilkiwi · Sep 16

A new #mimikatz release with #zerologon / CVE-2020-1472 detection, exploit, DCSync support and a lots of love inside ❤️

It now uses direct RPC call (fast and supports unauthenticated on Windows)

> [github.com/gentilkiwi/mim...](https://github.com/gentilkiwi/mimikatz)

Thank you: @SecuraBV

Abusing Exchange: One API call away from Domain Admin

🕒 11 minute read

In most organisations using Active Directory and Exchange, Exchange servers have such high privileges that being an Administrator on an Exchange server is enough to escalate to Domain Admin. Recently I came across a blog from the ZDI, in which they detail a way to let Exchange authenticate to attackers using NTLM over HTTP. This can be combined with an NTLM relay attack to escalate from any user with a

This phishing attack uses an unusual trick to spread further

Attackers enroll Outlook on BYO devices with Azure AD and then spread SharePoint PDF lures.



Written by Liam Tung, Contributor on Jan. 27, 2022

Okta Notifies Customers of LAPSUS\$ Attack

March 25, 2022

in LinkedIn

f Facebook

t Twitter

✉ Send

↻ Embed

Okta, which markets itself as a “leading provider of identity” in the healthcare, public sector, energy, financial services, technology, travel and hospitality, and nonprofit industries, has notified some of its customers that data may have been accessed by cybercriminal group Lapsus\$. (Late breaking news—Lapsus\$ may be a teenager living in the U.K.). According to Okta, in late January it “detected an attempt to compromise the account of a third party customer support engineer working for one of our subprocessors.” According to the forensic investigation, an attacker had access to the support engineer’s laptop for five days in January.

WRITTEN BY:

Robinson+Cole
Robinson+Cole Data Privacy
+ Security Insider

Contact

+ Follow



Linn Freedman

+ Follow

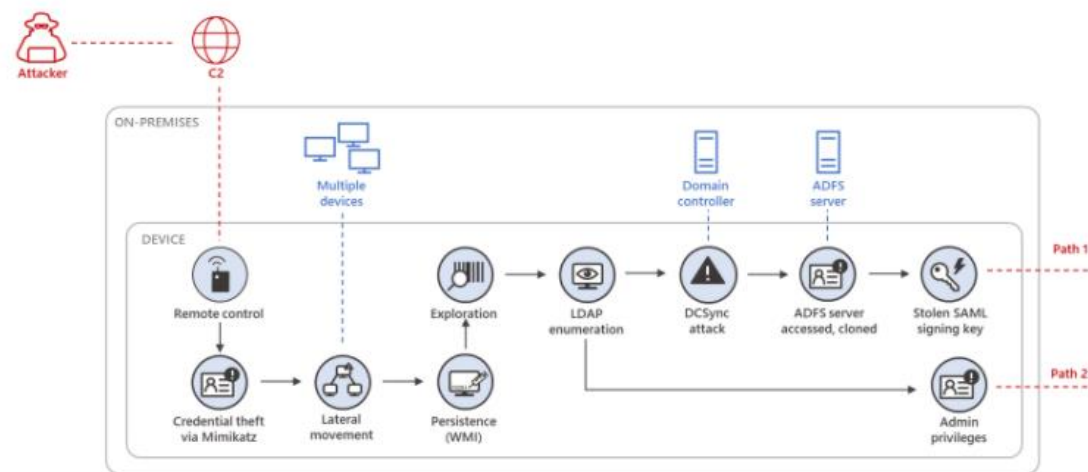
PUBLISHED IN:

Cyber Attacks

+ Follow

Solorigate

...after gaining administrative privileges in the organization’s on-premises network, and with access to the AD FS server itself, the attacker access and extract the SAML signing certificate. [December 28 2020]



PrintNightmare exploit

CVE-2021-1675 / CVE-2021-34527 exploit.

Reflective DLL implementation of the PrintNightmare PoC by Cornelis de Plaa (@Cneelis). The exploit was originally created by Zhiniang Peng (@edwardzpeng) & Xuefeng Li (@lxf02942370).

- It can be used as Remote Code Execution (RCE) exploit (screenshot 1),
- It can be used for Privilege Escalation (screenshot 2).

This implementation has some advantages compared to other public exploits:

- It uses MS-PAR protocol instead of MS-RPRN (credits @cube0x0).
- It is in Reflective DLL form, so can be used directly from Cobaltstrike or other C2 framework.
- It automatically finds the path of the printer driver.

Microsoft Fixes Azure Active Directory Issue Exposing Private Key Data

By Kurt Mackie | 11/18/2021

Microsoft announced on Wednesday that it fixed an Azure Active Directory private key data storage gaffe that affects Azure application subscribers, but affected organizations nonetheless should carry out specific assessment and remediation tasks.

Affected organizations were notified via the Azure Service Health Notifications message center, Microsoft indicated.

What is the PrintNightmare Vulnerability?

The vulnerability exists on all devices running Windows 7 or higher. It resides in the Windows Print Spooler service and affects the Windows Print Queue. To be more precise, the Print Queue service doesn't restrict access to the RpcAddPrinterDriverEx function, which enables an **attacker to run malicious programs on a users' device**. An attacker who successfully exploits this vulnerability is able to perform operations with system-level privileges, which means they can access, edit and delete sensitive data, install programs and create new privileged accounts.

README.md

PetitPotam

PoC tool to coerce Windows hosts to authenticate to other machines via MS-EFSRPC EfsRpcOpenFileRaw or other functions :)

The tools use the LSARPC named pipe with interface c681d488-d850-11d0-8c52-00c04fd90f7e because it's more prevalent. But it's possible to trigger with the EFSRPC named pipe and interface df1941c5-fe89-4e79-bf10-463657acf44d. It doesn't need credentials against Domain Controller :D

Disabling the EFS service seems not to mitigate the "feature".

Attacking tools are available for all

Downloading BloodHound Binaries

Pre-Compiled BloodHound binaries can be found [here](#).

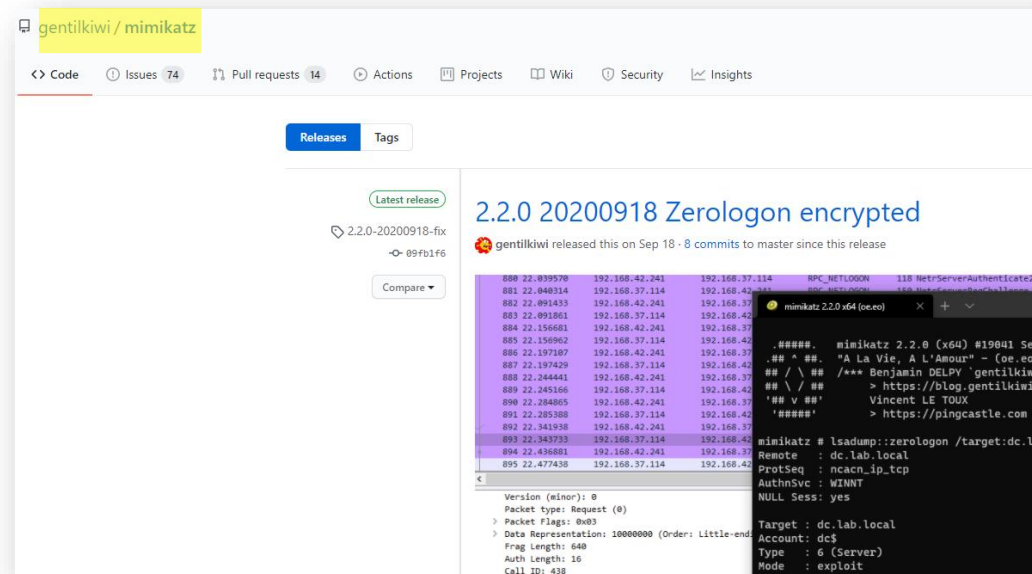
The rolling release will always be updated to the most recent source. Tagged releases are considered "stable" but will likely not have new features or fixes.

About BloodHound

To get started with BloodHound, check out the [BloodHound docs](#).

BloodHound is a single page Javascript web application, built on top of [Linkurious](#), compiled with [Electron](#), with a [Neo4j](#) database fed by a C# data collector.

BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment.



ADFSpoof

A python tool to forge AD FS security tokens.

Created by Doug Biensack (@doughsec) while at Mandiant FireEye.

Detailed Description

ADFSpoof has two main functions:

1. Given the EncryptedPFX blob from the AD FS configuration database and DKM decryption key from Active Directory, produce a usable key/cert pair for token signing.
2. Given a signing key, produce a signed security token that can be used to access a federated application.

This tool is meant to be used in conjunction with ADFSdump. ADFSdump runs on an AD FS server and outputs important information that you will need to use ADFSpoof.

If you are confused by the above, you might want to read up on AD FS first. For more information on AD FS spoofing I will post a link to my TROOPERS 19 talk and slides when they are released.

kerberoast

Kerberoast is a series of tools for attacking MS Kerberos implementations. Below is a brief overview of what each tool does.

Extract all accounts in use as SPN using built in MS tools

```
PS C:\> setspn -T medin -Q */*
```

Request Ticket(s)

One ticket:

```
PS C:\> Add-Type -AssemblyName System.IdentityModel
PS C:\> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "HTTP/web01.medin.
```

All the tickets

README.md

RiskySPNs

RiskySPNs is a collection of PowerShell scripts focused on detecting and abusing accounts associated with SPN (Service Principal Name). This module can assist blue teams to identify potentially risky SPNs as well as red teams to escalate privileges by leveraging Kerberos and Active Directory.

For detailed information: <http://www.cyberark.com/blog/service-accounts-weakest-link-chain/>

Usage

Install the module

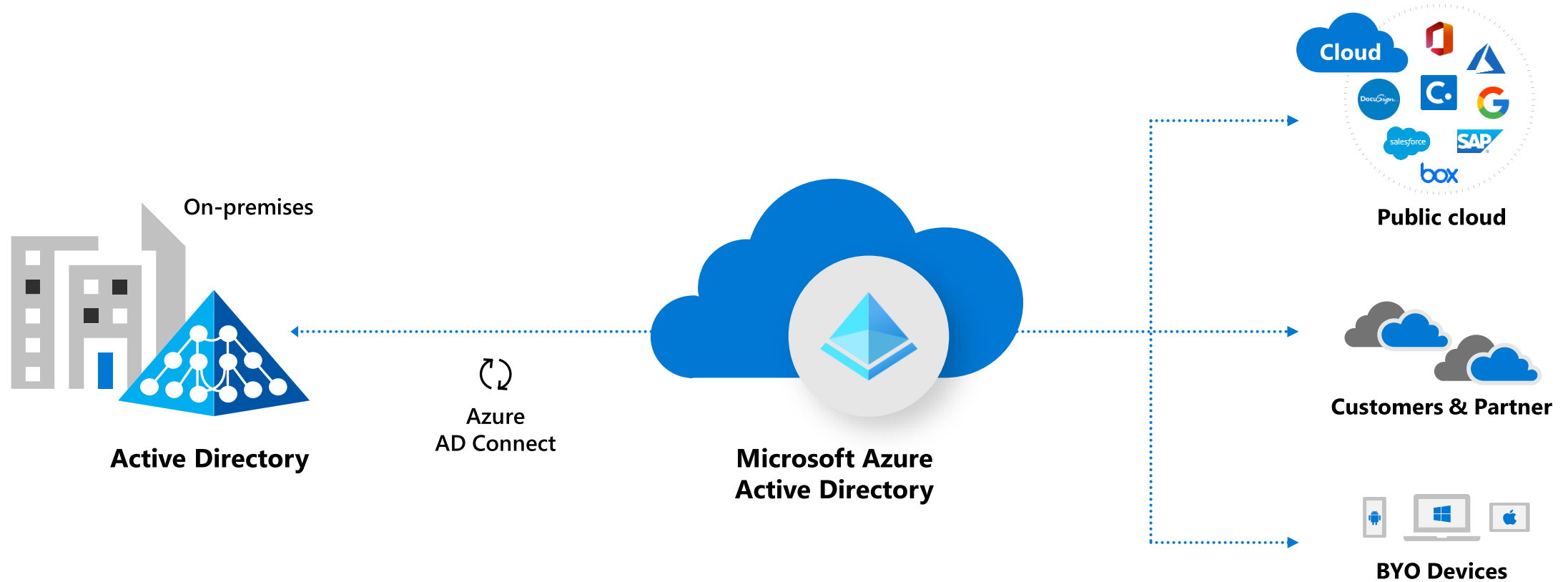
Challenges with securing identities

- On-premises and cloud identity platforms
- Identities aren't just humans
- Establishing baselines for prevention
- Multi-cloud and app explosion
- Identity and security tools are fragmented

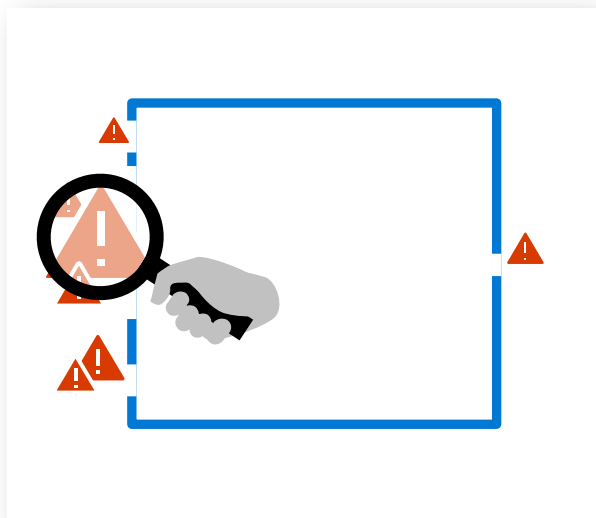


The Complexity of the Enterprise Identity Security Landscape

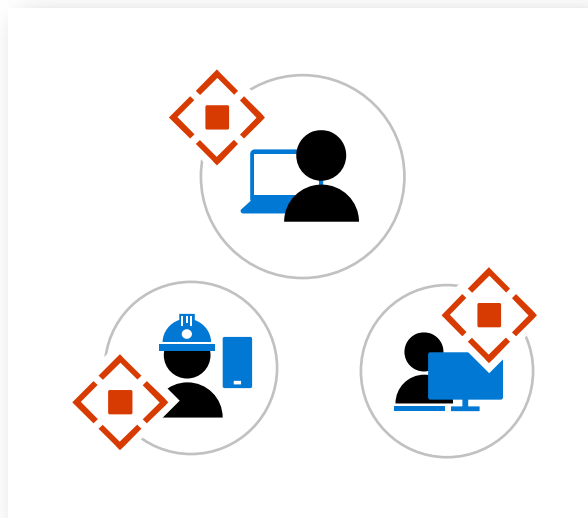
Enterprise security environments are complex and include both on-premises and cloud assets



A Broad Array of Identity Security Risks



It's easy to miss risky configurations . . .



Threats can originate anywhere . . .



Activity volume makes prioritization difficult . . .

It's a team sport



Identity admin

- » MFA and SSO
- » Real-time adaptive access
- » PAM & identity governance



SOC analyst

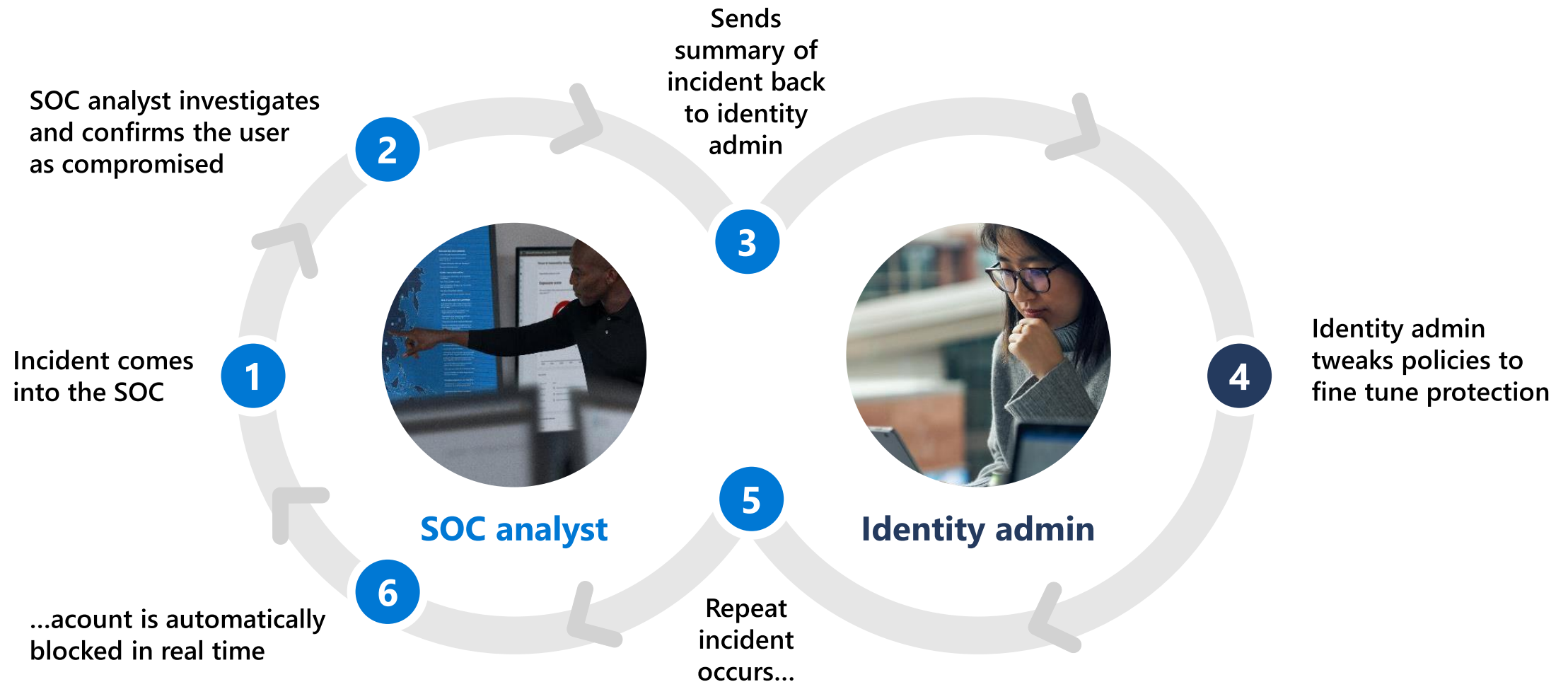
- » Detection and Investigation
- » Response
- » Automation

Common responsibilities:

Posture management | Policy configuration | Inventory



Identity admin and SOC analyst feedback loop



Microsoft's approach

Secure accounts and infrastructure



- Protect human and workload identities
- Modernization of identity infrastructure
- Proactive posture assessments
- Reconnaissance monitoring
- Highlight riskiest lateral movement paths

Detect attacks with industry-leading intel



- Real-time ML-based risk detections
- Revoke access in near real-time for critical events
- Cross-platform attack detections
- Role change alerts for privileged accounts
- Honeytoken account deception

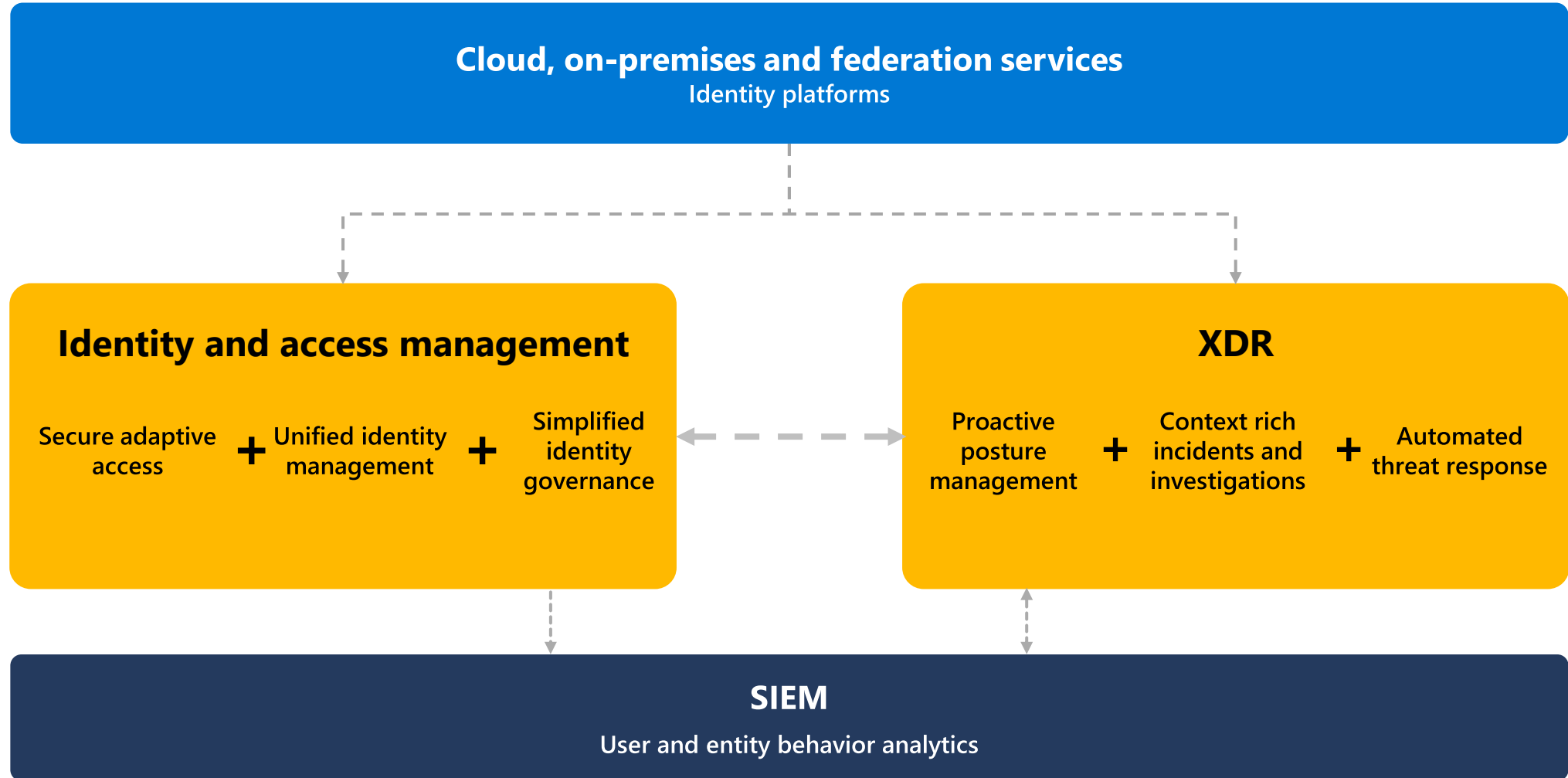
Tailored and unified experiences



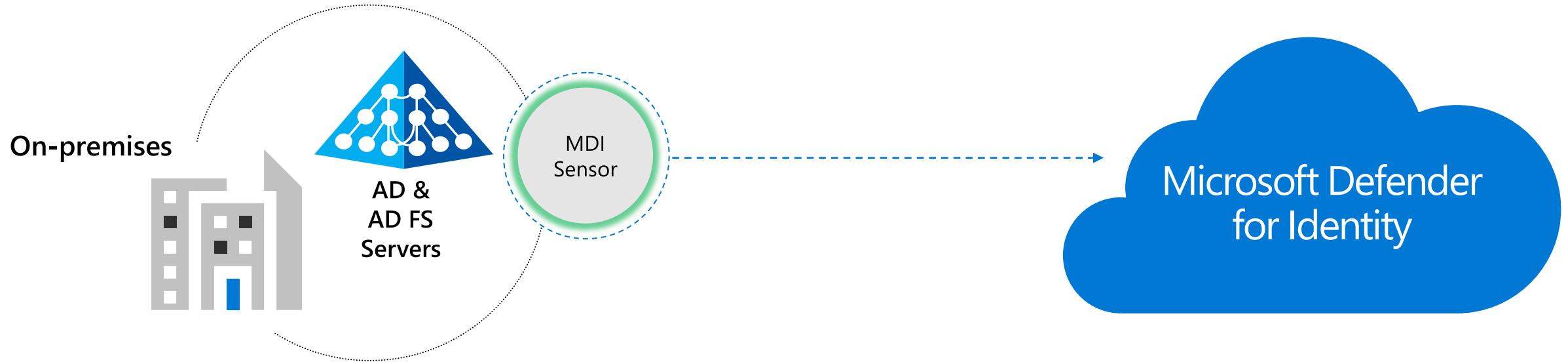
- Visualize investigations using all your signals
- Utilize cross-workload hunting and custom detections
- Combine identity sources into a single view
- Fine-tune policy configuration based on insights from incidents
- Improve effectiveness of response with pre-built risk workbooks

Cloud, on-premises and federated identity platforms

Unified threat protection architecture



MDI Data Sources and Technologies



Network traffic analytics

NTLM, Kerberos, LDAP, RPC, DNS, SMB

Security events and event tracing

Security Events
Event Tracing (ETW)
Profile AD entities

User behavior analytics

Profile users & entities behavior, identify behavior anomalies

Cloud based real-time detections

Data enrichment and correlation in the cloud, for real time detections

Microsoft Defender for Identity for Identity Protection

Microsoft Defender for Identity helps protect user identity as part of on-premises and cloud enterprise environments.



Prevent



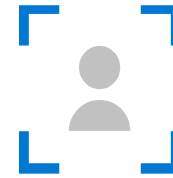
Proactive Identity
Security Posture
Assessments



Detect



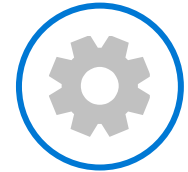
Real Time
Analytics and
Data Intelligence



Investigate



User
Investigation
Priority



Respond



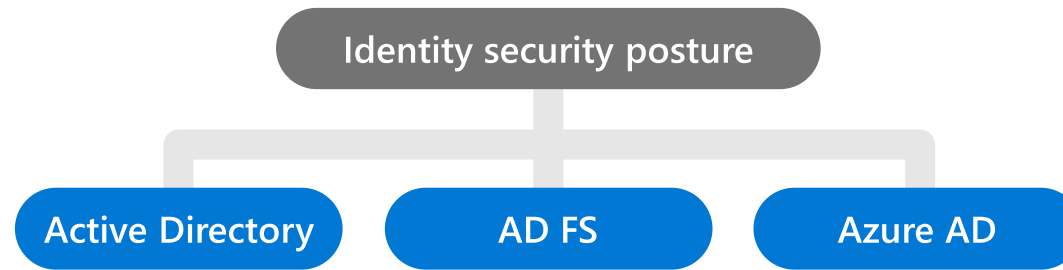
Automatic
Response to
Compromised
Identities

Cloud Scale, Continuous Updates

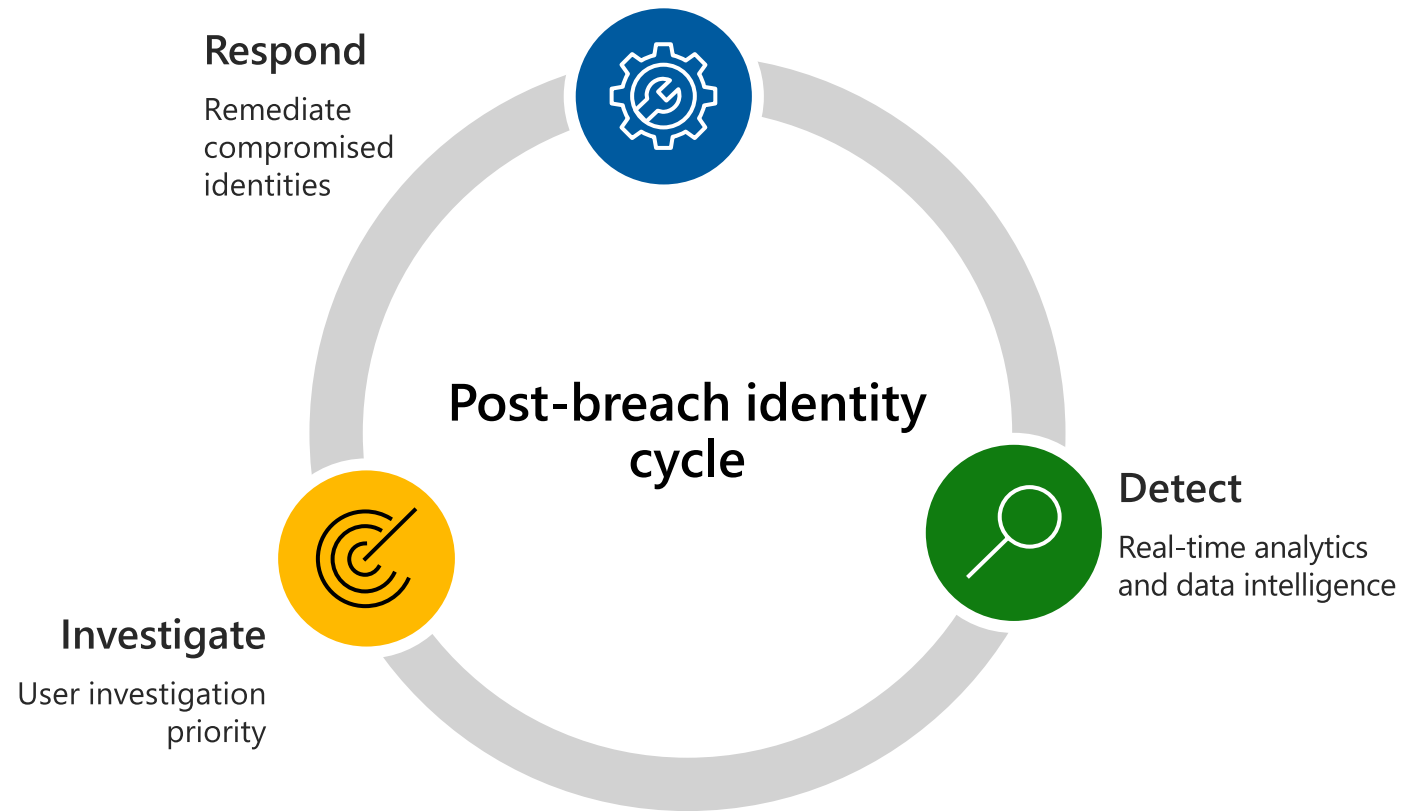
Identity security posture

Top improvement actions

- ✓ Enable MFA for Admins
- ✓ Dormant entries in sensitive groups
- ✓ Clear text credentials in place
- ✓ Use limited administrative roles
- ✓ Reduce risky lateral movement paths



Secure Score
▲ **49.86 %**



Detection of Identity related attacks

Security principal enumeration (LDAP)

Users group membership enumeration

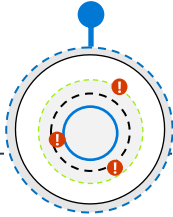
Users & IP address enumeration

Hosts & server name enumeration (DNS)

Resource access suspicious activities

Reconnaissance by targeted entity attributes

Discovery



NTLM Relay & NTLM tampering

Pass-the-Ticket

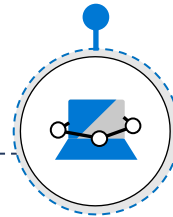
Pass-the-Hash, Overpass-the-Hash

Suspicious groups membership changes

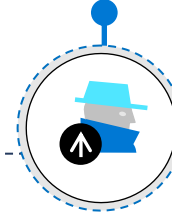
Suspicious SID history injection

Suspicious rogue certificate

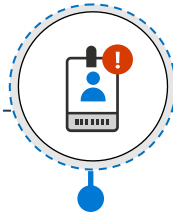
Lateral movement



Persistence



Initial access



Brute force attempts via ADFS

Suspicious VPN connection

Honey Token account suspicious activities

Logon/Failed logon & resource access suspicious activities

Suspected Kerberos SPN exposure

Suspicious DC Password change using NetLogon (CVE-2020-1472)

ADFS Dump Activity

Suspicious new ADFS trusted domain

Golden ticket attack

DCShadow, DCSync

AD Objects & hashes exfiltration (NTDS.DIT)

Code execution/Service creation on DC and ADFS

SMB packet manipulation

Skeleton Key

Golden ticket leveraging RBCD

DNS Remote code execution attempt (CV 2020-1305)

Activity Behavior Analysis by User, Peers, and Organization

- ✓ Login to devices
- ✓ Access to on-premises resources
- ✓ Remote connections to servers
- ✓ Access to cloud applications
- ✓ Usage of SharePoint Online sites
- ✓ User agent, location & ISP analytics
- ✓ Mailbox behavior
- ✓ Failed logins behavior



User Entity page & User Investigation Priority

Microsoft 365 security

Home

Incidents & alerts

Hunting

Action center

Threat analytics

Secure score

Learning hub

Endpoints

Search

Device inventory

Vulnerability management

Partners and APIs

Evaluation & tutorials

Configuration management

Email & collaboration

Investigations

Explorer

Submissions

Review

Campaigns

Threat tracker

Nick Carlsson

Admin System

SENSITIVE

User threat

Open incidents 0

Investigation prio... 30

Active alerts 0

Identity risk level Medium

Lateral movement paths

View recent

User exposure

Last seen Feb 16, 2021

Accounts 5

Logon Types 2

Locations 4

Matched files 0

Contact information

Email NickC@contoso.com

User risk

Lateral movement paths

Investigation priority score 516

Score is based on the last 7 days

How do we score?

Alerts Score: 177

Risky activities Score: 339

User's score compared to the organization 91%

Investigation priority

Alerts and risky activities that contributed to the score (last 7 days)

View all user alerts (545)

Today

+36 2/17/21, 4:52:03 PM Block download based on real-time content inspection (Silvia)

+23 2/17/21, 4:52:02 PM Block download of SSN in custom app (Silvia)

+3 2/17/21, 4:51:55 PM Download file: file Employees SSN information.docx Anomaly

+3 2/17/21, 4:51:48 PM Log on

+3 2/17/21, 4:51:47 PM Single sign-on log on

+3 2/17/21, 4:50:56 PM Single sign-on log on

Confirm user compromised

Require user to sign in again

Suspend user

User score in the last two weeks

Top 90% in your organization

Most frequent locations

Over the last 30 days

Filter...

Location	Activities	Proportion of t...	Last activity
United States	449	82%	February 17, 2021...
Israel	89	16%	February 17, 2021...
Netherlands	10	2%	February 17, 2021...
France	2	0.4%	February 10, 2021...

5 devices

Logged in devices in the last 180 days

Filter...

Device	Latest
financeserv53.contoso.com	2/11/21, 1:29:47 PM
rdpserv.contoso.com	2/16/21, 1:14:00 AM

Locations & Devices used

Advanced hunting in Microsoft 365 Defender

Advanced hunting

Schema

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- AppFileEvents
- CloudAppEvents

Email

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents

Get started Query

Run query + New Save

```
1 IdentityQueryEvents
2 | where Timestamp > ago(
3 | where ActionType == "S
4 | project QueryTime = Ti
5 | join kind=inner (
6 DeviceProcessEvents
7 | where Timestamp > ago(
8 | extend DeviceName = tou
9 | where InitiatingProces
10 | project ProcessCreatio
11 | where ProcessCreationT
12 | project QueryTime, Dev
```

Schema reference

Run query Save Share link Sample size: 10% Last 7 days Create detection rule Edit in KQL

Guided query

View in: All Clear all

AND

- Logon Events: EventType equals 2 selected
- File Events: EventType equals DeviceFileEvents: FileModified
- IP Address Events: EventType equals DeviceNetworkEvents: Connec...

Select a filter

- Other
- Process Events
- Recipient Activities
- Registry Events

Event Type

- PreviousRegistryKey
- PreviousRegistryValueData
- PreviousRegistryValueName
- RegistryKey

er to inbox

File activity by name or sha256

Protects the sensitive content throughout your organization, including cloud and endpoint to prevent oversharing of sensitive information.

Load example

Hunt for all alerts where user X is involved

Manages and governs data by configuring retention and deletion policies that allows the import, retention, and archiving of your data.

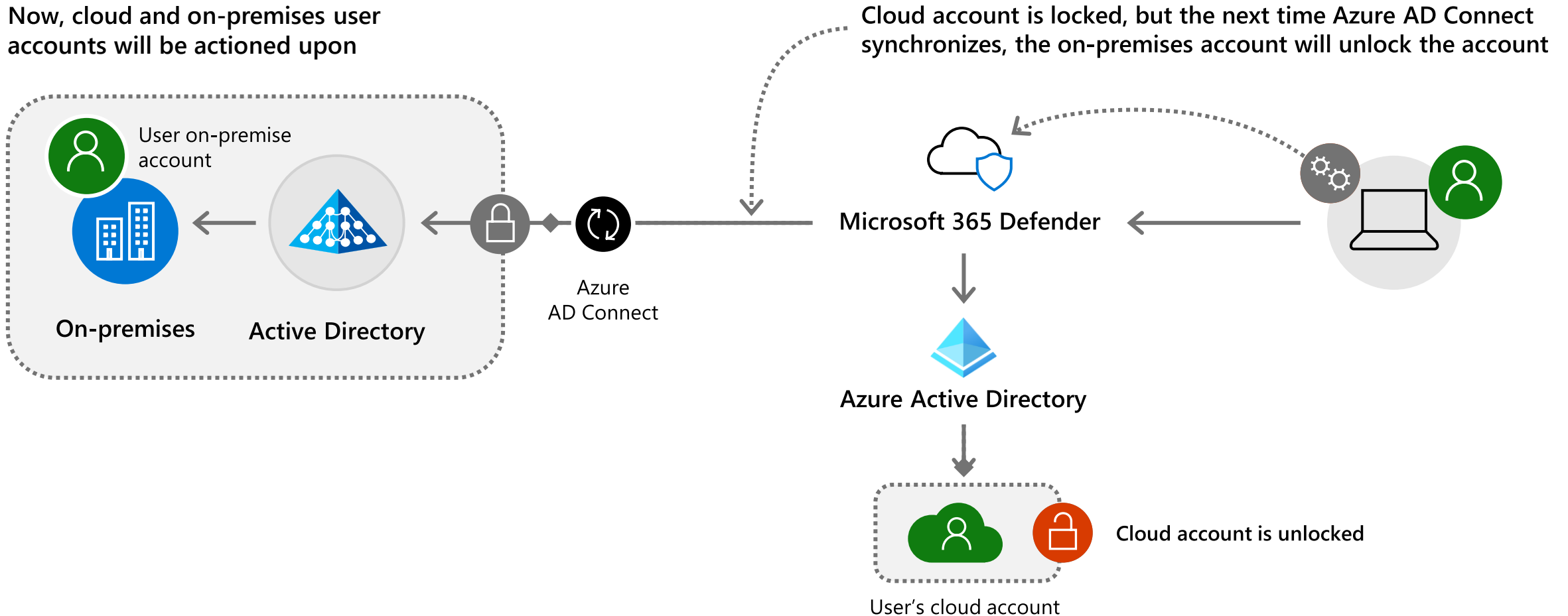
Load example

For example, you can now understand what Microsoft 365 Defender's advanced hunting capability allows you to do across all activities.

Response and remediation actions

Enabling cloud and on-premises accounts to be protected immediately

Now, cloud and on-premises user accounts will be actioned upon



Red vs Blue

To provide a safe playing field for a SOC team to improve investigating, managing and hunting for incidents generated in real time against a real-life environment.

The environment has onboarded devices, mailboxes, users and AAD accounts that resemble a corporate environment. Basic network and system information is shared.

Red team's mission

- Execute attacks against the blue team's environment, following paths and tactics and using tools taken from real world breach cases. Infiltrating the environment, move laterally and compromises assets until they get to their final goal.

Blue team's mission

- Analyze and investigate incidents and alerts, hunt for red team's activities, and report their findings at the end of the game.

At the end of the event, both teams meet. The red team is walking the blue team through the attack scenario in detail, while the blue team is sharing feedback on how they investigated and what challenges they faced during their investigation.

