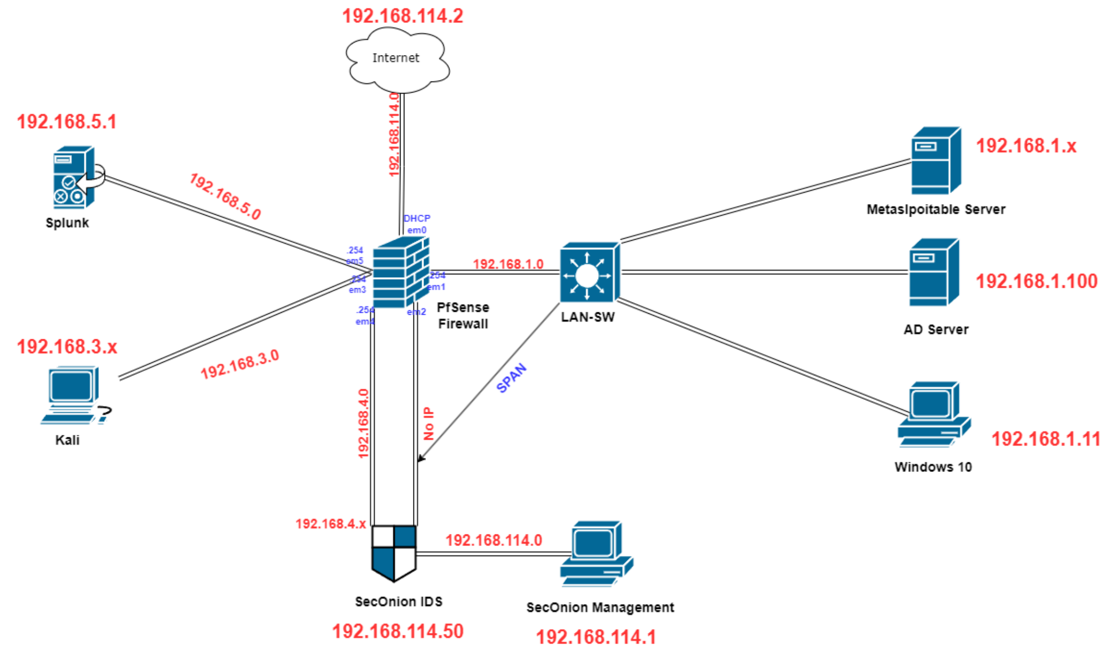
Monitoring & Detection Lab

1. Network specifications



External Subnet	192.168.114.0/24
Internal LAN Subnet	192.168.1.0/24
SPAN Port IP	No IP Address
Kali Subnet	192.168.3.0/24
Security Onion Logs Subnet	192.168.4.0/24
Splunk Server Subnet	192.168.5.0/24
Metasploitable Server IP	DHCP
AD Server	192.168.1.100
Windows 10 IP	192.168.1.11
Kali IP	DHCP
Splunk Server IP	192.168.5.1
Security Onion IP	192.168.114.50
Security Onion Management IP	192.168.114.1
DNS	8.8.8.8, 4.4.4.4

2. VMware Network Adapter

VMware Adapter	Network Connection	Role	PfSense Interfaces
Network Adapter 1	NAT	WAN	EM0

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

IP Subnet	Network Connection	Role	PfSense Interfaces	VMware Adapter
192.168.114.0/24	NAT	WAN	EM0	Network Adapter 1
192.168.1.0/24	VMNet2	LAN	EM1	Network Adapter 2
No IP Address	VMNet3	SPAN	EM2	Network Adapter 3
192.168.3.0/24	VMNet4	KALI	EM3	Network Adapter 4
192.168.4.0/24	VMNet5	SECONION	EM4	Network Adapter 5
192.168.5.0/24	VMNet6	SPLUNK	EM5	Network Adapter 6

3. Virtual Machine version

PfSense Firewall	pfSense-CE-2.7.2-RELEASE-amd64.iso
Windows 10	win10pro 10.0.19045 Build 19045
Ad server	Windows Server 2019 Standard 10.0.17763 Build 17763
Kali	kali-linux-2024.3-vmware-amd64
SecOnion	securityonion-2.4.100-20240903.iso
Metasploitable Server	Metasploitable 2.vmdk
Splunk Server	Ubuntu Server 23.04 (64bit).vmdk
SecOnion Management	Host System Windows 11

4. Host System Specification

Storage	WD_Black SN750 1TB NVMe Internal Gaming SSD
RAM	DDR4 64GB

Storage	**WD_Black SN750 1TB NVMe Internal Gaming SSD**
CPU	AMD Ryzen™ 7 5800X
Operating System	Windows 11 Pro
Virtualization Software	VMware Workstation 17 Pro