Magos Lab – Week 07: SIEM Introduction (Wazuh/Splunk)

# 🎯 Objectives

Practice using a SIEM to detect basic login events, understand alerting rules, and map logs to user behavior.

# 📋 Lab Tasks

* ☐ Install or access a Wazuh/Splunk demo instance.
* ☐ Create a rule to detect 5 failed login attempts within 2 minutes.
* ☐ Simulate login activity and view the alert in the dashboard.

# 💡 Challenge Task

☐ Map an alert to a relevant MITRE ATT&CK technique.

# 🧠 Reflection

How do detection rules balance between noise and visibility?