ESOF 422:

Advanced Software Engineering: Cyber Practices

Investigative models, Attacker Lifecycle

Reese Pearsall

Spring 2025

Investigation Models

NIST-800-61r2 provides guidelines and best practices for incident response

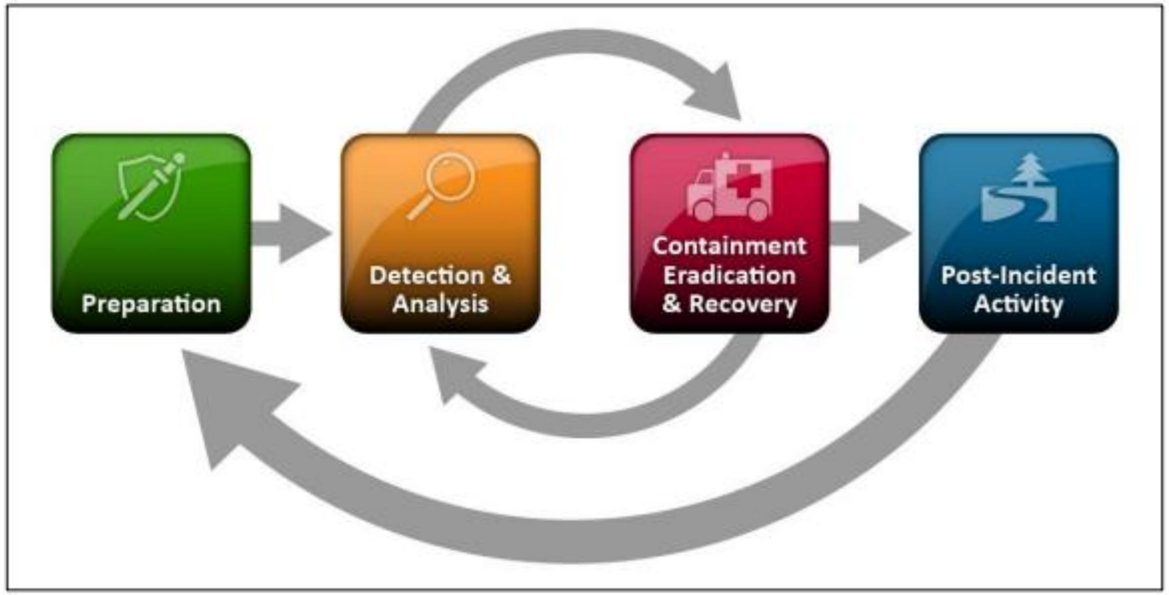
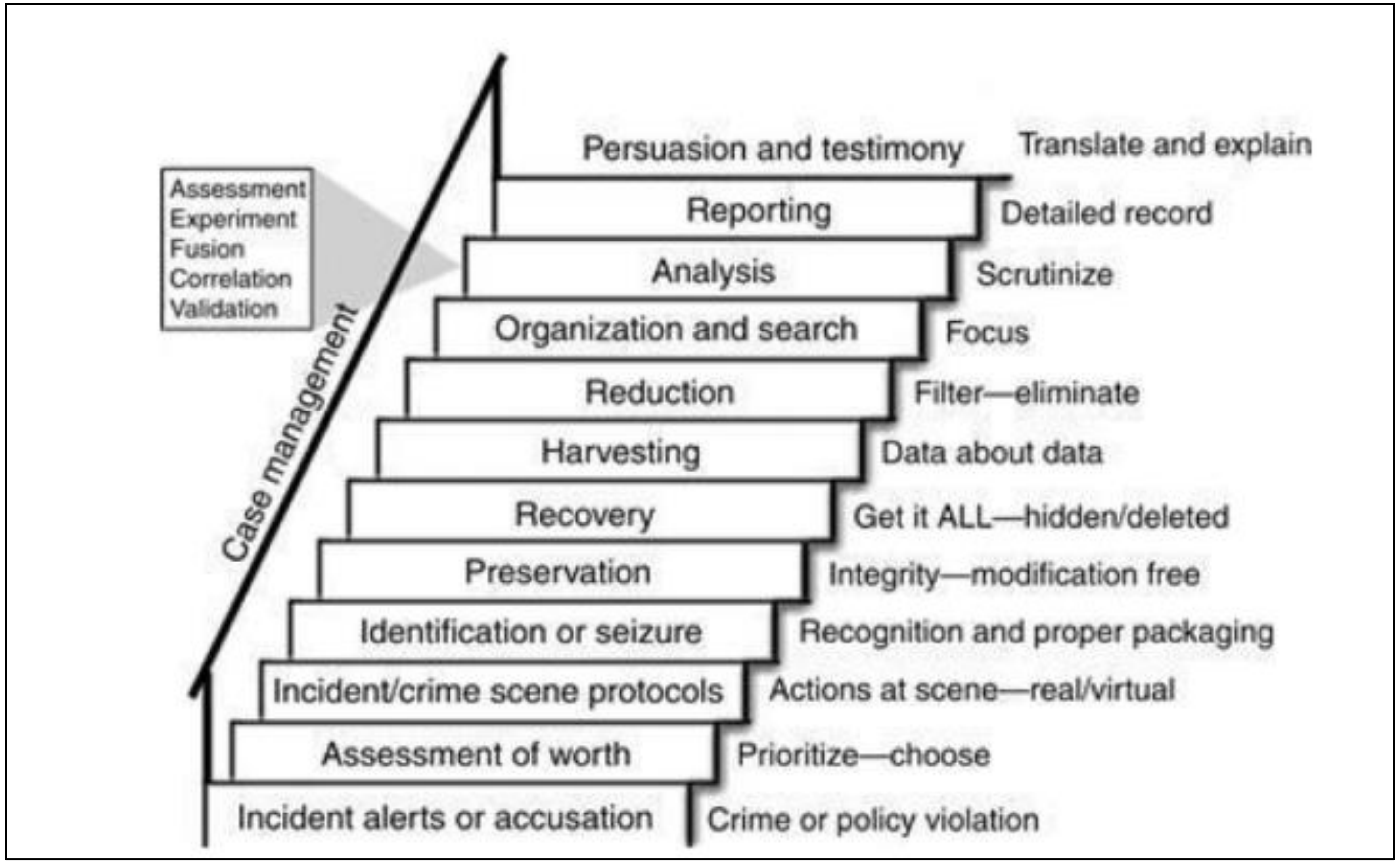


Figure 3-1. Incident Response Life Cycle

Other Investigation Models



Staircase Model

Preparation

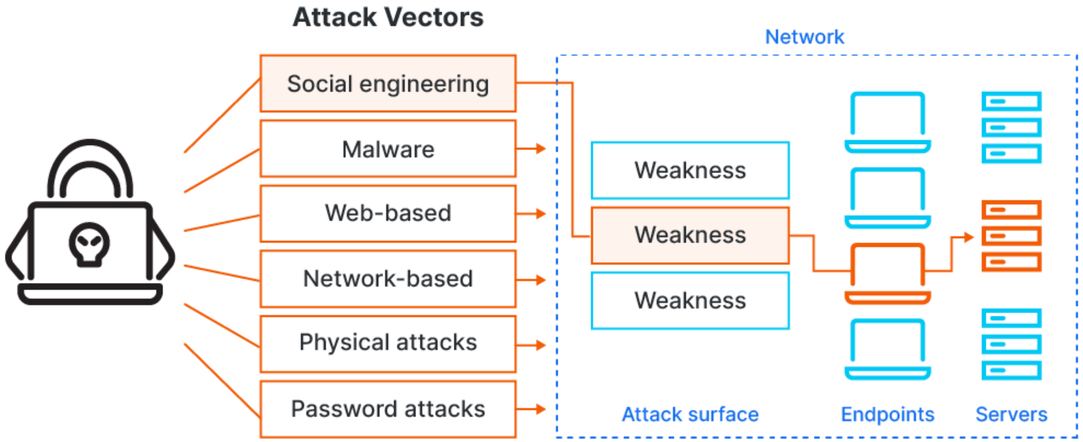
- Contact information for team members within and outside the organization, law enforcement agencies
- Issue tracking system
- Encryption software
- Secure storage facility

- Port lists
- Documentation
- Network diagrams and critical assets

Detection and Analysis

An **attack vector** is a method an attacker may use to exploit a vulnerability and compromise a system

An **attack surface** are a list of potential entry points and vulnerabilities an attacker could interact with



<u>Common attack vectors</u>:

- **External/Removable Media**- malicious USBs
- **Attrition**- a brute force method to disrupt or degrade a system or service (DDos)
- **Web-based exploits-** XSS, SSRF, etc
- **Impersonation**- spoofing, MITM, rogue wireless points
- **Loss or theft of equipment**

Detection and Analysis

A **precursor** is a sign that an incident may occur in the future.

An **indicator of compromise** is a sign that an incident may have occurred or may be occurring now**.**

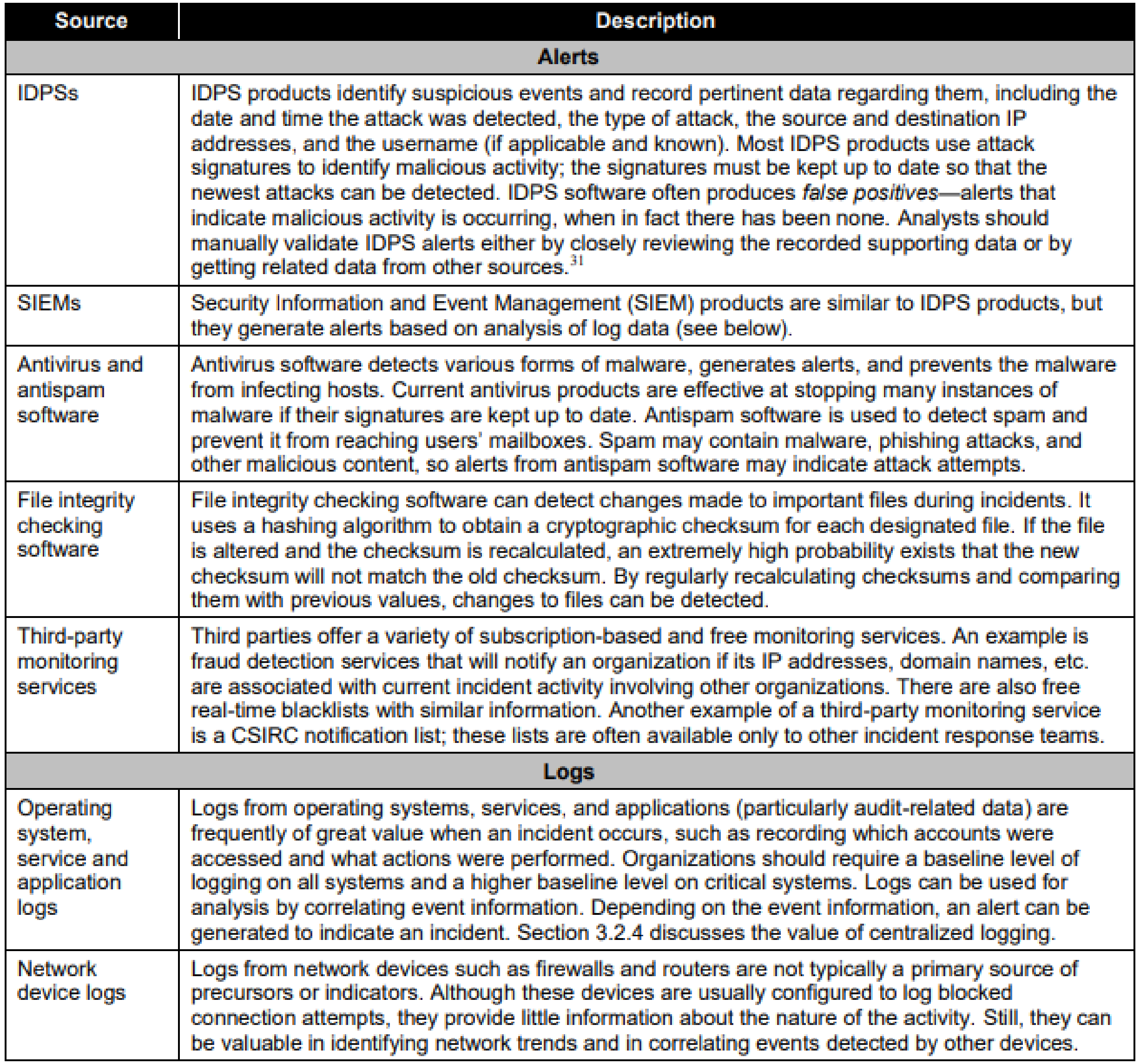
Example precursors:

- Web server log entries show usage of vulnerability scanner
- An announcement of new exploit that targets a vulnerability on the organization's mail server
- A public threat from a hacker group

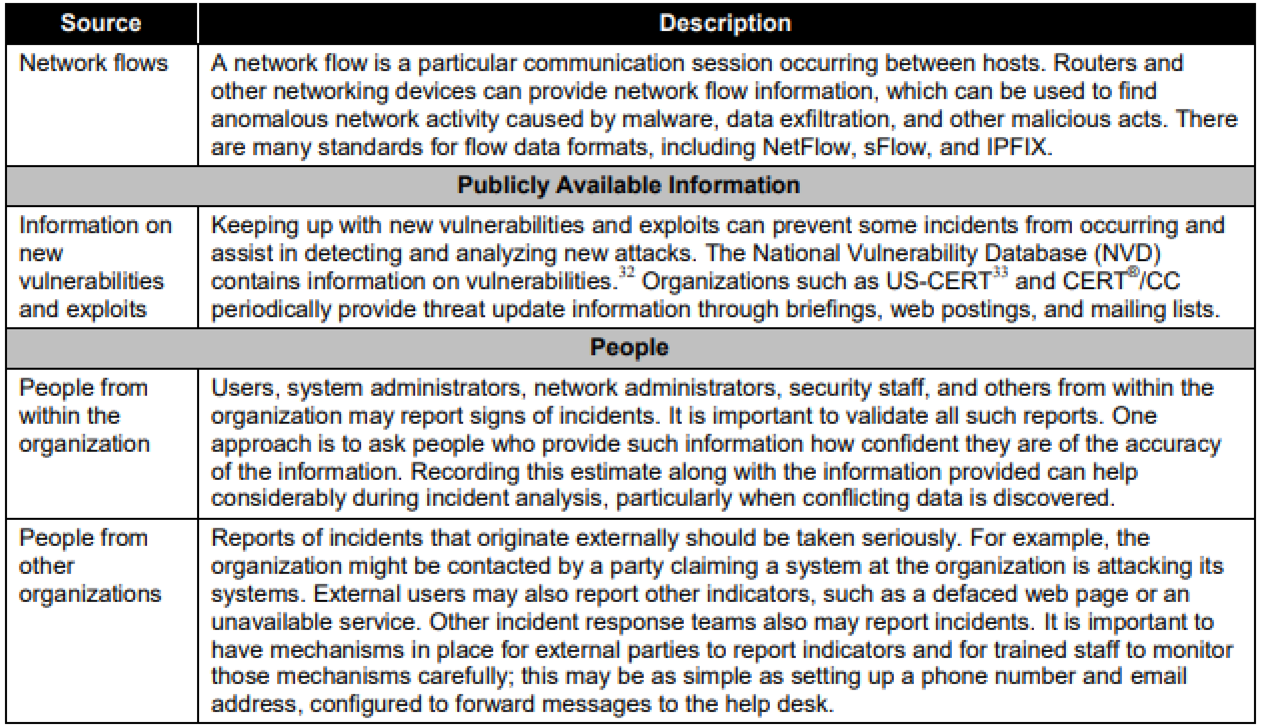
Example IOCs:

- Alert from an IDS or antivirus
- Unusual network traffic spike
- Unfamiliar IP addresses
- Multiple failed login attempts
- Unusual configuration changes
- Large number of bounced emails with suspicious content

Detection and Analysis



Source	Description
Alerts	
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives*—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.[31]
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident. Section 3.2.4 discusses the value of centralized logging.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.



Source	Description
Network flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities.[32] Organizations such as US-CERT[33] and CERT®/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

We can gather precursor and indicator information from a wide variety of sources (**defense in depth**!)

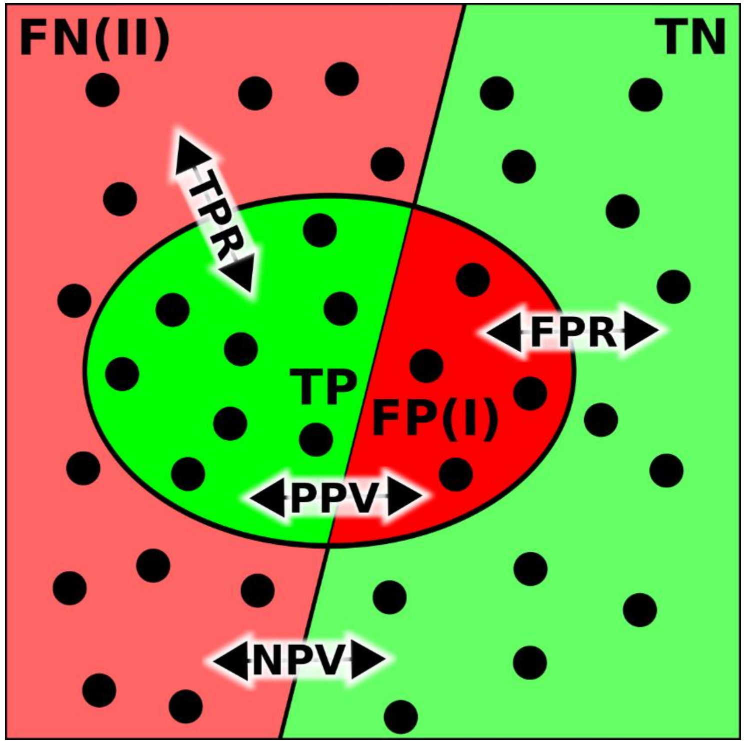
Detection and Analysis

True Positive – The detection system correctly identifies malicious activity

False Positive – The detection system incorrectly flags legitimate activity as a threat (false alarm)

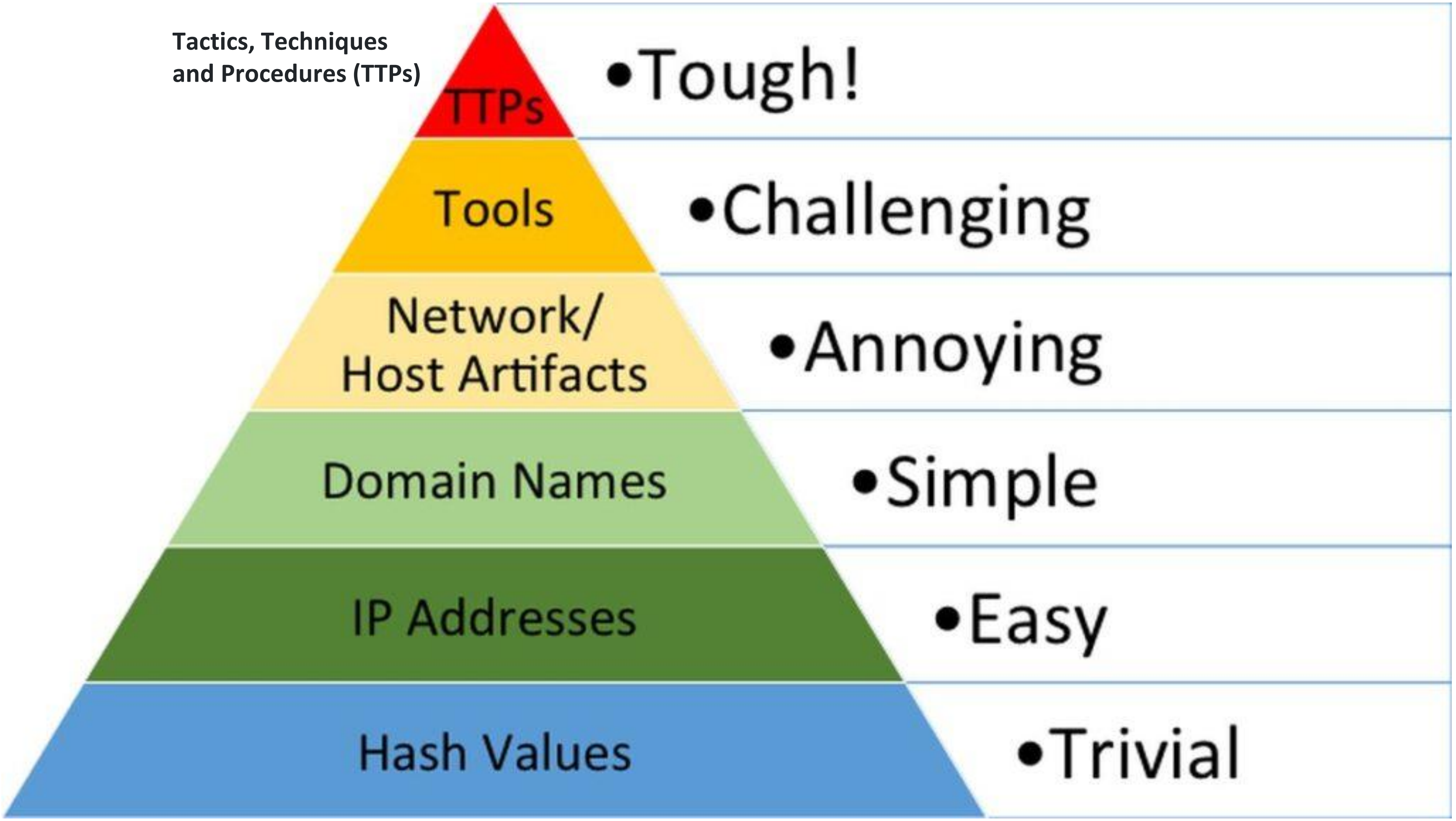
True Negative – The detection system correctly identifies normal, benign traffic

False Negative – The detection system fails to detect actual malicious traffic, thinking it is just benign traffic



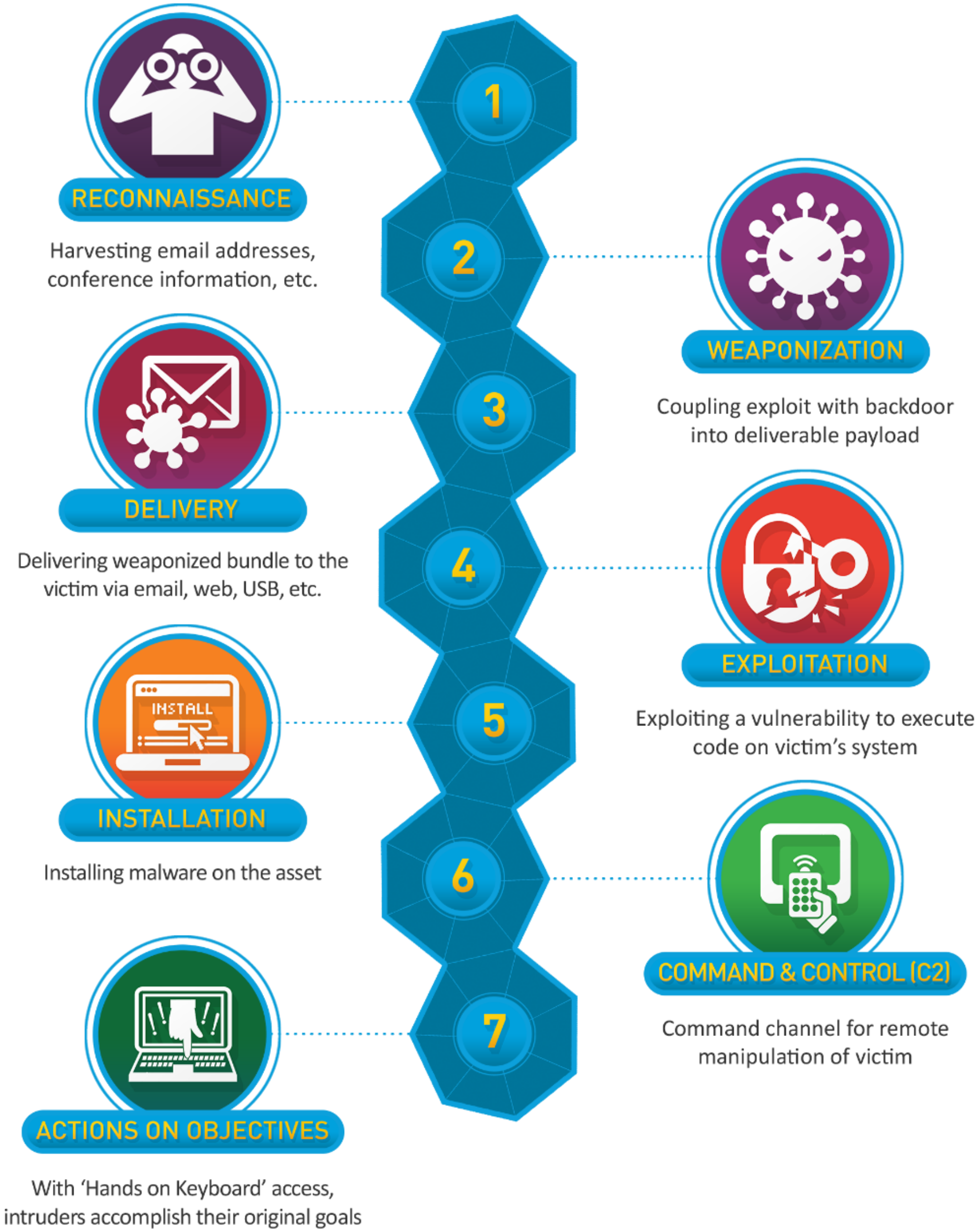
False Negatives are the scariest, and we want to minimize the number of false negatives for an IDS

Detection and Analysis



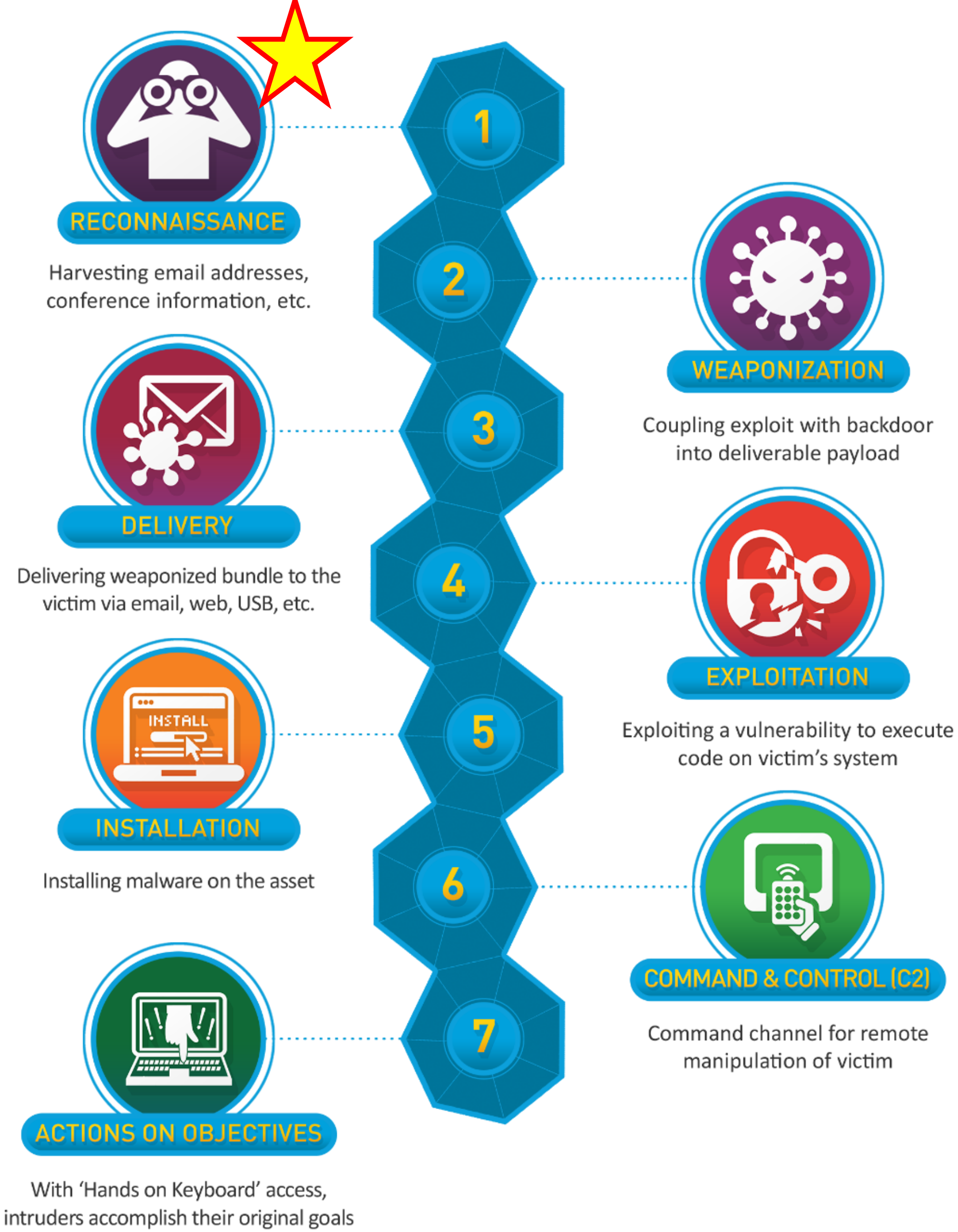
Pyramid of pain describes different indicators of compromise that can be found during investigation

- How easy they are to find
- How much pain they cause an attacker if we can implement appropriate countermeasures


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

In network forensic investigations, we can see evidence of these steps occurring!


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 1. Reconnaissance

Gather information about their target to understand potential vulnerabilities and points of entry

- Open Source Intelligence (OSINT)

  - look at public web pages, social media profiles, forums

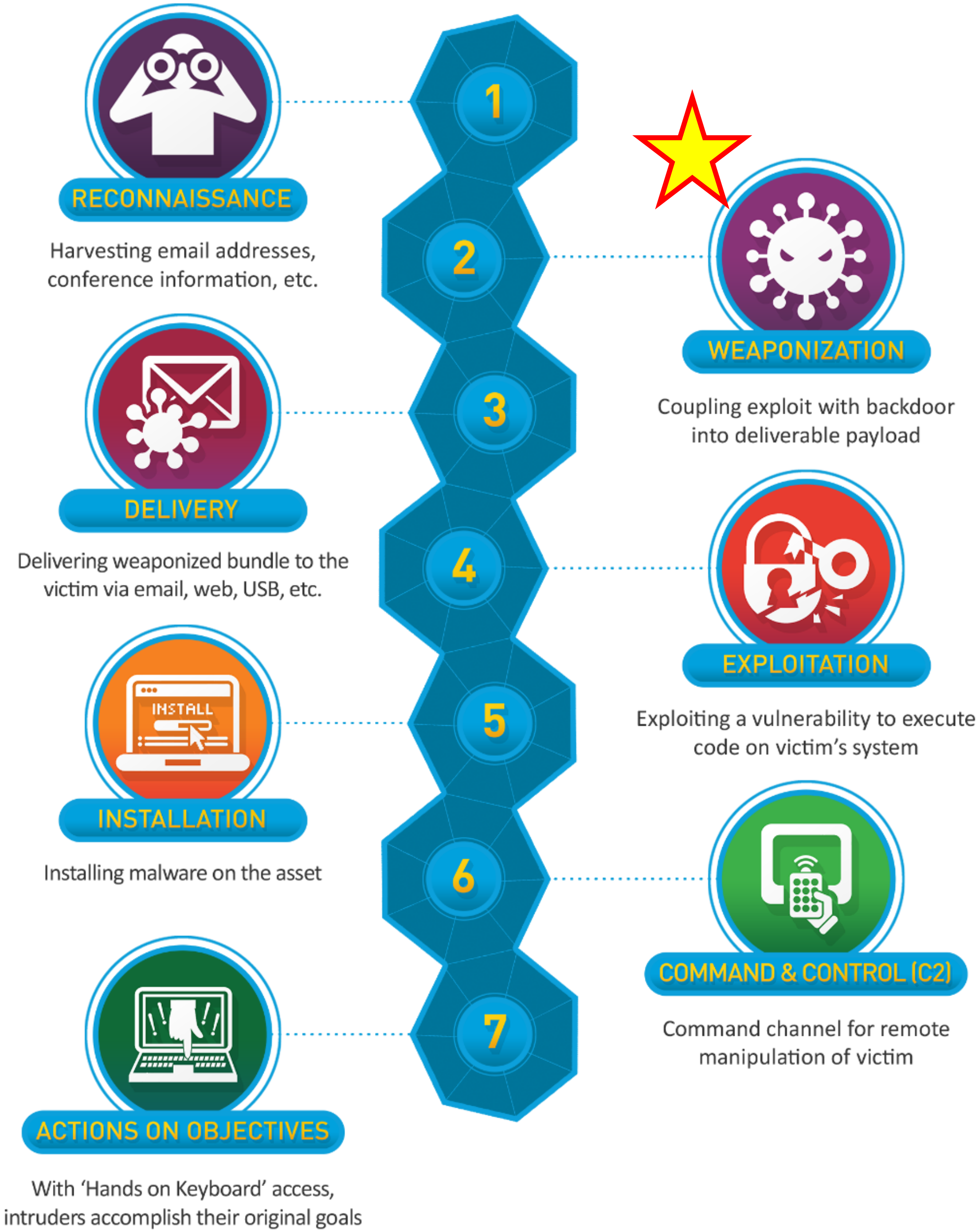
- Network Scanning

  - Use `nmap` to discover open ports and/or services

- Gather information for phishing

  - Email lists, credentials, etc

- Identify attack surface

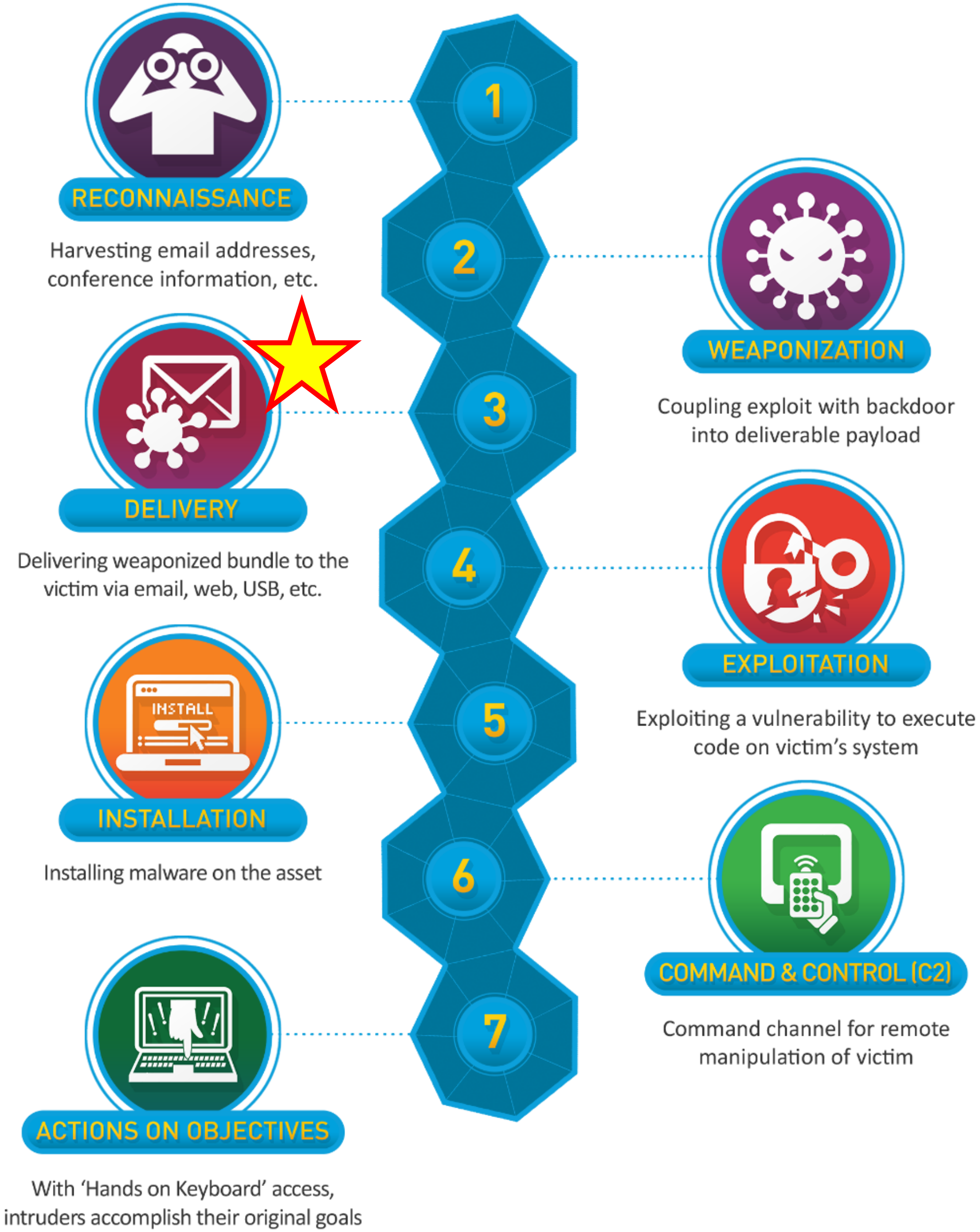

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 2. Weaponization

Create a tailored payload for your attack

- Malicious Emails
  - Phishing email, malicious macro file (.docx, .xlsx), zip file
- Trojan Software
  - Hide malicious payload in benign-looking software
- Language-specific payload for targeted vulnerability
- Malicious USB Drives

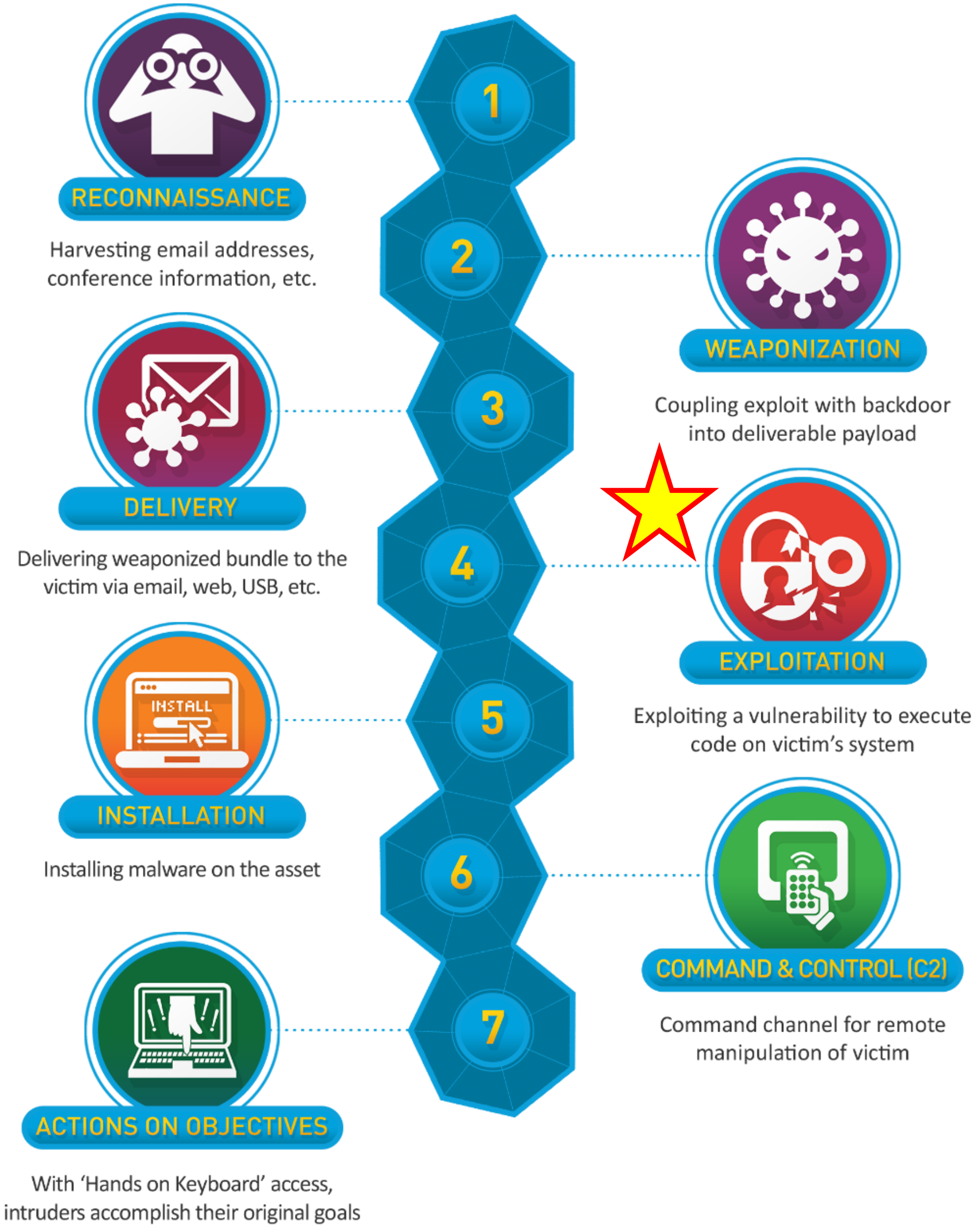

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 3. Delivery

Transmit payload to target victim

- Phishing Email(s)
- Send data to open port(s)
- Send malicious USB

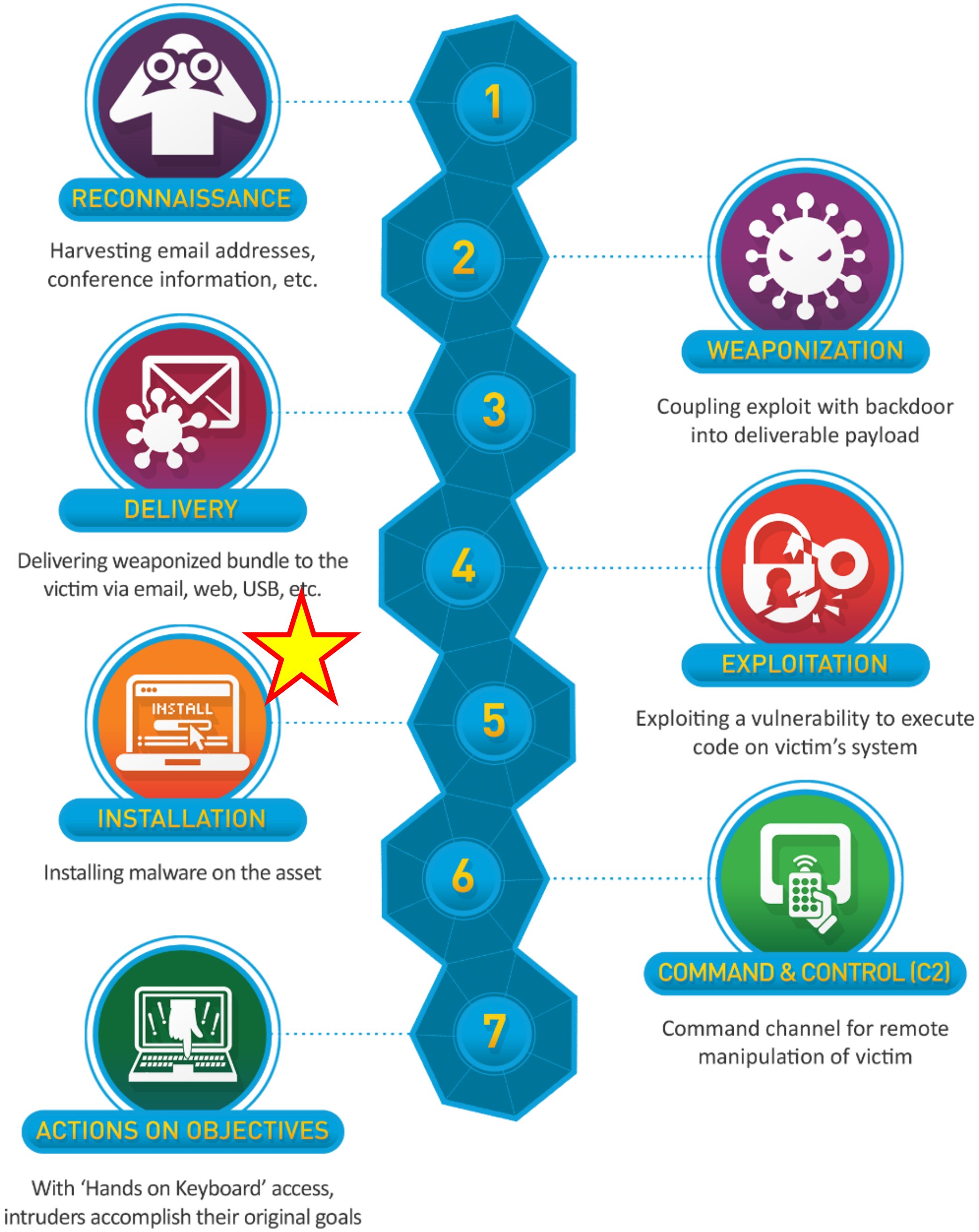

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 4. Exploitation

Payload is triggered, and vulnerability is exploited

- Victim opens malicious files
- Victim opens malicious ZIP
- Server accepts attacker's payload
- Victim plugs in USB device


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 5. Installation

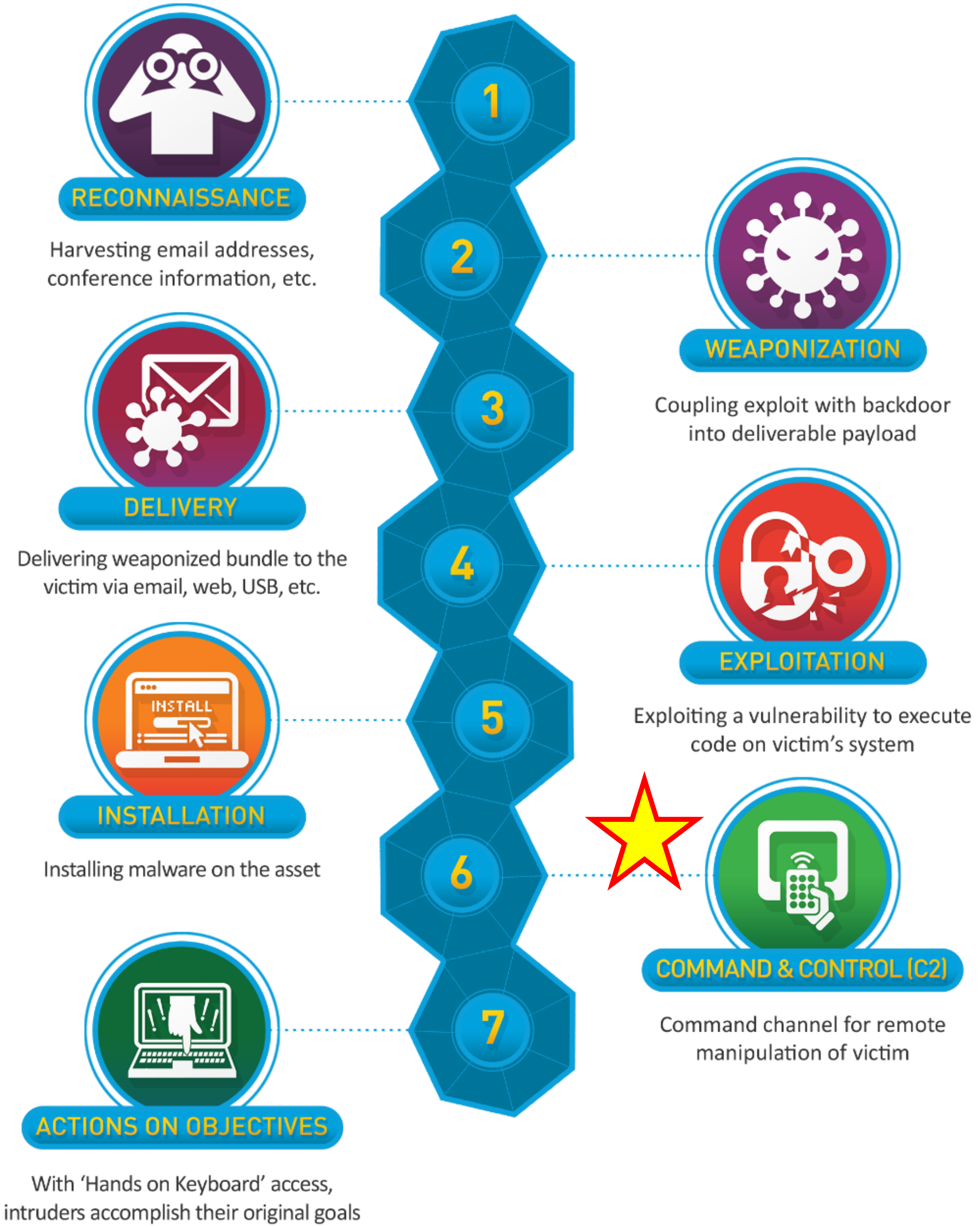
Find way to install malware to cause damage or gain persistence

- Remote Access Trojans (RATs)
  - Allows attack remote control over victim's system

- Keyloggers
  - Discover passwords or credentials

- Backdoor
  - Can be used to re-enter system later on

- **Lateral Movement**
  - Try to spread to other devices on a network

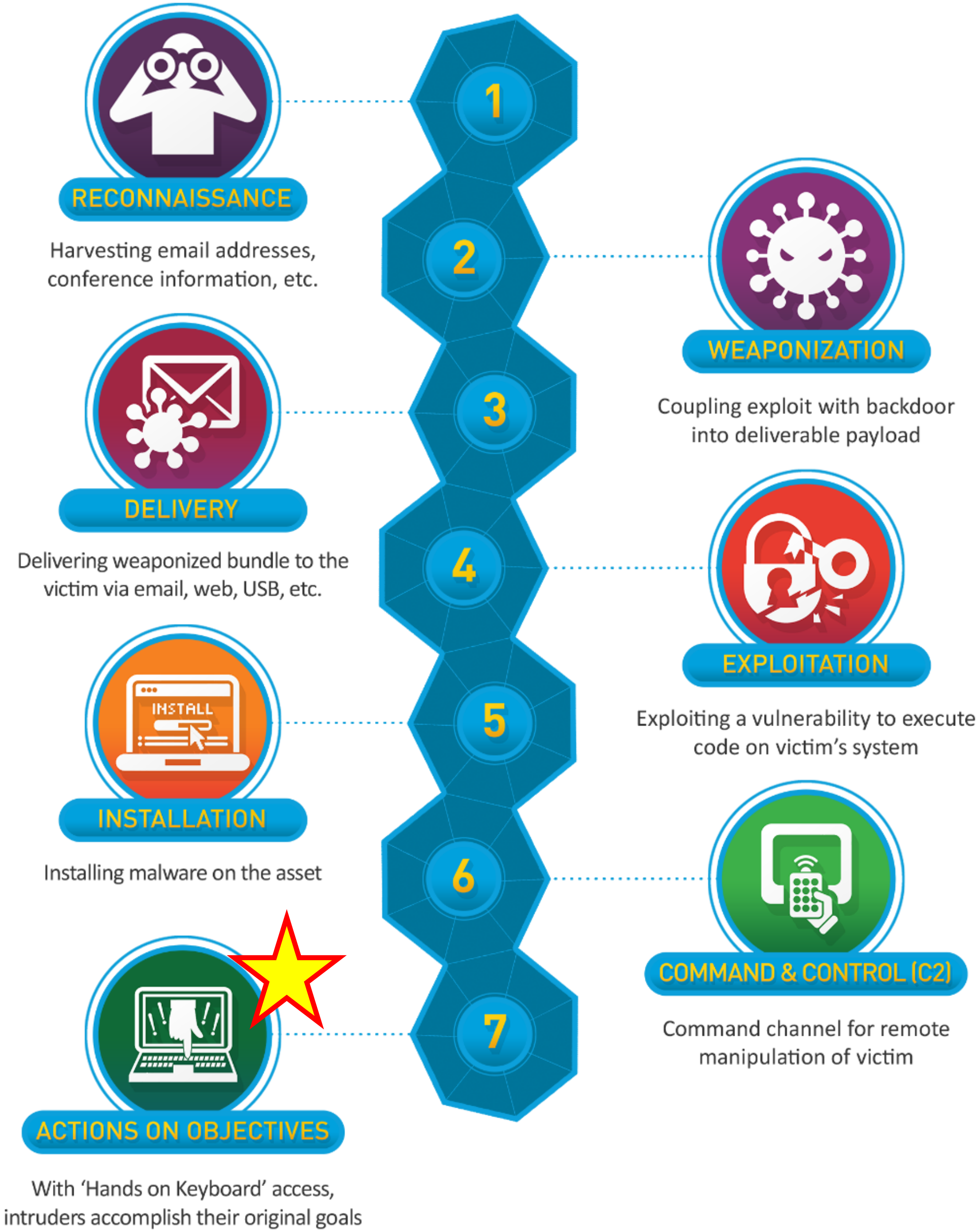

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 6. Command and Control

It is very common for attackers to “phone home” to a **command and control (C2)** server to be able to compromise the system remotely

- HTTPS/HTTP
- DNS Tunneling
- Peer-to-Peer for Botnets


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 7. Actions on Objectives

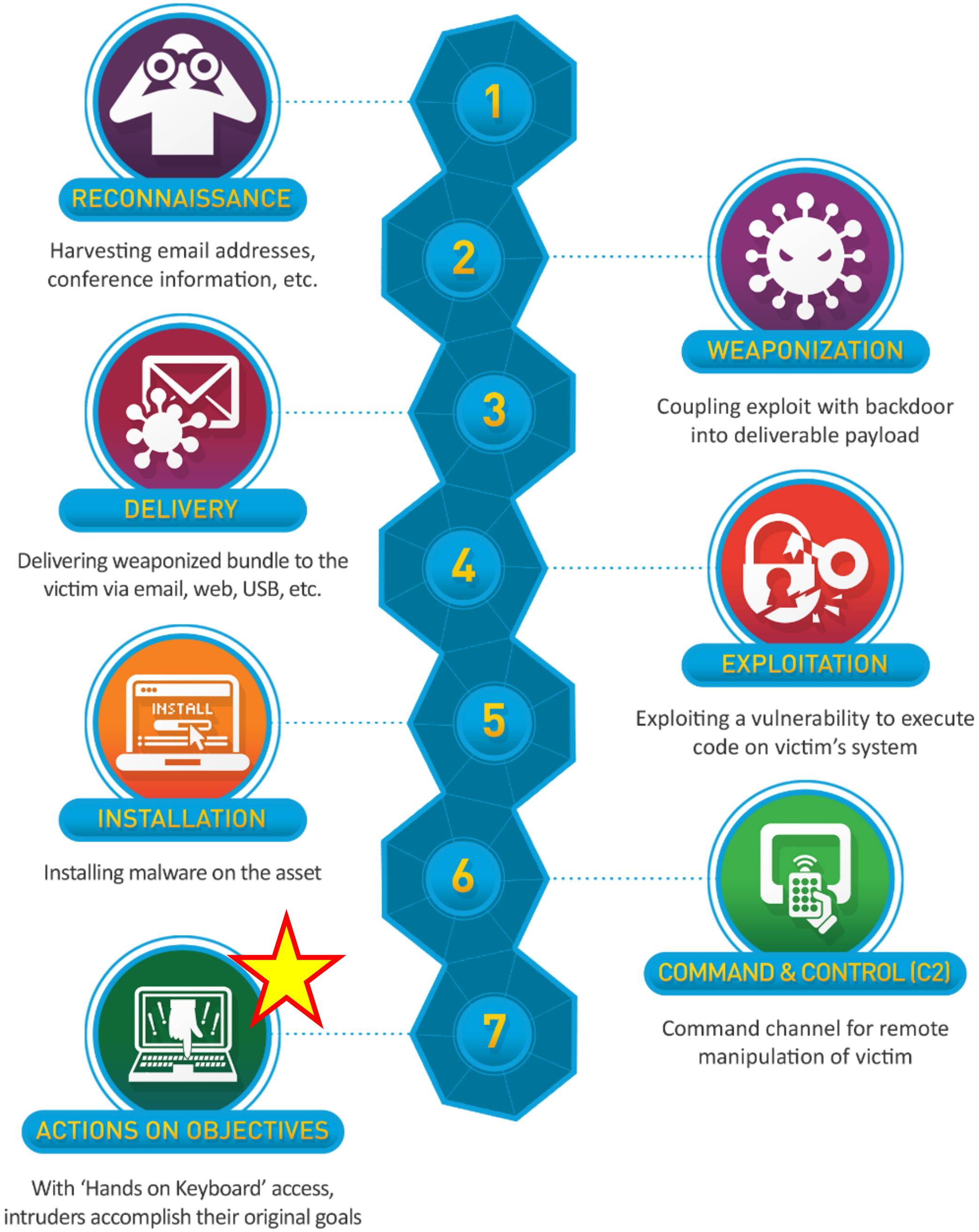
Malware is installed, attacker can remotely access a system, now do something evil

Data **exfiltration** – unauthorized transfer of data from a device or network

Delete Information

Ransomware

Deface website



1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 7. Actions on Objectives

Malware is installed, attacker can remotely access a system, now do something evil

Data **exfiltration** – unauthorized transfer of data from a device or network

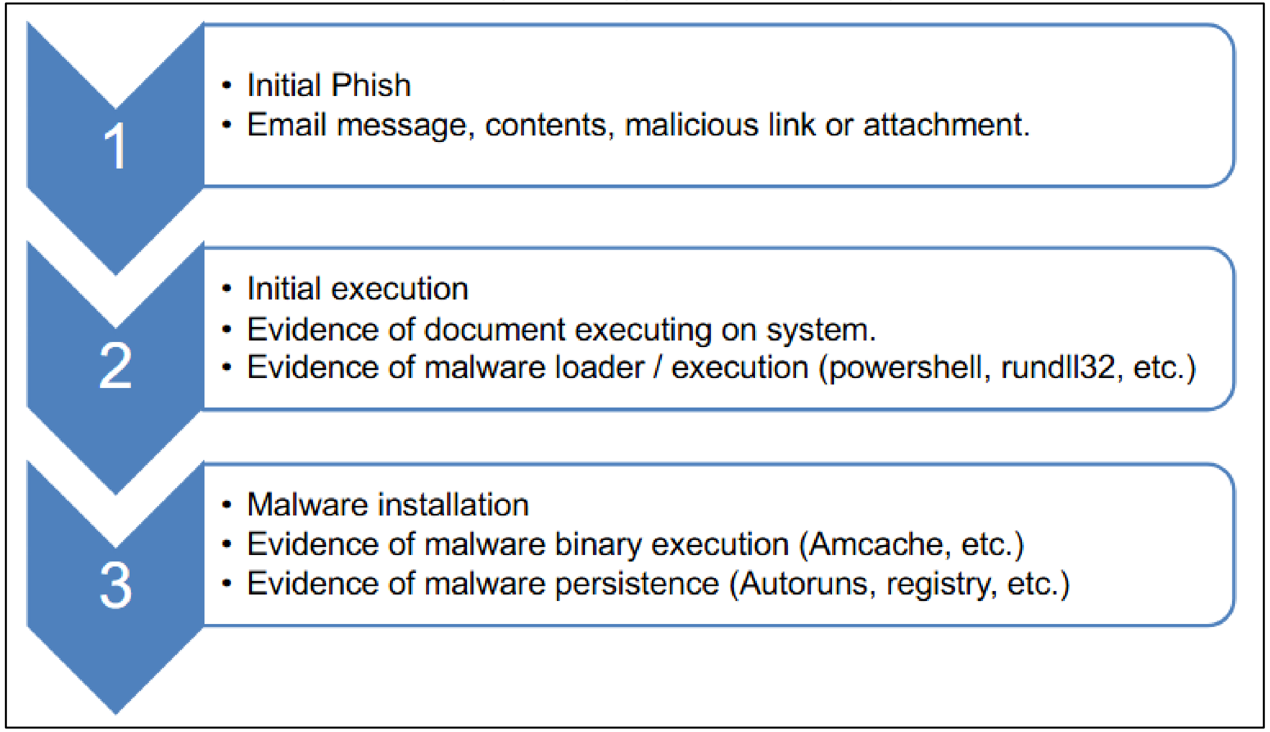
Delete Information

Ransomware

Deface website

Detection and **Analysis**

Analysis by attack lifecycle



1

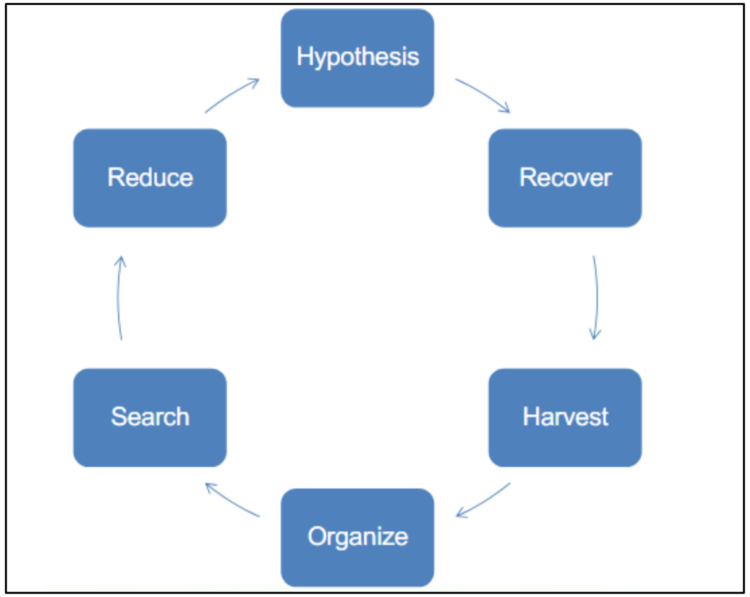
- Initial Phish
- Email message, contents, malicious link or attachment.

2

- Initial execution
- Evidence of document executing on system.
- Evidence of malware loader / execution (powershell, rundll32, etc.)

3

- Malware installation
- Evidence of malware binary execution (Amcache, etc.)
- Evidence of malware persistence (Autoruns, registry, etc.)



Hypothesis

Recover

Harvest

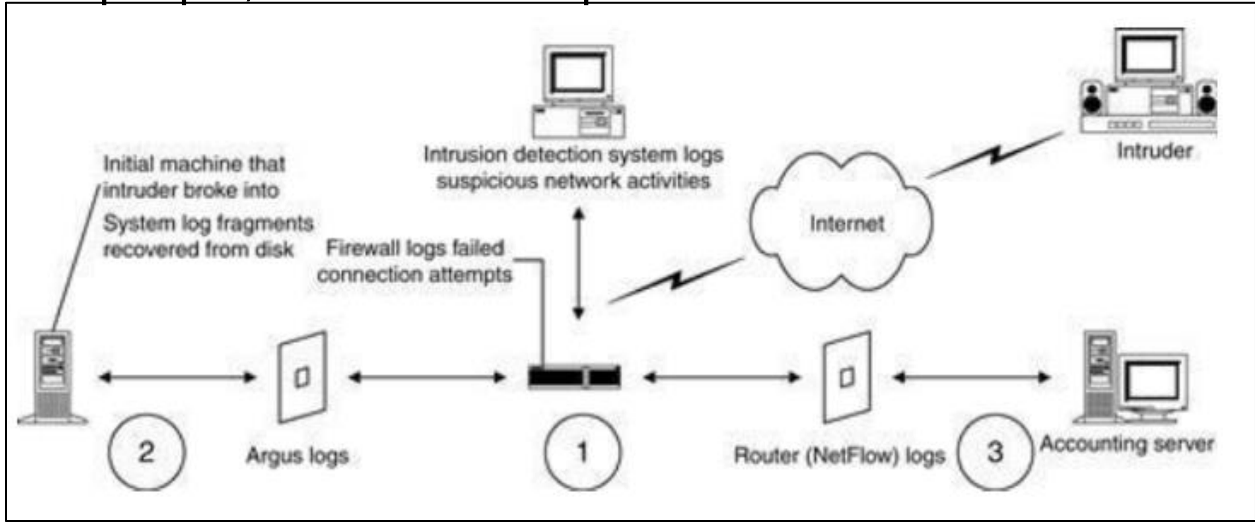
Organize

Search

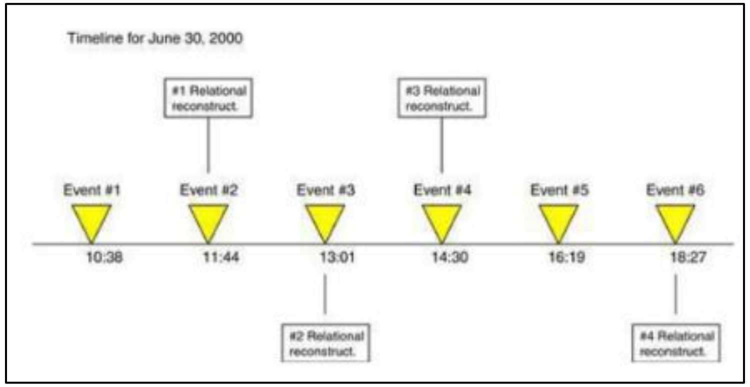
Reduce

Scientific Method

Relational Analysis- Track objects, people, and relationships



Initial machine that intruder broke into
System log fragments recovered from disk
Intrusion detection system logs suspicious network activities
Firewall logs failed connection attempts
Internet
Intruder
2
Argus logs
1
Router (NetFlow) logs
3
Accounting server



Timeline for June 30, 2000
#1 Relational reconstruct.
#3 Relational reconstruct.
Event #1
Event #2
Event #3
Event #4
Event #5
Event #6
10:38
11:44
13:01
14:30
16:19
18:27
#2 Relational reconstruct.
#4 Relational reconstruct.

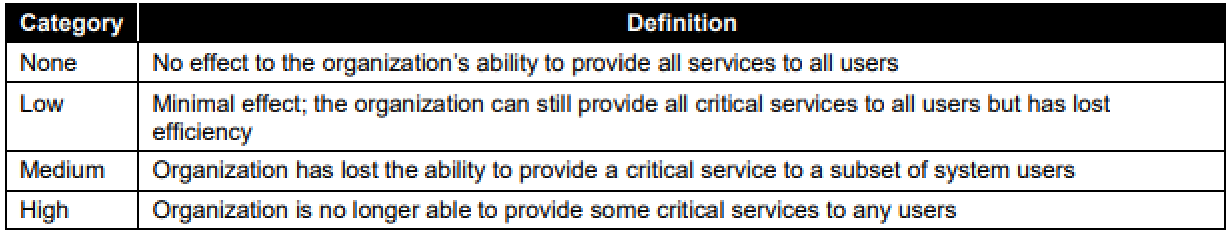
Chronological event analysis

Detection and Analysis

It is important to prioritize handling of incidents based on the following factors:

- **Functional Impact of the Incident**

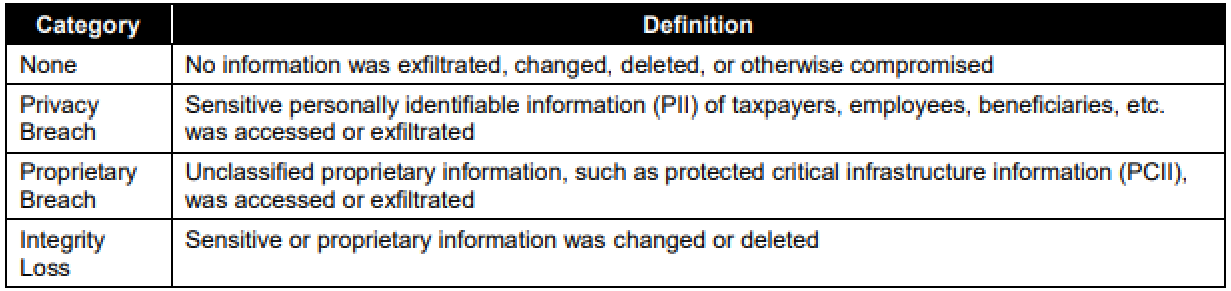
Table 3-2. Functional Impact Categories



Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

- **Information Impact of the Incident**

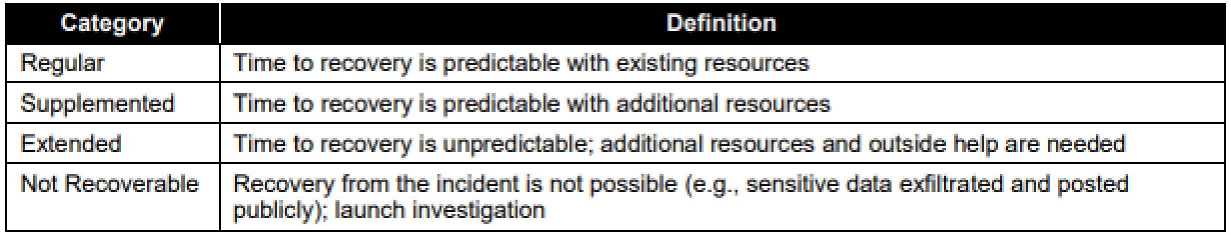
Table 3-3. Information Impact Categories



Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

- **Recoverability from the incident**

Table 3-4. Recoverability Effort Categories



Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

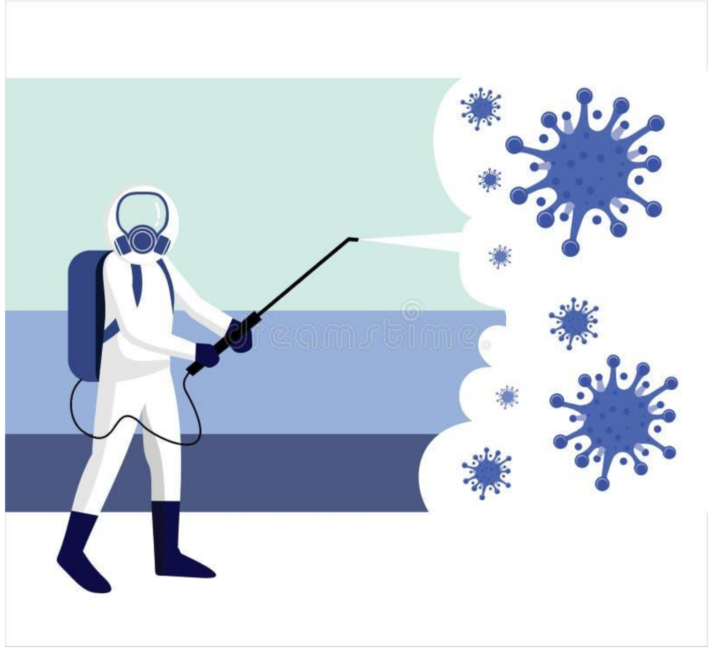
High functional impact and regular recoverability → good candidate for IT team to prioritize

Eradication, Containment, and Recovery

- **Containment** = limit spread of incident and damage
- Containment strategies vary and they must balance the need to prevent additional damage or theft with a need to maintain and collect evidence.
- Premature containment can lead to situations where an adversary is thought to be "evicted" but is not.
- Containment cannot occur without root cause analysis.
- Containment typically involves parallel network and identity efforts.

Eradication, Containment, and Recovery

- **Eradication-** removing adversary access. Eliminate vulnerability
- Good eradication and recovery strategies will take inputs from evidence collection and analysis and balance the business capabilities against attacker access.
- Must identify all affected hosts
- Phased approaches generally work better.



- **Recovery-** ensuring systems are functional within expected parameters

Evidence Gathering and Handling

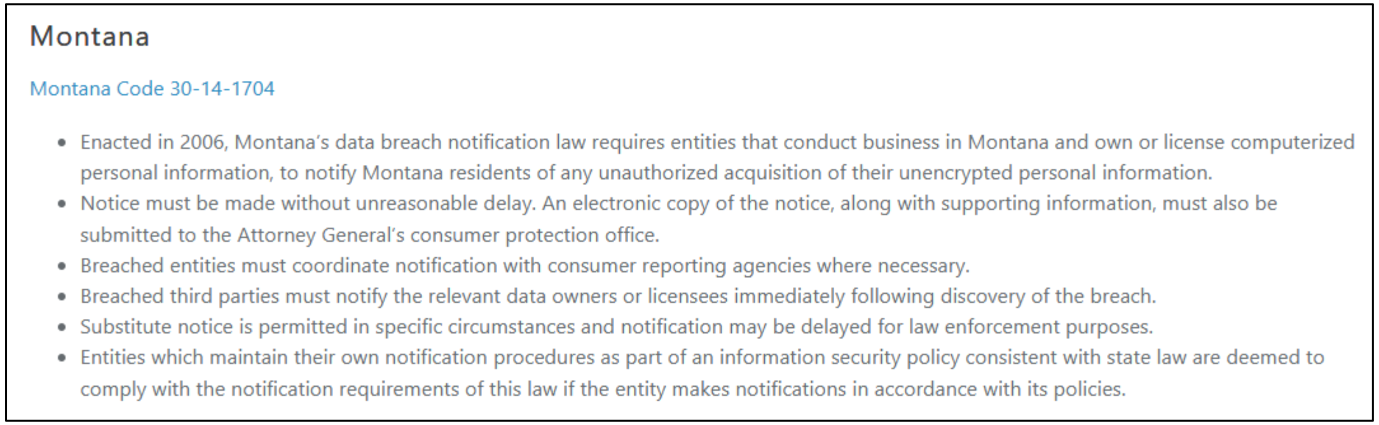
A detailed log should be kept for all evidence:

- Identifying information
- Name, title, and phone number of who has handled each piece of evidence
- Time and data (and time zone) of each occurrence of evidence handling
- Locations and where evidence was stored

Identifying Attacking Host:

- Validate the Attacking Host's IP address
- Researching IP addresses (WHOIS)
- Using Incident Databases
- Monitoring known attacker communication channels

Incident Notification



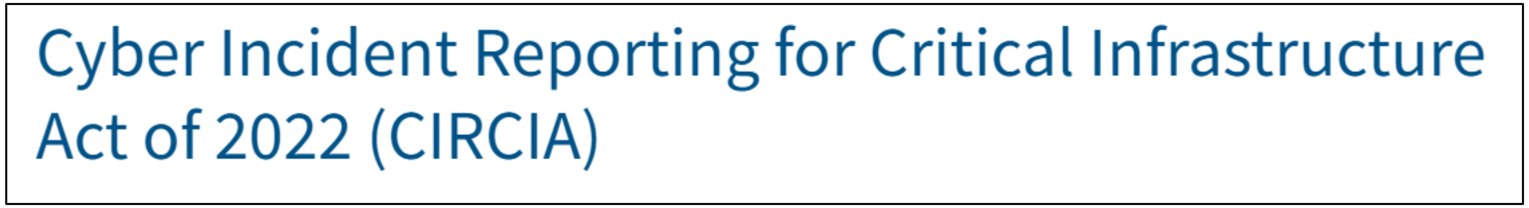
Montana

Montana Code 30-14-1704

- Enacted in 2006, Montana's data breach notification law requires entities that conduct business in Montana and own or license computerized personal information, to notify Montana residents of any unauthorized acquisition of their unencrypted personal information.
- Notice must be made without unreasonable delay. An electronic copy of the notice, along with supporting information, must also be submitted to the Attorney General's consumer protection office.
- Breached entities must coordinate notification with consumer reporting agencies where necessary.
- Breached third parties must notify the relevant data owners or licensees immediately following discovery of the breach.
- Substitute notice is permitted in specific circumstances and notification may be delayed for law enforcement purposes.
- Entities which maintain their own notification procedures as part of an information security policy consistent with state law are deemed to comply with the notification requirements of this law if the entity makes notifications in accordance with its policies.

Incident response policy typically involves notification to certain individuals or entities

- CIO
- Head of information security
- Security officer
- Legal department
- Cybersecurity and Infrastructure Security Agency (**CISA**)



Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Cybersecurity Information Sharing Act of 2015 allows for government agencies to share cybersecurity threat data amongst federal and nonfederal entities, to help strengthen cybersecurity defenses

- May expire in September. Congress currently debating renewal.

Post Incident Activity

Lessons learned

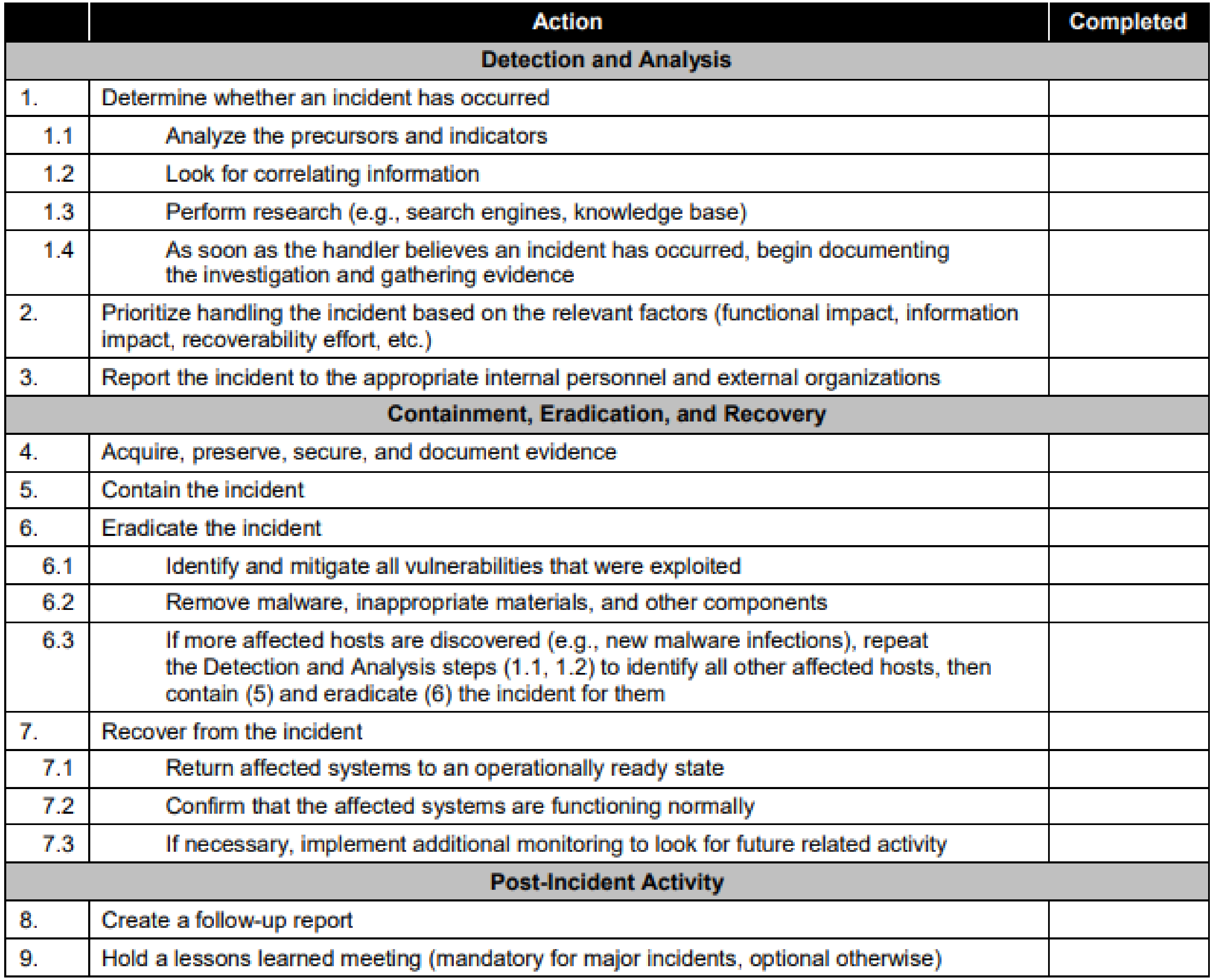
- What happened, when?
- Did staff and organization perform as expected
- What would staff do differently next time?
- What corrective actions should be taken?

Assess issues because on **prioritization** from the detection/analysis steps

Put together report, document the number of incidents, time per incident, objective assessment, and share with necessary parties

Retention- data and records may need to be kept for a certain amount of time, or until legal cases have resolved

Table 3-5. Incident Handling Checklist



	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Incident response can be a daunting task at first, so it may be helpful to keep a checklist of necessary tasks

Critical Focus Areas

Despite each investigation being unique, there are core investigations focus area almost all investigation includes:

<u>Core Areas</u>

- Customer Data
- Intellectual Property
- Financial and Payment system

<u>Core Functions</u>

- Local Authentication
- Remote Authentication
- Data Access

<u>Core Systems</u>

- Active Domain Controllers

Active Directory- (Microsoft) database of user accounts, groups, network resources, and security policies

- Email server
- Web application servers
- Remote Access Servers