Step 1: Preparation for Incident Handling and Response

Objectives:

At the end of this episode, I will be able to:

Understand what Incident Handling and Response (IH&R) is.

Explain what Step 1, Preparation for Incident Handling and Response, of the IH&R process is.

Identify the various roles and responsibilities of the IH&R Team.

Define what the key action(s) and area(s) of focus for setting up a computer forensics lab are.

Evaluate the current security posture of the organization.

External Resources:

Step 1: Preparation for Incident Handling and Response

What is Incident handling and response (IH&R)?

The process of finding out when the incident occurred, its impact, and cause.

It is the practice of managing the incident response processes, such as preparation, detection, containment, eradication, and recovery to overcome the impact of an incident quickly and efficiently.

Incident handling and response processes are important to provide a focused and structured approach for restoring normal business operations as quickly as possible after an incident and with minimal impact to the business.

IH&R processes are initiated by organization’s IH&R project team, executive manager, head of the information security department, or any other person designated by management.

Step 1: Preparation for Incident Handling and Response -

Organizations determine the need for an incident handling and response (IH&R) process based on the current security scenario, risk perception, business advantages of having such processes, legal compliance requirements, organizational policies, and previous incidents.

Factors impacting the IH&R process plan include the type of assets, services offered, storage devices, servers, and networking devices.

Defining Vision and Mission statements -

The IH&R vision statement reflects an organization’s goals for incident management capabilities. It defines the requirement, scope, and purpose of an IH&R process after evaluating the assets, devices, and data that needs to be secured.

To determine the required IH&R process, the incident handlers need to audit all the systems, devices, networks, storage media, applications, policies, protocols, services, previous attacks, and other business aspects.

The IH&R mission statement defines the purpose and scope of the planned incident handling and response capabilities.

Management Approvals and Funding -

Incident handlers should obtain the appropriate permission from management, stakeholders, and other authorized personnel to perform IH&R processes.

Justify the funding requirements based on the use of business analysis data to scope and tailor the funding request to align with business requirements.

IH&R Plan -

The IH&R plan refers to the set of instructions incident response team needs to follow to minimize the damage caused due to the incident, utilize resources efficiently, and reduce the response duration.

IH&R Policy -

A set of guidelines used to achieve the goals and objectives of an incident response initiative set by the IH&R plan.

IH&R Procedures -

Also referred to as standard operating procedures (SOPs), provide detailed step-by-step processes to implement the IH&R plan and policy.

The procedure(s) should include implementation of the complete lifecycle of IH&R processes; including detection, containment, eradication, and reporting.

It should also mention in detail the process of performing each task, techniques involved, tools required, persons to contact in case of emergency, authorities for providing approvals, documenting the process, preserving the evidences, and reporting the process.

NOTE: The main objective of developing IH&R procedures is to create a set of tasks that IH&R can repeatedly execute that result in a certain degree of automation with a minimized probability of errors in plan and policy implementation.

Incident Handling Criteria -

Include a set of checklists, tables, cheat-sheets, and flow charts that help in decision-making during IH&R procedures.

The incident handlers and responders must define incident handling criteria based on the organizational requirements, type(s) of incident, impact, business disruption, and other details.

IH&R Team - Managed by the incident handler will perform vulnerability analysis, establish well-defined security policies, detect indicators of compromise, handle legal issues, manage public relations, and provide proper reports regarding the incident.

NOTE: The Incident Response Team is also called the Computer Security Incident Response Team (CSIRT).

What are the Roles and Responsibilities of the IH&R Team?

It is the responsibility of the team to provide a single point of contact for reporting security incidents and issues, as well as obtain proper permissions to perform the incident response processes.

They must always be aware of changes in legal and regulatory requirements to ensure that all processes and procedures are valid and compliant.

They must regularly review existing controls to evaluate their strength and ability to detect and stop attacks.

The team must recommend steps, procedures, and technologies that can help the organization to prevent future security incidents.

They must establish good relationship with local law enforcement agency, government agencies, key partners, suppliers, and incident handling and response teams at other companies. This will help them in finding the current incident trends, gathering threat intelligence data, sharing incident data, and discussing new security trends.

In addition, the incident response team is responsible to perform the following:

```
▪ Issue alerts and warnings about attacks, security vulnerabilities, and
malware to the authorities, security teams, stakeholders, clients, and customers

▪ Gather information about hardware and software vulnerabilities and devise
methods for fixing these vulnerabilities

▪ Perform first response procedures and handle the artifacts at the incident
site

▪ Conduct deep analysis of the incident to identify the attacker and attack
vectors
```

Roles -

Information Security Officer (ISO) - governs the security posture of the organization and bears the responsibility of all IH&R activities in the context of overall organizational information security.

Responsible for setting incident handling and response goals, approving the process, granting permissions, and contacting the stakeholders and other management authorities of the organization.

Is the head all the members of the IH&R team including the incident manager and incident handler.

Provides incident handling guidance and training to the security team members across the organization, evaluate the actions and consequences, and suggest corrective actions required to handle the incidents.

Incident Manager (IM) - will manage all the incident handling and response activities.

Must be a technical expert having clear understanding and experience of handling security issues.

Will focus on the incident as well as analyze and review the process of handling it from a management and a technical point of view.

Security Analysts - support the incident manager by working directly with the affected systems and networks.

Incident Coordinators - act as the link between various groups by connecting different stakeholders affected by the incidents, such as incident handling teams, legal, human resources, clients, and vendors.

They help in the communication process and keep everyone updated.

Forensic Investigators - responsible for maintaining forensics readiness across the organization and implementing effective incident handling and response.

They must also preserve and submit the evidence required to legally prosecute the attackers.

Threat Researchers - supplement security analysts by researching threat intelligence data.

They gather all details of prevalent incident and security issues and help in making the users aware of them.

They use this information to build or maintain a database of internal intelligence.

System Administrators - help in gathering system information, separating the impacted systems from the network, and analyzing system data to detect and verify the incidents.

They can also help in containment and eradication by installing new patches, updates, and upgrading the systems across the organizations.

They are also responsible for backup, recovery of systems, and analyzing logs on the systems.

Network Administrators - responsible to examine the computer network traffic for signs of incidents or attacks such as DoS, DDoS, firewall breach, or other malicious code.

They install and use network sniffing and capturing tools as well as loggers to identify network events of an attack.

They must analyze the network logs, gather logs of suspicious activity, and help in detection of incidents at primary level.

They perform the necessary actions required to block network traffic from the suspected intruder.

Internal Auditors - ensure that the organization complies with the regulations, business standards, and laws related to the regions of operation.

They must regularly audit the policies and procedures followed by the organization to maintain information security.

They must ensure that the systems, devices, and other network resources are up to date and compliant with industrial regulations.

They must identify and report any security loopholes to the management.

Financial Auditors - responsible for calculating the costs involved such as damages or losses by the incident and costs incurred in incident handling and response.

They must estimate the cost of cyber insurance and claim it when required.

Human Resources - responsible for tracking, recording, reporting, and compensating human resource for all the billable hours for performing duties throughout the event.

They are responsible for counseling people after the event and notifying various people as per the company policy.

Public Relations - serves as a primary contact to the media and informs media about an event.

It updates the website information and monitors media coverage.

It is responsible for stakeholder communication.

IH&R Team Models -

Centralized Incident Response Team - a single team handles all the incident response functions of a small organization. It is most effective for quickly responding to incidents.

NOTE: This structure is best suited for organizations operating from a single location.

Distributed Incident Response Teams - each location will have a separate IH&R team to handle incidents.

The organization must operate these teams under a single authority and maintain coordination between them.

NOTE: This model is effective for large organizations with more geographic diversity.

Coordination Teams - generally play an advisory role. They are not directly responsible for incident response.

Coordination teams provide other IH&R team in the organization with information and logistic support for incident response.

IH&R Team Staffing - Organizations can use one of the three incident response team staffing methods:

```
▪ Employees
▪ Partially Outsourced
▪ Fully Outsourced
```

Developing Incident Readiness Procedures -

Building incident response toolkits, setting up a forensic lab, establishing reporting facilities and establishing structured record keeping facilities are some of the procedures that should be performed.

Setting Up a Computer Forensics Lab -

A Computer Forensics Lab (CFL) is a designated location for conducting computer-based investigation of the collected evidence in order to solve the case and find the culprit. The lab houses the instruments, software and hardware tools, suspect media, and the forensic workstations required to perform investigation of all types.

Forensics labs should have licensing from the concerned authorities to be trustworthy. The authorities provide these licenses after reviewing the lab and the facilities it has for performing the investigation.

Licenses include:

o ASCLD/LAB Accreditation
o ISO/IEC 17025 Accreditation

Establish Reporting Facilities -

Develop and publish detailed policies for reporting security incidents

Incident reporting policy should include:

```
▪ Ways to report an incident - Email, phone, fax, etc.

▪ Whom to report the incident to - IH&R team, local law enforcement agencies,
senior management, network administrators, etc. according to the type of incident

▪ Details to be reported - Intensity of the incident, circumstances that reveal
the incident, summary of hosts involved, description of the activity, type of
confidential data involved, etc...
```

Educate users to identify and report security incidents

Make computer security incidents reporting forms and templates available to all users

Establish Structured Record Keeping Facilities -

Evidence, records, reports, and other sensitive material are to be kept in a highly secure location

Every organization must contain its own structured record keeping facility which can be accessed only by IH&R team authorized personnel

Storage of the records and evidence can be centralized or decentralized, depending on the requirement of the organization

All the sensitive material must be provided with appropriate classification system like tokens, tags, etc...

Evaluate the Current Security Posture -

It is imperative to audit current security posture of the organization before implementing the incident and response capabilities.

NOTE: This step focuses on checking whether the organization complies with proven security management methodologies and best practices.

Check whether the organization supports efforts to comply with government and industry regulations.

Evaluate security of all organizational resources to identify the vulnerabilities, risks, and threats.

Steps involved in evaluating security include:

```
▪ Security auditing
▪ Vulnerability assessment
▪ Threat analysis
▪ Risk management
▪ Cyber trend analysis/threat intelligence
```

Analyze all system components including information, public facing systems, websites, email gateways, remote access platforms, mail systems, DNS, firewalls, passwords, PFT, IIS, web servers, etc...

Implement Security Policy, Procedures, and Awareness -

Security Policy - should help the IH&R team in executing the incident handling process efficiently.

Security Procedures - The IH&R team should have standard operational procedures (SOPs) for dealing with different types of attacks.

The incident handlers will define the SOPs and include the specific technical processes, techniques, checklists, and forms the incident response team should use during the response process.

NOTE: Test and validate the procedures for their effectiveness before implementing them.

Security Awareness - Create awareness about the incident handling processes among the employees and discuss their role in the IH&R team for handling the incidents quickly and efficiently. Train the users to implement secure practices across their systems, networks, accounts, and data as well as in cooperating with the IH&R team during and post-incident response procedures.

Implement Security Controls -

Organizations must implement strict security controls. Implement the following security controls:

```
▪ Access controls
▪ Encryption
▪ Intrusion Detection Systems (IDS)
▪ Firewall
▪ Honeypot
▪ De-Militarized Zone (DMZ)
```

Organizations must also secure network communications by implementing the following:

```
▪ Packet filters
▪ Virtual Private Network (VPN)
▪IPsec
▪ Secure Shell (SSH)
```

Cyber Insurance -

Refers to a contract between the organization and an insurer to protect related individuals from different threats and risks.

Provides protection or offers compensation if the incidents occur.

Offers support for investigation, incident response, forensics, legal settlements, compliant issues, etc...