ITDO6014
ETHICAL HACKING AND FORENSICS

Module 2: Digital Forensics Fundamentals

Introduction to Digital Forensics

- Digital Forensics (also widely known as computer forensics) is the process of investigating crimes committed using any type of computing device (such as computers, servers, laptops, cell phones, tablets, digital camera, networking devices, Internet of Things (IoT) device or any type of data storage device).
- Digital forensics is also responsible for examining attacks originated from cyberspace like ransomware, phishing, SQL injunction attacks, distributed denial-of-service (DDoS) attacks, data breach and any sort of cyberattacks that cause financial or reputation loses.

Introduction to Digital Forensics

- The ultimate goal of a digital forensics investigation is to preserve, identify, acquire and document digital evidence to be used in the court of law.
- Under this definition, digital forensics is used to investigate any crime that involves using electronic devices, whether these devices were used to commit or as a target of a crime.
- Having a digital forensics capability becomes very important for modern organizations to investigate internal policy violations and external attacks against their computerized systems, for instance, big corporations already have such capability that exceeds the capability of many government police departments.

Objectives of computer forensics

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.

Objectives of computer forensics

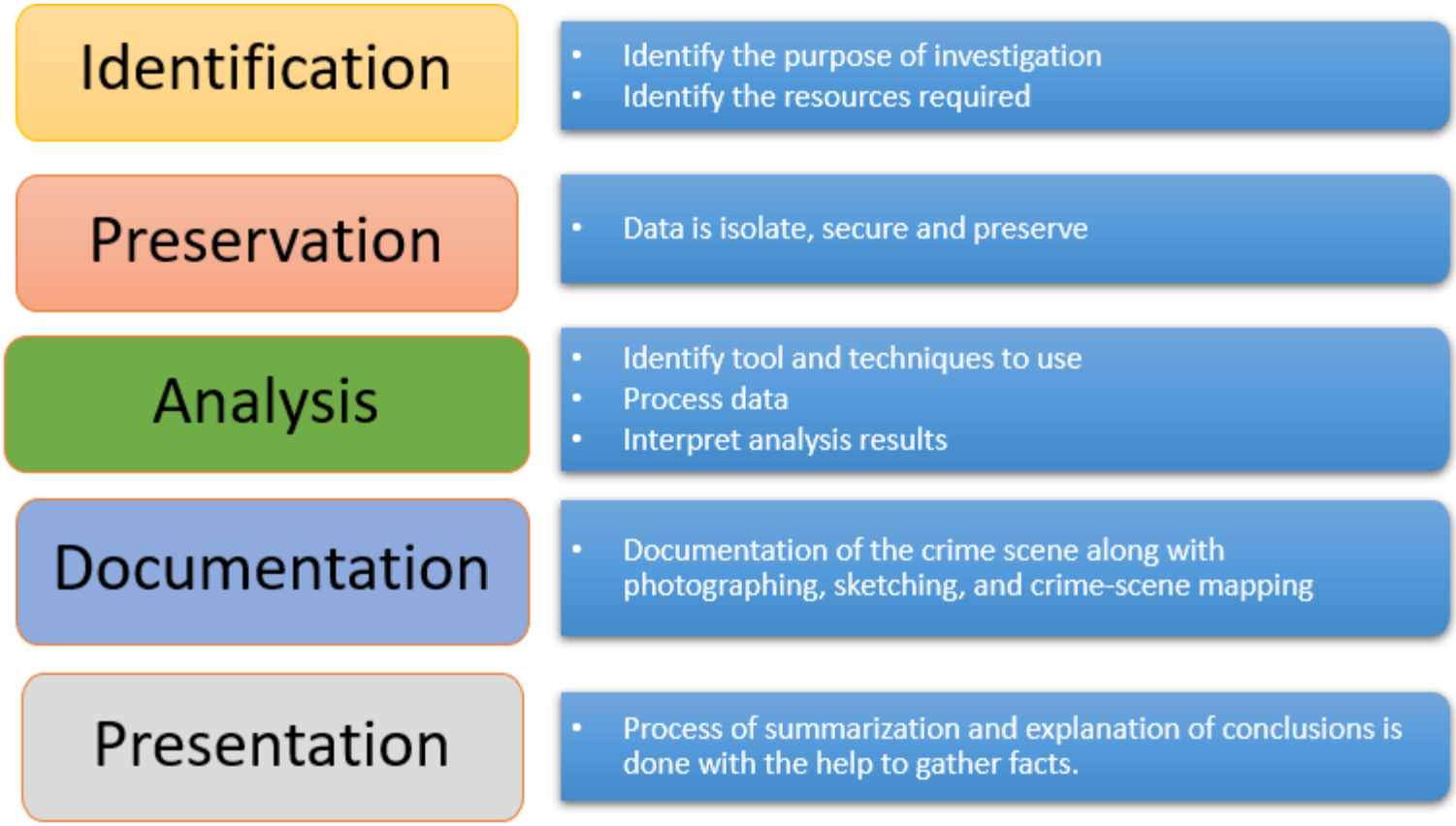
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

Process of Digital forensics

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

Process of Digital forensics



Process of Digital forensics

Identification

- It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).
- Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation

- In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

Process of Digital forensics

- **Analysis**
- In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.
- **Documentation**
- In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Process of Digital forensics

- **Presentation**
- In this last step, the process of summarization and explanation of conclusions is done.
- However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

Types of Digital Forensics

- The types of digital forensics are:
- **Disk Forensics:**
- It deals with extracting data from storage media by searching active, modified, or deleted files.
- **Network Forensics:**
- It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.
- **Wireless Forensics:**
- It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyze the data from wireless network traffic.

Types of Digital Forensics

- **Database Forensics:**
- It is a branch of digital forensics relating to the study and examination of databases and their related metadata.
- **Malware Forensics:**
- This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.
- **Email Forensics**
- Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.
- **Memory Forensics:**
- It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

Advantages of Digital forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

Digital Evidences

- To bring the guilty to justice, correctly collecting, analyzing, and presenting the right evidence is quintessential. Before proceeding with the investigation, however, you're going to need to know where and how to look for certain digital evidence.
- After all, collecting different types of digital evidence requires different tools and methodologies to be used in the process.

Digital Evidences

- When it comes to digital evidence, in essence, it can be anything from logs and all the way to video footage, images, archives, temporary files, replicant data, residual data, metadata, active data, and even data that's stored inside a device's RAM (otherwise known as volatile data), as long as they are regarded as part of clue for a digital investigation.

Digital Evidences

- **1. Logs**
- **OS logs**
- Examples include events pertaining to system access, security alerts, the duration of a user's login session, when the device was shut down, etc.
- Typically, OS logs are stored in a particular system directory (the exact location depends on the operating system in use).

Digital Evidences

- **Database logs**
- Since they mostly reveal what changes were made to a particular database, these can be a vital source of crime evidence as well as a useful approach for debugging and troubleshooting in the unfortunate event of any technical issues with the database in question.

Digital Evidences

- **Email logs**
- Often presented in a CSV format, email logs can reveal certain details about the sender and content, which includes their email address, time and date of delivery, delivery status, cc, bcc, subject, content type, and error codes (if applicable), while mostly stored in the email's header.
- many cyber criminals use email as their go-to communication channel for the purposes of extortion, financial crime, and distributing illegal materials.
- Alongside email logs, any file attachments also count as one of the evidence types, so they should be closely examined, right along with the server logs through which the email was sent.

Digital Evidences

- **Phone logs**
- A phone's infrastructure encompasses various kinds of evidence, including photos taken, videos recorded, system logs, app logs, and call logs, the latter of which contain crucial details such as the duration of a call, inbound and outbound numbers, etc.

Digital Evidences

- **Network logs**
- These can be viewed as different types of evidence because they also contain clues about what an individual was doing on the internet, including what websites that person has visited, what messages were exchanged with another party, and what the content of the messages was.

Digital Evidences

- **IP logs**
- Since everyone who browses the internet gets assigned a unique IP address, knowing this crucial detail allows a digital forensics investigator to trace their real identity and physical location by cooperating with ISPs.
- IP logs are often a crucial source of evidence when trying to hunt down a cyber-criminal.
- **Server logs**
- These kinds of logs are like digital journal that records the events taking place on a server. Examples include IP addresses that connected to the server at any point in time and also the duration of each session, any error logs, usernames that were used during the time of access, etc.

Digital Evidences

- **Device fingerprints**
- There are many forensic categories of devices where evidence can be found, and each device can generate a unique fingerprint that consists of its hardware specs, the OS it's running (down to the exact version), and even other odd bits and pieces such as the graphics drivers it's running or what fonts are installed.
- Therefore, even if a cybercriminal attempts to mask their IP when connecting to a server, the device fingerprint can be collected regardless.

Digital Evidences

- **2. Video footage and images**
- **3. Archives**
- Since archives are regular files accessible straight from the file explorer, they fall into the visible data type group.
- Various types of evidence can come in the form of an archive, whether it be:
- Zip/Rar/similar files
- Databases
- Backups
- Software-specific archives
- etc.

Digital Evidences

- **4. Active data**
- Have you ever noticed how popular content editors and word processors like Microsoft Word often create temporary files on your hard drive while you're in the midst of typing and working on a document?
- This is what's referred to as active data and it's a visible data type.
- In fact, many operating systems and applications can create this type of file, including:
- Email clients
- Image viewers
- Word processors
- Scanners, etc.

Digital Evidences

- **5. Metadata**
- metadata falls into the invisible data type category because it typically requires special software to be able to view it.
- For instance, a photo file on a hard drive or storage media can contain additional data regarding the file's creation such as where the photo was taken, otherwise known as EXIF data.

Digital Evidences

- **5. Metadata**
- This data is attached to the file and reveals details such as:
- Where the photo was taken
- The time and date the photo was taken
- What lens was used during the process
- The camera's model and brand
- Color profile and space
- and more.

Digital Evidences

- **6. Residual data**
- Residual data is deleted or overwritten data that may contain digital evidence if successfully recovered. Since it's not typically visible through a file browser, it's classified as an invisible data type.
- To understand the concept, you have to keep in mind that when someone deletes a file from a device, the data is still there – it's just unlinked from the file structure itself so it doesn't show up in a search or when viewing the contents of a hard drive or storage device through a file browser.

Digital Evidences

- **7. Volatile data**
- Volatile data is the kind of data that is not being written to the disk itself, hence belonging to the invisible data type category. Some viruses, for example, don't write themselves to the hard drive to leave minimal traces behind and avoid detection by antivirus software.
- Therefore, in order to detect them, the RAM needs to be checked and its contents analyzed by a qualified digital forensics analyst.

Digital Evidences

- **7. Volatile data**
- For obvious reasons, volatile data needs to be checked before the device is powered off, otherwise, it can be lost forever. To add additional complexity to the challenge, even the very act of launching a digital forensics tool and loading it into the device's RAM can change the RAM's contents, the very same thing we're trying to analyze.
- This is why analyzing volatile data can be especially tricky and often requires forensic ram imaging to preserve its contents in their original state.

Digital Evidences

- **8. Replicant data**
- On some occasions, various types of software or system processes will leave temporary backup files or directories behind to prevent the unfortunate scenario of losing data (for example, if the user forgets to save whatever they were working on and closes the program).
- An example of this would be Photoshop files and even temporary web cache files.

Digital Evidences

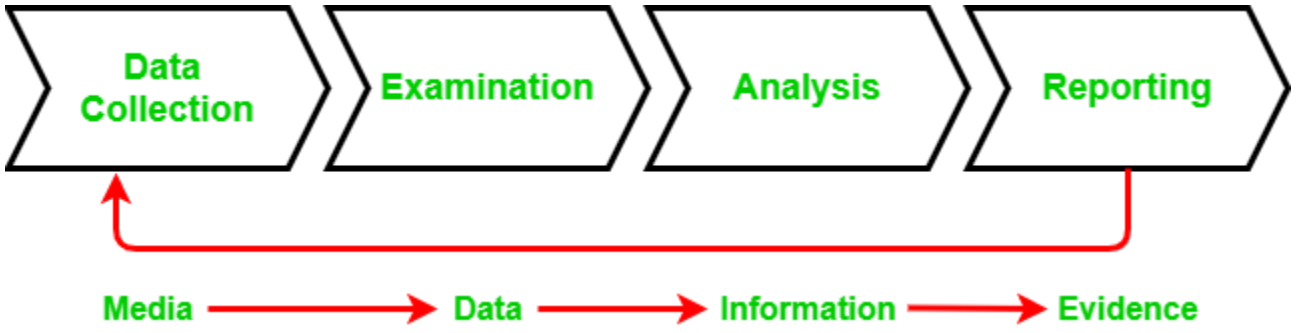
- **8. Replicant data**
- Other examples of replicant data include:
- Web cache and cookies

Chain of Custody – Digital Forensics

- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
- It demonstrates trust to the courts and to the client that the evidence has not tampered.

Chain of Custody – Digital Forensics

- In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.



Chain of Custody – Digital Forensics

- **Collection:**
  - When digital evidence is collected, the process begins with documenting the collection procedure. This documentation includes details such as the date and time of collection, the identity of the collector, the location of the evidence, and the tools or methods used.
- **Packaging and Labeling:**
  - Once collected, the evidence is securely packaged and labeled. The packaging must prevent tampering and contamination. Labels should include information like the case number, item description, and unique identifiers.

Chain of Custody – Digital Forensics

- **Sealing:**
  - The packaging is sealed to further ensure that the evidence remains intact. Seals may include tamper-evident features, and each seal should be documented in the chain of custody records.
- **Documentation:**
  - Detailed records are kept throughout the process. This includes documenting who had custody of the evidence, when and where it was transferred, and any changes in its condition.
- **Storage:**
- Evidence is stored in a secure and controlled environment. Access to the storage area is restricted, and conditions such as temperature and humidity are monitored to prevent damage.

Chain of Custody – Digital Forensics

- **Transfer:**
  - If the evidence needs to be transferred from one person or location to another (e.g., from the field investigator to the forensic analyst), the transfer is carefully documented, and the evidence is securely packaged for transportation.
- **Analysis:**
  - During the analysis phase, forensic examiners work on the evidence while maintaining a detailed record of their activities. Any changes made to the evidence or its original state must be documented.
- **Reporting:**
  - Findings and conclusions derived from the analysis are documented in a report. The report includes details about the methods used, the results obtained, and any potential implications of the findings.

Chain of Custody – Digital Forensics

- **Scenario: A Computer Hard Drive as Digital Evidence**
- **Collection:**
  - Investigator A collects a computer hard drive from a crime scene and documents the collection process, including date, time, location, and methods used.
- **Packaging and Labeling:**
  - The hard drive is placed in an anti-static bag, sealed, and labeled with a unique case number, description, and collector's name.
- **Sealing:**
  - The anti-static bag is sealed with tamper-evident tape, and the seal details are documented.

Chain of Custody – Digital Forensics

- **Documentation:**
  - Investigator A creates a detailed record of the evidence, including its condition at the time of collection and any observations.
- **Storage:**
  - The sealed evidence is stored in a secured evidence locker with controlled access.
- **Transfer:**
  - Investigator A transfers custody to Forensic Analyst B, documenting the transfer details, date, time, and condition of the evidence.
- **Analysis:**
  - Forensic Analyst B analyzes the hard drive, maintaining detailed records of the analysis process and any changes made during the examination.

Chain of Custody – Digital Forensics

- **Reporting:**
  - Forensic Analyst B produces a comprehensive report detailing the findings, methodologies, and any relevant information discovered during the analysis.
- Throughout this process, each person in possession of the evidence adheres to the Chain of Custody procedures, ensuring the integrity and reliability of the digital evidence for use in legal proceedings. The complete documentation of the Chain of Custody is crucial for establishing the evidence's credibility in court.

Anti Forensics

- Anti-forensics, also known as counter-forensics, refers to the techniques and methods employed to deliberately thwart or undermine digital forensic investigations. The goal of anti-forensics is to disrupt or manipulate the collection, analysis, and preservation of digital evidence, making it more challenging for forensic investigators to uncover information about cybercrimes or illicit activities. Individuals or entities engaging in anti-forensic practices often seek to cover their tracks, obscure evidence, or mislead investigators.
- Common anti-forensic techniques include:

Anti Forensics

- **Data Deletion:**
  - Permanently erasing or overwriting data to make it unrecoverable. This can include using secure deletion tools to overwrite free space on storage media.
- **Data Encryption:**
  - Encrypting sensitive data to prevent unauthorized access. If investigators do not have access to the decryption key, the information remains inaccessible.
- **Steganography:**
  - Embedding data within other files or media in a way that is not immediately apparent. This technique aims to hide the existence of information rather than encrypt it.

Anti Forensics

- **File System Manipulation:**
  - Altering file system metadata or timestamps to mislead investigators about the timeline of events or actions taken on a system.
- **Network Anonymization:**
  - Using techniques such as virtual private networks (VPNs), proxy servers, or Tor to obfuscate the source of network traffic, making it difficult to trace back to the original user.
- **Memory Scrubbing:**
  - Clearing or overwriting volatile memory (RAM) to eliminate traces of running processes or sensitive information stored in memory.

Anti Forensics

- **File Deletion and Shredding:**
  - Deleting files and then securely shredding the storage space previously occupied by those files to make recovery more difficult.
- **Attack on Forensic Tools:**
  - Targeting and disabling or evading forensic tools and software that investigators use to analyze systems.
- **Tampering with Timestamps:**
  - Manipulating file timestamps to create false timelines or hide the actual sequence of events.

Anti Forensics

- **Data Fragmentation:**
  - Splitting data into smaller fragments and storing them in different locations to complicate reconstruction and analysis.
- **Booby Trapping:**
  - Placing false or misleading information within systems to misdirect investigators and waste their time.
- It's important to note that engaging in anti-forensic activities is often illegal and can lead to serious legal consequences. Law enforcement and digital forensic professionals continually work to develop countermeasures and techniques to overcome challenges posed by anti-forensics. Despite these efforts, the cat-and-mouse game between forensic investigators and individuals using anti-forensic techniques continues to evolve in the cybersecurity landscape.

Incident Response

- Incident Response (IR) is a systematic approach to managing and mitigating the impact of security incidents on an organization's information technology infrastructure. The goal of incident response is to identify, contain, eradicate, recover, and learn from security incidents in order to minimize damage and reduce the risk of future incidents. It is a critical component of an organization's overall cybersecurity strategy.

Incident Response

- **1. Preparation:**
- **Incident Response Plan (IRP):** Develop a comprehensive incident response plan outlining the organization's strategy for responding to security incidents. This plan should define roles and responsibilities, communication procedures, and specific response procedures for different types of incidents.
- **Training and Awareness:** Ensure that personnel are trained on the incident response plan, including their roles and responsibilities. Regular training and awareness programs help to maintain a high level of readiness.
- **Tools and Resources:** Acquire and maintain the necessary tools, technologies, and resources for incident detection, analysis, and response. This may include intrusion detection systems, security information and event management (SIEM) systems, forensic tools, and communication channels.

Incident Response

- **2. Identification:**
- **Event Detection:** Use monitoring tools, logs, and alerts to identify potential security incidents. This can involve analyzing network traffic, system logs, and other data sources for signs of anomalous or suspicious activities.
- **Incident Triage:** Evaluate and prioritize incidents based on their severity and potential impact on the organization. Determine the appropriate level of response for each incident.

Incident Response

- **3. Containment:**
- **Isolation:** Contain the impact of the incident by isolating affected systems or networks. This may involve disconnecting compromised systems from the network to prevent further spread.
- **Remediation:** Implement immediate actions to stop the progression of the incident. This could include patching vulnerabilities, changing passwords, or disabling compromised accounts.

Incident Response

- **4. Eradication:**
- **Identify and Remove:** Identify the root cause of the incident and take steps to remove the source of the compromise. This may involve further investigation, forensics analysis, and applying additional security measures to eliminate vulnerabilities.
- **System Restoration:** Restore affected systems to a known good state. This may involve reimaging systems, reinstalling software, and applying necessary updates.

Incident Response

- **5. Recovery:**
- **Business Continuity:** Work towards restoring normal business operations. Ensure that critical systems and services are back online and functioning as expected.
- **Data Recovery:** Recover lost or compromised data from backups. Regularly test and update backup procedures to ensure data recovery capabilities.

Incident Response

- **6. Lessons Learned:**
- **Post-Incident Analysis:** Conduct a thorough analysis of the incident, including what went well and what could be improved. This involves reviewing the incident response process, identifying gaps or weaknesses, and updating the incident response plan accordingly.
- **Documentation:** Document all actions taken during the incident response process. This documentation is valuable for post-incident analysis, legal purposes, and for improving future incident response efforts.

Incident Response

- **7. Communication:**
- **Internal Communication:** Keep internal stakeholders informed throughout the incident response process. This includes communication with IT teams, executives, legal, and other relevant departments.
- **External Communication:** If required, communicate with external entities such as law enforcement, regulatory bodies, customers, or the public. Be transparent about the incident, its impact, and the steps being taken to address it.

Roles of CSIRT in handling incident.

- A Computer Security Incident Response Team (CSIRT) plays a crucial role in handling and responding to cybersecurity incidents within an organization. CSIRTs are responsible for coordinating and facilitating the organization's response to incidents, ensuring a structured and effective approach. Here are the key roles that a CSIRT typically performs in handling incidents:

Roles of CSIRT in handling incident.

- **1. Preparation:**
- **Developing Incident Response Plans (IRPs):** CSIRTs contribute to the creation and maintenance of incident response plans. These plans outline the organization's strategy for responding to different types of incidents and provide a structured framework for incident handling.
- **Training and Awareness:** Conduct training sessions and awareness programs for personnel across the organization. This includes training on incident response procedures, reporting mechanisms, and general cybersecurity best practices.
- **Tool and Resource Management:** Ensure that the CSIRT has access to the necessary tools, technologies, and resources to effectively detect, analyze, and respond to incidents. This may involve selecting and maintaining security tools, creating playbooks, and establishing communication channels.

Roles of CSIRT in handling incident.

- **2. Detection and Analysis:**
- **Monitoring and Alerting:** Continuously monitor the organization's networks, systems, and applications for signs of security incidents. CSIRTs use intrusion detection systems, log analysis, and other monitoring tools to identify potential threats.
- **Incident Triage:** Prioritize and categorize incidents based on their severity and impact. This involves analyzing available information to determine the appropriate response level for each incident.

Roles of CSIRT in handling incident.

- **3. Containment and Eradication:**
- **Isolation and Containment:** Take immediate actions to contain the impact of an incident. This may involve isolating affected systems or networks to prevent the spread of the incident.
- **Remediation and Eradication:** Identify the root cause of the incident and implement measures to eradicate the threat. CSIRTs work to remediate vulnerabilities, remove malware, and restore affected systems to a secure state.

Roles of CSIRT in handling incident.

- **4. Recovery:**
- **Business Continuity:** Collaborate with relevant teams to ensure business continuity and the restoration of critical services. CSIRTs contribute to the recovery process, helping to bring systems back online and verifying their integrity.
- **Data Recovery:** Assist in the recovery of lost or compromised data from backups. Validate and ensure the integrity of backup and recovery procedures.

Roles of CSIRT in handling incident.

- **5. Coordination and Communication:**
- **Internal Communication:** Maintain clear communication channels within the organization. CSIRTs collaborate with IT teams, management, legal, public relations, and other relevant stakeholders to provide updates and coordinate response efforts.
- **External Communication:** If necessary, communicate with external entities such as law enforcement, regulatory bodies, vendors, and affected parties. CSIRTs help manage external communication to minimize the impact of the incident on the organization's reputation.

Roles of CSIRT in handling incident.

- **6. Documentation and Reporting:**
- **Incident Logging:** Document all activities and decisions made during the incident response process. This documentation is critical for post-incident analysis, legal purposes, and compliance requirements.
- **Incident Reporting:** Prepare and submit incident reports to relevant internal and external parties. These reports include details about the incident, actions taken, lessons learned, and recommendations for improvement.

Roles of CSIRT in handling incident.

- **7. Continuous Improvement:**
- **Post-Incident Analysis:** Conduct thorough post-incident analyses to identify areas for improvement. CSIRTs play a key role in reviewing incident response effectiveness, identifying lessons learned, and updating incident response plans and procedures accordingly.
- **Training and Exercises:** Based on lessons learned, organize training sessions and exercises to enhance the preparedness of the organization and the CSIRT for future incidents.

Roles of CSIRT in handling incident.

- **8. Threat Intelligence Integration:**
- **Integrating Threat Intelligence:** CSIRTs leverage threat intelligence to enhance their incident detection and response capabilities. They stay informed about emerging threats, vulnerabilities, and attack techniques to proactively defend against potential incidents.
- **9. Legal and Regulatory Compliance:**
- **Ensuring Compliance:** CSIRTs work with legal and compliance teams to ensure that incident response activities align with legal and regulatory requirements. This includes data protection laws, breach notification obligations, and other relevant regulations.