



The image shows the cover of the book "CompTIA Security+ Guide to Network Security Fundamentals, Seventh Edition" by Mark Ciampa. The cover is white with a blue header and footer. The title "CompTIA Security+" is in large blue letters, with "Guide to Network Security Fundamentals" in smaller black text below it. The author's name "MARK CIAMPA" is at the bottom left. The Cengage logo is at the top left. The background of the cover features a stylized orange and white pattern.



A cluster of icons representing network security, including a cloud with a lock, a server, a shield, and a key.


Module 13: Incident Preparation, Response, and Investigation

1



A decorative graphic consisting of overlapping yellow, red, and blue squares with a black crosshair.

Module Objectives



A cluster of icons representing network security, including a cloud with a lock, a server, a shield, and a key.

- By the end of this module, you should be able to:
 - Explain the steps in preparing for a cybersecurity incident
 - Describe how to respond in an incident
 - List the steps in an incident investigation

2

2

Reasons for Cybersecurity Incidents



■ Cybersecurity incidents -two broad areas

- Weak account types
- Poor access control

■ Weak Account Types

- Strong authentication should be required on all user accounts
- Users accounts should be routinely reviewed for security
 - If necessary, some accounts may need to be deleted or strengthened
- Any of the following accounts should be prohibited:
 - Shared account
 - Generic account
 - Guest account

3

3

Reasons for Cybersecurity Incidents



■ Access control

- Granting or denying approval to use specific resources
- Physical access control
 - Fencing, hardware door locks, and mantraps to limit contact with devices
- Technical access control
 - Technology restrictions that limit users on computers from accessing data
- There are standard access control models that are used to help enforce access control

4

4

Reasons for Cybersecurity Incidents

Access Control Concepts

Identification

- The process of recognizing and distinguishing the user from any other user
- Example: a delivery driver presenting employee badge

Authentication

- Performed by checking the credentials
- Example: examining the delivery driver's badge

Authorization

- Granting permission to take action
- Example: allowing the delivery driver to pick up the package

Access

- The right given to access specific resources

Accounting

- A record that is preserved of who accessed the network, what resources they accessed, and when they disconnected from the network

5

5

Reasons for Cybersecurity Incidents

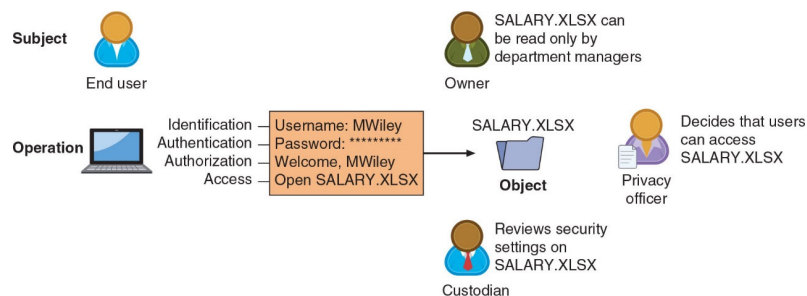


Figure 13-1 Technical access control roles and terminology

- **Object** is a specific resource
 - Example: file or hardware device
- **Subject** is a user or process functioning on behalf of a user
 - Example: computer user
- **Operation** is the action taken by the subject over an object
 - Example: deleting a file

6

6

Reasons for Cybersecurity Incidents



■ Access Control Schemes

- Standards that provide a predefined framework for hardware or software developers
- Use the appropriate scheme to configure the necessary level of control is part of **privileged access management**

■ Five major access control schemes

- *Discretionary Access Control (DAC)*
- *Mandatory Access Control (MAC)*
- *Role Based Access Control (RBAC)*
- *Rule Based Access Control*
- *Attribute-Based Access Control (ABAC)*

7

7

Reasons for Cybersecurity Incidents



■ Discretionary Access Control (DAC)

- The least restrictive
- Every object has an owner who has total control over their objects
- Owners can give permissions to other subjects over their objects
- Used on major operating systems
- DAC has two significant weaknesses:
 - It poses a risk in that it relies on decision by the end user to set the proper level of security
 - A subject's permissions will be "inherited" by any programs that the subject executes

8

8

Reasons for Cybersecurity Incidents



■ Mandatory Access Control (MAC)

- The most restrictive access control model
- The user has no freedom to set any controls or distribute access to other subjects
- Two key elements to MAC:
 - **Labels**
 - Every entity is an object and is assigned a classification label that represents the relative importance of the object
 - **Levels**
 - A hierarchy based on the labels is used
- MAC grants permissions by matching object labels with subject labels
 - The labels indicate level of privilege
- Microsoft Windows uses a MAC implementation called *Mandatory Integrity Control (MIC)*

9

9

Reasons for Cybersecurity Incidents



■ Role-Based Access Control (RBAC) I

- Sometimes called *Non-Discretionary Access Control*
- Access permissions are based on the user's job function
- RBAC assigns permissions to particular roles in an organization
 - Users are then assigned to those roles
- Objects are set to be a certain type, to which subjects with that particular role have access

■ Rule-Based Access Control

- Also called *Rule-Based Role-Based Access Control (RB-RBAC)*
- Dynamically assigns roles to subjects based on a set of rules defined by a custodian
- Each resource object contains access properties based on the rules
- When a user attempts access, the system checks the object's rules to determine access permission
- Often used for managing user access to one or more systems
 - Business changes may trigger application of the rules specifying access changes

10

10

Reasons for Cybersecurity Incidents



■ Attribute-Based Access Control (ABAC)

- Uses more flexible policies than Rule-Based AC
- ABAC can combine attributes
- Policies can take advantage of attributes such as:
 - Object attributes
 - Subject attributes
 - Environment attributes
- ABAC rules can be formatted using an *If-Then-Else* structure

11

11

Reasons for Cybersecurity Incidents



■ Access Control Lists (ACLs)


- A set of permissions attached to an object
- Specifies which subjects may access the object and what operations they can perform
 - When a subject requests to perform an operation on an object, the system checks the ACL for an approved entry
 - ACLs are usually viewed in relation to operating system files
 - ACLs provide **file system permissions** for protecting files managed by the OS

■ Limitations of ACLs:


- Using ACLs is not efficient
- ACLs can be difficult to manage in an enterprise setting where many users need to have different levels of access to many different resources
 - Adding, deleting, and changing ACLs on individual files can be time consuming and open to errors

12

12




Preparing for an Incident




- **Incident Response Plan**
 - A set of written instructions for reacting to a security incident
 - Includes six action steps to be taken when an incident occurs:
 - Preparation
 - Identification
 - Containment
 - Eradication
 - Recovery
 - Lessons learned
- At a minimum, an IRP should contain the following:
 - Documented incident definitions
 - Incident response teams
 - Reporting requirements/escalation
 - Retention policy
 - Stakeholder management
 - Communication plan

13

13



Preparing for an Incident





- **Studying Attack Frameworks**
 - Exploitation frameworks serve as models of the thinking and actions of today's threat actors
 - Three common attack frameworks include the following:
 - *MITRE ATT&CK*
 - *The Diamond Model of Intrusion Analysis*
 - *Cyber Kill Chain*
- **MITRE ATT&CK**
 - Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
 - The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community

■ <https://attack.mitre.org/#>

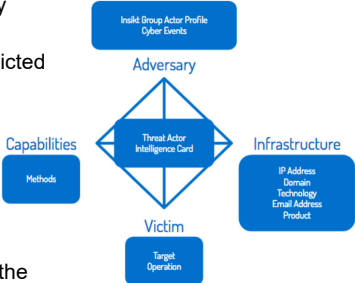
14

14



■ The Diamond Model of Intrusion Analysis

- An approach employed by several information security professionals to authenticate and track cyber threats.
- According to this approach, every incident can be depicted as a diamond
- Four components of the diamond
 - Adversary
 - Capability
 - Infrastructure
 - Victim.
- These four core elements are connected to delineate the relationship between each other
 - Analytically examined to further uncover insights and gain knowledge of malicious activities
- The main axiom of this model,
 - For every intrusion event, there exists an adversary taking a step toward an intended goal by using a capability over infrastructure against a victim to produce a result.”
 - An intrusion event is defined as how the attacker demonstrates and uses certain capabilities and techniques over infrastructure against a target.



15

15

■ Cyber Kill Chain



- A cybersecurity model created by Lockheed Martin that traces the stages of a cyber-attack, identifies vulnerabilities
- Helps security teams to stop the attacks at every stage of the chain.

■ Consists of 7 distinct steps:

- **Reconnaissance**
 - The attacker collects data about the target and the tactics for the attack.
 - Harvesting email addresses Gathering other information.
 - Automated scanners used by intruders to find points of vulnerability in the system
 - Scanning firewalls, IPS, etc to get a point of entry for the attack.
- **Weaponization**
 - Attackers develop malware by leveraging security vulnerabilities.
- **Delivery**
 - The attacker delivers the weaponized malware via a phishing email or some other medium.

16

16






■ **Cyber Kill Chain**- Consists of 7 distinct steps (contd.)

- **Exploitation**
 - The malicious code is delivered into the organization's system.
 - The perimeter is breached
 - The attackers get the opportunity to exploit the organization's systems by installing tools, running scripts
- **Installation**
 - A backdoor or remote access trojan is installed by the malware that provides access to the intruder.
- **Command and Control**
 - The attacker gains control over the organization's systems and network.
 - Attackers gain access to privileged accounts and attempt brute force attacks, search for credentials, and change permissions to take over the control.
- **Actions on Objective**
 - The attacker finally extracts the data from the system

17

17





■ **Cyber Kill Chain** - Based on these stages, the following layers of control implementation are provided:


- **Detect**
 - Determine the attempts to penetrate an organization.
- **Deny**
 - Stopping the attacks when they are happening.
- **Disrupt**
 - Intervene in the data communication done by the attacker and stops it then.
- **Degrade**
 - Limit the effectiveness of a cybersecurity attack to minimize its ill effects.
- **Deceive**
 - Mislead the attacker by providing them with misinformation or misdirecting them.
- **Contain**
 - Contain and limit the scope of the attack so that it is restricted to only some part of the organization.

18

18




Incident Response




- Steps that should be taken when responding to an incident include:
 - Taking advantage of Security Orchestration, Automation, and Response (SOAR) runbooks and playbooks
 - Performing containment
 - Making configuration changes

19

19




Use SOAR Runbooks and Playbooks




- **Security Orchestration, Automation, and Response (SOAR) product**
 - Help security teams manage and respond to security warnings and alarms
 - Allows a security team to automate incident response
- **Playbook**
 - A linear-style checklist of required steps and actions needed to successfully respond to specific incident types and threats
- **Runbook**
 - A series of automated conditional steps that are part of an incident response procedure
 - A playbook focuses more on manual steps to be performed and a runbook is usually actions that are performed automatically
- Most SOAR platforms have pre-configured “out-of-the-box” playbooks that are based on industry best practices and recognized standards

20

20




Perform Containment




- **Containment**
 - Limiting the spread of the attack
 - Most effective when the network has been properly designed
- A secure network design takes advantage of *network segmentation* based upon the principle of zero trust
- Network segments can be created based on business units, locations, or the level of sensitivity of the network data
- Network segmentation only restricts attackers by limiting access to other parts of the network
 - When an attack occurs, **isolation** is then used to segregate both the attacker and the infected systems from reaching other devices

:21

21




Make Configuration Changes




- To neutralize an attacker, limit the spread of the attack, and prevent additional successful incidents, it may be necessary to make configuration changes to devices and processes
- Configuration changes may need to be applied to the following:
 - Firewall rules
 - Content/URL filters
 - Digital certificates
 - Data loss prevention settings
 - Mobile device management settings

:22

22




Incident Investigation




- A cybersecurity incident should be fully investigated
- **Reasons to investigate include:**
 - To pinpoint how the incident occurred so that future incidents can be prevented
 - For regulatory compliance reporting
- Incident investigations involves:
 - Analyzing data sources
 - Performing a digital forensics investigation

:23

23




Data Sources




- **Log Files**
 - **Using data from log files**
 - Identifying log file sources, collecting data, and analyzing data
 - **Security logs**
 - Reveal the type of attacks that was directed at the network
 - How it successfully circumvented existing security defenses
 - **Network-based device logs**
 - Provide beneficial security data for an investigation
 - **System log files**
 - authentication servers in particular should be investigated
 - **Application log files**
 - Give information about attacks focused on different applications
 - **Vulnerabilities in voice and video communication**
 - Often compromised to allow attackers to pivot to other resources

:24

24



Data Sources




- Log Files**
 - Problems associated with log management are due to the following:
 - Multiple devices generating logs
 - Very large volume of data
 - Different log formats
 - Solutions to the problems Table 13-7


Solution	Description
syslog	syslog (system logging protocol) is a standard to send system log or event messages to a server.
nxlog	nxlog is a multi-platform log management tool and supports various platforms, log sources, and formats.
rsyslog	rsyslog (rocket-fast system for log processing) is an open source utility for forwarding log messages in an IP network on UNIX devices.
syslog-ng	syslog-ng is an open source utility for UNIX devices that includes content filtering.
journaltl	journaltl is a Linux utility for querying and displaying log files.

25

25




Data Sources




- Other Data Sources**
 - Data can be accumulated from other sources including the following:
 - IP monitors*
 - Metadata*
 - Analyzers*
 - Vulnerability scans*

26

26




Digital Forensics




- **Forensics**
 - The application of science to legal questions
 - Can be applied to technology
- **Digital forensics**
 - Uses technology to search for computer evidence of a cybercrime
 - Digital evidence can be retrieved from
 - computers, mobile devices, cell phones, digital cameras, and
 - virtually any device that has a processor, memory, or storage
- **Forensics Procedures**
 - When responding to an incident, five basic steps are followed:
 - Secure the crime scene
 - Preserve the evidence
 - Establish a chain of custody
 - Examine the evidence
 - Enable recovery

:27

27



Digital Forensics



- **Secure the Scene**
 - Individuals in the immediate vicinity should perform damage control:
 - Contact the incident response team
 - Secure physical security features
 - Quarantine electronic equipment
 - If necessary, report the incident to the appropriate external authorities
 - After the response team arrives, the first job is to secure the crime scene, which includes:
 - Physical surroundings should be documented
 - Photographs taken before anything is touched
 - Computer cables should be labeled
 - The team takes custody of entire computer along with any peripherals
 - The team interviews witnesses

:28

28

Digital Forensics

■ Preserve the Evidence

- **Preservation of the evidence** involves ensuring that important proof is not destroyed
- Digital evidence is very fragile
 - Evidence should be placed in bags that have tags or identifying labels
- Bags should be sealed to protect the evidence from being altered
 - A tamper-evident seal is a seal or tape that cannot be removed and reapplied without leaving obvious visual evidence
 - A tamper-resistant seal is designed to deter tampering with the bag
- If necessary, the judicial system may need to be involved to ensure the integrity of the evidence is maintained and can hold up in a court of law (admissibility)

29

29

Digital Forensics

■ Document Chain of Custody


- Documenting the evidence from the very beginning is called **provenance**
- Chain of custody documents that the evidence was maintained under strict control at all times and no unauthorized person was given opportunity to corrupt the evidence
- A chain of custody includes documenting:
 - All serial numbers of systems involved
 - Who handled and had custody of the systems and for what length of time
 - How the computer was shipped
 - Any other steps in the process

Property Record Number: _____				
EVIDENCE CHAIN OF CUSTODY TRACKING FORM				
Case Number: _____		Offense: _____		
Submitting Official: (Name/ID#) _____		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
Final Disposal Authority				
Item(s) # _____ on this document pertaining to (investigate) _____				
Signed: no longer needed as evidence and is now authorized for disposal by (check appropriate disposal method)				
<input type="checkbox"/> Return to Owner <input type="checkbox"/> Auction/Destroy/Over				
Name & ID# of Authorizing Official: _____		Signature: _____ Date: _____		
Witness to Destruction of Evidence				
Item(s) # _____ on this document were destroyed by Evidence Custodian _____ ID# _____				
In my presence on (date) _____ Signature: _____ Date: _____				
Release to Lawful Owner				
Item(s) # _____ on this document was/were released by Evidence Custodian _____				
Name _____ ID# _____ to _____				
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. <input type="checkbox"/> Yes <input type="checkbox"/> No				
This Evidence Chain of Custody form is to be retained as a permanent record.				


Figure 13-8 Chain of custody form

30

30




Digital Forensics




- **Examine for Evidence**
 - An **order of volatility** must be followed when examining evidence in order to preserve the most fragile data first
 - After a computer forensics expert creates a mirror image of a system, the original system is secured and the mirror image is examined to reveal evidence
 - Mirror image backup programs rely upon hashing algorithms as part of the validation process
 - Hidden clues also can be exposed by examining
 - RAM slack, drive slack, and metadata (data about data)

31

31




Digital Forensics




- **Enable Recovery**
 - A final analysis looks at recovering the data from the security event and the lessons that can be learned from it
 - **Strategic intelligence**
 - The collection, processing, analysis, and dissemination of intelligence for forming policy changes
 - **Strategic counterintelligence**
 - Involves gaining information about the attacker's intelligence collection capabilities

32

32




Digital Forensics




- **Forensics Tools**
 - Software forensics tools include the following:
 - A utility named DD (sometimes called DNU dd) is an imaging utility that requires only minimal resources to run and generates raw image files that can be read by many other programs
 - Memdump
 - Linux utility that “dumps” system memory
 - WinHex
 - Autopsy
 - Hardware forensics tools include the following:
 - A digital forensic workstation
 - A mobile device forensics tool

33

33



Digital Forensics



- **Cloud Forensics**
 - When dealing with a cloud incident, the following should be considered:
 - A right to audit clause in a cloud contract gives the customer the legal right to review the logs
 - When a cloud customer is notified by its cloud provider that an incident occurred, the immediate response will be to ask for details about the scope of the impact
 - The cloud provider may take weeks or months to provide this
 - The legal **regulatory/jurisdiction** laws that govern the site in which the cloud data resides may present difficulties

34

34

Summary



- Access control is granting or denying approval to use specific resources
- An access control list (ACL) is a set of permissions that is attached to an object
- An incident response plan is a set of written instructions for reacting to a security incident
- It is important to test an incident response plan by conducting exercises to make necessary adjustments
- Two elements that are closely associated with using SOARs are a SOAR playbook and a runbook
- Following a cybersecurity incident, it must be fully investigated
- IP software monitors can provide insight into an incident
- Forensics is the application of science to questions that are of interest to the legal profession
 - Digital forensics uses technology to search for evidence pertaining to a cybercrime or damage that occurred during a cyber incident
- As soon as the incident response team begins its work, it must start and maintain a strict chain of custody
- There are different software and hardware forensics tools available for analysis

35