

# Incident Handling best practices, standards & frameworks

## Objectives:

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

Understand what Incident Response Automation and Orchestration is.

Explain what the Incident Handling and Response Best Practices from OWASP, ENISA and the GPG18 and Forensic readiness planning (SPF) are.

Identify the various Incident Handling Standards that an IH&R team member should be familiar with.

Define what key action(s) and area(s) of focus an IH&R team member should associate with the various Incident Handling Standards.

## External Resources:

Incident Handling best practices, standards & frameworks

Understanding Incident Response Automation and Orchestration -

Incident response automation is the process of superseding manual IR actions with automatic IR actions using machines and tools.

NOTE: Automation helps with efficient handling and response to security incidents by sending timely notification about the incidents across the organization.

The automation of IR process assists in performing the following actions:

- Helps in investigating incidents by providing data from different sources, for example, past incidents information, threat intelligence, and SIEM.
- Provides functionality allowing responders to give instructions and change the configuration of various security controls.
- Reducing the time taken for analyzing the incidents and responding to them efficiently.
- Enables responders to pay more attention to the alerts generated by critical incidents rather than checking every alert and prioritizing them in order to respond to the most critical ones.

Incident response orchestration combines the abilities of the incident response team, tools, and processes to respond and handle information security incidents efficiently

What is the difference between automation and orchestration?

IR automation converts the manual process into an automated process based on the preset instruction from the responders.

IR orchestration involves combining automation with machine and human intelligence to build an environment that learns and evolves with changing situations.

Incident Handling and Response Best Practices - best practices provided by OWASP, ENISA, and GPG18 and Forensic readiness planning (SPF)

### 1. OWASP -

Audit and Due Diligence

Create a Response Team - Document the roles and responsibilities of the team members and communicate this clearly to all relevant stakeholders

Create a Documented Incident Response Plan - at a minimum should cover roles and responsibilities, investigation, triage and mitigation, recovery, and documentation process.

Identify All Triggers and Indicators

Investigate the Problem - A thorough investigation will require input from the incident response team and might require input from external resources. The investigation will document the incident details, including what to look for, who to involve, and how to document what is found.

Triage and Mitigation - the triage process should include the following activities:

- o Classification of the incident
- o Incident prioritization
- o Assigning specific tasks to specific people

Recovery - the transition from active incident to standard monitoring. The recovery procedure should include the steps for transition given the specifics of the organization's environment and approach.

Documentation and Reporting - critical actions that will always occur before, during, and after incident response.

Process Review - Can help the organization to answer the following:

- o Should the organization increase or decrease the number of incident handlers?
- o Whether the organization should develop automated procedures for incident handling?
- o What risks did the organization identify during the incident that need to be followed up for action and monitored closely?

Practice - It is important that the incident response team understand how important mock drills and practice are to the organization.

## 2. ENISA -

Workflow - Organize periodic (for example, twice a year) workshops to develop and review a common incident handling workflow.

Incident Handling Process - Organizations should start with the simple model and then, as the team becomes more experienced, develop the procedure further.

Legal Officer - Train one or a few team members in the most important legal aspects related to incident activities.

Incident Report -

- o Use network monitoring systems (for example, intrusion detection systems or any other threat monitoring systems) to actively look for incidents in organizational network
- o Subscribe to services which provide information about compromised machines
- o Monitor blacklists for records from the location where the organization operates

Incident Verification

Final Classification ( classify incidents according to what is ) -

- o reported by incident reporters
- o recognized by incident handlers at the very beginning of the incident handling process

Policies - a quality review process should be in place. The feedback on policies is then used and incorporated into the existing policies to make sure these policies are up to date.

Entry and Exit Procedures - Exit procedures should always be followed without question. The exit procedures should aim at the following:

- o Removing access to systems with confidential information (changing password, revoking certificates and keys, blocking accounts, and so on.)
- o Logging the actions of the employee leaving
- o Backing up all work
- o Revoking their roles in incident management
- o Interviewing to hand over to the next person
- o Performing an exit interview to learn for the future
- o Announcing staff change to constituents, parent organization, and other teams

Eradication and Recovery

## 3. GPG18 and Forensic readiness planning (SPF) -

There are 12 significant principles that organizations should observe as part of adoption of forensic readiness policy, which are as follows:

Principle 1 - Organizations must develop and implement a forensic readiness policy.

Principle 2 - Forensic readiness policy should be owned at a director level within an organization.

Principle 3 - Organizations should have a recognized and consistent point of contact for establishing and maintaining relationships during planning and exercises, and to act as a focal point during investigations or crisis management. The point of contact should work closely with organizations' legal department and other relevant stakeholders during every stage of each investigation.

Principle 4 - Forensic readiness policy requirements and the supporting capability should be defined with regard to the level of information risk or actual business needs to undertake digital forensic investigations.

Principle 5 - Organizations should adopt a scenario-based forensic readiness planning approach that learns from experience.

Principle 6 - Organizations should closely integrate forensic readiness plans with incident management and other related business planning activities.

Principle 7 - Investigations should seek to produce the best standard of digital forensic evidence. Practitioners should adopt the principles published by Association of Chief Police Officers (ACPO).

Principle 8 - Any internal or external digital forensic capability employed by an organization should apply formal quality assurance processes, and all staff involved in handling evidence during investigations should have an appropriate degree of competence.

Principle 9 - Organizations should maintain the quality and effectiveness of their records management systems in order that specific business records can be produced as evidence in court or to address any legal or regulatory requirement.

Principle 10 - Organizations should provide appropriate records retrieval processes and mechanisms in order that any requirement to disclose information can be efficiently and securely dealt with. Such disclosures must be handled in accordance with all relevant legislation and regulations.

Principle 11 - An open and collaborative approach should be adopted within organizations, wherever possible, to gain acceptance of methods used to support investigations and incident handling. All methods of investigation and detection of information security incidents must be lawful.

Principle 12 - Organizations should have a management review process that improves plans in accordance with experience and new knowledge.

#### Standards -

ISO 27000 series - The information security standard developed and published by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). It provides a global framework for effective information security management for all types of organizations.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization

Annex A.16: Information security incident management defines the controls for incident management
---

A16.1.1 Incident Management Responsibilities: Management responsibilities and procedures shall be established for an effective incident response

A16.1.2 Incident Reporting: Information security events shall be reported through appropriate management channels as quickly as possible

A16.1.3 Vulnerability Reporting: Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services

A16.1.4 Incident Assessment: Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents

A16.1.5 Incident Response: Information security incidents shall be responded to in accordance with the documented procedures

A16.1.6 Learning from Incidents: Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents

A16.1.7 Forensics: The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence

ISO 27002:2013 - gives guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration the organization's information security risk environment(s)

Section 16: Information security incident management states that information security events, incidents, and weaknesses (including near-misses) should be promptly reported and properly managed

The ISO/IEC 27035 series - a standard for dealing with "Information Security Incident Management" which defines recommendations and best practices for developing an efficient incident management plan and allows organizations to prepare for the incidents.

This standard is divided into three parts:

- ISO/IEC 27035-1:2016 Principles of incident management
- ISO/IEC 27035-2:2016 Guidelines to plan and prepare for incident response
- ISO/IEC 27035-3 Guidelines for incident response operations (draft)

ISO/IEC 27035-1:2016 - Presents basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach for detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.

ISO/IEC 27035-2:2016 - Provides guidelines to plan and prepare for incident response:

- o Information security incident management policy and commitment of top management
- o Information security policies, including those relating to risk management, updated at both the corporate level and system, service, and network levels
- o Information security incident management plan
- o Incident response team (IRT) establishment
- o Establish relationships and connections with internal and external organizations
- o Technical and other support (including organizational and operational support)
- o Information security incident management awareness briefings and training
- o Information security incident management plan testing

The Payment Card Industry Data Security Standard (PCIDSS) - A proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

PCIDSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data.

High Level Categories of action in PCIDSS:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Incident Handling and Response Requirements in PCIDSS:

- 12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
- 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach

Federal Information Processing Standards (FIPS) 200 -

The minimum-security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.

The security-related areas include:

- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and security assessments
- Physical and environmental protection
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Planning
- Personnel security
- Risk assessment
- Systems and services acquisition
- System and communications protection
- System and information integrity

#### NIST SP 800 Series -

This series includes best practices, guidelines, recommendations, technical details, and annual reports of NIST's cybersecurity activities.

SP 800 publications address and support the security and privacy needs of US Federal Government information and information systems.

NIST develops SP 800-series publications in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283.

NIST's Special Publication (SP) 800-86 defines integrating the forensic techniques into incident response approach, while the NIST's Special Publication (SP) 800-61 Rev.2 is a computer security incident handling guide.

#### Standard of Good Practice from Information Security Forum (ISF) -

The Standard, along with the ISF Benchmark, the ISF's comprehensive security control assessment tool, provides complete coverage of the topics set out in ISO/IEC 27002:2013, NIST Cybersecurity Framework, CIS Top 20, PCI DSS, and COBIT 5 for Information Security.

NERC 1300 Cyber Security - The standard to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets. This cybersecurity standard applies to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity.

Request for Comments (RFC) 2196 - A guide to setting computer security policies and procedures for sites that have systems on the internet.

This standard is useful for developing information security, including network security, incident response, and security policies and procedures for information systems connected on the internet.

#### Cyber Security Frameworks -

Center for Internet Security (CIS) Controls - A prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

<https://www.cisecurity.org>

COBIT - A business framework for IT governance and management toolset enabling managers to bridge the gap between control requirements, technical issues, and business risks. The framework offers globally accepted principles, practices, analytical tools, and models to help increase the trust in, and value from, information systems.

COBIT emphasizes regulatory compliance, helping organizations increase the value attained from IT, enables alignment, and simplifies the implementation of the enterprise's IT governance and control framework.

The COBIT Framework is based on five key principles for the governance and management of enterprise IT that include:

- Meeting stakeholder needs
- Covering the enterprise end-to-end
- Applying a single integrated framework
- Enabling a holistic approach
- Separating governance from management

<https://www.isaca.org/resources/cobit>

NIST SP 800-61 - Step-by-step instructions for new, or well-established, incident response teams to create a proper policy and plan.

NIST recommends that each plan should have a mission statement, strategies and goals, an organizational approach to incident response, metrics for measuring the response capability, and a built-in process for updating the plan as needed.

It includes the lifecycle for the incident handling and response that contains different phases such as:

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

<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>