Table of Contents

[Type of the Attackers 4](#_Toc175227269)

[5](#_Toc175227270)

[The Cube 5](#_Toc175227271)

[Malware: - 5](#_Toc175227272)

[Spyware: - 5](#_Toc175227273)

[Adware: - 6](#_Toc175227274)

[Backdoor: - 6](#_Toc175227275)

[Ransomware: - 6](#_Toc175227276)

[Scareware: - 6](#_Toc175227277)

[Rootkit: - 6](#_Toc175227278)

[Virus: - 6](#_Toc175227279)

[Trojan Horse: - 6](#_Toc175227280)

[Worms: - 7](#_Toc175227281)

[Different Methods of Infiltration 7](#_Toc175227282)

[Social Engineering : - 7](#_Toc175227283)

[Denial-of-Service:- 7](#_Toc175227284)

[Distributed DOS :- 7](#_Toc175227285)

[Botnet: - 8](#_Toc175227286)

[On-Path-Attacks: - 8](#_Toc175227287)

[Man-In-The-Middle (MITM) 8](#_Toc175227288)

[Man-In-The-Mobile(MITMO) 8](#_Toc175227289)

[SEO Poisoning: - 8](#_Toc175227290)

[Wi-Fi Password Cracking: - 8](#_Toc175227291)

[Password Spraying: - 9](#_Toc175227292)

[Dictionary Attacks: - 9](#_Toc175227293)

[Brute-Force Attacks: - 9](#_Toc175227294)

[Rainbow Attacks: - 9](#_Toc175227295)

[Traffic Interception:- 9](#_Toc175227296)

[Advanced Persistent Threats: - 9](#_Toc175227297)

[Security Vulnerability and Exploits:- 10](#_Toc175227298)

[Hardware Vulnerabilities: - 10](#_Toc175227299)

[Software Vulnerabilities: - 10](#_Toc175227300)

[Buffer Overflow: - 10](#_Toc175227301)

[Non-Validated Inputs: - 10](#_Toc175227302)

[Race Conditions: - 10](#_Toc175227303)

[Weaknesses in Security Practices: - 11](#_Toc175227304)

[Access Control Problems: - 11](#_Toc175227305)

[Methods To Safeguard Your Online Privacy 11](#_Toc175227306)

[Two Factor Authentication:- 11](#_Toc175227307)

[Open Authorization:- 11](#_Toc175227308)

[Don’t Get Spoofed : - 11](#_Toc175227309)

[Email and Web Browser Privacy: - 11](#_Toc175227310)

[Cybersecurity Devices and Technologies 12](#_Toc175227311)

[Firewalls: - 12](#_Toc175227312)

[Network Layer Firewall :- 12](#_Toc175227313)

[Transport Layer Firewall: - 12](#_Toc175227314)

[Application Layer Firewall: - 12](#_Toc175227315)

[Context Aware Layer Firewall: - 12](#_Toc175227316)

[Proxy Server: - 12](#_Toc175227317)

[Reverse Proxy Server: - 12](#_Toc175227318)

[Network Address Translation(NAT) Firewall: - 12](#_Toc175227319)

[Host-based Firewall: - 12](#_Toc175227320)

[Port Scanning: - 12](#_Toc175227321)

[Intrusion Detection and Prevention Systems: - 13](#_Toc175227322)

[Intrusion detection systems (IDSs) :- 13](#_Toc175227323)

[Intrusion prevention systems (IPSs) 13](#_Toc175227324)

[Real Time Detection: - 13](#_Toc175227325)

[Protecting Against Malware: - 14](#_Toc175227326)

[Secure Operations Center Team : - 14](#_Toc175227327)

[Incidence Response Team: - 14](#_Toc175227328)

[Threat Intelligence Team:- 14](#_Toc175227329)

[Security Infrastructure Engineering Team: - 14](#_Toc175227330)

[Security Best Practices : - 14](#_Toc175227331)

[Perform a risk assessment: - 15](#_Toc175227332)

[Create a security policy: - 15](#_Toc175227333)

[Physical security measures: - 15](#_Toc175227334)

[Human resource security measures: - 15](#_Toc175227335)

[Perform and test backups: - 15](#_Toc175227336)

[Maintain security patches and updates: - 15](#_Toc175227337)

[Employee access control: - 15](#_Toc175227338)

[Regular test incident response: - 15](#_Toc175227339)

[Implement a network monitoring analytics and management tools: - 15](#_Toc175227340)

[Implement network security devices: - 15](#_Toc175227341)

[Implement a comprehensive endpoint security solution: - 15](#_Toc175227342)

[Educate users: - 15](#_Toc175227343)

[Encrypt Data: - 16](#_Toc175227344)

[Behavior Approach to Cybersecurity 16](#_Toc175227345)

[Behaviour-Based Security:- 16](#_Toc175227346)

[1: - Honeypots: - 16](#_Toc175227347)

[2: - Cisco’s Cyber Threat Defense Solution Architecture: - 16](#_Toc175227348)

[NetFlow: - 16](#_Toc175227349)

[Penetration Testing: - 17](#_Toc175227350)

[1: - Planning: - 17](#_Toc175227351)

[2: - Scanning: - 17](#_Toc175227352)

[3: - Gain access 17](#_Toc175227353)

[4: - Maintain access 18](#_Toc175227354)

[5: -Analysis and reporting 18](#_Toc175227355)

[Impact Reduction: - 18](#_Toc175227356)

[Communicate the issue 18](#_Toc175227357)

[Be sincere and accountable 18](#_Toc175227358)

[Provide the details 18](#_Toc175227359)

[Find the cause 18](#_Toc175227360)

[Apply lessons learned 19](#_Toc175227361)

[Check and check again 19](#_Toc175227362)

[Educate 19](#_Toc175227363)

[Risk Management 19](#_Toc175227364)

[1: - Frame the risk 19](#_Toc175227365)

[2: - Access the risk 19](#_Toc175227366)

[3: - Respond to the risk 19](#_Toc175227367)

[4: - Monitor the risk 19](#_Toc175227368)

Introduction to the Cybersecurity

Cybersecurity   
Phishing  
Breaches

## Type of the Attackers

Organized Hacker

Armatures  
 'script kiddies'

Hackers

## 

Black Hat

White Hat

Gray Hat

# The Cube

The McCumber Cube is a model framework created by John McCumber in 1991 to help organizations establish and evaluate information security initiatives by considering all the related factors that impact them. This security model has three dimensions:

1. The foundational principles for protecting information systems.

(Confidentiality, Integrity, Availability)

1. The protection of information in each of its states.

(Processing, Storage, Transmission)

1. The security measures used to protect data.

(Awareness, training and education, Technology, Policy, and Procedure)

# Malware: -

Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system. Knowing what the different types are and how they spread is key to containing and removing them.

Different types of the malware

## Spyware: -

Designed to track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data, including sensitive personal information such as your online banking details.

## Adware: -

Designed to track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data, including sensitive personal information such as your online banking details.

## Backdoor: -

This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system.

## Ransomware: -

This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you cannot access it.

## Scareware: -

This is a type of malware that uses 'scare’ tactics to trick you into taking a specific action.

## Rootkit: -

This malware is designed to modify the operating system to create a backdoor, which attackers can then use to access your computer remotely. Most rootkits take advantage of software vulnerabilities to gain access to resources that normally shouldn’t be accessible (privilege escalation) and modify system files.

## Virus: -

A virus is a type of computer program that, when executed, replicates and attaches itself to other executable files, such as a document, by inserting its own code. Most viruses require end-user interaction to initiate activation and can be written to act on a specific date or time.

## Trojan Horse: -

This malware carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous. Trojans exploit your user privileges and are most often found in image files, audio files or games.

Unlike viruses, Trojans do not self-replicate but act as a decoy to sneak malicious software past unsuspecting users.

## Worms: -

This is a type of malware that replicates itself in order to spread from one computer to another. Unlike a virus, which requires a host program to run, worms can run by themselves. Other than the initial infection of the host, they do not require user participation and can spread very quickly over the network.

Worms share similar patterns: They exploit system vulnerabilities, they have a way to propagate themselves, and they all contain malicious code (payload) to cause damage to computer systems or networks.

# Different Methods of Infiltration

## Social Engineering : -

Social engineering is the manipulation of people into performing actions or divulging confidential information.  
Some of the common types of attack social engineering attacks

1:- Pretexting  
2:- Tailgating  
3:-Something for Something(quid pro quo)

## Denial-of-Service:-

Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out, even by an unskilled attacker. A DoS attack results in some sort of interruption of network service to users, devices or applications.

## Distributed DOS :-

A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources. For example:

* An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
* The **zombie** computers will constantly scan and infect more hosts, creating more and more zombies.
* When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

## Botnet: -

A bot computer is typically infected by visiting an unsafe website or opening an infected email attachment or infected media file. **A botnet is a group of bots**, connected through the Internet, that can be controlled by a malicious individual or group. It can have tens of thousands, or even hundreds of thousands, of bots that are typically controlled through a command and control server.

These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute-force password attacks. Cybercriminals will often rent out botnets to third parties for nefarious purposes.

## On-Path-Attacks: -

On-path attackers intercept or modify communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices.  
This type of attack is also referred to as a **man-in-the-middle**or **man-in-the-mobile** attack.

### Man-In-The-Middle (MITM)

This attack happens when a cybercriminal takes control of a device without the user’s knowledge. With this level of access, an attacker can intercept and capture user information before it is sent to it’s intended destination. These type of attacks are often used ­­­­to steal financial information.  
 There are many types of malware that possess MITM attack capabilities.

### Man-In-The-Mobile(MITMO)

It is a type of attack used to take control over a user’s mobile device. When infected, the mobile device is instructed to exfiltrate user-sensitive information and send it to the attackers. ZEUS is one of the example of malware package with MITOM capabilities. It allows attackers to capture two-step verification SMS messages that are sent to users.

SEO Poisoning: -  
 **Search Engine Optimization**  is about improving an organization’s website so that it gains greater visibility in search engine results.

While many legitimate companies specialize in optimizing w2ebsittes to better position them, attackers take advantage of popular search terms and use SEO to push malicious sites higher up the ranks of search results. This technique is called SEO Poisoning.

## Wi-Fi Password Cracking: -

Someone ask for private wifi password pretending to be friend and also want to check its network connection.

### Password Spraying: -

This technique attempts to gain access to a system by ‘spraying’ a few commonly used passwords across a large number of accounts.

### Dictionary Attacks: -

A hacker systematically tries every word in a dictionary or a list of commonly used words as a password in an attempt to break into a password-protected account.

### Brute-Force Attacks: -

The simplest and most commonly used way of gaining access to a password-protected site, brute-force attacks see an attacker using all possible combinations of letters, numbers and symbols in the password space until they get it right.

### Rainbow Attacks: -

Passwords in a computer system are not stored as plain text, but as hashed values (numerical values that uniquely identify data). **A rainbow table** is a large dictionary of precomputed hashes and the passwords from which they were calculated.

Unlike a brute-force attack that has to calculate each hash, a rainbow attack compares the hash of a password with those stored in the rainbow table. When an attacker finds a match, they identify the password used to create the hash.

### Traffic Interception:-

Plain text or unencrypted passwords can be easily read by other humans and machines by intercepting communications.

## Advanced Persistent Threats: -

Attackers also achieve infiltration through advanced persistent threats (APTs) — a multi-phase, long term, stealthy and advanced operation against a specific target. For these reasons, an individual attacker often lacks the skill set, resources or persistence to perform APTs.

Due to the complexity and the skill level required to carry out such an attack, an APT is usually well-funded and typically targets organizations or nations for business or political reasons.

Its main purpose is to deploy customized malware on one or more of the target’s systems and remain there undetected.

# Security Vulnerability and Exploits:-

It is a kind of a software and hardware defect. A program written to take advantage of a known vulnerability is referred to as an ***exploit*.** A cybercriminal can use an exploit against the vulnerability to carry out an attack , the goal of which is to gain access to the system , the data it hosts or a specific resource.

## Hardware Vulnerabilities: -

Hardware vulnerabilities are most often the result of hardware design flaws. For example, the type of memory called RAM consists of lots of capacitors (a component which can hold an electrical charge) installed very close to one another. However, it was soon discovered that, due to their close proximity, changes applied to one of these capacitors could influence neighbor capacitors. Based on this design flaw, an exploit called Rowhammer was created. By repeatedly accessing (hammering) a row of memory, the Rowhammer exploit triggers electrical interferences that eventually corrupt the data stored inside the RAM.

## Software Vulnerabilities: -

Software vulnerabilities are usually introduced by errors in the operating system or application code.  
Most software security vulnerabilities fall into several main categories.

### Buffer Overflow: -

Buffers are memory areas allocated to an application. A vulnerability occurs when data is written beyond the limits of a buffer. By changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes. This can lead to a system crash or data compromise, or provide escalation of privileges.

### Non-Validated Inputs: -

Programs often require data input, but this incoming data could have malicious content, designed to force the program to behave in an unintended way.

### Race Conditions: -

This vulnerability describes a situation where the output of an event depends on ordered or timed outputs. A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or at the proper time.

### Weaknesses in Security Practices: -

Systems and sensitive data can be protected through techniques such as authentication, authorization and encryption. Developers should stick to using security techniques and libraries that have already been created, tested and verified and should not attempt to create their own security algorithms. These will only likely introduce new vulnerabilities.

### Access Control Problems: -

Access control is the process of controlling who does what and ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls.

# Methods To Safeguard Your Online Privacy

## Two Factor Authentication:-

## Open Authorization:-

Open authorization (OAuth) is an open standard protocol that allows you to use your credentials to access third-party applications without exposing your password.

## Don’t Get Spoofed : -

A simple forged or spoofed email can lead to a massive data breach and perhaps cause irreversible damage to your reputation.

## Email and Web Browser Privacy: -

These problems can be minimized by enabling the in-private browsing mode on your web browser. Many of the most commonly used web browsers have their own name for private browser mode:

# Cybersecurity Devices and Technologies

## Firewalls: -

### Network Layer Firewall :-

This filters communications based on source and destination IP addresses.

### Transport Layer Firewall: -

Filters communications based on source and destination data ports, as well as connection states.

### Application Layer Firewall: -

Filters communications based on an application, program or service.

### Context Aware Layer Firewall: -

Filters communications based on the user, device, role, application type and threat profile.

### Proxy Server: -

Filters web content requests like URLs, domain names and media types.

### Reverse Proxy Server: -

Placed in front of web servers, reverse proxy servers protect, hide, offload and distribute access to web servers.

### Network Address Translation(NAT) Firewall: -

This firewall hides or masquerades the private addresses of network hosts.

### Host-based Firewall: -

Filters ports and system service calls on a single computer operating system.

## Port Scanning: -

In networking, each application running on a device is assigned an identifier called a port number. This port number is used on both ends of the transmission so that the right data is passed to the correct application. Port scanning is a process of probing a computer, server or other network host for open ports. It can be used maliciously as a reconnaissance tool to identify the operating system and services running on a computer or host, or it can be used harmlessly by a network administrator to verify network security policies on the network.

## Intrusion Detection and Prevention Systems: -

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are security measures deployed on a network to detect and prevent malicious activities.

### Intrusion detection systems (IDSs) :-

It can be a dedicated network device or one of several tools in a server , firewall or even a host computer operating system, such as windows or Linux, that scans data against a database of rules or attack signature , looking for malicious traffic.  
 If a match is detected , the IDS will log the detection and create an alert for a network administrator . It will not take actions and therefore it will not take action and therefore it will not prevent attacks from happening . The job of the IDS is to detect , log and report.

The scanning performed by the IDS slow down the network( Known as Latency). To prevent network delay, an IDS is usually placed offline , separated from regular network traffic. Data is copied or mirrored by a switch and then forward to the IDS for Offline detection.

### Intrusion prevention systems (IPSs)

An IPS can block or deny traffic based on a positive rule or signature match. One of the most well-known IPS/IDS system is Snort. The commercial version of snort Cisco’s Sourcefire. It can perform real-time traffic and port analysis , logging , content searching and matching , as well as detect probes, attacks and executes port scans. It also integrate with other third-party tools for reporting, performing and log analysis.

## Real Time Detection: -

Detecting attacks in real time requires actively scanning for attacks using firewall and IDS/IPS network devices. Next generation client and server malware detection with connections to online global threat centers must also be used. Today, active scanning devices and software must detect network anomalies using context-based analysis and behavior detection.

DDoS is one of the biggest attack threats requiring real-time detection and response. For many organizations, regularly occurring DDoS attacks cripple Internet servers and network availability. These attacks are extremely difficult to defend against because the attacks originate from hundreds, even thousands, of zombie hosts, and the attacks appear as legitimate traffic.

## Protecting Against Malware: -

One way of defending against zero-day attacks and advanced persistent threats (APTs) is to use an enterprise-level advanced malware detection solution, like Cisco’s **Advanced Malware Protection (AMP) Threat Grid**.

Thisis client/server software that can be deployed on host endpoints, as a standalone server or on other network security devices. It analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts for behaviors that reveal an APT. This approach provides a global view of malware attacks, campaigns and their distribution.

Different teams in the threat Grid: -

### Secure Operations Center Team : -

The Threat Grid allows the Cisco Secure Operations Center team to gather more accurate, actionable data.

### Incidence Response Team: -

The Incidence Response team therefore has access to forensically sound information from which it can more quickly analyze and understand suspicious behaviors.

### Threat Intelligence Team:-

Using this analysis, the Threat Intelligence team can proactively improve the organization’s security infrastructure.

### Security Infrastructure Engineering Team: -

Overall, the Security Infrastructure Engineering team is able to consume and act on threat information faster, often in an automated way.

## Security Best Practices : -

### Perform a risk assessment: -

Knowing and understanding the value of what you are protecting will help to justify security expenditures.

### Create a security policy: -

Create a policy that clearly outlines the organization’s rules, job roles, and responsibilities and expectations for employees.

### Physical security measures: -

Restrict access to networking closets and server locations, as well as fire suppression.

### Human resource security measures: -

Background checks should be completed for all employees.

### Perform and test backups: -

Back up information regularly and test data recovery from backups.

### Maintain security patches and updates: -

Regularly update server, client and network device operating systems and programs.

### Employee access control: -

Configure user roles and privilege levels as well as strong user authentication.

### Regular test incident response: -

Employ an incident response team and test emergency response scenarios.

### Implement a network monitoring analytics and management tools: -

Choose a security monitoring solution that integrates with other technologies.

### Implement network security devices: -

Use next generation routers, firewalls and other security appliances.

### Implement a comprehensive endpoint security solution: -

Use enterprise level antimalware and antivirus software.

### Educate users: -

Provide training to employees in security procedures.  
One of the most widely known and respected organizations for cybersecurity training is the SANS Institute. Click [here](https://www.sans.org/about/) to learn more about SANS and the types of training and certifications they offer.

### Encrypt Data: -

Encrypt all sensitive organizational data, including email.

# Behavior Approach to Cybersecurity

## Behaviour-Based Security:-

Behavior-based security is a form of threat detection that involves capturing and analyzing the flow of communication between a user on the local network and a local or remote destination. Any changes in normal patterns of behavior are regarded as anomalies and may indicate an attack.

Some of the behavior-based detection tools: -

### 1: - Honeypots: -

A honeypot is a behavior-based detection tool that lures the attacker in by appealing to their predicted pattern of malicious behavior. Once the attacker is inside the honeypot, the network administrator can capture, log and analyze their behavior so that they can build a better defense.

### 2: - Cisco’s Cyber Threat Defense Solution Architecture: -

This security architecture uses behavior-based detection and indicators to provide greater visibility, context and control. The aim is to know who is carrying out the attack, what type of attack they are performing and where, when and how the attack is taking place. This security architecture uses many security technologies to achieve this goal.

## NetFlow: -

NetFlow technology is used to gather information about data flowing through a network, including who and what devices are in the network, and when and how users and devices access the network.  
NetFlow is an important component in behavior-based detection and analysis. Switches, routers and firewalls equipped with NetFlow can report information about data entering, leaving and traveling through the network.

## Penetration Testing: -

Penetration testing, commonly known as pen testing, is the act of assessing a computer system, network or organization for security vulnerabilities. A pen test seeks to breach systems, people, processes and code to uncover vulnerabilities which could be exploited. This information is then used to improve the system’s defenses to ensure that it is better able to withstand cyber attacks in the future.

The five-step pen test process is given below

### 1: - Planning: -

The pen tester gathers as much information as possible about a target system or network, its potential vulnerabilities and exploits to use against it. This involves conducting passive or active reconnaissance (foot printing) and vulnerability research.

### 2: - Scanning: -

The pen tester carries out active reconnaissance to probe a target system or network and identify potential weaknesses which, if exploited, could give an attacker access. Active reconnaissance may include:

* port scanning to identify potential access points into a target system
* vulnerability scanning to identify potential exploitable vulnerabilities of a particular target
* establishing an active connection to a target (enumeration) to identify the user account, system account and admin account.

### 3: - Gain access

The pen tester will attempt to gain access to a target system and sniff network traffic, using various methods to exploit the system including:

* launching an exploit with a payload onto the system
* breaching physical barriers to assets
* social engineering
* exploiting website vulnerabilities
* exploiting software and hardware vulnerabilities or misconfigurations
* breaching access controls security
* cracking weak encrypted Wi-Fi.

### 4: - Maintain access

The pen tester will maintain access to the target to find out what data and systems are vulnerable to exploitation. It is important that they remain undetected, typically using backdoors, Trojan horses, rootkits and other covert channels to hide their presence.

When this infrastructure is in place, the pen tester will then proceed to gather the data that they consider valuable.

### 5: -Analysis and reporting

The pen tester will provide feedback via a report that recommends updates to products, policies and training to improve an organization’s security.

## Impact Reduction: -

While most organizations today are aware of common security threats and put considerable effort into preventing them, no set of security practices is foolproof. Therefore, organizations must be prepared to contain the damage if a security breach occurs. And they must act fast!

Actions organizations should take when a security breach is identified.

### Communicate the issue

Communication creates transparency, which is critical in this type of situation.

Internally, all employees should be informed and a clear call to action communicated.

Externally, all clients should be informed through direct communication and official announcements.

### Be sincere and accountable

Respond to the breach in an honest and genuine way, taking responsibility where the organization is at fault.

### Provide the details

Be open and explain why the breach took place and what information was compromised. Organizations are generally expected to take care of any client costs associated with identity theft services required as a result of a security breach.

### Find the cause

Take steps to understand what caused and facilitated the breach. This may involve hiring forensics experts to research and find out the details.

### Apply lessons learned

Make sure that any lessons learned from forensic investigations are applied to prevent similar breaches from happening in the future.

### Check and check again

Attackers will often attempt to leave a backdoor to facilitate future breaches. To prevent this from happening, make sure that all systems are clean, no backdoors are installed and nothing else has been compromised.

### Educate

Raise awareness, train and educate employees, partners and clients on how to prevent future breaches.

## Risk Management

Risk management is the formal process of continuously identifying and assessing risk in an effort to reduce the impact of threats and vulnerabilities. You cannot eliminate risk completely but you can determine acceptable levels by weighing up the impact of a threat with the cost of implementing controls to mitigate it***. The cost of a control should never be more than the value of the asset you are protecting.***

Lets discuss the risk management process

### 1: - Frame the risk

Identify the threats that increase risk. Threats may include processes, products, attacks, potential failure or disruption of services, negative perception of an organization's reputation, potential legal liability or loss of intellectual property.

### 2: - Access the risk

Determine the severity that each threat poses. For example, some threats may have the potential to bring an entire organization to a standstill, while other threats may be only minor inconveniences. Risk can be prioritized by assessing financial impact (a quantitative analysis) or scaled impact on an organization's operation (a qualitative analysis).

### 3: - Respond to the risk

Develop an action plan to reduce overall organization risk exposure, detailing where risk can be eliminated, mitigated, transferred or accepted.

### 4: - Monitor the risk

Continuously review any risk reduced through elimination, mitigation or transfer actions. Remember, not all risks can be eliminated, so you will need to closely monitor any threats that have been accepted.

# Tools for Incident Detection and Prevention:-

## 1: - SIEM

A Security Information and Event Management (SIEM) system collects and analyzes security alerts, logs and other real-time and historical data from security devices on the network to facilitate early detection of cyber-attacks.

## 2: - DLP

A Data Loss Prevention (DLP) system is designed to stop sensitive data from being stolen from or escaping a network. It monitors and protects data in three different states: data in use (data being accessed by a user), data in motion (data traveling through the network) and data at rest (data stored in a computer network or device).

### Cyber Attacks :-

Cyber attacks are deliberate attempts by individuals or groups to breach the security of a computer system, network, or digital device to steal, alter, or destroy data, disrupt services, or gain unauthorized access to systems. Cyber attacks can target individuals, businesses, governments, or entire infrastructures and can take many forms.

**Cyber Kill Chain: -**

The Cyber Kill Chain is a model developed by Lockheed Martin to outline the stages of a cyber attack and help organizations understand, detect, and respond to threats. It is often used in cybersecurity to break down an attack into manageable stages, allowing defenders to identify and disrupt the attack before it can cause significant harm**.**

1. **Reconnaissance:** The attacker starts by gathering information about the target. This is like doing research to find out where the target's weaknesses are.
2. **Weaponization:** The attacker then creates a malicious tool or code that can exploit the target's weaknesses. This is like building a tool to break into a house.
3. **Delivery:** The attacker sends the malicious tool to the target. This could be through an email attachment or a harmful link.
4. **Exploitation:** When the target opens the malicious tool or link, it activates and starts causing harm. This is like the attacker breaking into the house using the tool.
5. **Installation:** The attacker installs malicious software on the target's system to stay hidden and keep control. This is like setting up a hidden camera in the house to keep an eye on things.
6. **Command and Control:** The attacker communicates with the installed malware to control it and issue commands. This is like the attacker using a remote control to manage the hidden camera.
7. **Actions on Objectives:** Finally, the attacker achieves their goal, such as stealing data or damaging systems. This is like the attacker finding and taking valuable items from the house.

By understanding these steps, organizations can better protect themselves by stopping the attack at any stage.

What are different hashes?

Hashes are used to convert data into a fixed-size string of characters, which is usually a digest that represents the original data. Different types of hash functions are used for various purposes in computing and cybersecurity. Here are some common types:

**1. MD5 (Message Digest Algorithm 5)**

* **Output Length:** 128 bits (16 bytes)
* **Usage:** Commonly used for checksums and verifying data integrity. However, it's considered weak due to vulnerabilities that allow for hash collisions (two different inputs producing the same hash).
* **Example Hash:** d41d8cd98f00b204e9800998ecf8427e

**2. SHA-1 (Secure Hash Algorithm 1)**

* **Output Length:** 160 bits (20 bytes)
* **Usage:** Used for digital signatures and certificates. It has known vulnerabilities and is not recommended for security-sensitive applications.
* **Example Hash:** 5baa61e4c9b93f3f0682250b6cf8331b6d3c8c0a

**3. SHA-2 (Secure Hash Algorithm 2)**

* **Output Length:** Includes several variants, such as SHA-224, SHA-256, SHA-384, and SHA-512.
* **Usage:** Widely used in security protocols, including SSL/TLS and cryptocurrencies. SHA-256 is especially popular.
* **Example Hash (SHA-256):** e99a18c428cb38d5f260853678922e03abd73f01b6d4a4d5d1e4f51f8d35a7e0

**4. SHA-3 (Secure Hash Algorithm 3)**

* **Output Length:** Includes variants such as SHA3-224, SHA3-256, SHA3-384, and SHA3-512.
* **Usage:** The latest member of the Secure Hash Algorithm family, designed to provide higher security margins and different internal structure compared to SHA-2.
* **Example Hash (SHA3-256):** 6dcd4ce23d88e2f4c27f7d70fd679e68f4c5c6a8b9b9e9c89f8e8d59e8a72f07

In cybersecurity, **artifacts** are bits of evidence or data left behind by activities on a computer or network. They help investigators understand what happened during a security incident. Here’s a simple breakdown with examples:

**1. Log Files**

* **Definition:** Records of activities on a system or network.
* **Example:** A log file showing failed login attempts can indicate someone trying to break into an account.

**2. File Metadata**

* **Definition:** Information about files, like when they were created or last modified.
* **Example:** A file’s creation date might help find out when malware was added to a system.

**3. Network Traffic**

* **Definition:** Data sent over a network, which can reveal unusual activity.
* **Example:** Detecting a lot of data being sent to an unfamiliar website might suggest data theft.

**4. Registry Entries (Windows)**

* **Definition:** Settings and information stored in the Windows Registry.
* **Example:** Registry entries showing a new, unexpected startup program could indicate malware.

**5. File System Artifacts**

* **Definition:** Data about files and directories on a disk.
* **Example:** Finding hidden files that were recently added could point to a hacker’s tools.

**6. Temporary Files**

* **Definition:** Files created temporarily by programs or systems.
* **Example:** A temporary file containing a suspicious script might show that malware was executed recently.

**7. Browser Artifacts**

* **Definition:** Data from web browsers, like cookies or history.
* **Example:** Browser history showing visits to strange or suspicious sites might indicate a phishing attack.

**8. System Dumps**

* **Definition:** Snapshots of a system’s memory taken at a specific time.
* **Example:** A system dump revealing strange processes running could help identify malware.

**9. Configuration Files**

* **Definition:** Files that store system or application settings.
* **Example:** A configuration file changed to include new, unauthorized settings might be used by an attacker to maintain control.

**10. Executable Files**

* **Definition:** Files that run programs on a computer.
* **Example:** Finding a new executable file that you didn’t install could indicate malware.

In short, artifacts are clues left behind by digital activities, and analyzing them helps understand and address security issues.

In cybersecurity, various types of rules and frameworks are used to detect and respond to threats. Here’s a simple explanation of different rules and frameworks:

**1. SNORT Rules**

* **Definition:** SNORT is an open-source intrusion detection and prevention system (IDS/IPS). SNORT rules are used to define patterns and behaviors that indicate malicious activity.
* **Format:** Rules are written in a specific syntax that includes conditions and actions. For example, a SNORT rule might look for specific patterns in network traffic and trigger an alert if those patterns are detected.
* **Example:**

css

Copy code

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 80 (msg:"Possible SQL Injection"; content:"union select"; nocase; sid:1000001;)

This rule generates an alert if SQL injection patterns are detected in HTTP traffic.

**2. YARA Rules**

* **Definition:** YARA is a tool used for identifying and classifying malware by defining patterns in files or memory. YARA rules are used to match specific byte patterns or strings in files.
* **Format:** Rules are written in a flexible syntax that includes strings and conditions to identify specific file characteristics.
* **Example:**

bash

Copy code

rule ExampleRule

{

strings:

$a = "malicious\_code"

condition:

$a

}

This YARA rule detects files containing the string "malicious\_code."

**3. SIGMA Rules**

* **Definition:** SIGMA is an open standard for writing and sharing detection rules for log-based data. SIGMA rules help identify suspicious activities in log files and other security data.
* **Format:** Rules are written in YAML format and focus on log events, specifying conditions to detect specific patterns or behaviors.
* **Example:**

yaml

Copy code

title: Example Detection

logsource:

category: windows

product: windows

detection:

selection:

EventID: 4688

NewProcessName: '\*malicious.exe'

condition: selection

This SIGMA rule detects if a process named "malicious.exe" is created on a Windows system.

**4. SURICATA Rules**

* **Definition:** Suricata is an open-source IDS/IPS similar to SNORT. Suricata rules are used to detect and block malicious traffic on the network.
* **Format:** Suricata rules are similar to SNORT rules, with a focus on network traffic and behavior.
* **Example:**

css

Copy code

alert http $EXTERNAL\_NET any -> $HOME\_NET 80 (msg:"HTTP GET Request"; http.method; content:"GET"; sid:1000002;)

This rule triggers an alert for HTTP GET requests in network traffic.

**5. BALE (Behavior Analysis and Learning Engine) Rules**

* **Definition:** BALE is a behavior-based detection system. BALE rules are used to identify anomalous behavior patterns rather than specific signatures.
* **Format:** Rules focus on detecting deviations from normal behavior, rather than looking for known patterns or strings.
* **Example:** A BALE rule might detect unusual patterns in file access or network traffic that deviate from the established baseline behavior.

**Key Differences:**

* **SNORT and Suricata:** Focus on network traffic and use similar rule formats.
* **YARA:** Used for file and memory analysis, focusing on specific byte patterns or strings.
* **SIGMA:** Focuses on log-based data and is written in YAML format.
* **BALE:** Uses behavior-based rules to detect anomalies rather than specific patterns.

Each type of rule or framework serves a different purpose in the cybersecurity landscape, allowing for diverse approaches to threat detection and response.

SOAR

**SIEM** stands for **Security Information and Event Management**. It's a type of software solution used in cybersecurity to provide real-time analysis, monitoring, and management of security events and incidents across an organization's IT infrastructure. SIEM systems collect and aggregate log data from various sources, such as network devices, servers, and applications, and analyze this data to detect and respond to security threats.

**Key Functions of SIEM:**

1. **Data Collection and Aggregation:**
   * **Description:** SIEM systems collect log and event data from multiple sources across the network, including servers, firewalls, and security devices.
   * **Example:** Gathering logs from a web server, database, and network firewall into a centralized system.
2. **Normalization:**
   * **Description:** Converts collected data into a consistent format to make it easier to analyze.
   * **Example:** Converting log entries from different devices into a standardized format.
3. **Correlation:**
   * **Description:** Analyzes data from multiple sources to identify patterns and relationships that could indicate security threats.
   * **Example:** Correlating failed login attempts across multiple systems to identify a potential brute-force attack.
4. **Alerting:**
   * **Description:** Generates alerts based on predefined rules or anomalies detected during data analysis.
   * **Example:** Alerting security teams when suspicious behavior, such as unusual login patterns, is detected.
5. **Analysis and Reporting:**
   * **Description:** Provides tools for in-depth analysis of security events and generates reports for compliance and auditing.
   * **Example:** Producing a report on recent security incidents and trends for management review.
6. **Incident Response:**
   * **Description:** Facilitates the response to security incidents by providing actionable insights and integration with other security tools.
   * **Example:** Triggering automated responses or workflows to contain and mitigate identified threats.
7. **Compliance Monitoring:**
   * **Description:** Helps ensure adherence to regulatory requirements by tracking and documenting security events and controls.
   * **Example:** Generating compliance reports for standards like GDPR, HIPAA, or PCI-DSS.

**Benefits of SIEM:**

* **Enhanced Visibility:** Provides a comprehensive view of security events across the entire organization.
* **Improved Threat Detection:** Detects potential threats through data correlation and analysis.
* **Faster Incident Response:** Enables quicker identification and response to security incidents.
* **Compliance Support:** Assists in meeting regulatory requirements and generating necessary reports.
* **Centralized Management:** Streamlines security monitoring and management through a single platform.

**Example of SIEM in Action:**

1. **Log Collection:** A SIEM system collects logs from a company's firewall, web server, and user workstations.
2. **Correlation:** The system detects a pattern where multiple failed login attempts are followed by a successful login from an unusual location.
3. **Alerting:** An alert is generated to notify the security team of a potential security breach.
4. **Response:** The security team investigates the alert, determines that it’s a valid threat, and takes action to secure the system.

Overall, SIEM systems are critical for managing and securing an organization's IT environment by providing comprehensive visibility and actionable intelligence to address security challenges effectively.