What is Microsoft Sentinel

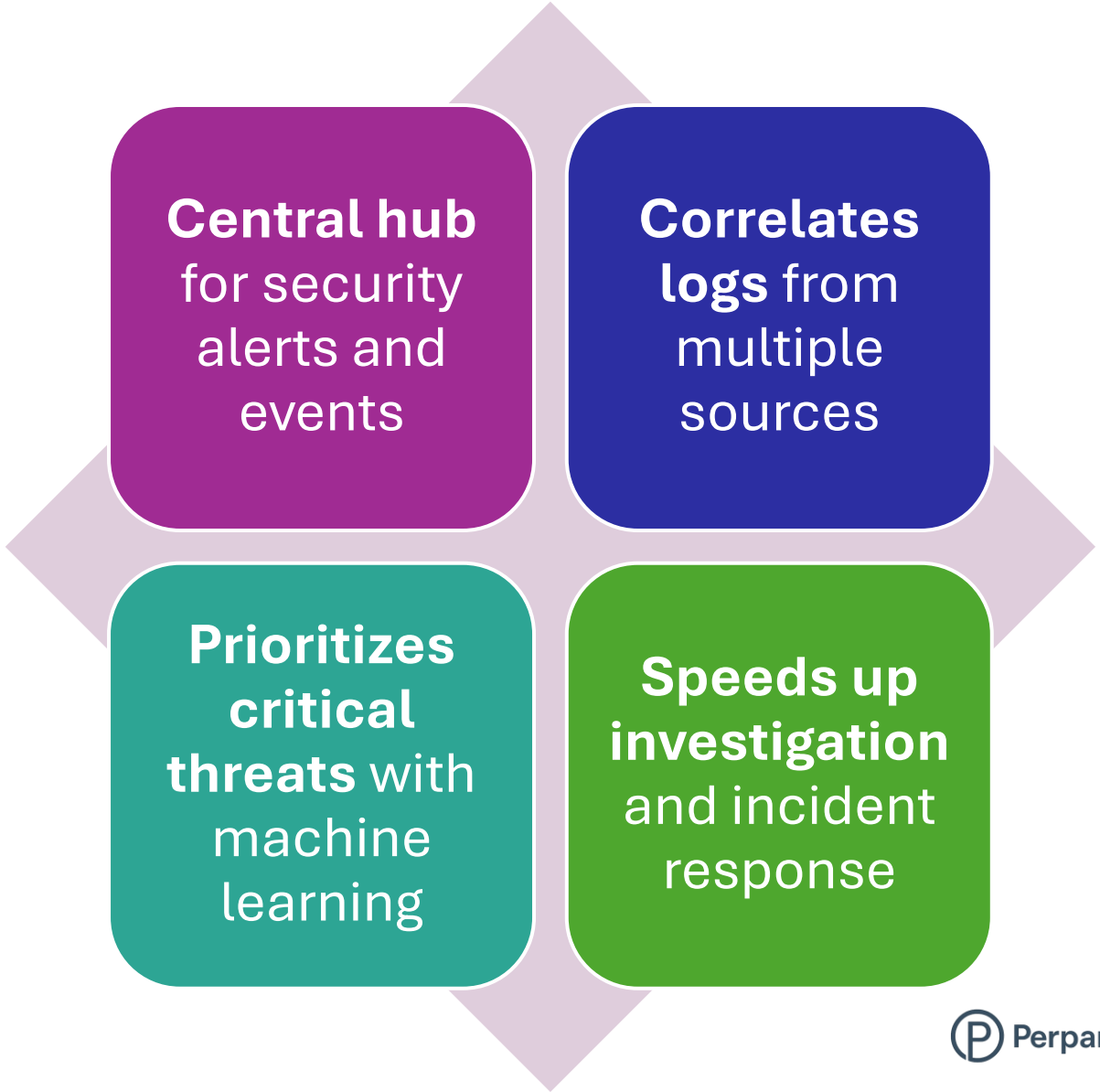
Thousands of alerts hit organizations every day. Sentinel cuts through the noise.

- Cloud-native **SIEM + SOAR** platform
- **Collects + analyzes** data from users, devices, apps, and infrastructure
- **AI-driven threat detection** and response
- Built for **cloud, hybrid, and on-prem environments**

PerparimLabs

Why Sentinel Matters

Visibility is power and Sentinel gives you the full picture.



PerparimLabs

How Sentinel Works

One pipeline. Four stages. Complete protection.

Collect: Connect data from Microsoft Entra ID, Microsoft 365, endpoints & more

Detect: Spot anomalies with analytics & threat intel

Investigate: Dive deep using entity graphs & queries

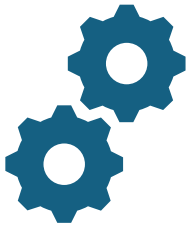
Respond: Automate actions with playbooks (Azure Logic Apps)

PerparimLabs

Why This Project Matters

Before we build, we need to understand the mission.

See how **Sentinel fits in your security ecosystem**



Understand **core building blocks**: data, rules, automation

Build the **foundation for upcoming hands-on labs**

PerparimLabs