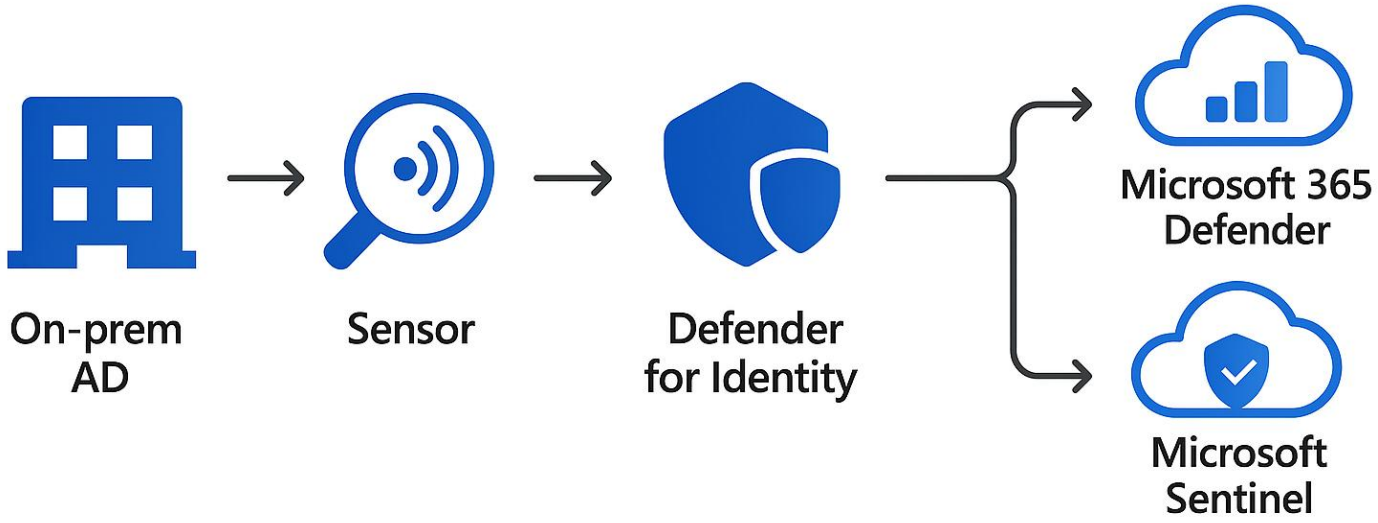
Hybrid Threat Detection with Microsoft Defender for Identity

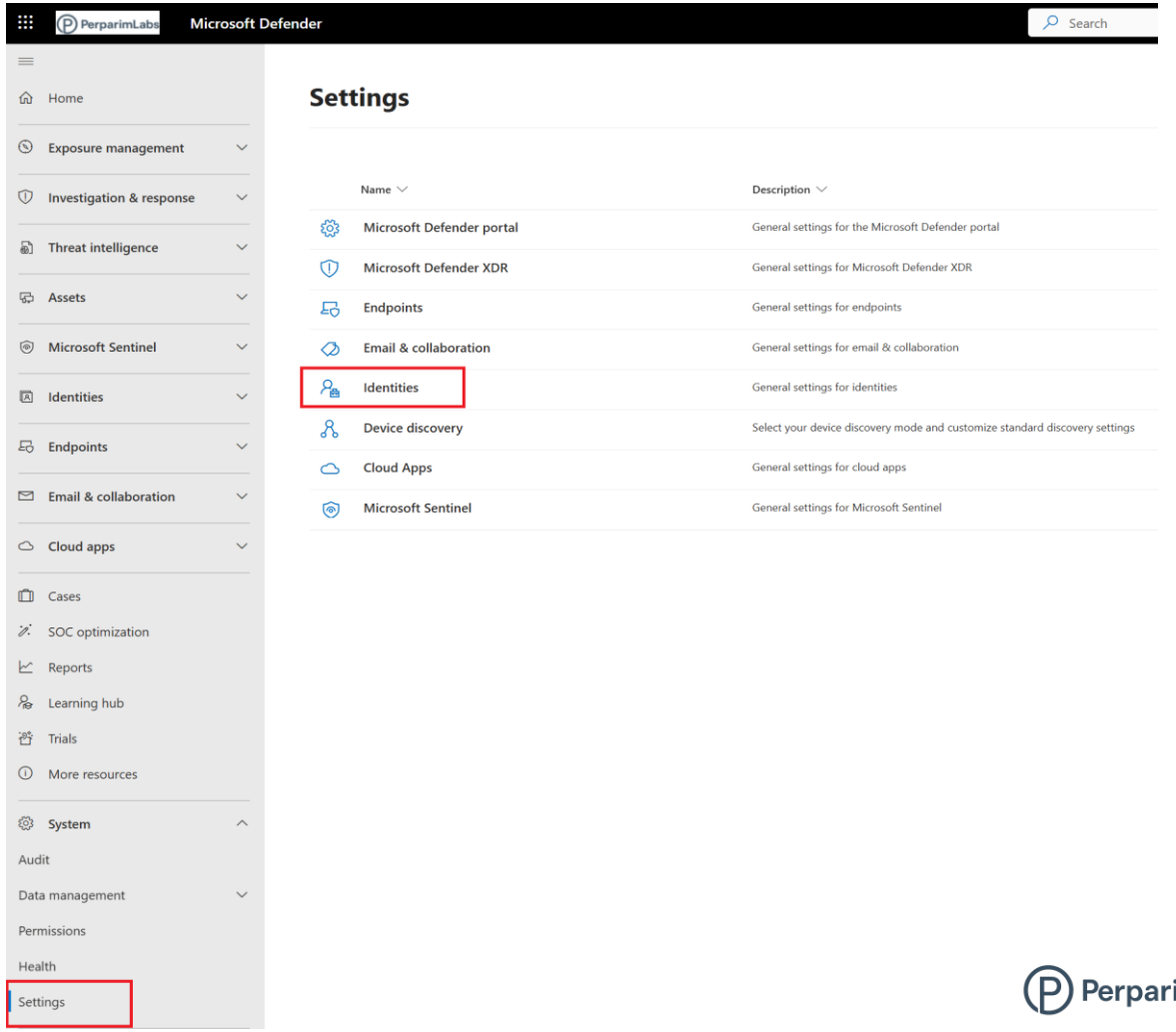


Defender for Identity bridges on-prem AD with Microsoft Security Graph to detect suspicious activities in real time.

PerparimLabs

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.



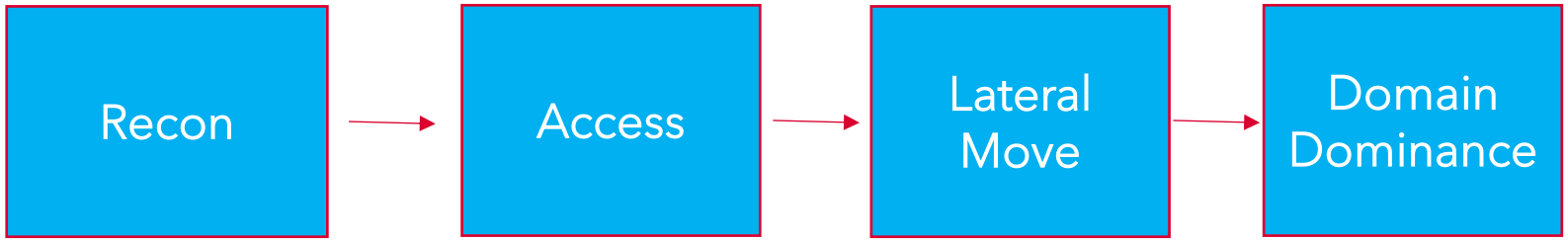
PerparimLabs

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.

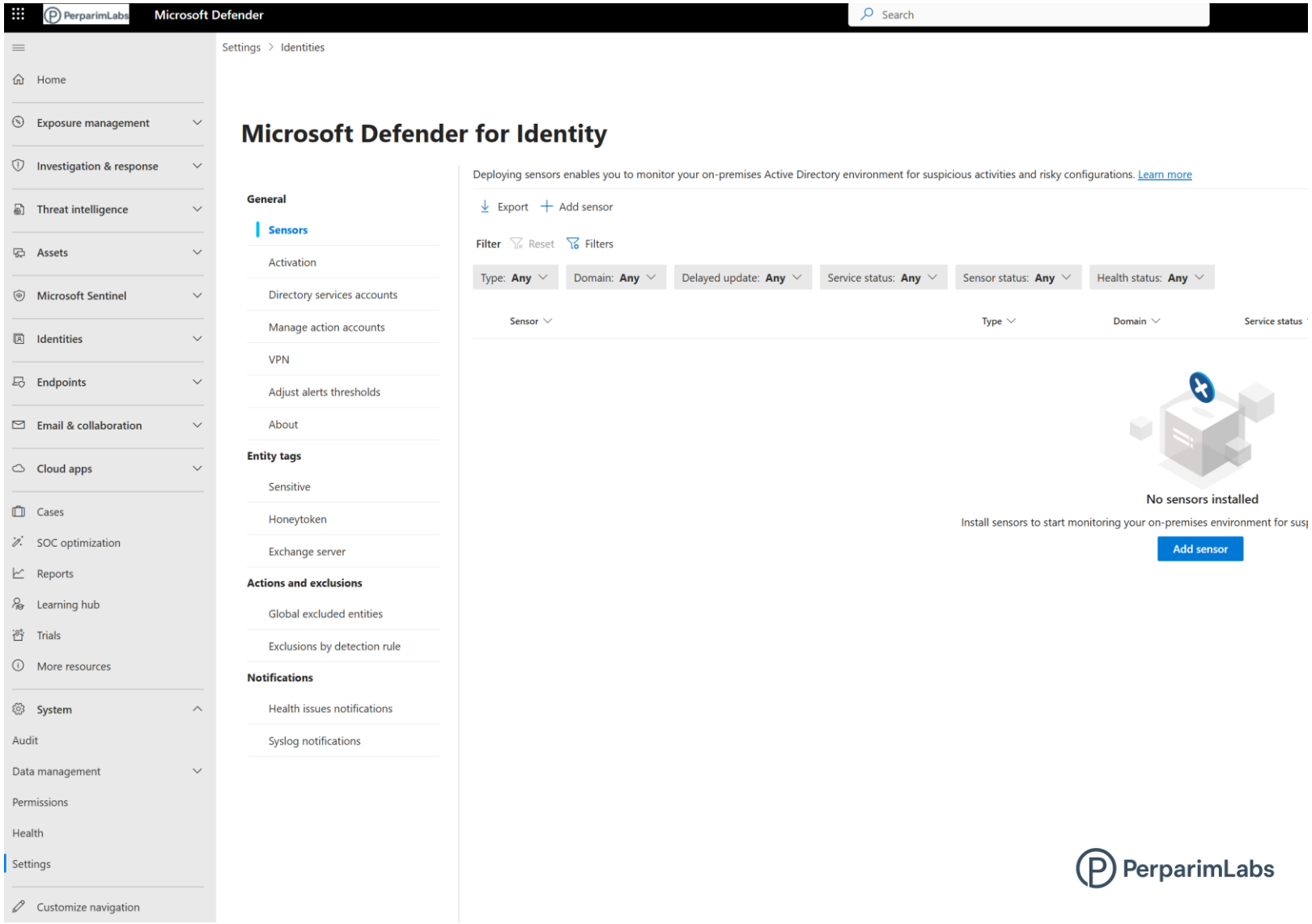
- Reduces the attack surface by continuously learning normal behavior and flagging anomalies.



PerparimLabs

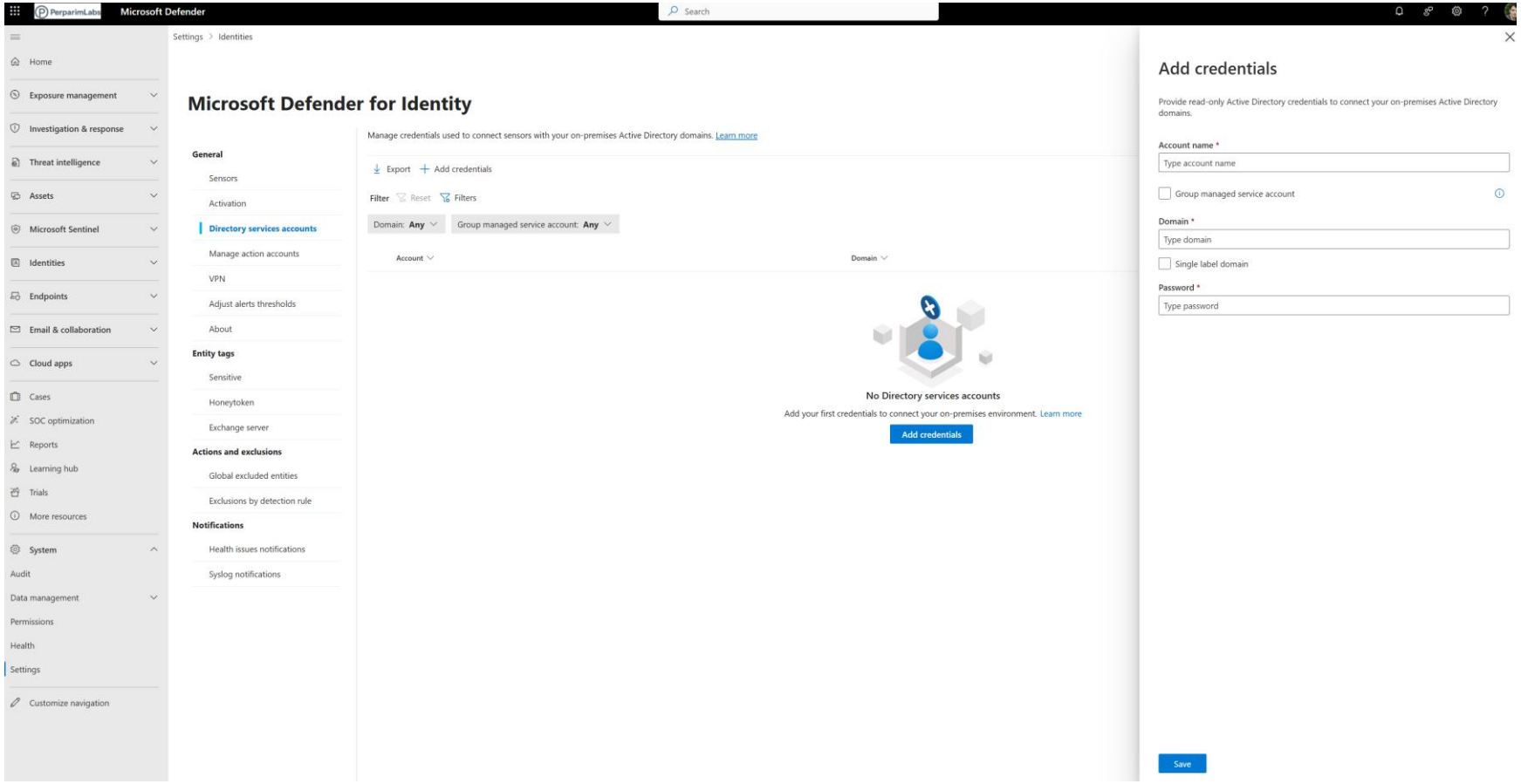
Adding a Sensor to Monitor On-Prem AD

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



Creating the Directory Service Account

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



PerparimLabs

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.

PerparimLabs

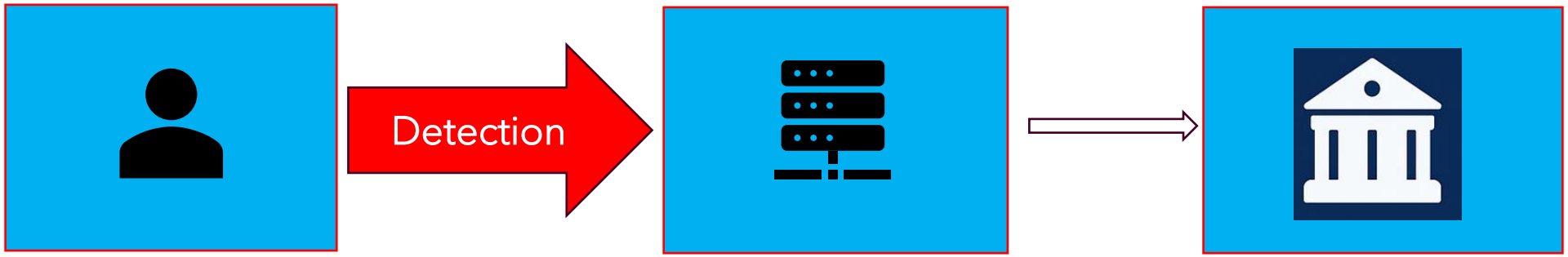
Connect Defender for Identity with Microsoft XDR Ecosystem

- 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.

PerparimLabs

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.



PerparimLabs

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.

PerparimLabs