EC-Council Certified Incident Handler

ECIH

https://securevalley-training.net/store

https://securevalley-training.net/boutique

Table of Contents

Introduction Générale

La cybersécurité est essentielle pour protéger les données et les systèmes des organisations contre des attaques potentielles, en particulier dans un environnement où les cybermenaces deviennent de plus en plus sophistiquées. Les incidents de sécurité peuvent se produire sous diverses formes, telles que des attaques par phishing, des intrusions réseau ou des compromissions de comptes. Une réponse rapide et structurée à ces incidents est cruciale pour limiter les dégâts, restaurer les services, et prévenir les futures attaques.

Le module 05 se concentre sur la réponse aux incidents de sécurité par email, un vecteur d'attaque courant utilisé pour propager des menaces comme les malwares et les ransomwares. Il explore les processus de détection, de confinement, d'éradication et de récupération, ainsi que l'utilisation d'outils spécifiques pour identifier et répondre aux attaques par email. Ce module aborde également les bonnes pratiques en matière de sécurité des emails, y compris l'authentification et la formation des utilisateurs.

Le module 06, quant à lui, traite des incidents de sécurité réseau. Il explore différents types d'incidents, tels que les attaques par déni de service (DoS/DDoS), le spoofing ARP, l'exfiltration de données et les accès non autorisés. Ce module met en évidence l'importance de la détection précoce des menaces sur le réseau, du confinement des systèmes affectés, et de l'éradication des intrusions. Il fournit des méthodes pratiques pour analyser et répondre aux attaques réseau en utilisant des outils comme Wireshark, Snort et les systèmes SIEM, tout en mettant l'accent sur les mesures préventives à adopter pour réduire le risque de futures attaques.

En maîtrisant ces processus et outils, les professionnels de la cybersécurité sont mieux préparés à protéger les systèmes et données critiques des entreprises contre les menaces persistantes.

Module 1: Introduction to Incident Handling and Response

---

1. What Is an Incident?

In cybersecurity, an *incident* is any event that threatens the security of an information system, data, or network. It may be intentional (like a hacking attempt) or unintentional (such as a system failure or human error). The goal of incident handling is to detect, respond to, and mitigate these events before they cause damage.

An incident becomes significant when it affects the confidentiality, integrity, or availability (CIA) of an organization's data and systems.

Examples include:

- Unauthorized access attempts
- Data breaches
- Malware infections
- Denial of Service (DoS) attacks
- Insider misuse

2. What Is Incident Handling and Response?

Incident Handling refers to the process of managing incidents in real-time. It includes detection, documentation, and immediate action to contain and analyze the incident.

Incident Response is a broader term that involves planning, managing, and improving the organization's ability to respond to incidents over time. It includes lessons learned and applying that knowledge to future situations.

Together, these processes aim to reduce damage, improve recovery, and prevent future incidents.

3. Goals of Incident Handling and Response

- Detect incidents as early as possible
- Minimize the impact on operations

- Contain the incident to prevent further damage
- Recover systems and data quickly and securely
- Preserve evidence for legal or internal investigation
- Learn from the incident and improve the overall security posture

4. Categories of Cybersecurity Incidents

1. Malware-related: Ransomware, spyware, trojans
2. Unauthorized Access: External hackers or insider abuse
3. Phishing/Social Engineering: Deceptive emails or messages
4. Data Exfiltration: Unauthorized copying of data
5. Denial of Service: Disrupting services by overwhelming systems
6. Misconfiguration: Insecure system or network setups
7. Policy Violation: Employees violating company rules
8. Physical Security Breaches: Unauthorized access to secure areas

5. Incident Response Lifecycle (Preview)

The full process is covered in the next module, but here's a preview:

- Preparation
- Detection and Analysis
- Containment, Eradication, Recovery
- Post-Incident Activities

Preparation is the foundation of effective response. Without it, teams may act too slowly or incorrectly when an incident occurs.

6. Stakeholders in Incident Handling

Successful response requires coordination among:

- IT Security Teams
- Legal and Compliance
- Management and Executives
- Human Resources (in insider threat cases)

- Law Enforcement (for serious crimes)

All departments must know their role during an incident.

7. Importance of Policies and Procedures

Organizations need clear policies that define:

- What constitutes an incident
- Who to notify
- How incidents are prioritized
- How evidence should be collected and preserved
- When external help (e.g., law enforcement) should be involved

Without policies, response efforts become disorganized and ineffective.

8. Legal and Regulatory Considerations

Many industries are subject to data protection laws:

- GDPR (EU)
- HIPAA (Healthcare, US)
- PCI-DSS (Payment Card Industry)

Failing to respond to incidents properly can result in legal penalties, loss of customer trust, and damage to reputation.

Incident handlers must ensure:

- Logs are kept
- Evidence is preserved
- Notifications are made on time
- Privacy laws are respected

9. Characteristics of a Good Incident Handler

- Technical Knowledge: Networking, malware, OS
- Analytical Thinking: Ability to diagnose and prioritize
- Communication Skills: Clear reporting and updates
- Calm Under Pressure: Quick, thoughtful decision-making

- Ethical Mindset: Trustworthy and law-abiding

Incident handling is not only technical—it's strategic and human-centered.

10. Lab – Simulated Phishing Attack Detection and Initial Response

Objective: Learn to detect and respond to a simulated phishing email.

Tools Needed:

- A test email environment (can be simulated in Outlook or Gmail)
- A web browser
- Note-taking app or document editor

Steps:

1. Receive Suspicious Email
   Open an email that appears to come from your bank or HR department asking you to click a link.
2. Analyze the Indicators
   - Check the sender's address
   - Hover over links to see the actual URL
   - Look for poor grammar or urgency tactics
3. Do NOT Click
   Record all signs that make the email suspicious.
4. Report the Email
   - Forward the email to the security team or use your organization's "Report Phishing" button
   - Document the time, sender, subject, and suspicion indicators
5. Initial Containment
   - Warn colleagues (without causing panic)
   - Check if anyone else received or clicked the link
6. Post-Incident
   - Update your response documentation
   - Conduct a short briefing with your team
   - Review what worked well and what can be improved

Module 2: Incident Handling and Response Process

---

1. Introduction

The Incident Handling and Response (IHR) process is a structured approach used to manage cybersecurity incidents efficiently. It provides a consistent way to detect, assess, respond to, and recover from incidents while minimizing business impact.

The most common framework consists of **6 phases**:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

2. Phase 1: Preparation

Preparation is the foundation of incident response. A well-prepared organization is faster and more effective in dealing with incidents.

Key Actions:

- Develop an Incident Response Plan (IRP)
- Establish communication channels
- Define roles and responsibilities
- Train the incident response team
- Set up monitoring and detection tools (e.g., SIEM, IDS)
- Conduct regular drills and tabletop exercises

Example: Having a clear call tree, updated contacts, and access to forensic tools before an incident occurs.

3. Phase 2: Identification

This phase involves detecting and confirming whether an event is actually a security incident.

Sources of Detection:

- System logs
- Intrusion Detection Systems (IDS)
- Antivirus alerts
- User reports
- Network traffic anomalies

Key Questions:

- What happened?
- When did it happen?
- Who is affected?
- What systems are involved?

Action: Start an incident log with time stamps and observations.

4. Phase 3: Containment

The goal of containment is to limit the spread or impact of the incident. It can be **short-term** (immediate response) or **long-term** (permanent measures).

Short-term Containment Examples:

- Disconnect affected systems from the network
- Disable user accounts
- Block malicious IPs or domains

Long-term Containment Examples:

- Apply patches
- Change configurations
- Harden systems

Containment helps prevent data loss, lateral movement, and further compromise.

5. Phase 4: Eradication

Once the threat is contained, remove the root cause and eliminate malicious artifacts.

Actions:

- Remove malware, trojans, backdoors
- Patch exploited vulnerabilities
- Reset credentials
- Analyze indicators of compromise (IoCs)

Goal: Ensure that the threat actor or code is completely removed from the environment.

6. Phase 5: Recovery

This phase focuses on restoring systems and services to normal operations.

Steps:

- Restore systems from backups (if clean)
- Monitor systems for signs of reinfection
- Reconnect to the network gradually
- Validate system functionality

Key Considerations:

- Choose the right time to restore services
- Monitor for at least 24-72 hours post-recovery

7. Phase 6: Lessons Learned

After handling the incident, teams must review what happened and how to improve the process.

Goals:

- Identify what went well and what didn’t
- Update incident response plans and playbooks
- Train staff on the findings
- Prepare for similar threats in the future

Questions to Ask:

- Was the incident detected promptly?
- Were communications clear?
- Could the attack have been prevented?
- Are tools and systems adequate?

8. Importance of Documentation

Every phase must be thoroughly documented for:

- Legal and compliance purposes
- Organizational memory
- Improving future response

Documentation should include:

- Timeline of events
- Impact assessment
- Technical analysis
- Communication logs
- Remediation actions

9. Integration With Other Teams

Effective incident response requires cooperation between:

- Security team (technical analysis and mitigation)
- Legal team (regulatory and legal concerns)
- Public relations (if the incident is public)
- Management (decision making and approvals)
- HR (for insider-related incidents)

Clear communication protocols and reporting structures are essential during incidents.

10. Lab – Simulate a Full Incident Handling Cycle

Objective: Practice all 6 phases of the incident handling process using a simulated malware infection.

Scenario: A user reports a strange file running on their workstation. Your task is to handle this as an incident.

Tools Needed:

- Virtual machine (Linux or Windows)
- Basic system monitoring tools (Task Manager, Process Explorer, Sysinternals, or htop)
- Notepad or Google Docs for logging

Instructions:

1. **Preparation**
    - Open your checklist for incident response.
    - Create a folder to store logs and notes.
2. **Identification**
    - Simulate log analysis or receive a "suspicious" file from a user.
    - Identify signs of compromise (e.g., unknown process, suspicious file).
3. **Containment**
    - Disconnect the VM from the network.
    - Disable affected services or accounts.
4. **Eradication**
    - Remove the malicious file.
    - Delete associated registry entries or startup services.
5. **Recovery**
    - Reboot the system.
    - Reconnect to the network and observe for any anomalies.
6. **Lessons Learned**
    - Write a 1-page report explaining what happened and how you would improve response next time.

Module 3: Forensic Readiness and First Response

---

1. Introduction

In the context of cybersecurity incidents, **forensic readiness** refers to an organization's ability to collect, preserve, protect, and analyze digital evidence properly so it can be used during investigations, legal proceedings, or internal audits. The **first response** is the initial reaction to a security incident, and it plays a critical role in ensuring that evidence is not tampered with or lost.

2. Objectives of Forensic Readiness

- Ensure that digital evidence is admissible in court.
- Reduce the cost and time of investigations.
- Minimize disruption during incident handling.
- Enable rapid and accurate decision-making in crisis situations.
- Increase deterrence by showing preparedness for legal follow-up.

3. Principles of Digital Forensics

1. **Preservation** – Do not alter data during collection.
2. **Identification** – Identify sources of potential evidence.
3. **Collection** – Gather data using reliable, court-accepted methods.
4. **Analysis** – Examine data to determine what happened.
5. **Documentation** – Keep accurate records of every action taken.
6. **Presentation** – Prepare the evidence for reporting or legal use.

4. Digital Evidence Types

Digital evidence can include:

- System and application logs

- Network captures
- Email archives
- Hard drives or memory dumps
- USB and removable media
- Screenshots
- Authentication records

Each must be collected and handled in a way that maintains the **chain of custody** and prevents tampering.

---

5. Chain of Custody

The **chain of custody** is the documented process that tracks the movement and handling of evidence from collection to courtroom. It should include:

- Who collected the evidence
- When it was collected
- How it was collected
- Where it was stored
- Who accessed it and why

Improper chain of custody may lead to the **inadmissibility of evidence** in legal cases.

6. Role of the First Responder

A **first responder** is the person or team that first arrives at the scene of a cyber incident. Their role is crucial in ensuring that evidence is preserved and the right procedures are followed.

Responsibilities include:

- Secure the scene (physically or digitally)
- Avoid changing the state of the system
- Document everything (time, actions, system status)
- Notify appropriate personnel (e.g., incident response or forensic team)
- Take screenshots, photos, or notes
- Prevent further damage (e.g., disconnect from the network)

7. Common Mistakes During First Response

- Shutting down the system improperly
- Running untrusted tools on a live system
- Using USB drives or storage on infected systems
- Failing to record what actions were taken
- Alerting the attacker or user involved prematurely
- Breaking the chain of custody

8. First Response Procedure (Step-by-Step)

1. **Assess the Scene** – Is it safe to approach? Is the device still on?
2. **Isolate the System** – If appropriate, disconnect from the network (avoid shutdown).
3. **Document Everything** – Date, time, what you saw, what you did.
4. **Capture Volatile Data** – If you are trained and it's safe, collect RAM, running processes, and network connections.
5. **Secure Storage Media** – Label hard drives and devices clearly.
6. **Notify the Incident Response Team** – Transfer control to experts for detailed analysis.

9. Tools Used in First Response and Forensics

Tool Name	Purpose
FTK Imager	Forensic image acquisition
Volatility	Memory analysis
Autopsy	File system analysis
Wireshark	Network packet analysis
dd	Disk cloning in Linux
EnCase (commercial)	Full digital forensic suite
md5sum/sha256sum	Hash verification

Important: Always use **write blockers** when accessing hard drives to prevent modification.

10. Lab – Simulate a Forensic First Response

Objective: Practice responding to an incident and capturing forensic evidence without contaminating it.

Scenario: A suspicious file has been found on a USB device connected to a compromised Linux virtual machine.

Instructions:

1. **Prepare Tools**: Install dcfldd, md5sum, and optionally Autopsy or FTK Imager.
2. **Isolate the System**: Disconnect the virtual machine from the network.
3. **Document the Situation**: Note the time, user, and system details.
4. **Collect Volatile Data** (Optional Advanced Step): Use ps, netstat, top to view current activity and save output.
5. **Image the USB**:
6. sudo dcfldd if=/dev/sdb of=/mnt/evidence/usb.img hash=md5 hashlog=/mnt/evidence/hash.log
7. **Verify Hash**:
8. md5sum /mnt/evidence/usb.img
9. **Preserve Evidence**: Store the image and documentation in a separate folder or external device.

Module 4: Handling and Responding to Malware Incidents

---

1. Introduction

Malware (malicious software) is a primary cause of modern cybersecurity incidents. It includes viruses, worms, Trojans, ransomware, spyware, rootkits, and more. A strong incident response plan must include structured steps to detect, contain, analyze, and recover from malware attacks.

2. Objectives of Malware Incident Handling

- Detect and identify malware infections.
- Minimize damage and prevent spread.
- Collect and preserve forensic evidence.
- Analyze malware behavior to understand its impact.
- Restore affected systems and monitor for re-infection.

3. Common Malware Types

Type	Description
Virus	Infects files and spreads via replication.
Worm	Spreads automatically across networks.
Trojan	Disguised as legitimate software.
Ransomware	Encrypts files and demands payment.
Spyware	Steals data without user knowledge.
Rootkit	Hides malicious activity or malware.
Botnet	Network of infected devices controlled remotely.

4. Malware Indicators (IoCs - Indicators of Compromise)

- High CPU/memory usage
- Unexpected outbound connections
- Unknown processes running
- Disabled security tools
- Suspicious files (e.g., .exe, .bat, .vbs)
- Changes in system configuration or registry
- Unusual log entries or error messages

5. Malware Incident Handling Process

Step 1: Preparation

- Deploy updated antivirus and endpoint detection and response (EDR) tools.
- Conduct user awareness training.
- Define escalation paths.

Step 2: Detection and Analysis

- Use antivirus/EDR alerts, SIEM logs, and user reports.
- Analyze suspicious files using tools like:
    - **VirusTotal**
    - **Hybrid Analysis**
    - **Cuckoo Sandbox**
    - **Any.run**

Step 3: Containment

- Disconnect infected machines from the network.
- Block malicious domains, IPs, and hashes.
- Isolate malware samples for safe analysis.

Step 4: Eradication

- Remove malware using antivirus or manual methods.
- Patch vulnerabilities used by malware.
- Delete or clean infected files.

Step 5: Recovery

- Restore from clean backups.
- Re-enable and update security controls.
- Monitor system for signs of reinfection.

Step 6: Lessons Learned

- Perform root cause analysis.
- Update incident response playbooks.
- Educate staff about the specific attack vector used.

6. Tools for Malware Incident Response

Tool	Purpose
Wireshark	Analyze malicious traffic.
Sysinternals Suite (Autoruns, Process Explorer)	Analyze live Windows systems.
PEStudio	Static malware file analysis.
Procmon	Monitor system calls in real time.
Volatility	Memory forensics for malware analysis.
FTK Imager	Create forensic copies of infected systems.

7. Best Practices

- Never analyze malware on a production system.
- Use isolated virtual machines with no internet access for analysis.
- Take snapshots before and after infection.
- Create hash values of malware files before analysis.
- Avoid clicking suspicious links or running unknown attachments.

8. Malware Containment Techniques

- Disable shared folders and network shares.

- Apply firewall rules to block communication.
- Use DNS sinkholing for known malicious domains.
- Kill malicious processes and disable autoruns.

9. Reporting and Documentation

- Record:
    - Infection vector
    - Malware name (if known)
    - Systems affected
    - Steps taken to contain and remove
- Include malware hashes and analysis reports.
- Store in your IR documentation for compliance and audit.

10. Lab – Analyzing and Responding to a Malware Infection

Objective: Analyze a real malware sample in a safe environment and simulate an incident response.

Environment Setup:

- Use **Remnux** or a virtual machine with tools like **Wireshark**, **Autoruns**, **Process Hacker**, and **PEStudio**.

Steps:

1. **Download a benign malware sample** from a safe source (e.g., https://thezoo.morirt.com – for education).
2. **Verify hash** before proceeding.
3. **Use PEStudio** to analyze the file statically.
4. **Run the malware in a sandboxed environment** and monitor:
    - Processes created
    - Files dropped
    - Registry changes
    - Network connections
5. **Use Wireshark** to capture traffic.

6. **Document findings**, including:
    - File name and hash
    - Malicious behavior
    - Persistence methods
7. **Simulate containment**: Kill the process and clean startup entries.
8. **Erase the VM snapshot** to avoid contamination.

Outcome: You'll learn how malware behaves, how to analyze it, and how to respond effectively without causing harm to your real system.

Module 05: Network Forensics

---

1. Introduction

Email remains the most common attack vector used by cybercriminals to deliver threats such as phishing, malware, ransomware, social engineering, and business email compromise (BEC). Rapid identification and response to email security incidents is crucial to prevent data breaches and financial loss.

2. Objectives of Email Incident Response

- Detect email-based threats early.
- Contain and prevent further compromise.
- Identify affected users or systems.
- Remove malicious content.
- Educate users and improve email security posture.

3. Common Email Threats

Threat	Description
Phishing	Fraudulent email tricking users into revealing information.
Spear Phishing	Targeted phishing email aimed at specific individuals.
Business Email Compromise (BEC)	Impersonation of executives to trick employees.
Malicious Attachments/Links	Files or URLs that deliver malware.
Spoofing	Forged sender email address.
Spam	Unsolicited and irrelevant bulk email.

4. Email Incident Indicators

- Unexpected emails from known contacts.
- Emails with urgent language or financial requests.
- Misspelled domains or sender names.
- Unusual attachments (.exe, .js, .scr).
- Suspicious login attempts after phishing.
- Reports from users about strange emails.

5. Email Incident Handling Process

Step 1: Detection

- Use email gateways and security filters (e.g., Microsoft Defender, Proofpoint, Mimecast).
- Monitor reports from users and analyze headers, links, and attachments.
- Search logs in SIEM for signs of compromise.

Step 2: Containment

- Quarantine or delete the email.
- Block sender domains and IPs at the email gateway.
- Revoke access if user credentials were stolen.
- Isolate infected devices if malware was opened.

Step 3: Eradication

- Remove malicious emails from mailboxes (PowerShell, admin tools).
- Clean affected systems.
- Invalidate compromised credentials.
- Remove malicious email rules created by attackers.

Step 4: Recovery

- Re-enable secure access to email accounts.
- Monitor activity for signs of persistence.
- Restore lost emails from backups if needed.
- Ensure endpoint protections are active.

Step 5: Post-Incident Activities

- Document full timeline and impact.

- Update detection rules and policies.
- Conduct phishing simulations and awareness training.
- Improve spam filters and domain authentication (SPF, DKIM, DMARC).

6. Tools for Email Threat Detection

Tool	Use
VirusTotal	Analyze suspicious attachments/links.
Email Header Analyzer	Investigate email source.
Microsoft 365 Security Center	Review user activity and quarantine emails.
PowerShell Scripts	Search and delete emails across multiple mailboxes.
PhishTool / MISP	Analyze and share phishing indicators.

7. Email Authentication Mechanisms

- SPF (Sender Policy Framework): Verifies that sender IP is allowed to send for the domain.
- DKIM (DomainKeys Identified Mail): Signs messages to prove authenticity.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Prevents spoofing and provides reports.

Enabling SPF, DKIM, and DMARC protects users from forged and spoofed emails.

8. Best Practices

- Train users to recognize phishing attempts.
- Disable macros in Office documents by default.
- Use secure email gateways and sandboxing.
- Implement 2FA for email accounts.
- Regularly monitor mailbox rules and login locations.

9. Sample Email Incident Flow

1. Phishing email received by a staff member.
2. Email contains link to fake login page.
3. Victim enters credentials, attacker logs in.
4. Attacker sets up mail forwarding rules.
5. SIEM detects suspicious login from another country.
6. IR team is alerted:
    - Password reset
    - Mail rules removed
    - Fake email link blocked
    - Awareness sent to all employees

10. Lab – Simulate a Phishing Attack and Response

Objective: Simulate and investigate a phishing email to practice incident response.

Tools: Try using a phishing simulation platform (like GoPhish) in a test environment.

Steps:

1. Create a fake login page and phishing email template.
2. Send it to a test user in a safe, isolated lab.
3. Monitor activity:
    - Email headers
    - Link clicks
    - Credentials entered
4. Detect it using your email filtering system.
5. Respond:
    - Quarantine the message
    - Revoke any test user credentials
    - Remove malicious emails via admin panel
6. Document and generate a report.

Module 6: Handling and Responding to Network Security Incidents

---

1. Introduction

Network security incidents target the **availability, integrity, and confidentiality** of organizational data by exploiting vulnerabilities in networks, devices, and protocols. Quick and structured responses to these incidents are critical to minimizing damage, downtime, and potential data exfiltration.

2. Objectives of Network Incident Response

- Detect and identify suspicious or unauthorized activity in the network.
- Contain and isolate affected systems or segments.
- Eliminate malicious activities or intrusions.
- Restore normal network operations safely.
- Implement preventive measures to reduce future incidents.

3. Types of Network Security Incidents

Type	Description
DoS/DDoS Attacks	Overwhelming a service to make it unavailable.
Man-in-the-Middle (MitM)	Intercepting traffic between two parties.
ARP Spoofing	Redirecting traffic by sending fake ARP messages.
Port Scanning	Reconnaissance to identify open services.
Unauthorized Access	Gaining access to restricted systems.
Data Exfiltration	Covertly stealing data over the network.

4. Indicators of Network Security Incidents

- Unusual outbound traffic patterns.

- Unexpected ports and protocols in use.
- Spikes in bandwidth usage.
- Unauthorized devices or IP addresses on the network.
- Repeated failed login attempts from specific IPs.
- IDS/IPS alerts or firewall rule triggers.

5. Network Incident Response Process

Step 1: Detection and Analysis

- Use SIEM tools, IDS/IPS, and NetFlow logs to monitor anomalies.
- Identify affected hosts, communication patterns, and traffic sources.
- Analyze log data from firewalls, switches, and routers.

Step 2: Containment

- Isolate affected hosts or network segments (VLAN, ACLs).
- Disable compromised interfaces or block malicious IPs.
- Use sinkholes or honeypots to divert and observe traffic.

Step 3: Eradication

- Remove malware or unauthorized software.
- Patch known vulnerabilities.
- Disable rogue devices and revoke credentials.

Step 4: Recovery

- Restore from clean backups.
- Monitor network for any signs of persistence or reentry.
- Gradually reconnect isolated systems.

Step 5: Post-Incident Review

- Document timeline, attacker methods, and impact.
- Update firewall rules, ACLs, and IDS/IPS signatures.
- Educate staff on lessons learned and improve IR policies.

6. Common Tools Used

Tool	Use
Wireshark	Packet-level analysis.
Snort/Suricata	Intrusion detection and alerting.
Tcpdump	Lightweight traffic capture.
NetFlow/sFlow	Network traffic flow monitoring.
SIEM (e.g., Splunk, ELK)	Correlation and incident alerts.
Firewall Logs	Detect blocked or suspicious traffic.

7. Case Study: ARP Spoofing Detection and Response

1. **Symptom**: Internal user reports slow and unstable connection.
2. **Detection**:
    - Wireshark shows repeated ARP replies mapping gateway IP to a different MAC address.
    - IDS flags ARP poisoning.
3. **Containment**:
    - Isolate suspected machine via switch port control.
    - Implement static ARP entries on critical devices.
4. **Eradication**:
    - Remove malicious tool from attacker's machine.
    - Patch and harden network devices.
5. **Recovery**:
    - Monitor traffic and resume normal operations.
6. **Post-Incident**:
    - Deploy ARP inspection on switches.
    - Conduct awareness on internal threats.

8. Preventive Measures

- **Network Segmentation**: Separate sensitive systems using VLANs.
- **Access Control**: Enforce least privilege on firewalls and switches.

- **Encryption**: Use VPNs or TLS to protect data-in-transit.
- **Patching**: Regularly update firmware and network device OS.
- **Anomaly Detection**: Train systems to recognize behavioral changes.

9. Best Practices

- Maintain a well-documented network map and inventory.
- Centralize logging for all network devices.
- Regularly simulate network-based attack scenarios.
- Conduct vulnerability assessments and penetration tests.
- Enforce multi-factor authentication for remote access.

10. Lab – Investigating Suspicious Network Traffic

Objective: Analyze a network capture for signs of scanning or malware communication.

Steps:

1. Use **Wireshark** to open a .pcap file from a simulated attack.
2. Apply filters like ip.addr == X.X.X.X or tcp.flags.syn == 1.
3. Identify signs of:
    - Port scanning (many SYNs, no replies).
    - C2 traffic (regular beaconing patterns).
    - DNS tunneling (long encoded queries).
4. Take note of IPs and ports involved.
5. Create a timeline and report your findings.

Module 7: Handling and Responding to Web Application Security Incidents

---

1. Introduction

Web applications are a prime target for attackers because they are often exposed to the internet and may contain sensitive data. Attackers exploit vulnerabilities like **SQL injection**, **XSS**, and **broken authentication** to gain unauthorized access or manipulate web-based systems. Effective incident handling is critical to minimize damage and prevent recurrence.

2. Objectives of Web Application Incident Response

- Identify and validate web-related attacks or breaches.
- Mitigate the impact and block further exploitation.
- Analyze the attack vector and remediate vulnerabilities.
- Protect user data and restore secure application functionality.
- Strengthen application security post-incident.

3. Common Web Application Attacks

Attack Type	Description
SQL Injection (SQLi)	Injecting SQL commands to access or modify databases.
Cross-Site Scripting (XSS)	Injecting malicious scripts into web pages.
File Inclusion	Loading unauthorized files through web inputs.
Broken Authentication	Exploiting weak or misconfigured login systems.
Cross-Site Request Forgery (CSRF)	Forcing a user to perform unintended actions.
Remote Code Execution (RCE)	Executing malicious code on the server.

4. Signs of a Web Application Incident

- Unusual spikes in traffic or error logs.
- Multiple failed login attempts.
- Unrecognized changes in web content.
- Alerts from Web Application Firewalls (WAFs).
- Complaints from users about unauthorized actions.
- Detection of web shells or backdoors.

5. Web Application Incident Response Process

Step 1: Detection and Triage

- Monitor application logs and WAF alerts.
- Use tools like OWASP ZAP, Burp Suite, or custom scanners.
- Identify impacted endpoints, users, and data.

Step 2: Containment

- Disable vulnerable features or endpoints.
- Enforce WAF rules and rate limiting.
- Lock down affected user accounts.

Step 3: Eradication

- Remove any malicious scripts, files, or code.
- Patch the underlying vulnerability (e.g., sanitize inputs).
- Restore secure configurations (e.g., reset API keys, regenerate sessions).

Step 4: Recovery

- Deploy updated, secure application code.
- Inform users if their data was exposed.
- Monitor for re-exploitation attempts.

Step 5: Post-Incident Actions

- Review and update secure coding practices.
- Conduct code reviews and penetration tests.
- Train developers and operations teams.

6. Tools for Investigation

Tool	Use
Burp Suite	Analyze HTTP requests/responses, find vulnerabilities.
OWASP ZAP	Automated scanner for web app weaknesses.
Nikto	Scan web servers for misconfigurations.
Log analyzers (GoAccess, Splunk)	Review and correlate web logs.
ModSecurity	WAF that logs and blocks malicious requests.

7. Case Study: SQL Injection in Login Page

Scenario: A user logs in without valid credentials.

1. **Detection**:
    - Logs show the use of ' OR '1'='1 in input fields.
    - Unusual database query execution patterns.
2. **Containment**:
    - Disable login temporarily.
    - Enforce WAF rules to block SQLi patterns.
3. **Eradication**:
    - Sanitize all database inputs using parameterized queries.
    - Remove user accounts created through unauthorized access.
4. **Recovery**:
    - Reinstate login page with input validation.
    - Monitor access attempts and database changes.
5. **Post-Incident**:
    - Educate developers on secure coding.
    - Review all database access controls.

8. Preventive Measures

- Input validation and output encoding.
- Use frameworks that support **prepared statements**.
- Implement strong authentication and session management.
- Regularly update and patch application components.
- Enforce least privilege on database and server access.
- Deploy a Web Application Firewall (WAF).

9. Best Practices

- Use security headers (CSP, X-Frame-Options, etc.).
- Store credentials securely (e.g., bcrypt for passwords).
- Apply rate limiting and CAPTCHA for login forms.
- Conduct secure code reviews before deployment.
- Follow OWASP Top 10 guidelines.

10. Lab – Simulating and Analyzing an XSS Attack

Objective: Understand how a simple XSS attack works and how to detect/prevent it.

Steps:

1. Set up a simple vulnerable comment box (or use DVWA).
2. Inject a payload like <script>alert("XSS")</script>.
3. Observe the behavior in the browser and logs.
4. Add input sanitization to strip scripts.
5. Re-test to confirm the vulnerability is fixed.

Module 8: Handling and Responding to Cloud Security Incidents

---

1. Introduction

Cloud environments introduce new attack surfaces and risks due to shared responsibility models, multi-tenancy, and remote access. Incident response in cloud systems must account for service provider roles, API exposure, and dynamic infrastructure. Responders must be prepared to handle cloud-native threats effectively.

2. Cloud Computing Models

- **IaaS (Infrastructure as a Service)** – User manages OS, storage, apps (e.g., AWS EC2, Azure VM).
- **PaaS (Platform as a Service)** – User manages apps; provider manages platform (e.g., Heroku).
- **SaaS (Software as a Service)** – Everything is managed by the provider (e.g., Google Workspace).

Understanding the model helps define **incident response boundaries**.

3. Common Cloud Security Incidents

Type	Description
Account Takeover	Attacker gains access to cloud credentials.
Misconfigured Storage Buckets	Publicly exposed data (e.g., AWS S3 buckets).
API Abuse	Attackers exploit open or insecure cloud APIs.
Cryptojacking	Cloud resources used for unauthorized mining.
Privilege Escalation	Gaining excessive permissions in cloud roles.
Data Exfiltration	Sensitive data downloaded or transferred externally.

4. Indicators of a Cloud Incident

- Suspicious API requests (e.g., access from unknown IPs).
- Abnormal login patterns or geolocation anomalies.
- Unexpected infrastructure changes (VMs, firewalls, buckets).
- Alerts from CSPM tools or SIEMs.
- Unusual billing spikes (suggesting abuse or misuse).
- Unauthorized data downloads or changes.

5. Cloud Incident Handling Process

Step 1: Detection

- Use cloud-native logs: AWS CloudTrail, Azure Monitor, Google Cloud Logging.
- Integrate alerts with SIEM (e.g., Splunk, ELK, Sentinel).

Step 2: Analysis

- Identify root cause: access keys leak, exposed APIs, IAM policy issues.
- Analyze logs and correlate suspicious events across services.

Step 3: Containment

- Revoke access tokens, disable affected accounts or keys.
- Lock down misconfigured services (e.g., change S3 bucket permissions).
- Isolate compromised resources (e.g., infected VM).

Step 4: Eradication

- Remove malware, reimage VMs, rotate credentials.
- Fix misconfigurations and vulnerabilities.

Step 5: Recovery

- Restore cloud services using secure templates (Infrastructure as Code).
- Monitor for reoccurrence using cloud watch rules and alerts.

Step 6: Lessons Learned

- Review IAM policies and security group rules.
- Implement tighter controls (e.g., MFA, audit trails).

- Update incident response playbooks for cloud-specific threats.

6. Key Cloud Security Tools

Tool	Purpose
AWS GuardDuty	Threat detection and monitoring.
Microsoft Defender for Cloud	Security posture management and alerts.
GCP Security Command Center	Threat detection in Google Cloud.
CSPM Tools (e.g., Prisma Cloud, Dome9)	Cloud Security Posture Management.
SIEM (e.g., Splunk, Sentinel)	Aggregating logs and threat analysis.

7. Case Study: S3 Bucket Misconfiguration

Scenario: A sensitive S3 bucket was publicly accessible, and data was leaked.

1. **Detection**:
    - CloudTrail logs show anonymous access to sensitive files.
    - Data from the bucket found on external forums.
2. **Containment**:
    - Change bucket permissions to private.
    - Revoke public URLs and access keys.
3. **Eradication**:
    - Audit all buckets using automated scripts.
    - Implement a policy to deny public access by default.
4. **Recovery**:
    - Restore backup data to a new, secure bucket.
    - Notify affected users or clients.
5. **Post-Incident**:
    - Enforce encryption and access logging.

- Enable continuous monitoring and alerts for new bucket configurations.

8. Best Practices for Cloud Incident Prevention

- Use **MFA** for all admin accounts.
- Enforce **least privilege** with IAM roles.
- Regularly audit **storage and firewall rules**.
- Automate security scans using IaC templates.
- Rotate **access keys** and **secrets** frequently.
- Use **encryption** at rest and in transit.

9. Communication with Cloud Providers

- Understand the **Shared Responsibility Model**.
- Contact the provider's security team via official incident response channels.
- Document timelines and actions for compliance.
- Use provider SLAs and support tiers to escalate response.

10. Lab – Cloud Credential Leak Simulation

Objective: Simulate an AWS IAM credential leak and respond to it.

Steps:

1. Generate IAM access keys (test environment only).
2. Simulate a leak by posting them on a private repo.
3. Use CloudTrail and GuardDuty to detect unauthorized access.
4. Rotate or delete leaked keys.
5. Apply least privilege IAM policies.
6. Set up automatic alerts for new key creation.

Module 9: Handling and Responding to Insider Threats

---

1. Introduction

An **insider threat** is a risk posed by individuals within an organization—such as employees, contractors, or business partners—who have access to internal systems or data and use that access to cause harm, whether intentionally or unintentionally.

Unlike external threats, insider threats are more difficult to detect due to the legitimacy of access. Responding effectively requires both technical and behavioral strategies.

2. Types of Insider Threats

Type	Description
Malicious Insider	Intentionally steals data, causes damage, or commits fraud.
Negligent Insider	Carelessly mishandles data (e.g., weak passwords, clicking phishing links).
Compromised Insider	User whose credentials or devices are hijacked by an external attacker.

---

3. Common Insider Threat Incidents

- Unauthorized file access or copying.
- Data exfiltration via USB, cloud storage, or email.
- Misuse of privileged access or admin rights.
- Installation of unauthorized software or malware.
- Leaking confidential business information.
- Abuse of email or internal communication platforms.

4. Indicators of Insider Threat Activity

- Accessing data not relevant to one's job role.
- Downloading large volumes of files, especially after hours.
- Using unauthorized devices or file-sharing platforms.
- Frequent policy violations or security alerts.
- Sudden changes in behavior or disgruntlement.
- Attempts to bypass security controls or audit logs.

5. Insider Threat Handling Process

Step 1: Detection

- Use **User and Entity Behavior Analytics (UEBA)** tools.
- Monitor system logs, file access patterns, and email traffic.
- Correlate alerts with HR data (e.g., exit notices, role changes).

Step 2: Analysis

- Validate whether the activity violates policies.
- Determine intent: accidental, negligent, or malicious.
- Identify the systems, data, or accounts impacted.

Step 3: Containment

- Revoke or limit access rights immediately.
- Disable compromised accounts or isolate affected devices.
- Block data transmission paths (e.g., external email, file sharing).

Step 4: Eradication

- Remove unauthorized tools or malware.
- Apply security policy updates and system patches.
- Educate user if the case was unintentional.

Step 5: Recovery

- Restore altered or lost data from backups.
- Reinstate systems with stricter access controls.
- Resume monitoring post-recovery to prevent recurrence.

Step 6: Lessons Learned

- Conduct a post-incident review with HR and management.
- Update policies and access controls.
- Train users and raise awareness on insider threats.

6. Tools for Insider Threat Detection

Tool	Purpose
SIEM (e.g., Splunk, IBM QRadar)	Collects and analyzes log data for abnormal activity.
UEBA (e.g., Exabeam, Varonis)	Detects deviations in user behavior.
DLP (e.g., Symantec, Digital Guardian)	Prevents unauthorized data movement.
Endpoint Monitoring (e.g., CrowdStrike, ESET)	Tracks endpoint activities and alerts on anomalies.

7. Case Study: Intellectual Property Theft by a Departing Employee

Scenario: A software developer planning to leave the company downloads the entire source code repository to a personal cloud drive.

Response Steps:

1. **Detection**:
    - DLP alerts on large file transfers.
    - UEBA flags unusual cloud storage usage.
2. **Containment**:
    - Immediately disable user's access to repositories and accounts.
    - Block external storage access on company network.
3. **Eradication**:
    - Ensure the downloaded data is no longer accessible externally.
    - Secure backup copies and log all access attempts.
4. **Recovery**:
    - Conduct code audits for potential backdoors.
    - Reinforce access control on intellectual property.

5. **Lessons Learned**:
    - Enforce offboarding procedures (access removal).
    - Apply least privilege and strict role-based access.
    - Regular insider threat awareness training.

8. Preventive Measures

- Implement **Zero Trust Architecture** (never trust, always verify).
- Enforce **least privilege** and time-bound access controls.
- Apply **multi-factor authentication (MFA)**.
- Monitor privileged accounts using PAM tools.
- Conduct **exit interviews** and immediate access revocation.
- Perform periodic audits of user activities and permissions.

9. Role of HR and Legal Teams

- HR should monitor behavioral changes and employee satisfaction.
- Legal team assists in handling breaches of policy or law.
- Policies should clearly define acceptable use and consequences.
- Coordinate with management to take appropriate disciplinary or legal actions.

10. Lab – Insider Data Leak Simulation

Objective: Simulate and detect a data exfiltration attempt.

Steps:

1. Create a user account with access to confidential files.
2. Simulate the user uploading files to Dropbox or sending them via email.
3. Use a DLP solution to generate alerts on sensitive data movement.
4. Apply response: block transfer, disable account, log incident.

Conclusion Générale :

La cybersécurité repose aujourd'hui sur une capacité à réagir rapidement et efficacement face aux incidents, qu'ils proviennent de courriels malveillants ou de compromissions réseau. L'analyse, la détection, et la réponse aux menaces doivent être structurées et soutenues par des outils adaptés, des processus clairs et une sensibilisation constante des utilisateurs.

En mettant en œuvre des mécanismes de prévention, en surveillant activement les systèmes, et en répondant de manière coordonnée aux incidents, les organisations peuvent limiter les impacts, protéger leurs données sensibles et renforcer leur posture de sécurité globale. La vigilance, la réactivité et l'amélioration continue sont les piliers d'une défense efficace face aux cybermenaces actuelles.