Incident Handling Process (HTB)

▼ introduction

- **Incident handling** is a clearly defined set of **procedures** to **manage** and **respond** to security incidents in a computer or network environment.
- types of incidents
  - intrusion incidents
  - those caused by malicious insiders
  - availability issues
  - loss of intellectual property
- An `event` is an action occurring in a system or network. Examples of events are:
  - A user sending an email
  - A mouse click
  - A firewall allowing a connection request
- An `incident` is an event with a negative consequence.
  - Data theft
  - Funds theft
  - Unauthorized access to data
  - Installation and usage of malware and remote access tools

▼ Cyber Kill Chain (attack lifecycle)

(7) different stages

1. `recon` (information gathering)
   - Passive (Linkden / insta / job ads / partners / documentations)
   - Active (poking and scaning web apps , IP addresses..etc)
   - identify the present antivirus or EDR technology in the target organization.
2. `weaponize` (developing the malware to be used for initial access)
   - embed it into some type of exploit or deliverable payload

- This malware is crafted to be extremely lightweight and undetectable by the antivirus and detection tools.

3. `delivery` (delivering the exploit/payload to the victim)
   - Traditional approaches are phishing emails (contain a malicious attachment or a link to a web page)
     - The web page can either contain an **exploit** or **hosting** the malicious payload to **avoid sending it through email scanning tools**.
     - the web page can also mimic a legit website
     - social engineering **pretext**
   - there are cases where physical interaction is utilized to deliver the payload via USB tokens and similar storage tools, that are purposely left around.
4. `exploitation` (when an exploit or a delivered payload is triggered)
   - the attacker typically attempts to execute code on the target system in order to gain access or control
5. `installation` (the initial stager is executed and is running on the compromised machine.)
   - Some common techniques
     - **Droppers:** a small piece of code that is designed to install malware on the system and execute it. it may be delivered through email attachments, malicious websites, or social engineering tactics.
     - **Backdoors:** a type of malware that is designed to provide the attacker with ongoing access to the compromised system. (may be installed during the exploitation stage or delivered through a dropper.)
     - **Rootkits:** a type of malware that is designed to hide its presence on a compromised system. (used in the installation stage to evade detection by antivirus software)
6. `command and control` (the attacker establishes a remote access capability to the compromised machine.)
   - advanced groups will utilize separate tools in order to ensure that multiple variants of their malware live in a compromised network, and if one of them gets discovered and contained, they still have the means to return to the environment.
7. `action` (objective of the attack)
   - exfiltrating confidential data
   - obtain the highest level of access possible
   - deploy ransomware

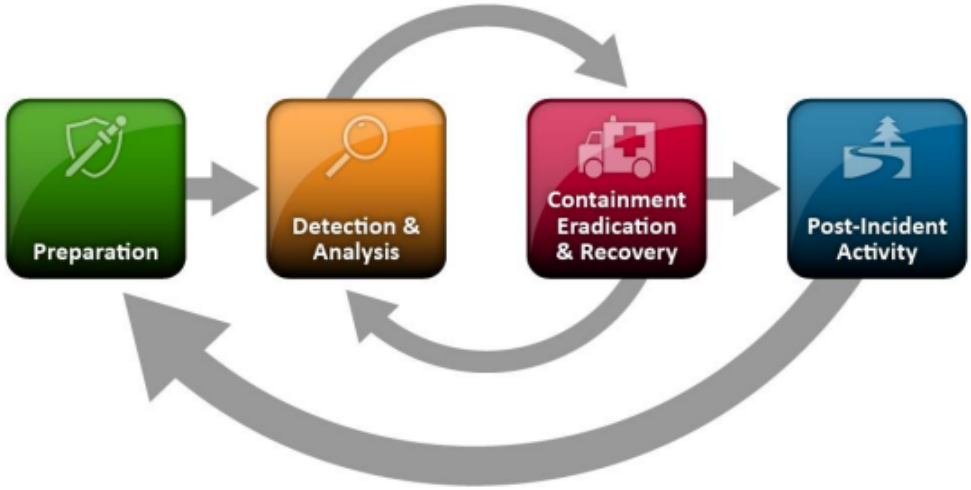
- ….etc

> It is important to understand that adversaries won't operate in a linear manner (like the cyber kill chain shows). Some previous cyber kill chain stages will be repeated over and over again. If we take, for example, the `installation` stage of a successful compromise, the logical next step for an adversary going forward is to initiate the `recon` stage again to identify additional targets and find vulnerabilities to exploit, so that he moves deeper into the network and eventually achieves the attack's objective(s).

- Our objective is to stop an attacker from progressing further up the kill chain, ideally in one of the earliest stages.

▼ Incident Handling Process Overview

- `incident handling process` defines a capability for organizations to prepare, detect, and respond to malicious events



- the process is not linear but cyclic.

Incident handling has two main activities:

- `investigating`
  - Discover the initial '**patient zero**' victim and create an (ongoing if still active) **incident timeline**
  - Determine what **tools** and **malware** the adversary used
  - **Document** the **compromised systems** and what the adversary **has done**

- `recovering`
  - creating and implementing a recovery plan
  - a report is issued that details the cause and cost of the incident.
  - Additionally, "lessons learned" activities are performed

Stages of the Incident Handling Process

1. Preparation

- we have two separate objectives
  1. the establishment of incident handling **capability** within the organization.
  2. the ability to protect against and prevent IT security incidents by **implementing** appropriate **protective measures, such as:**
     a. endpoint and server hardening
     b. active directory tiering
     c. multi-factor authentication
     d. privileged access management

Preparation Prerequisites

we need to ensure that we have:

1. Skilled incident handling team members
2. Trained workforce (through security awareness activities)
3. **Clear policies and documentation**
   - **roles** and **Contact info** of incident handling team members and all other teams
   - Incident response **policy**, **plan**, and **procedures**
   - **Network diagrams**
   - **Baselines** of systems and networks, out of a golden image and a clean state environment
   - Organization-wide **asset management database**
   - User accounts with **excessive privileges**
   - Ability to acquire hardware, software, or an external resource without a complete procurement process
   - Forensic/Investigative cheat sheets
4. **Tools (software and hardware)**

These include, but are not limited to:

- **Additional** forensic workstation for each incident handling team member to preserve disk images and log files, perform data analysis, and investigate without any restrictions
    - (malware will be tested here, so tools such as antivirus should be disabled)
- **Digital forensic image acquisition** and analysis tools
- **Memory capture** and analysis tools (volatility)
- **Live response capture and analysis**
- **Log analysis tools**
- **Network capture and analysis tools**
- Network **cables** and **switches**
- **Write blockers**
- **Hard drives for forensic imaging**
- **Power cables**
- **Screwdrivers**, **tweezers**, and other relevant tools to **repair** or **disassemble** hardware devices if needed
- **Indicator of Compromise** (IOC) creator and the ability to search for IOCs across the organization
    - An Indicator of Compromise (IOC) is a piece of evidence or artifact that suggests the presence of a security incident or compromise.
    - It can be a **file hash**, **IP address**, **domain name**, **URL**, **file name**, **registry key**, **network traffic pattern**, or **behavioral anomaly**.
    - IOCs are used to identify and detect malicious activities or intrusions in investigations.
- **Chain of custody forms**
- **Encryption software**
- **Ticket tracking system**
    - a software application or platform that helps organizations manage and track various types of requests, issues, or incidents reported by users or customers
- **Secure facility** for **storage** and **investigation**
- **Incident handling system independent** of your organization's infrastructure

- Many of the tools mentioned above will be part of what is known as a `jump bag` - always ready with the necessary tools to be picked up and leave immediately.

- **communications** about an incident should be conducted through channels that **are not part of the organization's systems**
    - assume that adversaries have control over everything and can read communication channels such as email.

Some of the highly recommended protective measures in Preparation

DMARC (email protection against phishing)

- to reject emails that 'pretend' to originate from your organization.
- **testing is mandatory**; otherwise you risk blocking legitimate emails with no ability to recover them.

Endpoint Hardening (& EDR)

- Endpoint devices (workstations, laptops, etc.) are the entry points for most of the attacks that we are facing on a daily basis
- There are a few widely recognized endpoint hardening standards such as **CIS** and **Microsoft baselines** and these should be the building blocks for your organization's hardening baselines.

Some highly important actions

- Disable **LLMNR/NetBIOS**
- Implement **LAPS** and remove **administrative privileges** from regular users
- **Disable** or **configure PowerShell** in "**ConstrainedLanguage**" mode
- Enable **Attack Surface Reduction** (ASR) rules if using Microsoft Defender
- Implement **whitelisting**.
    - Consider at least blocking **execution from user-writable** folders (Downloads, Desktop, AppData, etc.).
    - These are the locations where exploits and malicious payloads will initially find themselves.
    - Remember to also block script types such as .**hta**, .**vbs**, .**cmd**, .**bat**, .**js**, and similar. Please pay attention to **LOLBin** files while implementing whitelisting. they are used in the wild as **initial access** to **bypass whitelisting**.
- Utilize **host-based firewalls**. As a bare minimum, **block** **workstation-to-workstation communication** and **block** **outbound traffic to LOLBins**

> **Outbound** traffic refers to traffic that originates from inside your own network.

> **Inbound** traffic refers to any traffic coming to your network

- Deploy an **EDR product**. At this point in time, **AMSI** provides great visibility into obfuscated scripts for antimalware products to inspect the content before it gets executed. It is highly recommended that you only choose products that integrate with **AMSI**.

Network Protection

- Business-critical systems must be isolated
- connections should be allowed only as the business requires
- Internal resources should really not be facing the Internet directly (unless placed in a DMZ)
- consider IDS/IPS systems (Their power really shines when **SSL/TLS interception** is performed to identify malicious traffic based on content)
    - **SSL/TLS interception :**
        1. **Decryption and Inspection of the packets**
        2. **Re-encryption and Forwarding**
- ensure that only **organization-approved** devices can get on the network.
    - Solutions such as **802.1x (IEEE Standard for port-based network access control)** can be utilized to reduce the risk of bring your own device (**BYOD**) or malicious devices connecting to the corporate network
- If you are a **cloud-only** company using, for example, Azure/**Azure AD**, then you can achieve similar protection with **Conditional Access policies (allow access to organization resources only if you are connecting from a company-managed device)**

Privilege Identity Management / MFA / Passwords

- common mistake is that admin users either have a weak (but often complex) password "**Password1!**". It contains an upper-case, lower-case, digit, and a special character, but regardless of that, it is easy to guess. or a shared password with their regular user account (which can be obtained via multiple attack vectors such as **keylogging**)
- **Multi-factor authentication** (MFA) is another identity-protecting solution that should be implemented at least for any type of administrative access to **ALL** applications and devices.

Vulnerability Scanning

- Perform continuous vulnerability scans of your environment and remediate at least the "high" and "critical" vulnerabilities discovered.

User Awareness Training

- Training users to recognize suspicious behavior and report it when discovered
- Periodic "**surprise**" testing should also be part of this training, including, for example, monthly phishing emails, dropped USB sticks in the office building, etc.

Active Directory Security Assessment

- The best way to detect security misconfigurations or exposed critical vulnerabilities is by looking for them from the **perspective of an attacker.**

Purple Team Exercises

- Purple team exercises are essentially security assessments by a red team that either continuously or eventually inform the blue team about their actions, findings, any visibility/security shortcomings, etc.
- Such exercises will help in identifying vulnerabilities in an organization while testing the blue team's defensive capability in terms of logging, monitoring, detection, and responsiveness.

2. Detection & Analysis Stage

- this phase involves all aspects of detecting an incident, such as utilizing sensors, logs, and trained personnel. It also includes information and knowledge sharing, utilizing context-based threat intelligence.
- Segmentation of the architecture and having a clear understanding of and visibility within the network are also important factors.
- Threats are introduced to the organization via an infinite amount of attack vectors, and their detection can come from **sources** such as:
  - An **employee** that notices abnormal behavior
  - An **alert** from one of our **tools** (EDR, IDS, Firewall, SIEM, etc.)
  - **Threat hunting activities**
  - **A third-party notification** informing us that they discovered signs of our organization being compromised
- It is highly recommended to create **levels of detection** by logically categorizing our network as follows.
  - Detection at the **network perimeter** (using FWs, **internet-facing network** IDS/IPS, DMZ, etc.)
  - Detection at the **internal network level** (using local FWs, **host** IDS/IPS, etc.)
  - Detection at the **endpoint level** (using **antivirus systems**, **endpoint detection** & **response** systems, etc.)
  - Detection at the **application level** (using **application logs**, **service logs**, etc.)

Incident Severity & Extent Questions

→ When handling a security incident, we should also try to answer the following questions to get an idea of the incident's severity and exent:

1. What is the exploitation impact?
2. What are the exploitation requirements?
3. Can any business-critical systems be affected by the incident?
4. Are there any suggested remediation steps?
5. How many systems have been impacted?
6. Is the exploit being used in the wild?
7. Does the exploit have any worm-like capabilities?

→ As you can imagine, high-impact incidents will be handled promptly, and incidents with a high number of impacted systems will have to be escalated.

Incident Confidentiality & Communication

→ all of the information gathered should be kept on a **need-to-know basis**, unless applicable **laws** or a **management decision** instruct us otherwise. There are multiple reasons for this.

→ The adversary may be, for example, an employee of the company, or if a breach has occurred, the communication to internal and external parties should be handled by the appointed person in accordance with the legal department.

Initial Investigation

we should aim to collect as much information as possible at this stage about the following:

- **Date**/**Time** when the incident was reported. Additionally, who **detected** the incident and/or who **reported** it?
- **How** was the incident detected?
- **What** was the incident? Phishing? System unavailability? etc.
- Assemble a list of **impacted systems** (if relevant)
- Document who has **accessed** the **impacted systems** and what **actions** have been taken. Make a note of whether this is an **ongoing** incident or the suspicious activity has been **stopped**
- **Physical location**, **operating systems**, **IP addresses** and **hostnames**, **system owner**, **system's purpose**, **current state** of the system
- (If **malware** is involved) List of IP addresses, time and date of detection, type of malware, systems impacted, export of malicious files with forensic information on them (such as hashes, copies of the files, etc.)

→ With the initially gathered information, we can start building an **incident timeline**.

→ This timeline will keep us organized throughout the event and provide an overall picture of what happened.

→ the timeline should contain the information described in the following columns:

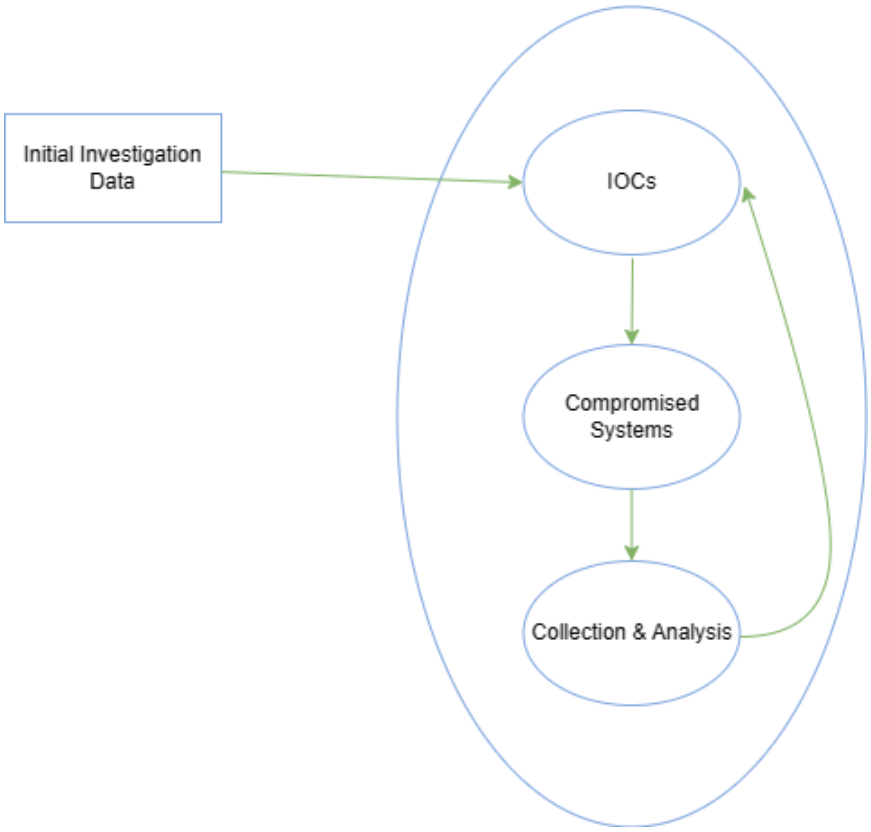
`Date`	`Time of the event`	`hostname`	`event description`	`data source`
09/09/2021	13:31 CET	SQLServer01	Hacker tool 'Mimikatz' was detected	Antivirus Software

The Investigation

- The investigation starts based on the initially gathered information that contain what we know about the incident so far
- we will begin a 3-step cyclic process that will iterate over and over again as the investigation evolves

1. **Creation** and **usage** of indicators of compromise (**IOC**)
    - An Indicator of Compromise (IOC) is a piece of evidence or artifact that suggests the presence of a security incident or compromise. It can be a file hash, IP address, domain name, URL, file name, registry key, network traffic pattern, or behavioral anomaly. IOCs are used to identify and detect malicious activities or intrusions in cybersecurity investigations.
    - a widely used standard for IOCs is **Yara**
    - there are free tools that can be utilized, such as **Mandiant's IOC Editor**
    - To leverage IOCs, we will have to deploy an **IOC-obtaining/IOC-searching tool**
        - A common approach is to utilize **WMI** or **PowerShell** for IOC-related operations in Windows environments.
    - we need to ensure that only connection protocols and tools that **don't cache credentials** upon a **successful login** are utilized (such as **WinRM**).
        - When "PsExec" is used with explicit credentials, those credentials are cached on the remote machine. (don’t use)
2. **Identification** of new **leads** and **impacted systems**
    - After searching for IOCs, you expect to have some hits that reveal other systems with the same signs of compromise.
3. **Data collection** and **analysis** from the new leads and **impacted systems**
    - we will want to collect and preserve the state of those systems for further analysis
    - there are multiple approaches to how and what data to collect (Depending on the system)

1. live response on a system as it is running (most common)
2. **shut down a system and then perform any analysis on it**
    a. not easy as much of the artifacts will only live within the **RAM memory** of the machine, which will be **lost** if the machine is turned off



→ Once the data has been collected, it is time to analyze it. This is often the most time-consuming process during an incident. **Malware analysis** and **disk forensics** are the most common examination types.

→ during the data collection process, you should keep track of the chain of custody to ensure that the examined data is court-admissible if legal action is to be taken against an adversary.

3. Containment, Eradication, & Recovery Stage

→ prevent the incident from causing more damage. (When the investigation is complete and we have understood the type of incident and the impact on the business)

Containment

- we take action to **prevent** the **spread** of the incident.

- containment actions are coordinated and executed **across all systems simultaneously**. Otherwise, we risk notifying attackers that we are after them
- We divide the actions into `short-term containment` and `long-term containment`.
- `short-term containment`
  - The actions here contain the damage and provide time to develop a more concrete remediation strategy.
  - Some of these actions can include, placing a system in a separate/isolated VLAN, pulling the network cable out of the system(s)
- `long-term containment`
  - we focus on persistent actions and changes.
  - changing user passwords, applying firewall rules, inserting a host intrusion detection system, applying a system patch, and shutting down systems.

Eradication

- Once the incident is contained, **eradication is necessary to eliminate both the root cause of the incident and what is left of it** to ensure that the adversary is out of the systems and network.
- Some of the activities in this stage include **removing** the **detected malware** from systems, **rebuilding some systems, and restoring others from backup.**
- Additional **system-hardening activities** are often performed during the eradication stage

Recovery

- we bring systems back to normal operation.
- When everything is **verified**, these systems are brought into the **production environment**.
- All restored systems will be subject to **heavy logging** and **monitoring** after an incident, as compromised systems tend to be targets again if the adversary regains access to the environment in a short period of time.
- Typical suspicious events to monitor for are:
  - **Unusual logons**
  - **Unusual processes**
  - **Changes to the registry in locations that are usually Falmodified by malware**

4. Post-Incident Activity

- In this stage, our objective is to **document** the **incident** and **improve** our **capabilities** based on **lessons learned** from it.

Reporting

→ A complete report will contain answers to questions such as:

- What and when happened?
- Performance of the team dealing with the incident in regard to plans, playbooks, policies, and procedures
- Did the business provide the necessary information and respond promptly to aid in handling the incident in an efficient manner? What can be improved?
- What actions have been implemented to contain and eradicate the incident?
- What preventive measures should be put in place to prevent similar incidents in the future?
- What tools and resources are needed to detect and analyze similar incidents in the future?