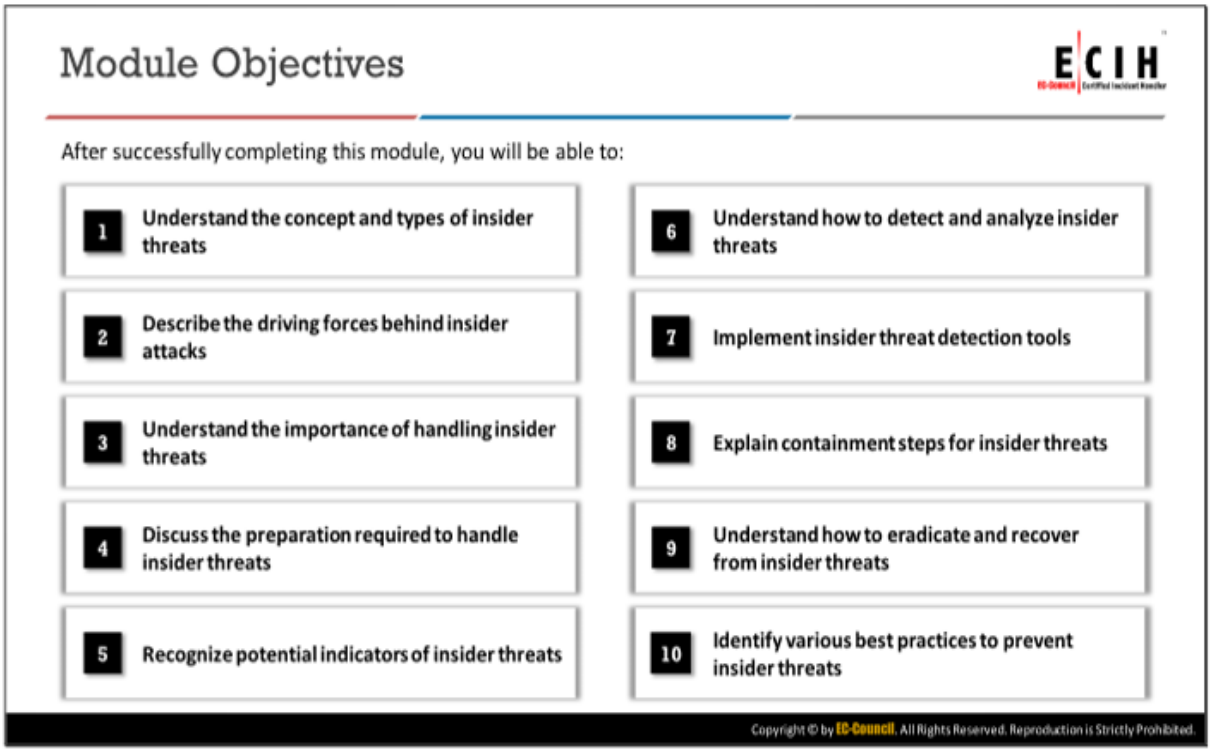
Module 09

Handling and Responding to Insider Threats

This page is intentionally left blank.



Module Objectives

Insider threats are more devastating because trusted people are involved, such as employees, third parties, contractors, or customers who have privileged access to various resources. Insiders can use their authorized privileges to directly misuse resources, affecting the confidentiality, integrity, and availability of information systems. Malicious insider activities may impact business operations and damage both the organization's reputation and profits.

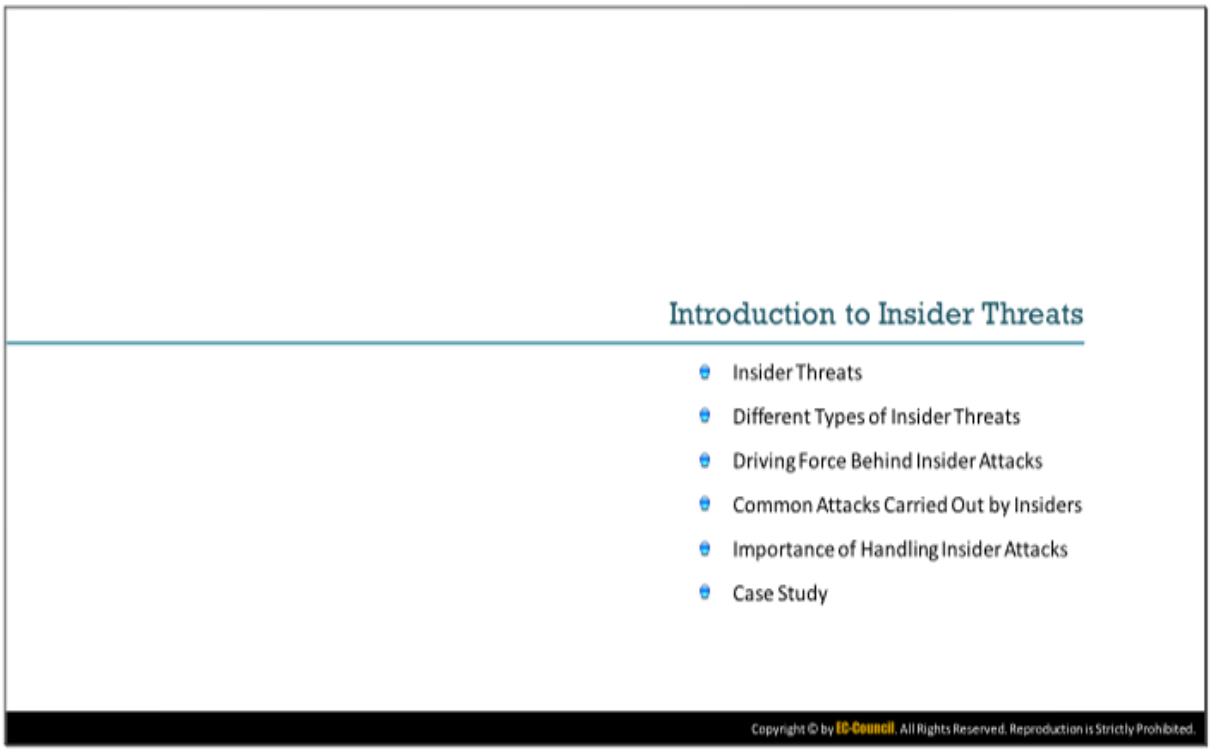
Incident responders should possess a complete understanding of insider threats, along with the detailed knowledge of handling and responding to these threats. After studying this module, incident responders will be able to gain knowledge on various steps involved in handling insider threats such as preparation, detection, analysis, containment, eradication, and recovery.

This module starts with an introduction to handling insider threats. It explains in detail about various types of insider threats, driving forces behind insider threats, and common attacks carried out by insiders. It discusses various preparation steps needed to handle insider threats. It explains in detail on how to detect and analyze insider threats. It also discusses various containment steps for insider threats. It gives an overview on the various steps needed to eradicate insider threats. It explains how to recover from insider threats and briefly discusses best practices for securing the organizational assets from insider threats.

At the end of this module, you will be able to:

- Understand the concept and types of insider threats
- Describe the driving forces behind insider attacks
- Understand the importance of handling insider threats
- Discuss the preparation required to handle insider threats

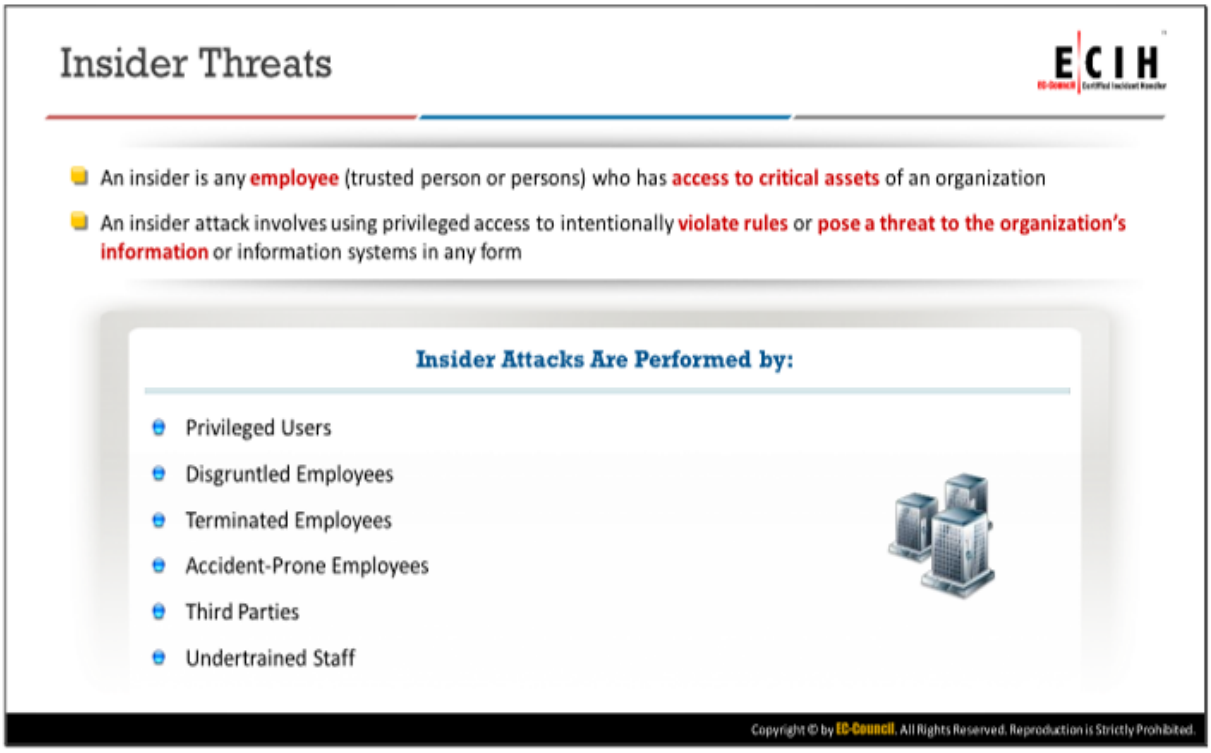
- Recognize potential indicators of insider threats
- Understand how to perform detection and analysis of insider threats
- Implement insider threat detection tools
- Explain containment steps for insider threats
- Understand how to eradicate and recover from insider threats
- Identify best practices to prevent insider threats

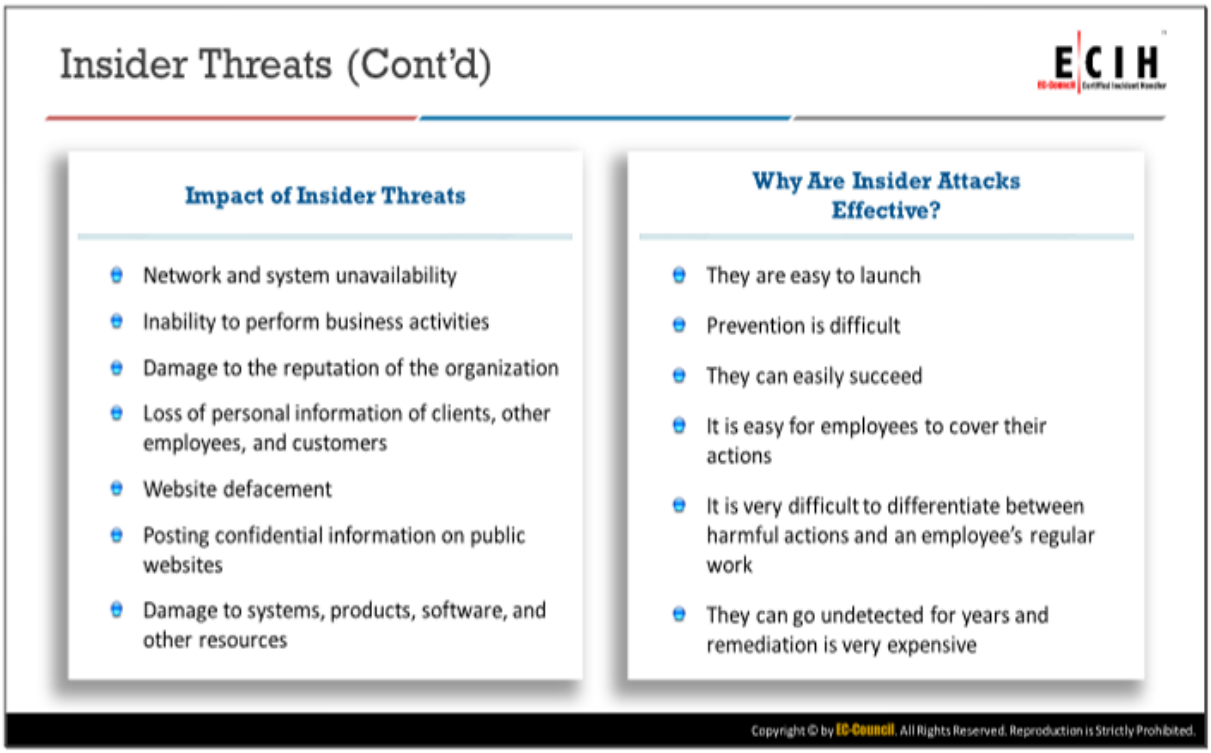


Introduction to Insider Threats

Insider threats are major risks currently faced by organizations. Most organizations carefully evaluate external threats and focus less on internal threats. Even after deploying efficient security controls to monitor and detect external threats, the most dangerous insiders may already have access to the internal systems and critical data. Hence, it is important for incident handlers to understand various threats and risks caused by insiders.

This section gives an overview on insider threats, types of insider threats, driving forces behind insider attacks, common attacks carried out by insiders, the importance of handling insider attacks, and case studies.





Insider Threats

An insider is any employee (trusted person) who has access to an organization's critical. An insider attack involves using privileged access to violate rules or intentionally threaten the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. They misuse the organization's assets to directly affect the confidentiality, integrity, and availability of information systems. Insiders can perform malicious activity on the organization's network, system, and database.

These attacks impact organization's business operations, reputation, and profit. It is difficult to figure out the source of an insider attack. Insider attacks may also cause great losses for the company. It is easier to launch an insider attack, and preventing such attacks is difficult.

Insider attacks are generally performed by:

- **Privileged Users**

  Attacks may come from an organization's most trusted employees, such as managers and system administrators, who have access to the company's confidential data. There is a higher probability that these individuals will misuse the data, either intentionally or unintentionally.

- **Disgruntled Employees**

  Attacks may come from unhappy employees or contract workers. Disgruntled employees, who intend to take revenge on their company, first acquire information and then wait for the right time to compromise the organization's resources.

- **Terminated Employees**

  Some employees take valuable information about the company with them when terminated. These employees can access company data even after termination using backdoors, malware, or their old credentials if they are not disabled.

- **Accident-Prone Employees**

  Unintentional data disclosure can occur when an employee loses a device, sends an email to incorrect recipients, or leaves their system logged in to systems that access confidential data.

- **Third Parties**

  Third parties like remote employees, partners, dealers, and vendors have access to company's information. Security of the systems they use can be difficult to monitor while the people accessing company information can be unpredictable.

- **Undertrained Staff**

  Trusted employees can become unintentional insiders due to a lack of cybersecurity training. They fail to adhere to cybersecurity policies, procedures, guidelines, and best practices.

Organizations where insider attacks are common include credit card companies, health care companies, network service providers, and financial and exchange service providers. With their authorized privileges, insiders can bypass physical and technical security measures and gather sensitive information from organizational systems and devices.

Insider attacks can impact the organization in several ways:

- Remove access to networks and systems
- Create an inability to perform business activities

- Damage the reputation of the organization
- Cause loss of client, employee, or customer personal information
- Website defacement
- Post confidential information on public websites
- Damage systems, products, software, and other resources

Why Are Insider Attacks Effective?

An insider attack is effective because:

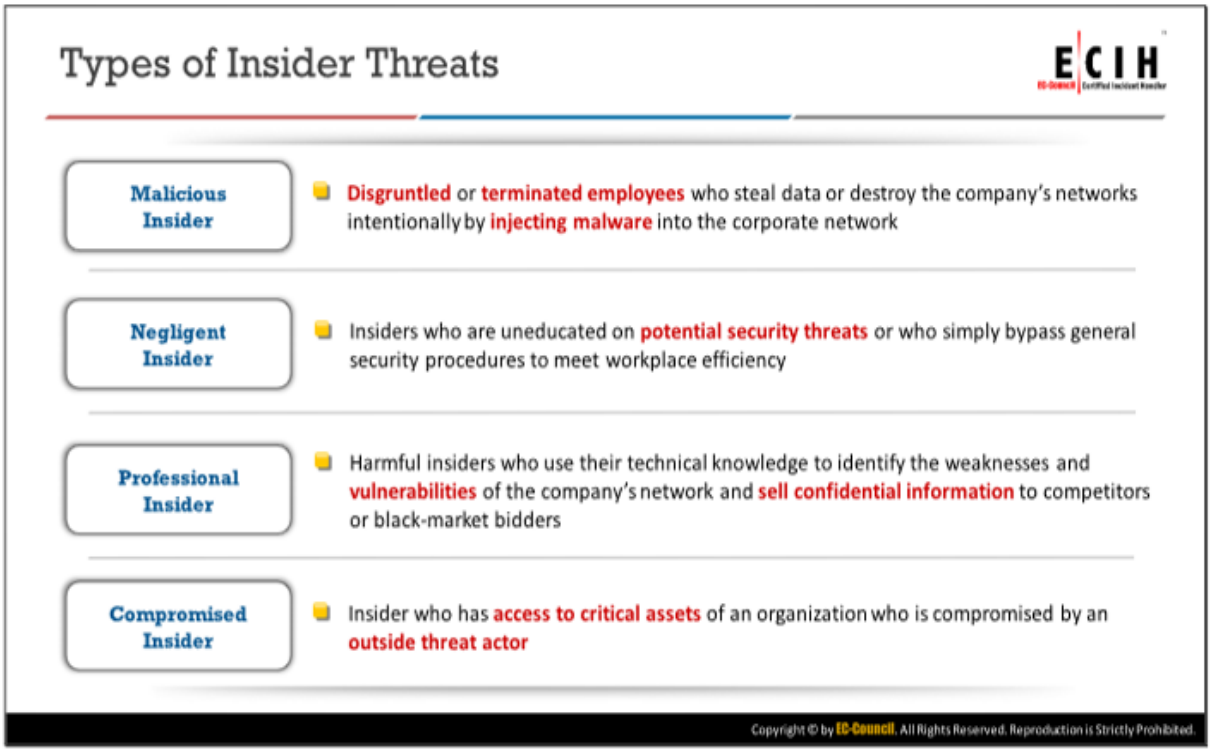
- Insider attacks can go undetected for years and remediation is expensive
- An insider attack is easy to launch
- Preventing insider attacks is difficult
- Inside attacker can easily achieve their goals
- It can be difficult to differentiate harmful, malicious activities from an employee's regular work actions from employee's regular work as it is hard to identify whether employees are performing malicious activities or not
- Even after detecting employees' malicious activities, they may deny responsibility and claim their activity was an unintentional mistake
- Employees can easily cover their actions by editing or deleting logs to hide their malicious activities

Example of Insider Attack: Disgruntled Employee

Most cases of insider abuse can be traced to individuals who are introverted, incapable of managing stress, experiencing conflict with management, frustrated with their job or office politics, lack respect, have not been promoted, or have been transferred, demoted, or terminated, among other reasons. Disgruntled employees may also pass company secrets and intellectual property to competitors for monetary gain, thus harming the organization.

Disgruntled employees can use steganography programs to hide company secrets and later send the information as innocuous-looking messages, such as images or sound files to competitors. Since the messages are hidden, this malicious behavior may go unnoticed.

Figure 9.1: Example of insider attack—disgruntled employee



Types of Insider Threats

There are four types of insider threats. They are:

- **Malicious Insider**

  Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injecting malware into the corporate network.

- **Negligent Insider**

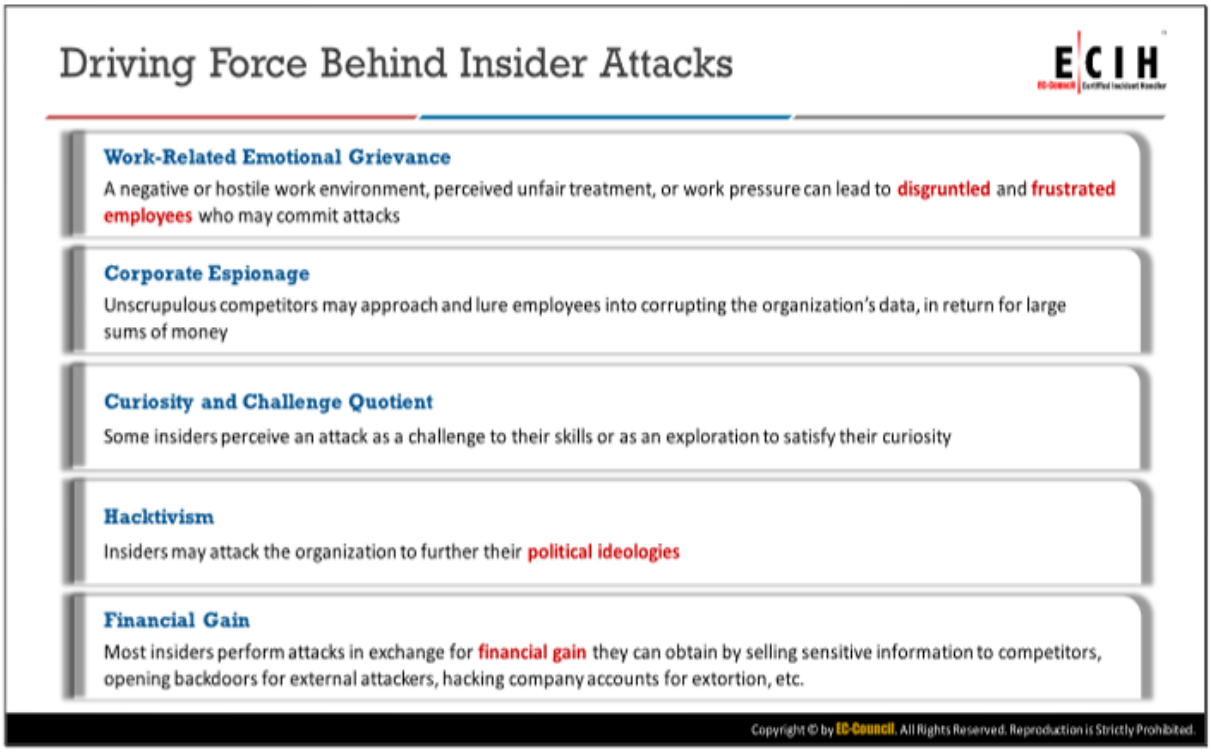
  Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency, are more vulnerable to social engineering attacks. Many insider attacks result from employees' lax behavior regarding security measures, policies, and practices.

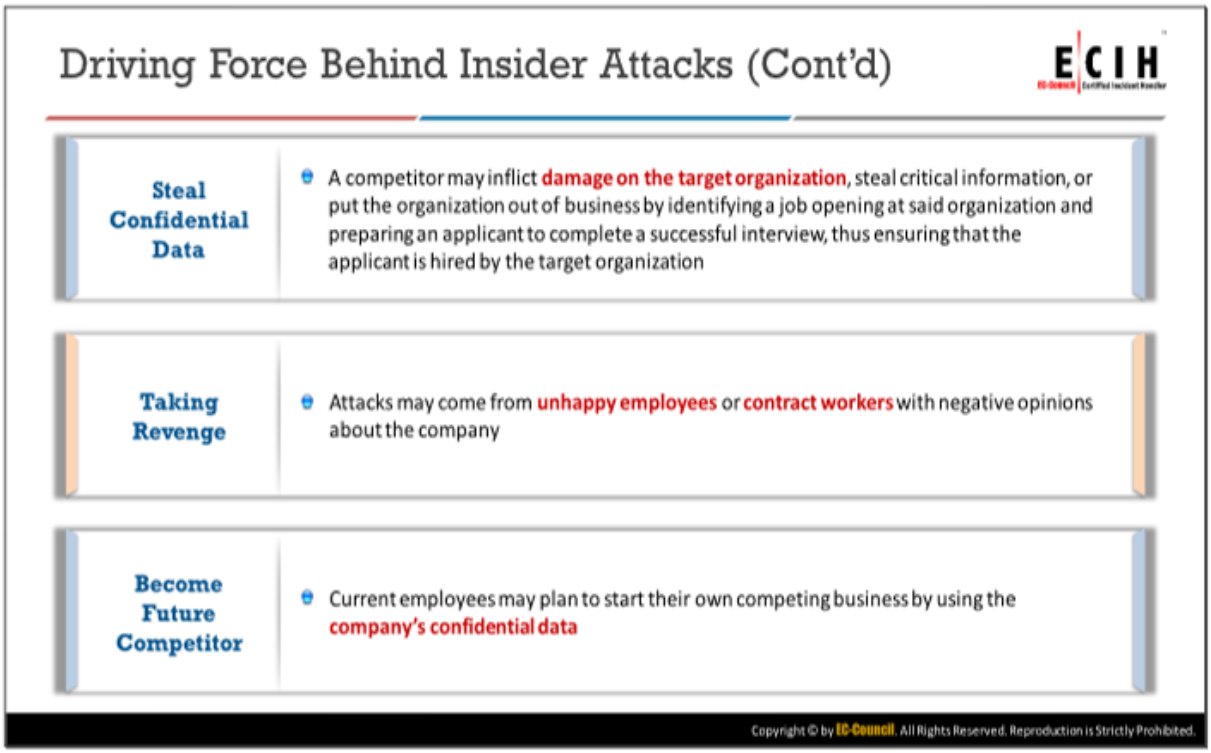
- **Professional Insider**

  Professional insiders are the most harmful threats; they use their technical knowledge to identify weaknesses and vulnerabilities of the company's network in order to sell confidential information to competing companies or black-market bidders.

- **Compromised Insider**

  Outsiders compromise insiders who have access to an organization's critical assets or computing devices. This type of threat is more difficult to detect since the outsider masquerades as a genuine insider.





Driving Force Behind Insider Attacks

Most insider attacks take place to fulfill financial needs, while others result from the insider's hostility, revenge, and greed.

The following can be the driving force for an insider to commit an attack:

- **Work-Related Grievance**

  If an organization has a negative or hostile work environment, an employee may become disgruntled due to perceived unfair treatment or work pressure and attack the organization's systems. Frustrations about work can also lead users to commit insider attacks.

- **Corporate Espionage**

  Unscrupulous competitors may approach and lure employees into corrupting the organization's data for payment. Employees may be asked to steal sensitive information, such as project or board meeting details, tender quotes, and future plans.

- **Challenge**

  Some insiders see an attack as a challenge for their skills and perform the attack for the thrill of overcoming this challenge. This can include employees from security or hacking teams who want to try their skills against new types of security methods implemented across the organization.

- **Curiosity**

  Generally, students of security programs perform insider attacks to fulfill their curiosity. They can perform these attacks to ascertain their hacking capabilities or to check the extent of their hacking products.

- **Hacktivism**

  This is a mechanism in which employees attack the organization to make political statements or embarrass a company by publicizing sensitive information. These types of attackers can also be persons who want to publicize the crimes of organizations or governments against the people.

- **Financial Gains**

  Most insiders perform attacks for financial gain because they expect to sell sensitive information to competitors, opening backdoors for external attackers, hacking company accounts for extortion, and so on. The insider sells sensitive information of the company to competitors, steals colleagues' financial details for personal use, or manipulates companies or personnel financial records.

- **Steal Confidential Data**

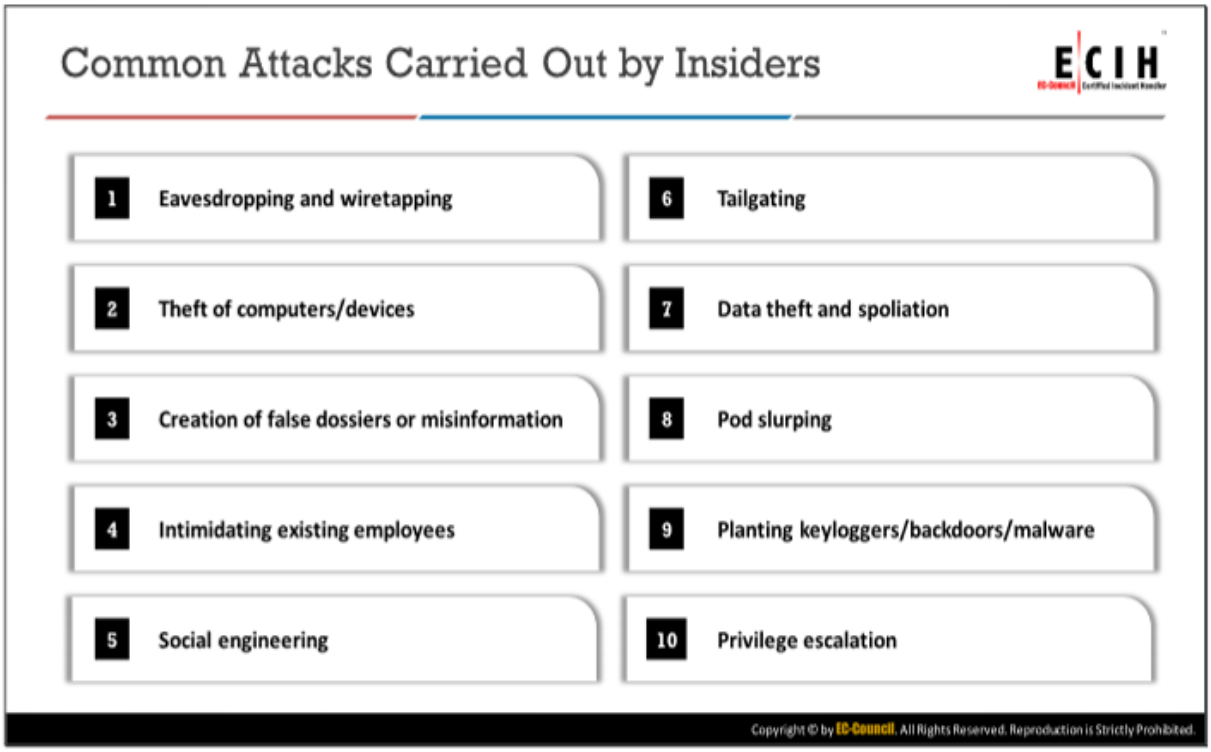
  A competitor may inflict damage to the target organization, steal critical information, or put them out of business, by just finding a job opening, preparing someone to get through the interview, and having that person hired by the target organization.

- **Taking Revenge**

  It takes only one disgruntled person to take revenge and compromise a company. Attacks may come from unhappy employees or contract workers with negative opinions about the company.

- **Become Future Competitor**

  Current employees may plan to start their own competing business by using the company's confidential data. These employees may access and alter company's clients list.



Common Attacks Carried Out by Insiders

The following are the most common types of attacks carried out by insiders:

- **Eavesdropping and Wiretapping**

  Eavesdropping is overhearing a conversation surreptitiously. Insiders or corporate spies may use this method to collect confidential conversations from boardrooms, meeting halls, and corridors. To achieve this, the insiders can implant bugs, scanners, and tapping devices to overhear or hack phone conversations. They may also make use of web-based sniffing services to hack phone-based voice mail systems.

- **Theft of Computers/Devices**

  Insiders try to access sensitive data by stealing laptops, mobiles, and other portable electronic devices. To accomplish this, they may take advantage of negligent staff who misplace their portable devices. They may also steal parts of devices such as hard disks containing crucial information and using them to perform malicious activities.

- **Creation of False Dossiers or Misinformation**

  Insiders create and spread misleading information to spur dissonance within the employees of the organization. Insiders then try to exploit the resulting situation to gain the trust of employees, gather crucial data from them, and use it for performing attacks. Competitors also hire law firms or private investigators to compile false or misleading dossiers to discredit target organizations.

- **Intimidating Existing Employees**

  Insiders gather personal information about existing employees such as their spouses, children, personal life, religious activities, health, and medical information. They use this

information to blackmail, lure, physically abuse, and intimidate them to accomplish their malicious tasks.

- **Social Engineering**

  Social engineering is an art of manipulating people to divulge sensitive information to performing malicious actions. Most often, employees are not even aware of a security lapse on their part and inadvertently reveal an organization's critical information. Insiders mainly target help desk workers, receptionists, and security guards by employing new ways to get information and by misusing the individual's knowledge and access privileges.

- **Tailgating**

  Insiders gain access to confidential and restricted areas of the organization by resorting to tailgating. They might pretend to have forgotten their ID cards or enter an area after the authorized personnel without being noticed. This poses a threat to sensitive zones of organization such as data centers, meeting rooms, printer and fax zones, and administrative areas.

- **Data Theft and Spoliation**

  Corporate spies or insiders extract sensitive data by using hidden files, wireless networks, and hacking techniques, and using portable electronic and storage devices such as laptops, smartphones, tablets, and USB drives. They misuse the security features that most organizations use to filter and monitor incoming traffic if the organizations have failed to enable restrictions on outgoing traffic. This security vulnerability enables spies to store and extract sensitive data in bulk.

- **Pod Slurping**

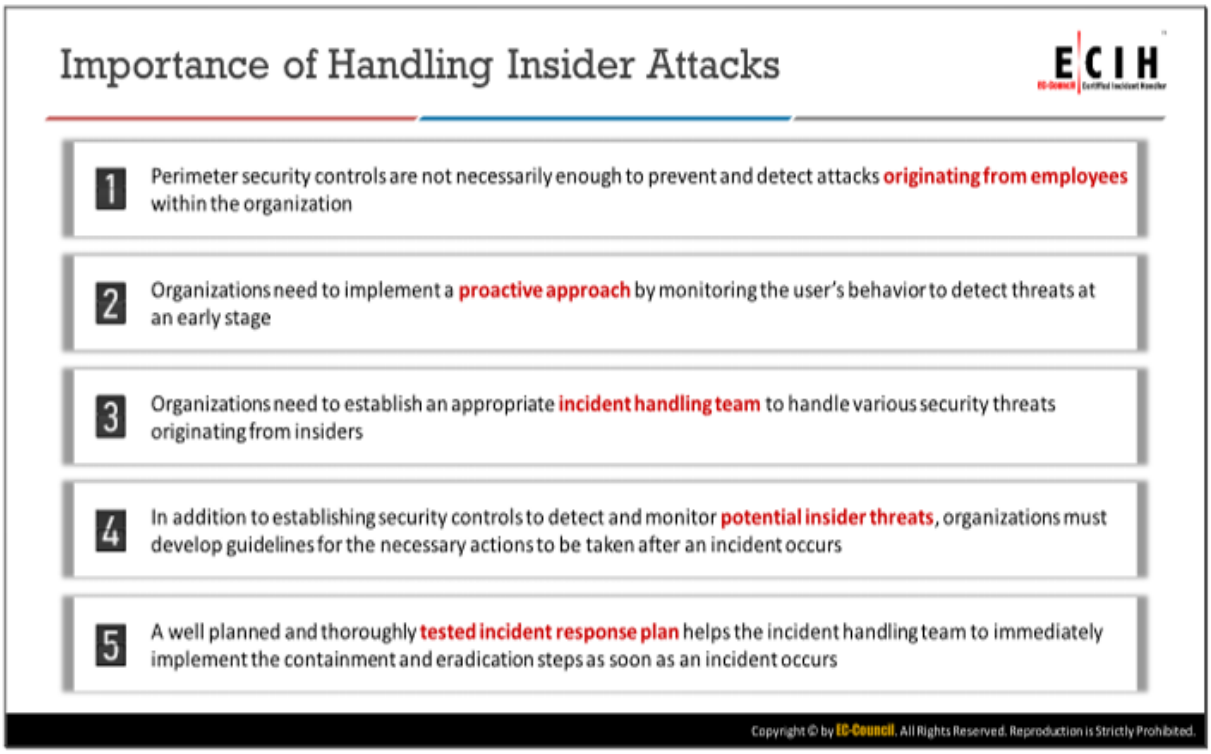
  In pod slurping, the attackers use portable storage devices such as iPods and USB sticks to steal sensitive data. Insiders use storage devices to introduce software tools that automatically runs when the device is connected. These tools can search networks for sensitive information and transfer it to the device.

- **Planting Keyloggers/Backdoors/Malware**

  Keylogging is a technique used to record or monitor the keystrokes of specific computer users. Backdoors compromise the security of target systems and gain illegitimate access to a network by injecting small programs that bypass authentication checks, such as gaining administrative privileges without passwords. Malware is a piece of malicious software that is designed to perform activities as intended by the attacker without user consent. Insiders can steal data by planting keyloggers, backdoors, or malware.

- **Privilege Escalation**

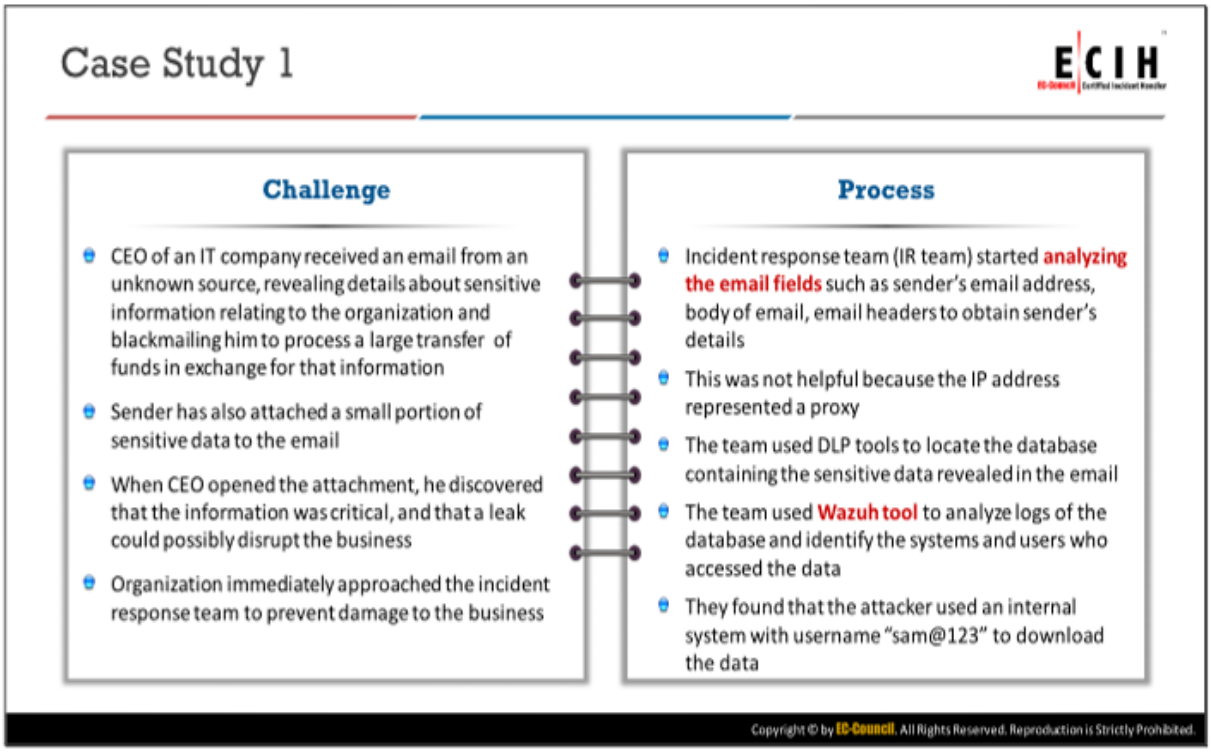
  In a privilege-escalation attack, insiders gain access to the network, data, and applications by taking advantage of bugs, design flaws, or misconfigurations in an operating system or an application to gain elevated access to resources which are normally protected from the application or user. Once insiders have gained access to a remote system with a valid username and password, they will attempt to increase their privileges.

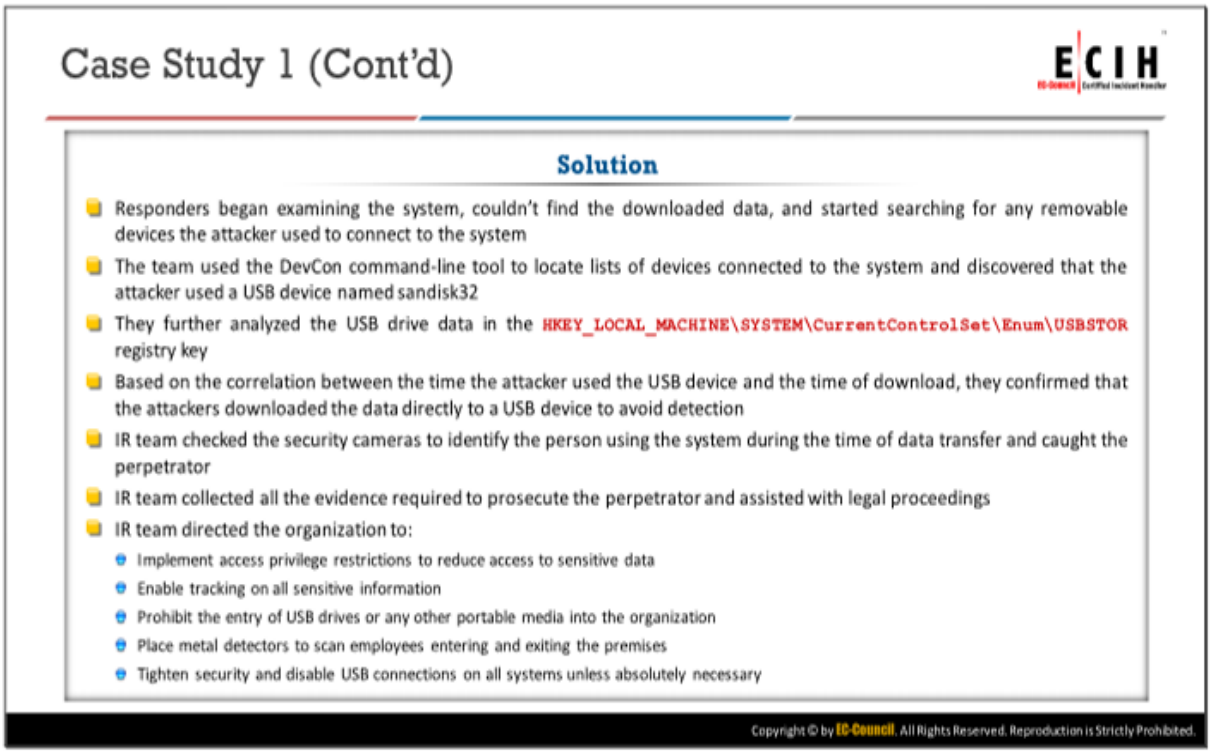


Importance of Handling Insider Attacks

Organizations are investing more on enhancing and strengthening perimeter security controls to prevent and detect various external attacks. These controls are not necessarily enough to prevent and detect internal attacks originating from employees within the organization. It is also difficult to monitor and detect insider attacks using traditional security tools. Organizations need to implement a proactive approach by monitoring the user's behavior to detect the threats at an early stage. To overcome the challenges in detecting insider threats, organizations need to go beyond technical metrics and security infrastructure and implement advanced analysis techniques such as threat intelligence and big data analytics.

Organizations need to establish appropriate incident handling teams to manage security incidents originating from insiders. Apart from establishing security controls to detect and monitor potential insider threats, organizations must also develop guidelines for the necessary actions to be taken after incidents occur. A well planned and thoroughly tested incident response plan helps the incident handling team immediately implement containment and eradication steps when necessary.





Case Study 1

- **Challenge**

  The CEO of an IT company received an email from an unknown person which revealed certain details about the organization's sensitive information and threatened to send the data to a competitor unless the sender is paid a significant amount of money. Sender has also attached small portion of sensitive data in the mail. After opening the

attachment, CEO found that the information is critical, and its leak can possibly disrupt the business. The CEO immediately approached the incident response team to prevent the damage.

- **Process**

  Incident response team began by analyzing the email fields such as sender's email address, body of email, and email headers to obtain sender's details. This was not helpful because the IP address represented a proxy. They used DLP tools to find the database containing the sensitive data revealed in the mail, then used the Wazuh tool to analyze database logs and identify the systems and users that had accessed the data. They found that the attacker had used an internal system with username "sam@123" to download the data.

- **Solution**

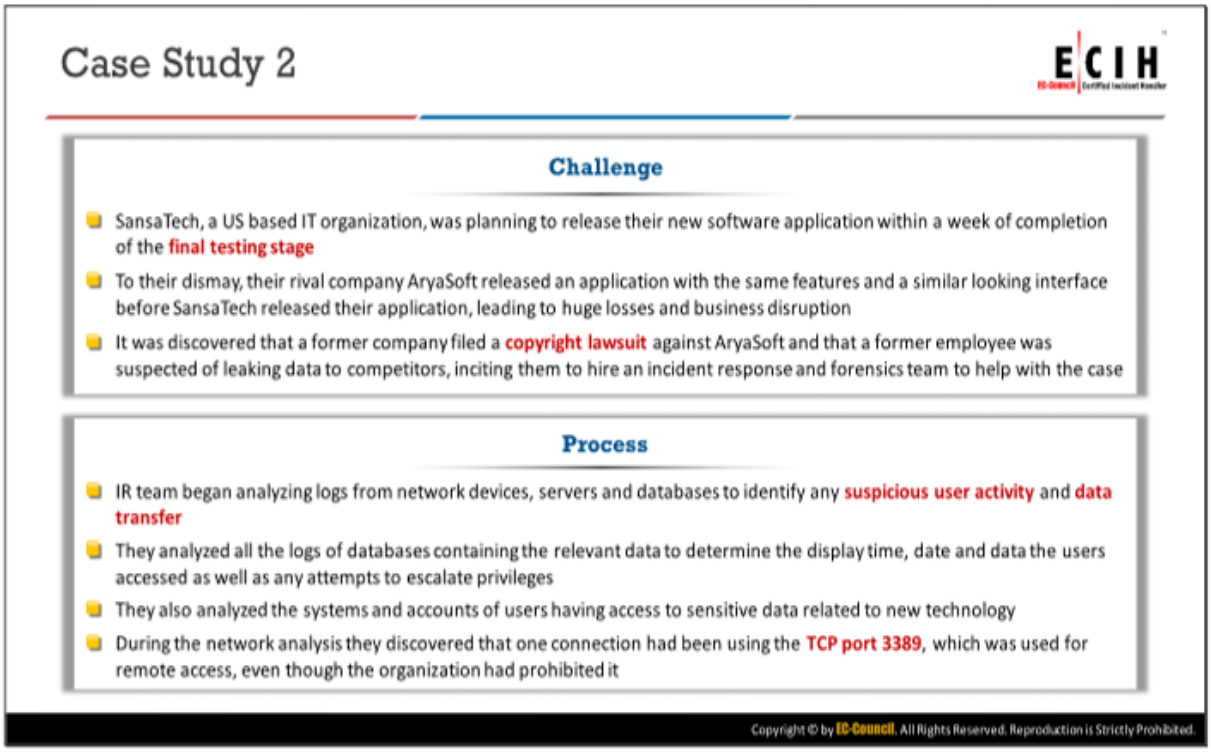
  Responders started examining the system. They could not find the downloaded data so began searching for any removable devices that had been connected by the attacker. They used the DevCon command-line tool to find list of devices connected to the system and found that the attacker had used an USB device named sandisk32. They further analyzed the USB drive data in the

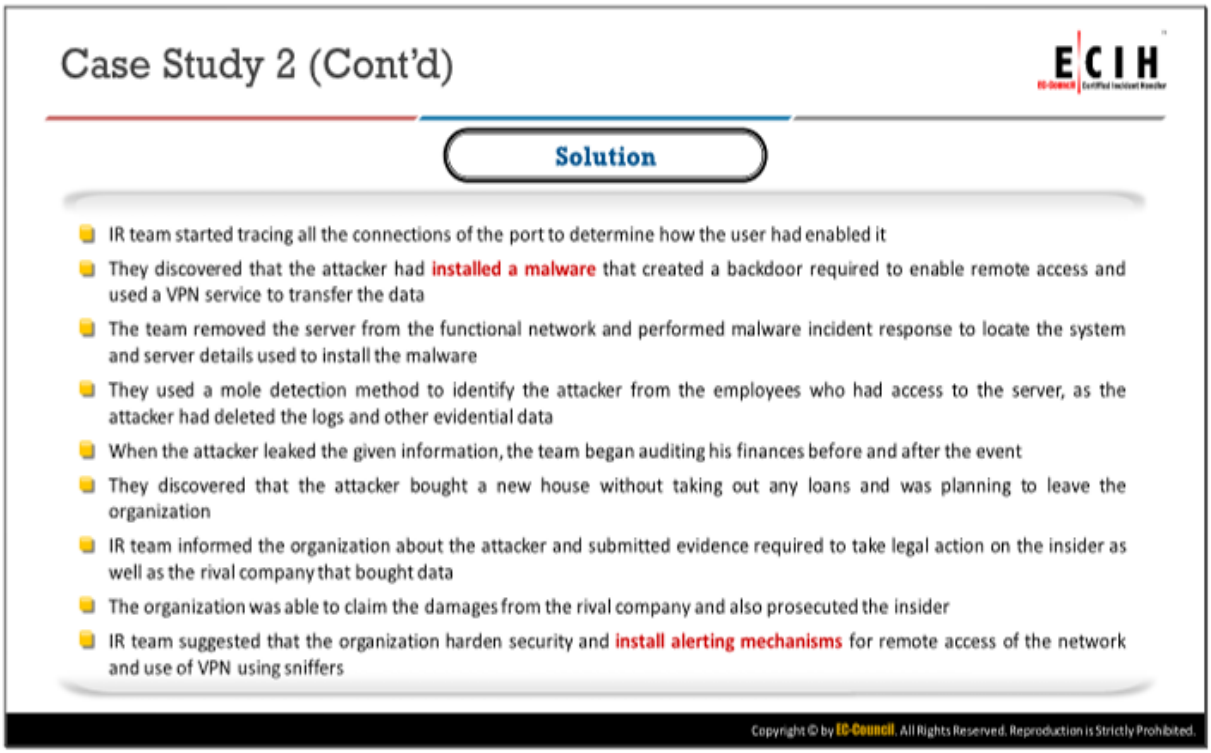
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR` registry key.

  By correlating the time the attacker had used the USB device and the time of download, they confirmed that the attacker had downloaded the data directly to USB to avoid detection. The IR team checked the security cameras to identify the individual using the system during the time of data transfer and caught the perpetrator.

  The IR team collected all the evidence required to prosecute the perpetrator and helped in legal proceedings as well. IR team suggested that the organization:

  - Implement access privilege restrictions to reduce the access of sensitive data
  - Enable tracking on all sensitive information
  - Prohibit the entry of USB drives or any other portable media into the organization
  - Place metal detectors to scan the employees entering and exiting the premises
  - Tighten security and disable USB connections on all systems unless access is business-necessary





Case Study 2

- **Challenge**

  SansaTech, a US-based IT organization, was planning to release their new software application within a week after they had completed their final testing stage. To their shock, their rival company AryaSoft released an application with the same features and a similar user interface, leading to huge losses and business disruption. SansaTech filed a

copyright suit against AryaSoft, suspecting that an employee had a hand in leaking data to AryaSoft. SansaTech hired an incident response and forensics team to help in the case.

- **Process**

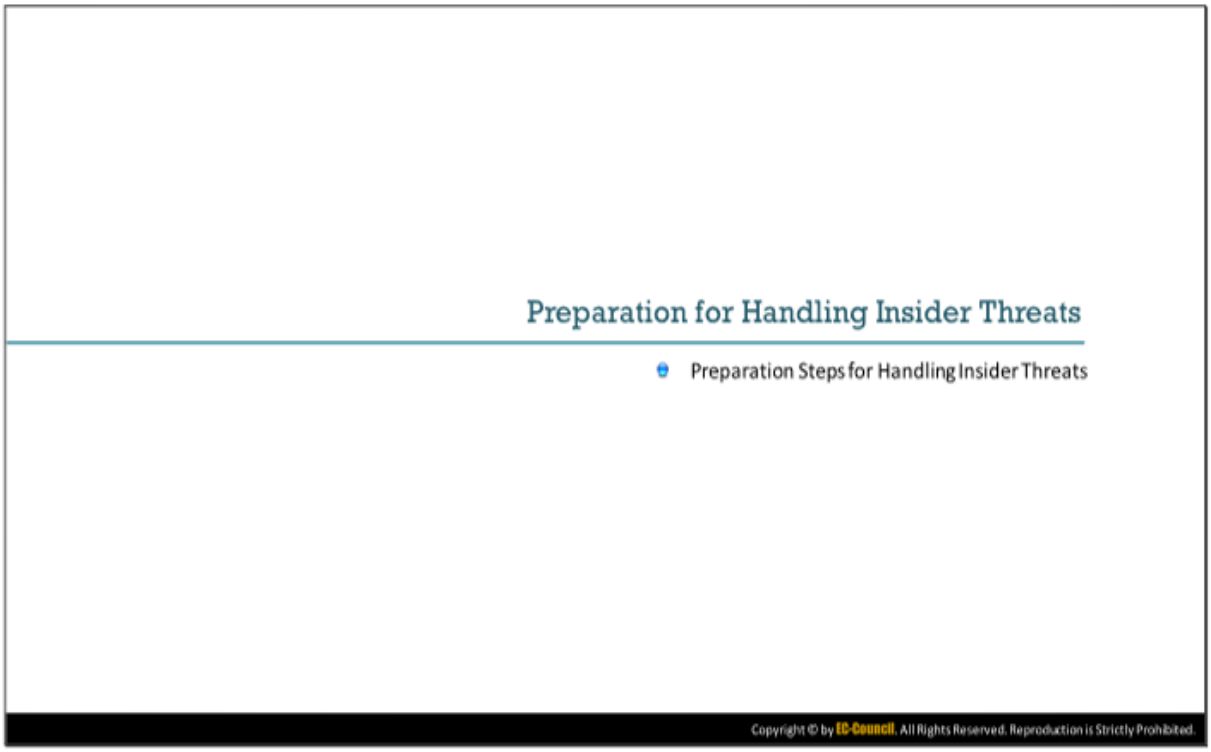
  The IR team started analyzing logs from network devices, servers, and databases to find any suspicious user activity or data transfer. They analyzed all logs of databases which contained the relevant data to determine the display time, date, and data accessed by the users as well as any attempts to escalate privileges. They also analyzed the systems and accounts of users who had access to sensitive data related to new technology. During the network analysis, they found that one connection had been using the TCP port 3389. This port had previously been used for remote access, but the organization had eventually prohibited its use.

- **Solution**

  The team started tracing all connections to the port to determine how the user had enabled it. They found that the attacker had installed malware that created a backdoor allowing remote access and used a VPN service to transfer the data. The team removed the server from the functional network and performed a malware incident response to find the system and server details used to install the malware.

  They used a mole detection method to determine the identity of the attacker based on the employees who had access to the server since the attacker had deleted logs and other data that could have been used as evidence. When the attacker leaked the given information, the IR team started auditing employee finances from before and after the event. They found that the attacker had bought a new house without taking any loans and was planning an exit from the organization. The IR team informed the organization about the attacker and submitted the evidence required to take legal action against both the attacker and the rival company.

  The organization was able to claim damages from the rival company and also prosecute the insider. The IR team suggested that the organization harden security and install alert mechanisms for remote network access and VPN use via sniffers.



Preparation for Handling Insider Threats

Establishing effective defense strategies is not sufficient to handle insider threats. Incident handling teams must be prepared to manage insider threats and define various processes needed to mitigate these incidents. Incident handling teams also need to combine the current security infrastructure with the security policies of the organization to effectively detect and quickly respond to the security incidents.

This section discusses various preparation steps needed to handle insider threats.

Preparation Steps to Handle Insider Threats

Insider threats continue to be a matter of concern for any organization because insiders have a significant advantage over others who might want to harm an organization. Insiders can use their current access to bypass technical and physical security measures. Insiders are also aware of policies, procedures, technologies, vulnerabilities, and exploitable flaws in the organization.

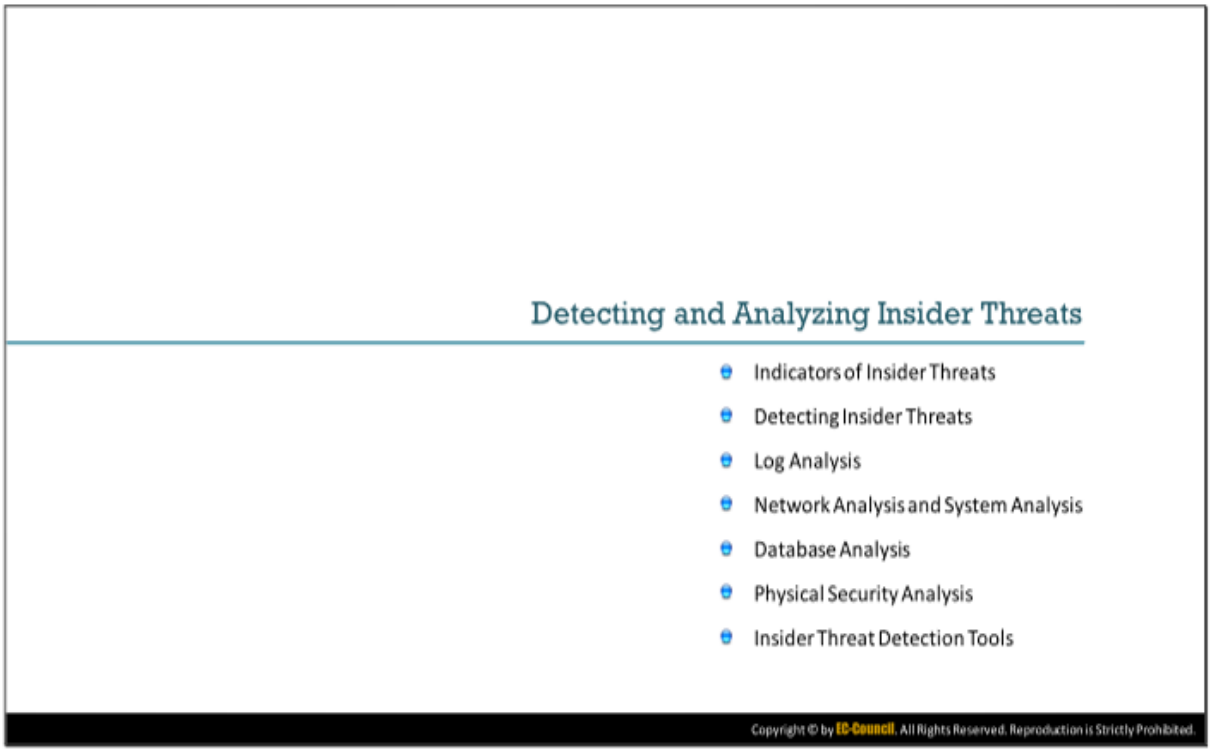
The organization must always be ready to handle or respond to insider threats. Preparing for an incident is essential in case the preventive measures fail to detect and stop an incident. Preparation for an insider incident is effective, but only when the organization can identify the threat as well as mitigate and resolve it quickly.

The following are various preparation steps to handle insider threats:

- Document, frame, and enforce policies to mitigate insider threats like data theft, modification, and IT sabotage.
- Preserve details of previous insider incidents and investigate them carefully when preparing an incident response plan.
- Create awareness and train employees how to safeguarding organizational data.
- Train employees to detect and avert social engineering attempts.
- Conduct regular security awareness trainings to sensitize employees of threats and the organization's security controls.
- Implement policies that prohibit employees from disclosing or forwarding any confidential information.

- Make employees aware of the need for security policies and access controls, their responsibilities and constraints of employment, and the consequences of violations.
- Train employees how to identify and report any policy violation or suspicious espionage events.
- Ensure that employees do not divulge any organizational secrets such as account credentials, service provider details, and information security procedures by creating awareness about the different communication channels that are prohibited for work purposes.
- Help them understand the security risks involved in exchanging information over phone, voice mails, messages, or unencrypted email.
- Identify and prioritize the critical assets of an organization and define a risk management strategy to protect these assets.
- Regularly audit and maintain records of all critical assets, such as servers, computer systems, and their accessories.
- Enable logging for all access attempts and regularly audit them to identify violations or attempts made to violate a security policy.
- Make sure that all the employees follow strict password and account management policies and implement a reporting mechanism that for unauthorized account access and potential attempts at social engineering.
- Follow the principle of least privilege when granting access to organizational resources.
- Enforce policies for separation of duties and providing minimum privileges required by employees to perform their duties.
- Monitor employee activities like phone calls and email.
- Use employee monitoring software to track computer activities using screen capturing, data, keystroke, idle time, printer, removable drives, and audio/video monitoring.
- Monitor the employee internet activities like browsing history, uploads, downloads, web access, data traffic, and other activities, such as accessed files and privilege misuse.
- Record physical entry and exit, system logins, network activities, accessed files, uploads and downloads, privilege misuse, and so on for all employees.
- Log and audit access violations and attempts to violate physical space and other equipment.
- Use physical monitoring devices such as CCTV cameras across the organization to record suspicious activities.
- Make sure that terminated employees will not have access to the physical space or non-public areas of the organization.
- Deploy data loss prevention, log management, IDS, SIEM, and behavior analysis tools.

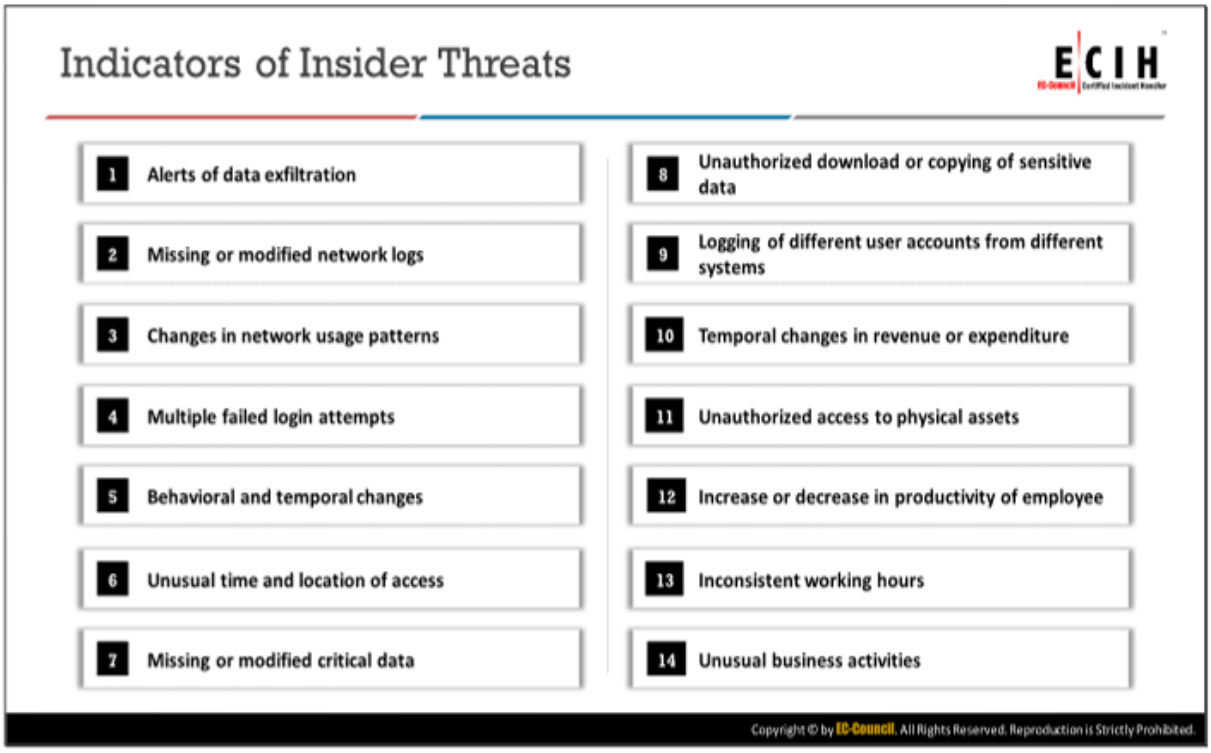
- Install honeypots to lure attackers to the seemingly soft target and identify potential attackers.
- Use honeytokens, which work the same way as honeypots, but at the directory or file level.
- Perform a thorough background check of new employees before hiring.
- Frame the organization's security policy to include that access cards or ID cards must be worn or displayed for all employees and visitors at all times.
- Define an acceptable level of loss and plan security policies accordingly.
- Implement application whitelisting and blacklisting to prevent employees from downloading and executing malicious software.



Detecting and Analyzing Insider Threats

Most data attacks come from the insiders, making it much more difficult to prevent or detect them. Insiders are often aware of the organization's security loopholes and can exploit them to steal confidential information. It is essential to carefully handle insider threats as they are difficult to thwart and can cause huge financial losses and business interruptions.

This section discusses indicators of insider threats, methods used to detect and analyze them, and how to perform log, network, system, database, and physical security analysis along with insider threat detection tools.



Indicators of Insider Threats

Indicators of insider threats are generally abnormal user activities that deviate from regular work activities. These represent unusual patterns of user behavior that require further analysis to identify the malicious motives and intents. The most common indicator of insider threat occurs when employees lack awareness about specific security measures. Incident handlers need to understand these indicators in order to detect and analyze various insider threats.

Following are some indicators of insider threats:

- **Alerts of Data Exfiltration**

  Alerts of unauthorized gathering and transmission of data on the network can represent an insider or malware attack. Insiders can also use paper, facsimile, hard drives, portable devices, and other computing equipment to gather and transfer sensitive data.

- **Missing or Modified Network Logs**

  Insiders may try to access log files to delete, modify, and edit unauthorized access events, file transfer logs, and so on from systems and network devices to avoid detection. Alerts of log modification deletion or access can represent attacks.

- **Changes in Network Usage Patterns**

  Changes in network patterns of the network specific protocols, size of the packets, sources and destinations, frequency of user application sessions, and usage bandwidth can indicate malicious activity.

- **Multiple Failed Login Attempts**

  The insider can try to log in to unauthorized systems or applications by brute force. Multiple failed login attempts may therefore indicate an insider threat.

- **Behavioral and Temporal Changes**

  Deviation from established behavior and temporal changes in employee behavior, such as spending capacity, frequent travel, anger management issues, constant conflicts with colleagues, and lethargic work performance can be fraud indicators.

- **Unusual Time and Location of Access**

  Any mismatch in the timeline of an event can be suspicious and can indicate an insider threat. For example, logging activities on an employee system when the employee is not present.

- **Missing or Modified Critical Data**

  Disgruntled employees can modify or delete sensitive data with an intention to damage the organization's reputation.

- **Unauthorized Download or Copying of Sensitive Data**

  Insiders use legitimate and malicious tools to extract data from the organization's perimeter. Insiders can install malware, Trojans, and backdoors to steal information.

- **Sending Sensitive Information to Personal Email Account**

  Insiders may send organization critical information to their personal email accounts with malicious intentions.

- **Logging of Different User Accounts from Different Systems**

  Unusual times of access combined with differences in the IP address used by the system to log in can represent malicious activities.

- **Temporal Changes in Revenue or Expenditure**

  Unexpected and unexplained changes in an employee's financial status can indicate an external source of income; the organization should audit their financial reports to see if the employee has been involved in malicious activity.

- **Unauthorized Access to Physical Assets**

  Activities such as employees using authorized assets without authentication, trying to escalate their privileges beyond their job requirement, or trying to gain physical access to assets can represent threats.

- **Increase or Decrease in Employee Productivity**

  Employees who are unproductive, threatening, have legitimate and illegitimate job concerns, and have disagreements regarding intellectual property rights tend to be suspicious. Sudden increases or decreases in their productivity can signify suspicious behavior.

- **Inconsistent Working Hours/Unusual Business Activities/Concealed or Frequent Foreign Trips**

  Employees with suspicious business activities like unusual login times, unusual office timings, unauthorized browsing and downloads, concealed foreign trips, and meetings with representatives from other countries/organizations are to be monitored.

- **Abnormal Access of Systems and User Accounts**

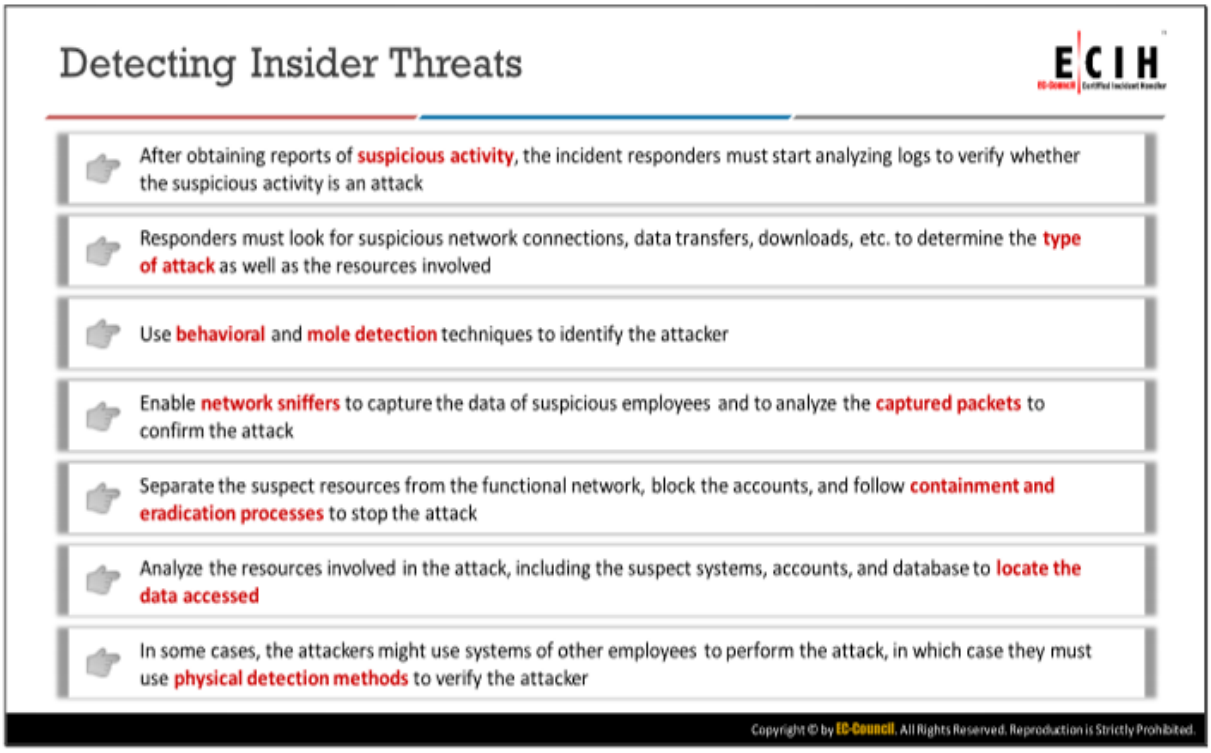
  Mismatch between the systems assigned and the user accounts accessing the systems may indicate an insider threat.

- **Irresponsible Social Media Behavior**

  Insiders may try to create a negative impact on the organization by posting unnecessary or inappropriate information on the social media websites.

- **Attempt to Access Restricted Zones**

  Employees with malicious intention may try to access restricted areas of the organization to collect sensitive information.

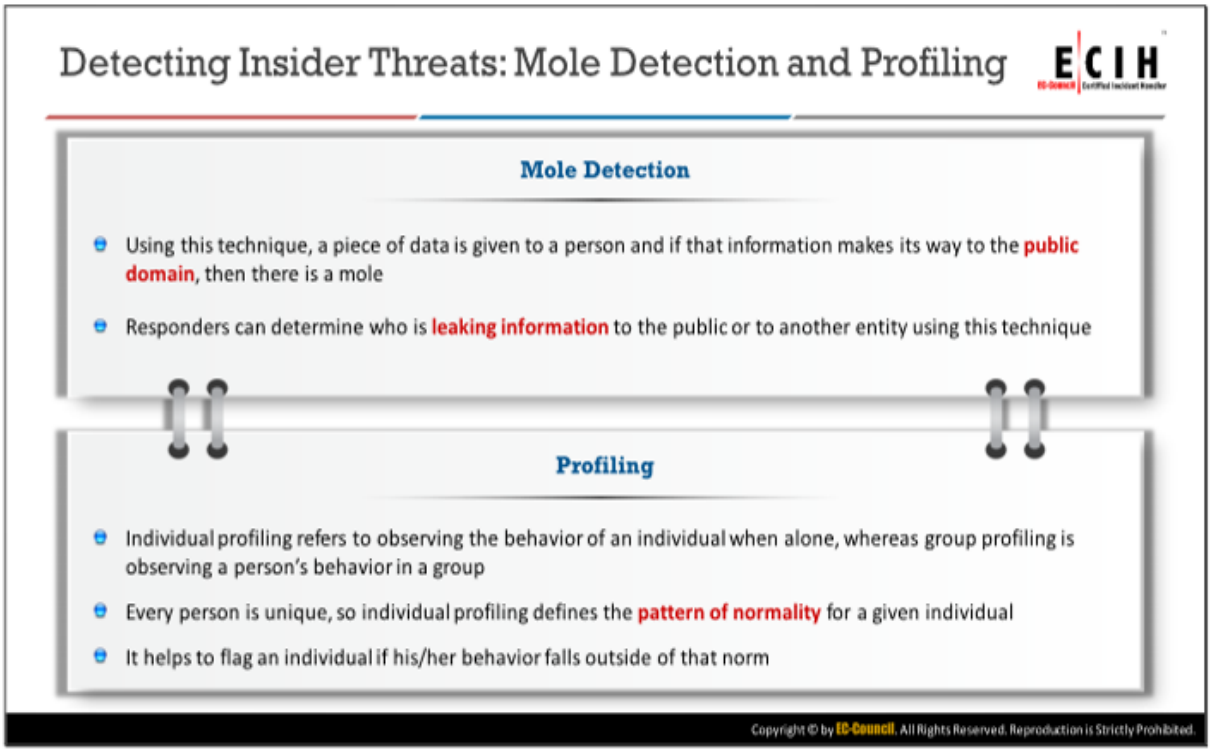


Detecting Insider Threats

After obtaining reports of suspicious activity, incident responders must start analyzing network logs, database logs, email logs, application logs, file access logs, and remote access logs, and perform memory analysis to check if the suspicious activity is an attack. Responders must look for suspicious network connections, data transfers, and downloads to determine the type of attack as well as the resources involved in it. Incident responders can use techniques such as behavioral analysis and mole detection to confirm the attacker. They can enable network sniffers to capture the data of suspicious employees and analyze the captured packets to confirm the attack. They also can consider factors such as misbehavior with coworkers and supervisors, dropping performance levels, little or no dedication toward work, and unexplained absences at work.

After confirming the attack, the responders must isolate suspicious systems or resources from the functional network. They must block all access of suspected employees including email, application accounts, physical access cards, and network credentials and follow containment and eradication processes to stop the propagation of the attack. They should analyze the resources involved in the attack including suspect systems, accounts, and databases to find the data accessed.

In some cases, the attackers might use systems or credentials of other employees to perform the attack. In this situation, incident responders must make use of physical security such as surveillance cameras to confirm the attacker.



Detecting Insider Threats: Mole Detection and Profiling

- **Mole Detection**

  A corporate mole is an employee who pretends to be a dedicated worker but performs malicious activities secretively. Mole detection is not technically sophisticated, but finding the individual who is leaking information is important. To identify a mole, the organization must provide each employee with unique piece of data and make them believe that it is crucial. The malicious employee will try to reveal the given information either for financial benefits or to damage the organization.

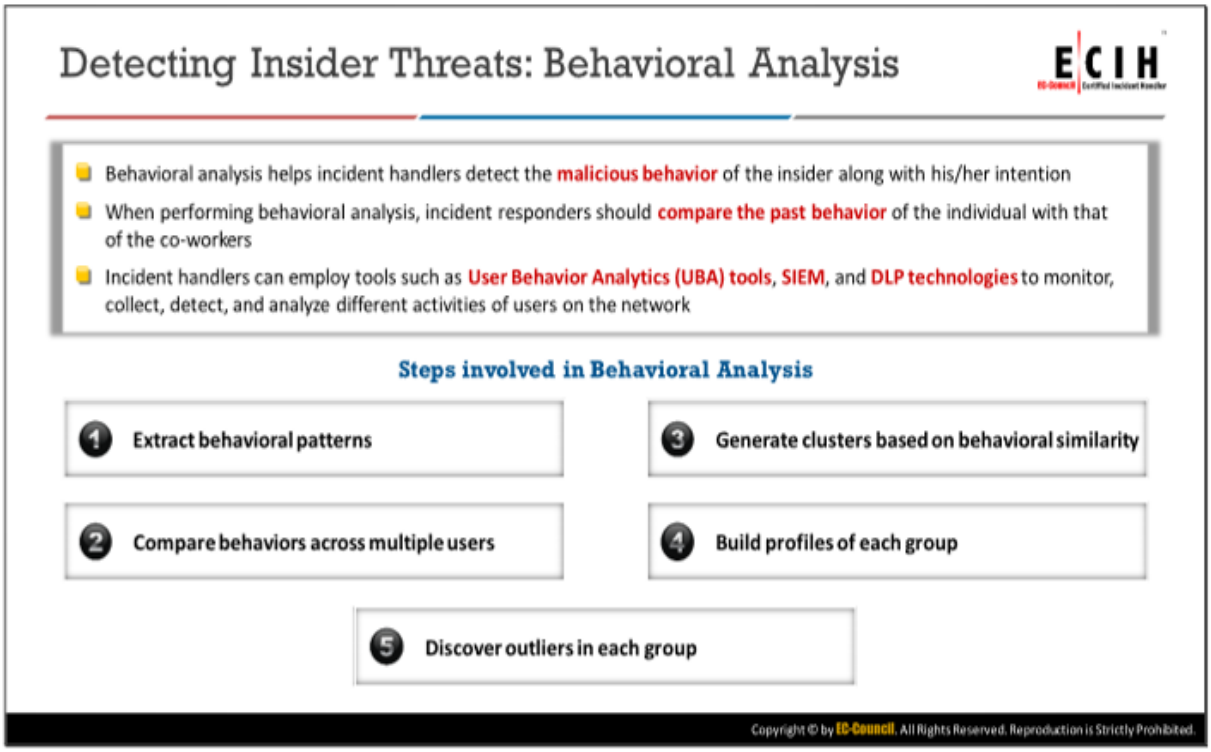
  The incident responders must then check if any of the information provided to the employees has made its way to the public domain. As each employee receives unique data, it will be easy for them to identify the mole. They can also confirm the suspect by pretending to be discussing sensitive information near the suspects and observing if they try to hear and leak the information.

- **Profiling**

  Profiling is an ideal way to detect insiders by identifying their behavior patterns. It is an excellent technique and includes two ways of performing it:

  - Individual profiling
  - Group profiling

  Individual profiling refers to observing the behavior of an individual when alone, whereas group profiling is observing a person's behavior in a group. Every person is unique, so individual profiling defines the pattern of normality for a given individual. It helps to flag the persons if their behavior falls outside of that norm. Note that an insider can make adjustment to his behavior, if he/she knows individual profiling is going on.



Detecting Insider Threats: Behavioral Analysis

Insider threats generally originate from within the organization and from insiders who behave differently than normal employees. Behavioral analysis helps incident handlers detect malicious insider behavior along with their intentions. While performing behavioral analysis, incident responders need to compare the individual's past behavior with that of their coworkers. This helps in detecting abnormal or malicious behavior.

The major challenge in performing behavioral analysis for detecting insider threats is building appropriate user behavioral profiles suitable for detecting insider threats and defining thresholds for each individual's normal and abnormal behavior. Also, the amount of data collected from internal networks is enormous and includes information such as work schedule patterns, internet browsing patterns, emails sent and received, usage of social media websites, and files accessed. It is important for the incident handlers to understand which data is critical for behavioral analysis.

Behavioral analysis includes the following processing steps:

- **Extract behavioral patterns**

  Capture all the data transmitted over the network between devices such as end systems, file, and application or database servers along with the external traffic to and from the internet. From this data, extract each user's behavioral patterns.

- **Compare behaviors across multiple users**

  Compare each user's behavioral pattern with the patterns of other users within the organization.

- **Generate clusters based on behavioral similarity**

  Create different user groups based on behavioral similarities. Generate threshold values for each group's boundaries.

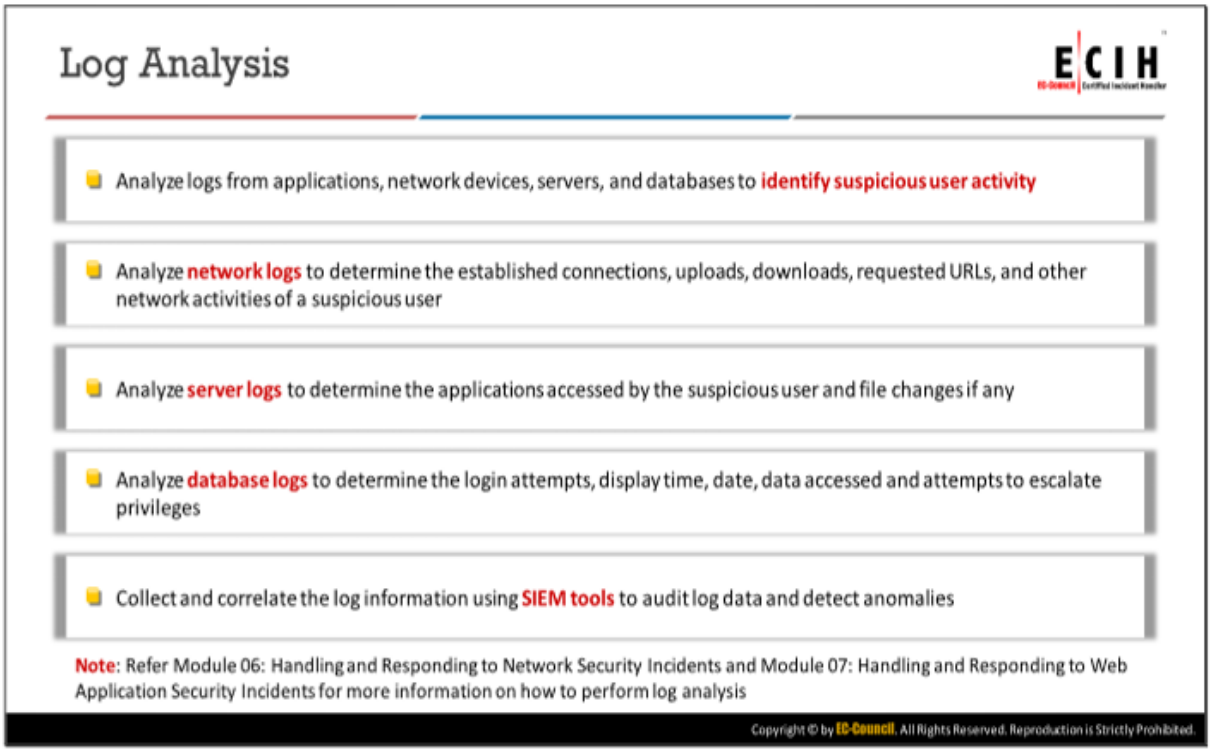
- **Build profiles of each group**

  Generate profiles of each group's behavioral pattern.

- **Discover outliers in each group**

  Outliers are identified as having behavior patterns falling outside threshold values so they can flagged as suspicious.

Incident handlers can employ tools such as user behavior analytics (UBA) tools, security information and event management (SIEM), and data loss prevention (DLP) technologies to monitor, collect, detect, and analyze different user activities. These technologies apply sets of rules that utilize machine learning to detect anomalous user behavior, perform statistical analysis, and generate alerts when a user attempts to perform any malicious action deviating from their normal behavior. Machine learning can detect more sophisticated attacks in which insiders dwell in the network and later move laterally to escalate privileges. This helps incident handlers gain more insight into the incident. Incident handlers can also use advanced technology such as user and entity behavior analytics (UEBA) that includes advanced algorithms to monitor the entities (users, devices, applications, servers, and so on) and identify security anomalies. These anomalies help in detecting the presence of malware and lateral movement of the insider. Incident handlers can use tools such as ObserveIT, DataRobot, CyberArk, and Ekran System to perform behavioral analysis.



Log Analysis

Analyzing log files help incident handlers detect the perpetrator. These files contain valuable data about activities performed on the system and network. Analyzing logs from network devices, servers, and databases to find suspicious user activities such as multiple login attempts, unauthorized file access, and privilege escalation. Log files can provide details like event dates and times, IP and MAC addresses of the source and destination computers, information accessed, URLs, login/logout information, and files accessed.

Incident handlers should analyze the following log files to detect a malicious insider in the target organization:

- **Network Logs**

  Analyzing network logs will help incident handlers understand established connections, uploads, downloads, requested URLs, and other network activities of a suspicious user. Different sources on a network or device produce their own respective log files. These sources may be operating systems, IDS, and firewall. Comparing and relating the log events help the incident handlers to deduce how the incident occurred and identify the insider responsible for that incident.

- **Server Logs**

  Analyzing server logs will help incident handlers to determine the applications the suspicious user has accessed and what file changes, if any, have been made. Server logs contain information such as the request made, client IP address, time of request, page requested, HTTP code, user agent, referrer, and bytes received.

- **Database Logs**

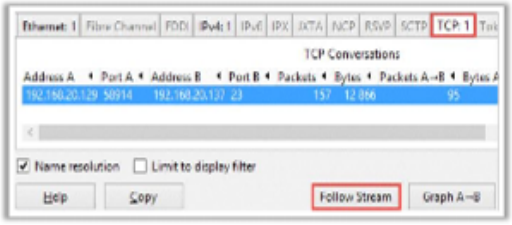
  Analyzing database logs will help to determine the display time, date, and data the user accessed, login attempts, and attempts to escalate privileges. Databases contain transaction logs that store details such as PageID of the modified page; length and offset of the page; commit, abort, and rollback information; the log sequence number (LSN); previous LSN; transaction ID number; type of database log; and the information about the changes that triggered the log record.

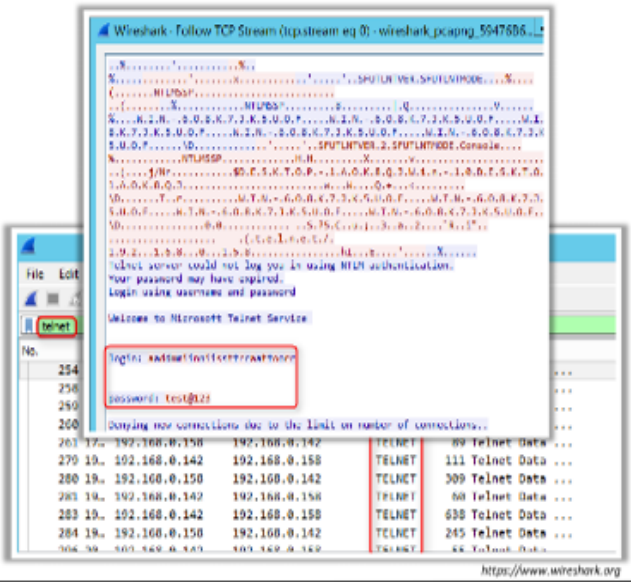
Incident handlers can use SIEM tools to analyze the details of suspicious users from log analysis and event correlation. Incident handlers can collect the log information and correlate them using SIEM tools to audit log data and detect anomalies. They can use the details of suspicious users from log analysis such as IP address and MAC address in SIEM tools to find relevant activities.

Note: Refer to Module 06: Handling and Responding to Network Security Incidents and Module 07: Handling and Responding to Web Application Security Incidents for more information on how to perform log analysis.

Network Analysis: Detecting Malicious Telnet Connections

- Incident handlers can use tools such as **Wireshark** to analyze and detect suspicious activities across the organizational network
- To perform network analysis, incident handlers must **enable filters** on network traffic using Wireshark
- Analyzing the network traffic, incident handlers can detect that an employee within the organization has initiated a **Telnet connection**, violating the security policy of the organization

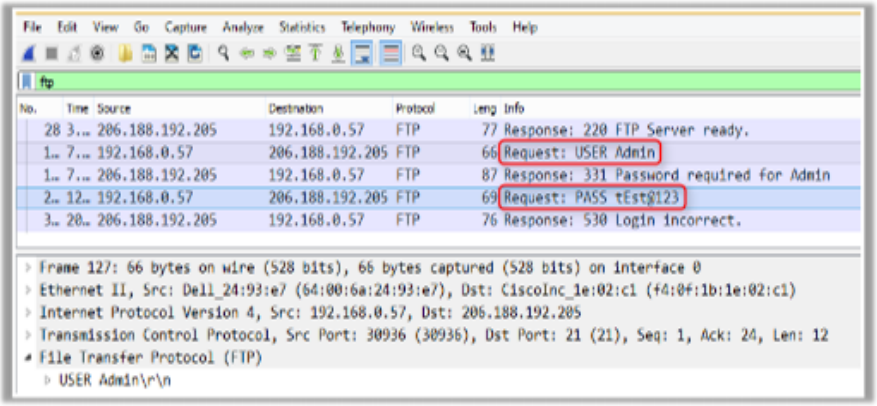




https://www.wireshark.org

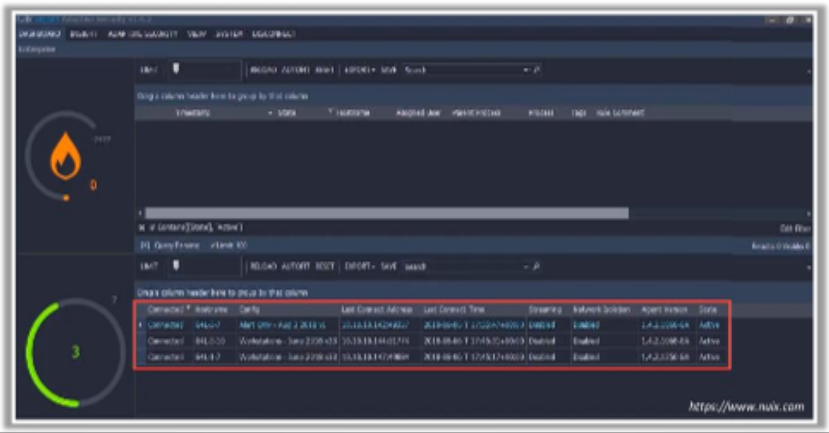
Network Analysis: Detecting Malicious FTP Connections

- FTP protocol sends and receives data in a clear text format over **TCP connections** and is easily **susceptible to sniffing attacks**
- Organizations enforce strict security policies in preventing the usage of FTP protocol for transferring files
- Screenshot shown below displays an **FTP connection** attempt with administrator credentials to transfer critical files



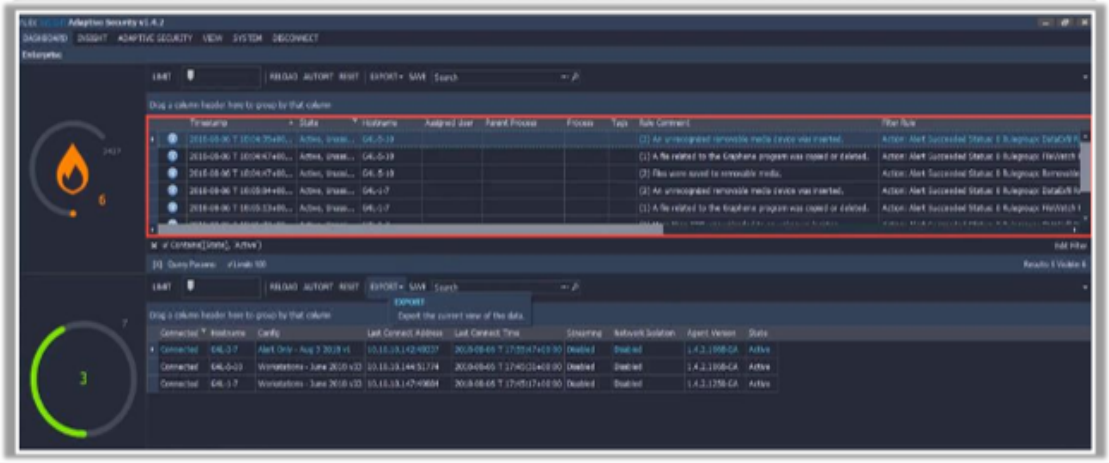
Network Analysis: Detecting Data Exfiltration

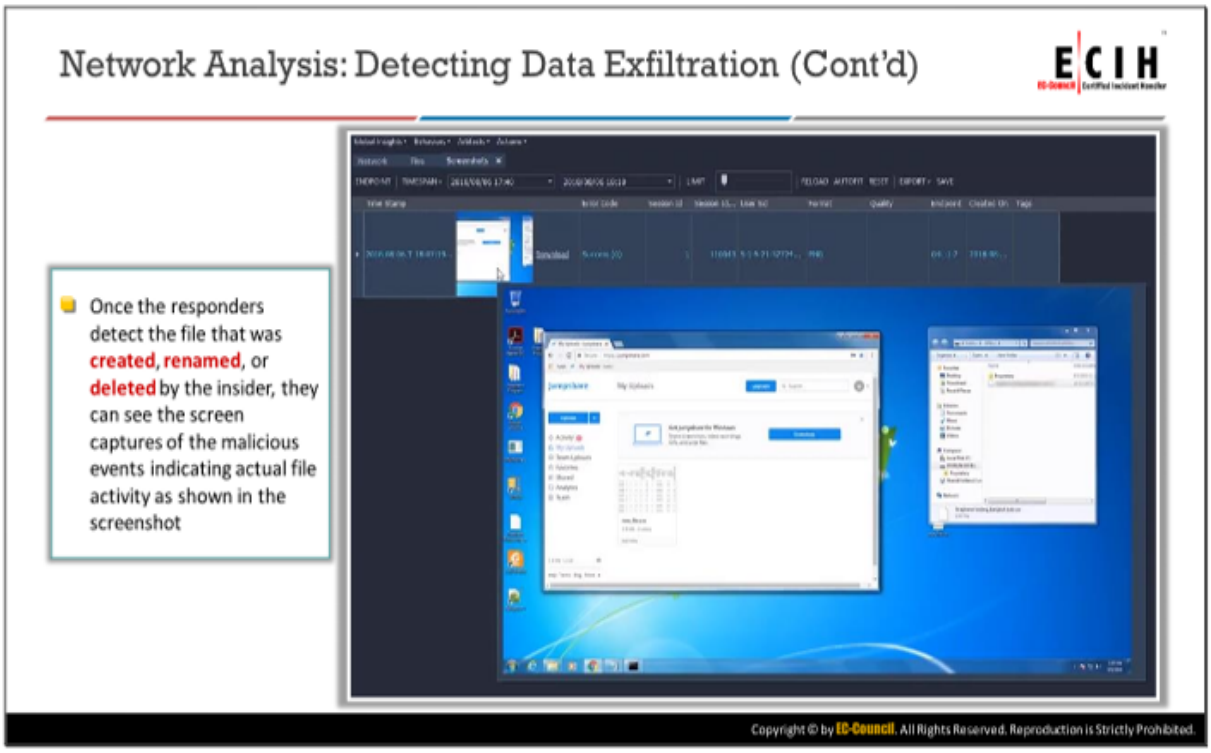
- An incident handler can detect a data exfiltration attack performed by an insider using the **Nuix Adaptive Security** tool
- In the enterprise console of the Nuix Adaptive Security tool, three endpoint systems are connected to the enterprise server, as shown in the screenshot
- These endpoints stream the data back to the server which helps with the **detection of potentially malicious events** in real time



Network Analysis: Detecting Data Exfiltration (Cont'd)

- For example, an employee has performed data exfiltration by plugging in the pen drive to one system, copying the file "**Account_Details.csv**" and later logging into another system, changing the name of the file, and uploading it to the cloud
- All of these activities can be captured by the Nuix Adaptive Security tool in the form of alerts, as shown in the screenshot





Network Analysis

Incident handlers need to perform network traffic analysis to detect anomalous network activities of malicious insiders. Network traffic analysis helps incident handlers detect established malicious connections, the type and number of devices accessed, and exfiltrated data.

- **Detecting Malicious Telnet Connections**

  Source: *https://www.wireshark.org*

  Incident handlers can use tools such as Wireshark to analyze and detect suspicious activities across the organizational network. To perform network analysis, incident handlers need to enable filters on network traffic using Wireshark. The screenshot shown on the slide is displaying the captured network traffic of the target organization. Analyzing this network traffic, incident handlers can detect that an employee within the organization has initiated a telnet connection violating the security policy of the organization.

  As shown in the screenshots given on the slide, by analyzing the telnet packets, incident handlers can detect that a malicious insider had used administrator credentials and established a telnet connection to transfer sensitive data of the organization.

- **Detecting Malicious FTP Connections**

  Similarly, incident handlers can use Wireshark to capture and analyze network traffic using FTP protocol. Generally, organizations enforce strict security policies in preventing the usage of FTP protocol for transferring files. FTP protocol sends and receives data in a clear text format over TCP connections and is easily susceptible to sniffing attack. The

screenshot given on the slide displays an FTP connection attempt with administrator credentials to transfer files containing critical information of the organization.

- **Detecting Data Exfiltration**

  Source: *https://www.nuix.com*

  Incident handlers can use Nuix Adaptive Security tool to set up certain rules that monitor the network as well as the number of events and activities associated with user accounts within the organization. These rules provide responders with the ability to detect malicious events and to intervene automatically in order to protect the network against threats.

  The screenshot given on the slide shows an enterprise console which depicts the behavior of three endpoint systems that are connected to the enterprise service. An incident handler can detect data exfiltration performed by an insider within an organizational network by using this information.

  These endpoints are streaming data back to the server, which helps an incident handler detect potentially malicious events in real time.

  For example, in an organization, employees can perform data exfiltration where they have plugged a USB drive into one system, copied a file "Account_Details.csv" and later logged in to another system, changed the name of the file, and uploaded it to the cloud.

  All these activities can be captured by the Nuix Adaptive Security tool in the form of alerts as shown in the screenshot given on the slide.

  In the screenshot given on the slide, the first alert, "An unrecognized removable media device was inserted," indicates that an employee has plugged a device into a system. This alert reveals that the inserted device is not authorized; therefore, it is regarded as unknown. Other alerts indicate various activities such as copying, creating, renaming, and uploading a file.

  The responder can examine the network activity from the alert in a specific time slot to determine the files that were transferred within the defined time period. In file system activities, by narrowing down the search to a specific file, the responder can determine the files that were created, renamed, or deleted as shown in the below screenshot.

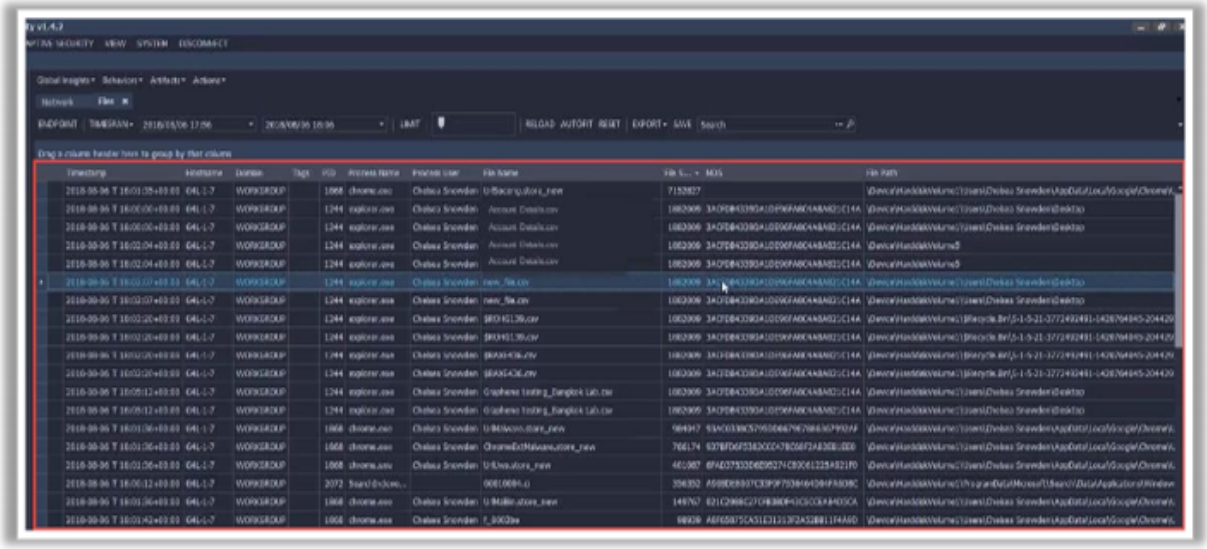
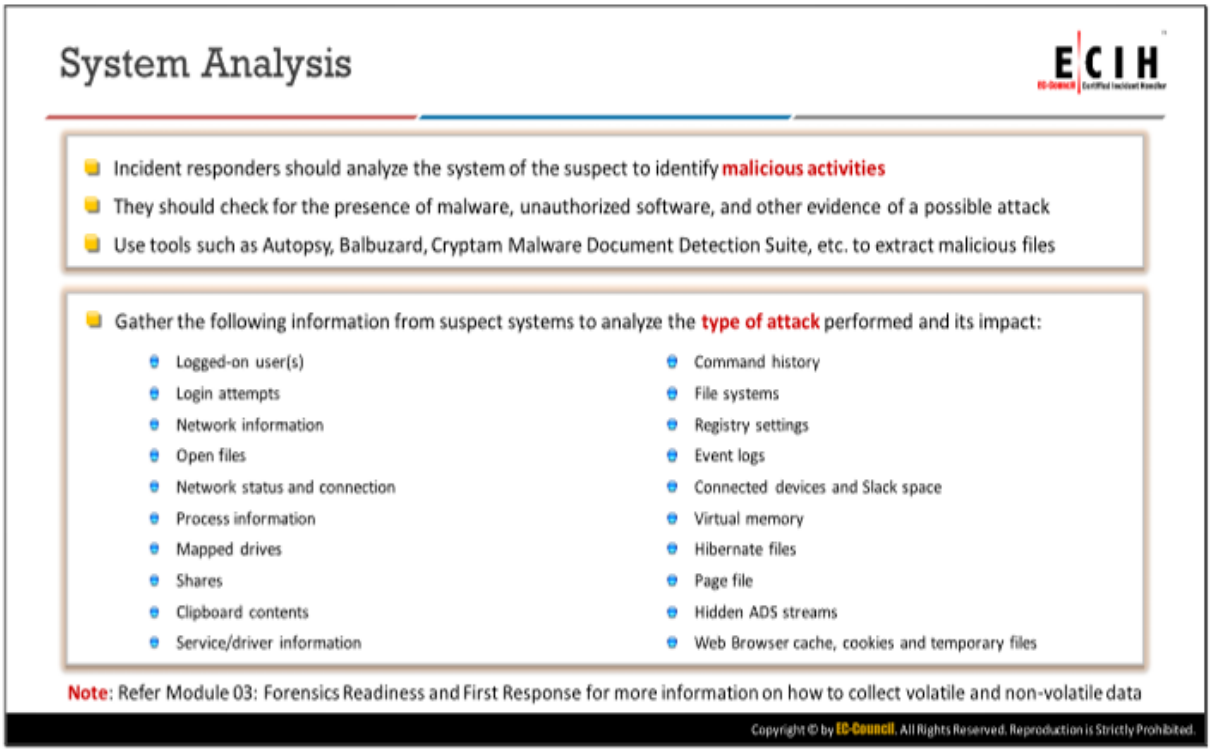


Figure 9.2: Screenshot of Nuix Adaptive Security tool showing renamed file

Once the responder detects the file that was created, renamed, or deleted by the insider, the screen captures can show the malicious events that indicate actual file activity, including an employee changing the stolen file name and uploading it to the cloud as shown in the screenshot given on the slide.

Using this Nuix Adaptive Security tool, the incident responder can also restore the deleted file to the enterprise server. The information gathered from the logs and user activities can assist the incident responder in identifying the malicious insider.



System Analysis

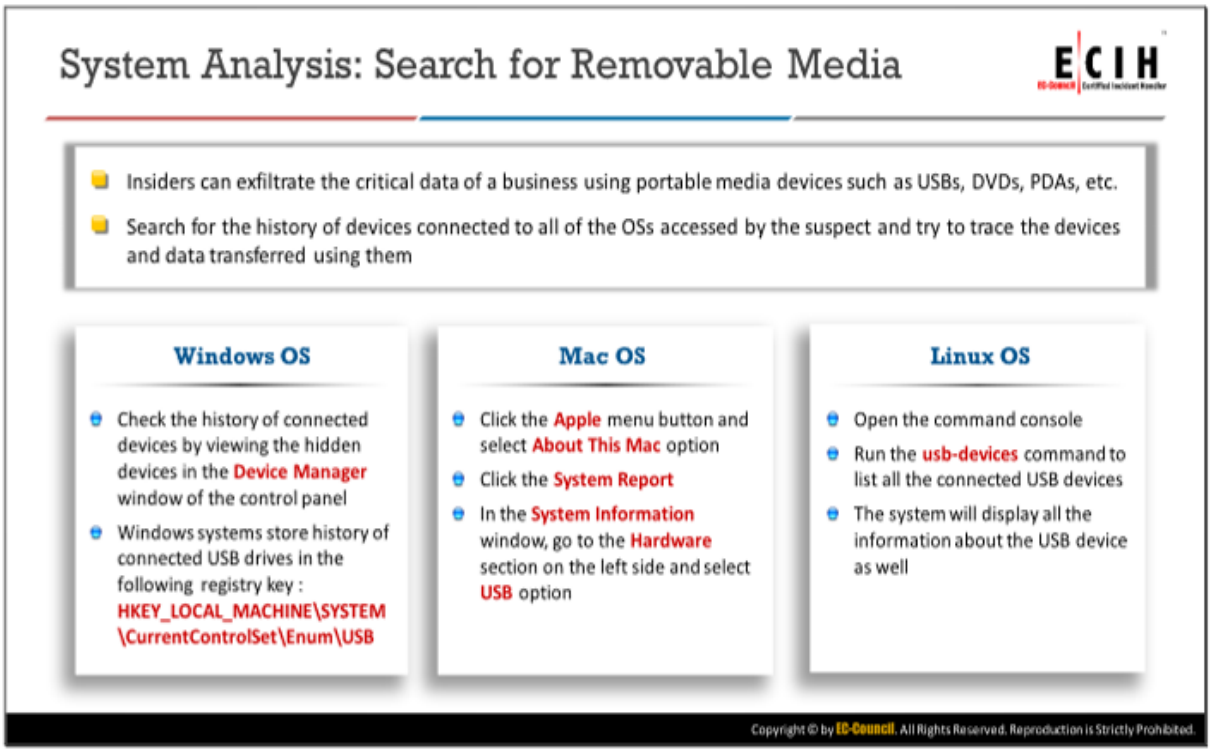
After determining which employees are suspected, the incident responders must conduct a thorough examination of their systems, networks, accounts, and other connected devices to find the traces of malware, unauthorized software, evidence of attack, and so on. The responders must gather the volatile and non-volatile information from the systems and analyze it to determine the type of attack performed and its impact.

Detect suspicious activity on a live system by analyzing the following:

- Logged-on user(s)
- Login attempts
- Network information
- Open files
- Network status and connection
- Process information
- Mapped drives
- Shares
- Clipboard contents
- Service/driver information
- Command history
- File systems
- Registry settings
- Event logs
- Connected devices
- Slack space
- Virtual memory
- Hibernate files
- Page file
- Hidden ADS streams
- Web browser cache, cookies, and temporary files

Incident responders can use tools such as Autopsy, Balbuzard, and Cryptam Malware Document Detection Suite to extract patterns of investigative interest from the systems.

Note: Refer to Module 03: Forensics Readiness and First Response for more information on how to collect volatile and non-volatile data.



System Analysis: Search for Removable Media

Insiders can use USB based portable media devices to connect to systems and exfiltrate sensitive information or upload malicious files onto the system and servers. Therefore, incident responders must check the suspect systems for use of removable media devices by analyzing special access points and registries that associated store data. Look for the history of devices connected to all the OSs accessed by the suspect and try to trace the devices and data transferred using them. Analyze the registry log files for details of the connected devices. This will provide information such as the name of the device, time of connection, and actions performed. Correlate these details with logs obtained from the network devices and servers to find the attack pattern.

Look for removable devices in Windows OS:

- Check the history of connected devices by viewing the hidden devices in the **Device Manager** window of the control panel.
- Windows systems stores the history of connected USB drives in the following registry key: **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB`**.

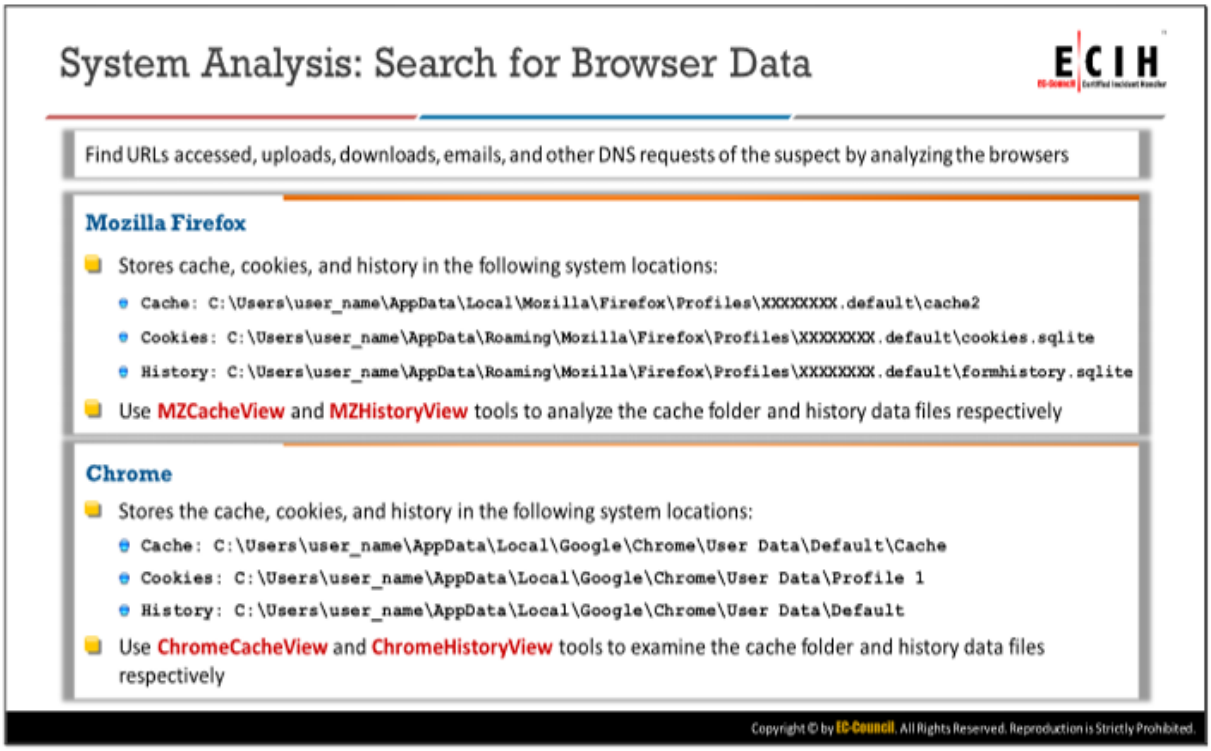
Look for removable devices in Mac OS:

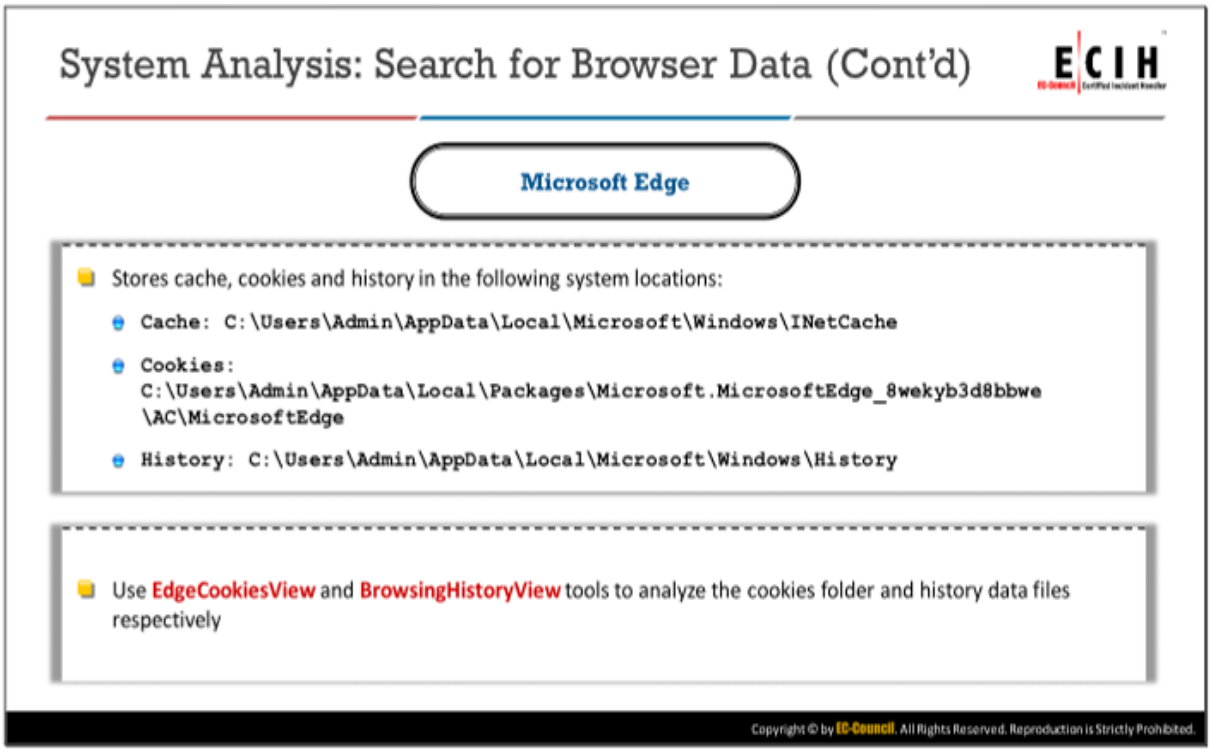
- Click the **Apple** menu button and select **About This Mac** option.
- Click the **System Report.**
- In the **System Information** window, go to the **Hardware** section on the left side and select **USB** option.

Look for removable devices in Linux OS:

- Open the command console.
- Run the **usb-devices** command to list all the connected USB devices.
- The system will display all the information about the USB device as well.

Incident handlers can use tools such as Plug and Play (PnP) Manager and USBDeview to analyze the connected removable devices on a system.





System Analysis: Search for Browser Data

Browsers connect with the internet and allow users to access external servers and cloud data. The browsers save system data in the form of cache, cookies, and history. Incident responders can gather this information and analyze it to find the type of connections the system made, protocols used, websites visited, and content accessed and downloaded. Incident responders can find URLs accessed, uploads, downloads, emails, and other DNS requests of the suspect using the following locations:

- **Mozilla Firefox**

  The Mozilla Firefox stores cache, cookies, and history in the following system locations:

  - **Cache**

    `C:\Users\user_name\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default\cache2`

  - **Cookies**

    `C:\Users\user_name\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite`

  - **History**

    `C:\Users\user_name\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\formhistory.sqlite`

  Use MZCacheView, MZCookiesView, and MZHistoryView tools to analyze the cache folder, cookie folder, and history data files, respectively.

- **Google Chrome**

  Google Chrome records the following information about browsing history on the system:

  - **Cache**

    `C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache`

  - **Cookies**

    `C:\Users\user_name\AppData\Local\Google\Chrome\User Data\Profile 1`

  - **History**

    `C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default`

  Use ChromeCacheView, ChromeCookiesView, and ChromeHistoryView tools to examine the cache folder, cookie folder, and history data files respectively.

- **Microsoft Edge**

  Microsoft Edge stores cache, cookies, and history in the following system locations:

  - **Cache**

    `C:\Users\Admin\AppData\Local\Microsoft\Windows\INetCache`

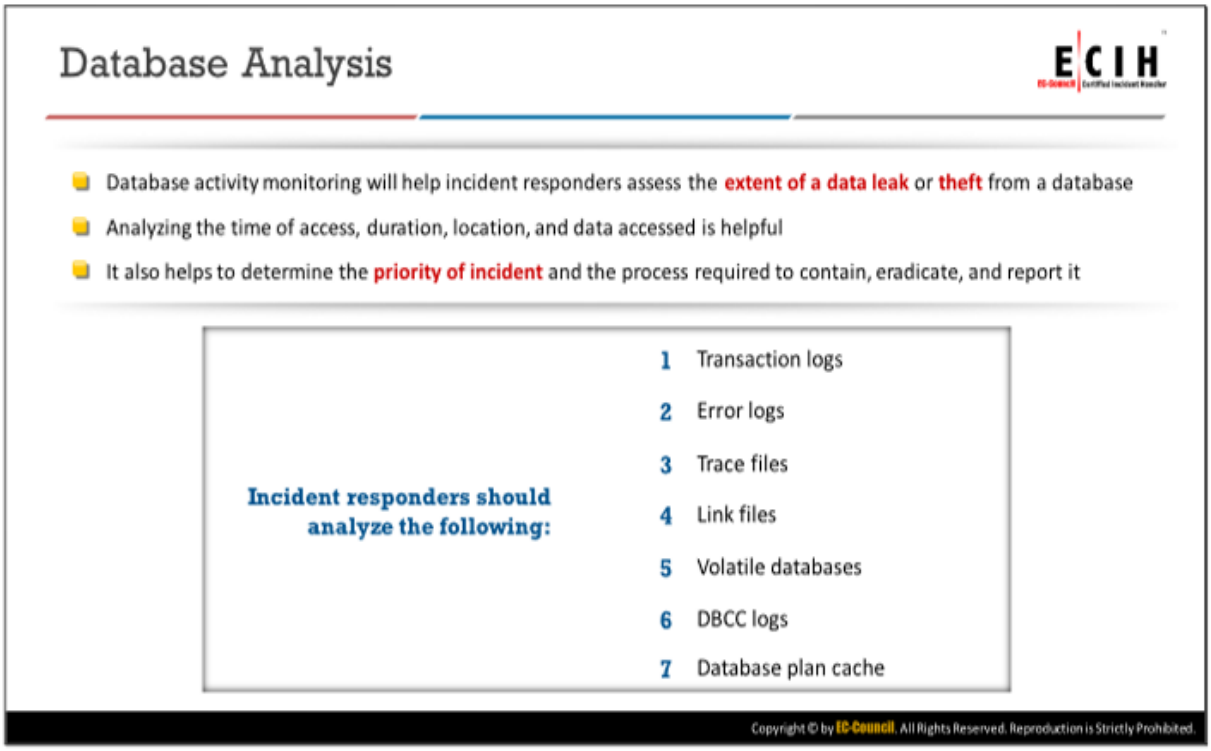
  - **Cookies**

    `C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe \AC\MicrosoftEdge`

  - **History**

    `C:\Users\Admin\AppData\Local\Microsoft\Windows\History`

  Use EdgeCookiesView and BrowsingHistoryView tools to analyze the cookies folder and history data files, respectively.

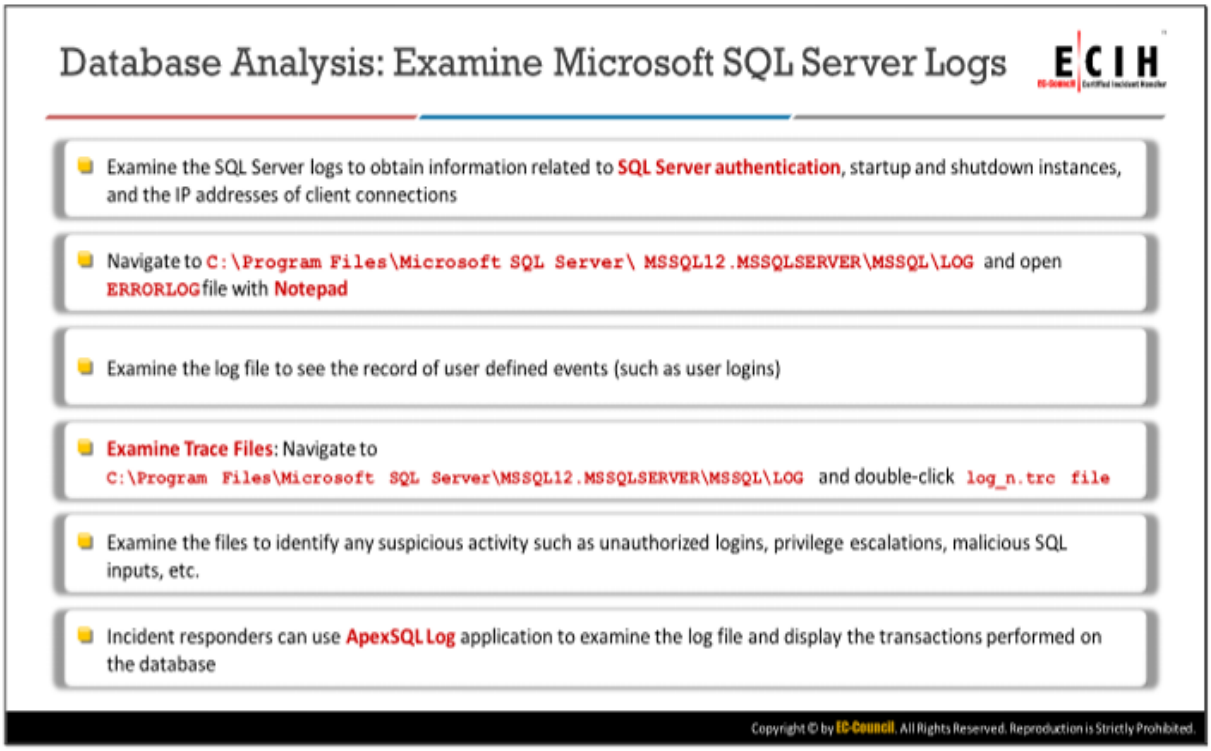


Database Analysis

Organizations store their most sensitive and valuable data in databases, but basic perimeter security provided to databases do not protect it from insiders. Database activity monitoring will help to detect and protect data from malicious insiders by terminating sessions that violate security policy. Database activity monitoring will help incident responders assess the extent of the data leak or theft from a database. It will also help responders analyze the time of access, duration, location, and data accessed. Finally, it helps to determine the priority of the incident and the process required to contain, eradicate, and report it. Incident responders need to analyze SQL database logs to detect attacks on the OS, protocol violations, unauthorized SQL activity, and so on. The perpetrators of high-risk violations should be terminated and the server should be quarantined. Incident responders should be able to monitor Oracle, SQL Server, DB2, MySQL, and other major databases.

The incident responders need to analyze the following:

- Transaction logs
- Error logs
- Trace files
- Link files
- Volatile database
- DBCC logs
- Database plan cache



Database Analysis: Examine Microsoft SQL Server Logs

- **Examine the SQL Server logs**

  Examine the SQL Server logs to obtain information related to SQL Server authentication, startup and shutdown instances, and the IP addresses of client connections.

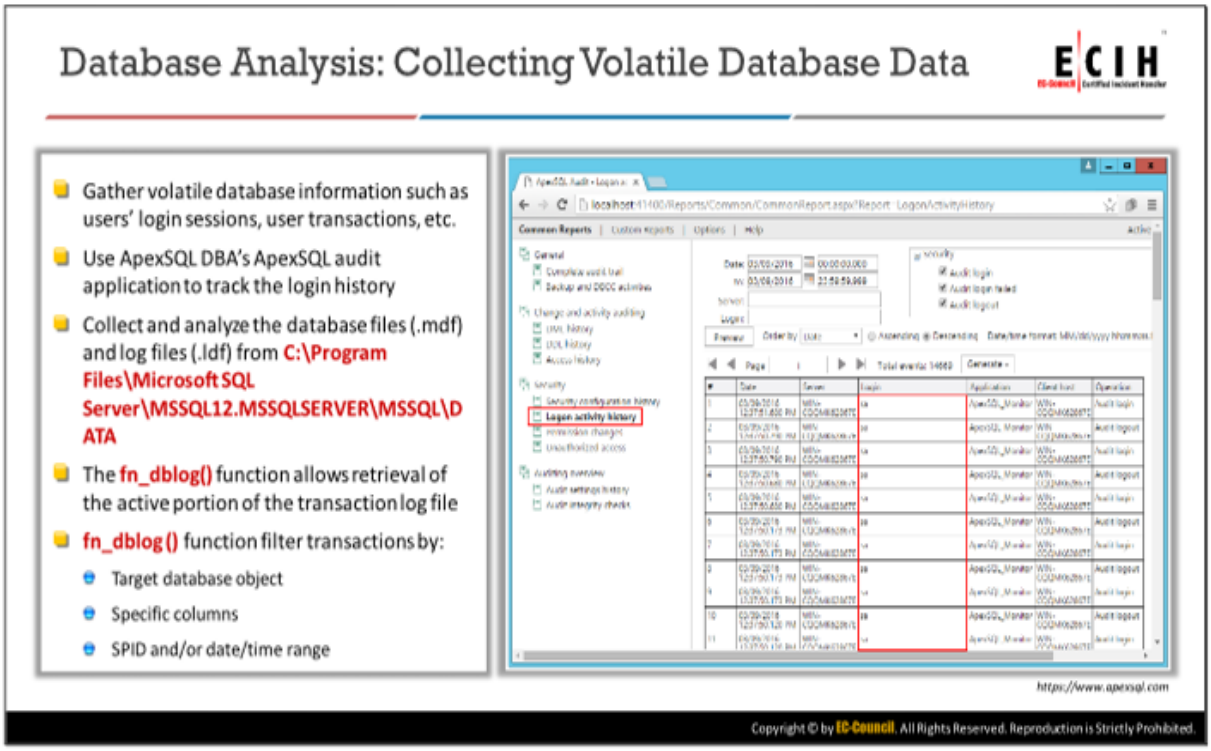
  - Navigate to

    `C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\LOG` and open `ERRORLOG` file with **Notepad.**
  - Examine the log file to see the record of user defined events (such as user logins).

- **Examine Trace Files**

  - Navigate to `C:\Program Files\Microsoft SQL Server\ MSSQL12.MSSQLSERVER\MSSQL\LOG` and double-click the `log_n.trc` file (where n is the last number in the sequence).
  - The trace file opens in a **SQL Server Profiler.**
  - Examine the files to identify any suspicious activity such as unauthorized logins, privilege escalations, and malicious SQL inputs.

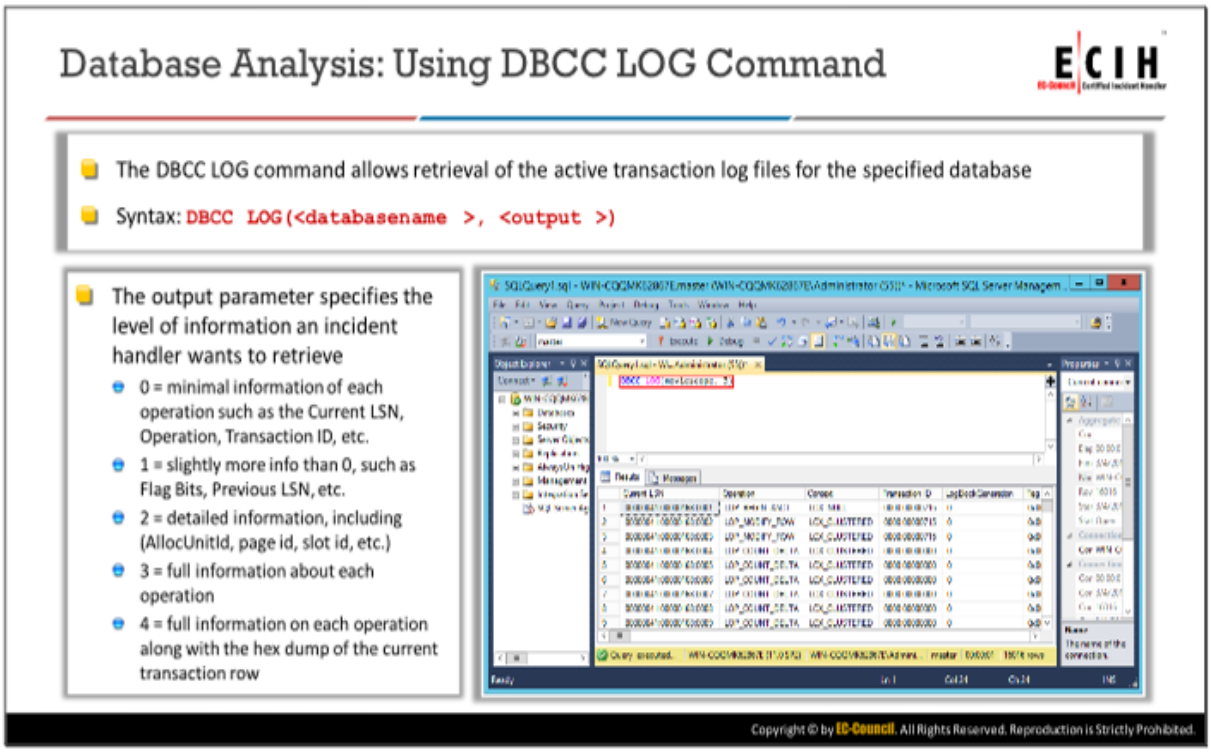
- Incident responders can use ApexSQL Log application to examine the log file and display the transactions performed on the database.



Database Analysis: Collecting Volatile Database Data

Incident responders must gather volatile database information such as users' login sessions and user transactions to find evidence of attack. The following methods will help IRT to collect the respective volatile data from the database:

- Use ApexSQL DBA's ApexSQL audit application to track the login history.
- Collect and analyze the database files (.mdf) and log files (.ldf) from `C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA`.
- These files contain complete data (in .mdf files) and logs (in .ldf files) pertaining to the databases.
- The fn_dblog() function allows to retrieve the active portion of the transaction log file.
- Filter the fn_dblog() function transactions by:
  - Target database object
  - Specific columns
  - SPID and/or date/time range



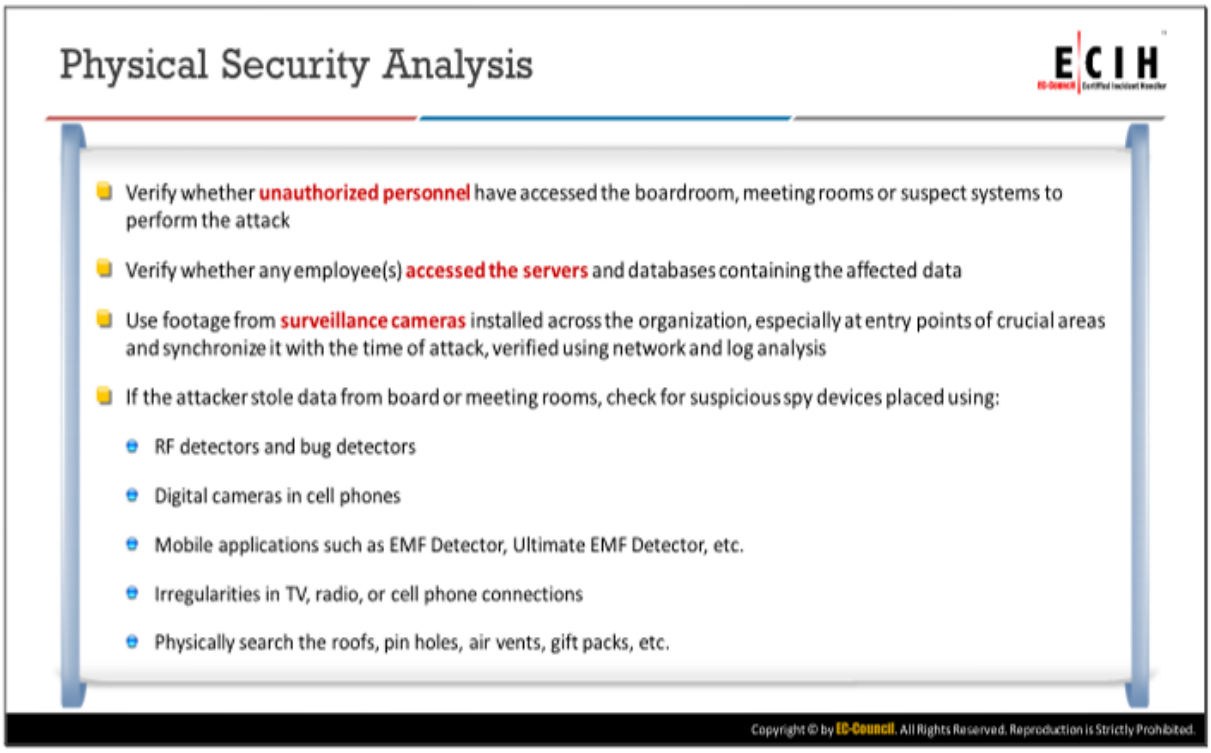
Database Analysis: Using DBCC LOG Command

Database Consistency Checker (DBCC) commands may give the incident responder valuable insight into what is happening within the server system. The DBCC LOG command allows incident handler to view and retrieve the active transaction log files for a specific database.

Syntax: **`DBCC LOG(<databasename >, <output >)`**

The output parameter specifies the level of information an incident handler wants to retrieve. It includes the following levels:

- 0 = minimal information of each operation such as the Current LSN, Operation, and Transaction ID
- 1 = slightly more info than 0, such as Flag Bits and Previous LSN
- 2 = detailed information, including (AllocUnitId, page id, slot id, etc.)
- 3 = full information about each operation
- 4 = full information on each operation along with the hex dump of current transaction row



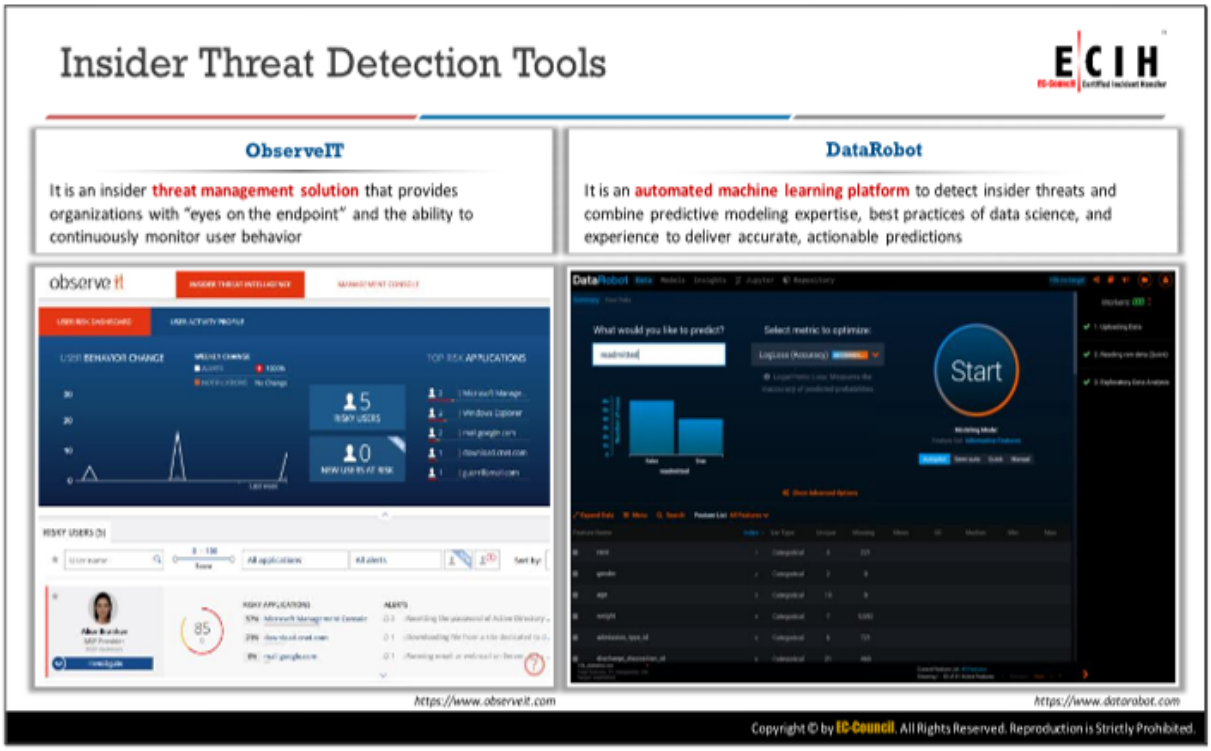
Physical Security Analysis

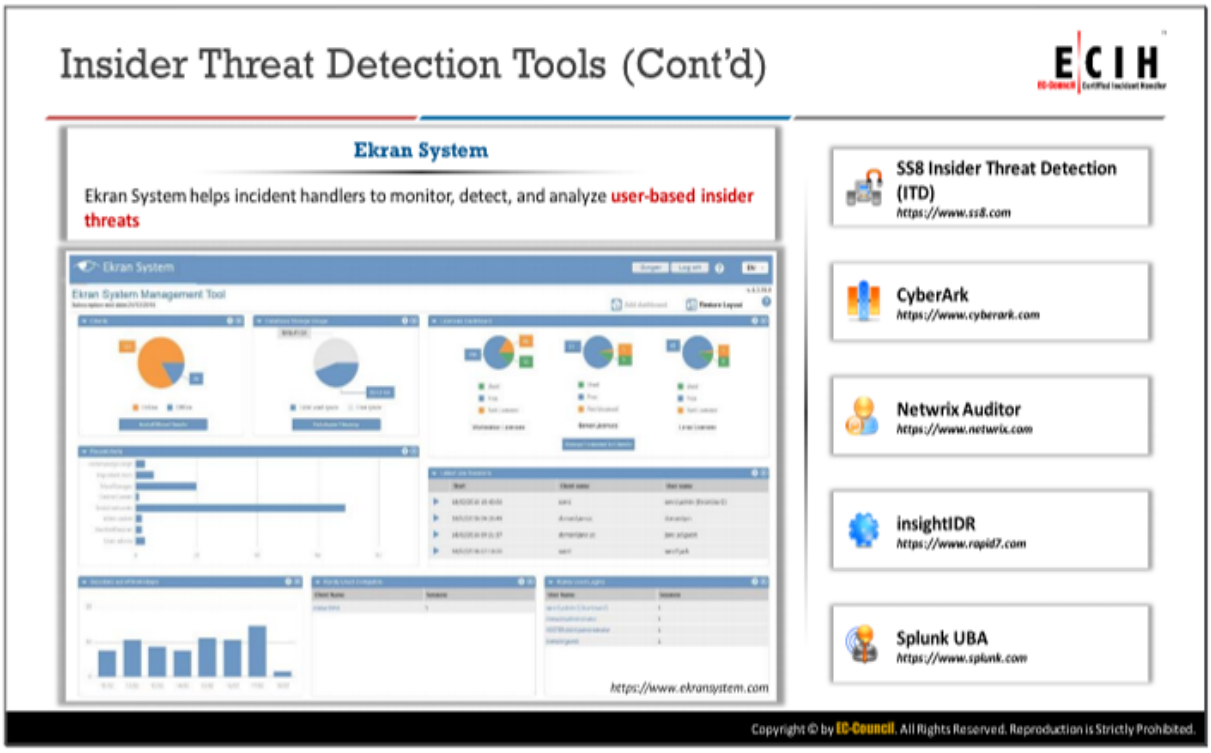
The key to detecting a malicious insider is awareness and observation of surroundings. Incident responders must use the physical surveillance devices installed across the organization to verify the presence of suspect employees during the attack and prove their involvement.

Incident response teams should perform the following to detect insiders who are using physical means of attack:

- Check for unauthorized employees or personnel in board or official meetings; there is a high probability that such employees are trying to breach the organization's information and are potential insider threats.
- Check board and meeting rooms for small lights flashing or weak sounds emitted from devices used to record or spy on meetings.
- Check if any employee had access to the servers and databases containing the affected data.
- Since insiders or spies generally tend to collect sensitive information from coworkers, use surveillance camera recordings to detect the suspicious persons responsible for such incidents.
- Use footage from surveillance cameras installed across the organization, especially at entry points to crucial areas and synchronize it with the time of attack using network and log analysis.
- If the attacker stole data from board or meeting rooms, check for unauthorized or suspicious spy devices placed using:

- RF detectors and bug detectors to detect devices like recorders, trackers, bugs, and other surveillance devices
- Digital cameras in cell phones to detect infrared light and polarized light
- Mobile applications like EMF Detector and Ultimate EMF Detector to detect electromagnetic waves
- Irregularities in TV, radio, or cell phone connections
- Manual searches in the roofs, pin holes, air vents, gift packs, and so on





Insider Threat Detection Tools

Insider threat detection tools help incident responders analyze user behavior, monitor user activities, and detect malicious incidents and suspicious users.

Discussed below are some of the important insider threat detection tools:

- **ObserveIT**

  Source: *https://www.observeit.com*

  ObserveIT enables organizations to quickly identify and eliminate insider threats. It is an insider threat management solution that provides organizations with "eyes on the endpoint" and the ability to continuously monitor user behavior. ObserveIT alerts the security and IT teams immediately about activities that put the organization at risk and offers all the context needed to respond. It uncovers risky user activity by identifying anomalous behavior. It investigates suspicious user activity in minutes. It reduces risk with real-time user alerts, blocking, and education.

- **DataRobot**

  Source: *https://www.datarobot.com*

  DataRobot is an automated machine learning platform for detecting insider threats that combines predictive modeling expertise, best practices of data science, and experience to deliver accurate, actionable predictions with full transparency and rapid deployment. It can be used by organizations to leverage their enterprise usage policies and individual employee data to develop, model, and deploy algorithms that allow for the detection of security breaches, theft or misuse of documents, and violations of clearance responsibilities.

  DataRobot assists incident responders in:

  - Detecting and predicting personnel that require enhanced monitoring or evaluation to prevent insider threats
  - Analyzing historical policy violations and using enhanced monitoring to proactively block future policy violations
  - Proactively monitor cleared personnel for possible security breaches

- **Ekran System**

  Source: *https://www.ekransystem.com*

  Ekran System helps incident handlers monitor, detect, and analyze user-based insider threats. It is a specialized enterprise insider threat detection software that meets the security needs of enterprises of any size. Using indexed session video records as a core format, the product provides multiple search, analysis, and incident response tools that enable employee fraud detection and third-party service provider monitoring.

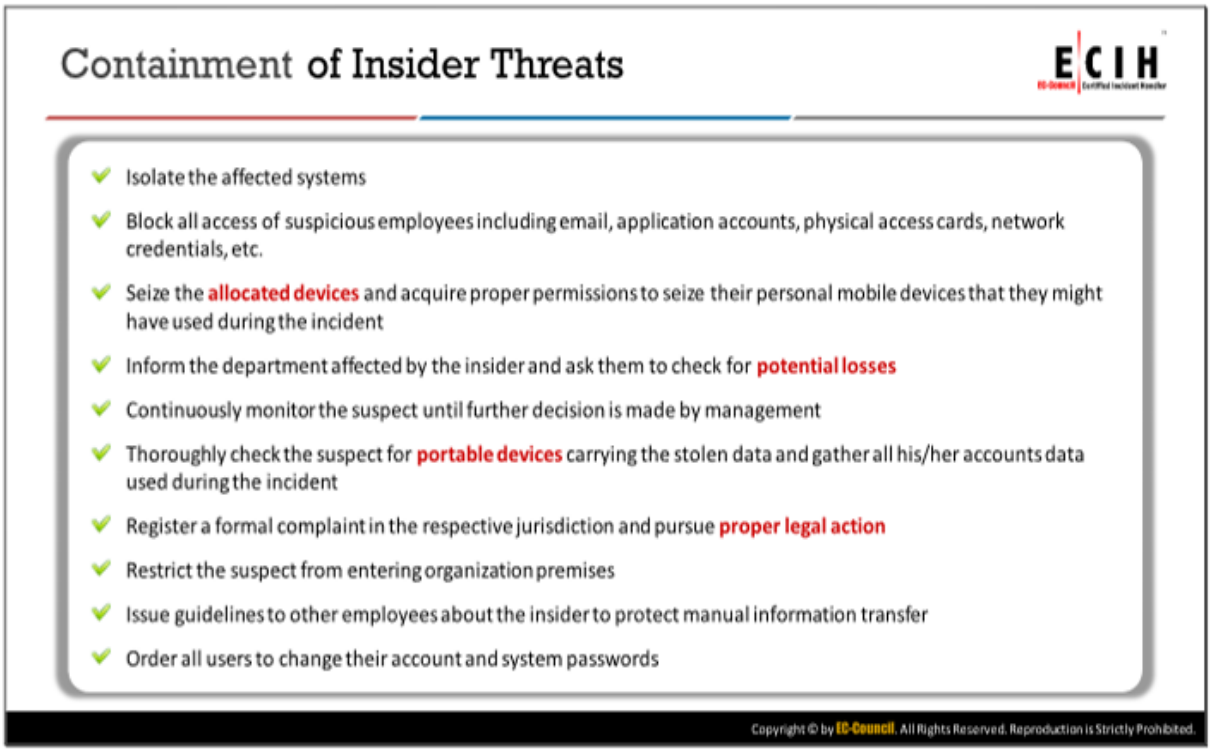
  Features:

  - Insider threat detection tool that does not interfere with business processes
  - Universal, user session monitoring with filtering options
  - Insider threat mitigation tools, including automatic incident response

- Several inbuilt access management tools
- Real-time alerts and scheduled reports
- Comprehensive base for any internal investigation
- Affordable and flexible licensing

Some additional insider threat detection tools include:

- SS8 Insider Threat Detection (ITD) (*https://www.ss8.com*)
- CyberArk (*https://www.cyberark.com*)
- Netwrix Auditor (*https://www.netwrix.com*)
- insightIDR (*https://www.rapid7.com*)
- Splunk UBA (*https://www.splunk.com*)
- Cognito™ (*https://vectra.ai*)
- Forcepoint UEBA (*https://www.forcepoint.com*)
- Securonix UEBA (*https://www.securonix.com*)
- Leidos' Arena ITI™ (*https://cyber.leidos.com*)
- Veriato Recon (*https://www.veriato.com*)



Containment of Insider Threats

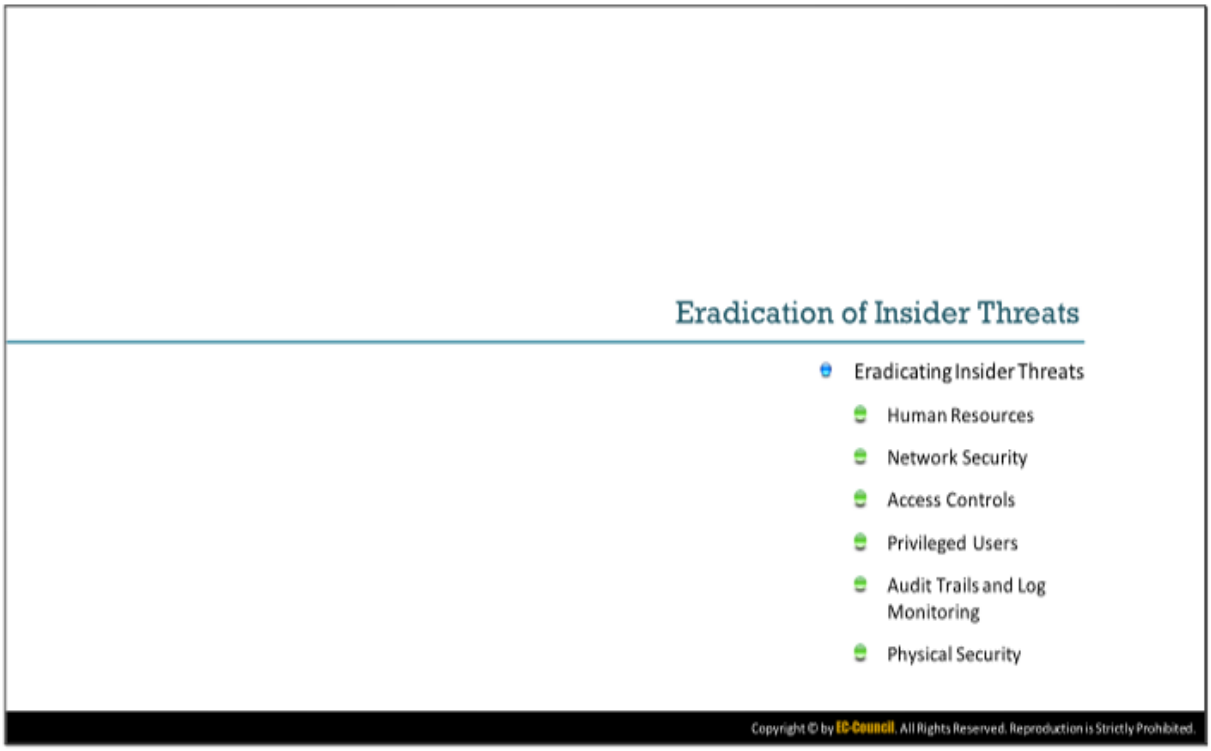
After the detection of an insider attack, containment is the incident responder team primary task. The main goal of the containment process is to minimize the damages posed by the insider attack and prevent it from propagating to other systems and resources within the organization.

This section discusses various steps to be followed for the containment of insider threats.

Threat response depends on the nature of insider threats and the organization's policies. Organizations can deploy automated or human involved responses. Containment of insider threat incidents requires both human elements and technical controls.

Discussed below are steps that must be performed as a part of containment process of insider threats:

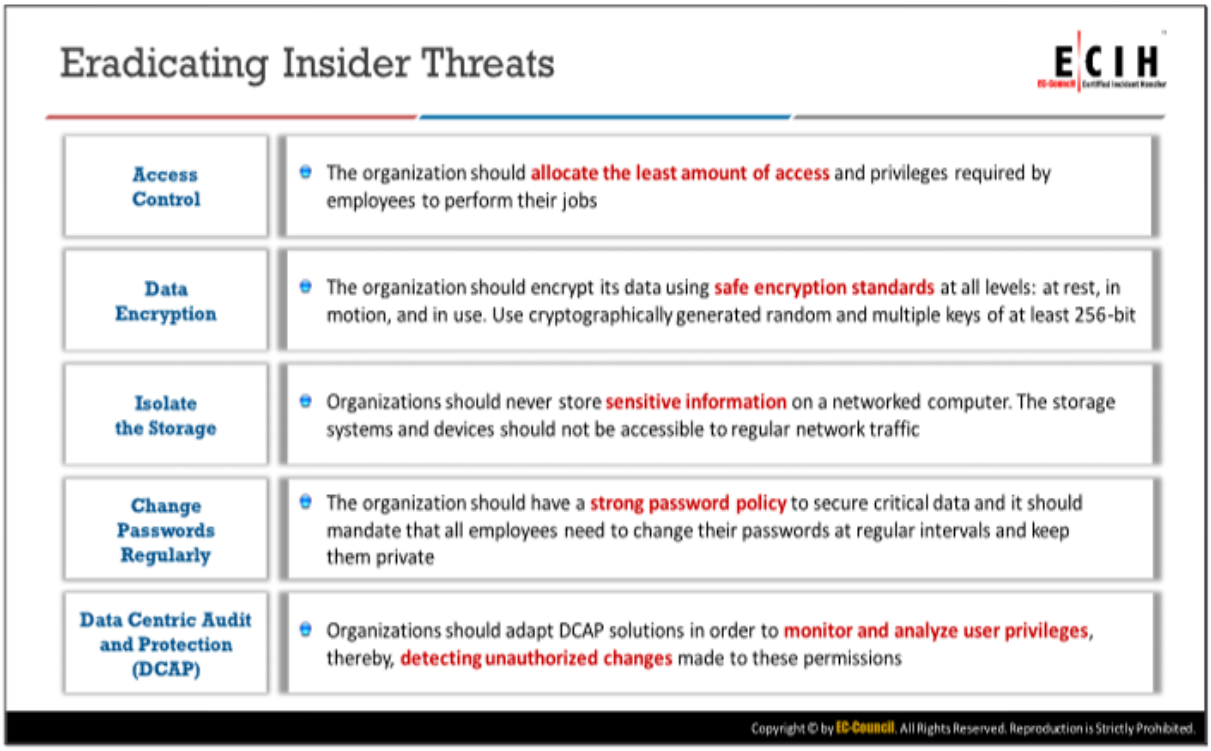
- After detecting the incident, incident responders must isolate the affected systems.
- The IT and computer security team should block the suspect's organizational email account and network credentials, seize company issued desktops, laptops, mobile or other devices, then check the attack vectors the insider used and focus on containment.
- Obtain appropriate permission to seize any personal devices that might have been used in the attack.
- Remove the individual's ability to access organization premises. Remove their system privileges and credentials. Prioritize the threats that lead to espionage and patch them.
- Examine and contain attack vectors such as malware, portable storage devices, secret cameras, phone tapping devices, and recording devices.
- Inform the affected department and request that they check for any potential losses.
- They should also give strict guidelines to other employees to discourage tailgating, use unauthorized drives, transfer data using unencrypted means, and discuss confidential matters in common areas. Change all users' system and account passwords.
- Continuously monitor the employees, contractors, third-party vendors, or outsiders identified as spies until the organization terminates them from the office.
- Thoroughly check the suspect for portable devices carrying the stolen data and gather all account data used during the incident.
- Register a complaint in the appropriate jurisdiction and take the proper legal action, up to and including prosecuting the responsible individual.
- The HR team should block all accesses of suspicious employees and put them under continuous monitoring until further decision from the management.



Eradication of Insider Threats

Due to the increase in cybercrime by insider, valuable information and records are becoming vulnerable to stealing, modification, and exfiltration. Therefore, incident responders must follow certain rules or guidelines essential for eradicating insider threats. Eradication is the key component of security incidents faced by an organization. It includes detecting malicious programs, stopping the network attack, and disabling the responsible user accounts. It is important to carry out eradication steps in order to further prevent malicious insiders from launching new attacks.

This section discusses various steps for human resources, network security, privileged users, access controls, audit trials and log monitoring, and physical security to eradicate insider threats.



Eradicating Insider Threats

The following are some techniques that incident responders can use to secure a company's confidential data and eradicate insider threats:

- **Access Control**

  The best method for controlling insider threats is limiting and controlling access. In almost every situation in which an insider compromises the company, the damage possible is increased because someone had more access than they needed to do their job. To eradicate insider attacks, the organization must allocate the least amount of access and privilege to the employees, which is required to perform their job. If employees require additional privileges, they must request them from supervisors who can scrutinize their necessity before they are granted.

- **Data Encryption**

  The organization should encrypt their data at all levels: at rest, in motion, and in use. To ensure safe encryption standards, an organization should implement usage of cryptographically generated random and multiple keys of at least 256-bit and sufficient length across its devices and application.

- **Isolate the Storage**

  Organizations should never store sensitive information on a networked computer. The storage systems and devices should not be accessible to regular network traffic, and only few trusted individuals should have access to it. Store the devices, systems, servers, and databases in secure environment with physical access restrictions. Use password and biometric authentication-based locks to protect these devices.

- **Change Passwords Regularly**

  The organization should have a strong password policy to secure critical data. The policy must mandate all employees to change their passwords at regular intervals and keep them private. Employees must also lock their system before leaving their workspace, even for a short time. The policy must also prohibit employees from exchanging their system or account passwords or saving passwords on their systems.

- **Data Centric Audit and Protection (DCAP)**

  Organizations should adapt DCAP solutions in order to monitor and analyze user privileges, thereby detecting unauthorized changes made to these permissions. A DCAP solution can be used to automate the process of managing user accounts and monitoring of usage patterns. Organizations can set up DCAP solutions that include automated tools to discover and classify their critical or sensitive data.

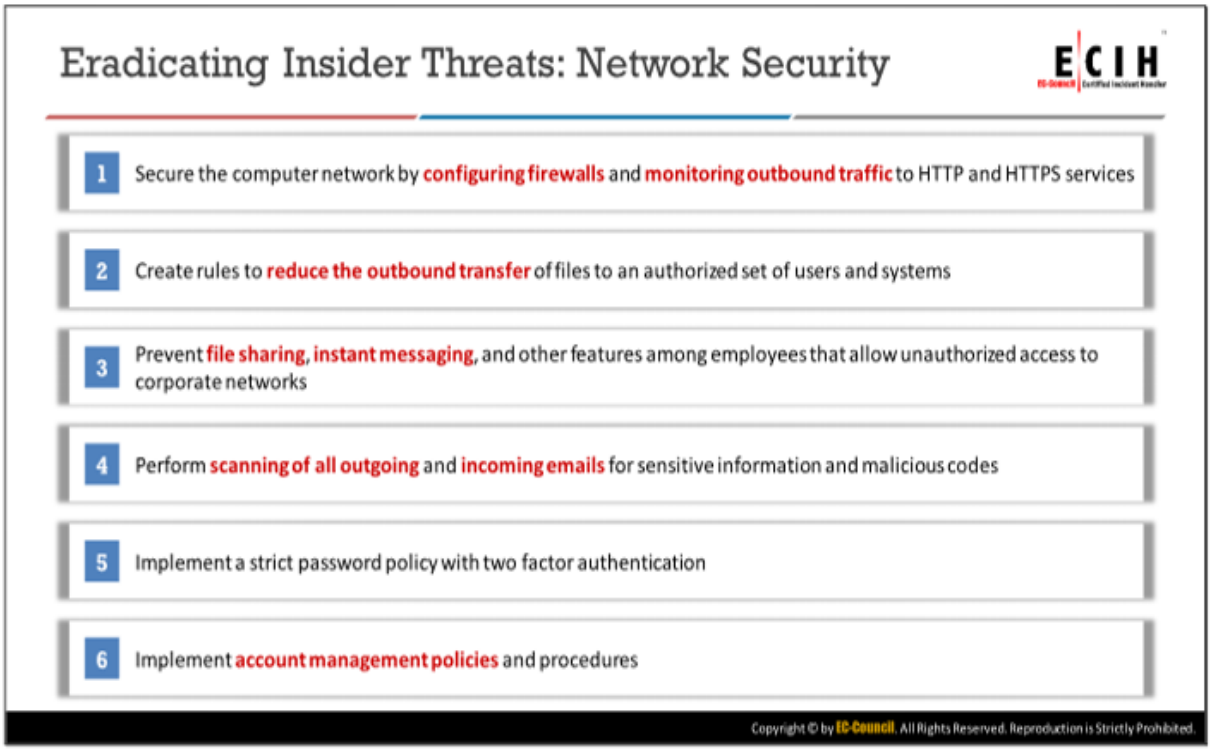
Eradicating Insider Threats: Human Resources

Most cybersecurity problems arise due to the actions and activities performed by an organization's own workforce. Therefore, the human resource department, along with information technology professionals, play a crucial role in eradicating insider threats from the organization.

The following are some of the steps that must be taken by the human resource department to eradicate insider threats:

- Create and implement policies pertaining to employee behavior and ethical use of information.
- Require employees to sign a confidentiality and nondisclosure agreement that describes their agreement with the company's confidentiality policies.
- Using interviews, feedback forms or surveys, allow employees to raise their concerns regarding the workplace and organization.
- Ensure that employees can express their feelings and problems at the workplace and provide suggestions to improve it. This helps to anticipate and manage negative workplace issues as well as helps the organization in examining employee behavior and satisfaction level.
- Keep track of employee expenditures and income generation activities as the unexpected and unexplained changes in financial status of an employee signify an income generated from external sources.

- Audit their financial reports to identify if the employee was involved in any fraud. In most of the cases employees commit an insider threat to the organization unintentionally or unknowingly.
- Provide them proper training and awareness regarding insider activities.
- Conduct a thorough background check on new employees and employees who hold sensitive positions.
- Check their history in previous organizations such as arrest history, history of policy violations, and evidence of financial problems.
- Organizations generally hire temporary employees from third parties, giving these individuals access to organization premises. Monitor all the activities carried out by this staff using surveillance cameras at all important areas.
- Examine and respond to the suspicious behavior of employees, beginning with the hiring process.



Eradicating Insider Threats: Network Security

To protect their networks, organizations are using various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and honeypots. Networks are the preferred targets for compromising an organization's security, and insiders continue to find new ways to breach network security and attack important assets.

The following network security guidelines will help the incident responders to eradicate insider threats:

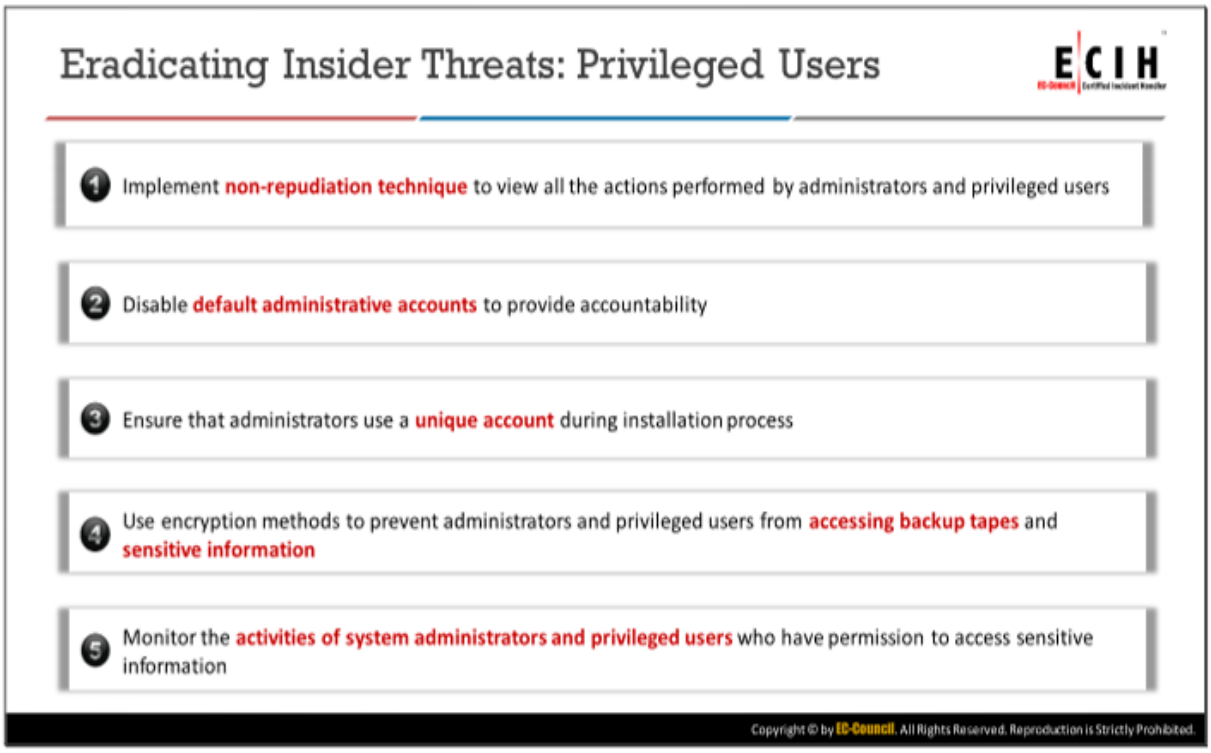
- Secure the computer networks by configuring firewalls and monitoring outbound traffic to HTTP and HTTPS services.
- Create rules to reduce the outbound transfer of files to an authorized set of users and systems.
- Prevent file sharing, instant messaging, and other features among employees that allow unauthorized access to corporate networks.
- Scan all outgoing and incoming emails for sensitive information and malicious codes.
- Implement a strict password policy with two factor authentication.
- Implement account management policies and procedures.
- Implement proper system administration safeguards for critical servers.

Eradicating Insider Threats: Access Controls

The best method for controlling insider threats is limiting and controlling access. In most situations in which insiders compromise the company, the incident occurs because employees have more system access than they need in order to do their job, although other factors of course contribute.

Following are the access control guidelines for eradicating insider threats:

- Enable access privileges to employees or users based on the routine performance of their job roles.
- Disable employees' ability to download content, install applications, enable remote access, modify system logs, or access the boot menu of their systems.
- Install modification alert tools on the user systems that flag attempts to change system settings.
- Regularly audit the access rights of the employees and revoke unnecessary access.
- Implement strict policies for accessing sensitive information.
- Never store sensitive information on a networked computer; store confidential data on a standalone computer that has no connection to other computers or telephone line.
- Document all access requests which are granted to users after being vetted by a supervisor.
- Ensure that employees get permission prior to accessing sensitive systems.
- Disable all an employee's access after termination, including accesses to premises, applications, accounts, and network devices.
- Change the passwords to wireless networks regularly.

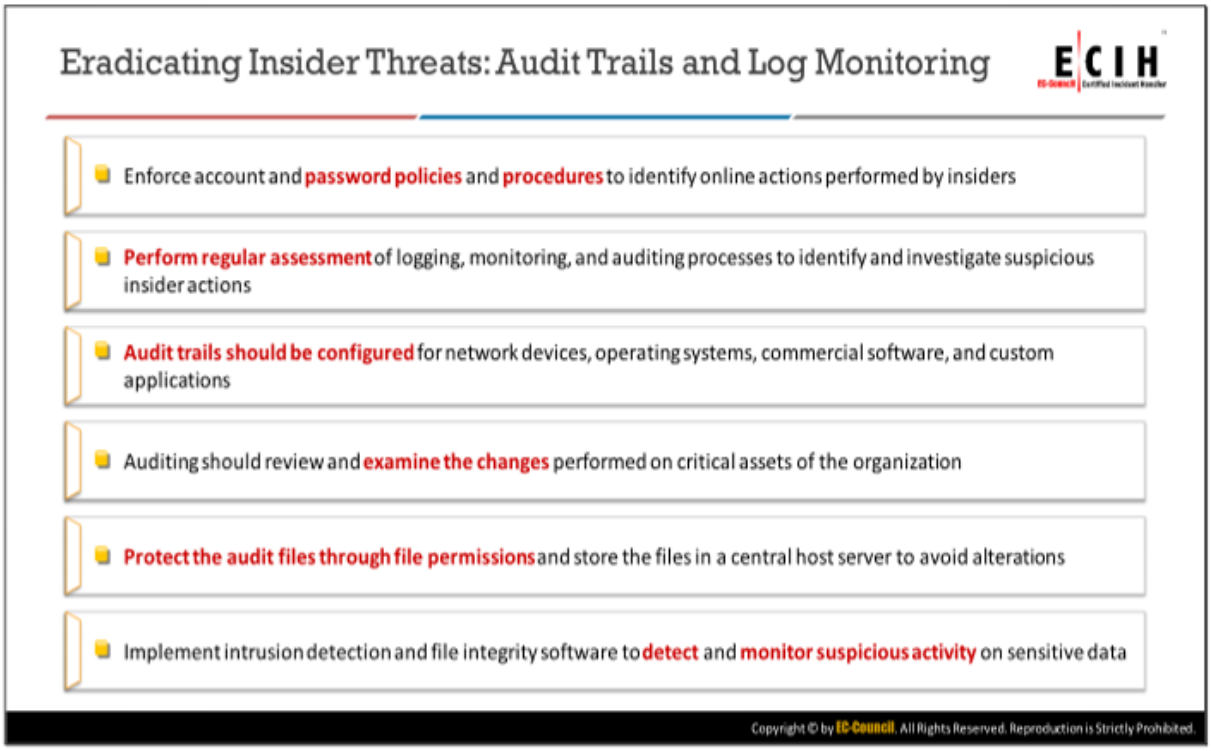


Eradicating Insider Threats: Privileged Users

Privileged user has a high level of access to the overall system. They can change the configuration settings, grant access to other employees as well as read and modify sensitive data. These privileged users can misuse their rights unintentionally or maliciously or attackers can trick them to perform malicious activities.

Incident handlers must consider the following guidelines to eradicate insider attacks by privileged users:

- Implement non-repudiation technique to view all the actions performed by administrators and privileged users.
- Disable the default administrative accounts to ensure accountability.
- Ensure that administrators use unique accounts during the installation process.
- Use encryption methods to prevent administrators and privileged users from accessing backup tapes and sensitive information.
- Monitor the activities of system administrators and privileged users who have permissions to access sensitive information.
- Control over the access to administrators and privileged users.

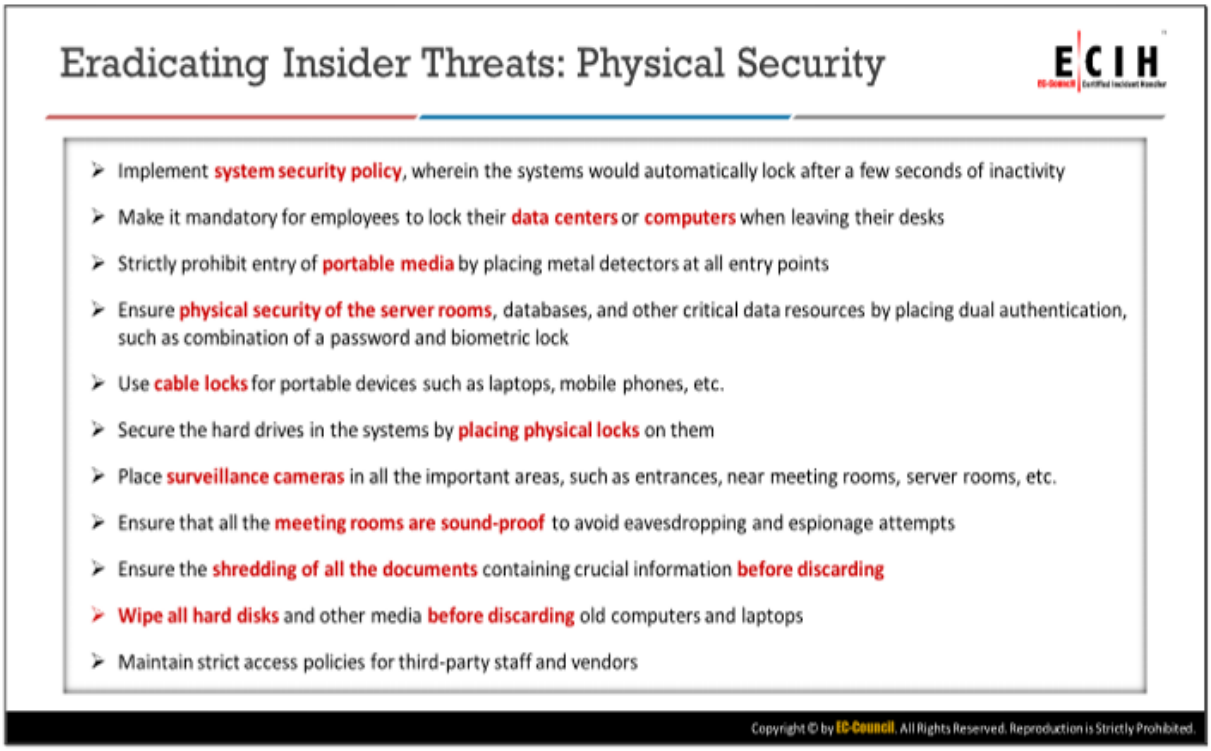


Eradicating Insider Threats: Audit Trails and Log Monitoring

Audit trails and log monitoring is a primary source of information that helps in identifying security gaps and detecting various vulnerabilities that can be exploited to launch attacks. The following are some of the audit trails and log monitoring guidelines that can assist incident responders to eradicate insider threats:

- Enforce account and password policies and procedures to ensure that employees regularly change their passwords by using password management tools and active directory configurations.
- Implement measures to monitor the online activities of insiders. Monitoring controls may include the use of employee monitoring software and configuring gateway firewalls to log web traffic.
- Organizations should properly consider the legal implications before using monitoring controls to avoid any legal liabilities. They should notify the employees that the organization will log all their activities related to the organizational systems and data.
- Perform regular assessment of logging, monitoring, and auditing processes to identify and investigate suspicious insider actions. Organizational logging policies should clearly outline the size of logs and the timeframe for storing logs in order to achieve predetermined business, monitoring, and investigation objectives.
- Configure audit trails for network devices, operating systems, commercial software, and custom applications. Audit trails help organizations to retrieve specific logs from a large storage system.
- Auditing should review and examine the changes performed on the critical assets of any organization.

- Protect audit files through file permissions and store them in a central host server to avoid alterations. Maintain a chain of custody document for log file accessing and handling.
- Implement intrusion detection and file integrity software to detect and monitor suspicious activity on sensitive data.

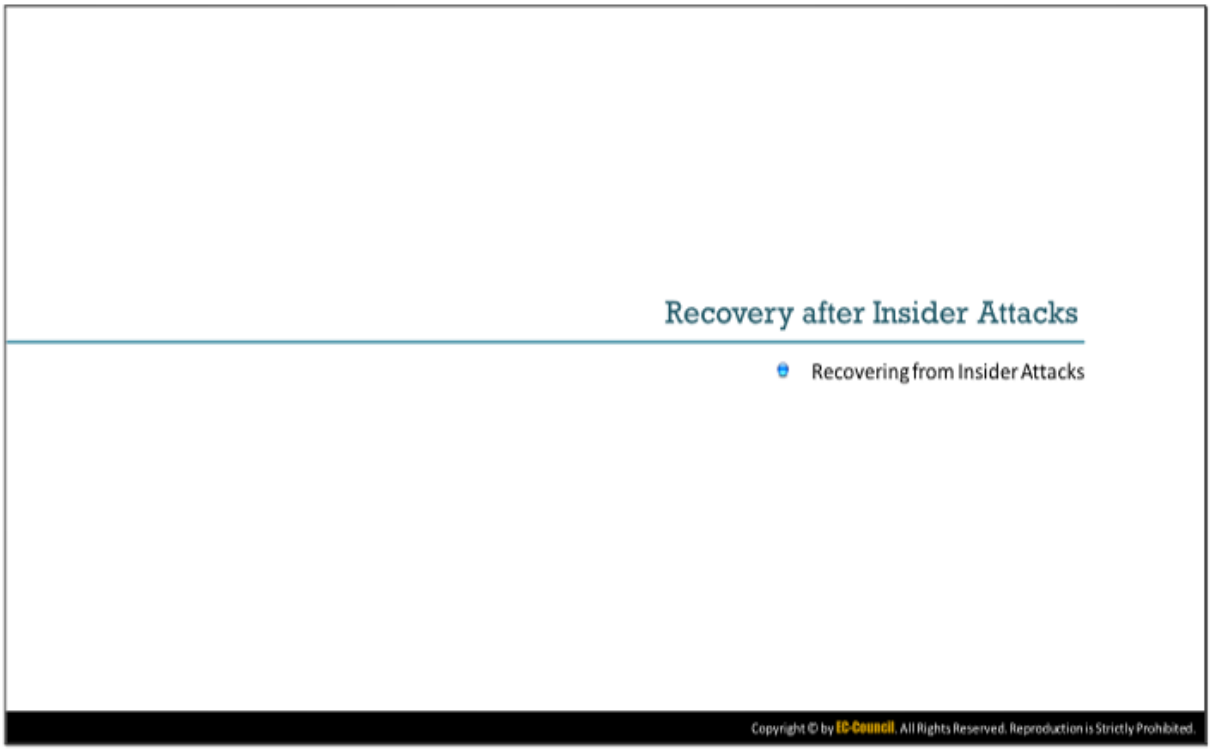


Eradicating Insider Threats: Physical Security

Organizations must implement strict physical security rules and policies to eradicate insider threats. Following are the physical security guidelines for eradicating insider threats:

- Ensure proper logging devices with ID and biometric scanning abilities at all the entry and exit points.
- Deploy security guards to investigate unauthorized entry or to stop employees from taking unauthorized personnel onto the organization's premises.
- Implement system security policy, wherein the systems automatically lock after a certain amount of inactivity.
- Make it mandatory for employees to lock their data centers or computers when leaving their desks.
- Strictly prohibit entry of portable media by placing metal detectors at all entry points.
- Ensure physical security of the server rooms, databases, and other critical data resources by placing dual authentication, such as combination of a password and biometric lock.
- Use cable locks for portable devices like laptops and smart phones.
- Secure the hard drives in the systems by placing physical locks on them.
- Place surveillance cameras at all the important areas, such as entrance, near meeting rooms, and server rooms.
- Ensure that all the meeting rooms are sound proof to avoid eavesdropping and espionage attempts.

- Ensure that all documents which contain crucial information are shredded before discarding
- Wipe all the hard disks and other media before discarding the old computers and laptops.
- Have strict access policies for third-party staff and vendors.



Recovery after Insider Attacks

Cyberattacks that originate from within the organization can have a severe impact on the business, regardless of its size, industry, or location. While prevention from such attacks is key to limiting the impact of cybercrimes on a business, having a proper recovery strategy is mandatory. Therefore, the incident response team must follow the correct right steps after the occurrence of an attack, so that the impact can be managed efficiently. The recovery process must begin immediately.

This section discusses the various steps that must be taken by the incident responders to recover from insider attacks.

Recovering from Insider Attacks

Recovering data which has been sold or exfiltrated is not possible unless the theft is discovered before the insider has had the opportunity to send or sell it. Incident responders must immediately interview the attacker to uncover the location of the data and its copies (if any) and try to trace it. Once the details of the entities who have purchased the data have been discovered, try to issue legal proceedings against both them and the insiders.

To recover from the attack, incident responders should:

- Gather the evidence required for legal proceedings through forensic processes. This evidence will also help the organization file an insurance claim and recover damages.
- If the stolen data impacts user accounts, change the passwords of all the accounts and make two-factor authentication mandatory. If application data is stolen, use copyright to prevent other companies from using it.
- If the attacker has damaged any data or placed malware, the incident responder must remove all traces of malware and recover the data from backups.
- Implement recovery processes and backups to continue business operations after the incident.
- Develop and implement the data backup plan to recover any data affected by the attack.
- Secure backup media and its content from alteration, theft, or destruction. Administrators should ensure that regular backups are performed and tested for integrity and availability.

- Implement separation of duties and configuration management procedures to perform backups on computer systems, networks, and databases.
- Implement a person-to-person rule to secure the backup process and physical media.
- Maintain a chain-of-custody document for accessing and handling backup media.
- Developing a data backup plan requires the investment of time and money, but it is far better than burden of recreating data. The main primary task is to understand what data should be backed up and protected.

  As a part of data backup plan, determine the following:

  - What data should be backed up?
  - Which compression method should be used?
  - How often do backups need to run?
  - What type of backups should be run?
  - What kind of media should be use for backup?
  - Where should backup data be stored to ensure security?

Best Practices Against Insider Threats

The incident response team must implement and adopt appropriate best practices in order to secure the organizational network from insider attacks. These practices eliminate the possibility of cyberattacks originating from malicious insiders, thus improving the security infrastructure of the organization.

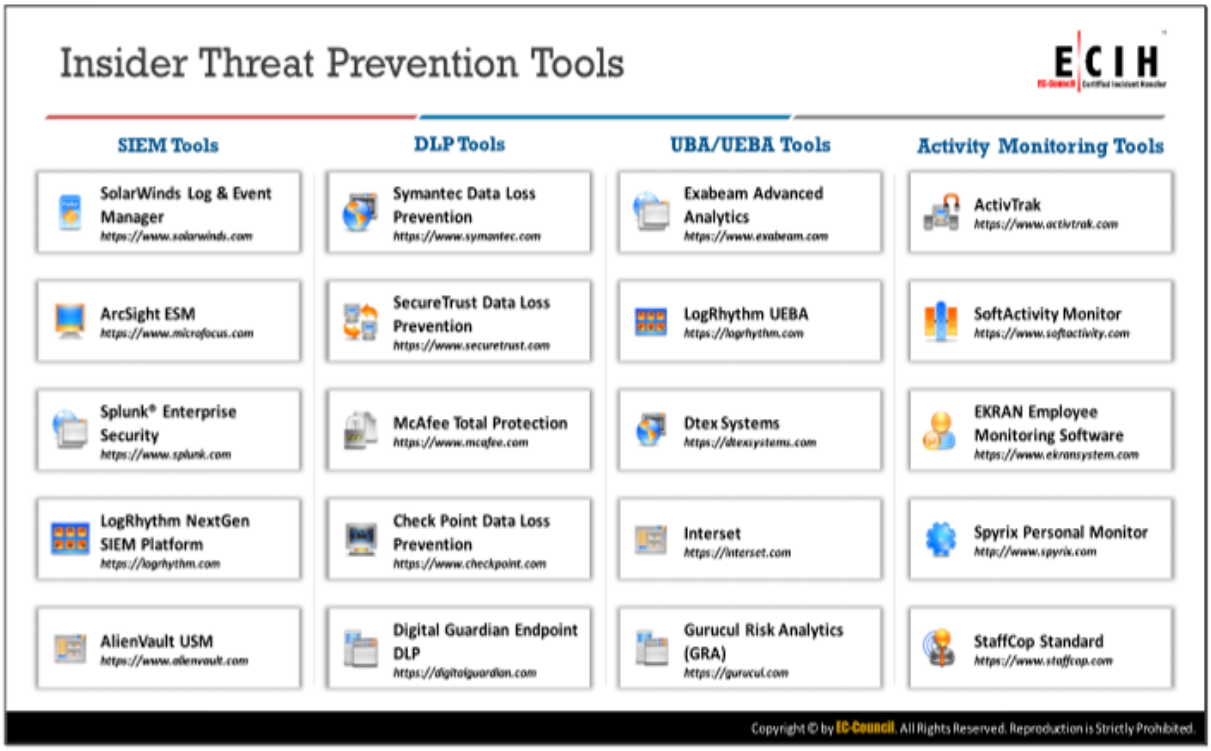
This section discusses various best practices for securing the organization from insider threats.

Best Practices Against Insider Threat

The following are the best practices recommended to avoid insider threats:

- Monitor employee behaviors and employee computer systems.
- Implement secure backup and disaster recovery processes for business continuity.
- Disable remote access and screen sharing activities for all users.

- Anticipate and manage the negative issues that may occur at the workplace.
- Make sure that users are not allotted unnecessary account privileges.
- Implement system change controls and consider insider threats in the system/software development life cycle.
- Disable the use of USB drives and other portable storage media on the network, systems, and all other devices to protect physical extraction of data.
- Enforce a security policy which addresses all your concerns.
- Develop an insider incident response plan.
- Do not ignore physical security check.
- Background verification of new employees is mandatory and must include a thorough check for legal issues.
- Shred documents prior to disposal to destroy sensitive material.
- Secure the dumpsters used by the organization with no trespassing signs posted.
- Provide regular training to employees on security awareness.
- Lock the confidential rooms such as phone closets, server rooms, and wire closets to prevent unauthorized access
- Place laptop locks to prevent laptop theft or tampering.
- Never leave business details on voice mail or email broadcast messages.
- Disable users from installing unauthorized software or accessing malicious websites using the corporate network.
- Prevent hardware tampering by locking computer cabinets.
- Ensure that hard drives used in company computers are wiped and destroyed before they are discarded.
- Implement a periodic organization-wide risk assessment program.
- Enforce strict account management and password policies.
- Monitor egress traffic in order to detect unauthorized use of encryption, indicating an attempt to remove data from network.
- Develop network segmentation and network segregation techniques where critical data is stored.



Insider Threat Prevention Tools

Traditional security controls such as passwords, firewalls, and intrusion detection systems are not sufficient prevent attacks which originate internally as many employees already have access to the organization's critical assets. Therefore, to protect critical organizational assets from insider threats, organizations need to deploy different levels of security using controls such as SIEM solutions, DLP tools, UBA/UEBA tools, and activity monitoring tools. These tools log, monitor, detect, alert, analyze, and prevent various malicious activities originating from within the organization.

- **SIEM Solutions**

  Security Incident and Event Management (SIEM) solutions provide the ability to build custom queries, generate alerts, retrieve data from multiple data sources, and enhance the potential analytical capability to prevent, detect, and respond to various insider threats.

  Listed below are some of the important SIEM solutions:

  - SolarWinds Log & Event Manager (*https://www.solarwinds.com*)
  - ArcSight ESM (*https://www.microfocus.com*)
  - Splunk® Enterprise Security (*https://www.splunk.com*)
  - LogRhythm NextGen SIEM Platform (*https://logrhythm.com*)
  - AlienVault USM (*https://www.alienvault.com*)
  - RSA NetWitness (*https://www.rsa.com*)
  - IBM QRadar SIEM (*https://www.ibm.com*)

- McAfee Enterprise Security Manager (*https://www.mcafee.com*)
- EventLog Analyzer (*https://www.manageengine.com*)

- **Data Loss Prevention (DLP) Tools**

  Data loss prevention (DLP) tools scan network traffic to find the exfiltration of sensitive data and alert administrators. Organizations must use DLP tools to ensure detection of loss or the misuse or access of sensitive data by unauthorized personnel. DLP tools can classify confidential and business critical data, as well as identify violation of policies outlined by the organization. Use DLP alerts to protect and prevent users from sharing data accidentally or maliciously.

  Listed below are some of the important DLP tools:

  - Symantec Data Loss Prevention (*https://www.symantec.com*)
  - SecureTrust Data Loss Prevention (*https://www.securetrust.com*)
  - McAfee Total Protection (*https://www.mcafee.com*)
  - Check Point Data Loss Prevention (*https://www.checkpoint.com*)
  - Digital Guardian Endpoint DLP (*https://digitalguardian.com*)
  - Clearswift's Adaptive DLP (*https://www.clearswift.com*)
  - Trend Micro™ Integrated DLP (*https://www.trendmicro.com*)
  - Sophos SafeGuard Enterprise Encryption (*https://www.sophos.com*)
  - WatchGuard Data Loss Prevention (DLP) (*https://www.watchguard.com*)

- **UBA/UEBA Tools**

  User Behavior Analytics (UBA)/User and Entity Behavior (UEBA) Tools collect user activity details from multiple sources and use artificial intelligence and machine learning algorithms to perform user behavior analysis to prevent and detect insider threats before the fraud is perpetrated.

  Listed below are some of the important UBA/UEBA tools:

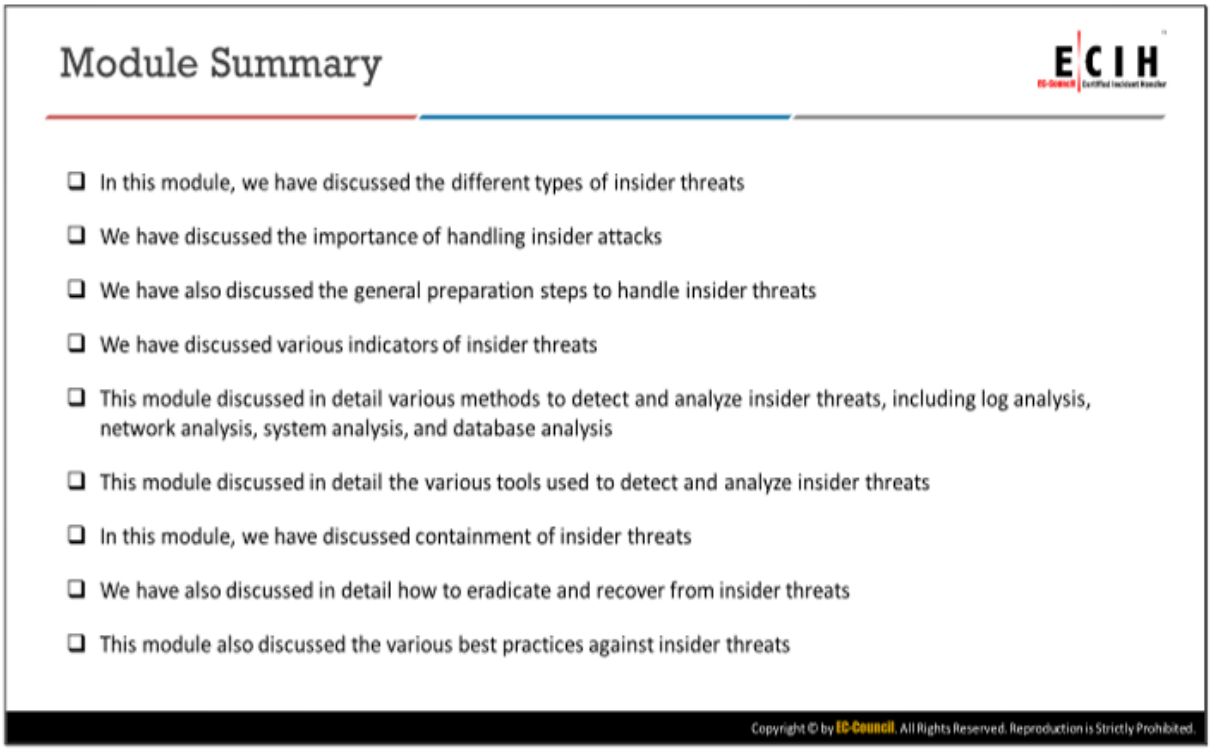
  - Exabeam Advanced Analytics (*https://www.exabeam.com*)
  - LogRhythm UEBA (*https://logrhythm.com*)
  - Dtex Systems (*https://dtexsystems.com*)
  - Interset (*https://interset.com*)
  - Gurucul Risk Analytics (GRA) (*https://gurucul.com*)
  - Securonix UEBA (*https://www.securonix.com*)
  - ZoneFox (*https://www.zonefox.com*)

- **Activity Monitoring Tools**

  Activity monitoring tools record all user activity on the organizational networks, systems, and other IT resources. These tools record the user's keystrokes, capture screenshots, monitor internet usage, monitor software usage, and helps in tracking various user activities in the organizational network.

  Listed below are some of the important activity monitoring tools:

  - ActivTrak (*https://www.activtrak.com*)
  - SoftActivity Monitor (*https://www.softactivity.com*)
  - EKRAN Employee Monitoring Software (*https://www.ekransystem.com*)
  - Spyrix Personal Monitor (*http://www.spyrix.com*)
  - StaffCop Standard (*https://www.staffcop.com*)
  - Hubstaff Employee Monitoring Software (*https://hubstaff.com*)
  - iMonitor EAM (*http://www.imonitorsoft.com*)
  - Employee Desktop Live Viewer (*https://www.nucleustechnologies.com*)
  - Veriato Investigator (*https://www.veriato.com*)
  - Personal Inspector (*http://www.spyarsenal.com*)
  - REFOG Personal Monitor (*https://www.refog.com*)
  - Screenshot Monitor (*https://screenshotmonitor.com*)
  - Power Spy (*http://www.ematrixsoft.com*)
  - NetVizor (*https://www.netvizor.net*)
  - SentryPC (*https://www.sentrypc.com*)



Module Summary

In this module, we have discussed the types of insider threats; the importance of handling insider attacks; the general preparation steps to handle insider threats; and various indicators of insider threats. We have discussed in detail various methods, such as log analysis, network analysis, system analysis, and database analysis, to detect and analyze insider threats.

This module discussed various tools that could be used to detect and analyze insider threats. In this module, we have discussed containment and eradication of insider threats. This module also discussed how to recover from insider attacks. This module ended with an overview discussion on best practices against insider threats.

Glossary

A

- **Availability:** Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users.
- **Authenticity:** Authenticity refers to the assurance of genuine and uncorrupted communications, documents, or other data.
- **Advanced Persistent Threat (APT):** Advanced Persistent Threat is an attack that focuses on stealing information from a victim machine without alerting its user.
- **Anti-Forensics:** Anti-forensics, also known as counter forensics, is a set of techniques that attackers or perpetrators use to interfere with, avert, or sidetrack the forensic investigation process.
- **Artifact Wiping:** Artifact Wiping refers to the process of permanently deleting or destroying evidence files using various tools and techniques, such as disk-cleaning utilities file-wiping utilities, and disk degaussing/destruction techniques.
- **Abduction:** Abduction is defined as taking away a person by persuasion, fraud, or open force or violence.
- **Availability Attacks:** Availability attacks aim at obstructing the delivery of wireless services to legitimate users, either by crippling those resources or by denying users access to WLAN resources
- **Access Control:** Access control refers to how web applications grant access to create, update, and delete any record, content, or functions to some privileged users and restrict other users.

B

- **Botnet:** A botnet is a huge network of compromised systems used by attackers to perform denial-of-service attacks.

C

- **Confidentiality:** Confidentiality is the assurance that the designated information is only accessible for those who are authorized to have access.
- **Cloud Computing:** Cloud computing is an on-demand delivery of IT capabilities in which IT infrastructure and applications are provided to subscribers as a metered service over a network.
- **Cyber Terrorists:** Cyber terrorists are individuals with a wide range of skills who are motivated by religious or political beliefs to create a fear of large-scale disruption of computer networks.
- **Control Analysis:** The control analysis is the process of analyzing various security controls implemented by the organization to eradicate or minimize the probability of a threat source exploiting a system vulnerability.
- **Center for Internet Security (CIS):** Center for Internet Security Controls are 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.
- **COBIT:** COBIT is a business framework for IT governance and a management toolset that enables managers to bridge the gap between control requirements, technical issues, and business risks.

- **Cyber Law:** Cyber law, or Internet law, refers to any laws that deal with protecting the Internet and other online communication technologies.
- **Cyber Insurance:** Cyber insurance refers to a contract between the organization and an insurer to protect related individuals from various online threats and risks.
- **Computer Forensics:** Computer forensics refer to a set of methodological procedures and techniques that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal and/or administrative proceeding.
- **Chain of Custody:** Chain of custody is a legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory.
- **Clipboard:** The clipboard is a temporary storage area where the system stores data during copy and paste operations.
- **Cyberstalking:** Cyberstalking is a crime in which attackers harass an individual, group, or organization using emails or IMs (instant messengers).
- **Child Pornography:** Child pornography is a criminal offense where a child or a minor is depicted of engaging in sexually explicit conduct such as photographs, film, video, pictures, or computer-generated images or pictures, whether made or produced by electronic, mechanical, or other means.
- **Child Abduction:** Child abduction is the offense of wrongfully removing or wrongfully retaining, detaining, or concealing a minor.
- **Computer Network:** A computer network is a group of computers linked together for easy sharing of information and resources.
- **Configuration:** Configuration refers to the essential settings that help websites and applications with hardware and software components to produce their required output.
- **Cross-site request forgery (CSRF) Attack:** Cross-site request forgery, also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page.
- **Containment:** Containment is a crucial step in the incident management process that focuses on preventing additional damage.
- **Cloud Computing:** Cloud computing is an on-demand delivery of IT capabilities that provides IT infrastructure and applications to subscribers as metered services over networks.
- **Cloud Consumer:** A cloud consumer is a person or organization that maintains a business relationship with cloud service providers and uses cloud computing services.
- **Cloud Service Provider (CSP):** A cloud provider, also called a cloud service provider, is a person or organization that makes services available to the customers.
- **Cloud Auditor:** A cloud auditor is a party that performs an independent examination of cloud service controls with the intent of expressing an opinion thereon.
- **Corporate Mole:** A corporate mole is an employee who pretends to be a dedicated worker but performs malicious activities secretively.

D

- **Defense in depth:** Defense in depth is a security strategy in which several protection layers are placed throughout an information system.

- **De-Militarized Zone (DMZ):** A DMZ is a small network placed between the organization's private network and an outside public network.
- **Documenting:** Documenting is the process of writing down all the actions the investigators have performed during their investigation.
- **Digital Evidence:** Digital evidence is defined as "any information of probative value that is either stored or transmitted in a digital form." It helps incident responders and investigators find the perpetrator.
- **Disk Degaussing:** Disk degaussing is a process by which a magnetic field is applied to a digital media device, resulting in a device entirely devoid of any previously stored data.
- **Denial-of-Service (DoS) Attack:** Denial-of-Service, or DoS, is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources by its legitimate users.
- **Distributed Denial-of-Service (DDoS) Attack:** A Distributed Denial-of-Service or DDoS attack is a large-scale, coordinated attack on the availability of services on a victim's system or network resources. DDoS attacks are launched indirectly through many compromised computers (botnets) on the internet.
- **Distributed Reflection Denial-of-Service (DRDoS) Attack:** A distributed reflection denial-of-service attack, also known as a "spoofed" attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.

E

- **Espionage:** Espionage involves stealing the proprietary information of any organization and passing it to other organizations with the motive of negatively impacting its reputation or for some financial benefit.
- **Evidence Handling:** Evidence handling, or preservation is an integral part of the evidence-gathering process.
- **Evidence Assessment:** Evidence assessment is the process of relating the obtained evidential data to the incident to understand how the complete incident took place.
- **Encryption:** Encryption is the process of translating data into a secret code so that only authorized personnel can access it.
- **Email Bombing:** Email bombing refers to the process of repeatedly sending an email message to a particular address at a specific victim's site.
- **Email Origin:** Email origin refers to the details about the source used to send the email.
- **Elasticity:** Elasticity refers to the ability of a single cloud to handle the data, accounts, systems, and applications of various organizations.

F

- **Forensic Readiness:** Forensic readiness refers to an organization's ability to make optimal use of digital evidence during a limited period of time and with minimal investigation costs.
- **Forensic Readiness Planning:** Forensic readiness planning refers to a set of processes required to achieve and maintain forensic readiness.
- **Forensic Policy:** Forensic policy is a set of procedures describing the actions an organization must take to preserve and extract forensic evidence during an incident.
- **First Responder:** The term "first responder" refers to the person who is the first to arrive at the crime scene to assess it and alert the management and incidence response teams.

- **Forensic Data Acquisition:** Forensic data acquisition is the process of imaging or collecting information from various media in accordance with certain standards for analyzing its forensic value.
- **Forensic Investigation Report:** A forensic investigation report is a statement of allegations and conclusions drawn from computer forensic investigation.

H

- **Hacktivism:** Hacktivism is when hackers break into government or corporate computer systems as an act of protest
- **Hacktivists:** Hacktivists are individuals who promote a political agenda through hacking, especially by defacing or disabling websites.
- **Honeypot:** A honeypot is a computer system on the internet intended to attract and trap people who attempt unauthorized or illicit utilization of the host system.

I

- **Information Security:** Information security is defined as "a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable."
- **Integrity:** Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose.
- **Information Asset:** An information asset can be defined as a piece of information identified as being important to an organization.
- **Information Security Policy:** Information security policy defines the basic security requirements and rules to be implemented in order to protect and secure an organization's information systems.
- **Insider Attack:** An insider attack is an attack by someone from within an organization who has authorized access to its network and who is aware of the network architecture.
- **Insider Threat:** Insider threat refers to a threat that originates from within the organization; it is typically carried out by a privileged user, disgruntled employee, terminated employee, accident-prone employee, third party, or undertrained staff.
- **Industrial Spies:** Industrial spies are individuals who try to attack companies for commercial purposes.
- **Information Warfare:** The term "Information Warfare," or InfoWar, refers to the use of information and communication technologies (ICT) to take competitive advantages over an opponent.
- **Intelligence-based Warfare:** Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems.
- **Information Security Incident:** Information security incident is a network or host activity that impacts the security of information stored on network devices or systems with respect to confidentiality, integrity, or availability.
- **Intangible Cost:** Intangible cost refers to the expenditures that the organization cannot calculate directly or value accurately.
- **Incident Management:** Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore normal service operations as quickly as possible and prevent the future reoccurrence of the incident.

- **Incident Handling and Response (IH&R):** Incident handling and response is the process of taking organized and careful steps when reacting to a security incident or cyberattack.
- **Impact Analysis:** The impact analysis involves estimating the adverse impact caused by the exploitation of a vulnerability by a threat source.
- **Incident Response Automation:** Incident response automation is the process of superseding manual IR actions with automatic IR actions using machines and tools.
- **Incident Response Orchestration:** Incident response orchestration is an approach for responding to security incidents that occur in an organization.
- **Incident Handling and Response (IH&R) Team:** An IH&R team is a group of technically skilled people capable of carrying out various functions such as threat intelligence, evidence analysis, and investigating users.
- **Incident Impact Assessment:** Incident impact assessment refers to the process of determining all types of losses that have occurred because of an incident.
- **Incident Response:** Incident response is the process of developing a strategy to address the occurrence of any security breach in a system or network.
- **Inappropriate Usage:** Inappropriate usage refers to incidents in which a user violates an organization's acceptable computing use policies.
- **Injection Flaws:** Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query.
- **Input Validation Flaws:** Input validation flaws refer to a web application vulnerability where the input from a client is not validated before being processed by the web application and backend servers.
- **Insider:** An insider is any employee (trusted person) that has access to the critical assets of an organization.
- **Individual Profiling:** Individual profiling refers to observing the behavior of an individual when alone, whereas group profiling is observing a person's behavior in a group.

L

- **Likelihood Analysis:** Likelihood analysis is the calculation of the probability that a threat source will exploit an existing system vulnerability.
- **Live/Volatile Data Acquisition:** This is the process of acquiring volatile data from a working computer (either locked or in sleep mode) that is already powered on.
- **Logic Error:** A logic error is a coding flaw that causes performance issues in the application or website, resulting in undesired or unwanted output.
- **Local File Injection (LFI):** Local File Injection is an attack in which an attacker exploits vulnerable inclusion procedures implemented in a web application.

M

- **Malicious Code Attack:** A malicious code attack is an attack generated by malicious programs such as viruses, Trojan horses, worms, etc.
- **Memory Residents:** Memory residents refer to programs that always remain in the internal memory and for which the operating system has no permission to swap out to external storage.
- **Metadata:** Metadata refers to information that stores details of data.

N

- **Non-repudiation:** Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message
- **Network:** A network is a collection of computers and other hardware connected by communication channels to share resources and information.
- **NIST Risk Management Framework:** NIST Risk Management Framework is a structured and continuous process that integrates information security and risk management activities into the system development lifecycle (SDLC).
- **Nonvolatile Evidence:** Nonvolatile evidence refers to permanent data that is stored on secondary storage devices, such as hard disks and memory cards.

O

- **Organized Hackers:** Organized hackers are professional hackers who aim to attack a system for profit.
- **Offensive Information Warfare:** This refers to information warfare that involves attacks against the ICT assets of an opponent.
- **Orchestration:** Orchestration refers to the process of combining humans, processes, and technologies to gain better results.

P

- **Phishing:** Phishing is the practice of sending illegitimate e-mail that falsely claims to be from a legitimate site in an attempt to acquire a user's personal or account information.
- **Pre-assessment Phase:** The pre-assessment phase refers to the preparatory phase for assessment. It includes defining policies and standards, defining the scope of the assessment, designing appropriate information protection procedures, and identifying and prioritizing critical assets to create a good baseline for vulnerability management.
- **Post Assessment Phase:** Post assessment phase is also known as the recommendation phase, which is performed after an assessment.
- **Payment Card Industry Data Security Standard (PCI DSS):** The Payment Card Industry Data Security Standard is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
- **Policy:** A policy is a set of guidelines used to achieve the goals and objectives of the incident response initiative set by an IH&R plan.
- **Password:** A password refers to any combination of words, letters, numbers, and special characters used for security processes, such as user authentication, or to grant user access to a resource.
- **Packer:** A packer is a program used to compress or encrypt executable programs.
- **Pharming:** Pharming, also known as domain spoofing, is an advanced form of phishing in which an attacker redirects the connection between an IP address and its target server.
- **Packet Sniffing:** Packet sniffing is the process of monitoring and capturing all data packets passing through a given network by using a software application or a hardware device.
- **Permanent DoS (PDoS) Attacks:** Permanent DoS attacks, also known as phlashing, purely target hardware and cause irreversible damage.
- **Packet Traceback:** Packet Traceback refers to the process of tracing back attack traffic.

- **Private Cloud:** A private cloud, also known as an internal or corporate cloud, is cloud infrastructure that a single organization solely operates.
- **Privileged Users:** Privileged users are persons with unlimited permissions in the systems, such as user endpoints, organization data, cloud services, customer data, etc.

R

- **Ransomware:** Ransomware is a type of malware that restricts access to a computer system's files and folders and demands an online ransom payment to the malware creator(s) in order to remove the restrictions.
- **Recreational Hackers:** Recreational hackers are hackers who hack to learn and explore. This is done by exploiting or manipulating technology.
- **Remediation:** Remediation refers to steps taken to mitigate found vulnerabilities, such as evaluating the vulnerabilities, locating risks, and designing responses for the vulnerabilities, etc.
- **Risk:** Risk refers to a situation involving exposure to danger or the possibility that something unpleasant or unwelcome will occur.
- **Risk Management:** Risk management refers to a set of policies and procedures to identify, assess, prioritize, minimize, and control risks.
- **Risk Assessment:** Risk assessment refers to the identification of risks, estimation of impact, and determination of sources in the process of recommending proper mitigation measures.
- **Risk Mitigation:** Risk mitigation is a strategic approach to preparing to handle risk and reduce its impact on an organization.
- **Risk Determination:** Risk determination is a crucial task in a risk assessment effort. It is a complex process that depends upon various tangible and intangible factors.
- **Risk Level:** Risk level is an assessment of the resulted impact on a network.
- **Risk Matrix:** A risk matrix scales the risk occurrence/likelihood probability along with its consequences or impact.
- **Risk Avoidance:** Risk avoidance refers to preventing risk by curbing the cause and/or consequence of a risk.
- **Risk Management Plan:** A risk management plan is defined as a process that is designed to identify, eliminate, or mitigate risks that can cause damage to an organizational network and systems.
- **Recovery:** Recovery is a significant step to restore whatever services or materials might have been affected during an incident.
- **Relevance:** The term "relevance" refers to the connection between the digital evidence and the fact to be proven.
- **Reconnaissance:** Reconnaissance refers to gathering information. In reconnaissance attacks, attackers make an attempt to gather the target network's crucial information and perform the attacks.
- **Remote File Injection (RFI):** Remote File Injection is a technique that targets underlying web application vulnerabilities and launches attacks from a remote server.

S

- **Script Kiddies:** Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software that has been developed by real hackers.

- **State-Sponsored Hackers:** State-sponsored hackers are individuals employed by a government to penetrate the information systems of other governments to gain top-secret information from and cause damage.
- **Suicide Hackers:** Suicide hackers are individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment.
- **Signs of an Incident:** Signs of an incident refer to the alerts, warnings, reports, complaints, and issues that represent an ongoing or completed security attack on an organization or its resources.
- **Static Data:** Static data refer to nonvolatile data that do not change state after the system shuts down.
- **Static Data Acquisition:** Static data acquisition refers to the process of extracting and gathering unaltered data from storage media.
- **Steganography:** Steganography is the technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of the data.
- **Spam:** Spam refers to unsolicited or undesired emails that are sometimes used to distribute malicious links and attachments, cause network congestion, perform phishing and financial fraud, and other bad behavior.
- **Skimming:** Skimming refers to stealing credit/debit card numbers by using special storage devices called skimmers or wedges when processing the card.
- **Social Engineering:** Social engineering is the art of convincing people to reveal confidential information.
- **Sessionization:** Sessionization refers to a process in data processing that is used to analyze user activities within a certain time period.
- **Structured Query Language (SQL):** Structured Query Language is a programming language meant for database management systems.

T

- **Threat:** A threat refers to an undesired event that attempts to access, exfiltrate, manipulate, or damage the integrity, confidentiality, security, and availability of an organizational resource.
- **Threat Actor:** A threat actor or malicious actor is a person or entity responsible for an incident or who has the potential to impact the security of an organization's network.
- **Tangible Cost:** Tangible cost refers to an organization's direct expenditure due to an incident.
- **Threat Assessment:** Threat assessment is the process of examining, filtering, transforming, and modeling of acquired threat data to extract threat intelligence.
- **Threat Target and Assets:** Threat target and assets are the organizational resources that are attacked by a threat actor in order to gain complete control of or steal information to launch further attacks on an organization.
- **Threat Intelligence:** Threat intelligence, usually known as Cyber Threat Intelligence (CTI), is the collection and analysis of information about threats and adversaries and the act of drawing patterns that provide an ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyberattacks.
- **Threat Contextualization:** Threat contextualization refers to the process of assessing threats and their impacts in various conditions.
- **Threat Correlation:** Threat correlation helps organizations to monitor, detect, and escalate various evolving threats to organizational networks.

- **Threat Attribution:** Threat attribution is the process of identifying and attributing the actors behind an attack, their goals and motives, and any sponsors

U

- **Unauthorized Access:** Unauthorized access refers to obtaining illegal access to systems or network resources to steal or damage information.

V

- **Vulnerability:** Vulnerability is the existence of weakness in design or an implementation error that, when exploited, leads to an unexpected and undesirable event that compromises the security of the system.
- **Vulnerability Research:** Vulnerability research is the process of discovering vulnerabilities and design flaws that open networks, operating systems, and applications to attack or misuse.
- **Vulnerability Assessment:** Vulnerability assessment is the examination of the ability of a system or application, including current security procedures and controls, to withstand assault.
- **Vulnerability Management Life Cycle:** Vulnerability management life cycle is an important process that helps in finding and remediating security weaknesses before they are exploited.
- **Vulnerability Assessment Phase:** Vulnerability assessment phase refers to identifying vulnerabilities in an organization's infrastructure, including the operating system, web applications, web server, and other technologies.
- **Volatile Evidence:** Volatile evidence refers to temporary information on a digital device that requires a constant power supply. The volatile evidence is deleted if the power supply is interrupted.
- **Volatile Information:** Volatile Information refers to data stored in the registries, cache, and RAM of digital devices.
- **Virtualization:** Virtualization refers to the platform in a cloud that allows the clients to install the virtual machines, systems, and servers required to run applications.

W

- **Weight of the Digital Evidence:** The term "weight of the digital evidence" refers to how much the digital evidence changes the probability of the fact in question.
- **Wireless Network:** A wireless network is an unbounded data communication system that uses radio frequency technology to communicate with devices and obtain data.
- **Wireless Network Security Incident:** A wireless network security incident refers to a security event that happens due to accidental or intentional activities in a wireless network.
- **Web Applications:** Web applications are software programs that run on web browsers and act as an interface between users and web servers through web pages.
- **Web Application Firewall (WAF):** A Web Application Firewall consists of either software or hardware that defines a set of rules for HTTP conversation to filter out malicious data.
- **Web Application Fuzz testing:** Web Application Fuzz testing (fuzzing) is a black box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications.

This page is intentionally left blank.

References

Module 01: Introduction to Incident Handling and Response

1. Information Asset, from http://www.yourwindow.to/information-security/gl_informationasset.htm.
2. What is an Information Asset?, from http://informationassetdevelopment.com/what.html.
3. Business Assets, from http://informationassetdevelopment.com/what.html.
4. User account policy, from https://en.wikipedia.org/wiki/User_account_policy.
5. Remote access policy, from https://en.wikipedia.org/wiki/Remote_access_policy.
6. Information security policy, from https://en.wikipedia.org/wiki/Information_protection_policy.
7. Vangie Beal, Insider Attack, from https://www.webopedia.com/TERM/I/insider_attack.html.
8. Joe Jenkins, (2002), Internet Security and Your Business - Knowing the Risks, from https://www.symantec.com/connect/articles/internet-security-and-your-business-knowing-risks.
9. Critical Infrastructure - Threats and Terrorism, from https://fas.org/irp/threat/terrorism/sup2.pdf.
10. (2015), Damage control: The Cost of Security Breaches its Security Risks Special Report Series, from https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf.
11. Cyber Security for Business: Impact of Cyber Attack on your Business, from https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business.
12. (2015), How Data Breaches Can Affect Brand and Reputation, from https://blog.vitrium.com/document-security-protection-drm-blog/how-data-breaches-can-affect-brand-and-reputation.
13. Information Warfare / Infowar, from http://www.yourwindow.to/information-security/gl_informationwarfareinfowar.htm.
14. Types of Incidents, from http://www.bu.edu/tech/services/security/cyber-security/sensitive-data/reporting/types.
15. Computer Forensics and Incident Response Essentials, from http://media.wiley.com/product_data/excerpt/67/07645263/0764526367.pdf.
16. Adam Abresch, (2017), Incident Response Plan: Detection, from http://blog.sbbinsure.com/cyber-risk-blog/incident-response-plan-detection.
17. (2016), Incident Handling Management, from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/incident_handling_management-handbook.
18. (2008), Incident Response Management Overview, from https://sc.edu/about/offices_and_divisions/division_of_information_technology/security/docs/irmanagement.pdf.
19. (2011), Good Practice Guide for Incident Management, from http://www.ifap.ru/pr/2011/n110121a.pdf.
20. Margaret Rouse, Incident Response, from https://searchsecurity.techtarget.com/definition/incident-response.
21. Ramesh Warrier, (2014), 5 Advantages of an Incident Readiness Program, from https://www.ebrp.net/5-advantages-of-an-incident-readiness-program.

22. (2017), How Your Company Benefits from an Incident Management System, from https://www.entry.com/how-your-company-benefits-from-an-incident-management-system.
23. Gaye Connell, (2016), 5 Benefits of Having a Proactive Incident Response Plan, from https://www.valasecure.com/blog/5-benefits-of-having-a-proactive-incident-response-plan.
24. Glossary of Vulnerability Testing Terminology, from https://www.ee.oulu.fi/research/ouspg/Glossary/https://www.ee.oulu.fi/research/ouspg/Glossary.
25. Thomas R. Peltier, Justin Peltier, and John A. Blackley, (2003), Managing A Network Vulnerability Assessment, from https://www.taylorfrancis.com/books/9780203503041.
26. (2011), What is a vulnerability assessment, from http://resecure.me/pdf/17542.pdf.
27. Marcelo Silva, (2012), Vulnerability Assessment, from https://www.slideshare.net/CelloLtd/info-security-vulnerability-assessment.
28. How System Configuration Files are Secured, from https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-3_N5-5/SysAdmin_ASR5500/21-3-ASR5500_SysAdmin/21-3-ASR5500_SysAdmin_chapter_0100000.pdfs.
29. Kevin Beaver, Know Your Network Infrastructure Vulnerabilities to Avoid Hacks, from https://www.dummies.com/programming/networking/know-your-network-infrastructure-vulnerabilities-to-avoid-hacks.
30. Dimitar Kostadinov, (2014), Cyber Threat Analysis, from https://resources.infosecinstitute.com/cyber-threat-analysis/#gref.
31. What is cyber threat analysis?, from https://www.quora.com/What-is-cyber-threat-analysis.
32. Nick Lewis, (2011), How to implement an enterprise threat assessment methodology, from https://searchsecurity.techtarget.com/tip/How-to-implement-an-enterprise-threat-assessment-methodology.
33. Charles P. Pfleeger, Jonathan Margulies, and Shari Lawrence Pfleeger, (2015), Introduction to Security in Computing, 5th Edition, from http://www.informit.com/articles/article.aspx?p=2301451&seqNum=2.
34. (2018), Threat Risk Modeling, from https://www.owasp.org/index.php/Threat_Risk_Modeling.
35. S Vidalis and A Blyth, (2002), Understanding and Developing a Threat Assessment Model, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.6557&rep=rep1&type=pdf.
36. (2019), Cyber Threat Intelligence, from https://en.wikipedia.org/wiki/Cyber_threat_intelligence.
37. Robert M. Lee, (2014), Cyber Threat Intelligence, from https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence.
38. (2017), Cyber Threat Intelligence - Moving cyber security to the heart of our business, from https://cdn2.hubspot.net/hubfs/407136/PDFs/KPMG/KPMG_CyberThreatIntelligence_brochure.pdf.
39. (2014), Threat Intelligence: What Is IT, and How Can it Protect You from Today's Advanced Cyber Attacks, from https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf.
40. (2016), What Is Threat Intelligence? Definition and Examples, from https://www.recordedfuture.com/threat-intelligence-definition.
41. Wang Wei, (2015), What is Threat Intelligence and How It Helps to Identify Security Threats, from https://thehackernews.com/2015/11/what-is-cyber-threat-intelligence.html.
42. (2014), CANSO Cyber Security and Risk Assessment Guide, from https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf.

43. Steve King, (2016), Cyber Threat Intelligence: Context is King, from https://www.netswitch.net/cyberthreat-intelligence-context-is-king.

44. (2017), Threat intelligence sharing challenges: Understand the context of cyber events, from https://www.helpnetsecurity.com/2017/04/07/threat-intelligence-sharing-challenges.

45. Niranjan Mayya, (2016), Contextualization in Security Analytics, from https://www.linkedin.com/pulse/contextualization-security-analytics-niranjan-mayya.

46. (2018), Contextualization, from https://en.wikipedia.org/wiki/Contextualization_(computer_science).

47. Phil Hollows, (2002), Security Threat Correlation: The Next Battlefield, from https://www.esecurityplanet.com/views/article.php/1501001/Security-Threat-Correlation-The-Next-Battlefield.htm.

48. David LeBlanc, Kevin Lam, and Ben Smith, (2004), Assessing Network Security, from https://www.oreilly.com/library/view/assessing-network-security/0735620334.

49. (2014), Risk assessment A brief guide to controlling risks in the workplace, from http://www.hse.gov.uk/pubns/indg163.pdf.

50. Margaret Rouse, Risk Analysis, from https://searchsecurity.techtarget.com/definition/risk-analysis.

51. Introduction to Risk Analysis, from http://www.security-risk-analysis.com/introduction.htm.

52. Gary Stoneburner, Alice Oguen, and Alexis Feringa, (2002), Risk Management Guide for Information Technology Systems from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf.

53. (2012), Guide for Conducting Risk Assessments, from http://www.documentcloud.org/documents/4064145-nistspecialpublication800-30r1.html.

54. Martin, (2017), How to Perform a Business Impact Analysis, from https://www.cleverism.com/business-impact-analysis.

55. (2017), Conduct a business impact analysis, from https://www.business.qld.gov.au/running-business/protecting-business/risk-management/preparing-plan/impact-analysis.

56. Methodology - Business Impact Methodology (BIA) and Risk Assessment (RA, from https://www.coralesecure.com/images/files/Methodology-Business-Impact-Analysis-and-Risk-Assessment.pdf.

57. Margaret Rouse, (2015), Business Impact Analysis (BIA), from https://searchstorage.techtarget.com/definition/business-impact-analysis.

58. (2007), Business Impact Analysis, from http://cdn.ttgtmedia.com/searchSecurityChannel/downloads/443_Disaster_04_(2).pdf.

59. (2017), Analyze and Evaluate the Impact of Risks, from https://www.business.qld.gov.au/running-business/protecting-business/risk-management/preparing-plan/analyse.

60. Laura Lynn Ray, (2017), Incident Response Plan Training Classes Prepare Staff for a Dangerous Situation, from https://www.linkedin.com/pulse/incident-response-plan-training-classes-prepare-staff-laura-lynn-ray.

61. Incident Response Plan, from https://www.doa.la.gov/OTS/InformationSecurity/ISP-IncidentResponsePlan-v.1.0-Clean.pdf.

62. Emily J. Stebbins Wheelock and Al Turgeon, (2018), Guide to Risk Assessment and Response, from https://www.uvm.edu/sites/default/files/UVM-Risk-Management-and Safety/Guide_to_Risk_Opportunity_Assessment_Response.pdf.

63. Jim Meyer, (2013), Risk Assessment and Incident Response, from http://coordinatedresponse.com/risk-assessment-and-incident-response.

64. David Hill, (2018), Information Security Incident Response Policy, from https://www.liverpool.ac.uk/media/livacuk/computingservices/regulations/information-security-incident-response-policy.pdf.

65. (2014), Reporting risk, from https://www.accaglobal.com/content/dam/acca/global/PDF-technical/financial-reporting/pol-afb-rr.pdf.

66. (2018), Risk Report, from https://www.tuigroup.com/en-en/investors/corporate-governance/risk-report.

67. (2017), Treating risks, from https://www.business.qld.gov.au/starting-business/protect-business/managing-risk/treating.

68. Risk Treatment, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment.

69. Stephen Watts, (2017), IT Security Vulnerability vs Threat vs Risk: What's the Difference?, from https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference.

70. (2015), Plan of Action and Milestones Process Guide, from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_6-2_Plan_of_Action_and_Milestones_Process_Guide.pdf.

71. (2017), 7 Tips to Reduce Risks of Data Breaches, from https://www.helpnetsecurity.com/2017/11/02/reduce-security-risk.

72. (2017), Review and update your risk management plan, from https://www.business.qld.gov.au/running-business/protecting-business/risk-management/preparing-plan/review-update.

73. Risk Management Process, from https://pm4id.org/chapter/11-2-risk-management-process.

74. NIST Risk Management Framework, from https://csrc.nist.gov.

75. Julia Kisielius, (2017), Incident Response Orchestration: What Is It and How Can It Help?, from https://www.alienvault.com/blogs/security-essentials/incident-response-orchestration-what-is-it-and-how-can-it-help.

76. Allen Rogers, (2017), What is Incident Response Orchestration?, from https://www.resilientsystems.com/cyber-resilience-knowledge-center/incident-response-blog/incident-response-orchestration.

77. Incident Response Orchestration, from https://www.opsgenie.com/incident-response-orchestrationhttps://www.opsgenie.com/incident-response-orchestration.

78. Tom Brennan, Top 10 Considerations for Incident Response, from https://www.owasp.org/images/b/bd/IR_Top_10_Considerations_-_Slides-v2.pdf.

79. (2010), Good Practice Guide for Incident Management, from https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

80. (2015), Good Practice Guide Forensic Readiness, from https://www.ncsc.gov.uk/content/files/guidance_files/GPG%2018%20-%20Forensic%20Readiness%20-%20Issue%201.2%20-%20Oct%2015%20-%20NCSC%20Web.pdf.

81. ISO/IEC 27000 Family - Information Security Management Systems, from https://www.iso.org/isoiec-27001-information-security.html.

82. ISO/IEC 27001:2013, from https://www.iso.org.

83. ISO/IEC 27002, from https://www.iso.org.

84. (2016), ISO/IEC 27035-1:2016, from https://www.iso.org/standard/60803.html.

85. (2016), ISO/IEC 27035-2:2016, from https://www.iso.org/standard/62071.html.

86. Payment Card Industry Data Security Standard (PCI DSS), from https://www.pcisecuritystandards.org.
87. Federal Information Processing Standards (FIPS) 200, from https://csrc.nist.gov.
88. (2018), NIST Special Publication 800-series General Information, from https://www.nist.gov/itl/nist-special-publication-800-series-general-information.
89. (2018), NIST Special Publication 800-series, from https://csrc.nist.gov/publications/sp800.
90. (2016), The Standard of Good Practice for Information Security 2016, from https://www.securityforum.org/uploads/2016/07/SoGP-2016-Exec-Summary-FINAL-260716.pdf.
91. Critical Infrastructure Protection Committee (CIPC), from https://www.nerc.com/comm/CIPC/Pages/default.aspx.
92. (2004), Cyber Security Definitions, from https://www.nerc.com/pa/Stand/Cyber%20Security%20Permanent/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf.
93. Chip Moore, (2015), NERC CIP Overview, from http://caper-usa.com/wp-content/uploads/2017/04/CIP-Overview.pdf.
94. Margaret Rouse, (2012), NERC CIP (Critical Infrastructure Protection), from https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection.
95. NERC Critical Infrastructure Protection Standards, from ftp://ftp.mrynet.com/operatingsystems/HP-MPE/docs.hp.com/en/541358-002/apas02.html.
96. Barbara Y. Fraser, (1997), RFC 2196, from https://tools.ietf.org/html/rfc2196.
97. (2015), Site Security Handbook, from https://en.wikipedia.org/wiki/Site_Security_Handbook.
98. (2019), CSIRT (RFC), from http://www.csirt.org/rfc_csirt/index.html.
99. CIS controls, from https://learn.cisecurity.org/20-controls-download.
100. CIS Controls, from https://www.cisecurity.org/controls.
101. (2018), COBIT, from https://en.wikipedia.org/wiki/COBIT.
102. Sarah K. White, (2019), What is COBIT? A framework for alignment and governance, from https://www.cio.com/article/3243684/methodology-frameworks/what-is-cobit-a-framework-for-alignment-and-governance.html.
103. (2018), Updated NIST Guide is a How-To for Dealing with Computer Security Incidents, from https://www.nist.gov/news-events/news/2012/08/updated-nist-guide-how-dealing-computer-security-incidents.
104. Vanessa Henri, (2018), Incident Response Planning in a Nutshell, from https://www.hitachi-systems-security.com/blog/data-breach-notification-laws.
105. Sarbanes Oxley Act (SOX), from https://www.sec.gov.
106. Health Information Privacy, from https://www.hhs.gov/hipaa/index.html.
107. Federal Information Security Management Act (FISMA), from https://csrc.nist.gov.
108. Gramm-Leach-Bliley Act (GLBA), from https://www.ftc.gov.
109. Data Protection Act 2018, from http://www.legislation.gov.uk.
110. General Data Protection Regulation (GDPR), from https://www.eugdpr.org.
111. The Digital Millennium Copyright Act (DMCA), from https://www.copyright.gov.
112. Section 107 of the Copyright Law mentions the doctrine of “fair use”, from https://www.copyright.gov.

113. Online Copyright Infringement Liability Limitation Act, from https://www.copyright.gov.
114. The Lanham (Trademark) Act (15 USC §§ 1051 - 1127), from https://www.uspto.gov.
115. The Electronic Communications Privacy Act, from https://www.fas.org.
116. Foreign Intelligence Surveillance Act, from https://www.fas.org.
117. Protect America Act of 2007, from https://www.justice.gov.
118. Privacy Act of 1974, from https://www.justice.gov.
119. National Information Infrastructure Protection Act of 1996, from https://www.nrotc.navy.mil.
120. Computer Security Act of 1987, from https://csrc.nist.gov.
121. Freedom of Information Act (FOIA), from https://www.foia.gov.
122. Computer Fraud and Abuse Act, from https://www.energy.gov.
123. Federal Identity Theft and Assumption Deterrence Act, from https://www.ftc.gov.
124. The Trade Marks Act 1995, from https://www.legislation.gov.au.
125. The Patents Act 1990, from https://www.legislation.gov.au.
126. The Copyright Act 1968, from https://www.legislation.gov.au.
127. Cybercrime Act 2001, from https://www.legislation.gov.au.
128. The Copyright, Etc. and Trademarks (Offenses and Enforcement) Act 2002, from http://www.legislation.gov.uk.
129. Trademarks Act 1994 (TMA), from http://www.legislation.gov.uk.
130. Regulation of Investigatory Powers Act 2000, from http://www.legislation.gov.uk.
131. Police and Justice Act 2006, from http://www.legislation.gov.uk.
132. Criminal Justice Act 2008, from http://www.legislation.gov.uk.
133. Financial Services Act 2012, from http://www.legislation.gov.uk.
134. Protection of Children Act 1978, from http://www.legislation.gov.uk.
135. Copyright Law of People's Republic of China (Amendments on October 27, 2001), from http://www.npc.gov.cn.
136. Trademark Law of the People's Republic of China (Amendments on October 27, 2001), from http://samr.saic.gov.cn.
137. The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957, from http://www.ipindia.nic.in.
138. Information Technology Act, from http://www.dot.gov.in.
139. Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage, from http://www.cybercrimelaw.net.
140. Penal Code Article 615 ter, from http://www.cybercrimelaw.net.
141. The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000), from http://www.iip.or.jp.
142. Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1, from https://laws-lois.justice.gc.ca.
143. Computer Misuse Act, from https://sso.agc.gov.sg.
144. Trademarks Act 194 of 1993, from http://www.cipc.co.za.

145. Copyright Act of 1978, from http://www.nlsa.ac.za.
146. Copyright Law Act No. 3916, from https://home.heinonline.org.
147. Industrial Design Protection Act, from http://www.kipo.go.kr.
148. Copyright Law, 30/06/1994, from https://www.wipo.int.
149. Computer Hacking, from http://www.cybercrimelaw.net.
150. Unauthorized modification or alteration of the information system, from https://www.domstol.no.
151. Article 139 of the Basic Law, from https://www.basiclaw.gov.hk.

Module 02: Incident Handling and Response Process

152. Christopher Budd, (2008), Why Create a Security Incident Response Process, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512623(v=technet.10).
153. Responding to IT Security Incidents, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875825(v=technet.10).
154. Paul Cichonski, Tom Millar, TimGrance, and Karen Scarfone, (2012), Computer Security Incident Handling Guide, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
155. Michelle Drolet, (2018), 6 Steps for Building a Robust Incident Response Plan, from https://www.csoonline.com/article/3203705/security/10-steps-for-a-successful-incident-response-plan.html.
156. Kelly McCracken, (2018), 10 Steps to Develop an Incident Response Plan You'll Actually Use, from https://engineering.salesforce.com/10-steps-to-develop-an-incident-response-plan-youll-actually-use-6cc49d9bf94c.
157. (2018), How to Develop an Incident Response Plan in 9 Simple Steps, from https://resources.infosecinstitute.com/develop-incident-response-plan-9-simple-steps/#gref.
158. UITSEC CSIRT, from https://www.uitsec.com/wp-content/uploads/2017/03/organization-cs%C4%B1rt-708x1024.jpg.
159. (2004), Incident Management Checklist, from http://www.continuitycentral.com/feature0155.htm.
160. IIJ CSIRT Advisory Solution, from https://www.iij.ad.jp/en/biz/csirt.
161. Customized Setup for Dedicated Cyber Investigation, from http://www.forensicsware.com/lab-setup.html.
162. Brian Evans, (2015), Is Your Computer Forensic Laboratory Designed Appropriately?, from https://securityintelligence.com/is-your-computer-forensic-laboratory-designed-appropriately.
163. The Investigator's Office and Laboratory, from http://faculty.olympic.edu/kblackwell/docs/cmptr238/Online%20Book%20Preview/Chapter%203/0-619-21706-5_03_op.pdf.
164. (2019), CSIRT Incident Report Form, from http://faculty.olympic.edu/kblackwell/docs/cmptr238/Online%20Book%20Preview/Chapter%203/0-619-21706-5_03_op.pdf.
165. Mr. Carlos Galán, Mr. José Antonio Mañas and Innotec System, (2018), National Security Framework Cyber-Incident Management, from https://www.ccn-cert.cni.es/en/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2025-ccn-stic-817-national-security-framework-cyber-incident-management/file.html.

166. US-CERT Federal Incident Notification Guidelines, from https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.

167. (2017), Information Security Incident Handling, from https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM02.pdf.

168. (2017), Risk Management Handbook (RMH) Chapter 8: Incident Response, from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-8-Incident-Response.pdf.

169. Computer Security Incident Response Team (CSIRT) Services Framework, from https://www.first.org/education/FIRST_CSIRT_Services_Framework_v1.1.pdf.

170. Jason Creasey, Ian Glover, (2013), Cyber Security Incident Response Guide, from https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

171. (2017), Manage Post Incident Activities, from https://docs.servicenow.com/bundle/kingston-security-management/page/product/security-incident-response/concept/c_PostIncidentReview.html.

Module 03: Forensic Readiness and First Response

172. (2008), Computer Forensics, from https://www.us-cert.gov/sites/default/files/publications/forensics.pdf.

173. Jau-Hwang Wang, (2019), Computer Forensics – An Introduction, from http://www-users.cs.umn.edu/~aleks/icdm02w/wang.ppt#332,5,Background.

174. Linda Volonino, and Reynaldo Anzaldua, Steps to Take in a Computer Forensics Investigation, from https://www.dummies.com/computers/pcs/computer-security/steps-to-take-in-a-computer-forensics-investigation.

175. (2004), Computer Forensics – Part 1: An introduction to Computer Forensics, from http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf.

176. (2008), Acquire the Data, from https://docs.microsoft.com/en-us/previous-versions//cc162837(v=technet.10).

177. Guide to Computer Forensics and Investigations, from http://www.cps.brockport.edu/~shen/cps301/Chapter2.ppt.

178. Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang, (2006), Guide to Integrating Forensic Techniques into Incident Response, from https://csrc.nist.gov/publications/detail/sp/800-86/final.

179. Introduction to the Incident Response Process, from http://media.techtarget.com/searchNetworking/Downloads/IncidentResponseChapter2.pdf.

180. Robert Rowlingson, (2004), A Ten Step Process for Forensic Readiness, from https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf.

181. Michael B. Mukasey, Jeffrey L. Sedgwick , and David W. Hagy, (2008), Electronic Crime Scene Investigation: A Guide for First Responders, from https://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

182. Crime Scene Investigation, from http://www.angelfire.com/sc3/cjrp/csi.html.

183. First Responder's Manual, from http://www.linuxsecurity.com/resource_files/documentation/firstres.pdf.

184. Aric W. Dutelle, (2010), Documenting the Crime Scene, from http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=184.

185. Filip Maertens, (2009), Digital Evidence in Computer Forensic Investigations, from https://www.slideshare.net/fmaertens/IFA-8-Maart-2007-Computer-Forensics?src=related_normal&rel=580655.

186. Dr. Frederick B. Cohen, Fundamentals of Digital Forensic Evidence, from http://all.net/ForensicsPapers/HandbookOfCIS.pdf.

187. Harley Kozushko, (2003), Digital Evidence, from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf.

188. DAC Janet Williams QPM, (2012), ACPO Good Practice Guide for Digital Evidence, from http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

189. Scientific Working Group on Digital Evidence (SWGDE), from https://www.swgde.org.

190. Keith Mancini, Forensic Photography, from http://www.westchestergov.com/labsresearch/ForensicandTox/forensic/photo/forphotoframeset.htm.

191. Tom Olzak, (2007), Computer forensics: Collecting physical evidence, from https://www.techrepublic.com/blog/it-security/computer-forensics-collecting-physical-evidence.

192. Todd G. Shipley, and Henry R. Reeve, (2006), Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, from http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf.

193. Norman PAN, (2005), First Responder Collection and preservation of evidence, from https://www.pisa.org.hk/event/forensics_1st-responder.pdf.

194. Joan E. Feldman, Collecting And Preserving Electronic Media, from http://www.forensicfocus.com/collecting-preserving-electronic-media.

195. Martin Mulazzani, Markus Huber ,and Edgar Weippl, Social Network Forensics: Tapping the Data Pool of Social Networks, from https://www.sba-research.org/wp-content/uploads/publications/socialForensics_preprint.pdf.

196. Jennifer Richter, Nicolai Kuntze, and Carsten Rudolph, Securing Digital Evidence, from https://www.vogue-project.de/cms/upload/pdf/EvidentialIntegrity.pdf.

197. What is volatile data?, from http://www.computerforensicsspecialists.co.uk/blog/what-is-volatile-data.

198. Data Acquisition, from https://www.omega.com/prodinfo/dataacquisition.html.

199. Aleksander Kołcz, Abdur Chowdhury, and Joshua Alspector, Data duplication: an imbalance problem?, from http://www.site.uottawa.ca/~nat/Workshop2003/imbalance-kolcz.pdf.

200. (2018), Acquisition, from https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Acquisition.

201. Live Response: Collecting Volatile Data (Windows Forensic Analysis), from http://what-when-how.com/windows-forensic-analysis/live-response-collecting-volatile-data-windows-forensic-analysis-part-1.

202. (2005), The ps Command, from http://www.linfo.org/ps.html.

203. (2005), The pstree Command from http://www.linfo.org/pstree.html.

204. pstree - Unix, Linux Command, from http://www.tutorialspoint.com/unix_commands/pstree.htm.

205. (2017), Linux top command, from https://www.computerhope.com/unix/top.htm.

206. (2019), dd (Unix), from https://en.wikipedia.org/wiki/Dd_(Unix).

207. ls - Unix, Linux Command, from http://www.tutorialspoint.com/unix_commands/ls.htm.

208. Silver Moon, (2013), 10 basic examples of Linux ps command, from https://www.binarytides.com/linux-ps-command.

209. (2018), ps (Unix), from https://en.wikipedia.org/wiki/Ps_(Unix).

210. (2005), Forensic Collection and Analysis of Volatile Data, from http://science.hamptonu.edu/compsci/docs/iac/vte_lab_forensic_volatile.pdf.

211. Gary Newell, (2018), How To Use The Linux Top Command To Show Running Processes, from https://www.lifewire.com/linux-top-command-2201163.

212. (2017), Forensic data analysis, from https://en.wikipedia.org/wiki/Forensic_data_analysis.s

213. Yaniv Assor, (2016), Anti-VM and Anti-Sandbox Explained, from https://www.cyberbit.com/blog/endpoint-security/anti-vm-and-anti-sandbox-explained.

214. (2016), How Malware Detects Virtualized Environment (and its Countermeasures), from https://resources.infosecinstitute.com/how-malware-detects-virtualized-environment-and-its-countermeasures-an-overview/#gref.

215. (2013), Anti-Forensics 2, from https://resources.infosecinstitute.com/anti-forensics-2/#gref.

216. Kristy Westphal, Steganography Revealed, from http://www.crime-research.org/library/Steganography.html.

217. Vangie Beal, Steganography, from https://www.webopedia.com/TERM/S/steganography.html.

218. Gary C. Kessler, (2001), Steganography: Hiding Data Within Data, from https://www.garykessler.net/library/steganography.html.

219. (2018), Anti-computer forensics, from https://en.wikipedia.org/wiki/Anti-computer_forensics.

220. Dr. Ajeet Singh Poonia, (2014), Data Wiping and Anti Forensic Techniques, from https://ijact.in/index.php/ijact/article/viewFile/136/109.

221. (2013), Anti-Forensics – Part 1, from https://resources.infosecinstitute.com/anti-forensics-part-1.s

222. Anti-computer Forensics - Artifact Wiping, from http://www.liquisearch.com/anti-computer_forensics/artifact_wiping.

223. Vangie Beal, Encryption, from https://www.webopedia.com/TERM/E/encryption.html.

224. (2019), Encryption, https://en.wikipedia.org/wiki/Encryption.s

225. Simson Garfinkel, (2011), Anti-Forensics: Techniques, Detection and Countermeasures, from https://wenku.baidu.com/view/bea9a1e981c758f5f61f677a.html.

226. Andre Hawari, Anti-Forensics Techniques, Detection and Countermeasures, from https://www.academia.edu/15441665/Anti-Forensics_Techniques_Detection_and_Countermeasures.

227. Anti-Forensics Techniques, Detection and Countermeasures, from https://eforensicsmag.com/download/anti-forensics-techniques-detection-and-countermeasures.

Module 04: Handling and Responding to Malware Incidents

228. Security Threat Report, from https://www.sophos.com.

229. (2003), Trojans FAQ, from http://techgenix.com/trojans-faq/#faq1193.

230. (2014), Emsisoft Malware Library, from https://blog.emsisoft.com/en/7472/emsisoft-malware-library.

231. (2019), Ransomware, from https://en.wikipedia.org/wiki/Ransomware.

232. Computer Worms, from https://userpages.umbc.edu/~dgorin1/432/worms.htm.

233. Ed Skoudis, (2003), Trojan Horses, from http://www.informit.com/articles/article.aspx?p=102181&seqNum=2.

234. Shahram Monshi Pouri, and Nikunj Modi, Trojans and Backdoors, from https://www.it.uu.se/edu/course/homepage/sakdat/ht06/assignments/pm/programme/modi-monshipouri.pdf.

235. Farzad, (2010), Introduction to Trojans and Backdoors, from https://www.symantec.com/connect/articles/introduction-trojans-and-backdoors.

236. (2011), Malware Risks and Mitigation Report, from https://www.nist.gov/sites/default/files/documents/itl/BITS-Malware-Report-Jun2011.pdf.

237. Murugiah Souppaya, and Karen Scarfone, (2013), Guide to Malware Incident Prevention and Handling for Desktops and Laptops, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

238. (2008), Malicious Code Incident Prevention, from http://gta.georgia.gov/sites/gta.georgia.gov/files/imported/vgn/images/portal/cit_1210/0/60/107925573Malicious%20Code%20Incident%20Prevention%20SS-08-033.01.pdf.

239. Vijay, (2017), 7 Definitive Signs Of A Malware Infection On Your Computer, from https://www.techworm.net/2017/02/7-definitive-signs-malware-infection-computer.html.

240. How can I tell if I have malware and what can I do about it?, from https://us.norton.com/internetsecurity-malware-how-can-i-tell-if-i-have-malware-and-what-can-i-do-about-it.html.

241. (2016), 7 Warning signs of malware infection, from http://www.techadvisory.org/2016/03/7-warning-signs-of-malware-infection.

242. Neil J. Rubenking, (2018), 7 Signs You Have Malware and How to Get Rid of It, from https://in.pcmag.com/software/75824/7-signs-you-have-malware-and-how-to-get-rid-of-it.

243. Identifying the Signs and Symptoms of Malware Threats, from https://www.webroot.com/in/en/home/resources/articles/pc-security/malware.

244. (2018), Signs of Malware Infected Computer and How To Get Rid of It, from https://www.techsupportall.com/signs-of-malware-infected-computer-and-how-to-get-rid-of-it.

245. Aaron Stern, (2013), 10 Signs of a Malware Infection, from https://www.kaspersky.com/blog/signs-of-malware-infection/2505.

246. Anand Khanse, (2010), Prefetch Folder: How to view and tweak Prefetch Files in Windows, from https://www.thewindowsclub.com/how-to-view-contents-of-prefetch-file.

247. Garrett Pewitt, (2016), Windows 10 Prefetch and WinPrefetch View, from http://www.forensicexpedition.com/2016/12/08/windows-10-prefetch-and-winprefetch-view.

248. Lenny Zeltser, Introduction to Malware Analysis, from https://zeltser.com/media/docs/intro-to-malware-analysis.pdf.

249. Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard, (2011), Malware Analyst's Cookbook, from https://repo.zenk-security.com/Virus-Infections-Detections-Preventions/Malware%20Analyst%27s%20Cookbook.pdf.

250. Monitor Windows scheduled tasks, from https://cronitor.io/docs/windows-scheduled-task-monitoring.

251. Windows Scheduled Task Monitor, from http://www.solarwinds.com/documentation/en/flarehelp/sam/content/sam-windows-scheduled-task-monitor-sw2577.htm.

233. Ed Skoudis, (2003), Trojan Horses, from http://www.informit.com/articles/article.aspx?p=102181&seqNum=2.

234. Shahram Monshi Pouri, and Nikunj Modi, Trojans and Backdoors, from https://www.it.uu.se/edu/course/homepage/sakdat/ht06/assignments/pm/programme/modi-monshipouri.pdf.

235. Farzad, (2010), Introduction to Trojans and Backdoors, from https://www.symantec.com/connect/articles/introduction-trojans-and-backdoors.

236. (2011), Malware Risks and Mitigation Report, from https://www.nist.gov/sites/default/files/documents/itl/BITS-Malware-Report-Jun2011.pdf.

237. Murugiah Souppaya, and Karen Scarfone, (2013), Guide to Malware Incident Prevention and Handling for Desktops and Laptops, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

238. (2008), Malicious Code Incident Prevention, from http://gta.georgia.gov/sites/gta.georgia.gov/files/imported/vgn/images/portal/cit_1210/0/60/107925573Malicious%20Code%20Incident%20Prevention%20SS-08-033.01.pdf.

239. Vijay, (2017), 7 Definitive Signs Of A Malware Infection On Your Computer, from https://www.techworm.net/2017/02/7-definitive-signs-malware-infection-computer.html.

240. How can I tell if I have malware and what can I do about it?, from https://us.norton.com/internetsecurity-malware-how-can-i-tell-if-i-have-malware-and-what-can-i-do-about-it.html.

241. (2016), 7 Warning signs of malware infection, from http://www.techadvisory.org/2016/03/7-warning-signs-of-malware-infection.

242. Neil J. Rubenking, (2018), 7 Signs You Have Malware and How to Get Rid of It, from https://in.pcmag.com/software/75824/7-signs-you-have-malware-and-how-to-get-rid-of-it.

243. Identifying the Signs and Symptoms of Malware Threats, from https://www.webroot.com/in/en/home/resources/articles/pc-security/malware.

244. (2018), Signs of Malware Infected Computer and How To Get Rid of It, from https://www.techsupportall.com/signs-of-malware-infected-computer-and-how-to-get-rid-of-it.

245. Aaron Stern, (2013), 10 Signs of a Malware Infection, from https://www.kaspersky.com/blog/signs-of-malware-infection/2505.

246. Anand Khanse, (2010), Prefetch Folder: How to view and tweak Prefetch Files in Windows, from https://www.thewindowsclub.com/how-to-view-contents-of-prefetch-file.

247. Garrett Pewitt, (2016), Windows 10 Prefetch and WinPrefetch View, from http://www.forensicexpedition.com/2016/12/08/windows-10-prefetch-and-winprefetch-view.

248. Lenny Zeltser, Introduction to Malware Analysis, from https://zeltser.com/media/docs/intro-to-malware-analysis.pdf.

249. Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard, (2011), Malware Analyst's Cookbook, from https://repo.zenk-security.com/Virus-Infections-Detections-Preventions/Malware%20Analyst%27s%20Cookbook.pdf.

250. Monitor Windows scheduled tasks, from https://cronitor.io/docs/windows-scheduled-task-monitoring.

251. Windows Scheduled Task Monitor, from http://www.solarwinds.com/documentation/en/flarehelp/sam/content/sam-windows-scheduled-task-monitor-sw2577.htm.

252. Windows Servers Scheduled Tasks & Processes Auditing, from https://www.manageengine.com/products/active-directory-audit/windows-member-servers-scheduled-tasks-processes-auditing.html.

253. Amulya Podile, Keerthi Gottumukkala and Krishna Sastry Pendyala, (2015), Digital Forensic Analysis Of Malware Infected Machine- Case Study, from http://www.ijstr.org/final-print/sep2015/Digital-Forensic-Analysis-Of-Malware-Infected-Machine-Case-Study.pdf."

254. (2016), Volatility, from http://computersecuritystudent.com/FORENSICS/VOLATILITY/VOLATILITY2_2/lesson3/index.html.

255. Frank Boldewin, (2011), Hunting malware with Volatility, from http://www.reconstructer.org/papers/Hunting%20malware%20with%20Volatility%20v2.0.pdf.

256. Gleeda, (2017), Command Reference, from https://github.com/volatilityfoundation/volatility/wiki/Command-Reference.

257. (2011), Memory Forensics: Analyzing a Stuxnet Memory Dump (And you can too!), from https://cyberarms.wordpress.com/2011/11/10/memory-forensics-analying-a-stuxnet-memory-dump-and-you-can-too.

258. Yashashree Gund, (2014), Malware analysis using volatility, from https://www.slideshare.net/somnathyash/malware-analysis-using-volatility.

259. Ahmad, (2017), How to install and use Volatility memory forensic tool, from https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool.

260. Paula, Memory Dump Analysis – Extracting Juicy Data, from https://cqureacademy.com/blog/forensics/memory-dump-analysis.

261. (2017), Debugging Tools for Windows (WinDbg, KD, CDB, NTSD), from https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger.

262. Singhgurjot, (2015), Memory image forensic analysis using Volatility tool in kali linux, from https://singhgurjot.wordpress.com/2015/09/02/memory-image-forensic-analysis-using-volatility-tool-in-kali-linux.

263. Tigzy, (2014), KernelMode Rootkits: Part 3, kernel filters, from https://www.adlice.com/kernelmode-rootkits-part-3-kernel-filters.

264. File Filter Drivers, from https://flylib.com/books/en/1.242.1.59/1.

Module 05: Handling and Responding to Email Security Incidents

265. Lawrence C. Miller, Types of Threats to E-mail Security on a Home Network, from https://www.dummies.com/computers/computer-networking/network-security/types-of-threats-to-e-mail-security-on-a-home-network.

266. (2018), Latest Trend of Email Scam – CEO Email Scam, from https://www.police.gov.hk/ppp_en/04_crime_matters/ccb/fst.php?msg_id=cct_30.

267. (2018), Examples of HMRC Related Phishing Emails and Bogus Contact, from https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples.

268. (2008), Phishing: Examples & its prevention methods, from http://chowkamleeng.blogspot.com/2008/06/phishing-examples-its-prevention.html.

269. The Phishing Guide (Part 1) Understanding and Preventing Phishing Attacks, from http://www.technicalinfo.net/papers/Phishing.html.

270. Stu Sjouwerman, (2018), Data Games: Phishing as an Endless Quest for Exploitable Data, from https://www.scmagazine.com/home/opinions/data-games-phishing-as-an-endless-quest-for-exploitable-data.

271. Margaret Rouse, (2017), Spear Phishing, from https://searchsecurity.techtarget.com/definition/spear-phishing.

272. Smishing, vishing, and phishing, from https://www.forensicaccountingservices.com/fraudvault/smishing-vishing-and-phishing.

273. Margaret Rouse, Email Virus, from https://searchsecurity.techtarget.com/definition/email-virus.

274. Doug Olenick, (2017), Email Malware, Phishing and Spam Attempts Hit New Highs For 2017, from https://www.scmagazine.com/email-malware-phishing-and-spam-attempts-hit-new-highs-for-2017/article/680281.

275. Ben Nahorney, (2017), Internet Security Threat Report 2017, from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf.

276. Al Pascual, Kyle Marchini, Sarah Miller, (2018), 2018 Identity Fraud: Fraud Enters a New Era of Complexity, from https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

277. (2015), The 10 Major Types of Identity Theft, from https://www.idtheftauthority.com/types.

278. (2011), The 6 Types of Identity Theft, from https://securingtomorrow.mcafee.com/consumer/family-safety/the-6-types-of-identity-theft.

279. Types of Identity Theft and Fraud, from https://www.colorado.gov/pacific/cbi/types-identity-theft-and-fraud.

280. Types of Identity Theft, from https://www.completeid.com/education-center/types-of-identity-theft.

281. The 7 Most Common Types of Identity Theft, from https://www.houstoncrimedefense.com/blog/the-7-most-common-types-of-identity-theft.

282. Clari Melo, (2018), Get to Know These Common Types of ID Theft, from https://www.igrad.com/articles/8-types-of-identity-theft.

283. Darrow Law Firm, Child Pornography under Texas Law, from https://www.hg.org/legal-articles/child-pornography-under-texas-law-29773.

284. Child Abduction Law - Child Kidnapping Law, from https://www.hg.org/child-abduction.html.

285. Gabor Szathmari, (2015), Phishing Incident Response Playbook, from https://www.demisto.com/phishing-incident-response-playbook.

286. Email Header, from https://www.arclab.com/en/kb/email/how-to-read-and-analyze-the-email-header-fields-spf-dkim.html.

287. Bala Ganesh, (2018), Email Header Analysis – Received Email is Genuine or Spoofed, from https://gbhackers.com/email-header-analysis.

288. Matt Moorehead, (2015), How to Explain SPF in Plain English, from https://blog.returnpath.com/how-to-explain-spf-in-plain-english.

289. How to Interpret SPF Authentication Verification Results, from https://help.returnpath.com/hc/en-us/articles/115000460632-How-to-interpret-SPF-authentication-verification-results.

290. Luis Fernandes, (2018), What Are the Different Results in Sender Policy Framework?, from https://support.gfi.com/hc/en-us/articles/360012880714-What-are-the-different-results-in-Sender-Policy-Framework-.

291. Garrett Dimon, (2016), How Does SPF Protect Your Domain From E-mail Spoofing?, from https://postmarkapp.com/guides/spf.

292. Paul Cunningham, (2016), Get the Most Out of Exchange Logs to Prevent Issues, from https://searchwindowsserver.techtarget.com/tip/Get-the-most-out-of-Exchange-logs-to-prevent-issues.

293. Checking the Mail Log, from https://mediatemple.net/community/products/dv/204643910/checking-the-mail-log.

294. (2018), Avoid Phishing Scams, from https://kb.iu.edu/d/arsf.

295. (2015), Dealing with the Problem of Targeted Email Attacks, from https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/network/deep-discovery/email-inspector/Dealing%20With%20the%20Problem%20of%20Targeted%20Email%20Attacks%20Osterman%20(1)-2.pdf.

296. (2016), How Can I Prevent Email-based Malware and Viruses Attacks?, from https://www2.owens.edu/faq/entry/440.

297. (2016), A Handy Guide on Handling Phishing Attacks, from https://blog.rapid7.com/2016/06/21/a-layered-approach-to-handling-phishing-attacks.

298. What to do When You Fall for An Email Scam, from https://us.norton.com/internetsecurity-online-scams-what-to-do-when-you-fall-for-an-email-scam.html.

Module 06: Handling and Responding to Network Security Incidents

299. Fyodor, (1997), The Art of Port Scanning, from https://nmap.org/nmap_doc.html.

300. Steven J. Templeton, and Karl E. Levitt, Detecting Spoofed Packets, from http://seclab.cs.ucdavis.edu/papers/DetectingSpoofed-DISCEX.pdf.

301. Avi Kak, (2018), Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing, from https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf.

302. Prabhaker Mateti, (2001), Port Scanning, from http://www.cs.wright.edu/~pmateti/Courses/499/Probing/index.html.

303. Firewall/IDS Evasion and Spoofing, from https://nmap.org/book/man-bypass-firewalls-ids.html.

304. Sharan R, Hacking Techniques - Scanning Networks and Countermeasures, from http://hack-o-crack.blogspot.com/2010/12/hacking-techniques-scanning-networks.html.

305. Santosh Kumar, (2013), Detect/Analyze Scanning Traffic Using Wireshark, from https://www.koenig-solutions.com/documents/pentestextra-06-2013.pdf.

306. Peter Loshin, (2018), Denial of Service Attack, from https://searchsecurity.techtarget.com/definition/denial-of-service.

307. (2019), Denial-of-service attack, from https://en.wikipedia.org/wiki/Denial-of-service_attack.

308. (2007), Denial Of services [botnet] (DoS), from https://www.go4expert.com/articles/denial-services-botnet-dos-t3184.

309. What is a DDoS Attack?, from https://www.digitalattackmap.com/understanding-ddos.

310. Distributed Denial of Service (DDoS) Attack, from https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

311. Stephen M. Spechtv, and Ruby B. Lee, Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, from http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf.
312. Ping of Death, from https://searchsecurity.techtarget.com/definition/ping-of-death.
313. Jason Anderson, (2001), An Analysis of Fragmentation Attacks, from http://www.ouah.org/fragma.html.
314. Analysis of Fragmented Packet Traffic, from https://www.caida.org/research/traffic-analysis/fragments.
315. SYN Flood Attack, from https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack.
316. Ofer Shezaf, (2017), Brute Force: Anatomy of an Attack, from https://www.varonis.com/blog/brute-force-anatomy-of-an-attack.
317. Steve Gibson, (2002), DRDoS: Distributed Reflection Denial of Service, from https://homes.cs.washington.edu/~arvind/cs425/doc/drdos.pdf.
318. Blake Snow, (2009), Microsoft responds to Xbox Live denial-of-service attack, from https://arstechnica.com/gaming/2009/02/microsoft-responds-to-xbox-live-denial-of-service-attack.
319. Glenn Carl, George Kesidis, Richard R. Brooks, and Suresh Rai, (2006), Denial-of-Service Attack-Detection Techniques, from https://www.computer.org/csdl/mags/ic/2006/01/w1082-abs.html.
320. Dan Breslaw, (2016), Configuring mod_evasive to Protect Apache Servers, from https://www.incapsula.com/blog/configuring-mod_evasive-to-protect-your-apache-server.html.
321. Frank Kargl, Jörn Maier, Stefan Schlott, and Michael Weber, Protecting Web Servers from Distributed Denial of Service Attacks, from http://www10.org/cdrom/papers/409.
322. Gary C. Kessler, (2000), Defenses Against Distributed Denial of Service Attacks, from https://www.garykessler.net/library/ddos.html.
323. Hitesh Jethva, (2015), How to Protect Against DDoS with Mod_evasive on Apache Server, from https://www.maketecheasier.com/mod-evasive-protect-ddos.
324. (2009), A list of wireless network attacks, from https://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks.
325. (2009), How to prevent wireless DoS attacks, from https://searchsecurity.techtarget.com/feature/How-to-prevent-wireless-DoS-attacks.
326. Precious John Doe, A List of Internet and Network Attacks, from https://www.brighthub.com/computing/smb-security/articles/53949.aspx.
327. Applying Wireless Security Practices to Justice Information Sharing, from https://it.ojp.gov/documents/wirelesssecurity.pdf.

Module 07: Handling and Responding to Web Application Security Incidents

328. Jason Steer, (2013), The Need for Incident Response from https://www.fireeye.com/blog/executive-perspective/2013/11/the-need-for-incident-response.html.
329. Pierluigi Paganini, (2013), Why do We Need For Incident Response Plan? from http://securityaffairs.co/wordpress/20032/security/need-incident-response.html.
330. SC Staff, (2017), Web Application Attacks Accounted For 73% of All Incidents Says Report from https://www.scmagazineuk.com/web-application-attacks-accounted-73-incidents-says-report/article/1474238.
331. (2017), OWASP Top 10 Application Security Risks - 2017 from https://www.owasp.org/index.php/Top_10-2017_Top_10.

332. (2016), Sensitive Data Exposure Vulnerability: Causes and Prevention from Image: https://medium.com/@BreezeTelecom/sensitive-data-exposure-vulnerability-causes-and-prevention-4c86a19df70d.

333. abodiford, (2014), Sensitive Data Exposure from https://www.slideshare.net/abodiford/sensitive-data-exposure.

334. Ian Muscat, (2017), What is XML External Entity (XXE)? from https://www.acunetix.com/blog/articles/xml-external-entity-xxe-vulnerabilities.

335. (2017), XXE Injection Attacks – XML External Entity Vulnerability With Examples from https://www.darknet.org.uk/2017/10/xxe-injection-attacks-xml-external-entity-vulnerability-examples.

336. Alex Coleman, User Authentication and Access Control in a Web Application from https://selftaughtcoders.com/user-authentication-access-control-web-application.

337. Serialization and Deserialization in Java from https://www.javatpoint.com/serialization-in-java.

338. (2008), Path Traversal and URIs, from https://phucjimy.wordpress.com/category/document-security.

339. (2013), Code Injection, from https://www.owasp.org/index.php/Code_Injection.

340. (2017), Web Application Attack Trends from https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Web-Application-Attack-Trends-2017-eng.pdf.

341. (2013), Cross Site Scripting Flaw, from https://www.owasp.org/index.php/Cross_Site_Scripting_Flaw.

342. (2017), Connection String Injection Attacks, from https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-builders.

343. Chema Alonso, Manuel Fernandez, Alejandro Martín, and Antonio Guzmán, Connection String Parameter Pollution Attacks, from https://blackhat.com/presentations/bh-dc-10/Alonso_Chema/Blackhat-DC-2010-Alonso-Connection-String-Parameter-Pollution-wp.pdf.

344. (2011), Session Prediction, from https://www.owasp.org/index.php?title=Session_Prediction&setlang=en.

345. Robert Auger, Buffer Overflow, from http://projects.webappsec.org/w/page/13246916/Buffer-Overflow.

346. (2010), Web Parameter Tampering, from https://www.owasp.org/index.php/Web_Parameter_Tampering.

347. (2015), Path Traversal, from https://www.owasp.org/index.php/Path_Traversal.

348. Chema Alonso, Rodolfo Bordon, and Antonio Guzman Y Marta Beltran, LDAP Injection & Blind LDAP Injection in Web Applications, from https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf.

349. Parameter Manipulation, from https://www.cgisecurity.com/owasp/html/ch11s04.html.

350. (2018), Cross-site Scripting (XSS), from https://www.owasp.org/index.php/Cross-site_Scripting_(XSS).

351. (2018), XSS Filter Evasion Cheat Sheet, from https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet.

352. Cross-Site Request Forgery (CSRF) Attack Lab, from http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_CSRF_Elgg/Web_CSRF_Elgg.pdf.

353. Web Application Attack : DOS and DDOS attack, from http://funwhichuwant.blogspot.com/2012/10/webapplication-attack-dos-and-ddos.html.

354. HTML Code Injection and Cross-site scripting, from http://www.technicalinfo.net/papers/CSS.html.

355. The Cross-Site Scripting (XSS) FAQ, from https://www.cgisecurity.com/xss-faq.html.

356. What is Cross-Site Scripting (XSS)?, from http://www.applicure.com/blog/what-is-cross-site-scripting.
357. LDAP Filters, from http://www.selfadsi.org/ldap-filter.htm.
358. (2018), XSS (Cross Site Scripting) Prevention Cheat Sheet, from https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet.
359. (2010), Unvalidated Input, from https://www.owasp.org/index.php/Unvalidated_Input.
360. Kevin Beaver, (2006), The importance of input validation, from https://searchsoftwarequality.techtarget.com/tip/The-importance-of-input-validation.
361. (2018), Code injection, from https://en.wikipedia.org/wiki/Code_injection.
362. (2019), File inclusion vulnerability, from https://en.wikipedia.org/wiki/File_inclusion_vulnerability.
363. Robert Auger, LDAP Injection, from http://projects.webappsec.org/w/page/13246947/LDAP%20Injection.
364. (2019), Cross-site scripting, from https://en.wikipedia.org/wiki/Cross-site_scripting.
365. (2009), CSRF Attacks and Web Forms, from https://haacked.com/archive/2009/04/02/csrf-webforms.aspx.
366. (2004), Cross-Site Request Forgeries, from http://shiflett.org/articles/cross-site-request-forgeries.
367. Robert Auger, (2010), The Cross-Site Request Forgery (CSRF/XSRF) FAQ, from https://www.cgisecurity.com/csrf-faq.html.
368. Cookie Poisoning, from https://www.imperva.com/resources/glossary/cookie-poisoning.
369. (2016), Buffer Overflow, from https://www.owasp.org/index.php/Buffer_Overflow.s
370. Abodiford, (2014), Sensitive Data Exposure, from https://www.slideshare.net/abodiford/sensitive-data-exposure.
371. Injection Flaws, from http://www.ids-sax2.com/articles/Injection-Flaws.htm.
372. Incident Response, from https://www.incapsula.com/web-application-security/define-security-incident-response.html.
373. (2008), Testing for SQL Wildcard Attacks (OWASP-DS-001), from https://www.owasp.org/index.php/Testing_for_SQL_Wildcard_Attacks_(OWASP-DS-001).
374. Fahmida Y. Rashid, (2015), 5 Signs your Web Application Has Been Hacked from https://www.infoworld.com/article/2999475/security/5-signs-your-web-application-has-been-hacked.html.
375. (2012), Complete Cross Site Scripting (XSS) Cheat Sheets from http://breakthesecurity.cysecurity.org/2012/02/complete-cross-site-scriptingxss-cheat-sheets-part-1.html.
376. Jennifer Marsh, (2016), How to Detect and Analyze DDoS Attacks Using Log Analysis, from https://www.loggly.com/blog/how-to-detect-and-analyze-ddos-attacks-using-log-analysis.
377. (2010), HTML and JavaScript Injection, from https://www.codeproject.com/Articles/134024/HTML-and-JavaScript-Injection.
378. (2019), Unrestricted Upload of File with Dangerous Type, from https://cwe.mitre.org/data/definitions/434.html.
379. Ryan Barnett, (2011), ModSecurity Advanced Topic of the Week: Remote File Inclusion Attack Detection, from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/modsecurity-advanced-topic-of-the-week-remote-file-inclusion-attack-detection.

380. (2018), Log Analysis for Web Attacks: A Beginner's Guide, from https://resources.infosecinstitute.com/log-analysis-web-attacks-beginners-guide/#gref.

381. Anirudh Kondaveeti, (2015), Sequential Pattern Mining Approach for Watering Hole Attack Detection, from https://content.pivotal.io/blog/sequential-pattern-mining-approach-for-watering-hole-attack-detection.

382. T. Subburaj, and K. Suthendran, (2018), Digital Watering Hole Attack Detection Using Sequential Pattern, from https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_711.pdf.

383. Lenny Zeltser, 8 Practical Tips for Detecting a Website Compromise for Free, from https://zeltser.com/tips-for-detecting-website-compromise.

384. Installing ClamAV, from https://www.clamav.net/documents/installing-clamav.

385. Effective Log Management, from https://www.ncsc.gov.uk/content/files/protected_files/document_files/2014-05-07-Effective%20Log%20Management%20Booklet.pdf.

386. James Parsons, (2017), How to Stop Most Website Attacks Yourself in 5 Minutes from http://www.huffingtonpost.com/james-parsons/how-to-stop-most-website-_b_10014570.html.

387. (2010), Prevent Cross-Site Scripting Hacks With Tools, Testing from https://searchsecurity.techtarget.com/tip/Prevent-cross-site-scripting-hacks-with-tools-testing.

388. (2010), Preventing and Stopping SQL Injection Hack Attacks from https://searchsecurity.techtarget.com/tip/Preventing-and-stopping-SQL-injection-hack-attacks.

389. (2010), Distributed Denial-of-Service Protection: How to Stop DDoS Attacks from https://searchsecurity.techtarget.com/tip/Distributed-denial-of-service-protection-How-to-stop-DDoS-attacks.

390. Nathan Rossiter, (2014), Common Web Application Attacks and How to Prevent Them from https://www.business2community.com/crisis-management/common-web-application-attacks-prevent-0949592#HBjkC9q11Pmggx4d.97.

391. Eric Brune, (2018), 4 Common Web Application Security Attacks And What You Can Do To Prevent Them from https://www.instart.com/blog/4-common-web-application-security-attacks-and-what-you-can-do-prevent-them.

392. John Rogers, (2010), Web Attacks and How to Stop Them from https://www.nebraskacert.org/csf/CSF-Jun2010.pdf.

393. (2010), Improving Web Application Security: Threats and Countermeasures, from https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10).

394. (2017), Injection Prevention Cheat Sheet, from https://www.owasp.org/index.php/Injection_Prevention_Cheat_Sheet.

395. (2017), Top 10-2017 A2-Broken Authentication, from https://www.owasp.org/index.php/Top_10-2017_A2-Broken_Authentication.

396. (2010), Broken Authentication and Session Management, from https://www.owasp.org/index.php/Broken_Authentication_and_Session_Management.

397. (2018), Top 10-2017 A3-Sensitive Data Exposure, from https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure.

398. (2018), Top 10-2017 A4-XML External Entities (XXE), from https://www.owasp.org/index.php/Top_10-2017_A4-XML_External_Entities_(XXE).

399. (2018), Top 10-2017 A8-Insecure Deserialization, from https://www.owasp.org/index.php/Top_10-2017_A8-Insecure_Deserialization.

400. How to recover data that is missing or damaged as a result of a SQL injection attack, from https://solutioncenter.apexsql.com/recover-damaged-missing-data-due-to-sql-injection-attack.

401. XSS Attack Information from http://www.xssed.com.

Module 08: Handling and Responding to Cloud Security Incidents

402. (2013), Introduction to Cloud Computing, from https://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

403. Alok Tripathi, and Abhinav Mishra, (2011), Cloud computing security considerations, from https://www.semanticscholar.org/paper/Cloud-computing-security-considerations-Tripathi-Mishra/fd710d62f8db9621d97ab00acf1bb8e8d28e06b2.

404. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, from http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

405. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, (2013), An analysis of security issues for cloud computing, from https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5.

406. Cloud Security The definitive guide to managing risk in the new ICT landscape, from http://www.fujitsu.com/global/Images/WBOC-2-Security.pdf.

407. Dejan Lukan, (2014), Cloud Forensics: An Overview, from https://resources.infosecinstitute.com/overview-cloud-forensics/#gref.

408. Dejan Lukan, (2014), Cloud forensics: An intro to cloud network forensic data collection, from https://searchcloudsecurity.techtarget.com/tip/Cloud-forensics-An-intro-to-cloud-network-forensic-data-collection.

409. Craig Nelson, and Tomer Teller, (2016), Cloud Attacks Illustrated: Insights from the cloud provider, from https://www.rsaconference.com/writable/presentations/file_upload/air-r05f-cloud_attack_illustrated_insights_from_the_cloud_provider.pdf.

410. (2015), Cloud Computing: Attack Vectors and Counter Measures, from https://resources.infosecinstitute.com/cloud-computing-attacks-vectors-and-counter-measures/#gref.

411. Nurul Ab Rahman, (2014), A survey of information security incident handling in the cloud, from https://www.researchgate.net/publication/269403060_A_survey_of_information_security_incident_handling_in_the_cloud.

412. Man in the Cloud (MITC) Attacks, from https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf.

413. Incident Response, from https://cloudsecurityalliance.org/wp-content/uploads/2011/09/Domain-9.docx.

414. Sid Nag, Fred Ng, and David Edward Ackerman, (2016), A new way to streamline and simplify cloud security compliance with STARWatch, from https://star.watch/assets/White_Paper_Final-92109763d18ab1d34477ae944690ebb7549f51186123b7ac13beef30cc8bf8d7.pdf.

415. Shachaf Levi, Eran Birk, Esteban Gutierrez, Kenneth J. Logan, Jac Noel, Nooshin Zand Carlton Ashley, Thai Bui, and Paul Matthews, (2015), SaaS Security Best Practices; Minimizing Risk in the Cloud, from https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/saas-security-best-practices-minimizing-risk-in-the-cloud-paper.pdf.

416. Mike Rothman, (2016), Incident Response in the Cloud Age, from https://securosis.com/assets/library/reports/Securosis_CloudAgeIR_FINAL.pdf.

417. Rainer Poisel, Erich Malzer, and Simon Tjoa, Evidence and Cloud Computing: The Virtual Machine Introspection Approach, from http://isyou.info/jowua/papers/jowua-v4n1-7.pdf.

418. Doowon Jeong, Jungheum Park, Sangjin Lee, and Chulhoon Kang, (2015), Investigation Methodology of a Virtual Desktop Infrastructure for IoT, from https://www.hindawi.com/journals/jam/2015/689870.

419. Yucel Turel, and Romuald K. Kotowski, (2015), Cloud Computing Virtualization and Cyber Attacks: Evidence Centralization, from https://www.researchgate.net/publication/275021701_Cloud_Computing_Virtualization_and_Cyber_Attacks_Evidence_Centralization.

420. Yunting Lei, and Yuyin Cui, (2013), Research on Live Forensics in Cloud Environment, from www.atlantis-press.com/php/download_paper.php?id=10174.

421. Joshua I James, Ahmed F. Shosha, and Pavel Gladyshev, (2012), Digital Forensic Investigation and Cloud Computing, from https://www.researchgate.net/publication/259497217_Digital_Forensic_Investigation_and_Cloud_Computing.

422. Ory Segal, Web Application Forensics: The Uncharted Territory, from https://www.cgisecurity.com/lib/WhitePaper_Forensics.pdf.

423. Kwang Raymond, and Choo Ali Dehghantanha, (2016), Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, from https://www.elsevier.com/books/contemporary-digital-forensic-investigations-of-cloud-and-mobile-applications/choo/978-0-12-805303-4.

424. Erik Miranda Lopez, Seo Yeon Moon, and Jong Hyuk Park, (2016), Scenario-Based Digital Forensics Challenges in Cloud Computing, from https:// www.mdpi.com/2073-8994/8/10/107/pdf.

425. (2018), Incident Handling on Cloud Computing, from https://www.ukessays.com/dissertation/examples/computer-science/incident-handling-on-cloud-computing.php.

426. Security Incident Response Guide, from https://cloud.gov/docs/ops/security-ir.

427. Apurv, (2014), Incident containment in a cloud environment, from https://blog.cloudpassage.com/2014/04/29/incident-containment-in-a-cloud-environment.

428. Tim Erlin, (2015), Detecting Man-in-the-Cloud (MitC) Attacks with Adaptive Threat Protection, from https://www.tripwire.com/state-of-security/security-data-protection/detecting-man-in-the-cloud-mitc-attacks-with-adaptive-threat-protection.

Module 09: Handling and Responding to Insider Threats

429. Leron Zinatullin, (2014), Identifying and Preventing Insider Threats, from https://www.tripwire.com/state-of-security/incident-detection/identifying-and-preventing-insider-threats.

430. Wallix, (2016), The Psychology of the Insider Attack - Part II, from http://blog.wallix.com/the-psychology-of-the-insider-attack.

431. Margaret Rouse, (2012), Industrial Espionage, from https://whatis.techtarget.com/definition/industrial-espionage.

432. (2019), Cyber Spying, from https://en.wikipedia.org/wiki/Cyber_spying.

433. James Walsh, Industrial Espionage and Computer Forensics, from https://www.streetdirectory.com/travel_guide/114551/computers/industrial_espionage_and_computer_forensics.html.

434. Alex Taverner, (2016), Managing Insider Threats, from https://www.baesystems.com/en/cybersecurity/blog/managing-insider-threats.

435. Robert C. Covington, (2015), Physical security: The overlooked domain, from https://www.csoonline.com/article/2939322/security/physical-security-the-overlooked-domain.html.

436. (2014), How to Protect Insiders from Social Engineering Threats, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10).

437. Margaret Rouse, (2011), Rack Server (Rack-Mounted Server), from https://whatis.techtarget.com/definition/rack-server-rack-mounted-server.

438. Deb Shinder, (2007), 10 Physical Security Measures Every Organization Should Take, from https://www.techrepublic.com/blog/10-things/10-physical-security-measures-every-organization-should-take.

439. Insider Threat, from https://www.splunk.com/en_us/cyber-security/insider-threat.html.

440. (2015), Analytic Approaches to Detect Insider Threats, from https://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_451069.pdf.

441. Andrew Costis, (2017), Stop Insider Threats with LogRhythm's UEBA Capabilities, from https://logrhythm.com/blog/stop-insider-threats-with-logrhythms-ueba-capabilities.

442. George Moraetes, (2017), The CISO's Guide to Managing Insider Threats, from https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats.

443. Managing insider threat, A holistic approach to dealing with risk from within, from https://www.ey.com/Publication/vwLUAssets/EY-managing-inside-threat/$FILE/EY-managing-inside-threat.pdf.

444. (2016), Insider Threat Detection in Government Cyber Security, from https://www.virtru.com/blog/insider-threat-detection.

445. Margaret Rouse, (2017), User Behavior Analytics (UBA), from https://searchsecurity.techtarget.com/definition/user-behavior-analytics-UBA.

446. Javvad Malik, (2015), Insider Threats Defined, from https://www.alienvault.com/blogs/security-essentials/insider-threats-defined.

447. (2014), Combating the Insider Threat, from https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf.

448. (2013), Insider Threat Detection, from https://www.personaminc.com/itd/wp-content/uploads/2015/01/Personam-ITD-Whitepaper.pdf.

449. Amos Azaria, Ariella Richardson, Sarit Kraus, and V. S. Subrahmanian, (2014), Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data, from https://www.semanticscholar.org/paper/Behavioral-Analysis-of-Insider-Threat%3A-A-Survey-and-Azaria-Richardson/1ce1e3f9a839e685983dfad4ec3704f0b91a6396?navId=citing-papers.

450. (2018), Finding and Detecting Insider Threats and Advanced Persistent Threats - Part 1, from https://www.youtube.com/watch?v=CBp7uZSq4mE.

451. Profiles - Where Firefox stores your bookmarks, passwords and other user data, from https://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data.

452. Raymond, (2017), 2 Tools to Check the USB Devices Used on Your Computer, from https://www.raymond.cc/blog/find-out-what-usb-device-has-been-used-on-your-computer.

453. (2017), USB History Viewing, from https://www.forensicswiki.org/wiki/USB_History_Viewing.

454. Tom Rogers, (2008), Mac Tip: Where's Device Manager?, from https://www.youtube.com/watch?v=J1og_lUJmdQ.

455. (2018), Using USB Devices With your Mac, from https://support.apple.com/en-gb/HT201163.

456. (2017), About System Information on your Mac, from https://support.apple.com/en-in/HT203001.

457. (2013), McAfee Database Activity Monitoring, from https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-database-activity-monitoring.pdf.

458. Ed Tittel, (2015), Comparing the Top Database Security Tools, from https://searchsecurity.techtarget.com/feature/Comparing-the-top-database-security-tools.

459. (2018), Database Activity Monitoring, from https://en.wikipedia.org/wiki/Database_activity_monitoring.

460. MySQL Enterprise Monitor, from https://www.mysql.com/fr/products/enterprise/monitor.html.

461. (2009), Security & Counter-Surveillance, from https://warriorpublications.files.wordpress.com/2012/03/security-countersurveillance1.pdf.

462. (2019), Metal detector, from https://en.wikipedia.org/wiki/Metal_detector#Security_screening.

463. Robert C. Covington, (2015), Physical security: The overlooked domain, from https://www.csoonline.com/article/2939322/security0/physical-security-the-overlooked-domain.html.

464. Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak, (2012), Secure Backup and Recovery Strategy Key Against Insider Attack, from https://searchdisasterrecovery.techtarget.com/Secure-backup-and-recovery-strategy-key-against-insider-attack.

465. Mike Smith, (2018), Insider Threats: Preparation, Best Practices and Detection, from https://www.lepide.com/blog/insider-threats-preparation-best-practices-and-detection.

466. Dawn Cappelli, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeal, Best Practices for the Prevention and Detection of Insider Threats, from https://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/0321812573_ch06.pdf.

467. Linda Musthaler, (2008), 13 best practices for preventing and detecting insider threats, from https://www.networkworld.com/article/2280365/lan-wan/13-best-practices-for-preventing-and-detecting-insider-threats.html.

468. Troy Scavella, (2016), Detecting and Preventing the Insider Threat, from https://www.fireeye.com/blog/executive-perspective/2016/05/detecting_and_preven.html.

469. Margaret Rouse, (2014), Data Loss Prevention (DLP), from https://whatis.techtarget.com/definition/data-loss-prevention-DLP.

470. (2019), Data Loss Prevention Software, from https://en.wikipedia.org/wiki/Data_loss_prevention_software.