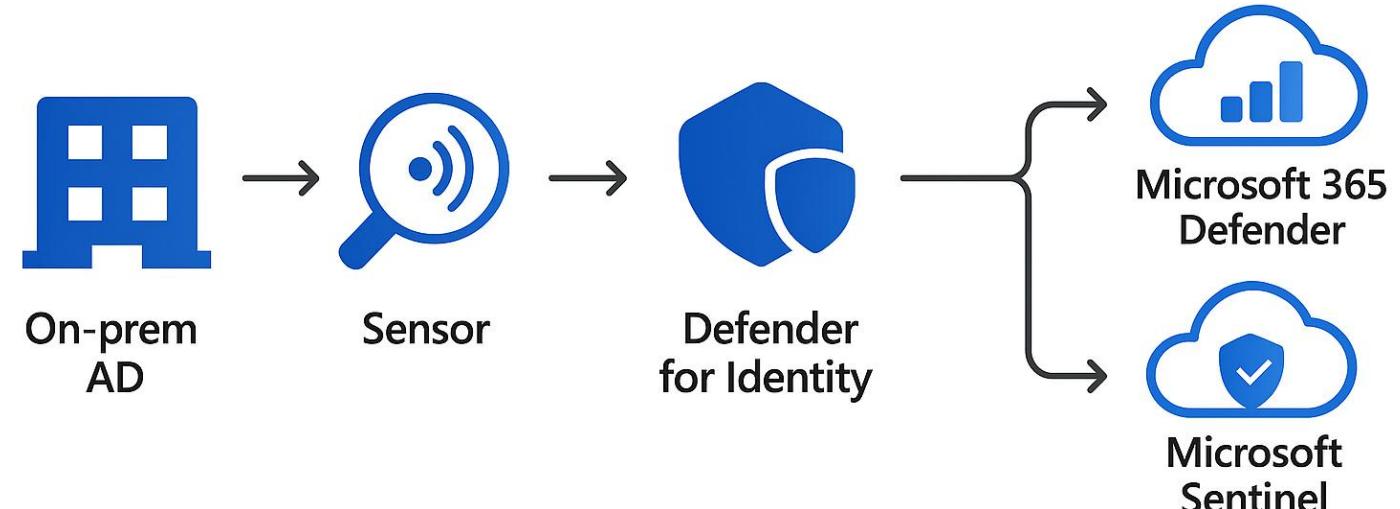


Microsoft
CERTIFIED

EXPERT



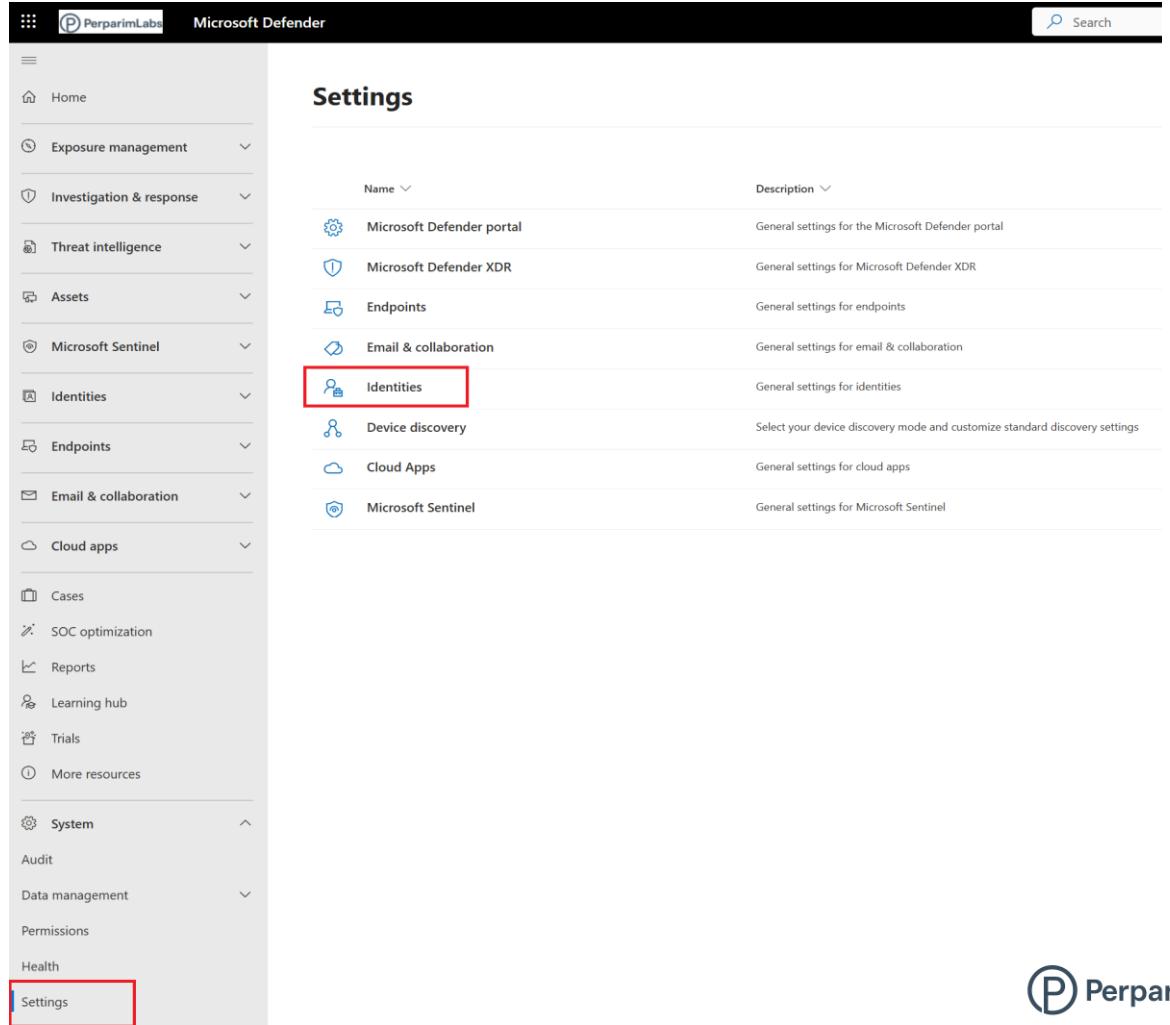
Hybrid Threat Detection with Microsoft Defender for Identity



Defender for Identity bridges on-prem AD with Microsoft Security Graph to detect suspicious activities in real time.

From Azure ATP to Defender for Identity

- Formerly known as Azure ATP – now Defender for Identity – expands visibility across users, devices & protocols like Kerberos and NTLM.

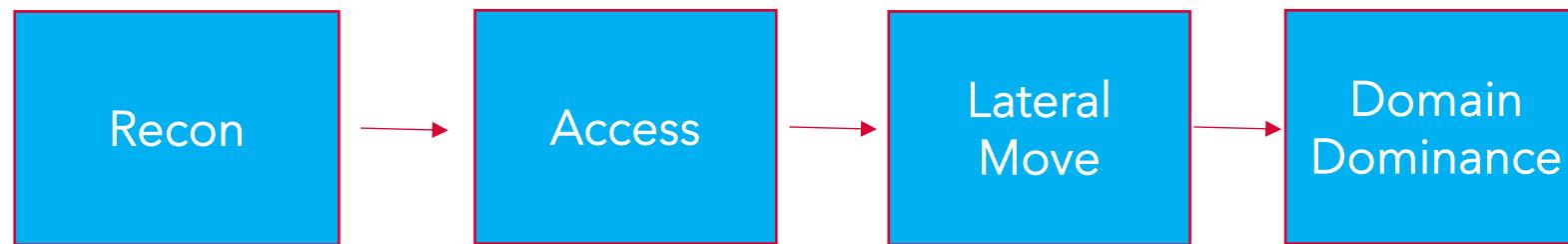


The screenshot shows the Microsoft Defender portal interface. The left sidebar contains a navigation menu with items like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities (which is expanded to show sub-options: Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, and More resources), System (Audit, Data management, Permissions, Health), and Settings. The main content area is titled 'Settings' and lists various configuration options. The 'Identities' option is highlighted with a red box. The table below lists the settings with their names and descriptions:

Name	Description
Microsoft Defender portal	General settings for the Microsoft Defender portal
Microsoft Defender XDR	General settings for Microsoft Defender XDR
Endpoints	General settings for endpoints
Email & collaboration	General settings for email & collaboration
Identities	General settings for identities
Device discovery	Select your device discovery mode and customize standard discovery settings
Cloud Apps	General settings for cloud apps
Microsoft Sentinel	General settings for Microsoft Sentinel

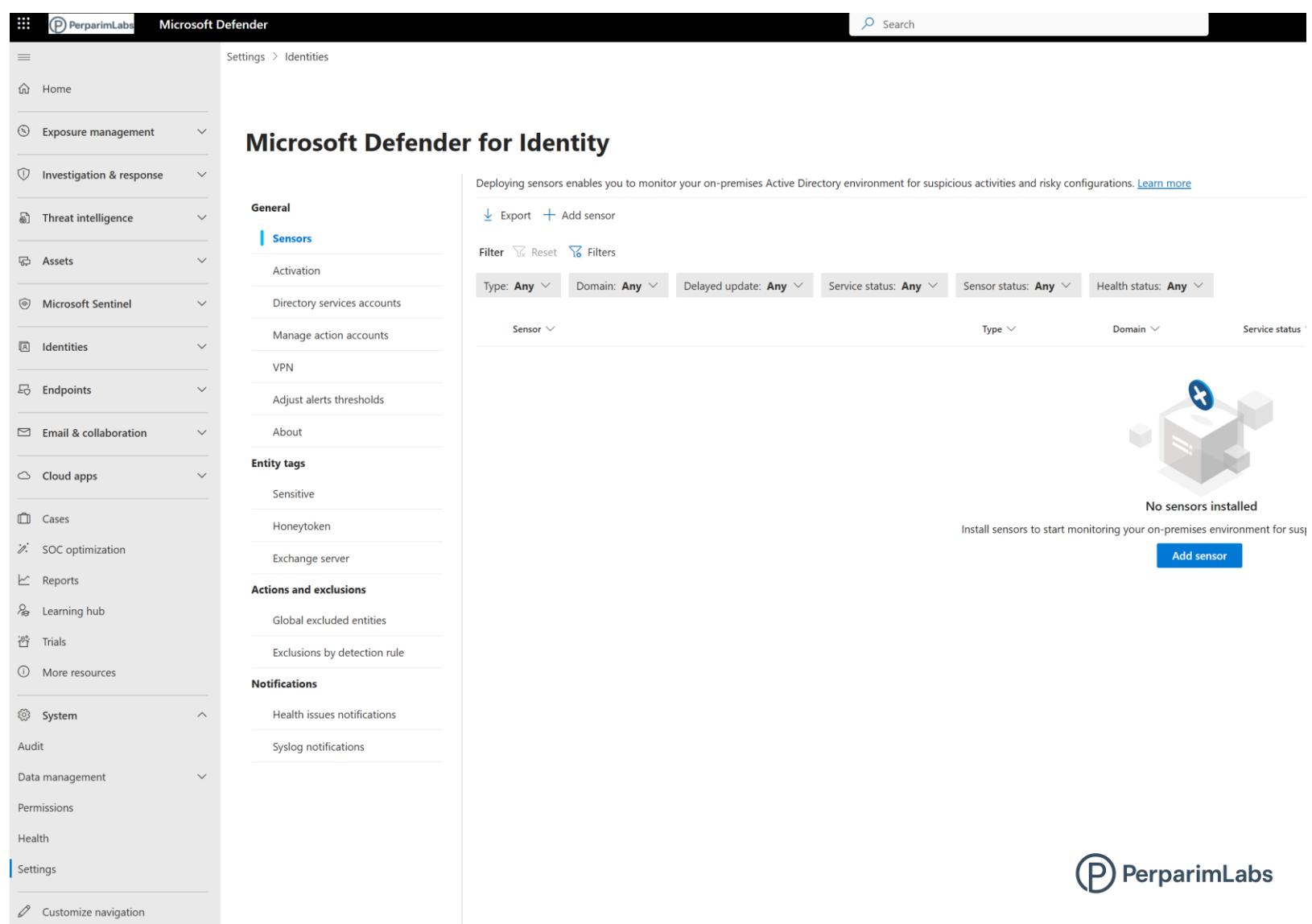
Understanding Identity Threats (Defender for Identity in Action)

- Microsoft Defender for Identity detects suspicious user and network activity by analyzing authentication patterns and AD traffic.
- Helps identify stages of an attack kill chain:
 - 1 **Reconnaissance** – attackers scan network ports and enumerate users.
 - 2 **Credential Access** – stolen credentials through phishing or brute-force.
 - 3 **Lateral Movement** – compromised account moves between servers.
 - 4 **Domain Dominance** – attacker gains control of key AD assets.
- Reduces the attack surface by continuously learning normal behavior and flagging anomalies.



Adding a Sensor to Monitor On-Prem AD

Added sensor from Defender for Identity → Settings → Identities → Sensors → Add Sensor to monitor on-prem domain controller.



Microsoft Defender

Settings > Identities

Microsoft Defender for Identity

Deploying sensors enables you to monitor your on-premises Active Directory environment for suspicious activities and risky configurations. [Learn more](#)

[Export](#) [Add sensor](#)

Filter [Reset](#) [Filters](#)

Type: Any Domain: Any Delayed update: Any Service status: Any Sensor status: Any Health status: Any

Sensor Type Domain Service status

No sensors installed

Install sensors to start monitoring your on-premises environment for suspicious activities and risky configurations.

[Add sensor](#)

General

Sensors

- Activation
- Directory services accounts
- Manage action accounts
- VPN
- Adjust alerts thresholds
- About

Entity tags

- Sensitive
- Honeytoken
- Exchange server

Actions and exclusions

- Global excluded entities
- Exclusions by detection rule

Notifications

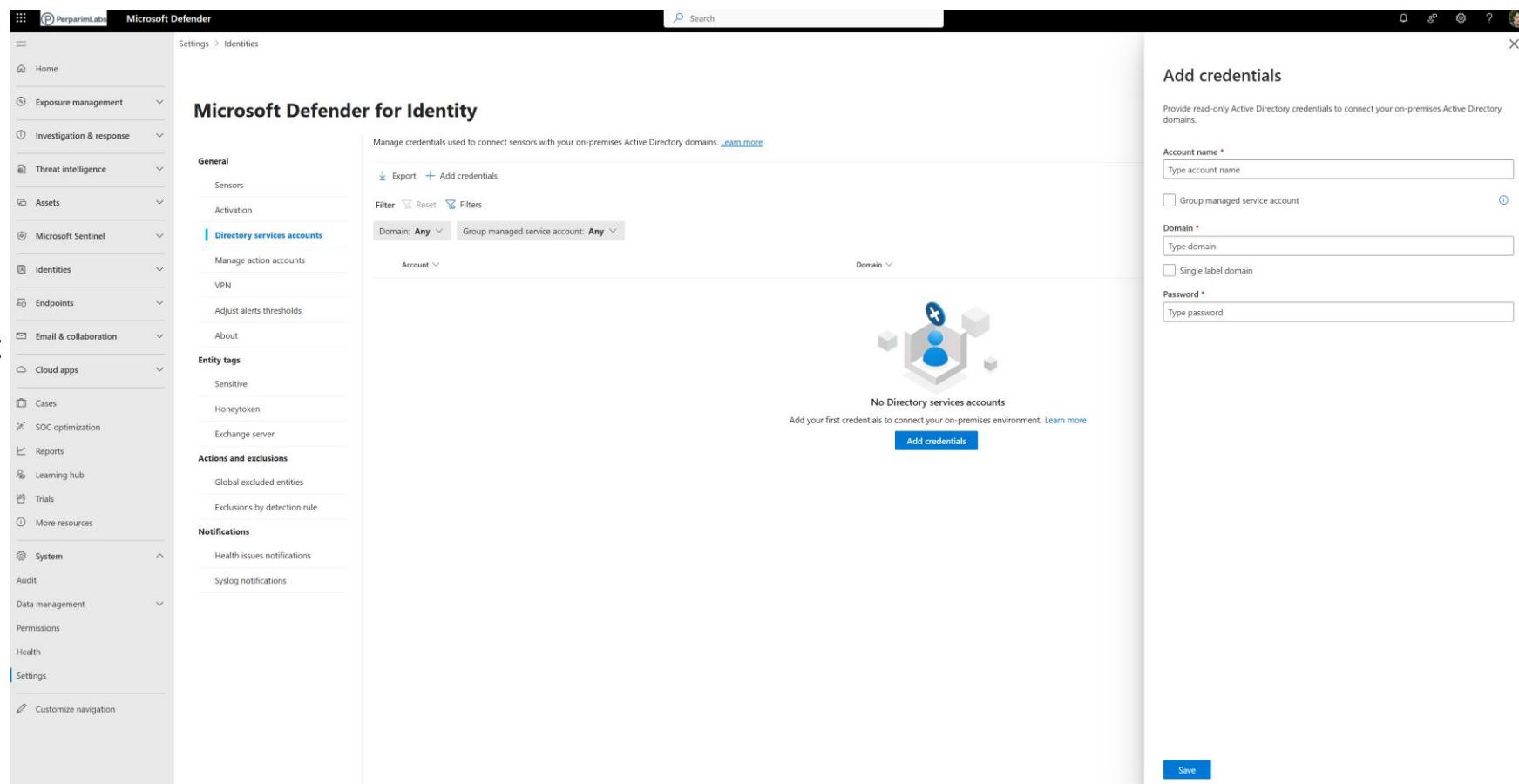
- Health issues notifications
- Syslog notifications

Customize navigation

PerparimLabs

Creating the Directory Service Account

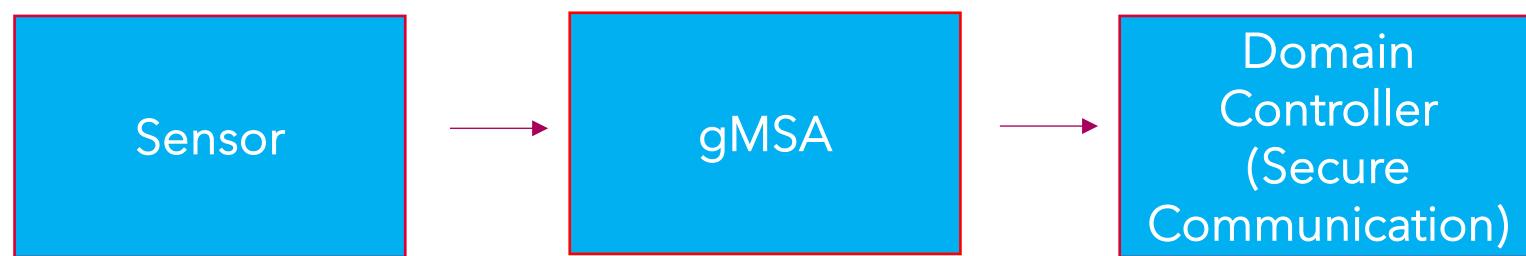
Created a dedicated account (e.g., `DefenderAdmin`) with least privilege to let sensor read AD logs and detect threats.



The screenshot shows the Microsoft Defender for Identity interface. The left sidebar includes sections like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, General (Sensors, Activation, Directory services accounts, Entity tags, Actions and exclusions, Notifications), System (Audit, Data management, Permissions, Health, Settings), and a Customize navigation option. The main content area is titled 'Microsoft Defender for Identity' and 'Manage credentials used to connect sensors with your on-premises Active Directory domains'. It features a 'General' tab with 'Directory services accounts' selected, showing a table with columns for 'Account' and 'Domain'. A 'No Directory services accounts' message with an 'Add credentials' button is present. The right side is a 'Add credentials' form with fields for 'Account name', 'Domain', and 'Password', along with checkboxes for 'Group managed service account' and 'Single label domain'.

Secure Sensor Authentication with gMSA

- Microsoft Defender for Identity sensors use a Group Managed Service Account (gMSA) to securely access domain resources.
- gMSA automates password management – credentials rotate automatically and are never exposed to admins.
- This ensures consistent, least-privilege access for the sensor service running on domain controllers.
- Using gMSA aligns with Microsoft's **Zero Trust principle of least privilege** and eliminates manual credential risks.



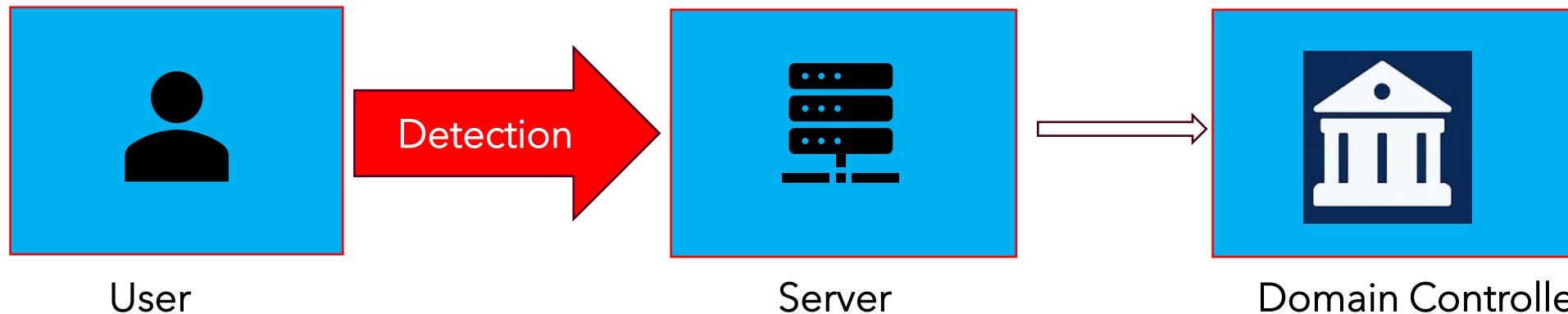
Connect Defender for Identity with Microsoft XDR Ecosystem

- Defender for Identity integrates natively with Microsoft Defender XDR and Microsoft Sentinel, enabling unified detection and response.
- Identity-based alerts from Defender for Identity appear directly within the XDR incident queue.
- Sentinel correlation rules enrich those alerts with **network, endpoint, and cloud telemetry**, creating a full attack story.
- This integration allows SOC teams to respond faster – from detection → investigation → containment in one platform.



Detecting Lateral Movement in Hybrid Environments

- Defender for Identity detected multiple failed logons followed by a successful RDP connection to another domain controller.
- The analytics engine correlated this behavior with abnormal Kerberos ticket requests.
- Sentinel investigation graph highlighted the path from **User** → **Server** → **Domain Controller**, confirming lateral movement.
- SOC team initiated containment – isolating the host and resetting compromised credentials.



Strengthening Hybrid Identity Security Posture

- Microsoft Defender for Identity delivers **deep visibility** into Active Directory activity – both on-premises and in the cloud.
- It transforms traditional directory monitoring into **proactive threat detection**.
- Combined with Defender XDR and Sentinel, it supports a complete **Zero Trust architecture** by correlating identity, device, and network signals.
- Recommended next steps:
 - 1 Expand deployment to all domain controllers.
 - 2 Integrate Sentinel playbooks for automated incident response.
 - 3 Continuously review Identity Security posture in Microsoft Secure Score.