

**November 12, 2024**

# **“Oops, They Hacked It Again: Responding to Cyber Incidents Like a Pro”**

**Foundations of Cybersecurity - CYBS 3213**

**Christopher Freeze, Ph.D.  
Assistant Professor, Cybersecurity  
OU Polytechnic Institute**



# Checking In

- What's the top takeaway from last class or classes that's sticking with you?
- Was there anything from last class or classes that didn't fully click? Anything you're still a little fuzzy on?

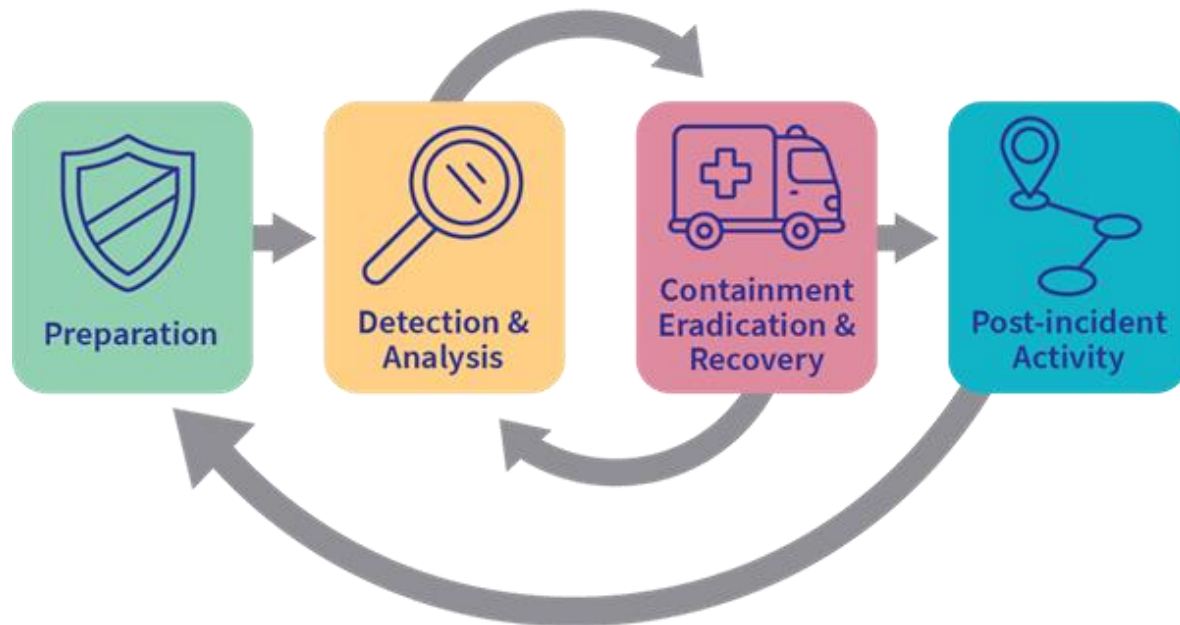
# Learning Outcomes

1. Understand and apply the key components of an effective Incident Response Plan (IRP), including preparation, containment, eradication, and recovery strategies.
2. Demonstrate knowledge of various digital forensics techniques, including evidence acquisition, preservation, and analysis, while maintaining the integrity of the evidence through proper chain of custody and provenance documentation.
3. Evaluate and implement appropriate containment and eradication techniques, such as quarantine, endpoint security reconfiguration, and the use of application approved/deny lists, in response to different types of cybersecurity incidents.

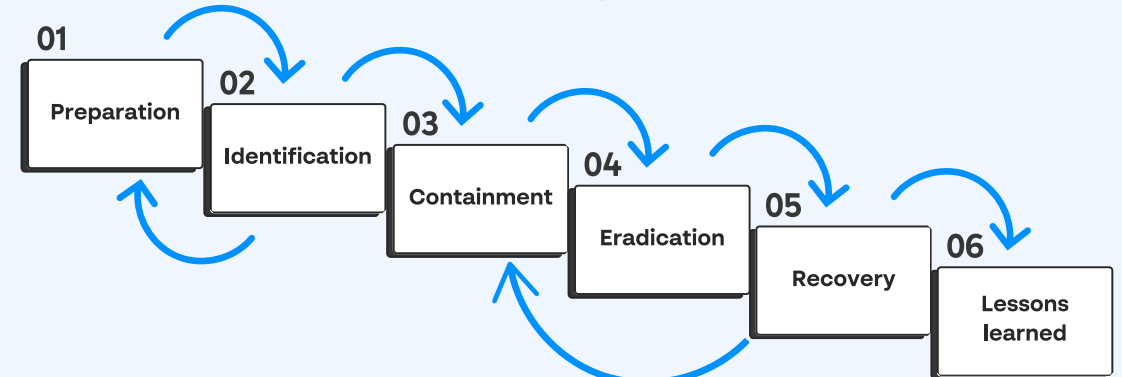
What is a cybersecurity incident  
or cybersecurity crises?

# Cyber Crisis Management Lifecycle

## Cyber Incident Response Cycle



## SANS Incident Response Process



# Incident Response

- Prevention
- Preparation
  - Incident Response Plan (IRP)
  - Incident Response Team (IRT)
- Response
  - Detection and Analysis (Identification)
  - Containment and Eradication Strategies
- Recovery
  - Post-incident Activity
  - Lessons learned (Hot wash)

# Detection and Analysis (Identification)

**Detection:** Security monitoring systems, such as intrusion detection systems (IDS), firewalls, and antivirus software. Alerts are generated for behaviors or patterns that match known threat signatures or unusual behaviors, triggering further investigation.

**Triage and Initial Analysis:** After an alert, the team prioritizes incidents based on potential impact and urgency. Examine logs, network traffic, and other relevant data to determine the legitimacy of the threat, often filtering out false positives.

**Scope and Impact Assessment:** Analysts attempt to understand the full scope of the incident—whether it affects a single device, user, or the entire network. They assess potential impact, including data confidentiality, integrity, or availability risks, to determine the severity of the incident.

# Containment and Eradication Strategies

**Containment:** This response strategy keeps a security incident from spreading across the network, protecting other resources.

**Isolation:** This strategy restricts the incident's effects to just one resource, preventing it from affecting others.

**Segmentation:** This approach limits the impact of an incident to a small section or group of network resources, rather than the entire network.

**Eradication:** Involves eliminating malicious files, closing exploited vulnerabilities, and ensuring no remnants of the attack remain in the system.

- Endpoint Detection and Response (EDR) Tools (CrowdStrike Falcon)
- SIEM (Security Information and Event Management) Solutions (Splunk)



# Recovery

## **1. Post-incident Activity**

- Restoring systems and data
- Implementing long-term fixes

## **2. Lessons Learned (Hot Wash)**

## **3. Root cause analysis**

- Investigators try to identify how the threat entered the system, whether it exploited a known vulnerability, involved social engineering, or used another attack vector. This helps to understand the entry point and method, critical for containing the threat.

# Incident Response Resources

## Software

- 1. Command-Line Interface (CLI):** This is a text-only screen where you type commands using a keyboard to control a computer or program.
- 2. Graphical User Interface (GUI):** This is a screen with visuals like menus and icons that you click on with a mouse or other pointing device to interact with a computer or program.
- 3. Network Platform:** This is a special interface, either text-based (CLI) or graphical (GUI), provided by a specific vendor to run commands or access software on their device.

# Incident Response Resources

Metadata - Background information about files, network activities, or data that helps investigators understand the context of an incident.

1. File metadata – Name, size, data, hash values
2. Network metadata - IP addresses, ports, protocols, packet sizes
3. User and Access metadata – Login attempts, privilege levels.
4. System metadata – logs from applications, operating systems
5. Email metadata – sender & receiver addresses, subject lines
6. Time metadata – event timestamps, sequence of actions



Data

**Filename:** Tadzik.jpg  
**Author:** Piotr Kononow  
**Date:** August 15, 2016 6:40:10PM  
**File:** 5,312 × 2,988 JPEG  
15.9 megapixels  
3,393,448 bytes  
(3.2 megabytes)  
**Camera:** Samsung SM-G920F  
4.3 mm  
**Lens:** Max aperture f/1.9  
(shot wide open)  
Auto exposure  
Program AE  
**Exposure:** 1/402 sec  
f/1.9  
ISO 40  
**Flash:** none



Metadata

DS 13.09.2018 19:10  
Dataedo Store <dataedo@dataedo.com>  
Your Dataedo order 2018/718  
Do dataedo@dataedo.com

Dataedo\_invoice\_2018-D-461.pdf  
792 KB



Thank you for choosing Dataedo. We are sure you will find it useful.  
You will find your keys below and invoice in attachment of this email.  
If you need any information or assistance respond to this email.

### Order details

**Order #:** 2018/718  
**Order date:** 2018/09/13  
**Status:** Paid  
**Payment method:** PayPal

### Items

Product	Price
Dataedo Pro - 1 Year Subscription	\$468
<b>Grand Total</b>	

### Your key

**Dataedo Pro - 1 Year Subscription (1 user)**  
ENJELJPDJDNLBMDHADENADDODPHOMLJI  
LHNFKANHKJBEAPEOIIAAODBLGFBMOFHD  
NKGLNIPPHMDIMDBPLELKKFMFDNCMAHBP  
BCGGNCBMJPNHPLIKGMDCCNAMKKPJHGHN  
FHADBHEIOKFDGEONIFCLJIMADANLENHL  
PDKBNPFJDDIEGNLCJMJFFPMKMIOGGAOO  
NKGLNIPPHMDIMDBPLELKKFMFDNCMAHBP  
BCGGNCBMJPNHPLIKGMDCCNAMKKPJHGHN

Data

Metadata

Properties

Settings

Importance Normal  
Sensitivity Normal

☐ Do not AutoArchive this item

Security

☐ Encrypt message contents and attachments  
☐ Add digital signature to outgoing message  
☐ Request S/MIME receipt for this message

Tracking options

☐ Request a delivery receipt for this message  
☐ Request a read receipt for this message

Delivery options

Have replies sent to  
☐ Expires after None 12:00 AM

Contacts...  
Categories ▼ None

Internet headers

Received: from 124135.cloudwaysapps.com (104.131.29.249) (HELO dataedo.com)  
by server1307517.home.pl (188.128.181.235) with SMTP (IdeaSmtpServer 0.83.148)  
id c6e24d77096d7dee; Thu, 13 Sep 2018 19:10:22 +0200  
Reply-To: <jm@dataedo.com>  
From: "Dataedo Store" <dataedo@dataedo.com>

Close

# Incident Response Resources

## Basic logs

1. Device logs – text-based file that records events
2. Traffic logs – captures incoming and outgoing network traffic
3. Audit logs – system-related events (user login attempts)
4. Syslog – network protocol that allows devices or apps to send log entries to syslog server; categorized by 8 severity levels

## Advanced logs

1. Advanced Log Entry – Structured JSON (JavaScript Object Notation); enriched data
2. Syslog Daemons -Background processes that collect, process, and route log messages
3. Advanced log types (Journalctl log; Dump file; SIP log)

# Containment and Eradication Techniques

- Quarantine – Isolating compromised endpoint or data to prevent spreading
- Endpoint Security Reconfiguration – Adjustments to quarantined endpoint
  1. **Patch Management:** Installing all necessary security updates.
  2. **Malware Protection:** Updating anti-malware software.
  3. **Host-Based Security:** Configuring a firewall on the host device.
  4. **Endpoint Hardening:** Deploying tools like EDR (Endpoint Detection and Response) or ETDR (Extended Threat Detection and Response).
  5. **Disk Hardening:** Applying disk encryption to secure stored data.
- Application Approved and Deny Lists
- Security Orchestration, Automation, and Response (SOAR)

# IR Attack Frameworks

- **MITRE ATT&CK – Catalogs various techniques**
  1. Organized into tactics (the “why” of an attack technique) and techniques (the “how”).
  2. Covers 14 tactics, including Reconnaissance, Resource Development, Initial Access, Execution, Persistence, ..., Impact.
  3. Provides detailed information on specific techniques used by attackers.
- **Diamond Model of Intrusion Analysis – Abilities**
  1. Four core elements: Adversary, Capability, Infrastructure, and Victim
  2. Focuses on the relationships between these elements.
  3. Includes meta-features like timestamps, phases, results, directions, methodology, and resources.



# IR Attack Frameworks

- Cyber Kill Chain – Steps an attacker must take
  - a. Seven stages: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives
  - b. Used to understand the anatomy of a cyberattack.
  - c. Helps in developing defensive strategies for each stage of an attack.
- In practice, these frameworks are often used complementarily. The ATT&CK framework can provide detailed techniques for each stage of the Kill Chain, while the Diamond Model can help analyze the relationships between different elements in an ATT&CK-based assessment.



# Attack Frameworks

# IR Attack Exercises

- IR Exercises: Evaluates an organization's IR capabilities by combining an attack framework with the organization's IRP. Types include:
  1. **Tabletop Exercise:** The IR team discusses each IRP step.
  2. **Walkthrough Exercise:** The team walks through each IRP step without action.
  3. **Simulation Exercise:** The team performs the IRP in a simulated attack.
- Failover – Automatically switching to backup systems
- Parallel processing – Using resources simultaneously for faster completion - different teams doing similar work on different segments

# Digital Forensics

- **Digital Forensics:** A branch of forensic science that involves collecting, analyzing, and reporting electronic data to investigate digital crimes, policy violations, data recovery, or reconstructing security incidents.
- **Digital Evidence:** Valuable electronic data in an investigation, such as files or logs relevant to a case (mirror the infected endpoint; system?)
- **Chain of Custody and Provenance:** Tracks handling of evidence and provides record of data origin and history.
- **Legal Holds:** A process to preserve data relevant to potential legal actions against an organization.

# Digital Evidence Acquisition

- Digital evidence can come from hardware (e.g., memory and storage) or software (e.g., logs). A **forensic artifact** is any data that could potentially serve as evidence.
- **Order of Volatility**: A prioritized sequence for collecting data in a forensic investigation, based on how quickly data disappears without power.
- Data **jurisdiction** affects data privacy, as cloud data stored worldwide is subject to local laws, impacting privacy & notification requirements
- Evidence Recovery: Forensics can recover deleted or damaged files through **file carving** and **file signatures**.



# Digital Forensics

© 2021 Messer Studios, LLC

Elle is conducting an exercise for her organization and wants to run an exercise that is as close to an actual event as possible. What type of event should she run to help her organization get this type of real-world practice?


---



- a. A simulation
- b. A tabletop exercise
- c. A walk-through
- d. A wargame

Wiping a drive and reinstalling from known good media is an example of what incident response option?


---

- a. Recovery
- b. Containment
-  c. Eradication
- d. Root cause elimination




What phase of the incident response process often involves adding firewall rules and patching systems to address the incident?

---


- a. Preparation
- b. Eradication
-  c. Recovery
- d. Containment

Brent wants to use a tool to help him analyze malware and attacks and wants to cover a broad range of tactics and tools that are used by adversaries. Which of the following is broadly implemented in technical tools and covers techniques and tactics without requiring a specific order of operations?


---

- a. The Diamond Model of Intrusion Analysis
- b. The Cyber Kill Chain
-  c. The MITRE ATT&CK framework
- d. The CVSS (Common Vulnerability Scoring System) standard

What forensic concept is key to establishing provenance for a forensic artifact?

- 
- a. Right to audit
  - b. Preservation
  -  c. Chain of custody
  - d. Timelines

What legal concept determines the law enforcement agency or agencies that will be involved in a case based on location?

- 
- a. Nexus
  - b. Nonrepudiation
  -  c. Jurisdiction
  - d. Admissibility

**November 14, 2024**

**Jeremy Zuniga - Presentation  
“Experiences with Incident  
Response and Digital Forensics”**

**Foundations of Cybersecurity - CYBS 3213**

**Christopher Freeze, Ph.D.  
Assistant Professor, Cybersecurity  
OU Polytechnic Institute**

