SOC and Network Visibility

NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

neoxnetworks.com

Need for SOC

- Protection against threats
- Continuous monitoring and incident response
- Regulatory compliance
- Minimizing damage from security incidents

Evolution

- 1st Generation SOC: 1973-1995
- 2nd Generation SOC: 1996-2001
- 3rd Generation SOC: 2002-2006
- 4th Generation SOC: 2007-2012
- 5th Generation SOC: 2013-Now

Operations

- Monitoring security events and logs
- Detecting and analyzing incidents
- Responding and recovering from incidents

Models

- In-house SOC
- Outsourced SOC
- Hybrid SOC
- SOC Capability Maturity Model Control Objectives for IT (COBIT)

Implementation

- SOC Key Performance Indicators (KPI) and Metrics
- Completion time
- Response time
- Overtime

People

- SOC Level-1 SecOps
- SOC Level-2 SecOps
- Incident Responder
- Subject-Matter Expert/Hunter
- SOC Manager
- Chief Info Security Officer (CISO)

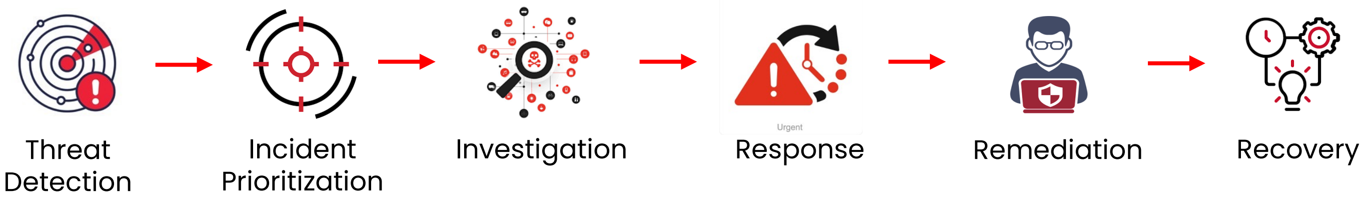
Processes

- Business processes
- Technology processes
- Operational processes
- Analytical processes

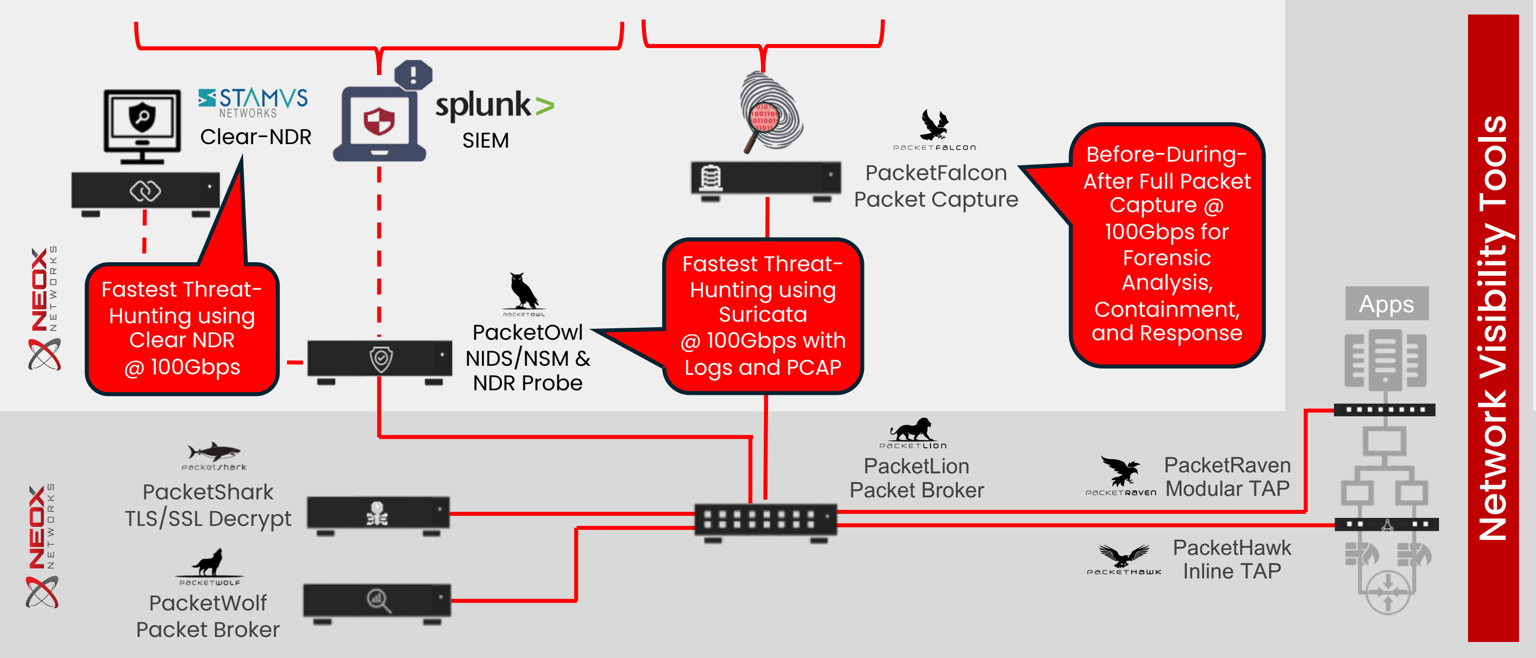
Technologies

- SOC dashboard
- SIEM tools
- Ticketing system
- Automated assessment tool
- Security monitoring tools
- Network visibility/forensics tools

Workflow



Threat Detection → Incident Prioritization → Investigation → Response → Remediation → Recovery



STAMVS NETWORKS
Clear-NDR
splunk>
SIEM
PacketFalcon
PacketFalcon Packet Capture
Fastest Threat-Hunting using Clear NDR @ 100Gbps
PacketOwl
PacketOwl NIDS/NSM & NDR Probe
Fastest Threat-Hunting using Suricata @ 100Gbps with Logs and PCAP
Before-During-After Full Packet Capture @ 100Gbps for Forensic Analysis, Containment, and Response
Apps
NEOX NETWORKS
PacketShark
PacketShark TLS/SSL Decrypt
PacketLion
PacketLion Packet Broker
PacketRaven
PacketRaven Modular TAP
PacketWolf
PacketWolf Packet Broker
PacketHawk
PacketHawk Inline TAP
NEOX NETWORKS
Network Visibility Tools