

#CyberSBC2024

Basics of Incident Management

Cybersecurity
Summer
Bootcamp



LEON - 2024

July 8 - 18, 2024

Leon, Spain

Organized by:



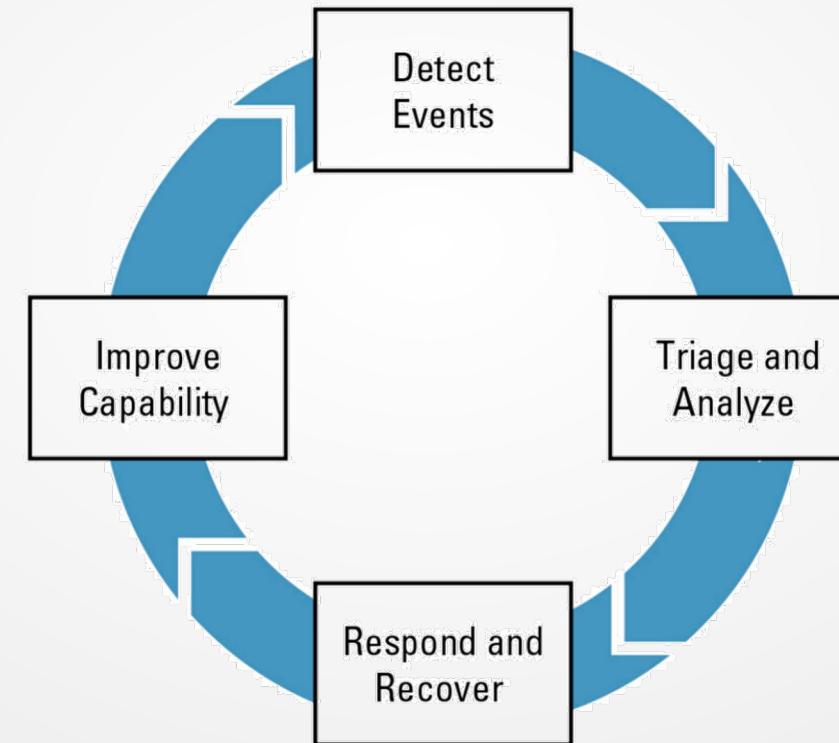
With the collaboration of:



Incident Response Lifecicle



Incident Response (IR) Lifecycle



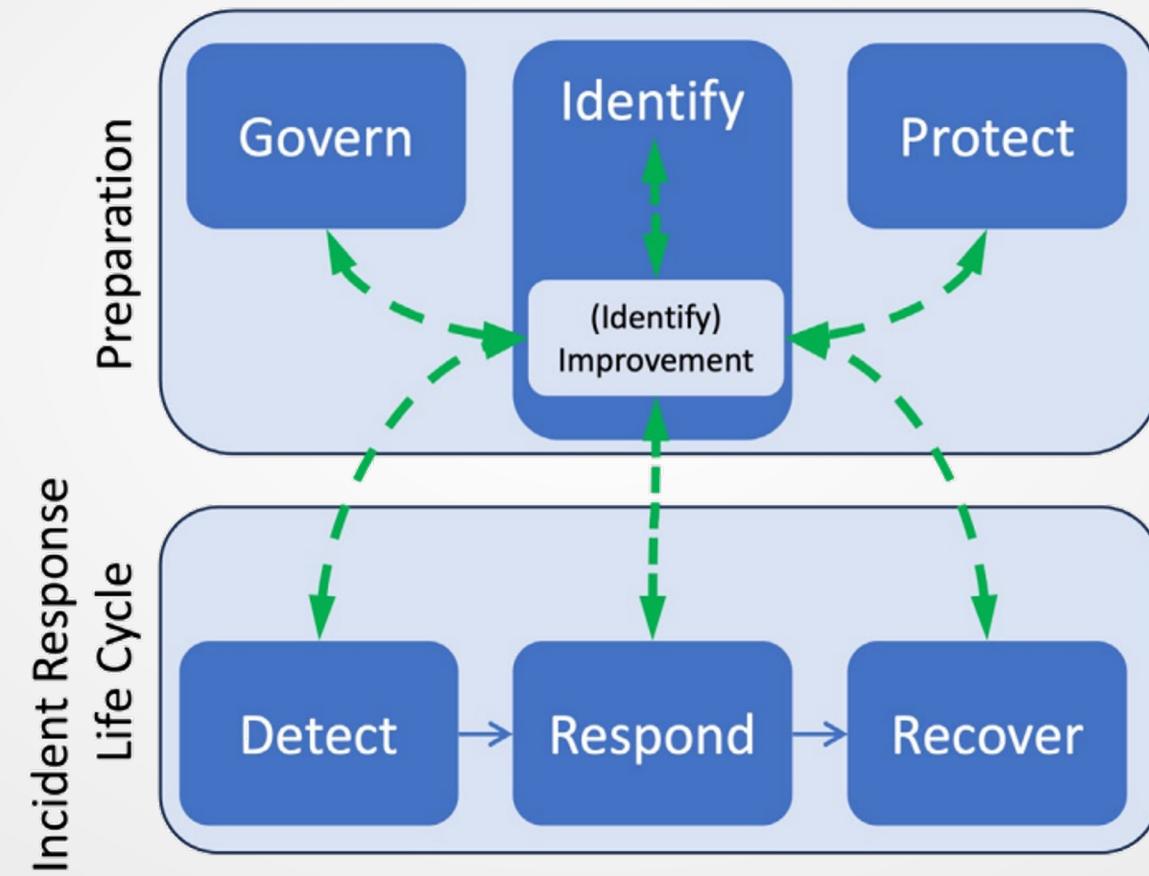
Organized by:



With the collaboration of:



Incident Response (IR) Lifecycle



Organized by:



With the collaboration of:

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)

Organized by:



With the collaboration of:



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

Organized by:



With the collaboration of:



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

Organized by:



With the collaboration of:



Incident Response Lifecycle

Detection and Analysis

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog ▾ Search ▾

ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. Stay tuned for registration details!

Home > Matrices > Enterprise

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator ↗ Version Permalink

layout: side ▾ show sub-techniques hide sub-techniques help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Cred Ac
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 tec
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (2)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Build Image on Host	Build Image on Host	Credentials from Password Stores (1)
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Account Manipulation (6)	Debugger Evasion	Deobfuscate/Decode Files or Information	Exploits for Credential Access (1)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Autostart Execution (14)	Deploy Container	Direct Volume Access	Forced Authentication (1)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process	Compromise Host Software	Forge V		
	Obtain						

Organized by:



With the collaboration of:



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

Organized by:



With the collaboration of:



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

Organized by:



With the collaboration of:



Incident Response Lifecycle

Detection and Analysis

- Document Incidents
- Prioritize Incidents
- 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

Organized by:



With the collaboration of:



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

Organized by:



With the collaboration of:



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

Organized by:



With the collaboration of:



Incident Response Lifecycle

Post Incident activity

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

Organized by:



With the collaboration of:



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>

Organized by:



With the collaboration of:





July 8 - 18, 2024

Leon, Spain

#CyberSBC2024
incibe.es/en/events/summer-bootcamp

Organized by:



With the collaboration of:

