



Security+

Domain 4: Security Operations Part 2

SY0-701

Brian Olliff

Defensive Engineering Instructor

Topics

Endpoint Protection

Email Security

Web Filtering

Identity Management

Multifactor Authentication

Security Automation

Incident Response Steps

IR Training & Testing

Digital Forensics

Learning Objectives

- Understand different tools and methods for protecting endpoints
- Be familiar with techniques used to protect email systems
 - + SPF, DKIM, DMARC
- Understand the purpose and basic configuration options for web filtering
- Be able to explain identity and access management systems
 - + Access controls, MFA, passwords, PAM
- Explain security automation and orchestration
- Understand incident response steps and procedures
- Be familiar with digital forensics & data sources for investigations

Endpoint Security Methods



Endpoint Protection Software

- Anti-virus (AV)
 - Signature-based detection
 - Not sufficient as only means of detection
 - Most will provide general malware protection
- Endpoint detection & response (EDR)
 - Designed to detect and take action on malware execution
 - Provides real-time/historical visibility into compromise (can use AI/ML)
 - Can assist with containment and remediation
 - Often managed by (and reports to) cloud portal
- Extended detection & response (XDR)
 - Includes data from EDR clients plus network, cloud, email, firewall, etc

Operating System Security

- Applies to servers and workstations (any OS)
- Multiple control methods
 - Access controls & authentication mechanisms
 - App security, secure coding, patch management
 - Endpoint protection, system monitoring
 - User awareness training
- Best practice secure baselines as starting point
 - Assist with ensuring systems are configured securely
 - Include standard hardening techniques

Operating System Security

- Group Policy
 - Windows centralized management/configuration with Active Directory
 - Enforce security settings, application installations, configurations, etc
 - Password policies, Windows Firewall, MS Updates
 - Policies “linked” to OUs in AD to apply settings to endpoints
- SELinux
 - Security feature in Linux kernel for access control policies
 - Provides granular control over every process & object
 - If access not needed - blocked
 - Allows better isolation of applications, system & file access restrictions
 - Helps prevent malicious (or broken) applications from causing harm

File Integrity Monitoring

- Designed to protect system files against unauthorized modification
- Audits files to ensure they match authorized versions
 - Implemented through hashing and signature verification
- Windows protections
 - Windows File Protection service automatically checks
 - System File Checker (SFC) tool can manually verify
- Component of multiple host-based IDS/IPS products
 - Can also be stand-alone product

User Behavior Monitoring

- UBA - User Behavior Analytics (UEBA - User and Entity)
- Monitors and analyzes behavior of users
- Designed to detect potential security anomalies
 - Insider threats, compromised accounts, fraud, etc
- Frequently uses ML detection techniques
 - Data science methods
 - Statistical analysis
- Establishes baseline of “normal” behavior
 - When and how systems/network accessed, resources used, etc
 - Compares activity against baseline to detect potential incidents

Email Security



The Problem

- Email not initially designed to be secure
- Headers are set by system that created email
 - Can result in misleading information
- Methods to verify sender & integrity of messages, reduce spam/phishing
 - Certificates get expensive, require everyone to purchase
- SPF - Sender Policy Framework
- DKIM - DomainKeys Identified Mail
- DMARC - Domain-based Message Authentication, Reporting & Conformance

SPF - Sender Policy Framework

- Provides a method to authenticate sender
 - Helps prevent address forgery (spoofing)
 - Verifies sending IP against list of approved IPs for domain
- DNS TXT record
- Domains can list all servers they send email from
- Receiving servers check SPF record (return-path)
 - If IP of sending server in record - pass
 - Routed as normal
 - If not - fail
 - Message rejected or quarantined

SPF Record

```
v=spf1 ip4=192.168.1.25 include:domain.com -all
```

- **v=spf1** - indicates SPF record & version
 - Record MUST begin with this
- **ip4=** - lists IP address of approved sending server (can have multiple)
- **include:** - check content of this domain SPF record
 - Commonly used to allow third-party senders
- **-all** - failing messages should be rejected
 - **~all** - mark as insecure/spam, but accept
 - **+all** - all messages should be accepted
 - Not commonly used

DKIM - DomainKeys Identified Mail

- Method to digitally sign all emails from domain
 - Provides authentication and integrity checking
- Uses public key cryptography
 - Public key stored in DKIM record (DNS)
 - Private key kept in sending email system(s)
- Sending server adds DKIM header
 - Information used to generate signature
 - Hash of message body
 - Algorithm used
 - Signature
- Receiving server verifies signature against public key

DKIM Header

```
DKIM-Signature: v=1; a=rsa-sha256; d=domain.com; s=mail-  
sel; bh=wMX6SFepjdgl+EfxcDEEtDNdrj05Kgv8e31+tACuzxw=;  
h=From:Subject:Date:To; b=tLlBRaVlrBKpLiu264ks4FyW.....
```

- **a** - algorithm used to compute signature
- **d** - domain of sender
- **s** - selector to use when looking up DNS record
- **bh** - hash of email body
- **h** - which headers used to create signature
- **b** - digital signature

DKIM DNS Record

Name	Type	Content	TTL
mail-sel._domainkey.domain.com	TXT	v=DKIM1; p=76E629F05F70F6853...	6000

- Name
 - **mail-sel** - Selector
 - **._domainkey** - Required to identify DKIM
 - **.domain.com** - Domain
- Content
 - **v=DKIM1** - indicates DKIM record
 - **p=76E629F05F70F6853...** - public key

DMARC - Domain-based Message Authentication, Reporting & Conformance

- DNS record
- Instructs receiving server what to do after checking SPF & DKIM
- Can also include information to send reports

Name	Type	Content	TTL
_dmarc.domain.com	TXT	v=DMARC1; p=quarantine; adkim=r; aspf=r; rua=mailto:email@thirdparty.com;	32600

- p=quarantine - Quarantine messages that fail SPF/DKIM
- adkim=r; aspf=r - Type of check (strict/relaxed)
- rua=mailto:email.... - Where to send DMARC reports

Email Security Gateway

- Spam filtering (inbound and outbound)
 - May also house end-user quarantines
- Attachment scanning (and quarantine)
 - Similar to AV/EDR scanning
- URL checking (sandbox detonation if possible)
- Phishing protection
 - Uses SPF, DKIM, & DMARC
- Outbound encryption
- DLP functionality
 - Protect against data leakage via email
 - Can assist with compliance requirements

Web Filtering



Web Filtering

- Blocks malicious or inappropriate websites
- Analyze web traffic in real-time to restrict based on various criteria
 - URL or IP address
 - Content category
 - Reputation
 - Keywords
- Scanning and filtering can be agent-based or proxy-based
- Multiple filtering methods
 - URL scanning
 - Content categorization
 - Organizational-defined rules
 - Reputation-based filtering

Agent-Based Filtering

- Software installed on endpoint that accesses websites
- Agents communicate with centralized management platform
 - Filtering rules and policies
 - Applied locally on devices
- Often cloud-based management
 - Allows filtering & enforcement regardless of device location
- All filtering occurs locally on device
 - Provides more granular control than centralized filtering
 - Easier HTTPS filtering
 - Application-specific filtering

Centralized Filtering

- Central proxy-based filtering (typically on-prem)
- Intermediate server between endpoint and websites
- Does not require any software installed on endpoints
 - Only filters when device is on network
 - Can filter traffic from ALL devices on network
- Proxy settings configuration required to route traffic
 - On-device configuration
 - Network router configuration
- Agent-based and centralized can use similar criteria for filtering

Filtering Methods

- URL Scanning
 - Filter examines requested URL
 - Can block known malicious content, inappropriate sites, or rule-based
- Content categorization
 - Websites get classified into various categories
 - Social networking, education, gambling, adult, webmail, etc
 - Rules defined to block or allow based on category
- Reputation-based
 - Databases of domains/URLs with assigned reputation scores
 - Scores based on behavior of site, history of content
- Rules
 - Org-defined rules based on needs and policies
 - Can use any filtering criteria to define rules

Web Filtering Challenges

- Over/under blocking
 - Rules and policies too restrictive or not restrictive enough
 - Blocking access to legitimate business-related sites
 - Malicious sites not being blocked correctly
 - Filtering requires continuous monitoring and adjusting
- HTTPS traffic
 - Encrypted and cannot be inspected/filtered without decryption
 - Requires proxy decrypt -> inspect -> re-encrypt
 - Cannot use original certificate from website
 - Privacy considerations

Identity & Access Management



Account Management

- Account provisioning
 - New employees, vendors, service accounts
 - Should use standard procedures or best practices
 - Identities are a form of trackable asset
- Identity proofing
 - Verify an individual is who they say they are
 - Usually using some form of official documentation
 - May involve background or employment check
- Issue credentials (other assets as needed)
 - Username, **temporary** password, MFA method(s)
 - Hardware & software assets

Account Management

- Permissions assignment
 - Identify job role and configure rights as required
 - Role-based, mandatory, or attribute-based access control
 - If privileged access needed, tagged for additional monitoring
- Training
 - General security awareness training
 - Organization-specific policies and procedures
 - Perpetual access to learning resources as needed
- Deprovisioning
 - Remove access rights when no longer needed
 - Disable/delete account according to organization policies

Permission Assignments

- All accounts and access should follow least-privilege
 - Minimum rights needed to perform job role
 - Mitigates impact in event of incident
 - Careful balance between security and functionality
- Continual monitoring of rights to eliminate authorization creep
 - Account granted additional permissions over time
 - Through direct access controls or added to roles/groups
 - Not removed when no longer needed
 - Often occurs when temporary rights are assigned

Federation & Single Sign-on



Directory Services

- Most based on LDAP (Lightweight Directory Access Protocol)
 - Developed from X.500 standard
- X.500 standard identifies objects by DN - distinguished name
 - Attribute-value pairs, comma separated
 - Most specific attribute listed first, becoming progressively broader
- Commonly included components in DN
 - CN - common name
 - OU - organizational unit
 - O - organization
 - C - country
 - DC - domain component

CN=Brian, OU=Training, O=INE, C=US, DC=ine, DC=local

Single Sign-On (SSO)

- Allows login/authentication using single identity
 - Log in to multiple independent applications/systems
- Users need one set of credentials
- Requires central authentication/authorization system
 - Active Directory
 - RADIUS
- Kerberos is common SSO protocol, esp in Windows networks
- **True** SSO prompts for login one time, automatically authenticates other systems

Kerberos

- Key Distribution Center (KDC)
 - Authenticates principals and issues tickets
 - Principals - users, service accounts, devices, applications
 - Consists of Authentication Service and TGS (Ticket Granting Service)
- Principal authenticates with KDC (domain controller in AD)
 - Sends request to authentication service for TGT (ticket granting ticket)
 - Request includes date/time of computer, user's hashed password
- Authentication service checks directory for presence of user account
 - Attempts to decode request by matching PW hash with one stored in AD
 - Verifies request has not expired
- Once verified, responds with TGT and TGS session key
 - TGT - includes client name, IP address, timestamp - encrypted with KDC key

Federation

- Network resources need to be accessible by more than just employees
 - Managing access for internal users is easy
 - Managing for external users (vendors, suppliers, customers) more difficult
- Federation
 - Organization “trusts” accounts created/managed by different network
- Allows identity sharing across boundaries
- Claims-based identity process
 - Principal attempts to access service provider, redirected to IdP (ID provider)
 - Principal authenticates with IdP, obtains claim (signed document/token)
 - Principal presents claim to service provider
 - Validates IdP has signed claim because of trust relationship
 - Service provider can connect authorized principal to its own account DB

SAML - Security Assertion Markup Language

- Allows a single login to gain access to multiple web-based systems
- Written in XML (eXtensible Markup Language)
- Shares authentication and authorization information
- Three components
 - Principal - user
 - Identity Provider (IdP) - authentication source
 - Service Provider - where user is logging in
- SOAP - Simple Object Access Protocol
 - Protocol often used for SAML messages
 - Encapsulated in HTTP/S connections

OAuth

- Open standard that allows authorization across third parties
 - Also allows sharing of other user information (name, email, etc)
- Uses JSON Web Token (JWT) formatting
- Consists of four different roles:
 - Client
 - Requesting entity - frequently another site/service/app
 - Resource server (API server)
 - What the client is attempting to access
 - Authorization server
 - Processes authorization requests
 - Resource owner (user)
 - Individual/entity controlling access to resources

Access Control Methods



Discretionary Access Control (DAC)

- Users directly “own” files/resources
 - Have full permissions to those resources
 - Can directly assign other users permissions
- Sally is manager of department
 - Owner of departmental folder
 - She assigns permissions for the rest of department
- Access Control Lists (ACLs)
 - Lists of “subjects” and level of authorization
- Used by majority of operating systems
- Risk of abuse
 - Any software run by user has full rights of that user
 - If user is admin, risk is significantly higher

Mandatory Access Control (MAC)

- Users do not have discretion to control access rights
- Much more secure than DAC
 - Often used on more sensitive systems, confidential data
- Built around using security labels/classifications
 - Users (subjects) are assigned a “clearance level”
 - Objects are assigned a security label or sensitivity level
 - Categories can also be used to further clarify, restrict
 - Used to enforce “need-to-know” rules
- Subjects only permitted access to objects at their clearance level or below

Role-Based Access Control (RBAC)

- Centrally administered manner of providing access
- Based around job duties and responsibilities
- Permissions are assigned to that role
- Users assigned directly to role
 - Permissions do not get assigned directly to individual identities
- Eases administration and management
- Roles can be “stacked” in hierarchies
 - Nurse role has access to “Nursing” folder
 - X-Ray Tech role has access to “Radiology” folder
 - Physician role contains both Nursing & X-Ray roles
- Additional rules can be added to create RB-RBAC
 - Simple or complex conditions

Attribute-Based Access Control (ABAC)

- Very fine-grained access control model
- Access decisions based on combination of subject/object attributes
 - Can include context-sensitive and system-wide attributes
 - Operating system being used
 - IP address of subject
 - Up to date patches and EDR software
- Capable of monitoring number and severity of alerts for user/device
- Can track requests to ensure time and geographic location allowed

Rule-Based Access Control

- Access control model where policies determined by system-enforced rules
 - Blanket term to apply to any similar model
 - RBAC, ABAC, MAC are examples of rule-based access control
- Conditional access
 - Can monitor system behavior throughout session
 - If certain conditions met, actions can be taken
 - Login permitted or not based on location
 - Account suspended if “impossible travel” login suspected
 - MFA required when accessing more sensitive data

Restrictions

- Additional methods to mitigate risk of account compromise
- Location-based policies
 - Restrict logins based on physical or logical location
 - Physical location determined by GPS/IPS
 - Logical location by IP address
- Time-based restrictions
 - Time-of-day - specific times an account is authorized to login
 - Duration-based - maximum amount of time account can stay logged in
 - Impossible travel/risky login - tracks location of logins over time
 - Temporary permissions policy - removes account from role after predetermined period of time

Multifactor Authentication



Multi-Factor Authentication (MFA)

- Using 2 or more forms of authentication to verify identity
 - Usually password + another authentication method
- Hardware and software implementations
 - Physical tokens
 - Security keys
 - Smart cards
 - Application-based tokens (software)
 - SMS delivery
- Authentication factors
 - Something you know
 - Something you have
 - Something you are
 - Somewhere you are

Something You Know

- Knowledge-based authentication
- Most common authentication type
- Most vulnerable authentication type
- Passwords
- Passphrases
 - More complex than password
 - Can be complete sentences (depending on system)
- Cognitive password
 - Information used to verify identity
 - Usually in the form of questions

Something You Have

- Ownership-based authentication
- Most frequently physical token or access card
 - Can also be software on a smartphone
- OTP - One Time Password
 - Typically seen as a code displayed on device
 - Or delivered via SMS - insecure
- Smart cards/security keys/NFC/RFID
 - Work using cryptographic keys
 - Smart cards usually inserted into device
 - Security keys normally USB
 - NFC/RFID typically swiped/held near reader

Something You Are

- Biometric authentication
- More difficult & expensive to implement
 - Usually used for more sensitive data/systems
- Physiological
 - “What you are”
 - Fingerprint, palm scan, eye scan, facial scan, etc
- Behavioral
 - “What you do”
 - Signature analysis, typing dynamics
- Much more difficult to impersonate identity
 - Knowledge-based can be guessed or brute-forced
 - Ownership-based can be stolen

Somewhere You Are

- Location-based authentication
- Geographic location
 - IP-based location
 - Device location services
- IP address
 - Region of the country/world (not always accurate, easy to fake)
 - Specific network segment within organization
 - Wi-Fi or cabled
- Not used as primary authentication factor
 - Often used for continuous authentication, esp for remote access

MFA Implementations



Soft Authentication Token

- One time code generated and sent to user (supplicant)
 - SMS or email delivery
 - 2-step authentication, instead of MFA
- Application installed on smartphone
 - Can display a code to enter
 - Similar to physical token
- Can also prompt user to accept/refuse login attempt
 - Normally in the form of a notification
- Most convenient from end-user point of view
- **Can** be excellent combination of usability and security
 - Multiple breaches occur due to user accepting attempt they didn't initiate

Hard Authentication Token

- Hardware token that user possesses
 - Can generate or receive token to identify/authenticate user
- Three types of token generation
 - Certificate-based
 - User controls private key, generates unique signed token
 - IdP verifies signature with public key
 - One-time password (OTP)
 - Token generated using hash function
 - Shared secret and synchronized seed
 - Token can only be used once
 - Fast Identity Online (FIDO) Universal 2nd Factor (U2F)
 - Public/private key pair for each account, no shared secret
 - Private key locked to hardware device

Hardware Token Types

- Smart card
 - Certificate-based authentication
 - Stores user's cert, private key, and PIN
 - Physical card inserted into/next to reader
- OTP
 - Generates token that user reads and enters
 - Does not interface with computer/device
- Security key
 - Portable HSM (hardware security module)
 - USB/NFC
 - Can support U2F or certificate-based
 - Must be “activated” when using

Biometric

- Enrollment
 - Sensor module acquires sample (fingerprint, iris, palmscan, etc)
 - Template created based on sample
- When authenticating, user is re-scanned and compared to template
- False rejection rate (FRR) - % measurement where user is not recognized
 - Prevents legitimate user from accessing resource
- False acceptance rate (FAR) - % measurement where non-auth allowed
 - Can lead to security breach
- Crossover error rate (CER) - where FRR and FAR meet
 - Lower number indicates more efficiency and reliability

Passwords



Common Terms

- Password length
 - Requirement for minimum and/or maximum # of characters
- Complexity
 - Specific character requirements (A, a, 1, !)
 - May also include other requirements (no username, char combos, etc)
- Password reuse
 - Using the same password for multiple services
 - *Or using same password that was recently used (password history)
 - Increases risk for credential stuffing attacks
- Expiration (also called password aging)
 - Requiring password change after period of time

Password Managers

- Applications that allow for secure password storage
- Recommended to use different password for every system/site
- Password vault is secured with “master password”
- Allow randomly generated passwords
 - Much harder to crack than ones based off words
- Vaults must be secured and encrypted
 - Centrally managed policies for PW manager applications
- Still some risk that passwords can be compromised
- Various vendors
 - Some offer enterprise options of software
 - Others are consumer level, but with enterprise support

Passwordless Authentication

- Eliminates the use of “something you know” authentication
- Uses roaming authenticator or platform authenticator
 - Security key (YubiKey)
 - Platform (Windows Hello, Face ID/Touch ID, etc)
- User configures method/gesture to confirm presence and authenticate
 - Fingerprint, face recognition, etc (validated by local authenticator)
- User registers with app/service (relying party)
 - Each service uses unique key pair
- When logging in, user performs previously configured method to unlock
- Relying party uses public key to verify signature and authenticate
- Attestation - device proves it is root of trust
 - Every key manufactured with attestation and model ID

Privileged Access Management



Privileged Access Management

- Accounts with elevated access are always needed
 - Shared accounts, service, root accounts, etc
 - Accounts not owned/used by one specific person
- Compromise on these accounts can have greater impact to org
- PAM - policies, procedures, and technical controls
 - Provide visibility into privileged accounts and their use
- Commonly used with other controls
 - MFA
 - Administrative workstation (jump box)

Just-In-Time (JIT) Access

- Methods to provision elevated access on-demand
 - Also known as zero standing privilege
- Three primary models
 - Temporary elevation
 - Admin permissions assigned for limited period of time
 - UAC in Windows; sudo in Linux
 - Password vaulting (brokering)
 - Process of “checking out” account for temporary use
 - Provides automation, documentation, accounting
 - Ephemeral credentials
 - System generates/enables account with/for admin access
 - Account deleted/access disabled once task completed

Automation & Scripting



Automation Purposes

- Multiple uses for automation
 - Streamline processes
 - Security controls
 - Efficiency improvement
 - Governance and change management processes
- Enables consistent & efficient security policy enforcement
- Monitoring and reporting benefits
 - Risk managers, senior leadership, system owners/administrators
- Assists with reducing human error and reducing time spent

Capabilities of Automation

- User and system/resource provisioning & deprovisioning
 - Create, modify, delete user accounts
 - Add, remove, audit account permissions
 - Deploy & manage resources
 - Servers, storage, network resources, etc
- Guardrails
 - Assist with monitoring and enforcing security compliance
 - Can monitor and flag risky behavior (or prevent)
- Security groups
 - Determines what resources users & systems can access
 - Manage based on job role and least privilege

Capabilities of Automation

- Ticketing platforms
 - Automatic generation of tickets from monitoring systems
 - Ticket routing based on predetermined rules
 - Automated escalation procedures
 - High priority incidents
 - SLA violations
- Service management
 - Enabling/disabling services on systems
 - Modify access rights based on needs

Capabilities of Automation

- Continuous integration and testing
 - Automatic verification and testing of code changes in development process
 - Can detect (possibly correct) integration errors
 - Improves quality of code and speeds up dev cycles
- APIs (Application Programming Interfaces)
 - Allows different software systems to communicate with each other
 - Automate workflows and integration in complex systems
 - SOAR - Security Orchestration, Automation, and Response

Automation Benefits and Considerations



Benefits

- Enhanced efficiency & time saving
 - Reduce need for manual repetitive tasks
 - Minimizes the occurrence of human error
 - “Workforce multiplier” - increase in productivity, more tasks in same time
 - Helps to reduce “operator fatigue”
- Improved detection and reaction times
 - If threat detected, automatic isolation, analysis/reporting, alerting, ticket generation, documentation, etc
- Enforcement of standardized baselines
 - Automatic configuration deployment to systems
 - Unauthorized changes automatically rolled back
- Automatic system deployment and scaling

Considerations

- Complexity
 - Requires thorough understanding and integration with org infrastructure
 - If poorly planned/implemented, can increase work required
- Cost
 - Initial cost of implementing is often high
 - Acquisition/development, sys integrations, training; licensing & maintenance
- Single point of failure
 - If automation system fails, large impact in multiple workflows/systems
- Technical debt due to improper implementation
 - Poor documentation, unstable integrations
 - Can lead to instability, increased costs, downtime, etc
- Ongoing support
 - Updates, patches, process improvement, training, etc

Incident Response Process



Incident Response

- Incident - attempted or successful attempt to compromise environment
 - Confidentiality, integrity, or availability
- Processes, resources, guidelines for dealing with incidents
- Incident response lifecycle
 - Preparation
 - Detection
 - Analysis
 - Containment
 - Eradication
 - Recovery
 - Lessons learned

Preparation

- Establish infrastructure that supports entire process
 - Incident detection - collection & analysis of logs, traffic, systems
 - Digital forensics - acquire and process data (memory, files, etc)
 - Case management - log incident details and coordinate response
 - Often in one software suite (SIEM and SOAR)
- Incident response team (CIRT, CERT, or CSIRT)
 - Led by senior executive to authorize actions
 - Managers to ensure day to day operations and coordinate response
 - Analysis and technicians
 - Legal, HR, PR

Preparation

- Communication plan
 - Clear lines of communication established **before** incidents
 - Often uses predefined call lists
 - Reporting information, notify affected parties
 - Prevent unintentional release of information (need-to-know only)
 - To public and to adversaries
 - Out of band communication (not tied to compromised infrastructure)
- Stakeholder management
 - Ensure those with privileged info do not disclose without authorization
 - Reporting obligations
- Incident response plan (IRP)
 - Formal list of procedures, contacts, resources, etc for various incident types

Detection

- Event correlation and analysis to determine evidence of incident
- Multiple methods to determine
 - Match event logs, errors, alerts, etc to known threat patterns
 - Deviations from baselines
 - Threat hunting - proactive inspection to search for evidence of compromise
 - Employee, customer, vendor notification
- Upon detection (or suspicion) of malicious event
 - Proper notification to response team
 - All employees should know how to report

Incident Response Analysis and Recovery



Analysis

- Investigation to determine if actual incident or false positive
 - If incident, priority assigned with escalation if required
- Identify type of incident and affected resources
 - Establishes category of incident and priority
- Data integrity - what data is at risk
- Downtime - business process disruptions
 - Degrade or interrupt completely
- Economic - evaluate effects in both short term and long term
- Scope - number/type of systems affected
- Detection time - amount of time between intrusion and detection
- Recovery time - longer times pose greater risk of more incidents

Analysis

- Threat intelligence required for effective analysis
 - Adversary TTP (tactics, techniques, and procedures)
- Cyber kill chain
 - Stages of attack (originally developed by Lockheed Martin)
 - Reconnaissance
 - Weaponization
 - Delivery
 - Exploitation
 - Installation
 - Command and Control (C2)
 - Actions on Objectives
- Playbooks to assist analysis with detection and analysis

Containment

- No standard approach - depends on situation
 - What has already happened as a result of incident?
 - What additional damage could occur in what timeframe?
 - What countermeasures are available?
 - What actions could alert adversary attack has been detected?
 - What evidence needs to be collected and preserved?
 - What notification or reporting is required
- Isolation-based containment
 - Remove affected device(s)/system(s) from environment
 - Device, server, subnet, user/service account
- Segmentation-based containment
 - Isolation, using network architecture (VLANs, ACLs, etc)

Eradication and Recovery

- Apply mitigations and other controls to remove intrusion
 - Completely dependent on environment and type of incident
- Restore any affected systems to remove any traces of incident
 - Intrusion tools, unauthorized changes, backdoors, malware, etc
 - Systems reconfigured to pre-incident state
 - Rebuild/reinstall if unable to restore
- Restore/recreate any affected accounts (changing passwords)
- Audit all security controls
 - Ensure not vulnerable to another attack
 - Same attack or new attack launched from gathered information
- Notify all affected parties, providing instructions to remediate if needed

Lessons Learned

- Review incident to determine cause, whether avoidable, how to avoid
- Typically involves meeting with all personnel involved in IR
 - Directly involved staff, other not directly involved
 - Focus on improving process, not assigning blame
- Lessons learned report (or after-action report)
 - RCA - root cause analysis: How was incident able to occur?
- Multiple approaches to determining root cause
 - Most involve asking questions about incident to determine causes
 - How was database copied without being alerted?
 - What systems were affected and what controls were involved?
 - Step through incident timeline to understand events, details, decisions

Incident Response Training & Testing



Training

- Incident detection training and reporting procedures
 - Enables responders to act quickly and effectively
- Incident response typically involves multiple teams/departments
 - Cross-training on IR plans is critical
- Lesson learned phase often shows opportunities for additional training
 - Security awareness or compliance training for users
 - Response training for analysis
- All training should not be technical in nature
 - IR activities are frequently stressful

Tabletop Exercises

- Training involving scenarios
 - Facilitator and responders
- Facilitator presents scenario, responders react to situation
 - Explain actions they would take to identify, contain, eradicate, etc
- Normally does not use computer systems
 - Can be used to consult documentation, look up information
 - Used more for simulation exercises
- One of least costly types of testing/training
 - Time for those involved

Simulations

- In contrast to tabletop, more expensive to implement
 - Requires use of computer systems, in depth scenarios and planning
- Typically team-based exercise
- Red team
 - Attempts intrusion using various methods
 - Similar to pen test
- Blue team
 - Responds to alerts/incident as red team is performing intrusion
 - Response and recovery activities
- Management (or other) team moderates and evaluates
 - Sometimes referred to as white team

Digital Forensics



Digital Forensics

- Collecting evidence from computer systems
 - Meets standards to be used in court of law
 - Standards and requirements may vary by location
- Due process
 - Set of procedures to ensure fairness
 - In US/UK - people only convicted of crimes using fair application of laws
- Legal hold
 - Any information has potential to be useful or relevant
 - Data/systems under legal hold must be preserved
 - Regulations, industry standards dictate some legal hold criteria
 - May also originate from law enforcement or attorneys

Chain of Custody

- Documentation that verifies integrity and proper handling of evidence
- Designed to protect organization
 - Accusations of tampering or mishandling of evidence
- Maintained and updated throughout entire process
 - Collection, analysis, storage, presentation, disposal, etc
- Requires every individual in process to log what, when, how
 - Evidence collected
 - Time/date of collection
 - Tools and methods used

Acquisition

- Processes to obtain “forensically clean” data
 - Requires that data can be legally seized/searched (BYOD)
 - Performed using various specialized tools
- Some evidence cannot be obtained if system is powered off
 - Other evidence cannot be obtained **until** system is powered off
- Order of volatility
 - CPU registers & cache memory
 - Non-persistent memory, routing tables, ARP cache, etc
 - Data on persistent storage (HDD, SSD, flash memory)
 - Remote logging and monitoring data
 - Physical configuration/topology
 - Archive media, printed documents

E-Discovery

- Filtering all data collected to find relevant evidence
- Data is securely stored in way that can be used as evidence
 - Chain of custody required
- Most of process is automated using various software tools
 - Identify file types and deduplicate data
 - Identify and sort metadata
 - Allows various search criteria to locate relevant data
 - Tags and keywords applied to discovered evidence for organization
 - Security to ensure integrity of evidence
 - Disclosure for other parties if needed

Maintaining Data

- Evidence preservation
 - Maintained throughout collection/acquisition processes
 - Access to evidence tightly controlled
 - Provenance - tracing source of evidence, showing no tampering
 - Write blocker used while collecting data
- Integrity & non-repudiation
 - Cryptographic hash of media is created
 - Bit-by-bit copy of data using imaging utility
 - Second hash performed - should match first
 - Second copy performed, matching hash, analysis performed on this copy

Reporting

- Summary of data collected and conclusions from analysis
- Report requires strong ethical principles
 - No bias - conclusions/opinions only from direct evidence
 - All analysis must be repeatable by third parties
 - Evidence must not be changed or manipulated
- Device may need to be manipulated to perform analysis
 - Disable lock feature on phone
 - Prevent remote wipe on phone
 - Reasons must be sound, documented, with process recorded

Log Data



Data Sources & Dashboards

- Incident response requires data sources to discover indicators
 - Logs files, error messages, firewall/IPS alerts
 - OS, endpoint, applications, security software, etc
 - Captured network traffic
 - Memory and file system data/metadata
- SIEM tools used to aggregate and correlate data from multiple sources
 - Alerts that detect threat indicators
 - Status reports - level of threats, # of incidents, etc
- Event dashboards
 - Starting console for day-to-day incident response
 - Summary of information from data sources
 - Visualizations, uncategorized alerts, etc

Operating System Logs

- Windows
 - Application logs - generated by app processes, crashes, installs, removals
 - Security - audit events (failed/successful logins, access allowed/denied)
 - Systems - generated by kernel processes (service startup, shutdown)
- Linux
 - Logging differs by distribution (some syslog, Journald)
 - /var/log/messages, /var/log/syslog - system events
 - /var/log/auth.log, /var/log/secure - login attempts, sudo usage
- MacOS
 - Unified logging system, accessible through Console app or “log” command

Application & Endpoint Logs

- Application logs - generated by application rather than OS
 - Can use Event viewer (Windows), syslog, flat files, internal to app
- Endpoint logs - typically generated by endpoint security software
 - Host-based firewalls, IDS
 - Vulnerability scanners
 - AV/EDR software
- Summary of events can show overall security/threat level
 - Quantity of malware detected, # of intrusion events, hosts missing patches
- Vulnerability scans
 - Can send information to SIEM (in addition to vuln report)
 - Missing patch information, baseline compliance issues
 - Accuracy depends on date of last scan

Network Logs

- Events generated by switches, routers, firewalls, etc
 - Information about device operation/status
 - Traffic and access logs
- Firewall logs
 - Data about firewall rule activity (connection allowed/blocked)
 - Can result in large number of logs
 - Date/time, interface, in/outbound traffic, source/destination IPs/ports
- IPS/IDS logs generated when traffic matches rules
 - Rule matched, packet info, action taken by IPS
- Packet capture used to analyze frame-by-frame information of traffic
 - Wireshark commonly used
 - Provides in-depth inspection of network data
 - All traffic not typically captured, only traffic that triggers rules

Metadata

- Properties about data/logs (data about the data)
- File
 - Creation, access, modification information (when, who, where)
 - Information can depend on file format (Word doc, image, etc)
- Web
 - Request/response properties and header information
 - Authorization & cookie information
 - Data may also be logged by web servers
- Email
 - All header information (sender, recipient, user/delivery agent)
 - SPF/DKIM/DMARC info, spam filtering
 - All information can be viewed in most email clients (not by default)

EXPERTS AT MAKING YOU AN EXPERT

