Domain 7: Security Operations (SecOps)

MIS-5903

https://community.mis.temple.edu/mis5903sec711summer2022

Security Operations – Key Topics

- Operations department responsibilities
- Administrative management responsibilities
- Assurance levels
- Configuration management
- Physical security
- Secure resource provisioning
- Network and resource availability
- Preventative measures
- Patch management
- Incident management
- Recovery strategies
- Disaster recovery
- Business continuity planning and exercises
- Liability
- Investigations
- Personal safety concerns

Role of Operations Department

- Due Care
- Due Diligence
- “Prudent Person” – responsible, careful, cautious, practical
- Maintain the Security – ensuring that people, applications, equipment, and overall environment are properly and adequately secured.

Administrative Management – Personnel Issues

- Separation of duties – minimizes conflict of interest; high-risk activities divided into separate roles
- Job rotation - over time more than one person performs tasks of various positions.
  - Backup individuals
  - Detective – identify fraud
- Complete list of roles identified, with tasks and responsibilities
- Mandatory vacations – alternate employee detects fraud when performing tasks for other staff on vacation (e.g. two full weeks)
- Least Privilege – just enough permissions and rights
- Need to Know

Control Group	Obtains and validates information obtained from analysts, administrators, and users and passes it on to various user groups.
Systems Analyst	Designs data flow of systems based on operational and user requirements
Application Programmer	Develops and maintains production software
Help Desk / Support	Resolves end-user and system technical or operations problems
IT Engineer	Performs the day-to-day operational duties on systems and applications
Database Administrator	Creates new database tables and manages the database
Network Administrator	Installs and maintains the LAN/WAN environment
Security Administrator	Defines, configures, and maintains the security mechanisms protecting the organization
Tape Librarian	Receives, records, releases, and protects system and application files backed up on media.
Quality Assurance	QA ensures that activities meet prescribed standards
Quality Control	QC ensures that activities, services, equipment, personnel operate within standards

Cybersecurity Analyst	Monitors the organization's IT Infrastructure and identifies and evaluates threats that could result in security incidents.
Incident Responder	Investigages, analyzed, and responds to cyber incidents within the organization.
Security Architect	Assesses security controls and recommends and implements enhancements.
Security Director	Develops and enforces security policies and processes to maintain the security and safety of all organizational assets.
Security Manager	Implements security policies and monitors security operations.
Software Developer	Develops and maintains production software
Threat Hunter	Proactively finds cybersecurity threats and mitigates them before they compromise the organization.

Security Personnel

- Implements and maintains security devices and software
- Carries out security assessments
- Creates and maintains user profiles; implements and maintains access control mechanisms
- Configures and maintains security labels in mandatory access control (MAC) environments
- Manages password policies
- Reviews audit logs

Accountability – Reviewing Audit Logs

- Logs should be reviewed routinely; identify variance from baseline
- Questions to ask:
  - Are users accessing information or performing tasks not necessary for their job description?
  - Are repetitive mistakes being made? (may indicate training)
  - Do too many users have rights and privileges to restricted data or resources?
- Clipping Levels – baseline for violation activities (e.g. IDS)
- Unusual or Unexplained Occurrences
- Deviations from standards
- Unscheduled Initial Program Loads (aka Rebooting)

Assurance Levels

- Operational assurance concentrates on architecture, embedded features, functionality that enable the customer to continually obtain the necessary level of protection
- Life-Cycle assurance pertains to how the product was developed and maintained

Configuration Management

- Process of establishing and maintaining effective system controls, which is part of operational security.
- System startup and shutdown sequences, error handling, restoration from known good sources
- Trusted Recovery – crash of freeze should not put the system into an insecure state
  - System reboot
  - Emergency system restart
  - System cold start

After a System Crash

- Enter into single user or safe mode
- Fix issue and recover files *in single user mode*
- Validate critical files and operations

Security Concerns

- Protect bootup sequence (C:, A:, D:)
- Do not allow bypass or disabling of system logs
- Do not allow system forced shutdowns
- Do not allow outputs to be rerouted

Input and Output Controls

- Data entered into a system should be in the correct format and validated to ensure it is not malicious
- Transactions should be *atomic*, that they cannot be interrupted (TOCTOU)
- Transactions must be timestamped and logged
- Safeguards implemented for output:
  - Cryptographic hashes or Message Authentication Codes
  - Output labeled to indicate sensitivity or classification
  - Once created, proper access controls (paper, digital, tape)
  - If no information, should contain “no output”
- ActiveX, Plug-Ins, Drivers should be signed

System Hardening

- Wiring, Network Equipment should be locked or physically inaccessible
- Portable Devices and Media secured both physically and technically
- Gold Master (GM) for workstations
  - Create new baseline
  - Disable or Remove unnecessary components
  - Use unprivileged users rather than root or system

Remote Access Security

- Two Factor Authentication
- Secure Protocols even on VPN
- Strong authentication
- Administered locally instead of remotely
- Only a few administrators

Physical Security

- Facility Access Control
  - Access control points identified, marked, monitored
- Locks – delay mechanism
  - Tumbler lock
  - Cipher locks – programmable – should have visibility shield
    - Door delay
    - Key override
    - Master keying
    - Hostage alarm
  - Device Locks
    - Switch controls
    - Slot locks
    - Port controls
    - Peripheral switch
    - Cable traps
- Lock bumping
- Lock Drilling
- Removal of Hinges, Doorframe

Personnel Access Controls

- Piggybacking
  - Turnstiles (vertical)
  - Mantrap
- Card Badge Readers
  - User activated readers – swipe card or enter a pin
  - System sensing access control readers (transponders)

External Boundary Protection Mechanisms

- Services
  - Control pedestrian and vehicle traffic flows
  - Various levels of protection for different security zones
  - Buffers and delaying mechanisms to protect against forced entry attempts

External Boundary - Control Types

- Access control mechanisms – locks and keys, card access, awareness
- Physical barriers – fences, gates, walls, doors, windows, protected vents, vehicular barriers
- Intrusion detection – perimeter sensors, interior sensors, annuciation mechanisms
- Assessment – guards, CCTV
- Response – guards, local law enforcement
- Deterrents – signs, lighting, environmental design

Fencing

- Heights:
  - Three to four – deter casual trespassers
  - Six to seven – considered too high to climb easily
  - Eight feet or higher – deter more determined intruder
- Barbed wire – angled to prevent
  - Angled inwards – prevents escape (e.g. prison)
  - Angled outwards – prevents entry
- Buried – posts, also fencing itself
- Lower gauge = thicker
- Perimeter Intrusion Detection and Assessment System (PIDAS) – sensors, can cause false alarms

Gates

- I – residential usage
- II – commercial where public access is expected
- III – Industrial usage where limited access expected (not serving the general public)
- IV – Restricted access – monitored either in person or via closed circuitry
- Bollards – allow pedestrian traffic

Lighting

- Zones should overlap
- Guard in areas of less light to offer glare protection
- Continuous lighting
- Standby lighting – different times
- Responsive area illumination (sensor)

Video

- Closed Circuit TV (CCTV) considerations:
  - Purpose
  - Internal or external
  - Field of view
  - Illumination of environment
  - Integration with other security controls (Guards, IDS, alarms)
- Use Charged Coupled Devices (CCDs)
  - Focal length
  - Digital vs Optical zoom
  - Depth of Field / Depth of Focus
  - Auto iris if lighting changes
  - Pan, Tilt, or Zoom (PTZ)
  - Coupled with annunciator systems

Intrusion Detection Systems

- Electromechanical – change or break in a circuit
- Photoelectric (photometric) – detect change in light beam
  - Cross-sectional uses hidden mirrors to create a “mesh”
- Passive Infrared (PIR) – detects changes of heat waves
- Acoustical detection – uses microphones
- Vibration sensors
- Wave pattern motion detectors – pattern is returned
- Proximity detector or capacitance detector – emits measurable magnetic field
- Electrostatic – creates electrostatic magnetic field

Patrol Force

- Guards – can sign in guests / visitors
- Dogs
  - High sense of smell and hearing
  - Cannot differentiate between authorized and unauthorized

Auditing Physical Access

- Date and time of access attempt
- Entry point where attempted
- User ID provided during attempt
- ANY unsuccessful access attempts, especially during unauthorized hours

Secure Resource Provisioning

- Asset inventory
  - Tracking hardware
  - Tracking software
    - Application whitelisting
    - Gold Master
    - Enforcing least privilege (only install required software)
    - Automated scanning
- Configuration Management – establishing and maintaining consistent baselines on systems
- Cloud services – IaaS, PaaS, SaaS

Change Control Process

- Request for Change
- Evaluate the Change
- Plan the Change
- Approval of Change
- Implementation
- Documentation of Change (approvals and denials)
- Review the (completed) Change
- Report to management

- Standard Changes (preauthorized – e.g. adding RAM)
- Emergency Changes (e.g. Zero Day Patch)
- Normal Changes

Resource Availability

- Redundant hardware – hot swapping
- Fault-tolerant solutions
- Service Level Agreements (SLAs)
- Solid operational Procedures
- Mean Time Between Failures (MTBF)
- Mean Time to Repair (MTTR)
- Single Point of Failure
- Clustering
- Grid Computing

Storage Fault Tolerance

- Redundant Array of Independent Risks (RAID)
- Direct Access Storage Device – hard drive
- Sequential Access Storage Device - tape drive
- Massive Array of Inactive Disks (MAID)
- Redundant Array of Independent Tapes (RAIT) (write only)
- Storage Area Networks
- Hierarchical Storage Management (HSM) – moves from faster media to near-line

Preventive Measures

- Understand the risk
- Use the right controls
- Use the controls correctly
- Manage your configuration
- Assess your operation

Examples of Preventive Measures

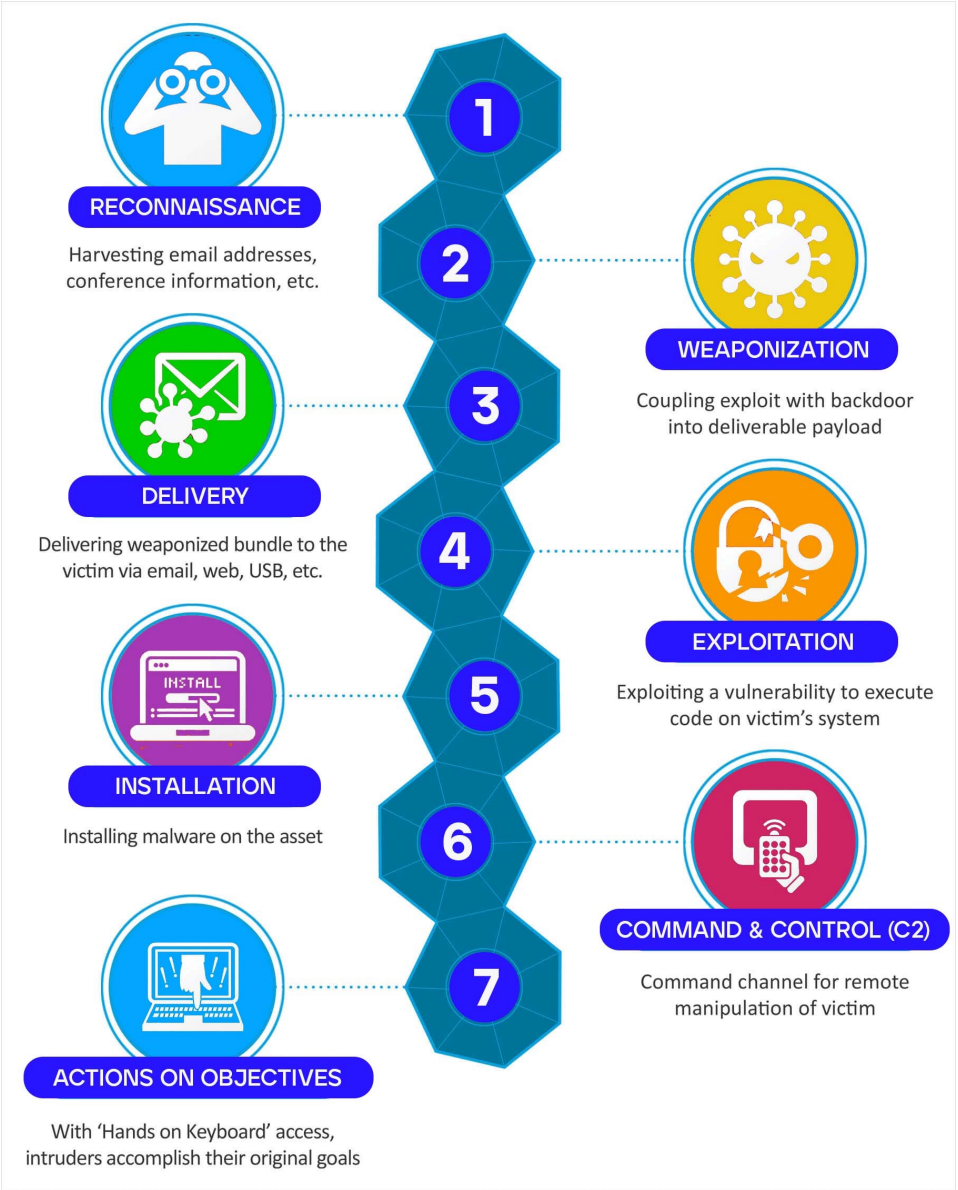
- Firewalls
  - Next Generation Firewall (can use external sources – policy server, Active Directory)
- Intrusion Detection and Prevention Systems
  - Host-based
  - Network-based
  - Wireless
- Blacklist – known bad resources
- Whitelist – known good resources
- Centrally Managed Patch Management
- User Entity Behavior Analysis (UEBA)

Antimalware

- 90 to 99.9% effective against *known* malware
- Sandboxing – application execution environment to isolate executing code

Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control (C&C)
- Actions on the Objective



Incident Management Process (General)

- Identify the event
- Analyze the event to determine counteractions
- Correct the problem(s)
- Keep the event from happening again

Incident Management Process (ISC)2

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Learn

BCP Issues

- Computer Equipment – hardware
- Software (backup, code escrow)
- Voice and Data Communications
- Human resources
- Transportation (equipment and personnel)
- Supplies (paper, forms, cabling)
- Documentation
- Environment (HVAC)
- Data and personnel security

Data Backups

- Full backup – all files – longest to backup, “quickest to recover”
- Differential backup – since last full, medium backup, medium recover
- Incremental – since last full or incremental
  - Shortest backup time
  - Longest recovery time – must restore multiple sessions
  - Sets archive bit to zero (0)
- Offsite
- Disk Shadowing – more than one copy (over time)
- Electronic vaulting – makes copies of files as modified and periodically copies in batches
- Remote Journaling – moves journal or transaction logs (deltas)
- Tape Vaulting – data sent over WAN link

Recovery

- Recovery Point Objective (RPO) – before incident
- Maximum Tolerable Downtime (MTD) – length of time organization can survive outage
- Recovery Time Objective (RTO) – recovery from tape
- Work Recovery Time (WRT) = remainder of MTD after RTO – testing processes
- Prioritize systems based on Business Impact Analysis (BIA)
- Insurance – addresses financial risk
  - Business Interruption
  - Cyber Insurance

Recovery Plans

Plan Type	Description
Business resumption plan	Focuses on how to re-create necessary business processes. (does not focus on IT)
Continuity of Operations (COOP) Plan	Establishes senior management and headquarters after a disaster. Commonly used by US government.
IT Contingency Plan	Plan for systems, networks, and major applications recovery procedures.
Crisis communications plans	Includes internal and external communications structure and roles. Contains previously developed statements to be released.
Cyber incident response plan	Focuses on malware, hackers, intrusions, attacks, and other security issues. Outlines procedures for incident response.
Disaster recovery plan	Focuses on how to recover various IT mechanisms after a disaster. (e.g. alternate site)
Occupant emergency plan	Establishes personnel safety and evacuation procedures

Investigation Process

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

Evidence Qualities

- Relevant – reasonable and sensible relationship to the findings
- Complete – present the whole truth of an issue
- Sufficient (believable) – persuasive to convince a reasonable person of the validity of the evidence; not subject to personal interpretation
- Reliable – consistent with the facts – cannot be circumstantial, and cannot be reliable if:
  - Based on someone's opinion
  - Copies of an original document

Evidence Lifecycle

- Collection and Identification
- Storage, Preservation, and Transportation
- Presentation in Court
- Return of the Evidence to the victim or owner

Different Types of Assessments

- Network – traffic, log, path tracing
- Media – disk imaging, timeline, registry, slack space, shadow volume
- Software – reverse engineering, malicious code review, exploit review
- Hardware/embedded device – dedicated appliance attack points, firmware and dedicated memory inspections, embedded operating system, virtualized software, and hypervisor analysis

Scientific Working Group on Digital Evidence:

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied
2. Upon seizing of digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for that purpose.
4. All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
6. Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Surveillance, Search, Seizure

- Fourth Amendment
  - Warrant required for search
  - Does not apply to actions by private citizens unless acting as law enforcement
  - Warrant is limited unless *exigent circumstances* exist – attempted destruction of possible evidence
- Enticement (e.g. honeypot) is legal
- Entrapment is neither ethical nor legal (did not originally have the intention)

Liability and Ramifications

- Due Care - organization did all it could have reasonable done
- Due Diligence – organization investigated all of the possible weaknesses and vulnerabilities
- Compliance – Legal, Contractual, Third-Party
  - Governance, Risk, Compliance

Next Steps…

- Continue Discussion on Class Website
- Next week class – Tuesday July 12th
- Questions?