Cybersecurity Monitoring & Detection Lab setup:

Tools: Security Onion (IDS), Splunk (SIEM), pfSense (Firewall), Attacker Simulation

1. Cybersecurity Monitoring: Overview

Definition:

Continuous surveillance of IT infrastructure (networks, systems, endpoints) to identify threats *before* they escalate into incidents.

Key Objectives:

- Detect anomalies, intrusions, and breaches in real-time.
- Enable proactive threat response via logs, alerts, and traffic analysis.
- Support compliance (e.g., NIST, ISO 27001).

Core Components:

- Intrusion Detection Systems (IDS) – Analyzes traffic for malicious patterns.
- Firewalls/IPS – Enforce policies and block suspicious activity.
- SIEM (Splunk) – Centralizes log analysis for correlation and investigation.

2. Lab Tools & Configurations:

Security Onion (IDS/NSM)

- Role: All-in-one network security monitoring (NSM) tool with:

- Suricata (signature-based detection).
- Zeek (behavioral analysis via network logs).
- Elastic Stack (log storage/dashboards).

- Workflow:

1. Monitors ingress/egress traffic for IOCs (Indicators of Compromise).
2. Generates alerts in the Alerts dashboard for analyst triage.
3. Supports forensic investigations via packet capture (PCAP) replay.

Splunk (SIEM)

- Use Case: Ingest and correlate Windows event logs (e.g., failed logins, PowerShell execution).
- Advantage: Enables timeline reconstruction of attacks via indexed logs.
- Query Example:

source="win_events.log" EventCode=4625 | stats count by src_ip

(Detects brute-force attempts by source IP.)

pfSense (Firewall):

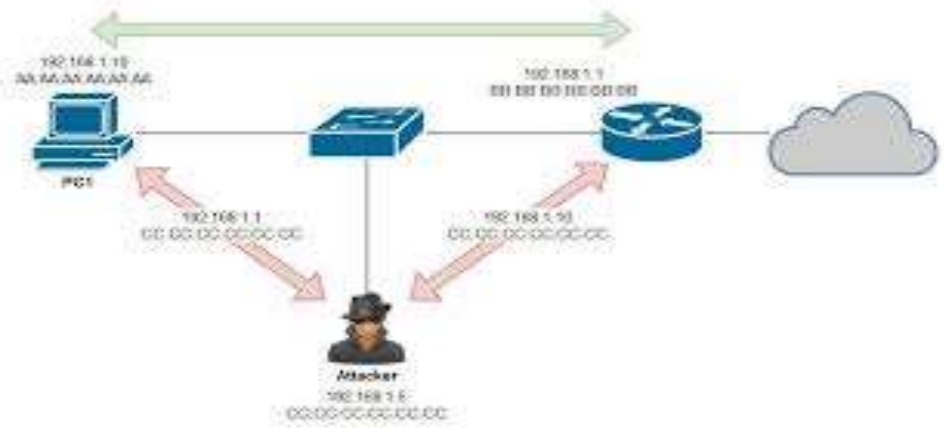
- Functions:

- Network segmentation (isolates LAN/WAN/DMZ).
- Stateful packet inspection (SPI) + DHCP management.
- Optional: VPN termination, IDS/IPS integration.

Attacker Machine (Kali Linux):

- Simulated Threats:

- Lateral movement (e.g., Pass-the-Hash).
- Exploit propagation (e.g., EternalBlue).
- Command-and-Control (C2) beaconing.



3. Key Takeaways:

- Defense-in-Depth: Layered monitoring (IDS + SIEM + Firewall) reduces blind spots.

- Threat Hunting: Use Splunk to pivot from alerts to raw logs (e.g., `eventvwr.msc` → EventID 4688).

- Incident Response: Security Onion's **Squert** GUI prioritizes alerts by severity.

4. References

- [Security Onion Documentation](https://docs.securityonion.net/)

- [Splunk Enterprise Security](https://www.splunk.com/en_us/cyber-security.html)

- [pfSense Official Guide](https://docs.netgate.com/pfsense/en/latest/)