Blue Team Toolkit (Enterprise MITRE Edition)

Overview

- Enterprise-focused defensive security toolkit.
- Aligned with MITRE ATT&CK; framework for structured threat detection.
- Supports log monitoring, incident detection, and alert automation.
- Designed for integration with Wazuh, Sysmon, and SIEM platforms.
- Helps security teams perform investigation and triage efficiently.
- Useful for SOC labs, monitoring environments, and enterprise deployments.

Author: Subash Lama

Role: DevOps & Security Automation Practitioner