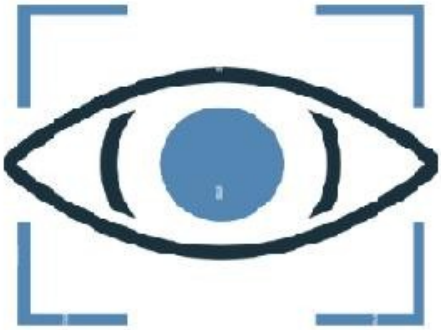
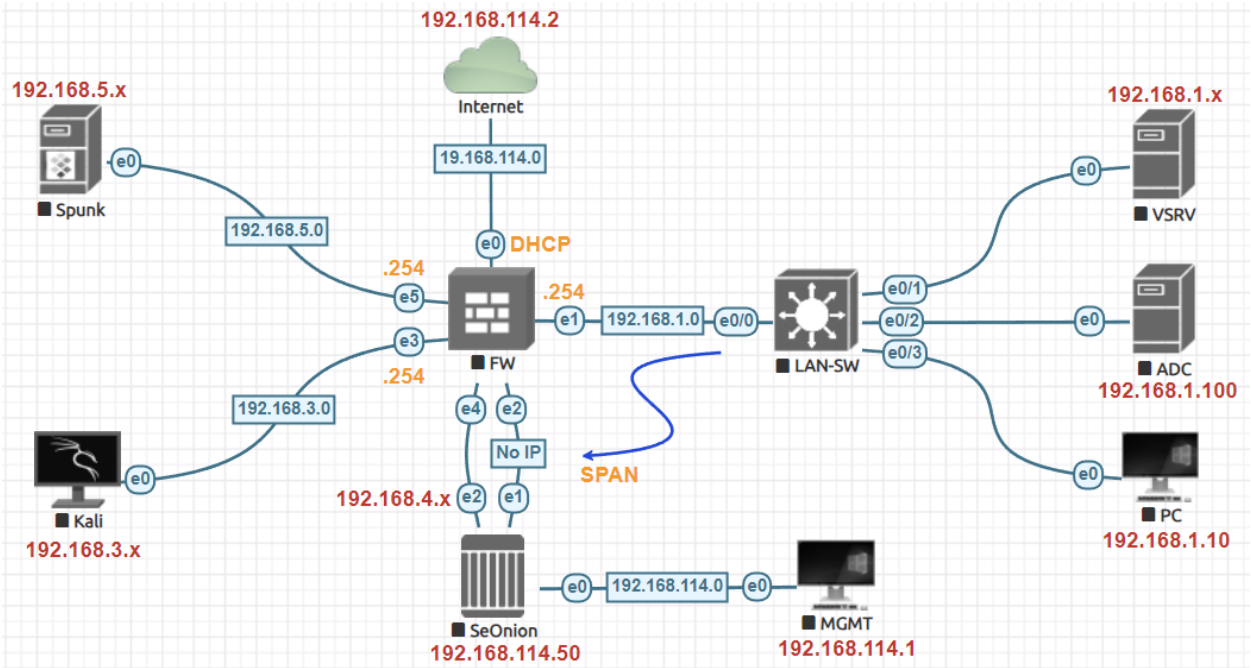
Cyber Security Monitoring and Detection:

Cyber Security Monitoring is the process of continuously monitoring IT infrastructure to detect cyber threats and data breaches.



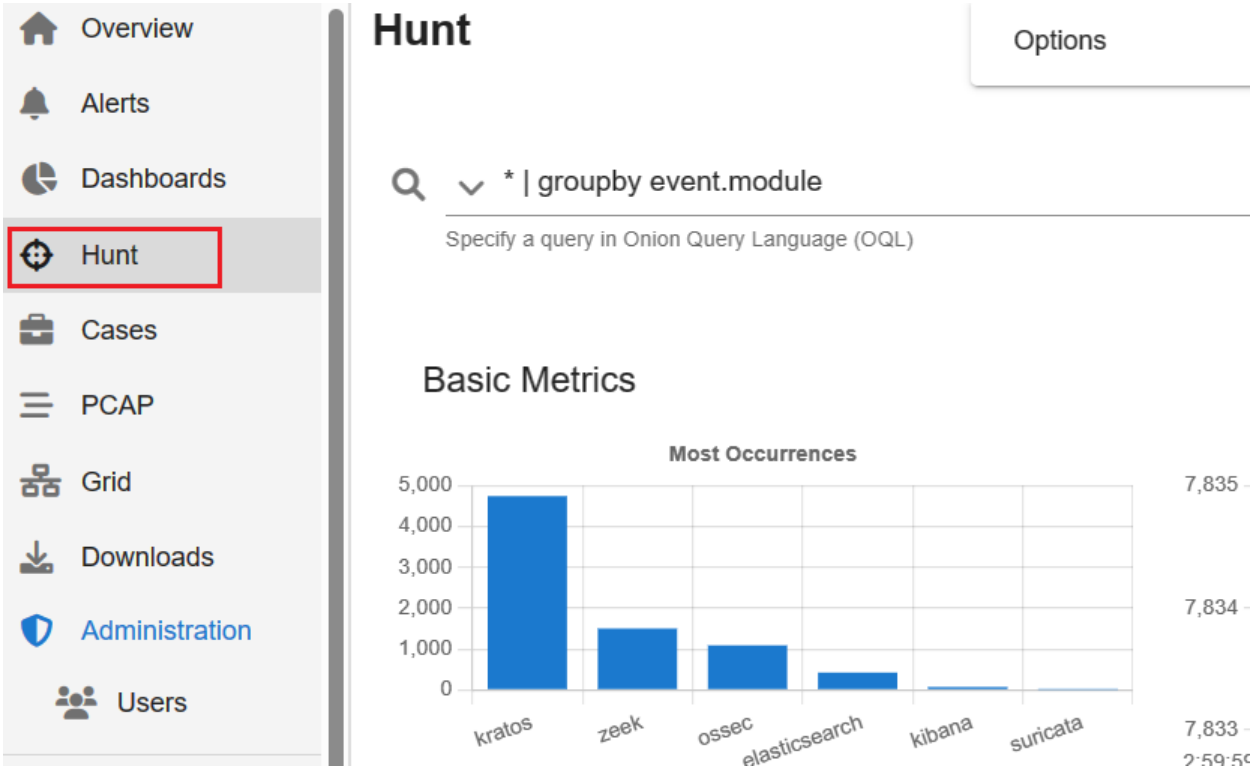
This Cybersecurity Lab has victim machines, IDS, Log Analysis, Active Directory, Firewall Application, and a Hacker Machine Kali Linux.



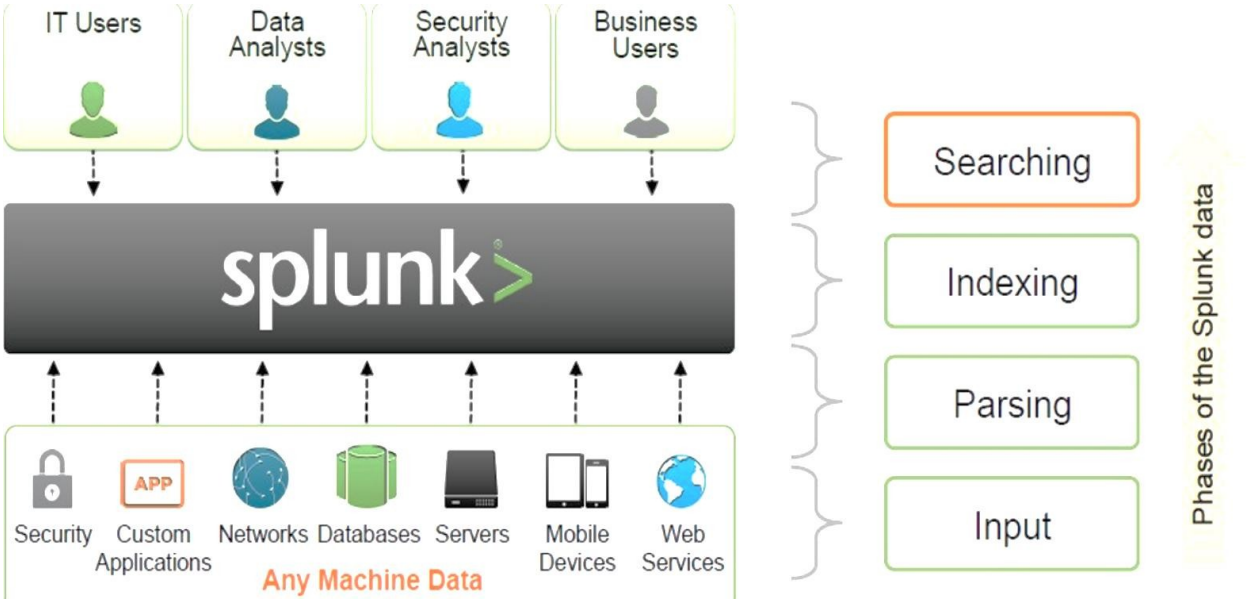
As an Intrusion Detection System, I used Security Onion which is a free IDS tool that can alert and log events that can possibly be malicious. This Security Onion as an all-in-one IDS, network security monitors with log management and forensic capabilities. The purpose of Security Onion is to monitor firewall traffic going to and from the network to identify malicious or suspicious activity. The “Alerts” page displays any activity that has come across as suspicious & is certainly the responsibility of the Cybersecurity analyst to investigate.

Security Onion SOLUTIONS

The purpose of the Hunting tab is to effectively identify threats within the event. Any event that is in the Alerts page can be turned into a “Case” -which is essentially an investigation tab. In the Cases tab you can look at all of your on-going investigations, reviewing the status.



For this lab, Splunk as a Log Analyzer is configured to receive windows logs from the forwarder so that the Analyst can investigate the events. This is going to be useful for when the Windows machines are attacked, as the logs will show the events.



pfsense will be configured as a firewall to segment the network and route traffic this firewall is also configured as DHCP Server as well.

Kali Linux will be used as an Attacker Machine to propagate different forms of offensive actions against the Domain Controller (DC) and the other machines in the LAN Segment.