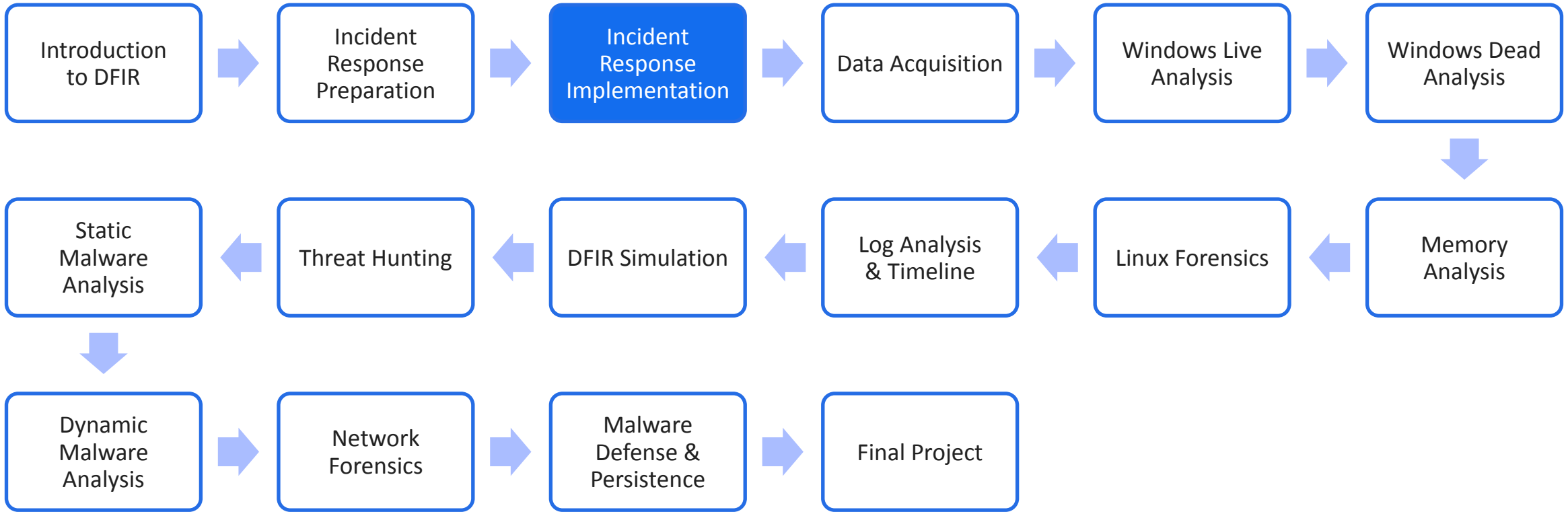
Cybersecurity Professional Program

Incident Response Implementation

Introduction to Digital Forensics
& Incident Response

Digital Forensics & Incident Response

Course Path



Objectives

Learn how to implement incident response procedures by understanding the SOC operation lifecycle, the incident response process, and general practices concerning chain-of-custody (CoC).

- SOC Operation & Lifecycle
- Identification & Scoping
- Containment
- Intelligence Gathering
- Eradication
- Chain-of-Custody

Incident Response Implementation

SOC Operation & Lifecycle

SOC Relationship with IR

- SOC team isn’t responsible for incident handling.
- During an incident, SOC detects the event and notifies the IR team.

Coordination: Who do we talk to?

Management — Establishes response policy, budget, and staffing

Information Assurance — Ensures security controls and policy enforcement

IT Support — IT technical experts

Legal Support — Ensures legal & policy compliance

Public Affairs — Diplomatic communication with the public

Human Resources — Insider threat situations, employees who violate policies

BCP/DR — Works closely and in parallel with IRT

Physical Security — Organization-wide drills regarding facilities

SOC Model Criteria

1. 24x7x365 availability required?
2. Employee morale
3. Cost
4. Expertise
5. Turnover & burnout
6. Decision points
7. Private information & NDA
8. Investment planning
9. Tooling & correlation
10. Training, practice, and exercises

Incident Response Implementation

Identification & Scoping

Importance of Methodology

Methodology
A predefined method of performing an action.

Procedures
Guidelines and instructions.

Incident Uniqueness
Every incident is unique, and procedures may not cover every possibility.

Preparation for Attack Scenarios

- Estimate and prepare to address attack scenarios.
- Enumerate different attack scenarios.
- Test methodology.
- Develop procedures.

Unknown Scenarios
We can't know everything, so experience is always very important!

Attack Scenarios

External Media — Information obtained via USB or external drive

Attrition — Defenses are gradually worn down, brute-force attack

Web — Cross-site scripting

Email — Phishing

Impersonation — Man-in-the-Middle, social engineering

Improper Usage — Violation of acceptable usage policy, disciplinary action by HR

Loss/Theft — Stolen laptop or mobile device

Espionage — Hired employees may be selling company secrets

Incident Detection

Automation & Orchestration
Obtaining a timeline from host and network-based tools.

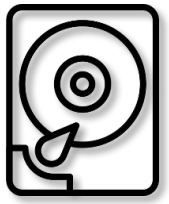
Precursor
Information that indicates an attack may be imminent.

Indicators
Pointers to an incident that may be underway.

Undetected Incidents

Undetected Incidents
Not all incidents are obvious or detected.

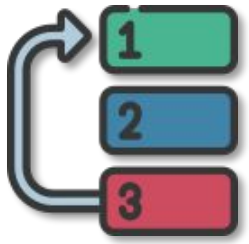
Vigilance
Notice anything out of the ordinary? Do we have the right tools to discover an incident?



Log & Artifact Retention
Long log retention and 3rd party experts.

Incident Analysis & Priority

Incident Analysis
Gather information, determine the incident's scope of impact, produce an initial report.



Prioritize Incidents
Prioritize by function, information sensitivity, and difficulty of recovery.

> Prioritizing Practice: Determine which incident should be handled first.

Lab DFIR-03-L1

Identification & Scoping

20–30 Min

Mission

Prioritize five different incidents according to the order in which they should be addressed.

Steps

- Review the incidents provided in the lab.
- Apply the methodology of function, information, and recovery (FIR).

Environment & Tools

- Text editor

Related Files

- Lab document

Incident Response Implementation

Containment

Containment

Containment
The process of endeavoring to stop the spread of a cyber intrusion.

Scope & Strategy
The scope of the intrusion must be evaluated to apply an effective strategy.

Containment Strategies

Strategy	Definition
Blocklist/Allowlist Filtering	Block or allow a specific IP address range for network access.
Segmentation	Isolate infected networks from uninfected networks (less granular than blacklist/whitelist).
Indicators of Compromise (IoC)	Use and implement patterns of known attacks to prevent attack propagation (e.g. IPS).
Black Holing Shunt	DDoS traffic from a malicious network is dropped.
Email Filtering	Email filter controls updated with signatures/IoCs of phishing emails.
Host Isolation	Disconnect an infected system from the

Should We Sit and Wait?

- Delaying containment is not recommended.
- Be proactive and apply a containment strategy.
- Deception systems help containment and intelligence gathering.
- Apply containment as quickly as possible.

Containment

Lab DFIR-03-L2

Containing an Attack

20–30 Min

Mission

Isolate an infected system.

Steps

- Review ways of disabling access (unplugging) an infected VM.
- Review post-lab notes.

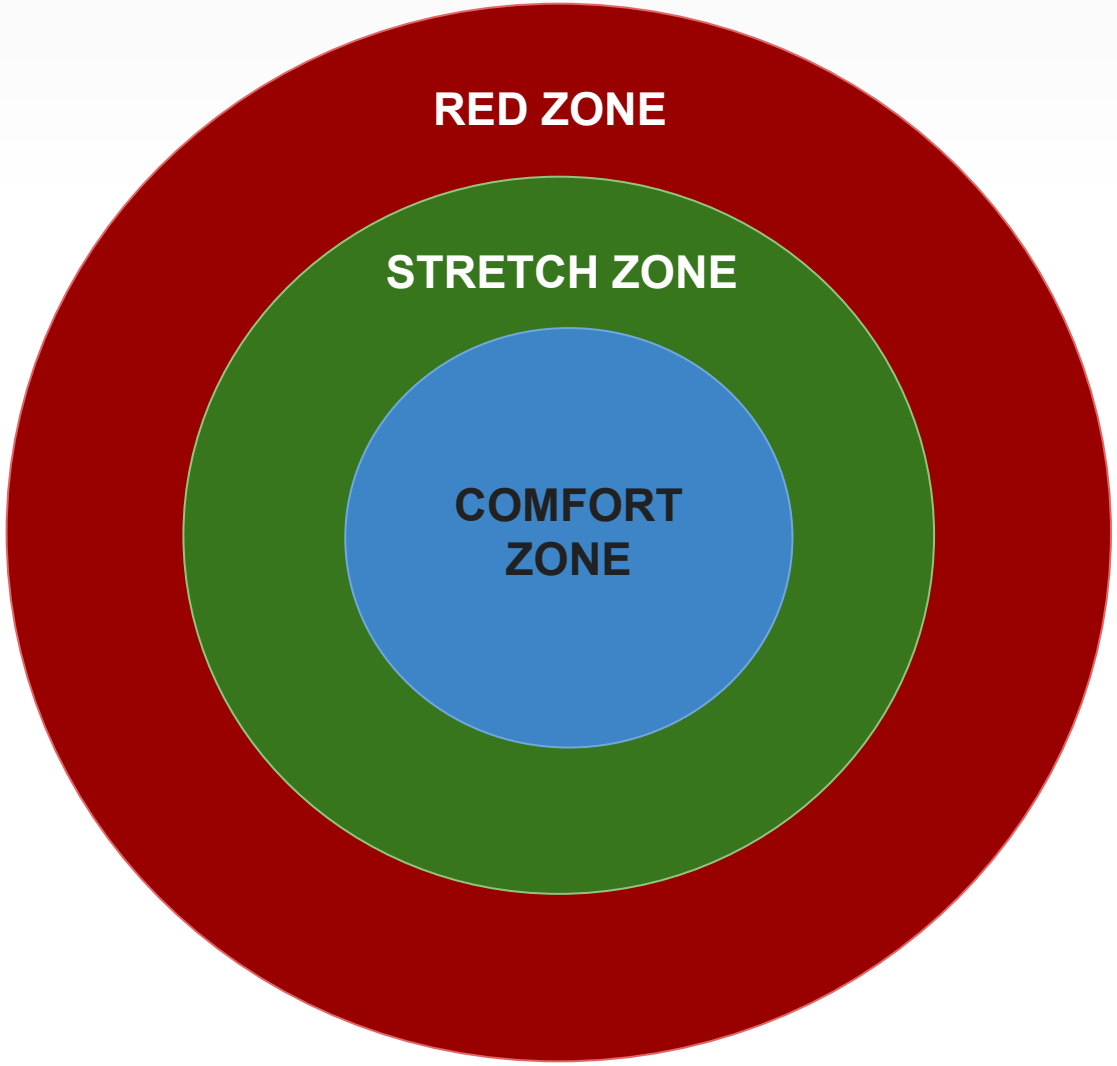
Environment & Tools

- VirtualBox
- Windows 7 VM

Related Files

- Lab document
- Windows 7 OVA

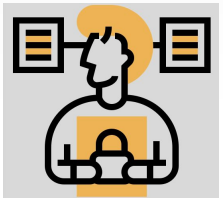
Pulse Check



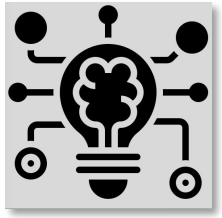
Incident Response Implementation

Intelligence Gathering

Intelligence Gathering



Threat Information
Information that helps understand how an attacker operates to improve protection.



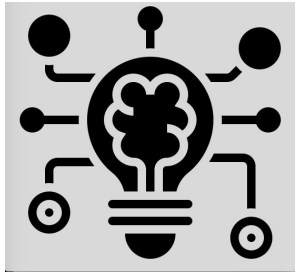
Threat Intelligence
Threat information that is processed and analyzed to devise more effective security measures.

> Threat intelligence is based on threat information and translates it into effective action.

Threat Information

Threat Information	Definition and Example
Precursors	Point to a possible attack – vendor advisories, detection of vulnerability scanner, and recon attempts.
Indicators	Point to a probable attack – malicious files reported in logs.
Tactics, Techniques, Procedures (TTPs)	How an intruder attacks - specific tools, vulnerabilities, botnets, etc.
Security Alerts	Typically sent by logs or SIEM.
Indicators-of-Compromise (IoC)	Evidence of a specific attack.
Protection Profiles	Systems must work with anti-virus apps, patches, and security upgrades.

Threat Intelligence



- Cybersecurity is a team effort.
- Information and threat intelligence must be shared.
- Knowledge must be shared.
- Information sharing and analysis organizations (ISAO) should be consulted.

Threat Intelligence Process

Threat Information

Precursors, IoC, TTPs

Team Review

Teams review threat information

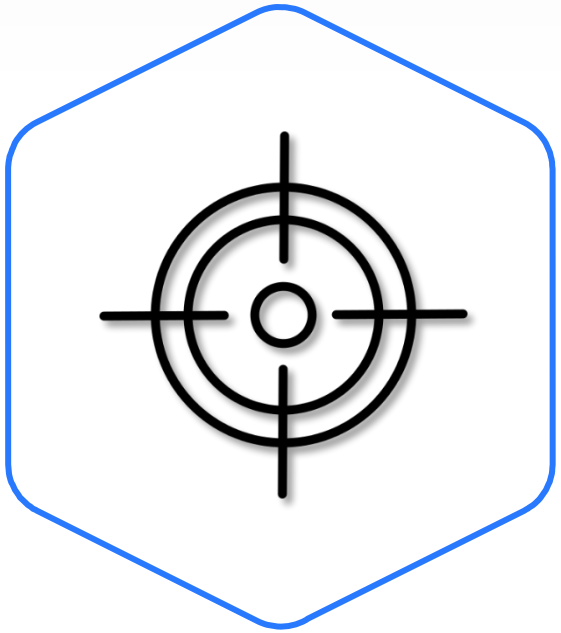
Synthesize & Report

Turn information into action

Threat Intelligence

Distributed to and produced by ISAO

Threat Hunting



- Know your system.
- Know your enemy.
- Proactively search for system IoCs.
- Review logs and other data for evidence and IoCs.
- Share information.

Threat Hunting Process

Knowledge

Know your system, and your enemy

Search

Proactively seek evidence and IoCs

Review

Review logs and data for IoCs

Report

Summarize findings

Sharing

Share threat information with the team

Deception Systems

Moving Target Defense
Diverts attacker resources to decoy systems.

Intelligence Gathering
Enables gathering of TTPs.

> Although significant investment and training is required, the defensive yield will be worth it.

Incident Response Implementation

Eradication

Eradication

- Eradication involves total removal of an intruder.
- First comes evidence gathering and containment.
- Examples: malware destruction, image recovery.

Incident Response Implementation

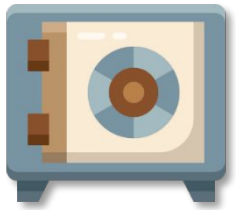
Chain-of-Custody

Chain-of-Custody (CoC)

Chain-of-Custody (CoC)

Critical process.

Document actions pertaining to forensic evidence.



CoC Process

The process is employed in any field in which forensic evidence must be presented in a court of law.

> Any action that involves forensic evidence must be documented, or the bad guys will not be punished.

Chain-of-Custody

CoC Process

Acquisition

Acquire forensic evidence

CoC Form

Bag and tag it!

Evidence Locker

Evidence belongs in a safe!

Check in/out

Who, What, Where, When, Why, How (5W1H)

CoC – The ‘Ws’ and ‘H’ of 5W1H

CoC Form Updates
You must update CoC documentation with detailed information that must be 100% accurate!

W/H	CoC Form Update
Why?	Why was the evidence accessed? (Example: to make a copy)
Where?	What is the location at which the evidence was accessed?
What?	What evidence was accessed? (Example: disk image)
When?	When was the evidence accessed?
Who?	Who handled the evidence?
How?	Method or procedure used to handle the evidence. (Example: disk image procedure)

NIST Sample Chain of Custody Form

Property Record Number: _____

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers.* U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM
(Continued)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)
☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ ID#: _____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian
_____ ID#: _____ to
Name _____
Address: _____ City: _____ State: _____ Zip Code: _____
Telephone Number: (____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers.* U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

Your 5W1H and procedure should be documented in the form.

CoC Form Completion Example

What? Procedure for imaging a disk taken from the safe.

Who? Name and title (Chief Investigator, Bob T.)

Where? 10 Incident Response Way, Hackville, 01010

When? Date and time (beware of time zones!)

Why? How? Analysis (why) Specific procedure (how)

The Procedure in CoC is Crucial

- Forensics experts are careful about details.
- It is important to acquire evidence prior to eradicating a malicious agent.
- Other professionals must be informed of what was done to the evidence via the CoC form.

Thank You

Questions?