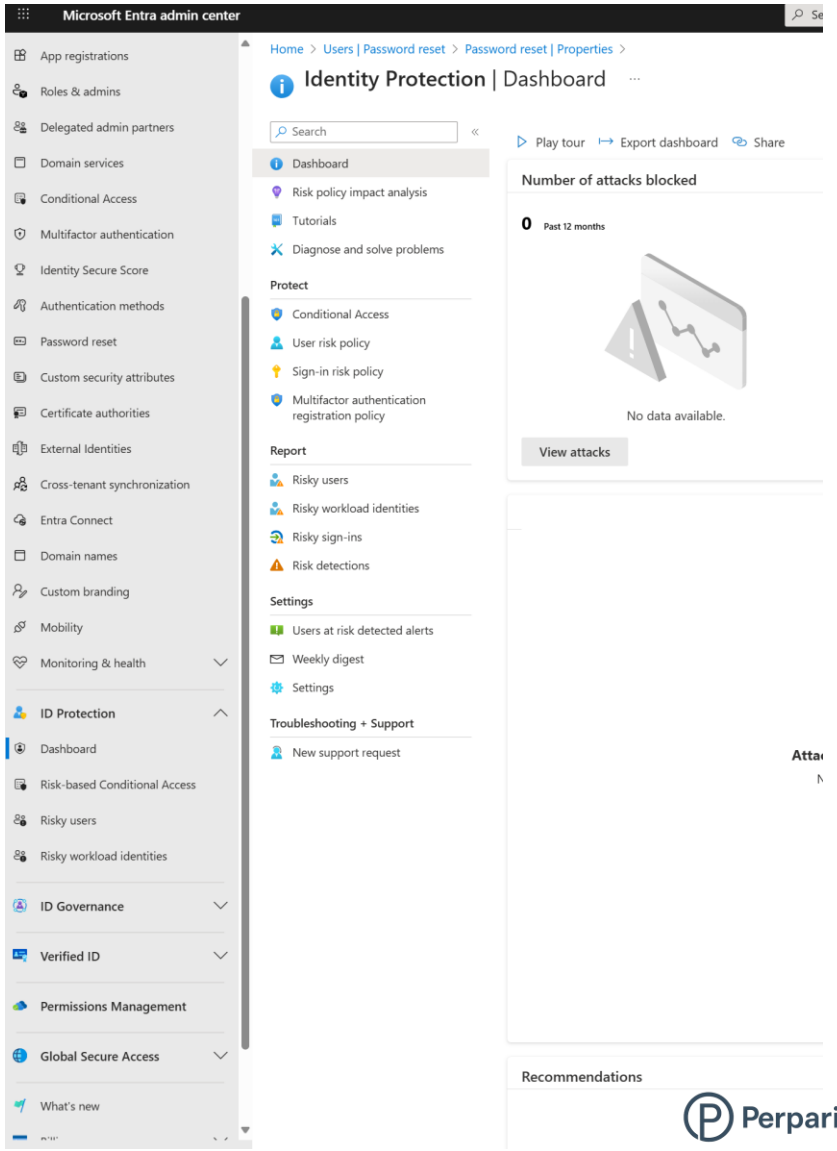
Investigating Identity Risks with Microsoft 365 Defender

From Detection to Response across Microsoft Entra ID, Defender, and Sentinel

PerparimLabs

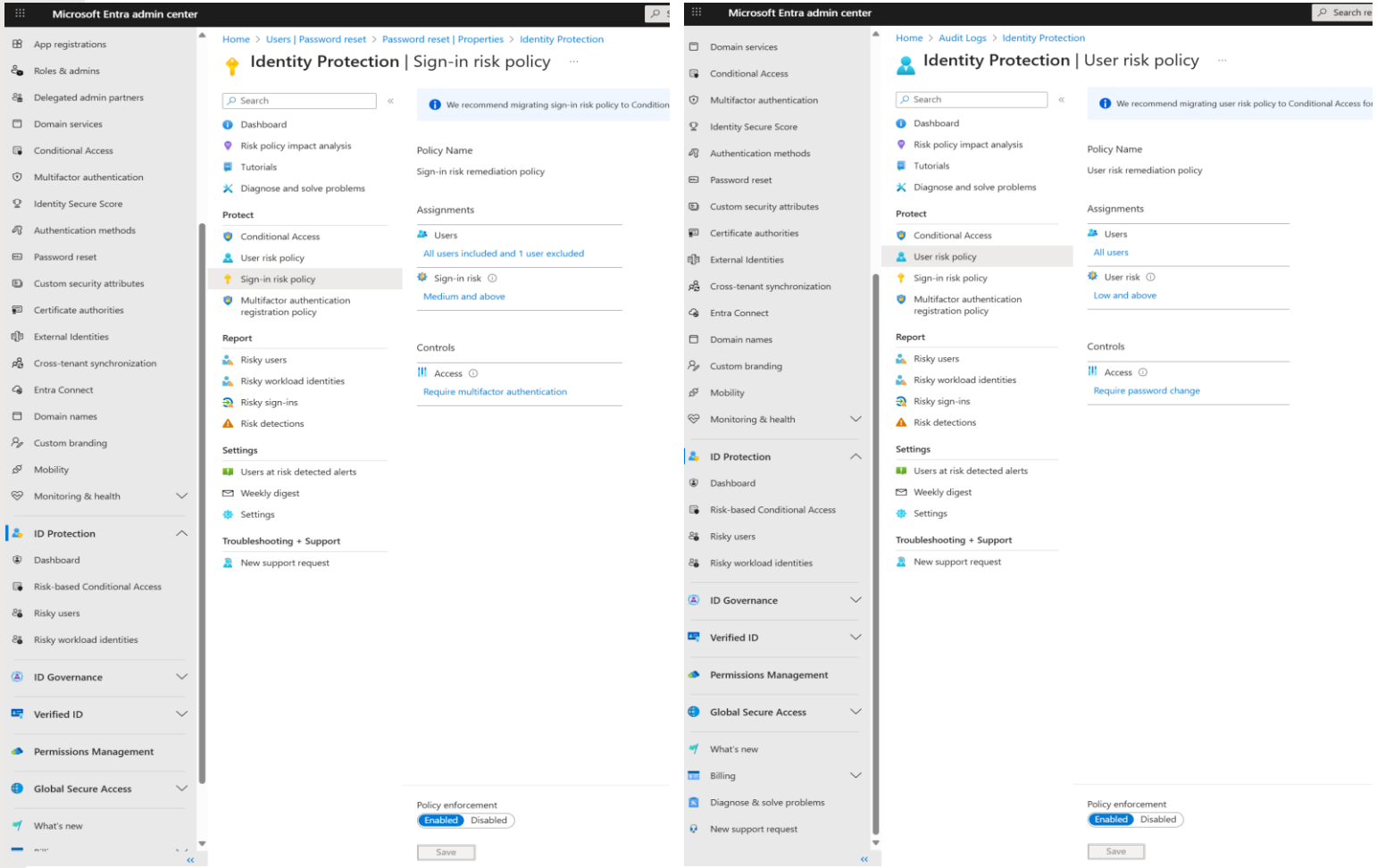
Why identity-based threats matter

- 80% of breaches begin with compromised credentials
- Entra ID Protection continuously analyzes sign-in and user risk
- Defender correlates those risks with incidents for deeper investigation



Risk detection powered by trillions of Microsoft signals

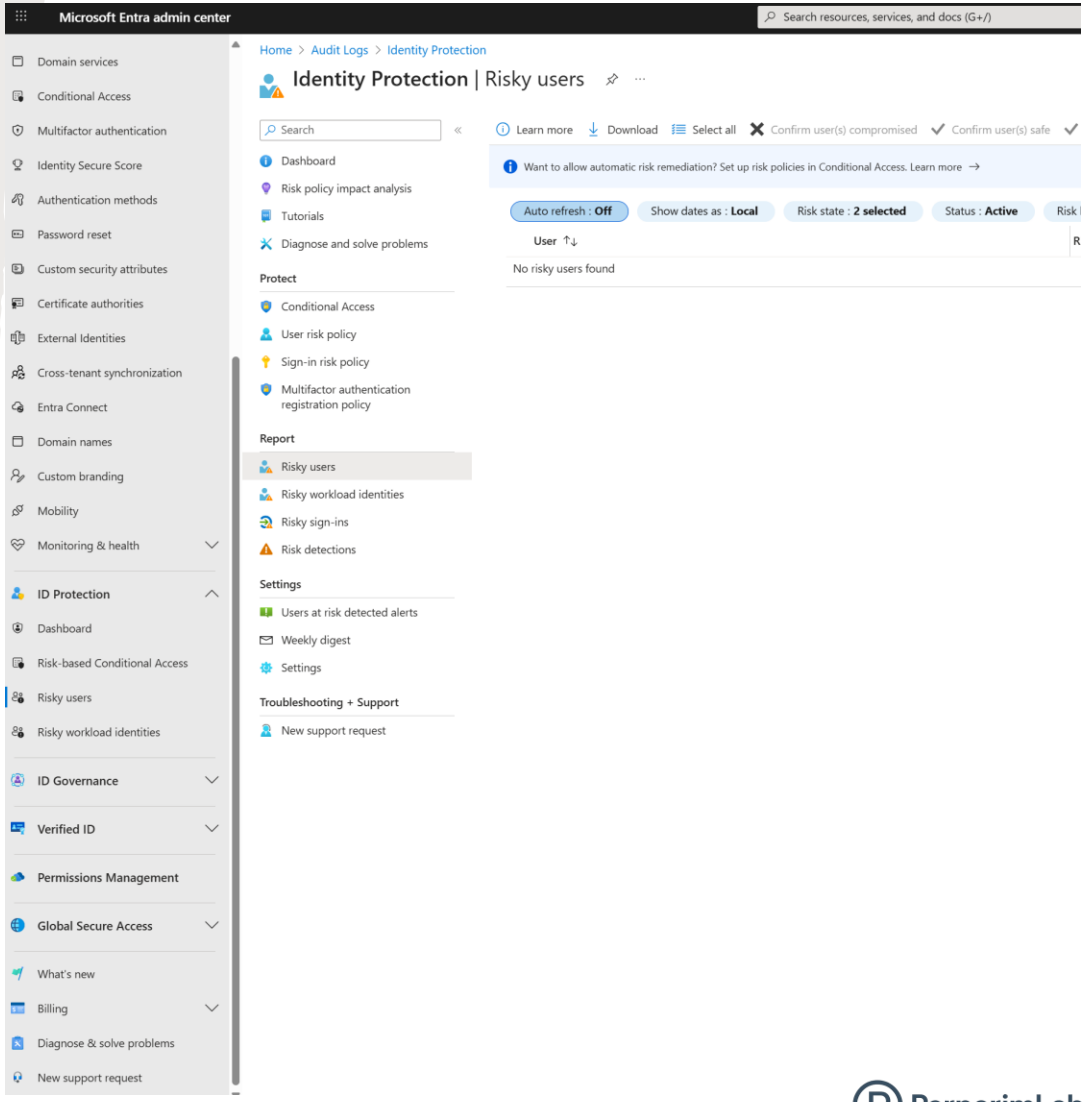
- Detects risky **sign-ins**, **users**, and **workload identities**
- Evaluates behaviors (location, time, device, IP reputation)
- Auto-remediates through MFA or password reset



PerparimLabs

Bridging detection with investigation

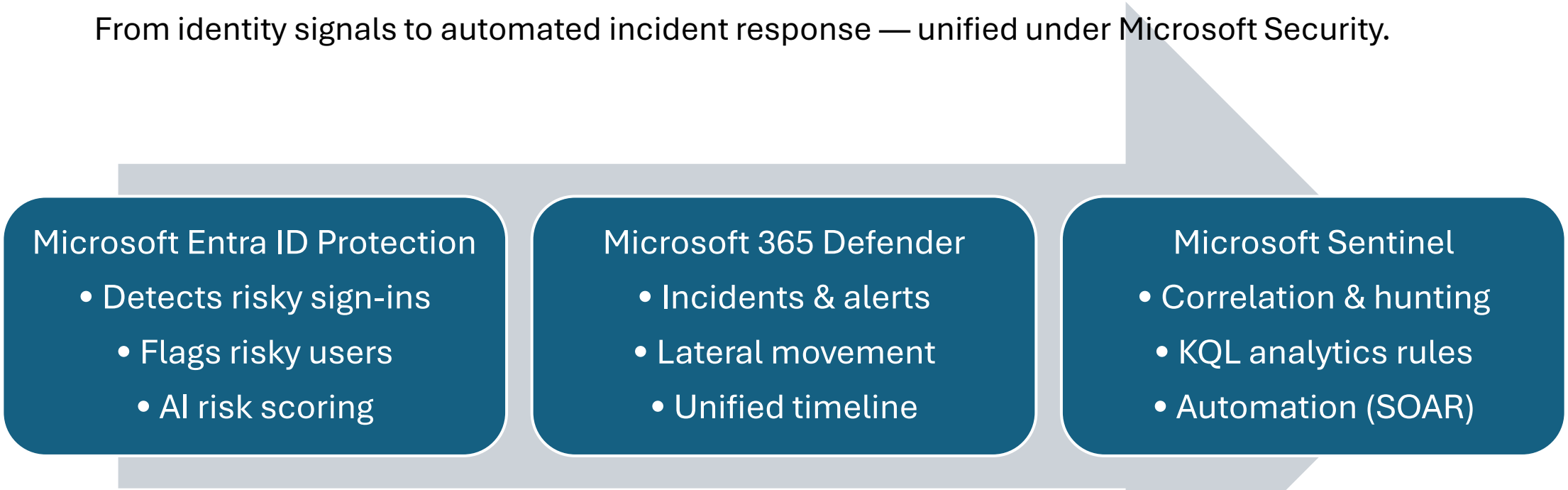
- Identity Protection flags a user as risky
- Admin clicks **“Investigate with Microsoft 365 Defender”**
- Defender aggregates alerts, devices, and lateral movement paths



PerparimLabs

Detection ➡ Investigation ➡ Response (Microsoft Security)

From identity signals to automated incident response — unified under Microsoft Security.

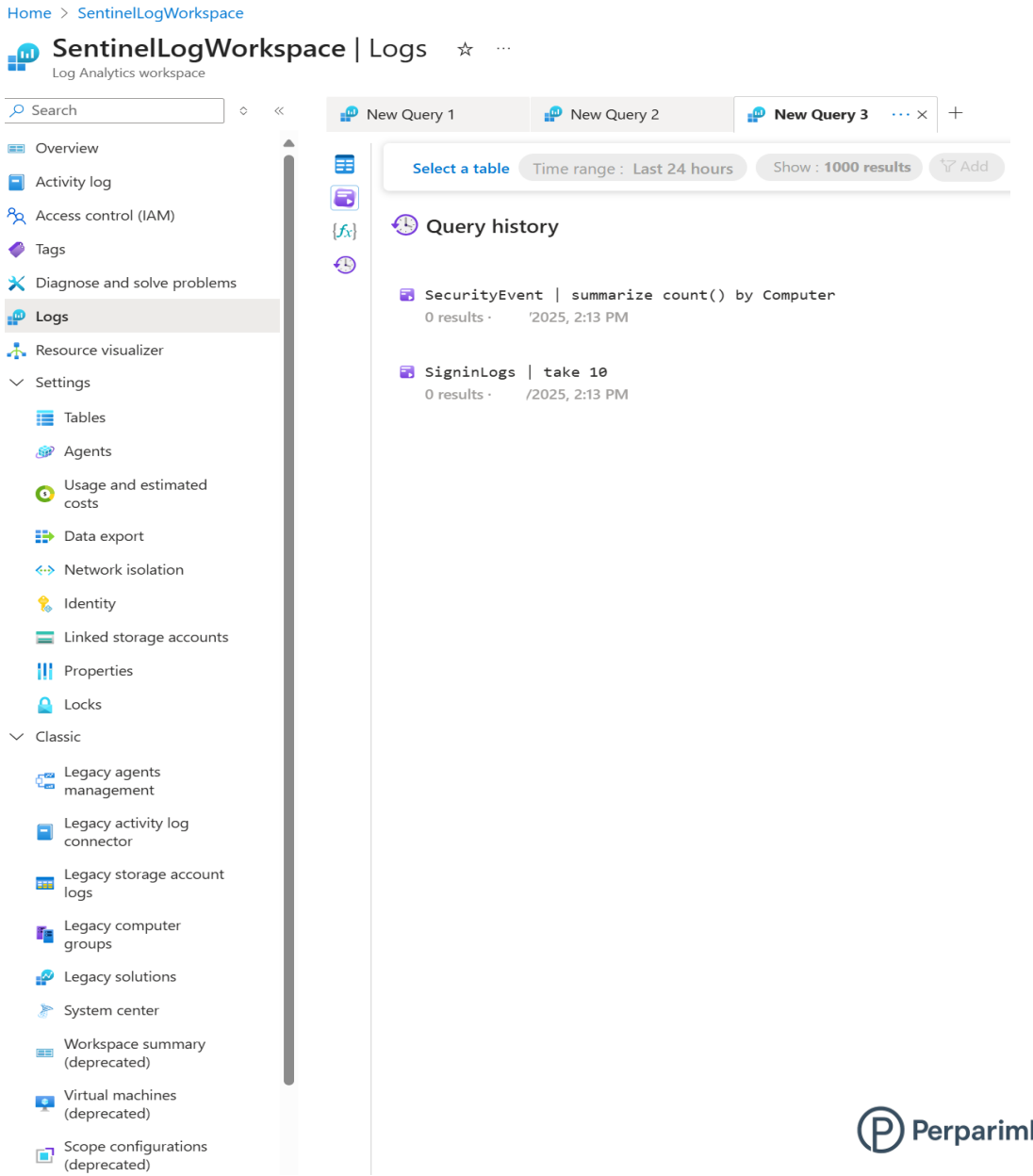


PerparimLabs

Identity is the new attack surface – align Detection → Investigation → Response in one ecosystem

Extending investigation into proactive hunting

- Logs and alerts from Entra + Defender feed Sentinel
- SOC analysts can run KQL queries for deep correlation
- Supports custom analytics rules and automation



PerparimLabs

Unified incident timeline

- Defender shows correlated alerts across workloads
- Provides user context, device timeline, and incident severity
- Helps SOC teams prioritize real threats faster

PerparimLabs

Lessons learned

- ✅ Entra ID Protection detects risk in real time
- ✅ Microsoft 365 Defender centralizes investigation
- ✅ Sentinel enables proactive threat hunting
- ✅ Together: Continuous detection, investigation, and response loop

PerparimLabs