1. SOC Fundamentals

I. The SOC and Its Role

I.I Key Functions of a SOC

- Reactive
  - Monitoring and Detection
  - Incident Response
  - Forensic Analysis
  - Malware Analysis
- Proactive
  - Threat Intelligence
  - Threat Hunting
  - Vulnerability Management
  - Security Awareness Training

II. Day in the Life of a SOC Analyst

- Alert Triage
  - Monitor the alert ticket queue
  - Asset credibility and severity
- Incident Triage
  - Information gathering
  - Follow processes
- First-Line Analysis and Investigation
  - Use tools/techniques to assess incident
  - Logs, network traffic, configs, OSINT
- Documentation and Reporting
  - Clear and concise
  - Findings, Actions, Resolutions
- Escalation and Collaboration
  - Coordinate response activities

- Continuous Improvement and Cross-Training

III. Information Security Refresher

CIA Triad

- Confidentiality
- Integrity
- Accessibility

AAA Framework

- Authentication
- Authorization
- Accounting

Vulnerabilities, Threats, Risks

- Vulnerability
  - Weakness in system
  - Can be exploited by threats to compromise CIA
  - Expose organization to THREATS
- Threat
  - Any potential danger to info or systems
  - Malware, phishing, denial of service
  - Takes advantage of a VULNERABILITY
- Risk
  - Likelihood of a THREAT exploiting a VULNERABILITY
  - Potential for loss and damage when a THREAT occurs

SOC Items of Interest

- Log
  - Record of events or actions
  - Used for monitoring and troubleshooting security incidents
- Security Event
  - Observable occurrence that has a potential significance for security
  - All incidents are events, not all events are incidents

- Security Incident
  - Occurrence that actually harms info or systems
  - Constitutes a violation of law, security policy, procedure, or acceptable use
- Alert
  - Notification generated by security systems or personnel
  - Indication of a potential security issue or suspicious activity

Security Controls

- Defense in Depth
  - Layered security
  - Multiple barriers to threats
- Administrative Controls
  - Security policies
  - Change management procedures
  - Incident response plans
- Technical Controls
  - Firewalls, EDR
  - IDS
  - MFA
- Physical Controls
  - Access Control system
  - Surveillance cameras, Biometrics

Controls

- Preventative Controls
  - ACLs, Firewalls, EDR, IPS
- Detective Controls
  - IDS, SIEM, logs, cameras
- Corrective Control
  - Backus, IR Plans, Patch Management
- Deterrent Control
  - Physical Barriers, signage, tamper seals
- Compensating Control
  - Network Segmentation, data masking

Risk Control Strategies

- Risk Transference
  - Cybersecurity insurance
  - Cloud providers
- Risk Acceptance
  - Acknowledge and tolerate a risk
- Risk Avoidance
  - Limit type of data stored on a server
- Risk Mitigation
  - Implementing patch management

Security Policies

- Acceptable Use Policies
  - What is/isn't allowed within organization
- Password Policy
  - Requirements for password creation
- Data Classification Policy
  - Categorize data based on sensitivity/importance
  - How to handle data at each level
- Change Management Policy
  - Planning/implementing changes to systems

IV. SOC Models, Roles, and Organizational Structures

SOC Models

- Internal SOC
- Managed SOC (MSOC)
- Hybrid SOC

SOC Roles

- SOC Analyst
- Specialized Roles
- Management Roles

V. Incident Management

Event Management

- Collection, normalization, analysis
- Logs, alerts, endpoints
- Identify abnormal or suspicious activities
- Security Information and Event Management

Incident Management

- Incident Identification
- Incident Classification
- Incident Investigation
- Incident Containment
- Incident Eradication
- Incident Recovery

Detection Outcomes

- False Positive - benign activity, system detected by mistake
- True Positive - correctly identified malicious activity
- False Negative - system failed to detect threat
- True Negative - benign activity

VI. SOC Metrics

- Mean Time to Detect (MTTD)
  - Lower MTTD = faster detection
- Mean Time to Resolution (MTTR)
  - Lower MTTR = more efficient IR
- Mean Time to Attend an Analyze (MTTA&A)
  - Lower = reduced response latency
- Incident Detection Rate
  - Higher rate = better visibility and monitoring
- False Positive Rates (FPR)

    - Lower rate = more accurate detection
- False Negative Rates (FNR)

Key Performance Indicators (KPIs)
Key Risk Indicators (KRIs)
Service Level Agreements (SLAs)

VII. SOC Tools

SIEM

- Log management
- Real-time Monitoring
- Alerting and Notification
- Incident Response
- Dashboards, Reports, Visualization
- Threat Intelligence

SOAR - Security Orchestration, Automation and Response

- Orchestration
- Automation
- Incident Response
- Integration
- Analytics and Intelligence

Incident Management Tools

- Incident Ticketing
- Alert Management
- Workflow Automation
- Collaboration

Network Security Monitoring

- Packet Capture and Analysis
- Network Traffic Analysis
- Intrusion Detection

- Integration with SIEM

Intrusion Detection and Prevention Systems

- Passive or active monitoring
- Generate alerts
- Actively block and prevent threats
- Logging and reporting

Endpoint Detection and Response

- Real-time endpoint monitoring
- User Entity Behavior Analytics (UEBA)
- Threat Detection and Prevention
- Incident Investigation
- Remediation and Response
- Integration with SIEM

Firewalls

- Network Firewalls
- Next-Generation Firewalls
  - Deep packet inspection
  - Layer 7
- Web Application Firewalls
  - Inspect HTTP traffic
  - Protect web applications
  - Layer 7

Threat Intelligence Platforms

- Data Aggregation and Enrichment
- Indicators of Compromise (IOCs)
- Normalization and Standardization
- Analysis and Prioritization
- Integration with SIEM

Forensic Analysis Tools

- Data Acquisition and Imaging
- File System Analysis
- Memory Forensics
- Registry Forensics
- Network Traffic Forensics

Malware Analysis Tools

- Dynamic Analysis
- Static Analysis
- Behavioral Analysis
- Signature and Pattern Matching
- Integration with TIPs

VIII. Common Threats and Attacks

Social Engineering

- Exploits humans
- Spoofing
- Phishing
  - Spear Phishing
  - Whaling
- Vishing
- SMiShing (SMS Phishing)
- Quishing (QR Code Phishing)

Malware

- Worm
  - Self replicating
  - Infect and propagate
  - Spreads across networks
  - Stuxnet, Blaster
- Spyware / Adware
  - Monitor user activity
  - Display unwanted advertisements

- Trojan
  - Disguised malware
  - Acting as legitimate software
  - RAT - Remote Access Trojan
  - Botnets
  - Deliver Ransomware
- Ransomware
  - Infection
  - Ransom Demand
  - Payment
  - Decryption
- Botnet
  - Network of compromised devices
  - Controlled by a remote attacker
  - Used to coordinate attacks
- File-less Malware
  - Memory-based malware
  - No traces on disk
  - Evade detection and logging
  - Living off the land

Identity and Account Compromise

- Usernames, passwords, SSN, PII
- Impersonation, fraud, theft
- Methods include
  - Phishing
  - Brute Force
  - Credential Stuffing
  - Social Engineering
  - Malware

Insider Threats

- Threats from the "inside"
  - Current or former employees
  - Contractors
  - Partners

- Malicious, careless, compromised
- Can lead to severe exposure and damage
  - Data breaches
  - IP theft
  - Reputation damage

Advanced Persistent Threats (APTs)

- Highly skilled, well funded adversaries
- Sophisticated
- Persistent
- Targeted
- Strategic Objectives

Denial-of-Service Attacks

- Disrupt the availability of systems
- Flood traffic and requests
- Intentional or accidental
- Distributed Denial-of-Service (DDoS)
  - Utilize multiple compromised systems
  - Amplification
  - Hard to defend and block

Data Breaches

- Data exposure, theft, or compromise
- PII, credentials, Financial records, IP
- Malicious actions and human error
  - Misconfiguration
  - Inadequate security controls

Zero Days

- Vulnerabilities previously unknown to vendor
- No patches, no mitigations
  - Zero days to patch
  - Zero days to protect

- Risk mitigation, risk avoidance

Supply Chain Attacks

- Exploits up the chain
  - Compromises security downstream
- Suppliers, vendors, partners,
- Malware propagates down
  - Hard to detect
  - Malware from "trusted" entities