Junior Security Analyst Intro

## **📓 Notes – Junior Security Analyst Intro**

(Quick personal learning log)

**Lab Name:** Junior Security Analyst Intro  
**Summary:**  
Introduces the SOC environment, Tier 1 analyst responsibilities, and common security monitoring workflows. Covers alert triage, log review, escalation procedures, and basic SOC tools.

**Key Points Learned:**

* Role of a Tier 1 SOC analyst: monitor alerts, investigate, escalate if necessary.
* Common tools: SIEM, IDS/IPS, EDR, ticketing systems.
* Importance of incident documentation and communication.
* Difference between true positive, false positive, false negative.
* SOC shifts and 24/7 monitoring workflows.

**Commands / Tools:**

* No hands‑on commands; primarily theory and workflow.

