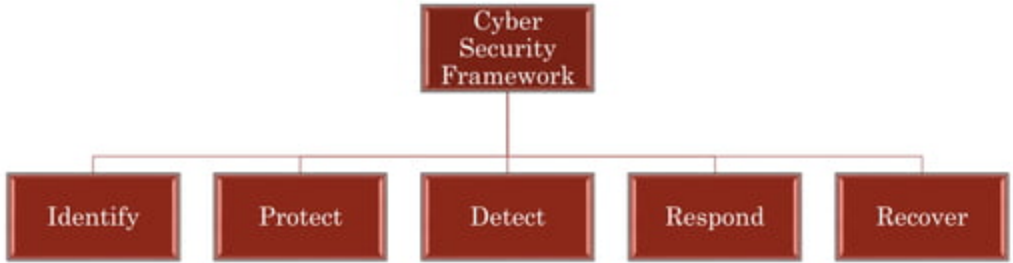
SECURITY OPERATION CENTER

Eng/ Ahmed Ayman Fahmy

OUTLINE

- Cyber Security Framework
- What is SOC ?
- SOC Team
- SOC process
- SOC Platform (Tools)
- Skills needed in a SOC
- Types of SOCs

CYBER SECURITY FRAMEWORK



CYBER SECURITY FRAMEWORK *(CONT.)*

- Identify
  - Identify threats which needed to protect our enterprise.
  - Control who can access your business information.
  - Require individual user accounts for each employee.
  - Create policies and procedures.
- Protect
  - Install and activate security controls (Firewalls, IDS/IPS, ….).
  - Patch your operating systems and applications routinely.
  - Secure your wireless access point and networks.
  - Setup web and E-mail filters.
  - Use encryption for sensitive data.
  - Train employees for security awareness.

CYBER SECURITY FRAMEWORK *(CONT.)*

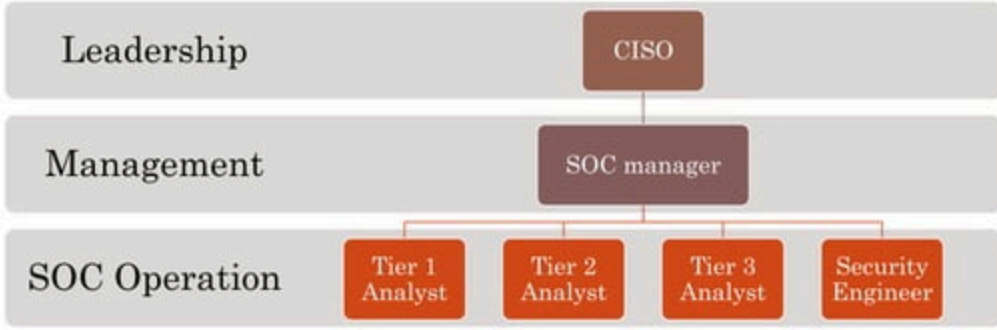
- Detect
  - Install and update anti-virus, anti-spyware and other anti-malware programs.
  - Maintain and monitoring Logs.
- Respond
  - Develop a plan for disasters for information security incidents.
- Recovery
  - Make full pack up of important data and information.

SECURITY OPERATION CENTER (SOC)

monitor, prevent, detect, investigate, and respond to cyber threats around the clock

SECURITY OPERATION CENTER (SOC) *(CONT.)*

- SOC Team



SECURITY OPERATION CENTER (SOC) *(CONT.)*

- **Tier 1 Analyst (Alert Investigator) :**
  - Monitor SIEM alerts.
  - Manages and configures security Monitoring Tools.
  - Alert priority.
  - Perform triage to confirm real security incident is taking place.
- **Tier 2 Analyst (Incident responder):**
  - Receives Incident and performs deep analysis.
  - Correlate with threat intelligence to identify threat actor.
  - Nature of the attack.
  - Data and systems affected.
  - Decide strategy for containment.
  - Remediation and recovery.

SECURITY OPERATION CENTER (SOC) *(CONT.)*

- **Tier 3 Analyst (SME / Threat Hunters):**
  - Vulnerability assessment.
  - Penetration testing.
  - Threat intelligence.
  - Threat Hunters who hunts threat which found their way into the network.
  - Unknown vulnerabilities and security gaps.
  - When major incident occurs join with Tier 2 analyst in responding and containing it.

SECURITY OPERATION CENTER (SOC) *(CONT.)*

- **Security Engineers (Platform Management):**
  - Automated Tools.
  - Integration between security controls and SIEM.

- **SOC manager:**
  - Responsible for hiring and training SOC staff.
  - Manage resources. (Metrics)
  - Manage team when responding to critical security incident.

SECURITY OPERATION CENTER (SOC) *(CONT.)*

- **SOC process**
  - Log source management
  - SIEM management
  - Use case management
  - Playbook management
  - Event management
  - Incident management
  - Vulnerability management

SOC PLATFORM (TOOLS)

- **SIEM** : Security Information and Event Management
- **SOAR** : Security Orchestration, Automation and Response
- **VMDR** : Vulnerability Management, Detection and response
- **NDR** : Network Detection and Response
- **EDR** : End-point Detection and response
- **TIP** : Threat Intelligence Platform
- **OST** : Offensive Security Tools

SKILLS NEEDED IN SOC

- **Tier 1 Analyst**
  - 2-3 years of professional experience.
  - Very good routing & switching knowledge.
  - Good system administration knowledge.
  - Understanding security system functions.
  - Knowledge of SIEM event management.
  - Certificates: CompTIA Cyber Security Analyst (CSA), SANS GMON

TIER 2 SKILLS (INCIDENT HANDLER)

- 4-5 years of professional experience
- 50% of the experience spent as Tier 1 analyst
- Very good routing & switching knowledge
- Very good Internetworking knowledge
- Very good system administration knowledge
- Good in End-point security knowledge
- Experience in operating Firewall, IDS, IPS,.....
- Knowledge of SIEM event management and Use case writing
- Certificates SANA GCIH

TIER 3 SKILLS (THREAT HUNTER)

- 6-9 years of professional experience
- 50% of the experience spent as Tier 2 analyst
- Very good programming knowledge
- Very good networking Knowledge
- Very good system administration knowledge
- Very good in End-point security knowledge
- Experience in digital Forensics
- Experience in using network traffic analysis, deception systems, vulnerability assessment and exploitation tools

TIER 4 SKILLS (ARCHITECT)

- 10-12 years of professional experience
- 50% of the experience spent as Tier 2 analyst
- Very good programming knowledge
- Very good networking Knowledge
- Very good system administration knowledge
- Very good in End-point security knowledge
- Experience in SIEM, SOAR, VMDR, EDR and NDR
- Experience in using network traffic analysis, deception systems, vulnerability assessment and exploitation tools
- Certifications: CISSP Certified Information Systems Security Professional (ISC)2, CISM Certified Information Security Manager ISACA.

TYPES OF SOC

Dedicated SOC	Classic SOC with dedicated full time staff, operated fully in house 24/7/365 operations.
Distributed SOC	Some full time staff and some part time, typically operates 8x5 in each region
Multifunctional SOC / NOC	Dedicated team which perform both functions of a network operation center and a SOC
Fusion SOC	Traditional SOC combined with new functions such as threat intelligence, operational technology
Command SOC / Global SOC	Coordinates other SOCs in global enterprise provide threat intelligence, situational awareness and guidance
Virtual SOC	No dedicated facility, part time members usually reactive and activated by security incident
Managed SOC	Many organizations turned to MSSP Managed Security Service Providers to provide SOC services on outsourced basis