Cybersecurity Management
GCS-1.3.Incident Response (IR)

2022-2023

Prof. Raül Roca

raul.roca-canovas@upc.edu

linkedin.com/in/roca-cybersecurity

Objectives

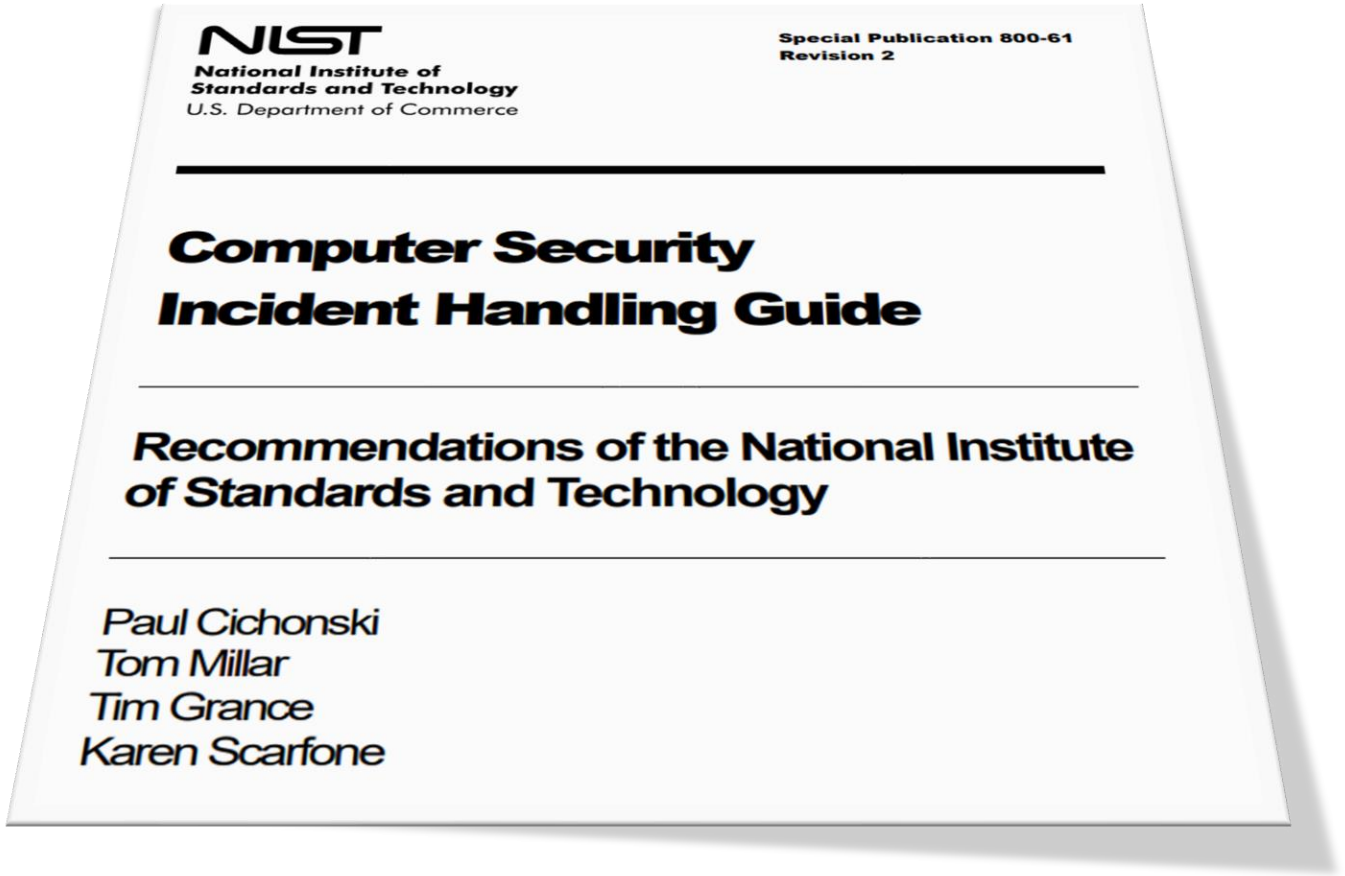
- To know the main concepts and definitions of IR.
- To know what a CSIRT is, how it is created, and what services it offers.
- To know the different phases of an incident response process.
- To know the primary forms to manage in an incident response process.
- To practice, using an example, a simulation of a IR.

Contents

- IR. Concepts & Definitions
- CSIRT
  - Creation
  - Services
- Incident Handling (or IR) Process
  - Preparation phase
  - Detection & Analysis phase
  - Containment, Eradication & Recovery (C,E&R) phase
  - Post-Incident Activity
- IR Forms
- Exercise: DDoS incident

IR. Concepts & Definitions

NIST Special Publication 800-61 Revision 2



For more information, please refer to Computer Security Incident Handling Guide by NIST.

Incident Response (IR). Definition

- Well-defined course of action whenever a computer or network security incident occurs.
- **NIST*→** only events with negative consequences are considered security incidents:
  - System crashes
  - Packet floods
  - Unauthorized use of system privileges
  - Unauthorized access to sensitive data
  - Execution of destructive malware
- IR. Scope
  - ***Incident handling is not only about intrusions!***
    - Malicious insiders, availability issues and loss of intellectual property all fall under the scope of incident handling as well.
- **Incident Response = Incident Handling**

**the Computer Security Incident Handling Guide by NIST*

Computer Security Incident Response Team (CSIRT)

CSIRT (CERT or IR Team). Definition

- NIST
  - *“An incident response team (IRT), also known as a Computer Security Incident Response Team (CSIRT) is responsible for providing incident response services to part or all of an organization.”*
- The IRT
  - Receives information on possible incidents
  - Investigates them
  - Takes action to ensure that the damage caused by the incidents is minimized.

CSIRT. Creation

- What services do we offer?
- Here?
  - From where? Where? When?
  - Where are we
  - Schedule / Time slots?
- How do we finance ourselves?
- Applicable regulations → http://escert.upc.edu/rfc-2350
- Forums International reference: TF-CSIRT, FIRST.org
- Dedicated or part-time team?
- Who?
- Centralized or distributed equipment?
- Resources: Humans + Technicians
- Skills of the members
- Contacts: TI-TERENA, FIRST, CSIRT.es ...

CSIRT. Services.

Service Categories

Reactive Services	Proactive Services	Security Quality Management Services
• Alerts and Warnings • **Incident Handling** • Artifact Handling	• Announcements • Technology Watch • Security Audits or Assessments • Configuration and Maintenance of Security Tools, Applications, and Infrastructures • Development of Security Tools • Intrusion Detection Services • Security-Related Information Dis-semination	• Risk Analysis • Business Continuity and Disaster Recovery Planning • Security Consulting • Awareness Building • Education/Training • Product Evaluation or Certification
• *Are triggered by an event or request, such as a report of a compromised host, widespread malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system.* • ***Core component** of CSIRT work.*	• *Provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events.* • *Performance of these services will directly reduce the number of incidents in the future.*	• *Augment existing and well-established services that are independent of incident handling and are traditionally performed by other areas of an organization such as the IT, audit, or training departments.*

CSIRT. Services.

Service Categories. Reactive Services

- Designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems.
- Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

Reactive Services

- **Alerts and Warnings**
- **Incident Handling**
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
  - Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- **Artifact Handling**
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

CSIRT. Services.

Service Categories. Proactive Services

- Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

Proactive Services

- **Announcements**
- **Technology Watch**
- **Security Audits or Assessments**
- **Configuration and Maintenance of Security Tools, Applications, and Infrastructures**
- **Development of Security Tools**
- **Intrusion Detection Services**
- **Security-Related Information Dissemination**

CSIRT. Services.

Service Categories. Security Quality Management Services

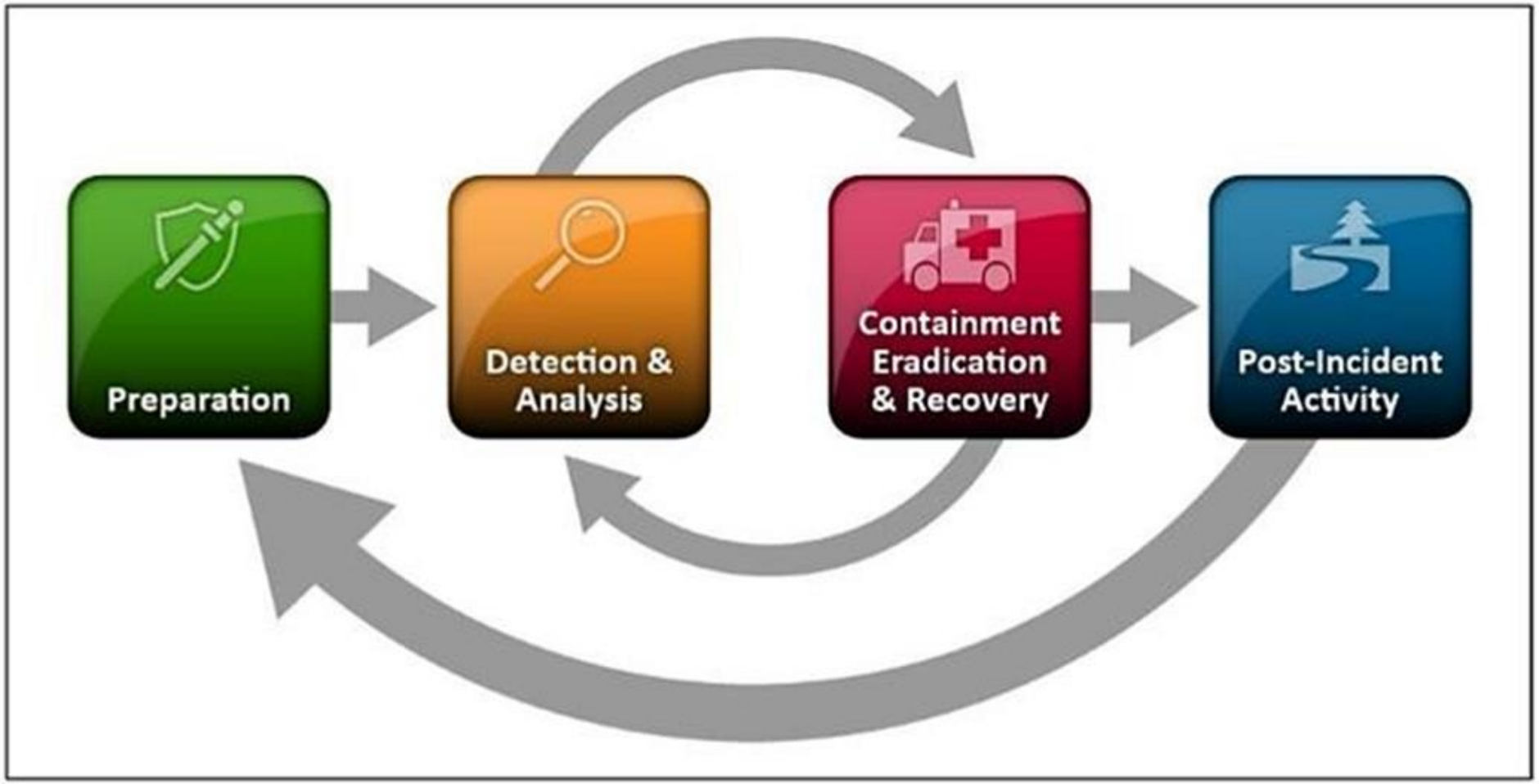
- Services designed to improve the overall security of an organization.
- By leveraging the experiences gained in providing the reactive and proactive services.
- These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks.

Security Quality Management Services

- **Risk Analysis**
- **Business Continuity and Disaster Recovery Planning**
- **Security Consulting**
- **Awareness Building**
- **Education/Training**
- **Product Evaluation or Certification**

Incident Handling (or IR) Process

IR. The 4 phases or *"The IR life cycle (IRLC)"*



IRLC. Preparation phase

IRLC. Preparation phase

- Includes everything related to an organization's IR readiness.

Employees	Documentation	Defensive Measures
• A Skilled Response Team • IT Security Training • Security Awareness/Social Engineering Exercises, etc.	• Well-defined policies • Well-defined response procedures • Maintaining a chain of custody of actions	• A/V, (H)IDS, DLP, EDR, Security Patches • SIEM, UTM, Threat Intelligence • NSM, Central Logging, Honeypots, etc.

IRLC. Preparation phase.

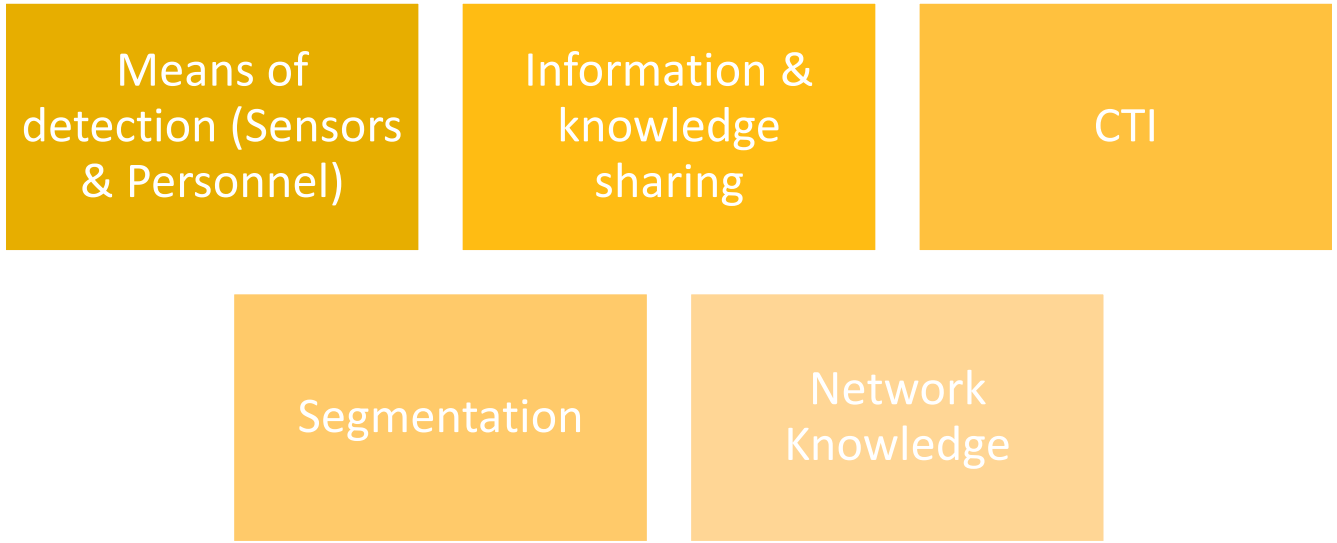
Key Points

- Multi-disciplinary team
- Determine minimum time to respond.
- Access to systems capabilities
- Establish a SPOC & reporting capabilities
- IR Starter Kit https://mediacenter.ibm.com/id/1_8a1usll7

IRLC. Detection & Analysis phase

IRLC. Detection & Analysis phase

- Includes everything related to detecting an incident:



IRLC. Detection & Analysis phase.

Key Points

- Assign a Primary Incident Handler
- Establish trust and effective information sharing
- Safeguard information sharing
- Establish levels of detection by logically categorizing your network
- Establish baselines, extend visibility, and know your limits:

IRLC. Detection & Analysis phase.

Damage-estimation questions

- Have we identified the impact of vulnerability exploitation?
- Are there any crown jewels that can be affected?
- What are the minimum requirements for effective exploitation?
- Is this being actively exploited in the wild?
- Is there a proposed remediation strategy?
- Is there threat intel/evidence that suggests increased spreading capabilities?

IRLC. Containment, Eradication & Recovery (C,E&R) phase

IRLC. C,E&R phase

- Includes everything related to

Containment	Eradication	Recovery

• Preventing an incident from getting worse
• Subphases
  • Short-Term Containment
  • System Back-Up
  • Long-Term Containment
	• Eliminating intruder artifacts
	• Understanding the root cause
	• Attack vectors & TTPs
		• Restoring
		• Monitoring

IRLC. C,E&R phase.

Before Containment. Very first steps

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:

IRLC. C,E&R phase.

Before Containment. Incident Classification

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:
  - **Type**

Denial of Service
External Exploitation
Internal Exploitation
Information Leakage
Malware
Malicious Email

IRLC. C,E&R phase.

Before Containment. Incident Classification

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:
  - Type
  - **Impact**

Incident affecting critical system(s)
Incident affecting non-critical system(s)
Incident affecting asset that requires no immediate investigation

***Impact is tightly connected with the Response Time*.**

IRLC. C,E&R phase.

Before Containment. Incident Classification

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:
  - Type
  - Impact
  - **Extend**

- Extensive compromise, including sensitive customer information
- Manageable intrusion and spreading
- Immediately detected or easily contained intrusion

Extent is tightly connected with the escalation level. For example, should the CISO's office or upper management be informed?

IRLC. C,E&R phase.

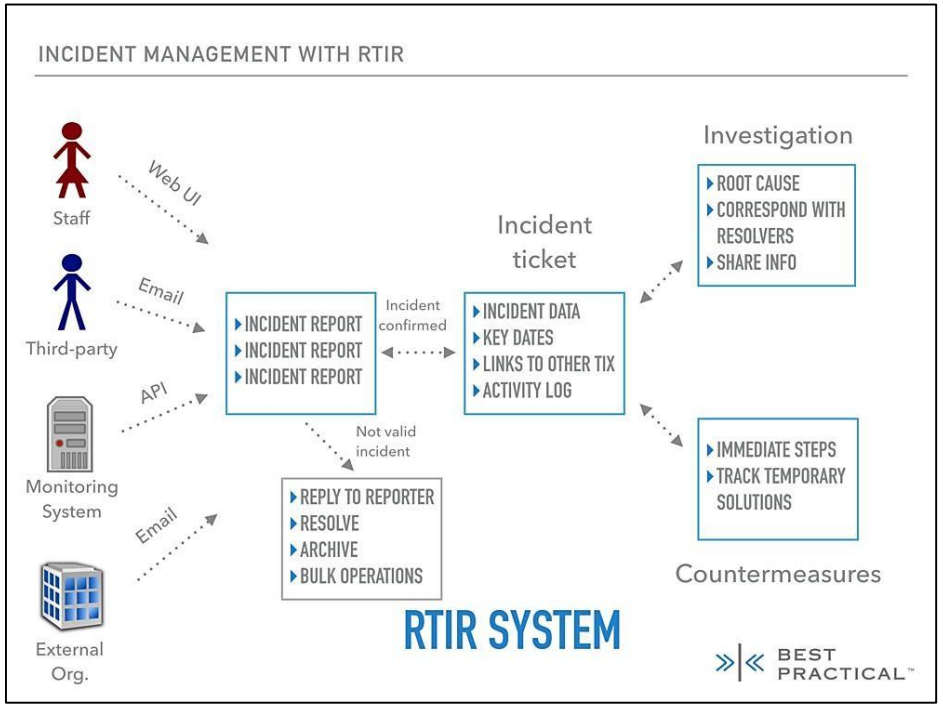
Before Containment. Incident Communication

- Senior management member
  - CIO/CISO/head of the legal dept., etc.
  - Escalating or help
  - Should be the first upper management individual who will be informed of an incident and provided with notes from the first responder.
- The communication flow should include
  - Security + Management (people) → affected business units will be informed

IRLC. C,E&R phase.

Before Containment. Incident Tracking Mechanism

- Handle multiple incidents
- Incident reporting mechanism
  - All tickets for the same incident.
- Example Tool
  - Request Tracker for Incident Response (RTIR)

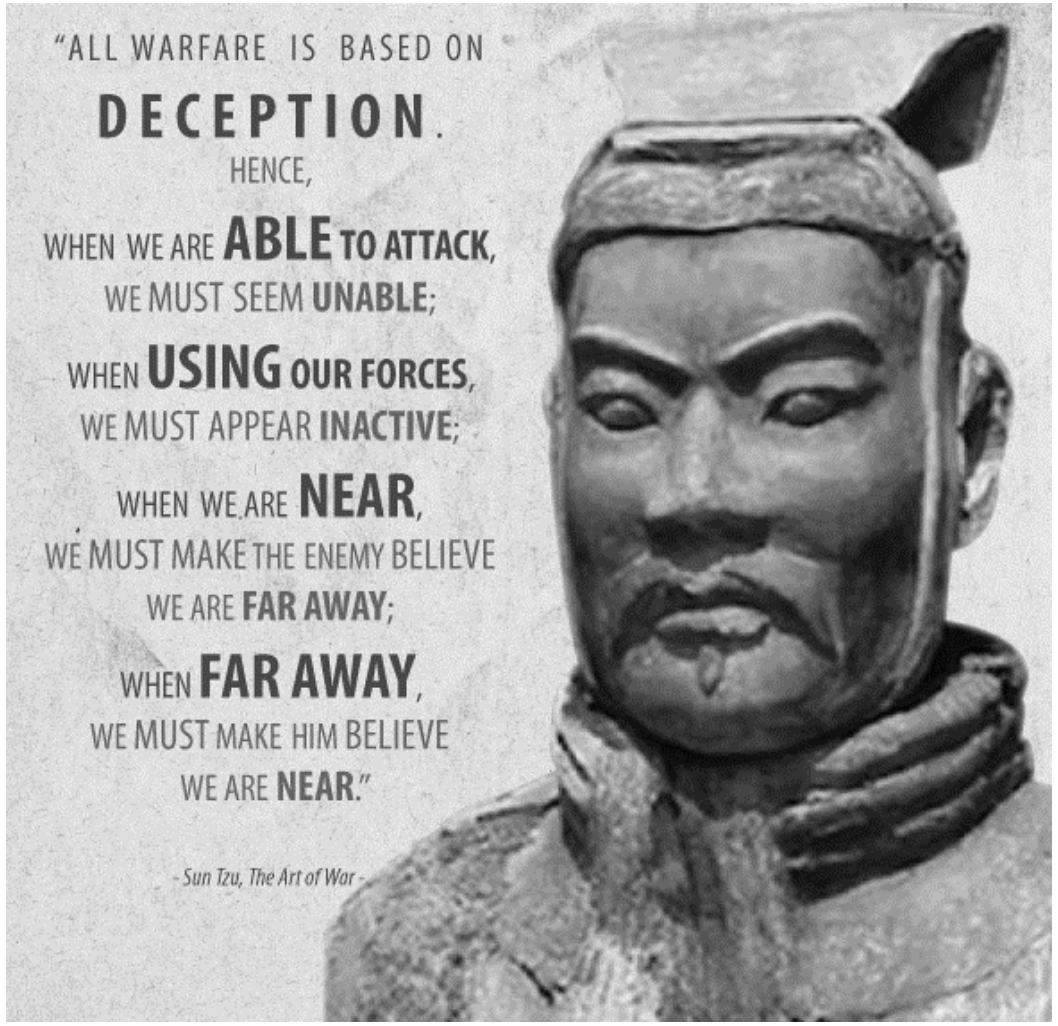


IRLC. C,E&R phase.

Before Containment. Low profile

- We should be
  - extremely careful
  - not to let the adversaries now our operations
  - no uploading binaries to cloud
  - no interacting infrastructures

- Act normally…



IRLC. C,E&R phase.

Containment. Subphases

- Containment is divided into the following subphases:
  - Short-term Containment
  - System Back-up
  - Long-term Containment

IRLC. C,E&R phase.

Containment. Short-term Containment

- Eliminate intrusion → without erasing tracks
- Actions
  - Isolated VLAN → White Network
  - Change DNS
  - Isolate the machine
  - Report to and seek permission from the business unit manager

IRLC. C,E&R phase.

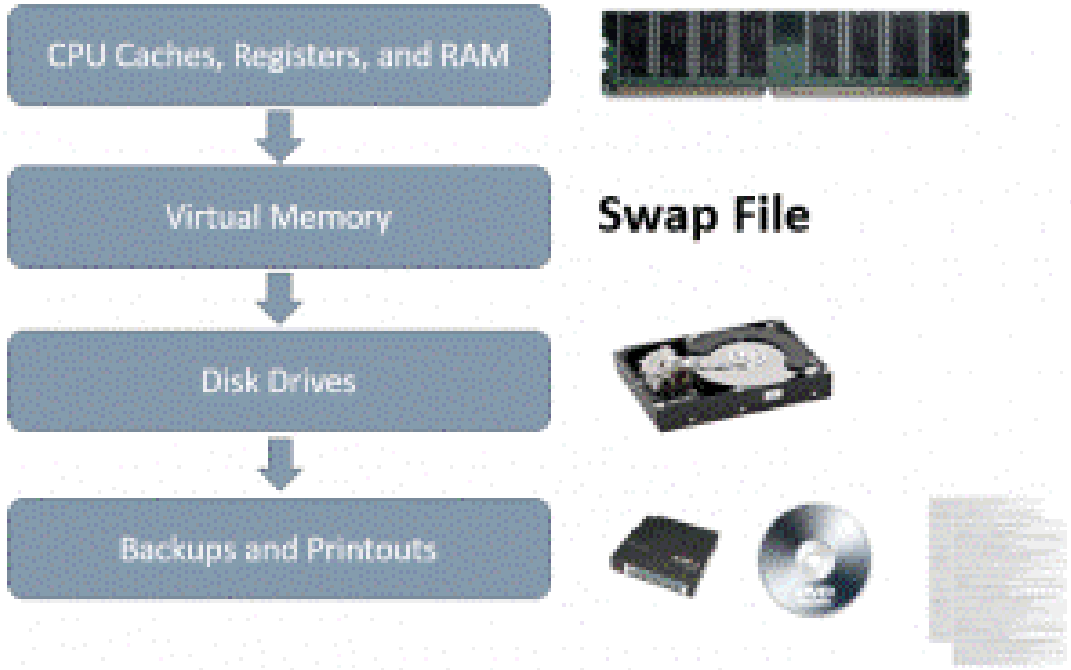
Containment. System Back-Up

- The next step is to make images of the affected system(s) for forensics activities.
- Before we go deeper into imaging, there is an important note to remember.

IRLC. C,E&R phase.

Containment. System Back-Up. Data Acquisition (DA)

- Preservation of evidence
  - → working with images
- Original image (oi)
  - saved
  - work with copies of the oi
- Data acquisition
  - → **order of volatility**
    - RAM → VMEm → ..



IRLC. C,E&R phase.

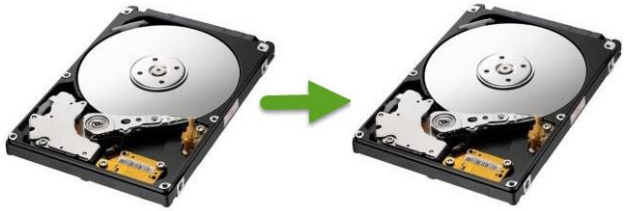
Containment. System Back-Up. DA. Types

- **Static Acquisition**
  - No volatile data (hard disks, flash disks).
- **Dynamic / Live Acquisition**
  - Volatile data.
  - Performed while a system is still powered on
  - RAM → find stored passwords, messages, domain names and IP address, etc …
  - Can also exist on disk → paging, temporary files, and even log files.
  - OS cannot be entirely trusted → rootkits
- Choosing which technique to apply depends on data volatility and the incident

IRLC. C,E&R phase.

Containment. System Back-Up. DA. Approaches

1. Cloning: Disk drive → disk drive

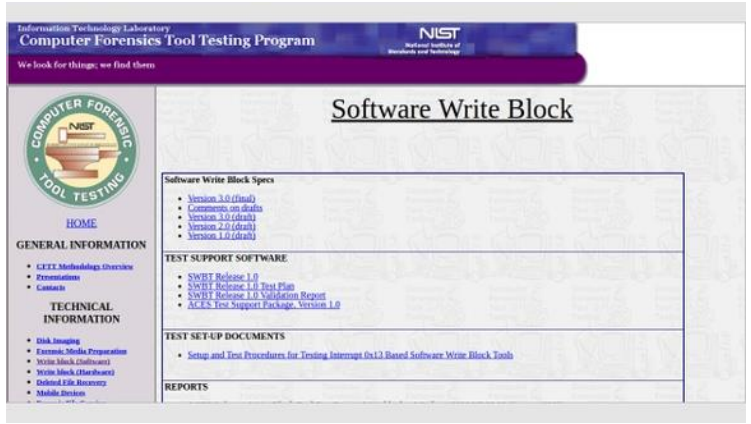


2. Imaging: Disk drive → image file
   - Mirrors the under investigation hard disk's content into an image file
   - Imaging a drive creates → "**forensic image**"
   - Scalability & Efficiency!

IRLC. C,E&R phase.

Containment. System Back-Up. DA. Write Blockers

- Risk
  - altering the original evidence
- Tools/software
  - acquiring data in a safer manner.
  - Write Blockers
    - achieve this by blocking the HD from writing.
  - Types
    - hardware-based or software- based.



IRLC. C,E&R phase.

Containment. Long-term Containment

- Before
  - Communicating with your ISP (DDoS attacks, worms, or phishing campaigns)
  - If you are not still able to determine the attacker's actions or even motives
    - Leaving the machine intact and closely monitor the attacker's next moves
  - Ensure that image and live acquisition activities have been completed.
  - The containment approach should first go through the respective **business unit manager (BUM)**.
    - Critical systems can't easily go down since they are related to core business processes or operations.
- If BUM agreed on taking the system down
  - Eradication phase = eliminate every attacker-related actions and residuals.
- If the affected system should stay as is → it's time for long-term containment

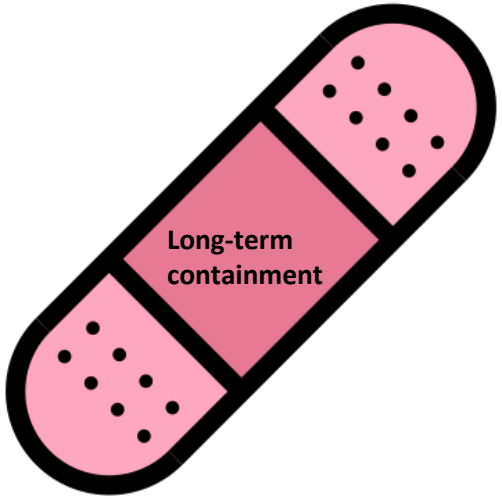
Affected & related system patching	(H)IDS insertion	Passwords and trusts changes	Additional ingress/egress rules (router & firewall)	Drop packets associated with a source or destination identified in the incident	Eliminate attacker access etc.

***Remember*: Keep administrators and business unit managers/representatives in the loop!**

IRLC. C,E&R phase.

Eradication.

- Long-term containment = a band-aid
- Eradication
  - to make sure the attacker is locked out
  - to identify the root cause and indicators of the incident.
    - Use information from the **Detection & Analysis** and **Containment**
  - to isolate the intrusion and identify the **attack vector**.
  - Drive-wiping before doing anything else.
    - ***Reformatting and reinstalling the OS or identifying a clean backup and reloading the data ONLY is a bad strategy!***



IRLC. C,E&R phase.

Eradication.Important phases

- Eliminating attacker residuals
  - Removing malware (backdoors, rootkits, malicious kernel-mode drivers, etc.)
  - Identify credential reuse (Remote Desktop, SSH, VNC, etc.)
- Improving defenses
  - Configuring additional router & firewall rules
  - Obscuring the affected system’s position
  - Null routing (DDoS)
  - System hardening, patching, and vulnerability assessment procedures, etc.

IRLC. C,E&R phase.

Recovery.

- Recovery → we will bring the affected systems back to production.
- Key points to consider are:
  - Process System Recovery
  - Restore of Operations
  - Monitoring

IRLC. C,E&R phase.

Recovery. Process System Recovery

- Once the affected system is restored, ask **the business unit** to
  - perform QA activities to ensure the system's running condition.
  - ensure the system includes everything needed for their operations.

IRLC. C,E&R phase.

Recovery. Restore of Operations

- A decision has to be made regarding when the restored system will enter production again.
- Consult/coordinate with the business unit for this matter.

IRLC. C,E&R phase.

Recovery. Monitoring

- Once the restored system is back to production:
  - Backdoors may still exist!
  - IDPS & HIDS → signs/patterns/signatures related to the original attack.
  - Analyze critical logs and events → signs of re-infection or re-compromise.
  - What to look for during the weeks (or even months) to come:
    - Changes to registry keys and values.
    - Abnormal processes
    - Abnormal user accounts.

IRLC. Post-Incident Activity

IRLC. Post-Incident Activity

- Right after recovery, the IRT should start constructing an objective, accurate and thorough **report** regarding the **lessons learned** from IR.
  - Identified weaknesses, oversights, and blind spots
  - Working processes and successful detection methods should also be included.
  - Don’t be afraid to mention how effective you were against specific stages of the attack.
- Schedule a meeting to discuss this report with all involved parties
  - System administrators, affected business unit representatives, IT security team, etc.
- Focus your energy on improving your processes, technological measures and **visibility**.

IR Forms

IR Forms

- There are IR Forms, which will come in handy during incident handling. Let’s look at some important forms you should preprint and use.
  - **Incident Contact List**
  - **Incident Detection**
  - **Incident Casualties**
  - **Incident Containment**
  - **Incident Eradication**

IR Forms.

Incident Contact List

- This form should contain the contact details of the organization’s:
  - CISO / CIO
  - SPOC of the incident handling or CSIRT team
  - Legal department contact
  - Public relations contact
  - ISP SPOC
  - Local cybercrime unit etc.

IR Forms.

Incident Detection

- This form should contain information such as:
  - The first person who detected the incident
  - The incident’s summary (type of incident, incident location, incident detection details, etc.)

IR Forms.
Incident Casualties

- This form should contain information such as:
  - Location of affected systems
  - Date and time incident handlers arrived
  - Affected system details (one form per affected system is advised)
    - Hardware vendor
    - Serial number
    - Network connectivity details
    - o Host Name | IP Address | MAC Address

IR Forms.
Incident Containment

- This form should contain information such as:
  - Isolation activities per affected system
    - Was the affected system isolated?
      - Date and time the system was isolated
      - Way of system's isolation
  - Back-up activities per affected system
    - Handler who performed the restoration
    - Back-up details etc.

IR Forms.

Incident Eradication.

- This form should contain information such as: (one form per affected system is advised)
  - Handler(s) performing investigation on the system
  - Was the incident’s root cause discovered?
    - Incident root cause analysis
  - Actions taken to ensure the incident’s root cause was remediated and the possibility of a new incident eliminated

Exercise: DDoS incident

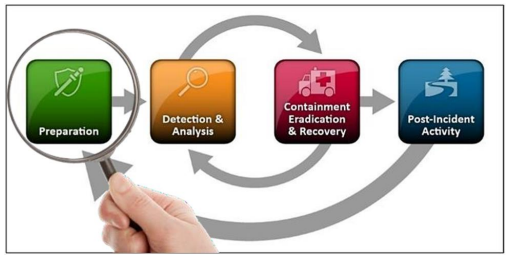
IR. DDoS

What is a DDoS attack?

https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

IR. DDoS.

Preparation



- **Objective**: Establish contacts, define procedures, and gather information to save time during an attack.
- **Actions**
  - ISP
  - Inventory
  - Network infrastructure
  - Internal contacts

The "preparation" phase is to be considered as the most important element of a successful DDoS incident response!

IR. DDoS.

Detection & Analysis

- **Objective**: Detect the incident, determine its scope, and involve the appropriate parties.
- **Actions**
  - Analyze the attack
  - Involve internal and external actors
  - Check the background

IR. DDoS.

Containment, Eradication & Recovery

Containment	Eradication	Recovery

• **Objective**
  • Mitigate the attack's effects on the targeted environment.
• **Actions**
  • Bottleneck?
  • Block DDoS traffic?
  • Blackhole Routing?
  • Alternate communication channel between you and your users/customers
  • Extortion? Try to buy time
	• **Objective**
	  • Take actions to stop the Denial of Service condition.
	• **Actions**
	  • Filtering (if possible at level Tier1 or 2)
	  • Traffic scrubbing/Sinkhole/Clean-pipe
	  • Blackhole Routing
		• **Objective**:
		  • Come back to the previous functional state.
		• **Actions**
		  • Assess the end of the DDoS condition
		  • Rollback the mitigation measures

IR. DDoS.

Post-Incident Activity

- **Objective**
  - Document the incident's details, discuss lessons learned, and adjust plans and defenses.
- **Actions**
  - Consider what preparation steps you could have taken to respond to the incident faster or more effectively.
  - If necessary, adjust assumptions that affected the decisions made during DDoS incident preparation.
  - Assess the effectiveness of your DDoS response process, involving people and communications.
  - Consider what relationships inside and outside your organizations could help you with future incidents.
  - Collaborate with legal teams if a legal action is in process.

References

Links

- *https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/software*
- *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*
- *RFC-2350: http: //escert.upc.edu/rfc-2350*
- *https://www.trusted- introducer.org/directory/teams/escert-upc.html*
- *https://first.org/members/teams/escert-upc*
- *https://www.csirt.es/index.php/es/objetivos*
- *https://ciberseguretat.gencat.cat/ca/funcio-i- serveis/resposta-incidents/*
- *https://www.ccn-cert.cni.es/gestion-de- incidentes/directrices-para-la-gestion-de- incidentes.html*
- *https://www.misp-project.org/*

Links

- *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*
- *https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*
- *https://www.wireshark.org/*
- *http://www.dmi.unipg.it/bista/didattica/sicurezza-pg/seminari2008-09/seminario_neri/seminario_neri.pdf*
- *http://www.iana.org/assignments/service-names-port-numbers/service-names-port- numbers.xhtml*
- *https://www.speedguide.net/ports.php*
- *https://docs.microsoft.com/en-us/azure/security/azure-log-audit*
- *https://www.first.org/resources/guides/csirt_case_classification.html*
- *https://bestpractical.com/rtir/*
- *https://github.com/meirwah/awesome-incident-response#incident-management*

Links

- *http://canarytokens.org/generate*
- *https://docs.microsoft.com/en-us/sysinternals/downloads/procmon*
- *http://www.chkrootkit.org/*
- *https://github.com/Tripwire/tripwire-open-source*
- *https://sourceforge.net/projects/aide/*
- *https://medium.com/@esmerycornielle/memory-management-paging-43b85abe6d2f*
- *https://www.heficed.com/kb/security/what-is-a-null-route/*
- *https://www.commandlinefu.com/commands/browse*
- *https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns*
- *https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer*