#CyberSBC2024

Basics of Incident Management

July 8 - 18, 2024

Leon, Spain

Organized by:

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

With the collaboration of:

Canadá

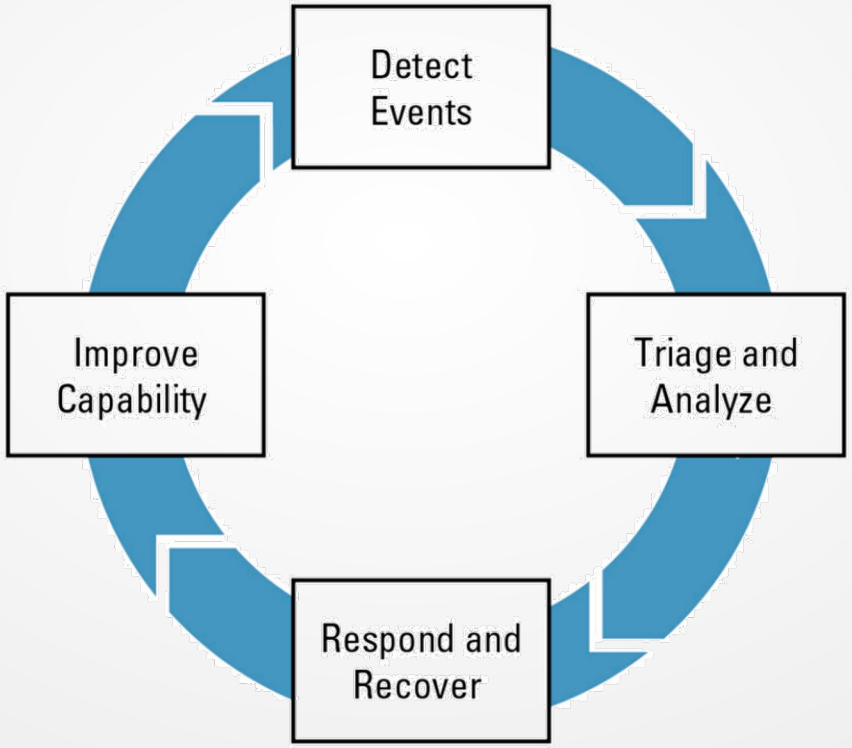
AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

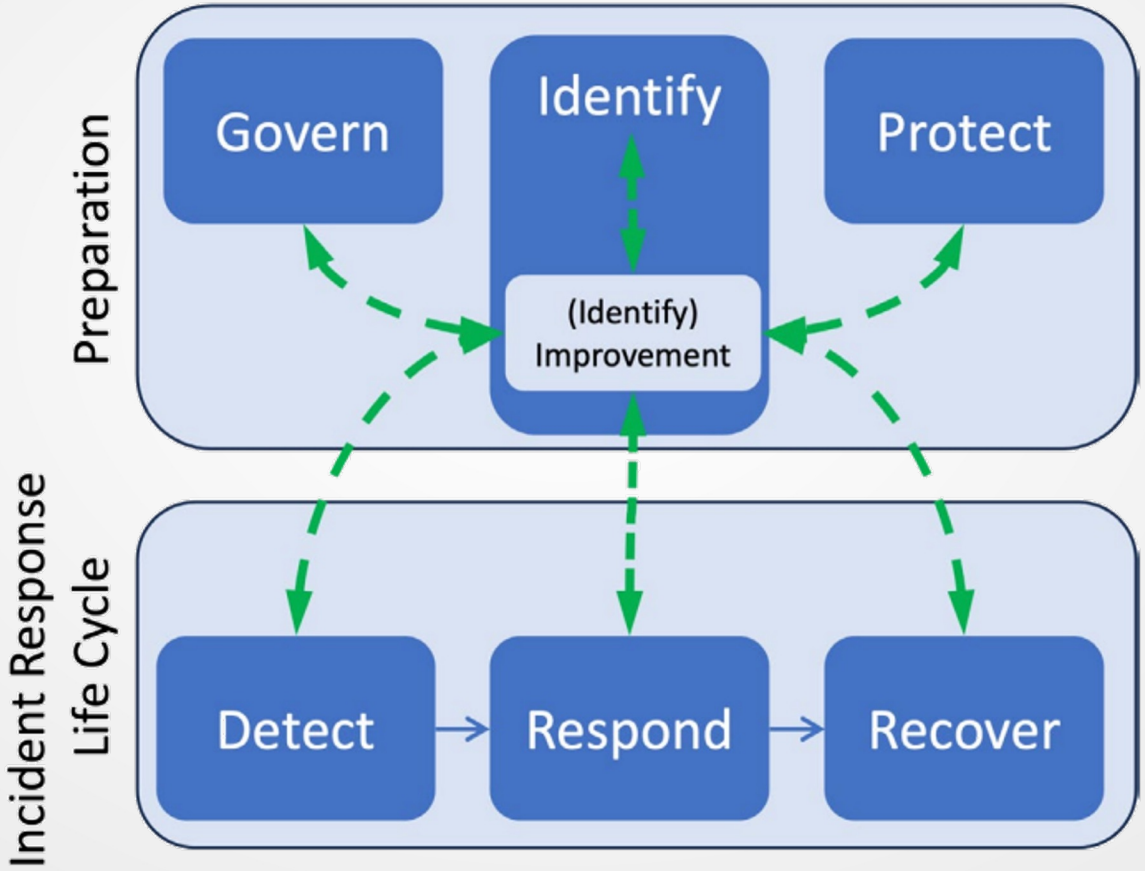
universidad de León

Incident Response Lifecicle

Incident Response (IR) Lifecycle



Incident Response (IR) Lifecycle



Incident Response (IR) Lifecycle

Previous Incident Response Life Cycle Phase	CSF 2.0 Functions
Preparation	Govern Identify (all Categories) Protect
Detection & Analysis	Detect Identify (Improvement Category)
Containment, Eradication & Recovery	Respond Recover Identify (Improvement Category)
Post-Incident Activity	Identify (Improvement Category)

Incident Response Lifecycle

Preparation

- Incident handler communications and facilities
- Incident analysis hardware, software, and resources
    - Backup devices
    - Removable media
    - Portable printers
    - Digital forensic software
    - Packet sniffers
    - Evidence storage bags
    - Port lists
    - Current baselines
    - Network diagrams
- Incident Mitigation Software

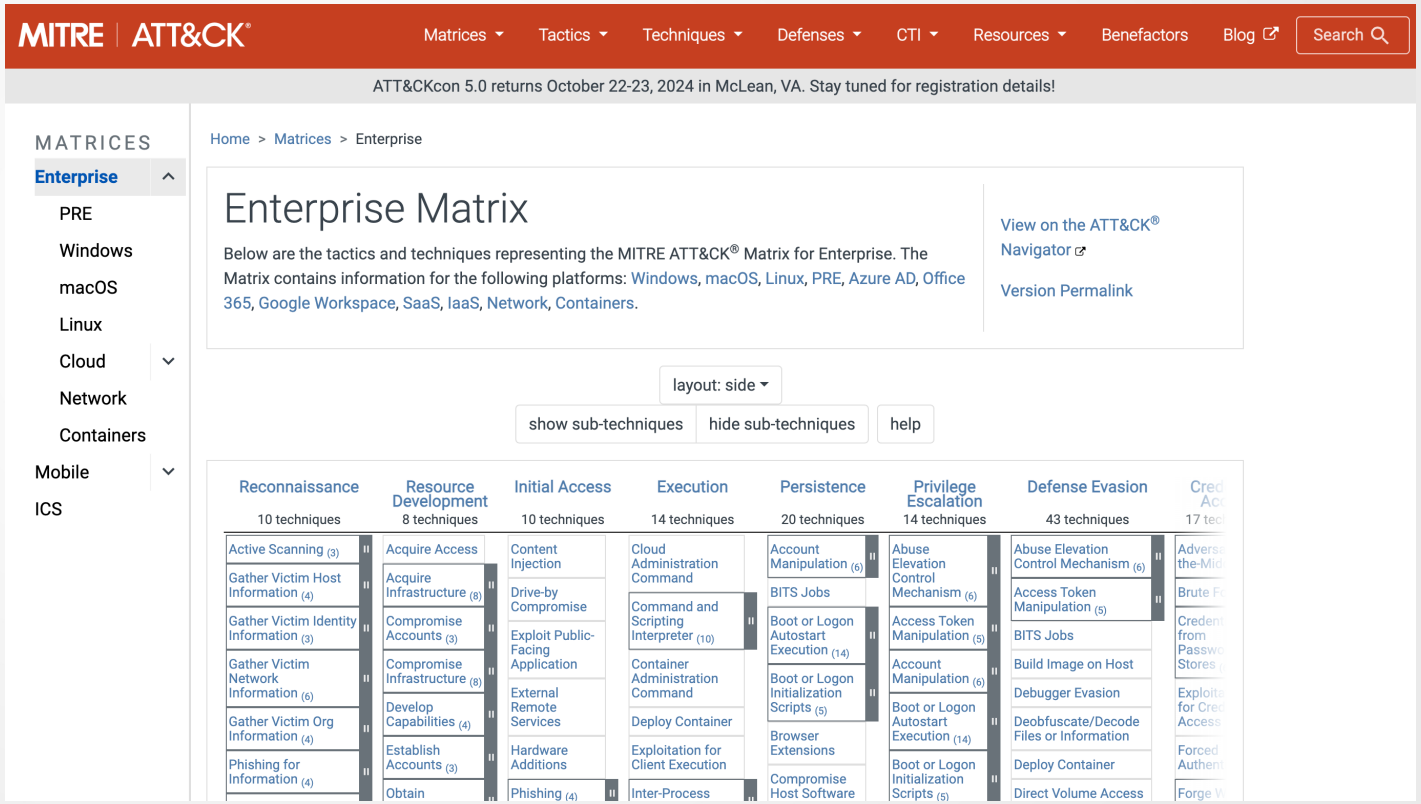
Incident Response Lifecycle

Detection and Analysis

- Classify attacks based on the attack vector
    - External media
    - Cloud
    - Web
    - Email
    - Impersonation
    - Improper usage
    - Equipment loss or theft
    - Other

Incident Response Lifecycle

Detection and Analysis



Organized by:

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

With the collaboration of:

Canada

AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

universidad de León

Incident Response Lifecycle

Detection and Analysis

- Detect signs of an incident
    - Alerts from your antivirus software or network intrusion detection sensor
    - Filenames with unusual characters
    - Evidence of auditing configuration changes
    - Failed login attempts from unfamiliar remote systems
    - Variations from normal network traffic

Incident Response Lifecycle

Detection and Analysis

- Analyze Incidents
  - Establish network and system profiles
  - Study normal behaviors
  - Retain logs
  - Correlate events across logs
  - Synchronize host clocks
  - Keep a knowledge base
  - Research unusual activity online
  - Use packet sniffers
  - Filter data
  - Get external help as needed

Incident Response Lifecycle

Detection and Analysis

- Document Incidents
- Prioritize Incidentes
- Notify Relevant individuals
    - Incident response team (internal or external)
    - Chief information officer (CIO)
    - Chief technology officer (CTO)
    - Chief information security officer (CISO) and other information security leaders
    - System owner
    - Public affairs department
    - Legal department
    - Law enforcement
    - Local CERT

Incident Response Lifecycle

Containment, eradication, & recovery

- Choose a containment strategy
  - Possibility of resource damage and theft
  - Evidence preservation
  - Service availability
  - Necessary time and resources
  - Effectiveness
  - Duration
- Gather Evidence
- Identify Attacking Host

Incident Response Lifecycle

Containment, eradication, & recovery

- Erradicate the threat and recover
  - Restore from clean backups
  - Rebuild systems
  - Replace compromised files
  - Install patches
  - Change passwords
  - Enhance network perimeter security

Incident Response Lifecycle

Post Incident activity

- Lessons learned
- Put together a follow-up report
- Share incident data
- Retain Evidence

-

NICE Skills and Knowledge for IR

NICE Skills and Knowledge for IR

Incident Response

https://niccs.cisa.gov/workforce-development/nice-framework/work-role/incident-response

Cybersecurity Summer Bootcamp

LEON - 2024

July 8 - 18, 2024

Leon, Spain

#CyberSBC2024

incibe.es/en/events/summer-bootcamp

Organized by:

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

With the collaboration of:

Canada

AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

universidad de León