17- Performing Incident Response

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

17.1- Summarize Incident Response Procedures

17.2- Utilize Appropriate Data Sources for Incident Response

17.3- Apply Mitigation Controls

Labs

Lab 24: Managing Data Sources for Incident Response

Lab 25: Configuring Mitigation Controls

17.1- Summarize Incident Response Procedures

17.2- Utilize Appropriate Data Sources for Incident Response

17.3- Apply Mitigation Controls

INCIDENT RESPONSE PROCESS

- Incident response policy sets the resources, processes, and guidelines for dealing with security incidents.
- Incident management is vital to mitigating risk.
- As well as controlling the immediate or specific threat to security, effective incident management preserves an organization's reputation.
- Incident response follows a well-structured process, such as that set out in the NIST Computer Security Incident Handling Guide special publication (nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf).

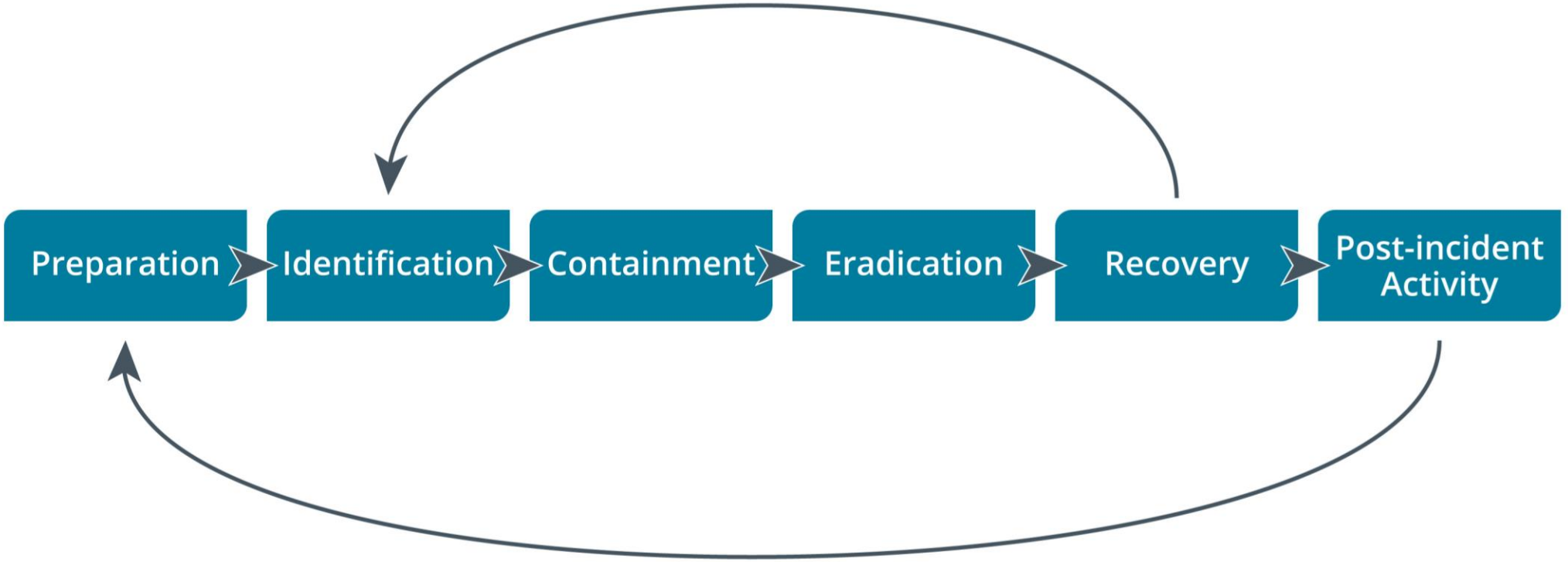
INCIDENT RESPONSE PROCESS (cont.)

- The following are the principal stages in an incident response life cycle:
  - ✓ Preparation—make the system resilient to attack in the first place, This includes hardening systems, writing policies and procedures, and setting up confidential lines of communication, It also implies creating incident response resources and procedures.
  - ✓ Identification—from the information in an alert or report, determine whether an incident has taken place, assess how severe it might be (triage), and notify stakeholders.
  - ✓ Containment—limit the scope and magnitude of the incident, The principal aim of incident response is to secure data while limiting the immediate impact on customers and business partners.
  - ✓ Eradication—once the incident is contained, remove the cause and restore the affected system to a secure state by applying secure configuration settings and installing patches.

INCIDENT RESPONSE PROCESS (cont.)

- The following are the principal stages in an incident response life cycle (cont.)
  - ✓ Recovery—with the cause of the incident eradicated, the system can be reintegrated into the business process that it supports, This recovery phase may involve restoration of data from backup and security testing, Systems must be monitored more closely for a period to detect and prevent any reoccurrence of the attack, The response process may have to iterate through multiple phases of identification, containment, eradication, and recovery to effect a complete resolution.
  - ✓ Lessons learned—analyze the incident and responses to identify whether procedures or systems could be improved, It is imperative to document the incident, The outputs from this phase feed back into a new preparation phase in the cycle.

INCIDENT RESPONSE PROCESS (cont.)



CYBER INCIDENT RESPONSE TEAM

- Preparing for incident response means establishing the policies and procedures for dealing with security breaches and the personnel and resources to implement those policies.
- One of the first challenges lies in defining and categorizing types of incidents.
- An incident is generally described as an event where security is breached or there is an attempted breach.
- NIST describes an incident as "the act of violating an explicit or implied security policy."
- In order to identify and manage incidents, you should develop some method of reporting, categorizing, and prioritizing them (triage), in the same way that troubleshooting support incidents can be logged and managed.

CYBER INCIDENT RESPONSE TEAM (cont.)

- As well as investment in appropriate detection and analysis software, incident response requires expert staffing.
- This team is variously described as a
  - ✓ Cyber Incident Response Team (CIRT) or
  - ✓ Computer Security Incident Response Team (CSIRT) or
  - ✓ Computer Emergency Response Team (CERT).
- Incident response might also involve or be wholly located within a security operations center (SOC).

INCIDENT RESPONSE PLAN

- An incident response plan (IRP) lists the procedures, contacts, and resources available to responders for various incident categories.
- The CSIRT should develop profiles or scenarios of typical incidents (DDoS attack, virus/worm outbreak, data exfiltration by an external adversary, data modification by an internal adversary, and so on).
- This will guide investigators in determining priorities and remediation plans.
- A playbook (or runbook) is a data-driven standard operating procedure (SOP) to assist junior analysts in detecting and responding to specific cyberthreat scenarios, such as phishing attempts, SQL injection data exfiltration, connection to a block-listed IP range, and so on.
- The playbook starts with a SIEM report and query designed to detect the incident and identify the key detection, containment, and eradication steps to take.

CYBER KILL CHAIN ATTACK FRAMEWORK

- Effective incident response depends on threat intelligence.
- Threat research provides insight into adversary tactics, techniques, and procedures (TTPs).
- Insights from threat research can be used to develop specific tools and playbooks to deal with event scenarios.
- A key tool for threat research is a framework to use to describe the stages of an attack.
- These stages are often referred to as a Cyber Kill Chain.

CYBER KILL CHAIN ATTACK FRAMEWORK (cont.)

CYBER KILL CHAIN ATTACK FRAMEWORK (cont.)

1. Reconnaissance—in this stage the attacker determines what methods to use to complete the phases of the attack and gathers information about the target's personnel, computer systems, and supply chain.
2. Weaponization—the attacker couples payload code that will enable access with exploit code that will use a vulnerability to execute on the target system.
3. Delivery—the attacker identifies a vector by which to transmit the weaponized code to the target environment, such as via an email attachment or on a USB drive.
4. Exploitation—the weaponized code is executed on the target system by this mechanism, **For example**, a phishing email may trick the user into running the code, while a drive-by-download would execute on a vulnerable system without user intervention.

CYBER KILL CHAIN ATTACK FRAMEWORK (cont.)

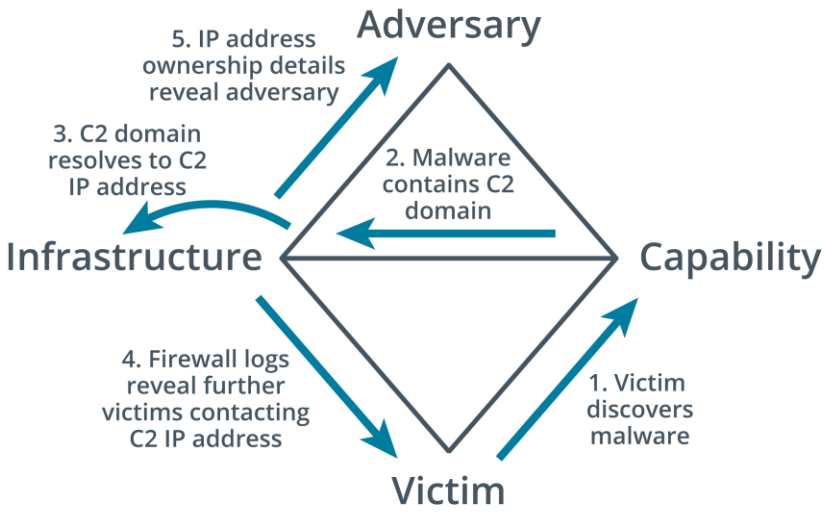
5. Installation—this mechanism enables the weaponized code to run a remote access tool and achieve persistence on the target system.
6. Command and control (C2 or C&C)—the weaponized code establishes an outbound channel to a remote server that can then be used to control the remote access tool and possibly download additional tools to progress the attack.
7. Actions on objectives—in this phase, the attacker typically uses the access he has achieved to covertly collect information from target systems and transfer it to a remote system (data exfiltration), An attacker may have other goals or motives, however.

OTHER ATTACK FRAMEWORKS

- MITRE ATT&CK
  - ✓ The MITRE Corporation's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) matrices provide access to a database of known TTPs.
  - ✓ This freely available resource (attack.mitre.org) tags each technique with a unique ID and places it in one or more tactic categories, such as initial access, persistence, lateral movement, or command and control.
  - ✓ The sequence in which attackers may deploy any given tactic category is not made explicit.

OTHER ATTACK FRAMEWORKS (cont.)

- The Diamond Model of Intrusion Analysis
  - ✓ The Diamond Model of Intrusion Analysis suggests a framework to analyze an intrusion event (E) by exploring the relationships between four core features: **adversary**, **capability**, **infrastructure**, and **victim**.
  - ✓ These four features are represented by the four vertices of a diamond shape.



17.1- Summarize Incident Response Procedures

17.2- Utilize Appropriate Data Sources for Incident Response

17.3- Apply Mitigation Controls

INCIDENT IDENTIFICATION

- Identification
  - ✓ is the process of collating events and determining whether any of them should be managed as incidents.

- First Responder
  - ✓ When a suspicious event is detected, it is critical that the appropriate person on the CIRT be notified so that they can take charge of the situation and formulate the appropriate response.
  - ✓ This person is referred to as the first responder.
  - ✓ This means that employees at all levels of the organization must be trained to recognize and respond appropriately to actual or suspected security incidents.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

- Coupled with an attack framework, notification will provide a general sense of where to look for or expect indicators of malicious activity.
- Incident analysis is greatly facilitated by a security information and event management (SIEM) system.
- A SIEM parses network traffic and log data from multiple sensors, appliances, and hosts and normalizes the information to standard field types.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) (cont.)

- Correlation
  - ✓ The SIEM can then run correlation rules on indicators extracted from the data sources to detect events that should be investigated as potential incidents.
  - ✓ You can also filter or query the data based on the type of incident that has been reported.
  - ✓ **Correlation** means interpreting the relationship between individual data points to diagnose incidents of significance to the security team.
  - ✓ A **SIEM** correlation rule is a statement that matches certain conditions.
  - ✓ These rules use logical expressions, such as **AND** and **OR**, and operators, such as **==** (matches), **<** (less than), **>** (greater than), and **in** (contains).

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) (cont.)

- Correlation (cont.)
  - ✓ **For Example**, a single-user logon failure is not a condition that should raise an alert.
  - ✓ Multiple user logon failures for the same account, taking place within the space of one hour, is more likely to require investigation and is a candidate for detection by a correlation rule.

```
Error.LogonFailure > 3 AND LogonFailure.User AND Duration < 1 hour
```

  - ✓ As well as correlation between indicators observed on the network, a **SIEM** is likely to be configured with a threat intelligence feed.
  - ✓ This means that data points observed on the network can be associated with known threat actor indicators, such as IP addresses and domain names.
  - ✓ AI-assisted analysis enables more sophisticated alerting and detection of anomalous behavior.

SIEM DASHBOARDS

- **SIEM** dashboards are one of the main sources of automated alerts.
- A SIEM dashboard provides a console to work from for day-to-day incident response.
- Separate dashboards can be created to suit many different purposes.
- An incident handler's dashboard will contain uncategorized events that have been assigned to their account, plus visualizations (graphs and tables) showing key status metrics.
- A manager's dashboard would show overall status indicators, such as number of unclassified events for all event handlers.

LOGGING PLATFORMS

- Log data from network appliances and hosts can be aggregated by a **SIEM** either by installing a local agent to collect and parse the log data or by using a forwarding system to transmit logs directly to the SIEM server.
- Also, organizations may not operate a SIEM, but still use a logging platform to aggregate log data in a central location.
- Syslog
  - ✓ Syslog provides an open format, protocol, and server software for logging event messages.
  - ✓ It is used by a very wide range of host types.
  - ✓ **For Example**, syslog messages can be generated by Cisco routers and switches, as well as servers and workstations.
  - ✓ It usually uses UDP port 514.

LOGGING PLATFORMS (cont.)

- journalctl
  - ✓ In Linux, text-based log files of the sort managed by syslog can be viewed using commands such as **cat**, **tail**, and **head**.
  - ✓ Most modern Linux distributions now use systemd to initialize the system and to start and manage background services.
  - ✓ Rather than writing events to syslog-format text files, logs from processes managed by systemd are written to a binary-format file called **journald**.
  - ✓ Events captured by journald can be forwarded to syslog.
- NXlog
  - ✓ NXlog (nxlog.co) is an open-source log normalization tool.
  - ✓ One principal use for it is to collect Windows logs, which use an XML-based format, and normalize them to a syslog format.

NETWORK, OS, AND SECURITY LOG FILES

- System and Security Logs
  - ✓ One source of security information is the event log from each network server or client.
  - ✓ Systems such as **Microsoft Windows**, **Apple macOS**, and **Linux** keep a variety of logs to record events as users and software interact with the system.
  - ✓ The format of the logs varies depending on the system.
  - ✓ Information contained within the logs also varies by system, and in many cases, the type of information that is captured can be configured.
  - ✓ When events are generated, they are placed into log categories. These categories describe the general nature of the events or what areas of the OS they affect.

NETWORK, OS, AND SECURITY LOG FILES (cont.)

- System and Security Logs (cont.)
  - ✓The five main categories of **Windows event logs** are:
    - Application—events generated by applications and services, such as when a service cannot start.
    - Security—Audit events, such as a failed logon or access to a file being denied.
    - System—events generated by the operating system and its services, such as storage volume health checks.
    - Setup—events generated during the installation of Windows.
    - Forwarded Events—events that are sent to the local log from other hosts.

NETWORK, OS, AND SECURITY LOG FILES (cont.)

- Network Logs
  - ✓ Network logs are generated by appliances such as **routers**, **firewalls**, **switches**, and **access points**.
  - ✓ Log files will record the operation and status of the appliance itself—the system log for the appliance—plus traffic and access logs recording network behavior, such as a host trying to use a port that is blocked by the firewall, or an endpoint trying to use multiple MAC addresses when connected to a switch.

- Authentication Logs
  - ✓ Authentication attempts for each host are likely to be written to the security log.
  - ✓ You might also need to inspect logs from the servers authorizing logons, such as **RADIUS** and **TACACS+** servers or **Windows Active Directory (AD) servers**.

NETWORK, OS, AND SECURITY LOG FILES (cont.)

- Vulnerability Scan Output
  - ✓ A vulnerability scan report is another important source when determining how an attack might have been made.
  - ✓ The scan engine might log or alert when a scan report contains vulnerabilities.
  - ✓ The report can be analyzed to identify vulnerabilities that have not been patched or configuration weaknesses that have not been remediated.
  - ✓ These can be correlated to recently developed exploits.

APPLICATION LOG FILES

- DNS Event Logs
  - ✓ A DNS server may log an event each time it handles a request to convert between a domain name and an IP address.
  - ✓ DNS event logs can hold a variety of information that may supply useful security intelligence, such as:
    - The types of queries a host has made to DNS.
    - Hosts that are in communication with suspicious IP address ranges or domains.
    - Statistical anomalies such as spikes or consistently large numbers of DNS lookup failures, which may point to computers that are infected with malware, misconfigured, or running obsolete or faulty applications.

APPLICATION LOG FILES (cont.)

- Web/HTTP Access Logs
  - ✓ Web servers are typically configured to log HTTP traffic that encounters an error or traffic that matches some predefined rule set.
  - ✓ The status code of a response can reveal quite a bit about both the request and the server's behavior.
  - ✓ Codes in the **400** range indicate client-based errors, while codes in the **500** range indicate server-based errors.
  - ✓ **For Example**, repeated 403 ("Forbidden") responses may indicate that the server is rejecting a client's attempts to access resources they are not authorized to.
  - ✓ A 502 ("Bad Gateway") response could indicate that communications between the target server and its upstream server are being blocked, or that the upstream server is down.

Lab

Lab 24: Managing Data Sources for Incident Response

17.1- Summarize Incident Response Procedures

17.2- Utilize Appropriate Data Sources for Incident Response

17.3- Apply Mitigation Controls

INCIDENT CONTAINMENT

- Containment techniques can be classed as either isolation-based or segmentation-based.

1. Isolation-Based Containment

- ✓ Isolation involves removing an affected component from whatever larger environment it is a part of.
- ✓ This can be everything from removing a server from the network after it has been the target of a DoS attack, to placing an application in a sandbox VM outside of the host environments it usually runs on.
- ✓ Whatever the circumstances may be, you'll want to make sure that there is no longer an interface between the affected component and your production network or the Internet.

INCIDENT CONTAINMENT (cont.)

1. Isolation-Based Containment (cont.)

- ✓ A simple option is to disconnect the host from the network completely, either by pulling the network plug (creating an air gap) or disabling its switch port.
- ✓ This is the least stealthy option and will reduce opportunities to analyze the attack or malware.
- ✓ If a group of hosts is affected, you could use routing infrastructure to isolate one or more infected virtual LANs (VLANs) in a black hole that is not reachable from the rest of the network.
- ✓ Another possibility is to use firewalls or other security filters to prevent infected hosts from communicating.

INCIDENT CONTAINMENT (cont.)

1. Isolation-Based Containment (cont.)

- ✓ Finally, isolation could also refer to disabling a user account or application service.
- ✓ Temporarily disabling users' network accounts may prove helpful in containing damage if an intruder is detected within the network.
- ✓ Without privileges to access resources, an intruder will not be able to further damage or steal information from the organization.
- ✓ Applications that you suspect may be the vector of an attack can be much less effective to the attacker if the application is prevented from executing on most hosts.

INCIDENT CONTAINMENT (cont.)

2. Segmentation-Based Containment

- ✓ Segmentation-based containment is a means of achieving the isolation of a host or group of hosts using network technologies and architecture.
- ✓ Segmentation uses **VLANs**, **routing/subnets**, and **firewall ACLs** to prevent a host or group of hosts from communicating outside the protected segment.
- ✓ As opposed to completely isolating the hosts, you might configure the protected segment as a sinkhole or honeynet and allow the attacker to continue to receive filtered (and possibly modified) output over the C&C channel to deceive him or her into thinking the attack is progressing successfully.
- ✓ Analysis of the malware code by reverse engineering it could provide powerful deception capabilities.

INCIDENT ERADICATION AND RECOVERY

- After an incident has been contained, you can apply mitigation techniques and controls to eradicate the intrusion tools and unauthorized configuration changes from your systems.
- Eradicating malware, backdoors, and compromised accounts from individual hosts is not the last step in incident response.
- You should also consider a recovery phase where the goal is restoration of capabilities and services.
- This means that hosts are fully reconfigured to operate the business workflow they were performing before the incident.
- An essential part of recovery is the process of ensuring that the system cannot be compromised through the same attack vector (or failing that, that the vector is closely monitored to provide advance warning of another attack).

INCIDENT ERADICATION AND RECOVERY (cont.)

- Eradication of malware or other intrusion mechanisms and recovery from the attack will involve several steps:
  - ✓ Reconstitution of affected systems—either remove the malicious files or tools from affected systems or restore the systems from secure backups/images.
  - ✓ Reaudit security controls—ensure they are not vulnerable to another attack, This could be the same attack or from some new attack that the attacker could launch through information they have gained about your network.
  - ✓ Ensure that affected parties are notified and provided with the means to remediate their own systems, **For Example**, if customers' passwords are stolen, they should be advised to change the credentials for any other accounts where that password might have been used (not good practice, but most people do it).

FIREWALL CONFIGURATION CHANGES

- Analysis of an attack should identify the vector exploited by the attacker.
- This analysis is used to identify configuration changes that block that attack vector.
- A configuration change may mean the deployment of a new type of security control, or altering the settings of an existing control to make it more effective.
- Historically, many organizations focused on ingress filtering rules, designed to prevent local network penetration from the Internet.
- In the current threat landscape, it is imperative to also apply strict egress filtering rules to prevent malware that has infected internal hosts by other means from communicating out to C&C servers.

FIREWALL CONFIGURATION CHANGES (cont.)

- Some general guidelines for configuring egress filtering are:
  - ✓ Allow only authorized application ports and, if possible, restrict the destination addresses to authorized Internet hosts.
  - ✓ Restrict DNS lookups to your own or your ISP's DNS services or authorized public resolvers, such as Google's or Quad9's DNS services.
  - ✓ Block access to "known bad" IP address ranges.
  - ✓ Block access from any IP address space that is not authorized for use on your local network.
  - ✓ Block all Internet access from host subnets that do not need to connect to the Internet, such as most types of internal server, workstations used to manage industrial control systems (ICSs), and so on.

Lab

Lab 25: Configuring Mitigation Controls