SOC und Network Visibility

NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

neox-networks.com

SOC-Zuständigkeiten

- Schutz vor Bedrohungen
- Kontinuierliches Monitoring und Incident Response
- Einhaltung von Vorschriften
- Schadenbegrenzung bei Sicherheitsvorfällen

Evolution

- 1. Generation SOC: 1973-1995
- 2. Generation SOC: 1996-2001
- 3. Generation SOC: 2002-2006
- 4. Generation SOC: 2007-2012
- 5. Generation SOC: 2013-Heute

Tätigkeiten

- Monitoring von Sicherheits-ereignissen und Protokollen
- Erkennen und Analysieren von Vorfällen
- Reaktion auf und Wieder-herstellung nach Vorfällen

Modelle

- In-House SOC
- Outsourced SOC
- Hybrid SOC
- SOC Capability Maturity Model Control Objectives für IT (COBIT)

Implementierungen

- SOC Key Performance Indicators (KPI) und Metriken
- Fertigstellungszeit
- Reaktionszeit
- Mehrarbeit

Involvierte Personen

- SOC Stufe-1 SecOps
- SOC Stufe-2 SecOps
- Incident Responder
- Fachexperte/Hunter
- SOC-Manager
- Chief Info Security Officer (CISO)

Prozesse

- Geschäftsprozesse
- Technologie-Prozesse
- Operative Prozesse
- Analytische Prozesse

Technologien

- SOC-Dashboard & SIEM-Tools
- Ticketing-System
- Autom. Assessment-Tool
- Tools für Security-Monitoring
- Netzwerkvisibilität/forensische Tools

Workflow