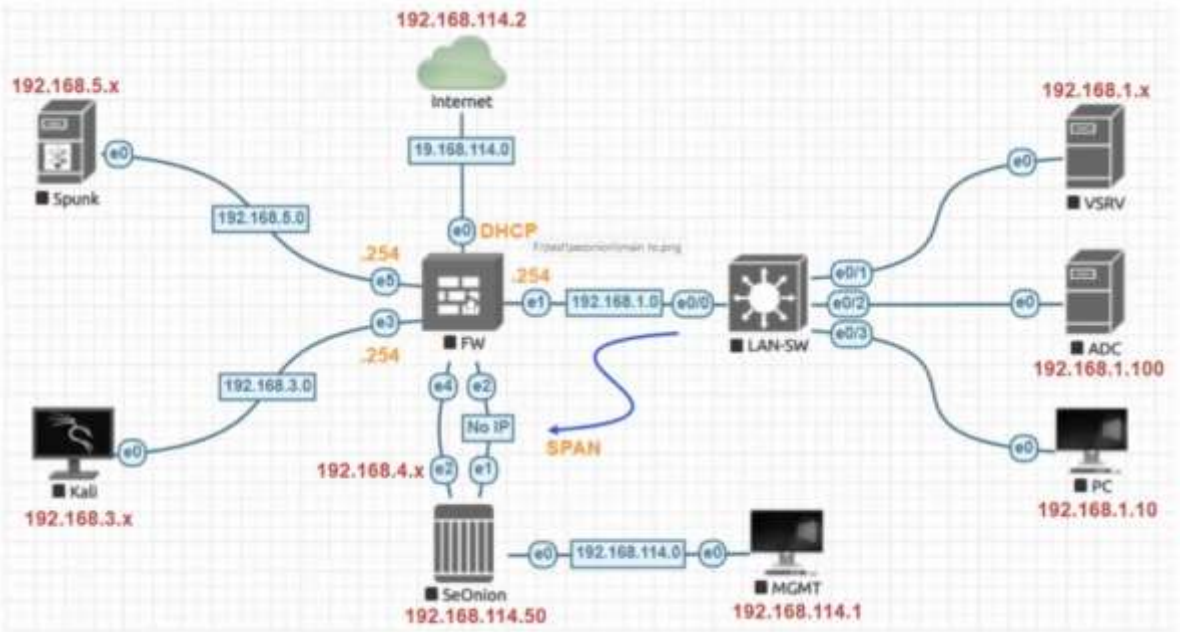
Cybersecurity monitoring and detection lab setup way:

Graphical view of lab setup:



Software/platform that use:

Firewall	pfSense-CE-2.6.0-RELEASE-amd64.iso
PC1	Win11 x64 Pro 2022.iso
ADC	Server 2019 En Jun 2020.iso
Kali	kali-linux-2023.2.vmdk
SecOnion	securityonion-2.3.250-20230519.iso
Metasploitable	Metasploitable 2.vmdk
Splunk	Ubuntu Server 22.10 (64bit).vmdk
MGMT	Host System Windows 11

Ip assigning:

External Subnet	192.168.114.0/24
Internal LAN Subnet	192.168.1.0/24
SPAN Port IP Address	No IP Address
Attacker Subnet	192.168.3.0/24
Security Onion Logs Subnet	192.168.4.0/24
Splunk Log Collector Subnet	192.168.5.0/24
Metasploitable IP Address	Through DHCP
ADC IP Address	192.168.1.100
PC1 IP Address	192.168.1.10
Attacker IP Address	Through DHCP
Splunk IP Address	Through DHCP
Security Onion IP Address	192.168.114.50
Security Onion MGMT IP Address	192.168.114.1
DNS	8.8.8.8, 4.4.4.4

Adapter info:

VMware Adopter	Network Connection	Role	PfSense Interfaces
Network Adopter	NAT	WAN	EM0
Network Adopter 2	VMNet2	LAN	EM1
Network Adopter 3	VMNet3	SPAN	EM2
Network Adopter 4	VMNet4	KALI	EM3
Network Adopter 5	VMNet5	SECONION	EM4
Network Adopter 6	VMNet6	SPLUNK	EM5

IP Subnet	Network Connection	Role	PfSense Interfaces	VMware Adopter
192.168.114.0/24	NAT	WAN	EM0	Network Adopter
192.168.1.0/24	VMNet2	LAN	EM1	Network Adopter 2
No IP Address	VMNet3	SPAN	EM2	Network Adopter 3
192.168.3.0/24	VMNet4	KALI	EM3	Network Adopter 4
192.168.4.0/24	VMNet5	SECONION	EM4	Network Adopter 5
192.168.5.0/24	VMNet6	SPLUNK	EM5	Network Adopter 6