



Get Proactive with Microsoft Sentinel



Investigate, Detect & Automate Threat Response Across Microsoft
Cloud





What Is Microsoft Sentinel?





-  Cloud-native SIEM & SOAR platform
-  Integrates with Microsoft 365, Entra ID, Defender
-  Combines detection, investigation, response, and automation
-  Collect – Logs & telemetry
-  Detect – Threats using analytics
-  Investigate – Visualize incidents
-  Respond – Automate with playbooks



Understand the Foundation: SIEM & SOAR







SIEM

- SIEM – Security Information & Event Management
-  Collects log data from across the environment
-  Correlates events across multiple sources
-  Enables threat detection & proactive monitoring
-  Normalizes data for deeper investigation



SOAR

- SOAR – Security Orchestration, Automation & Response
-  Automates repetitive security tasks
-  Responds to threats with prebuilt playbooks
-  Reduces alert fatigue & response time
-  Integrates with ITSM tools like ServiceNow, Jira, Teams

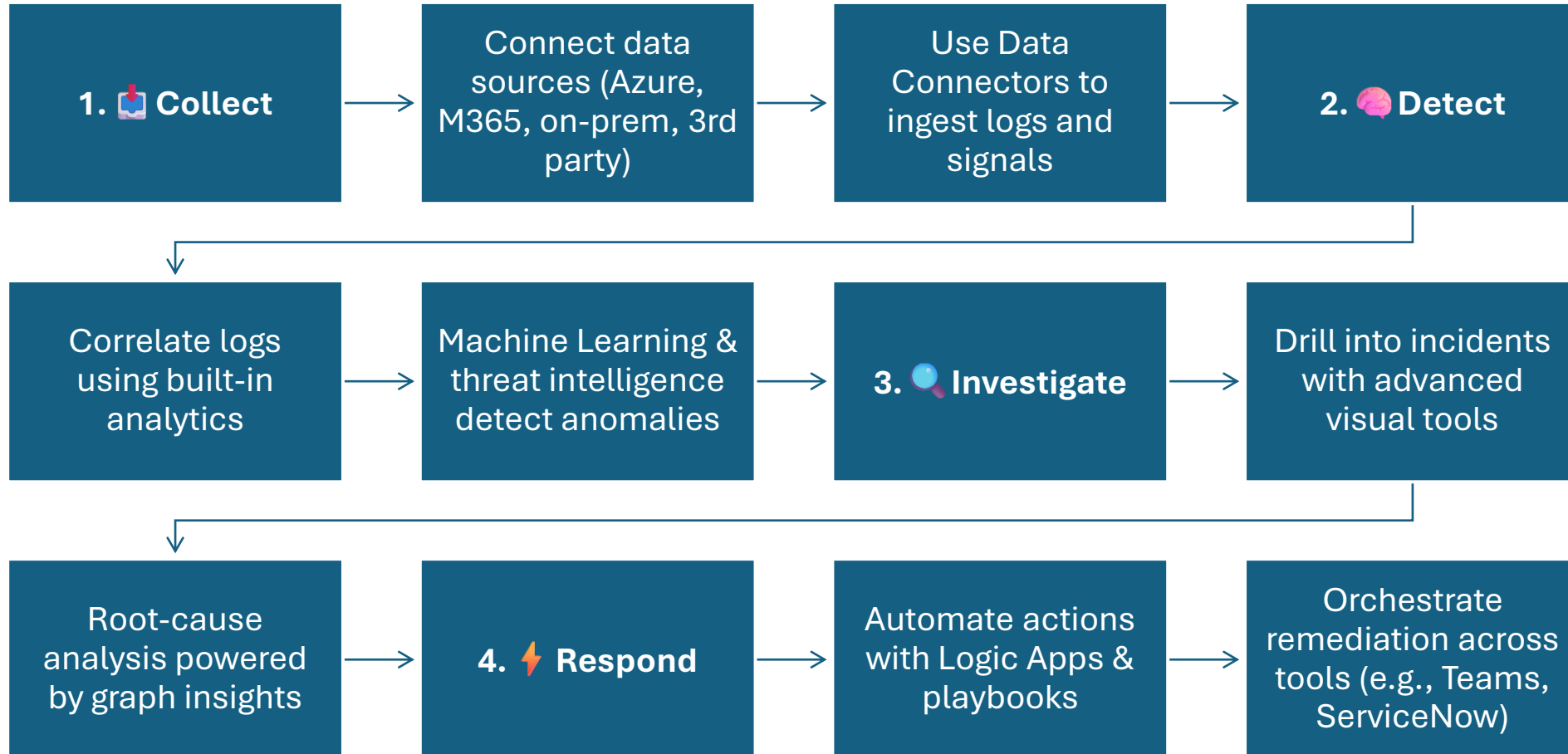
Why Microsoft Sentinel?

- ☁️ **Cloud-native** and scalable for enterprise needs
- 🗝️ **Unified security visibility** across Azure, M365, Entra ID & more
- ⚙️ **Built-in AI** and Machine Learning for threat detection
- 🧠 Correlates millions of signals into actionable incidents
- 🤝 Integrates with third-party tools and on-prem infrastructure
- 📊 Normalizes logs from different formats into one view


🛡️ Sentinel acts as your intelligent *Security Operations Center (SOC)* in the cloud.



The 4 Pillars of Microsoft Sentinel



Automate Threat Response with Logic Apps

 When a risky sign-in is detected →
Automatically disable user + notify admin in Teams



Sentinel uses **Playbooks** powered by **Azure Logic Apps**



Automate actions when alerts are triggered




Integrate with tools like:

Microsoft Teams, ServiceNow, Jira
Defender for Endpoint & Cloud Apps
Microsoft Entra ID
Webhooks and HTTP endpoints



Dive Deep: Investigate and Hunt with Microsoft Sentinel

- Sentinel provides **advanced investigation tools**
- Use dynamic **graph views** to visualize attack paths
- Correlate data across users, devices, and IPs
- Enables **Proactive Threat Hunting**  using:
 - Kusto Query Language (KQL)
 - Built-in workbooks & dashboards

You can trace how a compromised account moved laterally through systems and take action immediately.

Final Thoughts: Why Microsoft Sentinel Matters



- Sentinel is not just a SIEM; it's your *cloud-native security command center*
- Integrated across Microsoft Entra, Defender, and Azure — no extra complexity
- Automate response with playbooks and Logic Apps
- Scales easily from small teams to enterprise-level SOC's
- It gives you *eyes everywhere* — from Entra sign-ins to third-party alerts

linkedin.com/in/perparim-abdullahu-2b0530324

Follow for hands-on Microsoft Entra, Azure, and Security content.