

CompTIA Security+

Lecture 10

SY0-701

Risk Management and Incident Response

By
Dr. Khaled ELMenshawy

Lecture

10

LEARNING OUTCOMES

- Understanding risk management lifecycle.
- Understanding risk identification process and risk register.
- Differentiate between qualitative and quantitative analysis.
- Recognize risk treating methods.
- Understanding risk monitoring and reporting.
- Understanding supply chain risks.
- Understanding incident response process.
- Understanding threat hunting and Root Cause Analysis.
- Understanding incident response training and testing
- Understanding digital forensic procedures.
- Understanding Hardening

What is Likelihood?

Likelihood defines the level of certainty that some incidents is going to happen. There's two different ways to measure likelihood when we're talking about risk:

- **Quantitative**; Availability of historical and statistical data that enable us to calculate the percentage of the incidence of the threat.
- **Qualitative**; measuring things that are hard to put a number against. So using terms like (Low/Medium/High) or numbering system like (1 to 5) where (1) is extremely weak and (5) is extremely high.

What is Impact?

Impact is the actual harm caused by a threat. So, in order to have that impact you actually have a threat that has actually harm the system.

Using **likelihood** and **impact** if we got a lot of risk.

The National Institute of Standards and Technologies (NIST) has a big document called **SP 800-30**. This document includes all kinds of threats and vulnerabilities that the typical security person might be exposed to.

Why does risk is important in Cybersecurity?

Organizations need to manage their cybersecurity risks to protect their sensitive data and systems from malicious actors. It is an essential part of any organization's security program.

- How do we secure our IT infrastructure?
- How do we ensure the integrity of our data while making the employees able to access everything they need to?



*And that, in essence, is what **cybersecurity is all about understanding and protecting our assets, recognizing risks, addressing vulnerabilities, and minimizing the risks.***

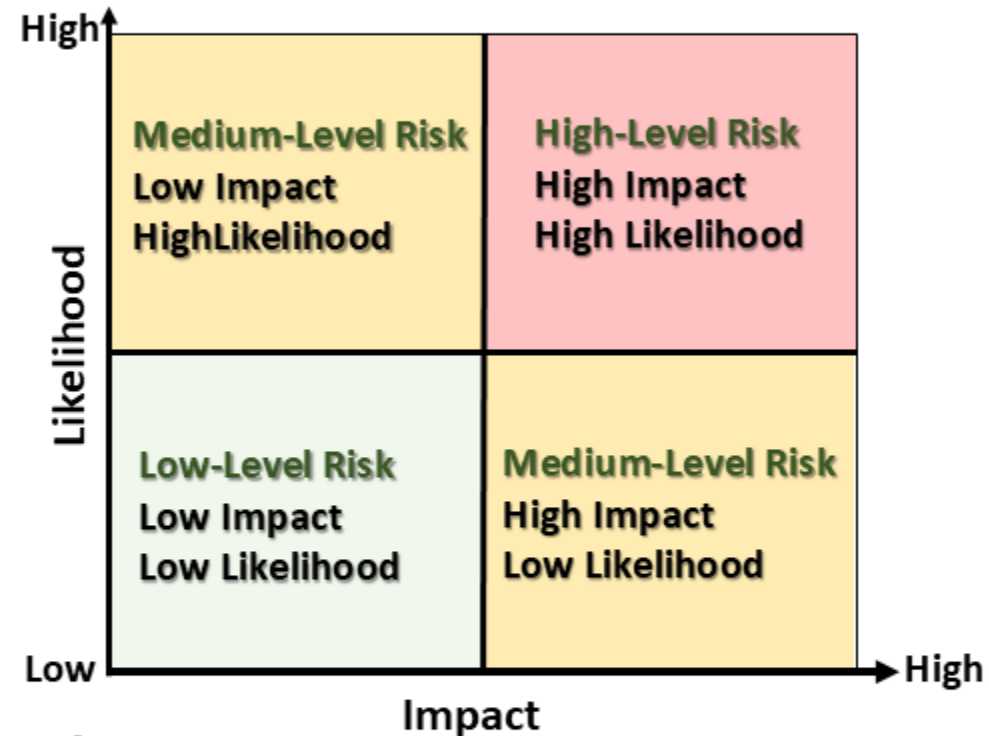
What is the Risk?

Risk is the likelihood of a threat actor taking advantage of a vulnerability by using a threat against an IT system asset.

$$\text{Threat} \rightarrow \text{Vulnerability} = \text{Risk}$$

Thus, $\text{Risk} = \text{Probability}(\text{Likelihood}) \times \text{Impact}$

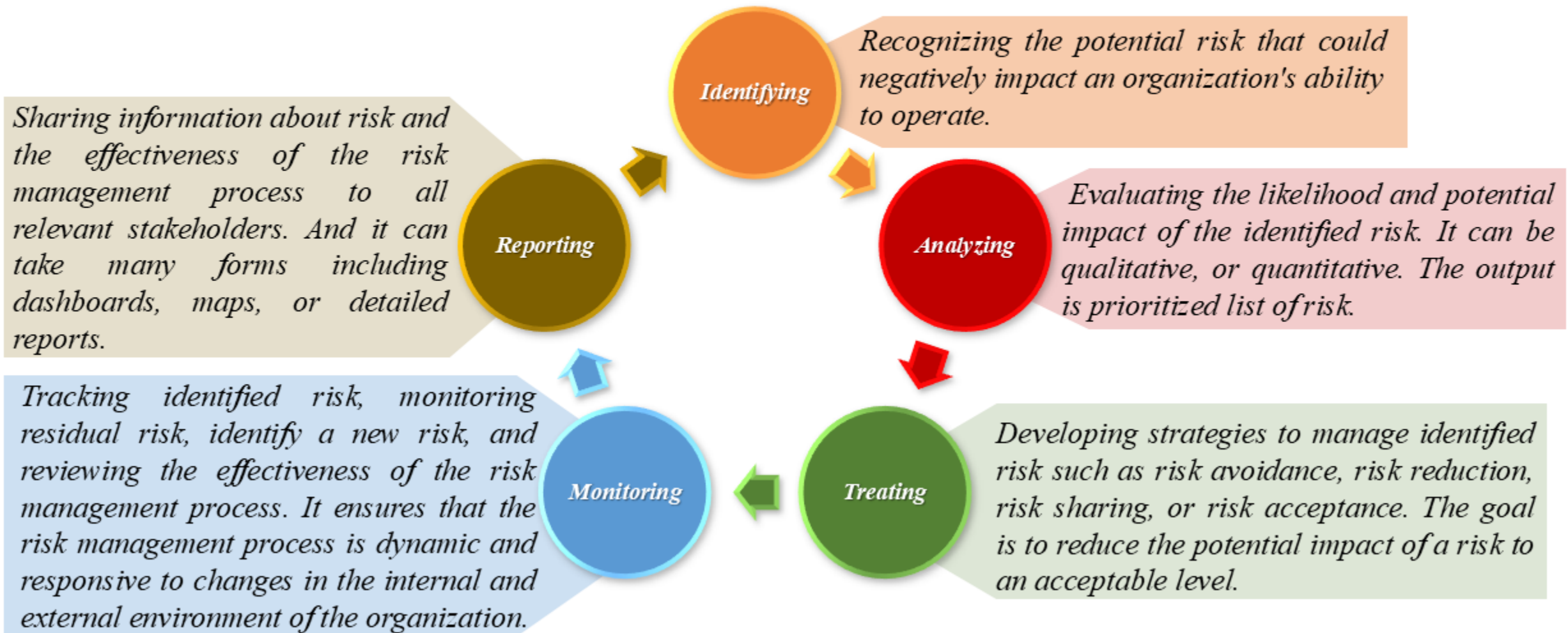
- Probability or Likelihood is a percentage value where $0 < \text{Probability} < 1$.
- Impact is a value where $0 < \text{impact} < 5$.



What is the Risk Management?

Risk Management a fundamental process that involves *identifying*, *analyzing*, *treating*, *monitoring*, and *reporting* risks to ensure that an organization's objectives are achieved.

Risk management Lifecycle



What is the Risk Identification?

Risk Identification; is recognizing potential risks that could negatively impact an organization's ability to operate or achieve its objectives.

Techniques can be used in risk identification, such as *brainstorming*, *checklists*, *interviews*, or *scenario analysis*.



The concepts of business impact analysis:

- *Recovery Time Objective (RTO)*; it is the *target time within which a business process must be restored* after a disruption to avoid unacceptable consequences.
- *Recovery Point Objective (RPO)*; It represents the *maximum acceptable amount of data loss* measured in time.
- *Mean Time to Repair (MTTR)*; It represents *the average time required to repair* a failed component or system.
- *Mean Time Between Failures (MTBF)*; It represents *the average time between failures*. A higher mean time between failures indicates a system that fails less frequently, which can be a sign of a reliable and well-maintained system.

[illegible]

Risk register components:

- **Risk Description**; is *providing a detailed description of the risk*. The description should be clear and concise enabling anyone reading the risk to understand the risk without requiring additional information.
- **Risk Impact**; refers to the *potential consequence or damage that a risk can cause if it occurs*. It could be in terms of cost, time, quality or any other critical objective.
- **Risk Likelihood**; is the *chance of a particular risk occurring*, interpreted using qualitative values such as low, medium, or high.

- **Risk Outcome**; is *the result of the risk, if it occurs*, it is directly related to the impact and likelihood of the risk. The outcome *helps in understanding the overall effect of the risk on the organization*. It involves examining how organization operations and objectives might change due to the impact of the risk event.
- **Risk Level (threshold)**; is determined by combining the impact and likelihood. It is the *scoring mechanism used to compute risk scores for identified risks*. It helps prioritize risk in deciding which risk require immediate attention, and the risk level can be categorized as high, medium, or low.
- **Risk Cost**; is the *financial impact it could have on the organization if the risk occurs*. It could be the cost of damage or the cost of mitigation of that risk.

- **Risk Tolerance**; or **risk acceptance** is the *degree of uncertainty an organization or individual is willing to handle while achieving their objectives **per individual risk***.
- **Risk Appetite (Risk Profile)**; is the *level of the total risk that an organization is willing to accept while pursuing its objectives*, and before any action to reduce the risk (including financial and operational impacts). *There are three main types of risk appetite*:
 - **Expansionary**; the organization's willing to take on more risk for the potential of higher returns.
 - **Conservative**; the organization prefers to take less risk even if it means accepting lower returns. This is common in businesses that prioritize stability and long-term sustainability.
 - **Neutral**; balance between taking calculated risk and ensuring steady growth.

- **Key Risk Indicators (KRI)**; are metric for *measuring the likelihood that the combined probability of an event and its consequences will exceed the organization's risk appetite* and have a profoundly negative impact on an organization's ability to be successful. In other words; they are metrics that predict potential risks that can negatively impact businesses.
- **Risk Owner (Responsibility)**; is the *person or group responsible for managing the risk*. They are responsible for monitoring their risk, implementing mitigation actions and updating the risk register as necessary.

What is the Qualitative Analysis?

Qualitative Analysis; is a *method of assessing risk based on the potential impact and likelihood of their occurrence*. It involves categorizing risk as high, medium, or low based on the potential effect of the project objectives.

The primary focus when using qualitative assessments is to quickly identify risks and generally use either numerical ratings (1-5) or colors (green, yellow, and red) to rank risks based on their likelihood of occurrence (frequency).

Using qualitative analysis;

The likelihood of a risk is determined based on past experience, statistical analysis or expert judgment.

Also, The impact could be in terms of cost, time, quality of other critical objectives. Both likelihood and impact are rated qualitatively as low, medium, or high.

Likelihood	Almost Certain		2 Risks	2 Risks	3 Risks	3 Risks	3 Risks
	Very Likely		4 Risks	5 Risks	4 Risks	3 Risks	2 Risks
	Likely		2 Risks	2 Risks	5 Risks	2 Risks	3 Risks
	Unlikely		3 Risks	5 Risks	2 Risks	3 Risks	4 Risks
	Rare		3 Risks	2 Risks	3 Risks	4 Risks	3 Risks
	Unspecified	6 Risks					
	Unspecified	1 Negligible	2 Low	3 Medium	4 High	5 Severe	
Impact Factor							

What is the Quantitative Analysis?

Quantitative Analysis; is a method of *evaluating risk that uses numerical measurements*. It provides a probabilistic analysis of potential future events and is typically used for financial, safety and scheduling decisions.

Quantitative risk assessments provide actionable results using cost-benefit analysis to easily prioritize risk mitigation processes and answer questions surrounding the financial and data impact of a cyber breach on your business. It takes more time and needs more resources and data.

Key components of Quantitative Analysis:

- Exposure Factor (EF); is the proportion of an asset that is lost in an event. It is expressed as a percentage between zero, no loss, and 100%, which is total loss.
- Single Loss Expectancy (SLE); is the monetary value expected to be lost in a single event. It's calculated by multiplying the value of the asset by the exposure factor.
- Annualized Rate of Occurrence (ARO); is the estimated frequency with which a threat is expected to occur within a year.
- Annualized Loss Expectancy (ALE); is the expected annual loss from a risk. It is calculated by multiplying the single loss expectancy by the annualized rate of occurrence.

Example:

If the server value equal 100,000 L.E and EF equal is 50%. If the server crashes once every two years, Calculate SLE and ALE.

Single Loss Expectancy (SLE) = Asset value $\times$ Exposure Factor (EF).

$$= 100,000 \text{ L.E} \times 50\% = 50,000 \text{ L.E}$$

The server crashes every two years, then Annualized Rate of Occurrence (ARO) = $\frac{1}{2} = 0.5$

Then Annualized Loss Expectancy (ALE) = SLE $\times$ ARO

$$= 50,000 \times 0.5 = 25,000 \text{ L.E}$$

There are four primary risk management strategies:

- *Transfer*; is *shifting the risk from the organization to another party*. insurance is the most common method of risk transference. risk transference does not eliminate the risk entirely, it simply shifts the responsibility for dealing with the financial consequences of the risk
- *Accept*; is deciding to *deal with the risk if and when it occurs*. This strategy is often used when the cost of preventing the risk is greater than the potential loss or when the risk is unlikely to have a significant impact.
- *Avoid*; is *changing plans or strategies to eliminate the risk entirely*. This is often the chosen strategy when the risk is too great to accept or transfer.

- *Mitigate*: is taking steps to reduce the likelihood or impact of that risk. This is the most common risk management strategy. It can involve a wide range of activities.



What is the Risk Monitoring?

Risk Monitoring; is the *process of tracking and identifying risks*, monitoring residual risks (*the likelihood and impact after specific mitigation, transference, or acceptance measures have been applied*), control risk (*how much less effective a security control has become over time*) identifying new risks, executing risk response plans and evaluating their effectiveness.



What is the Risk Reporting?

Risk Reporting; is the *process of communicating information about risk management activities, including the results of risk identification, assessment, response, and monitoring to the stakeholders of the business.* This information is often presented in the form of a risk report.



Why risk monitoring and reporting are important?

- *Informed decision making*; is providing valuable information that can be used in decisions making process.
- *Risk mitigation*; organization can be identified when a risk is becoming more likely or when potential impact is increasing. This allows them to take action to mitigate the risk before it becomes a problem.
- *Stakeholder communication*; Keep stakeholder informed by updates.
- *Regulatory compliance*; help to demonstrate compliance with security regulations.

What is the Supply Chain Risks?

Supply Chain Risks; is the vulnerabilities and threats that transfer to the organization through the products or services made or offered by a third party (supply chain vendor) which can be hardware manufacturers, software developers, or service providers.

Supply Chain Vendors types:

➤ *Hardware manufacturers;* when buying a product like a router, firewall or a switch from a specific vendor (supplier), it becomes clear that they are composed of hundreds of distinct little components. Each of these components is sourced from another various vendors (suppliers), and these components can each hold a potential vulnerability.

To prevent issues with our hardware, we really need to ensure that we conduct rigorous supply chain assessments to trace the origins of our hardware and to determine the integrity of the components in our enterprise networks.

➤ *Software developers and software providers;* is going to come from the software we purchase and install onto that enterprise network. The software could include vulnerabilities that transfer to the organization's network once it is installed.

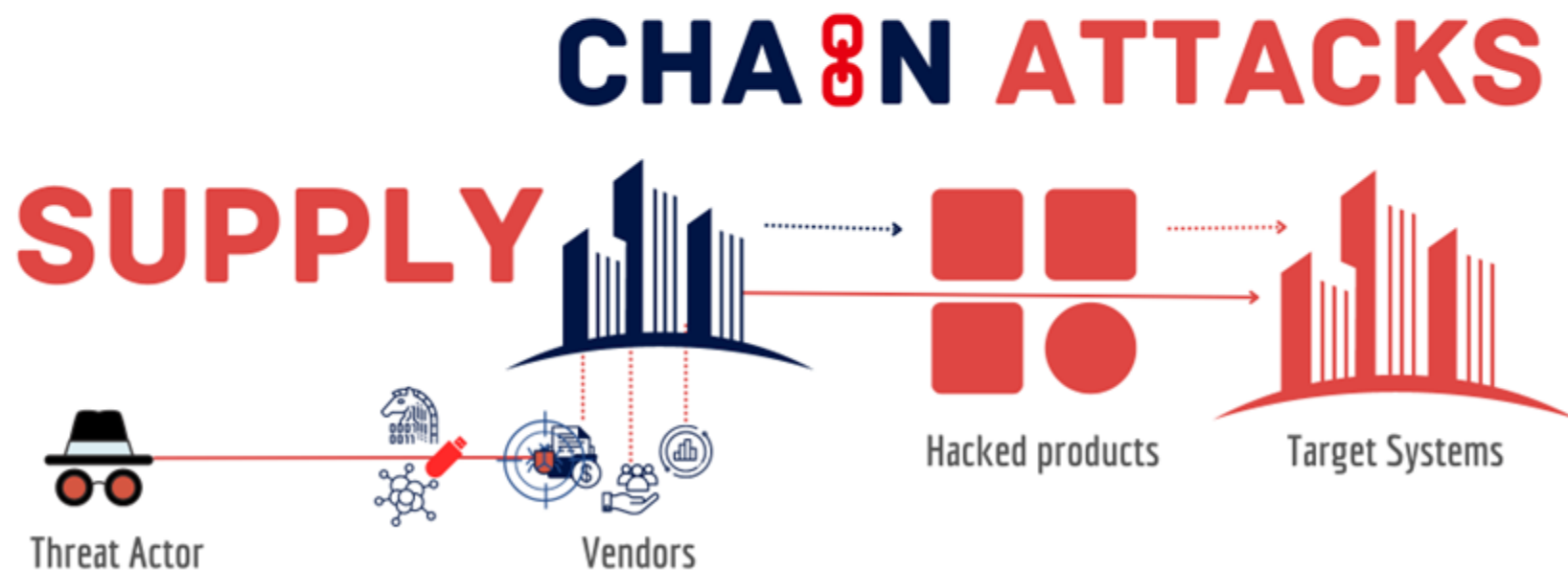
To avoid software risks, ensure it is properly licensed, authentic, and free of known vulnerabilities or bugs. Additionally, the software should be scanned with a good antivirus or anti-malware solution to ensure that it's free of any malicious code.

➤ *Service providers*; are vendors that provide the organization by a range of technology services and support tools such as cloud services (IaaS, SaaS, PaaS).

To avoid Service providers risks, evaluate their data security measures and ensure confidentiality and integrity .

What is the Supply Chain Attacks?

Supply Chain Attacks; is an attack that involves targeting a weaker link in the supply chain products or services to gain access to a primary target (organization network).



What is the Incident Response Process?

Incident Response Process; is *the process by which an organization handles a data breach or cyberattack.*

An *incident is an act of violating a security policy.* There are different ways to define the phases of an incident response, but one of the most commonly used is produced by National Institute of Standards and Technology (NIST). “*Computer Security Incident Handling Guide*”, special publication number 800-61

NISTNational Institute of
Standards and Technology
U.S. Department of CommerceSpecial Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute
of Standards and TechnologyPaul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

There are seven phases involved in incident response process:

- **Preparation;** is a phase where *cybersecurity professionals try to make the system resilient to attack* by hardening their systems and networks. The preparation phase is focused on *doing everything needed to get ready for future incident to occur*. During the preparation phase, also conducting a training, testing, and exercising of the staff.
- **Detection;** is a phase focused on *determining whether a security incident has occurred*.
- **Analysis;** is a phase when *an incident is examined and evaluated*. Analysts work to understand the scope and impact of the incident and to provide valuable insights into the nature and potential consequences.

- **Containment;** is a phase used to *limit the scope and magnitude of the incident by securing data and minimizing the impact on business operations* and the organization's customer and business partners.
- **Eradication;** is a phase focused on *removing the malicious activity from a given system* or network.
- **Recovery;** is a phase focused on *restoring the effective system and services to their normal secured state*. Recovery often involves restoring a system from a backup, installing security patches, or implementing configuration updates, to ensure that any vulnerabilities exploited during the incident have been fully and appropriately remediated.

➤ **Post-incident activity;** is a phase occurs after the system has been contained and malicious activity was eradicated, and the system is fully recovered and restored to operations. During the post-incident activity, **there are three major actions that occur:**

- **Root cause analysis;** is *identifying the initial source of an incident* and how to prevent it from occurring again. This analysis usually occurs using a four-step process:

- 1) Define the incident.
- 2) Determine the causal relationship that led to the incident.
- 3) Identify an effective solution.
- 4) Implement and track the solutions to ensure that the incident is fully resolved.

- **Lessons learned process;** is a formalized method to *document the things we have experienced during an incident*, what went right, what went wrong, and what could we do better next time.
- **After-action report;** is a *formalized report that collects information about what happened*. In this report, you should have the root cause analysis and the recommendations for improvements from the lessons learned.

What is the Threat Hunting?

Threat Hunting; is a cybersecurity technique that is *designed to detect the presence of threats that have not been discovered by normal security of monitoring*. Essentially, threat hunting is the act of being proactive in your defense as opposed to being reactive.

Threat Hunting involves the following:

- **Hypothesis;** is *performing threat modeling and determining what potential events have the highest likelihood and highest impact* if they were to occur.
- **Profiling threat actors and activities;** is *creating scenarios that show how a perspective attacker might attempt an intrusion* and what their objectives might be.

Incident Response Training and Testing

What is the incident response training and testing?

Training; is *ensuring employees and staff understand the processes, procedures, and priorities during an incident response.* **A first responder** should be trained on the *procedures* that he/she is going to follow when incident happen, *re-image a machine, removing malware,* and *change configuration settings.* **A manager** should be trained on *risk versus reward,* *managerial decision making* and *communication across the organization and outside the organization,* **A user** should be trained on the *way to report* if they suspect an incident is occurring.

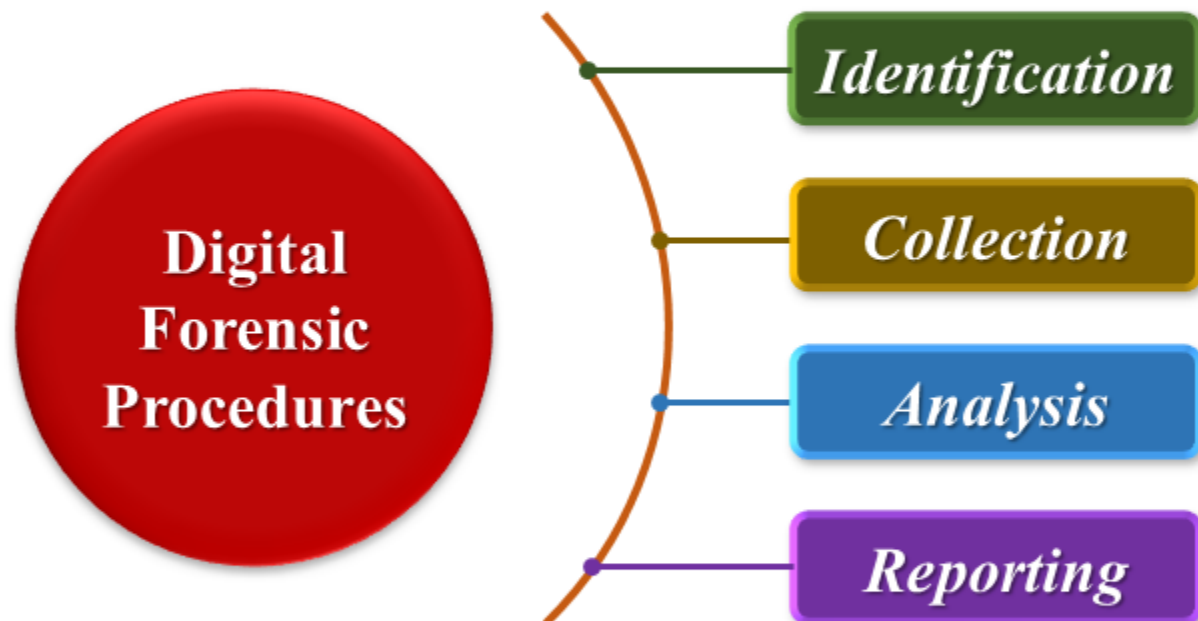
Incident Response Training and Testing

Testing; is *the practical exercise of incident response procedures*. With training, we are going to teach you what to do. In testing, we are going to make sure you know how to do it. when designing the test, we can do it in one of three major ways:

- **Tabletop Exercise (TTX);** is using an *incident response scenario against a framework of controls* and *not physically doing it in our networks*.
- **Penetration test;** is *simulating network intrusion based on threat scenarios*.
- **Simulation;** is *replicating a real incident for hands-on experience*. Simulation exercises could be *simple scenarios* (phishing attacks or ransomware infection) to *complex scenarios* (multi-stage attacks and data breaches).

What is the digital forensic procedures?

Digital forensic procedures; is a systematic process of *investigating and analyzing digital devices and data to uncover evidence for legal purposes*, often in the context of criminal investigations or legal disputes.



➤ **Identification;** is *ensuring the safety of the scene*, securing it to prevent any evidence contamination, and determining the scope of the evidence to be collected.

➤ **Collection;** is *the process of gathering, preserving, and documented physical or digital evidence*.

According to the NIST Special Publication 800-86 the data that should be collected are:

- Data from the system's memory.
- Capture data from the system state (ARP cache, routing table, etc.).
- Data from your storage devices.
- Capture network traffic and logs.
- Remotely stored archive data, including backups, cloud storage.

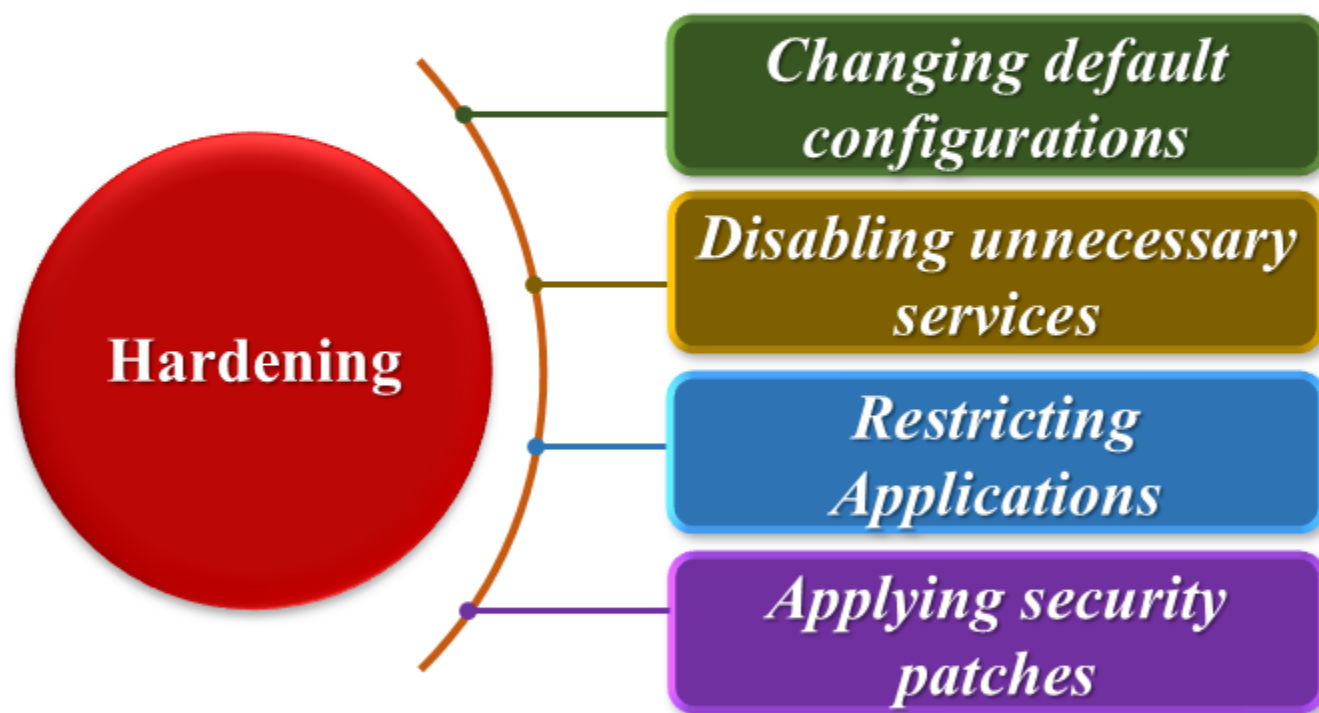
Chain of Custody; is a documented and verifiable record that tracks the handling, transfer, and preservation of digital evidence from the moment that it's collected until it is presented in a court of law. When collecting the evidences, it should be collected using processes such as:

- ***Disk imaging;*** is creating a bit-by-bit or logical copy of a storage device, preserving its entire content, including deleted files and unallocated space
- ***File carving;*** is extracting files and data fragments from storage media without relying on the file system.

- **Analysis;** involves *systematically scrutinizing the data to uncover relevant information*, such as potential signs of criminal activity, hidden files, timestamps, and user interactions.
- **Reporting;** is *documenting the finding, processes and methodologies used during digital forensic investigation*. This report serves as crucial evidence in legal proceedings and trials.

Legal Hold; is a *formal notification that instructs employees to preserve all potentially relevant electronic data, documents, and records*. Legal hold ensures that no evidence is tampered with, deleted, or lost. Preservation measures may include *making backup copies of electronic records, isolating critical systems, and implementing access controls* to prevent any unauthorized alterations.

➤ **Hardening**; is *the process of enhancing the security of a system, application, or network* by implementing a series of measures and configurations that reduces its exposure to vulnerabilities and potential threats.



➤ ***Changing default configurations;*** whenever installing a new piece of hardware or software, there are certain default configurations (factory default setting), usually they are not configured with security, but instead, they're configured to allow a new user to more quickly install and use the new piece of hardware or software.

- ***Default Passwords;*** Change the pre-configured password. Since these default passwords are published in the manual and in the manufacturer's online knowledge base articles, it is known to the public and must be changed to prevent unauthorized access to your network.

To provide the best level of protection possible *the password must meet the following parameters:*

- ✓ **Long;** Minimum 12 characters.
- ✓ **Unique;** used for one account only and not reused anywhere else.
- ✓ **Complex;** Consists of Uppercase and Lowercase letters, numbers, Special characters such as (! @ # \$ % ^ & * () - _ + = { } [] : ; , . ? / etc.).
- ✓ **Time Limited;** Must be changed after a certain period (e.g., 45 days).

- ***Disable any unneeded ports and protocols;*** each active and open port is going to act as a potential opening for an attacker to gain access into the systems. By minimizing the number of active ports (such as Telnet port 23) and running protocols, leads to reduce the attack surface. Also changing to secure version of protocols such as SMTP to SMTPS, and HTTP to HTTPS.

➤ **Disabling unnecessary services;** Services are a *type of application that runs in the background of the operating system, and it performs various functions* such as the print spooler. Any services that are unneeded should be disabled within the operating system.

Every service that runs:

- Listens on a port.
- Accepts requests.
- Has code that may contain vulnerabilities.
- Consume RAM, CPU, Disk I/O.
- Needs Patching, monitoring, and Reduce stability and performance.

➤ ***Restricting Applications;*** Each application installed in the device will take up valuable disk space, and is going to introduce additional code, that means additional vulnerabilities to the system because *every application that's installed on a computer must be managed, updated, and patched for security, and it provides yet another chance for a vulnerability to be introduced into our systems.*

The process of configuring a workstation or a server to provide only essential applications and services is known as ***Least functionality.***

Secure baseline image; is an image used for all the workstations that are getting installed in the company when they're first installed at the user desk. Now, this image will have the operating system and the minimum applications required for that organization.

- ***Applying security patches;*** When a software developer discovers a bug or error in their code, they're going to develop a code fix for it, and then release a software patch. Patch management can be a manual process, an automated process, or a combination of both.
- ***Hotfix;*** is a software patch that *involves a security issue* that should be applied immediately.
 - ***An Update;*** is *new functions and features*, can often introduce new security vulnerabilities that are going to require another hotfix to be implemented.
 - ***Service Pack;*** a bundle of security patches and hotfixes into a single installer.

