WEEK-1

CYBER SECURITY

BASICS:

- **Data** can be defined as a representation of **facts, concepts, or instructions in a formalized manner**, which should be suitable for **communication, interpretation, or processing by human or electronic machine**.
- Data is represented with the help of characters such as alphabets (A-Z, a-z), digits (0-9) or special characters (+, -, /, *, <,>, = etc.).
- **Information** is organized or classified data, which has some meaningful values for the receiver.
- Information is the processed data on which decisions and actions are based.
- For the decision to be meaningful, the processed data must qualify for the following characteristics −
  - **Timely** − Information should be available when required.
  - **Accuracy** − Information should be accurate.
  - **Completeness** − Information should be complete.
- Data processing is the re-structuring or re-ordering of data by people or machine to increase their usefulness and add values for a particular purpose.

- A **Computer network** is a system in which multiple computers are connected to each other to **share information and resources.**

A computer network can be categorized by their size. A **computer network** is mainly of **three types**:

- LAN(Local Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN (Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network **provides higher security**.

MAN (Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network (LAN).

WAN (Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education

The advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.

- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.
- **A person who uses the Internet**, Sometimes, person can be tracked on the Internet by hackers or unauthorize persons, they can be harmful to you by stealing your personal information.
- If you are **spending your more time on the Internet**, so it will be easier for hackers to find your personal information through various means.
- To **run business** without as much fear of being caught, the web deep, and the hidden places on the internet can also be a place for criminals. Additionally, there are several people that provide criminals more ways to solicit their goods.
- There are **various malicious users** and computer hackers that can steal your personal information and hack accounts, which can be used for identity theft and can be harmful to you personally.
- As the **Internet connects all computers to each other**, so hackers can quickly identify what computers are vulnerable to attack by scanning millions of computers.
- Additionally, the Internet also enables students to find others to do their homework and offers ways to cheat on their studies.
- **The frequently use of the Internet may infect your system from viruses** that can damage your valuable data, which is difficult to recover. These viruses enter into the system through USBs, CIDs, and the Internet. Also, because of viruses, your system can become totally worthless.

NETWORK SECURITY:

- Network security consists of the **policies, processes and practices** adopted to **prevent, detect and monitor unauthorized access, misuse, modification, or denial** of a computer **network** and network-**accessible resources.**
- Network security is a **set of technologies** that **protects** the usability and integrity of a company's infrastructure by preventing the entry or proliferation within a network of a wide variety of potential threats.
- Network security is any activity designed to protect the usability and integrity of your network and data.
    - It includes both hardware and software technologies
    - It targets a variety of threats
    - It stops them from entering or spreading on your network
    - Effective network security manages access to the network

- **Why network security?**
  - In today's hyper-connected world, network security presents a greater challenge as more business applications move to private and public clouds. Moreover, the applications themselves now tend to be virtualized and distributed across many locations, some of which are outside the physical control of IT security teams. With the number of attacks on companies climbing ever higher, protecting network traffic and infrastructure is critical.
- **Benefits of network security**
  - Network security is key to an organization's ability to deliver products and services to customers and employees. From online stores to enterprise applications to remote desktops, protecting apps and data on the network is essential to advancing the business, to say nothing of protecting an organization's reputation. In addition, effective network security can improve network performance by eliminating downtime due to successful attacks.
- **How does network security works?**
  - The elements of a complete, multi-layered security architecture that implements network security across an organization fall into two general categories: access control and threat control.
  - **AccessControl**
    Network security starts with access control. If bad actors gain access to a network, they can surveil traffic and map infrastructure. Once they have mapped infrastructure and applications, they can launch a DDoS attack or insert malware. Access control restricts the movement of bad actors throughout the network.
  - **ThreatControl**
    Even with access control in place, problems can arise. For instance, a bad actor may compromise an employee's credentials to gain entry. Thus the need for threat control, which operates on traffic that is already permitted. Threat control prevents the actions of bad actors from doing damage within the network.
- **What are the key tools of network security?**
  - A multi-layered approach to network security implements controls at numerous points within a network to provide comprehensive access control and threat control.
  - **Firewall :** A firewall establishes a barrier between the trusted and the untrusted areas of a network. Thus, a firewall performs access control and macro-segmentation based on IP subnets. The same firewall may also perform more granular segmentation, known as micro-segmentation.
  - **Load Balancer:** A load balancer distributes load based on metrics. By implementing specific mitigation techniques, a load balancer can go beyond traditional load balancing to provide the capability to absorb certain attacks, such as a volumetric DDoS attack.
  - **IDS/IPS :** The classic IDS/IPS is deployed behind a firewall and provides protocol analysis and signature matching on various parts of a data packet. Protocol analysis is a compliance check against the publicly declared specification of the protocol. Signature matching prevents known attacks such as an SQL injection.

- **Sandbox:** A sandbox is similar to an IDS/IPS, except that it does not rely on signatures. A sandbox can emulate an end-system environment and determine if a malware object is trying, for example, to execute port scans.
- **NTA/NDR:** NTA/NDR looks directly at traffic (or traffic records such as NetFlow) and uses machine learning algorithms and statistical techniques to evaluate anomalies and determine if a threat is present. First, NTA/NDR tries to determine a baseline. With a baseline in place, it identifies anomalies such as traffic spikes or intermittent communication.

DAY-1/1

What is Cyber Security?

• The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity.

• We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information.

• In some cases, it is also called electronic information security or information technology security.

- Cybersecurity is the ongoing effort to protect individuals, organizations and governments from digital attacks by protecting networked systems and data from unauthorized use or harm.

➢ **The three levels of protection**.

1. **Personal On a personal level**, you need to safeguard your identity, your data, and your computing devices.
2. **Organizational At an organizational level**, it is everyone responsibility to protect the organization‘s reputation, data and customers.
3. **Government As more digital information** is being gathered and shared, its protection becomes even more vital at the **government level**, where national security, economic stability and the safety and wellbeing of citizens are at stake.

Personal data:

➢ Protecting Your Personal Data Personal data is any information that can be used to identify you, and it can exist both offline and online

The difference between your offline and online identity.

1. Offline identity

Your offline identity is the real-life persona that you present on a daily basis at home, at school or at work. As a result, family and friends know details about your personal life, including your full name, age and address.

It‘s important not to overlook the importance of securing your offline identity. Identity thieves can easily steal your data from right under your nose when you‘re not looking!

2. Online identity

Your online identity is not just a name. It‘s who you are and how you present yourself to others online. It includes the username or alias you use for your online accounts, as well as the social identity you establish and portray on online communities and websites. You should take care to limit the amount of personal information you reveal through your online identity.

Many people think that if they don‘t have any social media or online accounts set up, then they don‘t have an online identity. This is not the case. If you use the web, you have an online identity.

Your Online Identity

It’s your first day on the job, and it’s time to choose a username for your online identity

Which of the following options would you choose?

This is your first chance to gain some valuable defender points at eLearning company @Apollo, so take your time and think carefully before making your choices.

- ✓ j.doe12
- ✓ jane.doe
- ✓ jdoe
- ✓ jdoe.IT
- ✓ jdoe1990

That’s right, well done! You sure know how to keep your online identity safe.

When choosing a username, it‘s important not to reveal any personal information. It should be something appropriate and respectful and should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.

Some other useful tips to help you generate your username:

- ✓ Don‘t use your full name or parts of your address or phone number.
- ✓ Don‘t use your email username.
- ✓ Don‘t use the same username and password combination, especially on financial accounts.
- ✓ Don‘t choose a super-odd username and then reuse it again and again — it makes you easier
- ✓ to track.
- ✓ Don‘t choose a username that gives clues to your passwords such as a series of
- ✓ numbers/letters or the first part of a two-part phrase, such as knock-knock or starlight, or the
- ✓ department in which you work, such as IT.
- ✓ Do choose a username that‘s appropriate for the type of account, i.e., business, social or personal.

Your Data

Personal data describes any information about you, including your name, social security number, driver license number, date and place of birth, your mother‘s maiden name, and even pictures or messages that you exchange with family and friends. Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy and potentially causing serious damage to your reputation.

How hackers can get their hands on your personal data.

1. Medical records

Every time you visit the doctor, personal information regarding your physical and mental health and wellbeing is added to your electronic health records (EHRs). Since the majority of these records are saved online, you need to be aware of the medical information that you share. And these records go beyond the bounds of the doctor‘s office. For example, many fitness trackers collect large amounts of clinical data such as your heart rate, blood pressure and blood sugar levels, which is transferred, stored and displayed via the cloud. Therefore, you should consider this data to be part of your medical records.

2. Education records

Educational records contain information about your academic qualifications and achievements. However, these records may also include your contact information, attendance records,disciplinary reports, health and immunization records as well as any special education records including individualized education programs (IEPs).

3. Employment and financial records

Employment data can be valuable to hackers if they can gather information on your past employment, or even your current performance reviews.

Your financial records may include information about your income and expenditure. Your tax records may include paychecks, credit card statements, your credit rating and your bank account details. All of this data, if not safeguarded properly, can compromise your privacy and enable cybercriminals to use your information for their own gain.

Where Is Your Data?

This has got you thinking. Only yesterday, you shared a couple of photos of your first day on the job with a few of your close friends. But that should be OK, right? Let's see..

1. You took some photos at work on your mobile phone. Copies of these photos are now available on your mobile device.
2. You shared these with five close friends, who live in various locations across the world.
3. All of your friends downloaded the photos and now have copies of your photos on their devices.
4. One of your friends was so proud that they decided to post and share your photos online. The photos are no longer just on your device. They have in fact ended up on servers located in different parts of the world and people whom you don't even know now have access to your photos.

What's More...

This is just one example that reminds us that every time we collect or share personal data, we should consider our security. There are different laws that protect your privacy and data in your country. But do you know where your data is?

1. Following an appointment, the doctor will update your medical record. For billing purposes, this information may be shared with the insurance company. In such cases, your medical record, or part of it, is now accessible at the insurance company.
2. Store loyalty cards may be a convenient way to save money on your purchases. However, the store is using this card to build a profile of your purchasing behavior, which it can then use to target you with special offers from its marketing partners.

Smart Devices

- Consider how often you use your computing devices to access your personal data. Unless you have chosen to receive paper statements, you probably access digital copies of bank account statements via your bank‘s website. And when paying a bill, it‘s highly likely that you‘ve transferred the required funds via a mobile banking app.
- But besides allowing you to access your information, computing devices can now also generate information about you.
- Wearable technologies such as smartwatches and activity trackers collect your data for clinical research, patient health monitoring, and fitness and wellbeing tracking. As the global fitness tracker market grows, so also does the risk to your personal data.

It might seem that information available online is free. But is privacy the price we pay for this digital convenience?

For example, social media companies generate the majority of their income by selling targeted advertising based on customer data that has been mined using algorithms or formulas. Of course, these companies will argue that they are not selling customer data, but sharing customer data with their marketing partners.
You can make up your own mind!

What Do Hackers Want?

So, with all this information about you available online, what do hackers want? Of course, they want your money.
Can you think of an example that you have experienced yourself or that you have heard or read about, where cybercriminals have accessed or tried to access financial information online?
Ans: A cybercriminal can take advantage of your relationships, accessing your online accounts and appealing to your good nature to try and trick you into wiring money to your friends or family in a time of need.
For example, there have been many reported cases of hackers impersonating family members and sending messages stating that they need money wired in order to get home from abroad after losing their wallets.
And while you may think that your frequent flyer air miles are not valuable to cybercriminals, think again. In 2015, cybercriminals hacked approximately 10,000 American Airlines and United accounts, booking free flights and upgrades using stolen credentials. Even though the frequent flyer miles were returned to the customers by the airlines, this example demonstrates the value of your login credentials.
Cybercriminals are certainly very imaginative when it comes to gaining access to your money. But that's not all they are after — they could also steal your identity and ruin your life.

Identity Theft

Not content with stealing your money for short-term financial gain, cybercriminals are invested in the long-term gain of identity theft.
Two examples of how they might do this.

1. Medical theft

Rising medical costs have led to an increase in medical identity theft, with cybercriminals stealing medical insurance to use the benefits for themselves. Where this happens, any medical procedures carried out in your name will then be saved in your medical records.

2. Banking

Stealing private data can help cybercriminals access bank accounts, credit cards social profiles and other online accounts. Armed with this information, an identity thief could file a fake tax return and collect the refund. They could even take out loans in your name and ruin your credit rating (and your life as well).

Who Else Wants My Data?

It's not just criminals who seek your personal data.
what other entities are interested in your online identity and why.

1. Your Internet Service Provider: Your ISP tracks your online activity and, in some countries, they can sell this data to advertisers for a profit. In certain circumstances, ISPs may be legally required to share your information with government surveillance agencies or authorities.

2. Advertisers: Targeted advertising is part of the Internet experience. Advertisers monitor and track your online activities such as shopping habits and personal preferences and send targeted ads your way.

3. Search Engines and Social Media Platforms: These platforms gather information about your gender, geolocation, phone number and political and religious ideologies based on your search histories and online identity. This information is then sold to advertisers for a profit.

4. Websites You Visits: Websites use cookies to track your activities in order to provide a more personalized experience. But this leaves a data trail that is linked to your online identity that can often end up in the hands of advertisers!

Protecting your organization data

Types of Organizational Data

1.Traditional Data

Traditional data is typically generated and maintained by all organizations, big and small. It includes the following:

1. Transactional data such as details relating to buying and selling, production activities and basic organizational operations such as any information used to make employment decisions.
2. Intellectual property such as patents, trademarks and new product plans, which allows an organization to gain economic advantage over its competitors. This information is often considered a trade secret and losing it could prove disastrous for the future of a company.
3. Financial data such as income statements, balance sheets and cash flow statements, which provide insight into the health of a company.

2. Internet of Things (IoT) and Big Data

IoT is a large network of physical objects, such as sensors, software and other equipment. All of these things are connected to the Internet, with the ability to collect and share data. And given that storage options are expanding through the cloud and virtualization, it's no surprise that the emergence of IoT has led to an exponential growth in data, creating a new area of interest in technology and business called 'Big Data.

Types of data

Sensitive and non- sensitive

- Sensitive information is **data that must be guarded from unauthorized access and unwarranted disclosure in order to maintain the information security of an individual or organization**.
- Sensitive data is confidential information that must be kept safe and out of reach from all outsiders unless they have permission to access it.

Here are some examples of sensitive data:

- Social security number, Biometric Data,
- Genetic Data, Home phone number,
- Home address, Health records, Passwords, Gender, Ethnicity,

- **non-sensitive data would include gender, date of birth, place of birth and postcode**.
- Although this type of data isn't sensitive, **it can be combined with other forms of data to identify an individual**.

Personal data, PII data

Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data is any piece of information that can be used to identify someone, simple as that!

Information such as:

- Name & surname
- Email
- Location data
- Home address
- IP address

- Personally, Identifiable Information (PII) is a legal term pertaining to information security environments. While PII has several formal definitions, generally speaking, it is information that can be used by organizations on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
- Non-sensitive PII can be transmitted in unsecure form without causing harm to an individual. Sensitive PII must be transmitted and stored in secure form, for example, using encryption, because it could cause harm to an individual, if disclosed.
- Organizations use the concept of PII to understand which data they store, process and manage that identifies people and may carry additional responsibility, security requirements, and in some cases legal or compliance requirements.

Data classification

Unclassified Data :

- Unclassified data can be defined as the data that has yet to be organized into categories or groups.
- Unclassified is a security classification assigned to official information that does not warrant the assignment of Confidential, Secret, or Top-Secret markings but which is not publicly-releasable without authorization.

Restricted Data:

- All data concerning the design, manufacture, and utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy but not including data declassified by the proper lawful authority
  - As defined in the Atomic Energy Act of 1954, all information concerning
    - the design, manufacture, or use of atomic weapons;

1. the production of special nuclear material; and
2. the use of special nuclear material in the production of energy.

Restricted data does not include information that has been declassified or removed from the Restricted Data category as defined in section 142 of the Atomic Energy Act of 1954.

Confidential Data:

Confidential data is personal identifiable information (PII) that you don't want anyone to obtain without your permission. This may include

- Social Security number
- Phone numbers of friends/family/colleagues/students
- Driver's license numbers
- Bank account numbers
- Tax information
- Passwords or passphrases
- Home address or phone numbers
- Employee ID number
- Digital images
- Any personal electronic documents containing personal text

Secret Data:

- Secret refers to national security information or material which requires a substantial degree of protection.
- The test for assigning Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security.
- Examples of *serious damage* include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.
- The classification Secret shall be sparingly used
- Confidential data is **information that is not available to the general public**. In general, it is personally identifiable information (as opposed to aggregated data) that is considered private in nature, such as health information, addresses, prior work experience, and financial data.

Top secret

Top Secret refers to **national security information or material which requires the highest degree of protection**. The test for assigning Top Secret classification is whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

DAY-1/2

Introduction and Basic concepts of cyber security

What is Cyber Security?

- The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity.
- We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information.
- In some cases, it is also called **electronic information security** or **information technology security**.

Security principles

CIA (Confidentiality, Integrity, Availability)

The basic tenets of information security are confidentiality, integrity and availability.

1. Confidentiality

Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. **Data encryption** is an excellent example of ensuring confidentiality.

2. Integrity

This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.

3. Availability

This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

(Authentication, Authorization, Accounting)

AAA is a standard-based framework used to control who is permitted to use network resources (through authentication), what they are authorized to do (through authorization), and capture the actions performed while accessing the network (through accounting).

1. Authentication The process by which it can be identified that the user, which wants to access the network resources, valid or not by asking some credentials such as username and password.

2. Authorization It provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication. After the authentication is successful, authorization can be used to determine what resources, is the user allowed to access and the operations that can be performed.

3. Accounting It provides means of monitoring and capturing the events done by the user while accessing the network resources. It even monitors how long the user has access to the network. The administrator can create an accounting method list to specify what should be accounted for and to whom the accounting records should be sent.

Vulnerability, Threat, Risk

Vulnerability

Vulnerability refers to a weakness in your hardware, software, or procedures. (In other words, it's a way hacker could easily find their way into your system.)

Types of Vulnerability

Vulnerabilities could be of many types, some of them are:

1. **Network-** Network vulnerability is caused when there are some flaws in the network's hardware or software.
2. **Operating system-** When an operating system designer designs an operating system with a policy that grants every program/user to have full access to the computer, it allows viruses and malware to make changes on behalf of the administrator.
3. **Human-** Users' negligence can cause vulnerabilities in the system.
4. **Process-** Specific process control can also cause vulnerabilities in the system.

Threat

A *threat* exploits a vulnerability and can damage or destroy an asset.

Types of Threat

Threats could be of three types, which are as follows:

1. **Intentional-** Malware, phishing, and accessing someone's account illegally, etc. are examples of intentional threats.
2. **Unintentional-** Unintentional threats are considered human errors, for example, forgetting to update the firewall or the anti-virus could make the system more vulnerable.
3. **Natural-** Natural disasters can also damage the data, they are known as natural threats

Risk

R*isk* refers to the *potential* for loss, damage, or destruction of an asset when a threat takes advantage of vulnerability.

Threats + Vulnerability = Risk

Types of Risk

There are two types of cyber risks, which are as follows:

1. External- External cyber risks are those which come from outside an organization, such as cyberattacks, phishing, ransomware, DDoS attacks, etc.

2. Internal- Internal cyber risks come from insiders. These insiders could have malicious intent or are just not be properly trained.

Attack and Impact

- Cyberattacks are malicious attempts to access or damage a computer or network system.
- Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.
- Cyberattacks can lead to the loss of money or the theft of personal, financial and medical information.
- These attacks can damage your reputation and safety.
- Any individual or group can launch a cyber attack from anywhere by using one or more various attack strategies.

People, Process and Technology

Effective and robust cyber security requires an information security management system (ISMS) built on three pillars: **people, processes and technology.**

1. *People*

IT teams are trained with the latest cyber security skills and qualifications to implement the controls, technologies, and best practices for your organisation.

2. *Process*

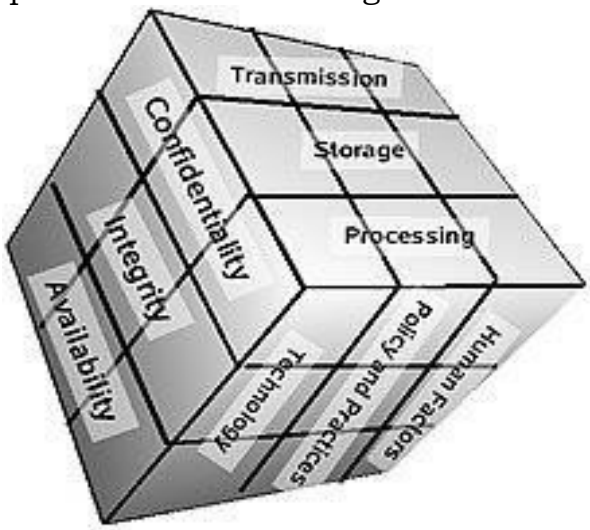
Bring in a coherent structure, and way of working to mitigate risks or deal with threats in real-time. Continually update documents because hackers are constantly evolving their attack techniques.

3. *Technology*

Technology can be deployed to prevent or reduce the impact of cyber risks, depending on your risk assessment and what you deem an acceptable level of risk.

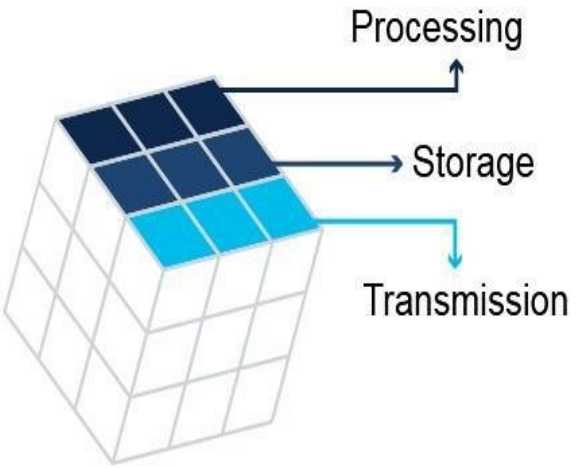
McCumbers Cube

- In 1991, John McCumber created a model framework for establishing and evaluating information security (information assurance) programs, known as **The McCumber Cube**.
- This security model is depicted as a three-dimensional Rubik's Cube-like grid.
- The concept of this model is that, in developing information assurance systems, organizations must consider the interconnectedness of all the different factors that impact them. The McCumber model helps one to remember to consider all important design aspects without becoming too focused on any one in particular.



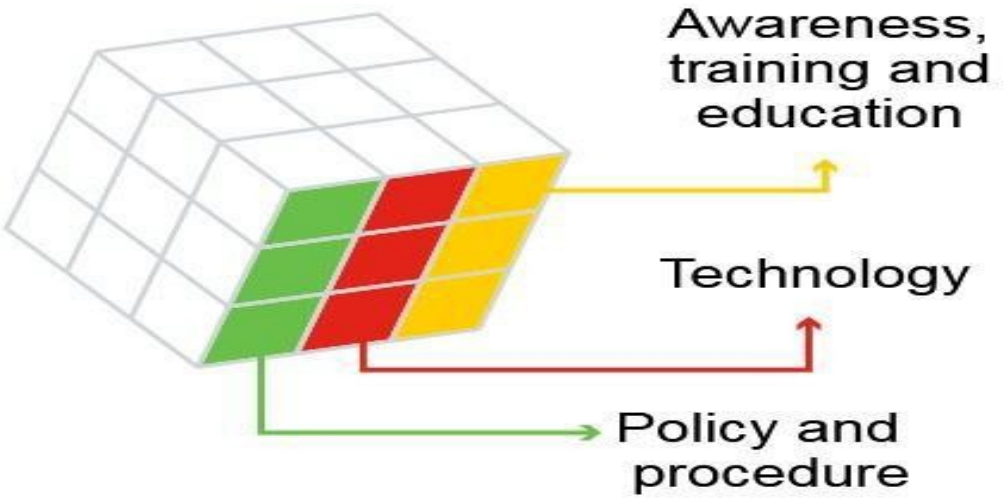
- **Confidentiality** is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes. Methods to ensure confidentiality include **data encryption**, **identity proofing** and **two factor authentications**.
- **Integrity** ensures that system information or processes are protected from intentional or accidental modification. One way to ensure integrity is to use a **hash function** or **checksum**.
- **Availability** means that authorized users are able to access systems and data when and where needed and those that do not meet established conditions, are not. This can be achieved by **maintaining equipment**, **performing hardware repairs**, **keeping operating systems and software up to date**, and **creating backups**.

The protection of information in each state



- **Processing** refers to data that is being used to perform an operation such as updating a database record (data in process).
- **Storage** refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive or USB drive (data at rest).
- **Transmission** refers to data traveling between information systems (data in transit).

The security measures used to protect data



- **Awareness, training and education** are the measures put in place by an organization to ensure that users are knowledgeable about potential security threats and the actions they can take to protect information systems.
- **Technology** refers to the software- and hardware-based solutions designed to protect information systems such as firewalls, which continuously monitor your network in search of possible malicious incidents.
- **Policy and procedure** refers to the administrative controls that provide a foundation for how an organization implements information assurance, such as incident response plans and best practice guidelines.

Desired goals

1. Confidentiality: assurance that sensitive information is not intentionally or accidentally disclosed to unauthorized individuals.
2. Integrity: assurance that information is not intentionally or accidentally modified in such a way as to call into question its reliability.
3. Availability: ensuring that authorized individuals have both timely and reliable access to data and other resources when needed.

Information states

1. Storage: **Data at rest (DAR)** in an information system, such as that stored in memory or on a magnetic tape or disk.
2. Transmission: transferring data between information systems - also known as **data in transit (DIT)**.
3. Processing: performing operations on data in order to achieve a desired objective.

Safeguards

1. Policy and practices: administrative controls, such as management directives, that provide a foundation for how information assurance is to be implemented within an organization. (examples: acceptable use policies or incident response procedures) - also referred to as **operations**.
2. Human factors: ensuring that the users of information systems are aware of their roles and responsibilities regarding the protection of information systems and are capable of following standards. (example: end-user training on avoiding computer virus infections or recognizing social engineering tactics) - also referred to as **personnel.**
3. **Technology**: software and hardware-based solutions designed to protect information systems (examples: anti-virus, firewalls, intrusion detection systems, etc.)

Cyber Security - Brief history

The origin of cybersecurity began with a research project. It only came into existence because of the development of viruses. The first cyber malware virus developed was pure of innocent mistakes. But cybersecurity has evolved rapidly because of the impeccable increase in the cybercrime law field on the Web.

The Cybersecurity checking began in the 1970s when researcher Bob Thomas created a computer program called Creeper that could move across ARPANET's network. Ray Tomlinson, the innovator of email, wrote the program Reaper, which chased and deleted Creepers. Reaper was the very first example of checking a malware antivirus software and the first self-replicating program i.e. Viruses, as it made first-ever computer worms and trojans.

After Creeper and Reaper, cyber-crimes became more powerful. As computer software and hardware developed, security breaches also increase. With every new development came an aspect of vulnerability, or a way for hackers to work around methods of protection. **In 1986**, the Russians were the first who implement the cyber power as a weapon. **Marcus Hess**, a German citizen, hacked into 400 military computers, including processors at the Pentagon. He intended to sell secrets to the KGB, but an American astronomer, Clifford Stoll, caught him before that could happen.

In 1988, an American computer scientist, **Robert Morris**, wanted to check the size of the internet. He wrote a program for testing the size of the internet. This program went through networks, invaded Unix terminals, and copied itself. The program became the first famous network virus and named as Moris worm or internet worm. The Morris worm could be infected a computer multiple times, and each additional process would slow the machine down, eventually to the point of being damaged. Robert Morris was charged under the ***Computer Fraud and Abuse Act***. The act itself led to the founding of the Computer Emergency Response Team. This is a non-profit research centre for issues that could endanger the internet as a whole.

Types of Cyber Security

Every organization's assets are the combinations of a variety of different systems. These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cybersecurity in the following sub-domains:

1. Network Security: It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.

2. Application Security: It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.

3. Information or Data Security: It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.

4. Identity management: It deals with the procedure for determining the level of access that each individual has within an organization.

5. Operational Security: It involves processing and making decisions on handling and securing data assets.

6. Mobile Security: It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.

7. Cloud Security: It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.

8. Disaster Recovery and Business Continuity Planning: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

9. User Education: End-user education is the process of educating and training users about the best security practices and safety measures to avoid letting in malware or other malicious software.

A good end-user security training program can help enhance the security in an organization when done properly. The training should be in a language and at a technical level that can be understood and followed by everyone.

Infrastructure:

The basic physical and organizational structures and facilities (includes hardware and software assets such as end-user devices, data center resources, networking systems, and cloud resources)

Network

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.

Cloud

"The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. Cloud servers are located in data centers all over the world.

IOT

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

The term IoT, or **Internet of Things**, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.
It's a physical object that connects to the Internet. It can be a fitness tracker, a thermostat, a lock or appliance – even a light bulb.

Application

A program (such as a word processor or a spreadsheet) that performs a particular task or set of tasks

Importance of Cybersecurity

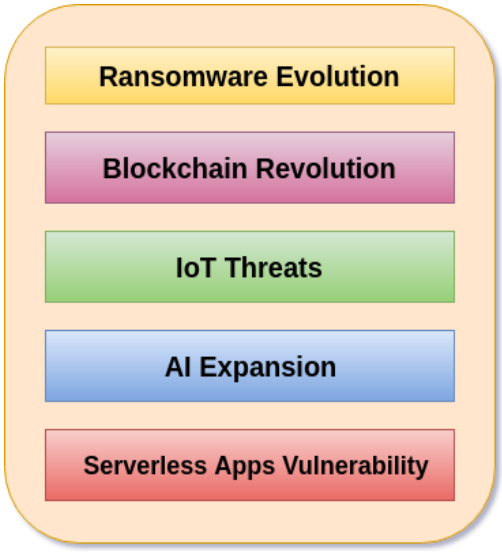
- Cybersecurity is just an ethical practice to protect our devices from hackers and make them more secure. People involved in cybersecurity perform security measures and operations in order to keep our data and devices safe. Cybersecurity basically deals with protecting our network, devices, and data from illegal and unauthorized access by other people. Hackers and cybercriminals use the Internet as an opportunity to crack into other's people devices by using spyware, malware and carrying out cyber-attacks.
- The main purpose of Cybersecurity is to protect all the users on the Internet from infected files, malware, and digital attacks which lead the users to access private sensitive information of users, extort ransom from users by using their private data or even disrupting important critical infrastructure like shutting down power supplies and military infrastructure.
- Cybersecurity helps to solve pre-built vulnerabilities in applications and helps them to remain stable throughout. More and more devices are getting connected to the Internet, hence it is more and more important to secure all the devices over the Internet to protect them all against unauthorized access.

Cyber Security Challenges

The recent important cybersecurity challenges are described below:

1. Ransomware Evolution

Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. After successful payment, access rights returned to the victim. Ransomware is the bane of cybersecurity, data professionals, IT, and executives.
Ransomware attacks are growing day by day in the areas of cybercrime. DRaaS solutions are the best defence against the ransomware attacks. With DRaaS solutions method, we can automatically back up our files, easily identify which backup is clean, and launch a fail-over with the press of a button when malicious attacks corrupt our data.



Cyber Security Challenges

2. Blockchain Revolution

The blockchain is a technology that enables cryptocurrencies like Bitcoin. The blockchain is a vast global platform that allows two or more parties to do a transaction or do business without needing a third party for establishing trust.

It is difficult to predict what blockchain systems will offer in regards to cybersecurity. The professionals in cybersecurity can make some educated guesses regarding blockchain. As the application and utility of blockchain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches.

3. IoT Threats

IoT is a system of interrelated physical devices which can be accessible through the internet. The connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network without any requirements of the human-to-human or human-to-computer interaction. The firmware and software which is running on IoT devices make consumer and businesses highly susceptible to cyber-attacks. When IoT things were designed, it is not considered in mind about the used in cybersecurity and for commercial purposes. So every organization needs to work with cybersecurity professionals to ensure the security of their password policies, session handling, user verification, multifactor authentication, and security protocols to help in managing the risk.

4. AI Expansion

AI short form is Artificial intelligence. It is an area of computer science which is the creation of intelligent machines that do work and react like humans. The key benefits with AI into our cybersecurity strategy has the ability to protect and defend an environment when the malicious attack begins, thus mitigating the impact. AI take immediate action against the malicious attacks at a moment when a threats impact a business. IT business leaders and cybersecurity strategy teams consider AI as a future protective control that will allow our business to stay ahead of the cybersecurity technology curve.

5. Serverless Apps Vulnerability

Serverless architecture and apps is an application which depends on third-party cloud infrastructure or on a back-end service such as google cloud function, Amazon web services (AWS) lambda, etc. The serverless apps invite the cyber attackers to spread threats on their system easily because the users access the application locally or off-server on their device. Therefore, it is the user responsibility for the security precautions while using serverless application.

The serverless apps do nothing to keep the attackers away from our data. The serverless application doesn't help if an attacker gains access to our data through a vulnerability such as leaked credentials, a compromised insider or by any other means then serverless.

Applications of Cybersecurity:

- **DDoS security:** DDoS stands for Distributed Denial for Service attack. In this digital attack, the attacker uses multiple numbers of devices to keep the web server engaged in accepting the requests sent by him from the multiple devices. It creates fake website traffic on the server. To deal with this, Cybersecurity helps to provide a DDoS mitigation service to help cope with it which diverts the traffic to the other cloud-based servers and the situation gets resolved.
- **Web Firewall:** A web application server-based firewall gets applied on a large area network and it checks all the incoming and outgoing traffic on the server and it automatically tracks and removes fake and malicious website traffic. This Cybersecurity measure helps to determine and enable auto-traffic monitoring by reducing attack risk.
- **Bots:** Nowadays, many hackers and attackers use bots to cause multiple device traffic on the server to make it crash. Cybersecurity helps to deal with identifying

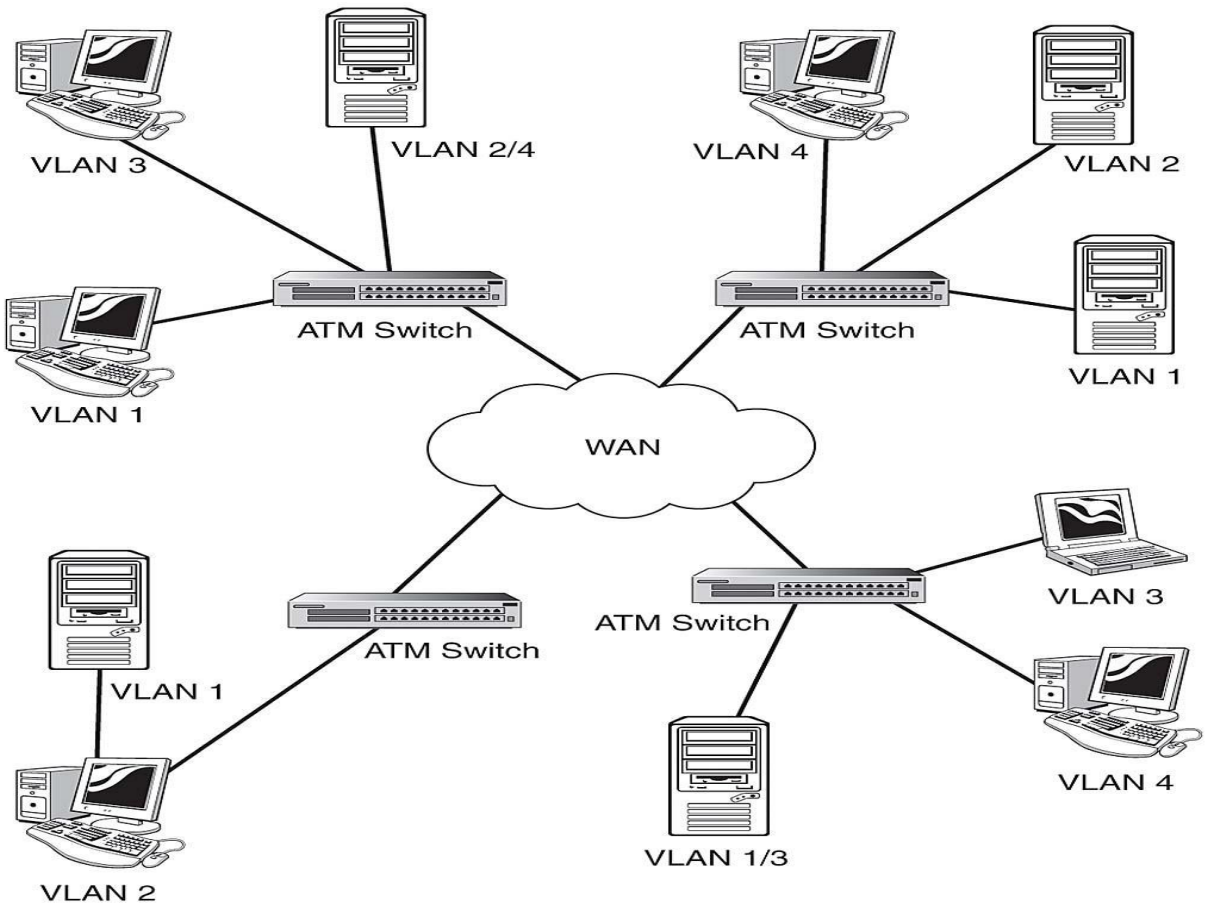
fake users i.e. bots and make them log out of their sessions so they don't affect the experience of the normal users.

- **Antivirus and Antimalware:** Cybersecurity is used to develop Antivirus and Antimalware software for preventing all the digital attacks on the computer and protecting these devices from data breaches, digital attacks, and unauthorized attacks from hackers. It also helps in maintaining network security and firewall systems for all the connected devices on the network.
- **Threat management systems:** Cybersecurity helps to deal with digital threats and attacks on computer systems. It identifies different points of vulnerabilities and bugs in the system that can be used by hackers and attackers to defy with it and it automatically optimizes all the defects in it with the ability to improve in performance issues. It also improves the ability to quickly overcome a digital attack and provide effective control to the users about the vulnerability issues.
- **Critical systems:** Cybersecurity helps to deal with the critical issue attacks that are carried out on large servers connected to wide-area networks. It maintains the standard high safety protocols for the users to comply with the cybersecurity measures so that to protect the devices. It monitors all the applications in real-time and checks regularly the safety of the servers, the network used by it, and the users themselves.
- **Rules and regulations:** Cybersecurity helps to create new rules and regulations for the users, attackers, and the people on the network to follow and comply with certain rules and norms while they are using the Internet. It gives the power to the authorities to look into security issues and optimize the network accordingly.

DAY-2/1

TOPOLOGY

- ✓ Topology defines the structure of the network of how all the components are interconnected to each other.
- ✓ A security topology is **the arrangement of hardware devices on a network with respect to internal security requirements and needs for public access**.
  For example, an Internet order firm will need Web servers that can be accessed by the public for placing orders.
- ✓ In turn, the Web servers will need access to internal database servers, and internal users (employees) will need access to the various servers and possibly to the Internet.
- ✓ when working with LANs. First, as LANs become more popular and faster, they tend to grow larger.
  - ❖ As a result, any broadcast messages reach a larger audience than was common even in recent history. Additionally, as more companies adopt organizational structures that are less hierarchical, employees can move from location to location more frequently.
- ✓ **A VLAN allows a group of computers to be virtually configured as a separate LAN**. **A VLAN can simply define a subset of a larger LAN or can include computers from various existing LANs.**



OSI REFERENCE MODEL

Before going into security, it is necessary to know the basics of networking and its models - the OSI model. It is a hypothetical networking framework that uses specific protocols and mechanisms in every layer of it. This model is used to divide the network architecture into seven different layers conceptually. These layers are:

- Physical layer.
- Datalink layer.
- Network layer.
- Transport layer.
- Session layer.
- Presentation layer.
- Application layer.

There also involves some security postures and mechanisms that a security professional must know to detect and put the security method effectively in every layer.

OSI Security Architecture defines the well-planned standard architecture for security features in computer networking. OSI architecture is internationally acceptable as it layers the flow of providing safety in an organization.

Need of OSI Architecture:

Below listed are the need for OSI Architecture in an organization:

1. Security Needs:

- OSI Architecture caters to the security needs of an organization.
- Safety and security are ensured by OSI Architecture to prevent risk and threats.

2. Systematic Arrangement:

- OSI Architecture gives a systematic approach to the security requirements of an organization.
- Security policies are well maintained through OSI Architecture.

3. Centralised Processing:

- OSI Architecture maintains a central processing environment.
- LAN and WAN help in the Centralised Processing of OSI Architecture.

Benefits of OSI Architecture:

Below listed are the benefits of OSI Architecture in an organization:

1. Providing Security:

- OSI Architecture in an organization provides the needed security and safety, preventing potential threats and risks.
- Managers can easily take care of the security and there is hassle-free security maintenance done through OSI Architecture.

2. Organising Task:

- Managers get the opportunity to organize tasks in an organization effectively.
- A well-planned standard architecture for security features enhances performance.

3. Meets International Standards:

- Security services are defined and recognized internationally meeting international standards.
- The standard definition of requirements defined using OSI Architecture is globally accepted.

Three Pillars of OSI Security Architecture:

OSI Security Architecture is categorized into three broad categories mentioned
Security Attacks,
Security mechanisms,
and Security Services.

- ✓ **Security Attacks:**

These are defined as the actions that put at risk an organization's safety. They are further classified into 2 sub-categories:

A. Passive Attack:

Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks.

Here, both the sender and receiver have no clue that their message/ data is accessible to some third-party intruder. The message/ data transmitted remains in its usual form without any deviation from its usual behavior. This makes passive attacks very risky as there is no information provided of the attack happening in the communication process. One way to prevent passive attacks is to encrypt the message/data that needs to be transmitted, this will prevent third-party intruders to use the information though it would be accessible to them. Passive attacks are therefore divided into two parts based on their behavior:

- **Message Content** is the type of passive Attack that involves the intruder stealing all the message/data transmitted. Here, the information gathered by the intruder is stolen unethically.
- **Masked Traffic Analysis:** This type of passive Attack involves messages/ data being encrypted before transmission. Here, the message being masked/ encrypted the intruder can't read the message but only understand the pattern and length of encryption.

B. Active Attacks:

Attacks in which both the sender and receiver have no clue that their message/ data is modified by some third-party intruder. The message/ data transmitted doesn't remain in its usual form and shows deviation from its usual behavior. This makes active attacks dangerous as there is no information provided of the attack happening in the communication process and the receiver is not aware that the data/ message received is not from the sender.

Active attacks are further divided into four parts based on their behavior:

- **Masquerade** is a type of active attack, the attacker tampers the information received by the receiver by claiming itself as the sender.
- **Replay** is a type of active attack, the attacker attacks the transmitted message through a passive channel and make the final message received by the receiver look like it's not authorized and safe
- **Modification of Message** is a type of active attack, the attacker modifies the transmitted message and makes the final message received by the receiver look like it's not authorized and safe
- **Denial of Services** is a type of active attack, the receiver is prevented from receiving the transmitted message as there is an overflow of requests to the receiver, which makes the services hampered from their usual behavior.

2. Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism. Security Mechanisms are also responsible for providing ways in which an attack can be prevented as soon as it is detected.

3. Security Services:

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

- **Authentication** is the most basic service to ensure that desired permission is well verified and safe
- **Access Control** ensures that only authorized users have access to the available resources.
- **Data Confidentiality** is responsible for ensuring that the data is kept extremely safe from third-party intruders.

- **Data Integrity** ensures that the transmitted information received by the receiver is well- authenticated and there is no tampering with the information received.
- **Non- repudiation** restricts the forwarding of the transmitted message by either of the parties(sender and receiver).

Implementation of Security Methods within the OSI Model

The **first three layers of the OSI model are called the media layers**.

1. Physical Layer is used for defining the technical qualifications of the data connectivity. Since the security in this layer is critical, so in case of any cyber danger (DoS attack), it is recommended to unplug the cable from the primary system.
   Safeguarding this layer needs bio-metric security, camera-based surveillance, key cards, and other physical monitoring.
2. Data Link Layer comprises of data packets transported from the physical layer. Any malfunctioning in this layer or data breach can impede the working of the network layer. Vulnerabilities that can be used and attacks that can be made in this layer are MAC address spoofing and virtual-LAN circumvention.
   So for protecting your system, common security mechanisms are MAC address filtering, assessment of wireless applications, checking of proper data encryption standards.
3. Network Layer is the last of the media layer and has an association with the real world. It deals with the addressing and routing of packets. IP address spoofing is one o the common attack of this phase. Strengthening this layer needs the techniques of firm anti-spoofing, proper implementation of firewalls and routing filters, and secure routing protocols.

The subsequent **four layers are host layers:**

1. Transport Layer - comes under the logical layer, which helps in transferring variable-length data sequence. The reliability of this layer can be achieved by ensuring the segmentation and de-segmentation mechanism and error control. For security purposes, this layer needs an appropriate firewall, restrictive admission of transmission protocols, and appropriate port number.
2. Session Layer - essentially manages the inter-system communication and sessions. The handling of local and remote application's interaction is done in this layer. In case of weak authentication methods, it can help attackers to perform a brute force. So the effective way of securing this layer is by ensuring appropriate encrypted key exchange, along with the restriction of unsuccessful session attempts using timing methods.
3. Presentation Layer - is used to standardize data with the help of various conversion schemes. But if there is poor conduct of malicious input, it can help cybercriminals exploit the system or even crash a system. Separate sanitized input and proper input validation can help protect the system from attackers.
4. Application Layer - contain the UI and the closest of all layers for the user-end. The widest range of cyber-attacks and security breaches is possible in this layer. It can lead to shutting down the network, stealing data, crashing the application, manipulating the information sent from source to destination, and many more.

When you think of networks as being structured in the seven layers of the ISO-OSI model, it makes sense that cybersecurity threats can happen at any layer. We can think of these layers as the “links” in our metaphorical chain. Moving outward from the user, data is entered into the network through software running on the Application layer. Through the Session, Transport, Network, and Data-Link layers and arriving at the other end, the Physical layer, the data travels back up the seven layers to arrive at its intended

destination. Each layer has its own protocols and other communication standards that govern its efficient operation.

Where do Cybersecurity threats happen?

Cybersecurity threats exist at all OSI-ISO model layers beginning at Layer 7 – the Application Layer because that's the place where users begin by interfacing to the network. For the purposes of creating the most comprehensive cybersecurity plan we must actually start BEFORE the Application Layer and address perhaps the biggest vulnerability in the entire network – **the user**. Users are human and far more subject to making costly errors than are computers and other digital devices which will perform the same function the same way every time.

The best example is found in one of the top malware attacks or threats in the cyber landscape – ransomware. Fraudsters send out a "phishing" email that looks very authentic, very much as if it actually comes from where it says it does. But somewhere in that email is a link for the user to click or an attachment for the user to open. The text provides powerful inducements to get the user to do so. Once they do their data is either encrypted, corrupted, or stolen. The only way to get it back is to pay a ransom, thus ransomware.

The attackers know the user is their best place to gain access.

Threats at each layer of the ISO-OSI model include:

APPLICATION LAYER THREATS

Security software developer F5 tells us, "Examples of application layer attacks include distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks. To combat these and more, most organizations have an arsenal of application layer security protections, such as web application firewalls (WAFs), secure web gateway services, and others." The team at SecurityIntelligence points out that, "*The application layer is the hardest to defend*. The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define with an intrusion detection signature. This layer is also the most accessible and the most exposed to the outside world. For the application to function, it must be accessible over Port 80 (HTTP) or Port 443 (HTTPS)." Other possible exploits at the Application Layer include viruses, worms, phishing, key loggers, backdoors, program logic flaws, bugs, and trojan horses.

Your cybersecurity plan must include Application Monitoring which is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source.

PRESENTATION LAYER THREATS

The most prevalent threats at this layer are malformed SSL requests. Knowing that inspecting SSL encryption packets is resource intensive, attackers use SSL to tunnel HTTP attacks to target the server.

Include in your mitigation plans options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure.

SESSION LAYER THREAT

DDoS-attackers exploit a flaw in a Telnet server running on the switch, rendering Telnet services unavailable.

In the regular maintenance portion of your plan be sure to remind operators to check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability.

TRANSPORT LAYER THREATS

According to Network World, “Many businesses use Transport Layer Security (TLS) to secure all communications between their Web servers and browsers regardless of whether sensitive data is being transmitted. TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an IETF standard intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP.”

NETWORK LAYER THREATS

Routers make decisions based on layer 3 information, so the most common network layer threats are generally router-related, including information gathering, sniffing, spoofing, and distributed denial of service (DDoS) attacks in which multiple hosts are enlisted to bombard a target router with requests to the point where it gets overloaded and cannot accept genuine requests.

The most effective protection is achieved by consistently observing best practices for router, firewall and switch configurations. At the router itself it is important to constantly assure that the router operating system is up to date on all security patches, packet filtering is kept enabled and any unused ports are blocked, unused services, and interfaces are disabled. Keep logging enabled and conduct regular auditing of any unusual activity that may occur.

It’s also advisable to place firewalls between your network and all untrusted networks. Always keep that firewall up to date with all issued security patches, enable packet filtering, and keep logging enabled so you can audit any anomalies.

Any switches on your network must also be kept updated with all security patches, with any unused interfaces or services disabled. Make certain that all switch traffic is encrypted.

DATA-LINK LAYER THREATS

Cisco explains that, “The data link layer provides reliable transit of data across a physical link. The data link layer is concerned with physical, as opposed to logical addressing, network topology, network access, error notification, ordered delivery of frames, and flow control. Frame-level exploits and vulnerabilities include sniffing, spoofing, broadcast storms, and insecure or absent virtual LANs (VLANs, or lack of VLANs). Network interface cards (NICs) that are misconfigured or malfunctioning can cause serious problems on a network segment or the entire network.”

Most companies that have experienced Address Resolution Protocol (ARP) spoofing, Media Access Control (MAC) flooding or cloning, Port Stealing, Dynamic Host Configuration Protocol (DHCP) Attacks, layer 2-based broadcasting or Denial of Service Attacks have immediately focused on improving port security. They also configure their switches to limit the ports that can respond to DHCP requests, implement static ARP and install Intrusion Detection Systems (IDS).

PHYSICAL LAYER THREATS

Ask any cybersecurity professional to define where the network is and they'll point at "the wires in the walls." What they're saying is that the copper and fiber-optic cables that connect everything together create the actual network that everything else uses. Most threats at this layer involve interruption of the electrical signals that travel between network nodes including the physical cutting of cables, natural disasters that bring flood waters which can cause short-circuits, or other human vandalism.

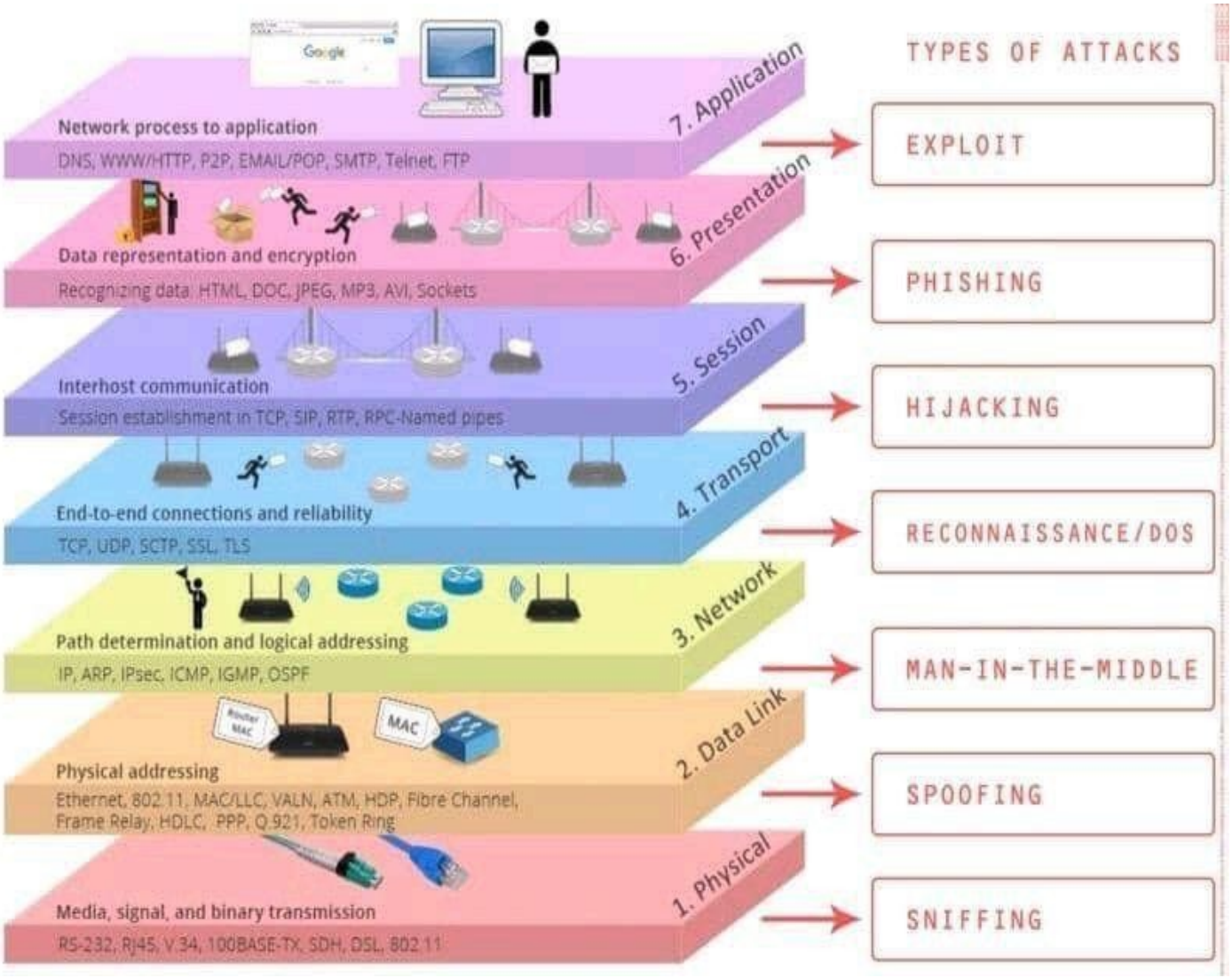
Many companies mitigate these failures by bringing in multiple circuits to the internet. It should be noted that this works well until a backhoe digs up a critical corner through which all carrier circuits run, thus disabling all of the multiple paths. The aftermath of many disasters illustrates the superior strategy being the placement of all network core elements such as servers and storage at multiple redundant cloud data centers. Should a major carrier cable be cut, only users will be affected, and they can switch to wireless access or other locations until repairs are completed.

Prevent Cybersecurity Threats Before they Become a Problem

Since users are our most unpredictable network component it is critical that your cybersecurity plan address best practices and operating requirements on your network, but the plan is equally important to the digital devices that help create the comprehensive defense we've been discussing. The purpose of a firewall, for example, is to enforce your security policies and rules. That's not possible if you have no security policies and rules.

Consider bringing cybersecurity end user safety training to your organization. This 2 hour, life, instructor-led course teaches end users how to be safe and spot digital threats online. For cybersecurity professionals, you should consider cybersecurity training certifications from Certified Ethical Hacker (CEH) to Certified Chief Information Security Officer (CCISO).

In the case of cybersecurity, a failure to plan is a short-term strategy. Fitting security in at every layer is just one piece of a comprehensive cybersecurity plan. Attacks will happen, and they will disrupt and disable operations, which is ultimately an existential hazard. Schedule a free cybersecurity consultation with a New Horizons cybersecurity expert now to review your plan.



Attacks can happen at different levels of the network models with different protocols.
I wanna present at least one attack by OSI layer division.

1. Sniffing (physical)

Back in the day when there was no remote home phone, you had to have multiple phones at home anyone can remember the problems that had been occurred when two people wants to speak on the phone someone else could grab another phone and hear the speeches. in the context of network security when packets are not encrypted someone else could intrude to your network and steal those packets with some sniffer applications that work on the **physical** layer of **OSI model** like Wireshark, Tcpdump, WinDump... some protocols that work on this layer and can be sniffed are:

Examples of protocols that use physical layers include:

- Digital Subscriber Line.
- Integrated Services Digital Network.
- Infrared Data Association.
- Universal Serial Bus (USB.)
- Bluetooth.
- Ethernet.

2. SPOOFING (Data Link)

Spoofing is the act of a person or a program that successfully identifies itself which is from an unknown source as being from a known, trusted source. Spoofing can apply to

emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server. IP spoofing and ARP spoofing, in particular, may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks that take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

3. man-in-the-middle (Network)

Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message, leaving them vulnerable cause an attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

4. Reconnaissance (Transport)

In the context of cybersecurity, reconnaissance is the practice of discovering and collecting information about a system. One of the most common techniques involved with reconnaissance is port scanning, which sends data to various TCP and UDP (user datagram protocol) ports on a device and evaluates the response. Some common examples of reconnaissance attacks include packet sniffing, ping sweeping, port scanning, phishing, social engineering, and internet information queries.

5. Hijacking (Session)

sometimes also known as **cookie hijacking** is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many websites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. these explosions can be carried out by these attacks

- **Cross-site scripting: XSS attacks** enable attackers to inject client-side scripts into web pages. It causes running codes, which is treated as trustworthy because it appears to belong to the server, on the victim computer. It allows the attacker to obtain a copy of the cookie or perform other operations.
- **Session side jacking:** where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie.
- **Malware** and unwanted programs can use browser hijacking to steal a browser's cookie files without a user's knowledge.

6. Phishing (presentation)

Phishing attacks are the practice of sending fraudulent messages that appear to come from a trusted source. It is usually performed through email. The goal is to steal sensitive data like credit card and login information or install malware on the victim's machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves.

7. Exploit (Application)

An exploit is a program that takes advantage of a bug or vulnerability in other systems. the cause vulnerability may be due to bad system configuration or a bug in a specific version of software installed on the victim system. Many exploits are designed to provide super user-level access to a victim system or are designed to cause DoS (denial of service)

or DDoS (distributed denial of service) attacks, in which attackers can bring down a website or critical system without even using an exploit.
for instance, BlueKeep is an exploitable vulnerability in Microsoft Remote Desktop Protocol (RDP) that can allow attackers to log in to a victim's computer remotely.

TCP/IP MODEL

TCP stands for Transmission Control Protocol. IP stands for Internet Protocol.
A Protocol is a:
"set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another"
(steves-internet-guide.com)
A Suite is a group of things forming a series or set usually designed to work together.
Definition: TCP/IP is a means of communication through protocols used on the Internet and computer networks.
TCP/IP is formally known as the Internet Protocol Suite.
Breakdown of TCP/IP – Four Layers
While Kahn and Cerf were working together, people considered having the TCP/IP Protocol Stack divided into different layers separating the functionality.

Layer 1 – Link Layer

Layer 2 – Internet Layer

Layer 3 – Transport Layer

Layer 4 – Application Layer

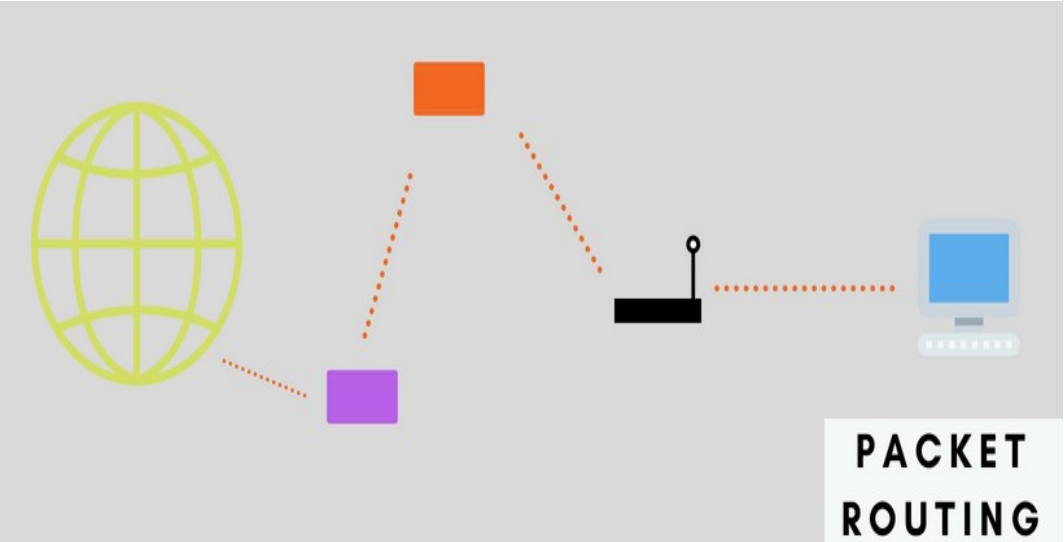
Layer 1 – Link Layer
The link layer is the layer used for local network connections where the host is attached. The link layer's tasks include LLC, MAC, data framing, addressing, and error detection and handling.

- Logical Link Control (LLC): Functions as an establishment and control of the coexistence of multipoint networks to be transported at the same time.
- Media Access Control (MAC): The MAC address refers to identifying a specific hardware piece. The MAC is used to control access to the network, and since many networks are shared (multiple connections within one network) it is necessary to have these rules for managing conflicts.
- Data Framing: Responsible for the conversion of final encapsulation for higher-level messages into frames that are sent over the network.
- Addressing: Labels the information with a specific destination location via MAC address.
- Error Detection and Handling: Lower-level network stack analysis.

Layer 2 – Internet Layer
The internet layer's main responsibility is to send packets across multiple networks through the process of routing via the router. This process is achieved through the use of an IP address.
The IP address has two main roles:

1. Host addressing (addressing the host ID portion, refer to what is host addressing?) and identification of an IP address
2. Packet Routing (which is the process of sending packets of data to the next closest network trying to reach the end destination)

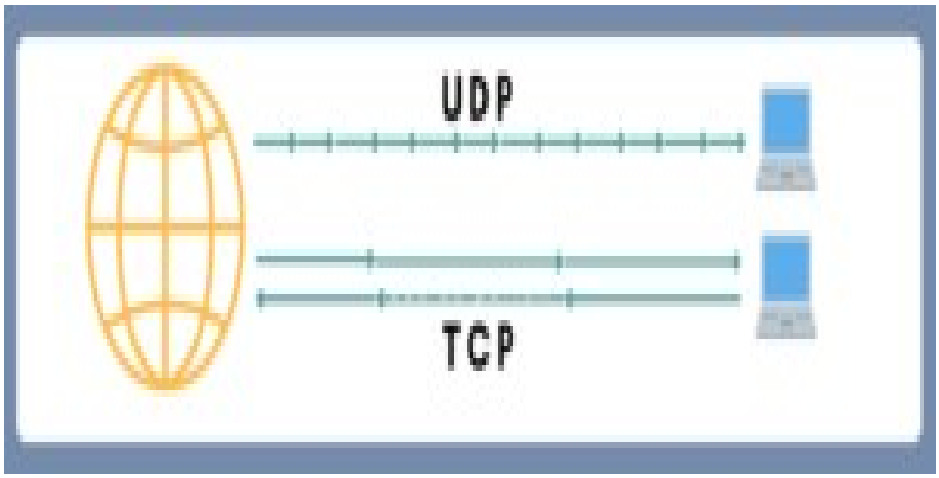
Through the process of routing, the internet layer makes possible internetworking, working with different IP networks, and establishes the Internet.
Now you know how the Internet works in the most basic way! (or maybe you already knew)



Layer 3 – Transport Layer
The transport layer creates basic data channels so that applications can use these channels for task-specific data exchange. This layer provides the process-to-process connectivity, allowing for the end part of a network node to establish a network (end-to-end) so that they are independent of the structure of the user data.
End-to-end transmission can be accomplished via TCP or UDP connections.
TCP connection-oriented protocols use a reliable byte stream so that:

- Data is in order
- Data is reduced to as little of errors as possible
- Duplicated data is deleted
- Lost data is resent
- Includes data traffic control

UDP connectionless-oriented protocols are unreliable using a weak checksum algorithm. UDP is typically used in applications that have a constant, continuous streaming datagram flow, compromising the quality of the content. UDP is typically used in VoIP, audio, video, streaming services, and live streaming.
Through the use of both TCP and UDP, specific packets of data can be created through channels allowing the data to transport from one network to another.



Layer 4 – Application Layer

The application layer uses protocols so that applications can provide user services and exchanging of application data can be established.

Some examples of application layer protocols include:

HTTP

FTP

SMTP

DHCP

DNS

Telnet

The TCP/IP protocol suite is vulnerable to a variety of attacks ranging from password sniffing to denial of service. Software to carry out most of these attacks is freely available on the Internet. These vulnerabilities-unless carefully controlled-can place the use of the Internet or intranet at considerable risk. This article classifies a range of known attack methods focusing in particular on SYN flooding, IP spoofing, TCP sequence number attack, TCP session hijacking, RST and FIN attacks and the Ping O' Death. The article concludes with an examination of the vulnerabilities of the common protocols carried by TCP/IP (including SMTP, Telnet, NTP, Finger, NFS, FTP, WWW and X windows) and proposes configuration methods to limit their vulnerability.

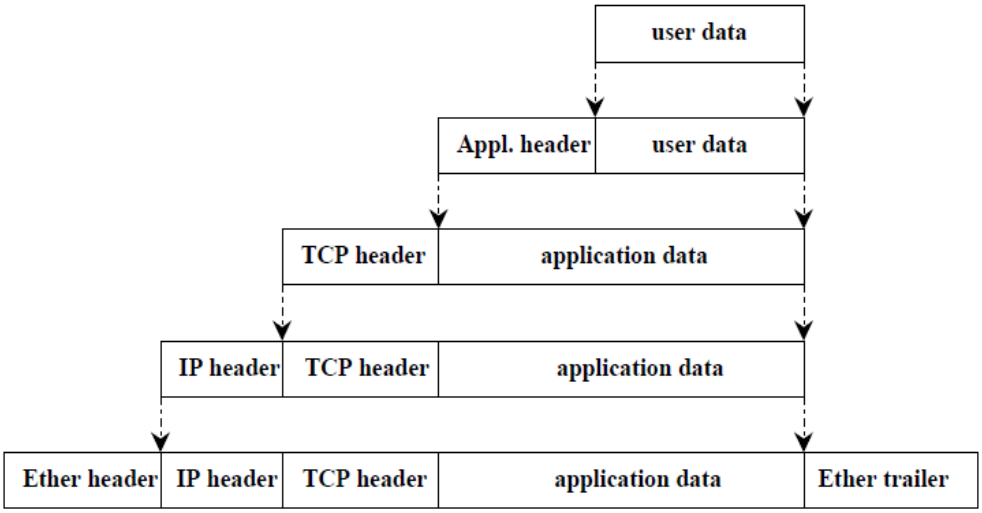


Figure 1: TCP/IP Protocol Stack

IP Address Spoofing:

IP address spoofing is the act of falsifying the content in the Source IP header, usually with randomized numbers, either to mask the sender's identity or to launch a reflected DDoS attack.

TCP Sequence Number Prediction:

A TCP sequence prediction attack is **an attempt to predict the sequence number used to identify the packets in a TCP connection**, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number to be used by the sending host.

Port Scanning:

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can't take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

Network Attacks

Denial of Service

The denial-of-service attacks attempt to prevent or delay access to the information or the information processing systems. The basic idea behind this type of attack is to tie up a service provider with bogus requests with intent to render it to unreliable or unusable.

SYN Flooding:

SYN flooding is a specially designed attack, which employs a flood of SYN packet to consume all available new network connectionson a targeted host, resulting in delays responding to legitimate network connection

requests and eventual halting the service provider [3]. Theoretically, this attack applies to all TCP connections, such as WWW, Telnet, e-mail, and so on.

Internet protocols:

we transfer the data in bulk, and the security of this data is very important, so Internet security provides that feature i.e., protection of data. There are different types of protocol exist like routing, mail transfer, and remote communication protocol. But the Internet security protocol helps in the security and integrity of data over the internet. There are many protocols that exist that help in the security of data over the internet such as **Secure Socket Layer (SSL)**, **Transport Layer Security (TLS)**.

1. **SSL Protocol :**
   - SSL Protocol stands for Secure Sockets Layer protocol, which is an encryption-based Internet security protocol that protects confidentiality and integrity of data.
   - SSL is used to ensure the privacy and authenticity of data over the internet.
   - SSL is located between the application and transport layers.
   - At first, SSL contained security flaws and was quickly replaced by the first version of TLS that's why SSL is the predecessor of the modern TLS encryption.
   - TLS/SSL website has "HTTPS" in its URL rather than "HTTP".
   - SSL is divided into three sub-protocols: the Handshake Protocol, the Record Protocol, and the Alert Protocol.
2. **TLS Protocol :**
   - Same as SSL, TLS which stands for Transport Layer Security is widely used for the privacy and security of data over the internet.
   - TLS uses a pseudo-random algorithm to generate the master secret which is a key used for the encryption between the protocol client and protocol server.
   - TLS is basically used for encrypting communication between online servers like a web browser loading a web page in the online server.
   - TLS also has three sub-protocols the same as SSL protocol – Handshake Protocol, Record Protocol, and Alert Protocol.

3. **SHTTP :**
   - SHTTP stands for Secure HyperText Transfer Protocol, which is a collection of security measures like Establishing strong passwords, setting up a firewall, thinking of antivirus protection, and so on designed to secure internet communication.
   - SHTTP includes data entry forms that are used to input data, which has previously been collected into a database. As well as internet-based transactions.
   - SHTTP's services are quite comparable to those of the SSL protocol.
   - Secure HyperText Transfer Protocol works at the application layer (that defines the shared communications protocols and interface methods used by hosts in a network) and is thus closely linked with HTTP.
   - SHTTP can authenticate and encrypt HTTP traffic between the client and the server.
   - SHTTP operates on a message-by-message basis. It can encrypt and sign individual messages.
4. **Set Protocol :**
   - Secure Electronic Transaction (SET) is a method that assures the security and integrity of electronic transactions made using credit cards.
   - SET is not a payment system; rather, it is a secure transaction protocol that is used via the internet.
   - The SET protocol provides the following services:
     - It establishes a safe channel of communication between all parties engaged in an e-commerce transaction.
     - It provides confidentiality since the information is only available to the parties engaged in a transaction when and when it is needed.
   - The SET protocol includes the following participants:
     - **Cardholder**
     - **Merchant**
     - **Issuer**
     - **Acquire**
     - **Payment Gateway**
     - **Certification Authority**
5. **PEM Protocol :**
   - PEM Protocol stands for privacy-enhanced mail and is used for email security over the internet.
   - RFC 1421, RFC 1422, RFC 1423, and RFC 1424 are the four particular papers that explain the Privacy Enhanced Mail protocol.
   - It is capable of performing cryptographic operations such as encryption, nonrepudiation, and message integrity.
6. **PGP Protocol :**
   - PGP Protocol stands for Pretty Good Privacy, and it is simple to use and free, including its source code documentation.
   - It also meets the fundamental criteria of cryptography.
   - When compared to the PEM protocol, the PGP protocol has grown in popularity and use.
   - The PGP protocol includes cryptographic features such as encryption, non-repudiation, and message integrity.

Network Resources:

The concept of Network resources emphasizes that communications networks are a fundamental resource component of all information systems. Network resources include: **Communication media, Examples include twisted pair wire, coaxial cable, fiber-optic cable, microwave systems, and communication satellite systems**.

Telecommunications networks like the Internet, intranets, and extranets have become essential to the successful operations of all types of organizations and their computer-based information systems. Telecommunications networks consist of computers, communications processors, and other devices interconnected by communications media and controlled by communications software. The concept of Network resources emphasizes that communications networks are a fundamental resource component of all information systems. Network resources include:

- ✓ **Communication media,** Examples include twisted pair wire, coaxial cable, fiber-optic cable, microwave systems, and communication satellite systems.
- ✓ **Network Support,** this generic category includes all of the people, hardware, software, and data resources that directly support the operation and use of a communications network. Examples include communications control software such as network operating systems and Internet packages.

In summary, these five components together make up the five-component framework, which are the five fundamental **components of an information system**.

- ✓ First you will need the hardware in order to start off your system.
- ✓ Then you must use the software in order to run you hardware.
- ✓ After you have set up your hardware and loaded up the software to run it, you will need data to input into your hardware.
- ✓ Once you have your data ready you will need procedures set in play to properly store your data within the system, and last you will need people in order to put in the data and keep the system up and running properly at all times.
- ✓ As you can see, you will need every component in order to ensure that you have a functional running information system.

Router and Firewall, Hub, switch – security issues:

Router

- ✓ A router is **a device that connects two or more packet-switched networks or subnetworks**.
- ✓ A network switch forwards data packets between groups of devices in the same network, whereas a router forwards data between different networks.
- ✓ It serves two primary functions: **managing traffic** between these networks by **forwarding data packets** to their intended IP addresses, and allowing multiple devices to use **the same Internet connection.**

security challenges associated with routers

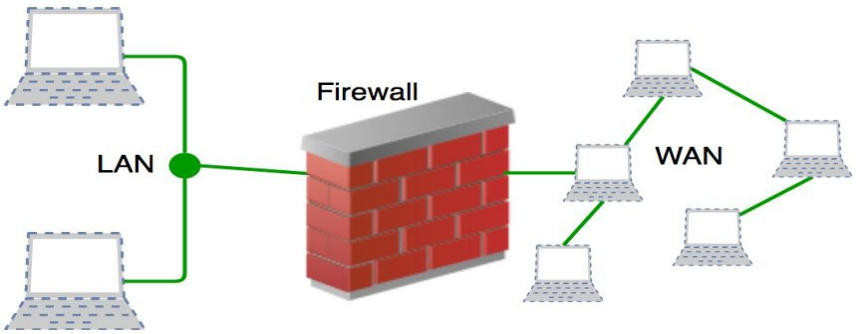
Vulnerability exploits: All hardware-based routers come with automatically installed software known as firmware that helps the router perform its functions. Like any other piece of software, router firmware often contains vulnerabilities that cyber attackers can exploit (one example), and router vendors periodically issue updates to patch these vulnerabilities. For this reason, router firmware needs to be updated regularly. Unpatched routers can be compromised by attackers, enabling them to monitor traffic or use the router as part of a botnet.

DDoS attacks: Small and large organizations often are the targets of distributed denial-of-service (DDoS) attacks directed at their network infrastructure. Unmitigated network layer DDoS attacks can overwhelm routers or cause them to crash, resulting in network downtime. Cloudflare Magic Transit is one solution for protecting routers and networks from these kinds of DDoS attacks.

Administrative credentials: All routers come with a set of admin credentials for performing administrative functions. These credentials are set to default values, such as "admin" as the username and "admin" as the password. The username and password should be reset to something more secure as soon as possible: attackers are aware of the common default values for these credentials and can use them to gain control of the router remotely if they are not reset.

Firewall:

- ✓ Firewall is **a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies**.
- ✓ A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- ✓ At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.



Firewalls also perform basic network level functions such as

- **Network Address Translation (NAT) and**
- **Virtual Private Network (VPN).**

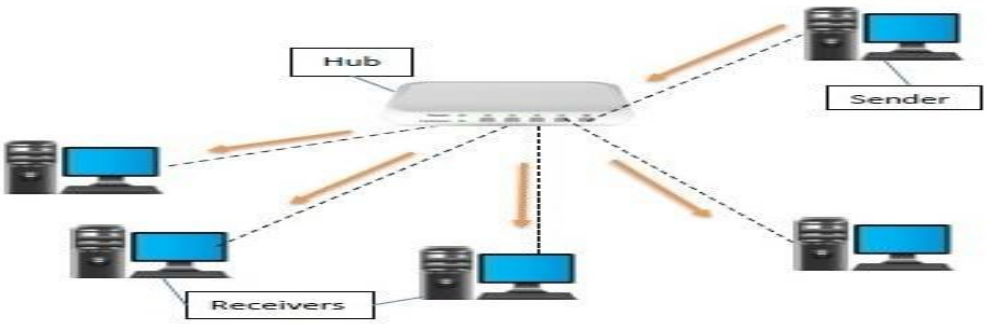
- ✓ Network Address Translation hides or translates internal client or server IP addresses that may be in a “private address range”, as defined in RFC 1918 to a public IP address.
- ✓ Hiding the addresses of protected devices preserves the limited number of IPv4 addresses and is a defense against network reconnaissance since the IP address is hidden from the Internet.
- ✓ Similarly, a virtual private network (VPN) extends a private network across a public network within a tunnel that is often encrypted where the contents of the packets are protected while traversing the Internet.
- ✓ This enables users to safely send and receive data across shared or public networks.
- ✓ Next Generation Firewalls inspect packets at the application level of the TCP/IP stack and are able to identify applications such as Skype, or Facebook and enforce security policy based upon the type of application.

- ✓ Today, UTM (Unified Threat Management) devices and Next Generation Firewalls also include threat prevention technologies such as intrusion prevention system (IPS) or Antivirus to detect and prevent malware and threats. These devices may also include sandboxing technologies to detect threats in files.
- ✓ As the cyber security landscape continues to evolve and attacks become more sophisticated, Next Generation Firewalls will continue to be an essential component of any organization's security solution, whether you're in the data center, network, or cloud.

Hub:

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.



Types of Hub

There are three types of the hub that are given below:

1. Passive Hub
2. Active Hub
3. Intelligent Hub

Passive Hub: The passive hubs are the connection point for wires that helps to make the physical network. It is capable of determining the bugs and faulty hardware. Simply, it accepts the packet over a port and circulates it to all ports. It includes connectors (10base-2 port and RJ-45) that can be applied as a standard in your network. This connector is connected to all local area network (LAN) devices.

Active Hub: As compared to a passive hub, it includes some additional features. It is able to monitor the data sent to the connected devices. It plays an important role between the connected devices with the help of store technology, where it checks the data to be sent and decides which packet to send first.

It has the ability to fix the damaged packets when packets are sending, and also able to hold the direction of the rest of the packets and distribute them. If a port receives a weak signal, but still it is readable, then the active hub reconstructs the weak signal into a stronger signal before its sending to other ports. It can boost the signal if any connecting device is not working in the network. Therefore, it helps to make the continuity of services in LAN.

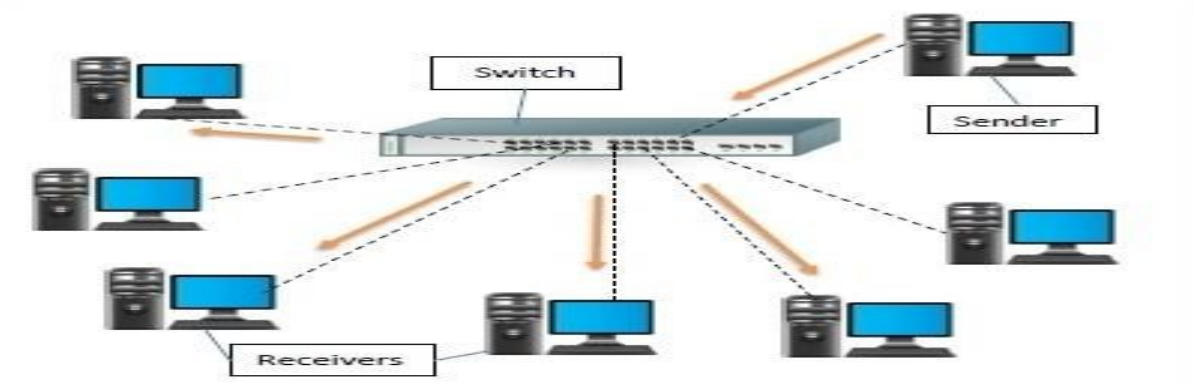
Intelligent Hub: It is a little smarter than passive and active hubs. These hubs have some kinds of management software that help to analyze the problem in the network and resolve them. It is beneficial to expend the business in networking; the management can assign users that help to work more quickly and share a common pool efficiently by using

intelligent hubs. However, it offers better performance for the local area network. Furthermore, with any physical device, if any problem is detected, it is able to detect this problem easily.

Switches

A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.

Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications.



Switching Basics for Cyber and Network Security

Network switches are used to connect computers and servers into a single network. The switch performs the function of a controller and allows the devices within a network to communicate with each other. This action is performed through packet switching, where data is received, processed, and forwarded to its destination from one computer to another. Information sharing as well as resource allocation through switching allows businesses to save money while improving productivity.

Routing Basics for Cyber and Network Security

While switches connect computers within a single network, routers are used to connect entire networks to each other. Data packets are received, processed, and forwarded from one network to another. Routing allows computers to link through the internet, thus allowing for information sharing between different networking systems.

Difference between Routing and Switching

Whereas switching creates a single network made up of individual computers, routing connects entire networks to each other. Routers perform a role similar to that of switches, but on a much larger scale. Thus, a router essentially acts as a dispatcher of data through the most efficient channels between networks.

Network Security Basics

What does routing and switching have to do with network security? Since information between computers and larger networks is transferred using routers and switches, they become the primary targets for hacking and information leaking. Thus, to ensure network security, it becomes essential to protect routers and switches against outside tampering.

Facets of Router and Switch Security

Router and switch security is becoming increasingly more sophisticated, and mainly deals with the following security concerns:

1. **User Authentication**

This involves any measures taken within a computer or a network, to ensure the computer user's identity. ID theft is becoming increasingly more common in the digital world, making it an increasingly important facet of network security.

2**. Next Gen Firewalls**

An integrated platform that is used to combine the traditional firewall with other network filtering devices to provide greater network security. The platform performs several security checks simultaneously through data packet inspection, and employing some manner of intrusion and prevention system, along with antivirus inspection and third party integration.

3. **Intrusion Detection**

This is a software or device feature that is used to monitor a computer or a network of computers in order to detect malicious activity or possible violations of network policy. In the event of a problem being detected that could compromise network security, the software sends an immediate alert to the relevant authorities, and, depending on the setting, takes some form of action to shut down the lines of communication with the device posing a threat.

4. **Intrusion Prevention**

The purpose of this kind of software is to take a preemptive approach towards network security. The device is programmed to actively take part in the identification of potential threats to network security and take swift action against them before the threat becomes a reality. Similar to an intrusion detection system, an intrusion prevention system monitors network traffic, but plays a more directly active role in neutralizing threats to security.

5. **Port Level Filters and Checks**

Thanks to the internet, information can be shared more quickly than ever, through the world wide network. The improvement in data sharing has also resulted in increasingly more mobile methods of data collection and transfer, such as thumb drives and hard disks. In order to ensure the network security is not threatened by these external devices, various port filters are available for the monitoring and detection of malicious software hiding within the external drives, which can enter the network through ports which are left unguarded.

The Future of Router and Switch Security

Routers and switches are becoming more intelligent, and are starting to incorporate features that are found in enterprise level data centers. Modern security features incorporate login blocking capabilities in case of wrong authentication information, preventing unauthorized devices from becoming a part of the network and prioritizing data traffic so that certain data packets are allowed to enter the network, while suspicious traffic is blocked automatically.

Port mirroring is also used to copy traffic from an unfiltered port to a secure port that can monitor and control the traffic. Network virtualization is another step forward towards intelligent routers and switches that can combine different LANs into a single super network.

DAY-2/2

How Does Cybersecurity Work?

Cybersecurity is designed to provide multiple layers of protection across all of the computers, networks, and programs used by a business. In order to create a unified defence against potential cyberattacks, it is important that the business, employees, processes, and technology are designed to work seamlessly together. Cybersecurity systems that function properly will be able to detect, investigate, and resolve potential weaknesses and vulnerabilities in the system before they can be exploited by a hacker or malicious software.

Hackers

- A hacker is a person who breaks into a computer system.
- A hacker is a highly-skilled computer programmer who uses their knowledge and skills to bypass a computer's security system as a means to access private information and data and achieve their goals.

There are two official definitions of hackers in the dictionary:

1. *an expert at programming and solving problems with a computer*
2. *a person who illegally gains access to and sometimes tampers with information in a computer system*

Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities −

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

Types of Hackers

Hackers can be classified into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker
4. Red Hat Hacker
5. Blue Hat Hacker
6. Green Hat Hacker

1. 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.

2. 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.

3. 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.

4. Red Hat Hacker

A red hat hacker shares some similarities with a white hat hacker. They have good intentions to save people from cyberattacks. But they mostly go about it the wrong way. In a quest to put up defenses against cyberattacks, a red hat hacker uses any means possible, even if they're illegal. Essentially, they do the right thing the wrong way.

5. Blue Hat Hacker

There are actually two different types of blue hat hacker.

One definition means that the blue hat hacker is out for revenge. They aren't motivated by money or fame, but the desire to inflict pain on their target who must have wronged them in one way or another.

But a blue hat hacker can also be an independent security expert. They are highly skilled at their job and are often invited by organizations to check the vulnerabilities in their networks.

A blue hat hacker is the go-to person if you want to deploy cybersecurity measures like penetration testing to secure your network. They initiate an attack on a system with the consent of the system owner to find effective ways to secure the network against such attacks.

6. Green Hat Hacker

A green hat hacker is a newbie to hacking. Although they are still learning the rules, they are eager to grow. And as a result of that, they do the most to prove their competence

Hacking methodologies

The following is a list of hacking techniques that you and your employees should know about and take every possible step to avoid.

Phishing Phishing is the most common hacking technique. All of our inboxes and text messaging apps are filled with phishing messages daily. These are messages that are disguised as either as an organization (Amazon, Netflix, etc.) or a person that you trust and will, in most cases, tell a story to trick you into clicking on a link or opening an attachment.

Bait and Switch Attack

- Using trusted marketing methods such as paid-for advertising on websites, attackers can trick you into visiting malicious sites. When websites sell advertising space, it can be purchased by rogue attackers. The bona fide advertisement can be replaced with a 'bad' link that can be used to download malware, lock up your browser, or compromise your systems.
- Alternatively, the advertisement may link to a legitimate website, but it will be programmed to redirect you to a harmful site.

Key Logger

- A key logger is a small piece of software that, when downloaded into your computer, will record every keystroke. The key logger will capture every keystroke on the keyboard, every username, password and credit card number, etc., exposing all of your data and personal information.

Denial of Service (DoS\DDoS) Attacks

- A Denial of Service attack is a hacking technique designed to flood your web server with a myriad of requests to the point that it overloads the web server resulting in a website crash.

- To do this, hackers will deploy botnets or zombie computers that have a single task, flood your web site with data requests.

Click Jacking Attacks

- This method tricks you into clicking on something different from what you thought you were clicking. The clickjacking element could be a button on a web page that, when clicked, performs another function, allowing others to take control of the computer. The host website may not be aware of the existence of the clickjacking element.

Fake W.A.P.

- A hacker can use software to impersonate a wireless access point (W.A.P.), which can connect to the 'official' public place W.A.P. that you are using. Once you get connected to the fake W.A.P., a hacker can access your data.
- To fool you, the hacker will give the fake W.A.P. an apparent genuine name such as "T.F. Green Aiport Free WiFi.'

Cookie Theft

- The cookies in your web browsers (Chrome, Safari, etc.) store personal data such as browsing history, username, and passwords for different sites we access. Hackers will send I.P. (data) packets that pass through your computer, and they can do that if the website you are browsing doesn't have an SSL (Secure Socket Layer) certificate.
- Websites that begin with **HTTPS://** are secure, whereas sites that start with **HTTP://** (no 'S') do not have SSL and are NOT considered secure.

Viruses and Trojans

- Viruses or Trojans are malicious software programs that, when installed on your computer, will send your data to the hacker. They can also lock your files, spread to all the computers connected to your network, and perform many other nasty actions.

Hacker's Methodology:

1. ***Foot printing***: This is a method that conducts a target analysis, identification and discovery typically through the use of open-source tools. This include dumpster diving, social engineering and the use of utility such as website hacking, treasurers, pings, network lookups etc.

2. ***Scanning***: This step extracts information from foot printing and explores more data from it. This step includes pore scanning, operating system identification and determining whether or not a machine is accessible.

3. ***Enumeration***: This is a phase where the hacker further interrogates a specific server to determine an operating system's software. It includes searching for network shared information, the specific version of the application running, user account, traffic and more.

4. ***Network Mapping***: This step is exactly as the name implies. Laying out an illustration of the target network includes taking all the resources, logs, target surveys, etc. to create a visualization of the target environment, this often looks different from the exploitative perspective.

5. ***Gaining Access***: This step is the exploitation process. This is about gaining access to a machine or network by the client's side, insider threat, supply interdiction or remote exploitation opportunity. Hackers use spear phishing, device exploitation and many more methods to conduct the exploitation.

6. ***Privilege Escalation***: Depending on the exploitation opportunity, hackers decide the intensity of the exploitation, what kind of privileges he wants to escalate. They conduct it through local exploit opportunity in order to gain system-level privileges, the highest possible user.

7. ***Post Exploitation***: This step is a compilation of many steps and is dependent upon the objective of the mission. It includes any combination of target surveys and remote

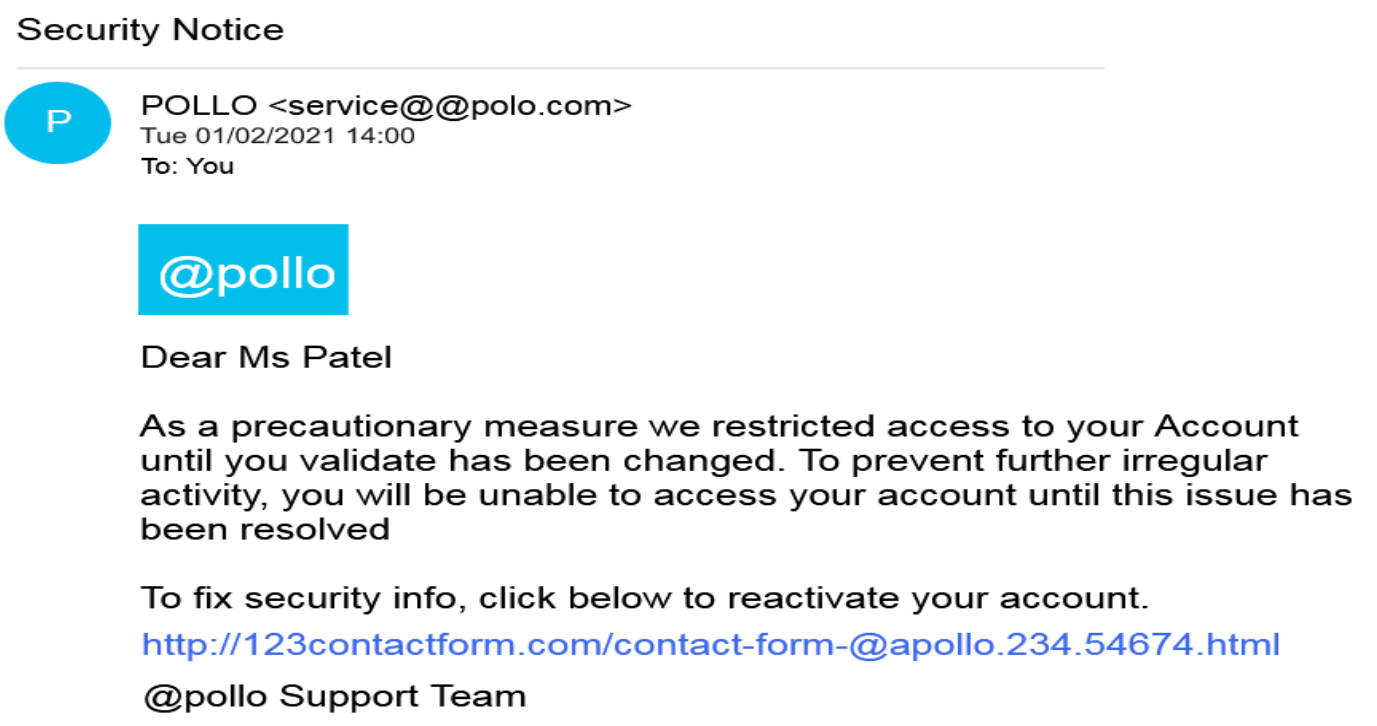
forensic analysis, cover track (cleaners), data collection, backdoor implant resistance, computer network attacks, delay target survey and more.

8. ***Forensic Analysis***: This step is to conduct analysis on the target machine for potential security mechanisms, fires or users which could either assist in obtaining the objective or harmed assessment. It basically analyses the target's operating environment.

9. ***Cover Tracks***: This is the process of removing any forensic relevant residue that was left behind as a result of exploitation. This is one of the most important steps that the hacker can perform.

10. ***Data Collection:*** The attacker is in the present to perform some activity, which involves extracting as much data as possible. Network traffic analysis is the key to this phase.

What Do You Think? A concerned customer has forwarded on what they believe to be a fraudulent email. It looks as if it has been sent by @Apollo but something appears a little 'phish-y.'



Take a look at the email. Which of the following indicates that it is in fact a phishing email? Don`t forgets, you have a chance to earn valuable defender points if you answer this correctly.

Select four correct answers,

- **The language, spelling and grammar**
- **Link URL**
- **Email address**
- **Graphics**
- Customer name

Ans: That's right! You know exactly what to look out for and have earned yourself some defender points — well done! Closer inspection reveals:

- that the sender's email domain is spelled incorrectly
- that the link URL is not pointing to @Apollo's website
- poor language, spelling and grammar
- low quality, pixelated graphics

Phishing emails can be hard to detect. For example, they will often address you by name to appear legitimate, but hackers can easily find this information on the Internet. So, it‘s important to stay alert and think before you click.

DAY-3/1

Analysing Cyber Attack

Types of Malware

- Cybercriminals use many different types of malicious software, or malware, to carry out their activities.
- 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.

Some of the most common malware.

1. 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. Spyware does this by modifying the security settings on your devices. It often bundles itself with legitimate software or Trojan horses.

2. Adware: Adware is often installed with some versions of software and is designed to automatically deliver advertisements to a user, most often on a web browser. You know it when you see it! It‘s hard to ignore when you‘re faced with constant pop-up ads on your screen. It is common for adware to come with spyware.

3.Backdoor: This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system. As a result, hackers can gain remote access to resources within an application and issue remote system commands. A backdoor works in the background and is difficult to detect.

4.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 can‘t access it. Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down. Ransomware is often spread through phishing emails that encourage you to download a malicious attachment or through a software vulnerability.

5. Scareware: This is a type of malware that uses 'scare ‘tactics to trick you into taking a specific action. Scareware mainly consists of operating system style windows that pop up to warn you that your system is at risk and needs to run a specific program for it to return to normal operation. If you agree to execute the specific program, your system will become infected with malware.

6. 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. Rootkits can also modify system forensics and monitoring tools, making them very hard to detect. In most cases, a computer infected by a rootkit has to be wiped and any required software reinstalled.

7.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. Viruses can be relatively harmless, such as those that display a funny image. Or they can be destructive, such as those that modify or delete data. Viruses can also be programmed to mutate in order to avoid detection. Most viruses are spread by USB drives, optical disks, network shares or email.

8. 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.

9. Worm: 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. Worms are responsible for some of the most devastating attacks on the Internet. In 2001, the Code Red worm had infected over 300,000 servers in just 19 hours.

Symptoms of Malware So now you know about the different kinds of malware. But what do you think their symptoms might be? Regardless of the type of malware a system has been infected with, there are some common symptoms to look out for. These include:

- an increase in central processing unit (CPU) usage, which slows down your device
- your computer freezing or crashing often
- a decrease in your web browsing speed
- unexplainable problems with your network connections
- modified or deleted files
- the presence of unknown files, programs or desktop icons
- unknown processes running
- programs turning off or reconfiguring themselves
- emails being sent without your knowledge or consent.

What Do You Think?

Match each of the descriptions to the correct malware type.

- Malware designed to track your online activity and capture your data : **Spyware**
- Software that automatically delivers advertisements: **Adware**
- Malware that holds a computer system captive until a payment is made to the attacker: **Ransmware**
- Malicious code that attaches to legitimate programs and usually spreads by USB drives, optical media, network shares or email: **Virus**
- Malicious code that replicates itself independently by exploiting vulnerabilities in networks: **Worms**

Method of Infiltration Social Engineering

Social engineering is the manipulation of people into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful, but they also prey on their weaknesses. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee's vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

Some common types of social engineering attacks.

Pretexting This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. For example, pretending to need a person's personal or financial data in order to confirm their identity.

Tailgating This is when an attacker quickly follows an authorized person into a secure, physical location.

Something for something (quid pro quo) This is when an attacker requests personal information from a person in exchange for something, like a free gift.

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.

The two main types of DoS attacks.

Overwhelming quantity of traffic This is when a network, host or application is sent an enormous amount of data at a rate which it cannot handle. This causes a slowdown in transmission or response, or the device or service to crash.

Maliciously formatted packets A packet is a collection of data that flows between a source and a receiver computer or application over a network, such as the Internet. When a maliciously formatted packet is sent, the receiver will be unable to handle it. For example, if an attacker forwards packets containing errors or improperly formatted packets that cannot be identified by an application, this will cause the receiving device to run very slowly or crash. DoS attacks are considered a major risk because they can easily interrupt communication and cause significant loss of time and money.

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. Many organizations. like Cisco, force network activities through botnet traffic filters to identify any botnet locations.

1. Infected bots try to communicate with a command and control host on the Internet.
2. The Cisco Firewall botnet filter is a feature that detects traffic coming from devices infected with the malicious botnet code.
3. The cloud-based Cisco Security Intelligence Operations (SIO) service pushes down updated filters to the firewall that match traffic from new known botnets.
4. Alerts go out to Cisco's internal security team to notify them about the infected devices that are generating malicious traffic so that they can prevent, mitigate and remedy these.

On-Path Attacks

This component is a flipcard comprised of flippable cards containing display image. Select the front face image to flip to the back face of these card to display associated text. 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: A MitM 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 its intended destination. These types of attacks are often used to steal financial information. There are many types of malware that possess MitM attack capabilities.

Man In The Mobile: A variation of man-in-middle, MitMo 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 example of a malware package with MitMo capabilities. It allows attackers to quietly capture two-step verification SMS messages that are sent to users.

SEO Poisoning

- You've probably heard of search engine optimization or SEO which, in simple terms, is about improving an organization's website so that it gains greater visibility in search engine results.
- Search engines such as Google work by presenting a list of web pages to users based on their search query. These web pages are ranked according to the relevancy of their content. While many legitimate companies specialize in optimizing websites 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.
- The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or attempt social engineering. Search engines such as Google work by presenting a list of web pages to users based on their search query. These web pages are ranked according to the relevancy of their content. While many legitimate companies specialize in optimizing websites 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. The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or attempt social engineering.

Wi-Fi Password Cracking

This is a multiple choice question. Once you have selected an option, select the submit button below You're enjoying your lunch in the canteen when a colleague approaches you. They seem distressed. They explain that they can't seem to connect to the public Wi-Fi on their phone and ask if you have the private Wi-Fi password to hand so that they can check that their phone is working. How would you respond?

Select the correct answer:

- —Yes, of course. Give me your phone and I'll put it in for you.‖
- —Sure. It's Xgff76dB.‖
- **"Mmm... I'm not sure we're allowed to use the private Wi-Fi network. Let me check with my manager first."**

Explanation: This colleague could be carrying out a social engineering attack, manipulating you to provide the password used to protect the organization's private wireless network. You can never be too careful – and, for answering correctly, you've earned some defender points. Well done! Hackers have other techniques up their sleeves. Some use **brute-force attacks**, testing possible password combinations to try and guess a password. Others are able to identify unencrypted passwords by listening in and capturing packets sent on the network. This is called **network sniffing**. If the password is encrypted, they may still be able to reveal it using a password cracking tool.

Password Attacks

Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

Some of the common password security attacks:

1. Password Spraying: This technique attempts to gain access to a system by _spraying' a few commonly used passwords across a large number of accounts. For example, a cybercriminal uses 'Password123' with many usernames before trying again with a second commonly-used password, such as _qwerty.' This technique allows the perpetrator to remain undetected as they avoid frequent account lockouts.

2. 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.

3. 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

4. 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.

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

If you store a password in clear, readable text, anyone who has access to your account or device, whether authorized or unauthorized, can read it

. **Cracking Times** It looks as if the hackers are trying everything to crack @Apollo's private Wi-Fi password. We have to make sure that the password is strong enough to withstand their attack! Take a look at the following passwords. Click the numbers to put them in the correct order according to how long you think it would take an attacker to crack each one using brute-force, where 1 is the shortest amount of time and 4, the highest.

Unorder Correct Order

- H$1gh#7iD@3

Password

- 3trawberry

Password

- K4km9n2R
- H$1gh#7iD@3

Explanation: You've secured the organization's private Wi-Fi password and earned some more defender points — great work! Carrying out brute-force attacks involves the attacker trying several possible combinations in an attempt to guess the password. These attacks usually involve a word-list file — a text file containing a list of words from a dictionary.

A program such as Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack or Medusa will then try each word and common combinations until it finds a match. Because brute-force attacks take time, complex passwords take much longer to guess.

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 targets systems and remain there undetected.

Security Vulnerability and Exploits *Security vulnerabilities* are any kind of software or 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 a vulnerability to carry out an *attack*, the goal of which is to gain access to a 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 basically 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 neighbour 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.

Meltdown and Spectre Google security researchers discovered Meltdown and Spectre, two hardware vulnerabilities that affect almost all central processing units (CPUs) released since 1995 within desktops, laptops, servers, smartphones, smart devices and cloud services. Attackers exploiting these vulnerabilities can read all memory from a given system (Meltdown), as well as data handled by other applications (Spectre). The

Meltdown and Spectre vulnerability exploitations are referred to as side-channel attacks (information is gained from the implementation of a computer system). They have the ability to compromise large amounts of memory data because the attacks can be run multiple times on a system with very little possibility of a crash or other error. Hardware vulnerabilities are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and good physical security are sufficient protection for the everyday user.

Software Vulnerabilities Software vulnerabilities are usually introduced by errors in the operating system or application code. **Select the logo to find out more about the SYNful Knock vulnerability discovered in Cisco Internetwork Operating System (IOS) in 2015.**

The SYNful Knock vulnerability allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco ISR routers, from which they could monitor all network communication and infect other network devices. This vulnerability was introduced into the system when an altered IOS version was installed on the routers. To avoid this, you should always verify the integrity of the downloaded IOS image and limit the physical access of such equipment to authorized personnel only.

Categorizing Software Vulnerabilities Most software security vulnerabilities fall into several main categories.

1. Buffer Flow: 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.

2. Non-Validated Input: Programs often require data input, but this incoming data could have malicious content, designed to force the program to behave in an unintended way. For example, consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.

3. 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.

4. Weaknesses in Security Practice: 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.

5. Access Control Problem: 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. Nearly all access controls and security practices can be overcome if an attacker has physical access to target equipment. For example, no matter the permission settings on a file, a hacker can bypass the operating system and read the data directly off the disk. Therefore, to protect the machine and the data it contains, physical access must be

restricted, and encryption techniques must be used to protect data from being stolen or corrupted.

Software Updates The goal of software updates is to stay current and avoid exploitation of vulnerabilities. Microsoft, Apple and other operating system producers release patches and updates almost every day and applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them. Despite the fact that organizations put a lot of effort into finding and patching software vulnerabilities, new vulnerabilities are discovered regularly. That‘s why some organizations use third party security researchers who specialize in finding vulnerabilities in software, or actually invest in their own penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited. Google‘s Project Zero is a great example of this practice. After discovering a number of vulnerabilities in various software used by end users, Google formed a permanent team dedicated to finding software vulnerabilities.

DAY 4/1
2.3. Data Maintenance

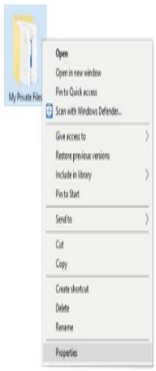
What Is Encryption? Encryption is the process of converting information into a form in which unauthorized parties cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form. Note that the encryption itself does not prevent someone from intercepting the data. It can only prevent an unauthorized person from viewing or accessing the content. In fact, some criminals may decide to simply encrypt your data and make it unusable until you pay a ransom.

How Do You Encrypt Your Data? Software programs are used to encrypt files, folders and even entire drives. Encrypting File System (EFS) is a Windows feature that can encrypt data. It is directly linked to a specific user account and only the user that encrypts the data will be able to access it after it has been encrypted using EFS. Select the headings to discover how to encrypt data using EFS in all Windows versions.

Step 1

Select one or more files or folders.

Step 2



Right click the selected data and go to '**Properties**.'

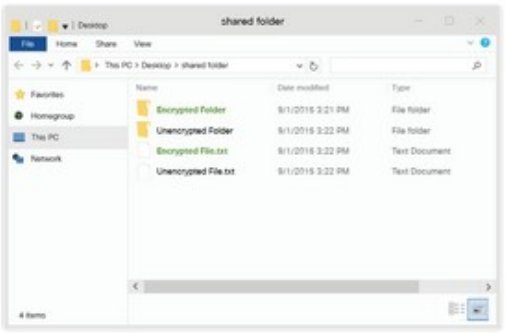
Step 3

Find and click '**Advanced**.'

Step 4

Select the '**Encrypt contents to secure data**' check box.

Step 5



Files and folders that have been encrypted with EFS are displayed in green as shown here.

Back Up Your Data Having a backup may prevent the loss of irreplaceable data. To back up data properly, you will need an additional storage location for the data and you must copy the data to that location regularly. **Some of these additional storage locations.**

1. **Home Network:** Storing your data locally means that you have total control of it.

2. Secondary location: You could copy all of your data to a network attached storage device (NAS), a simple external hard drive or maybe even back up important folders on thumb drives, CDs, DVDs or tapes. In this scenario, you are the owner of the data and you are totally responsible for the cost and maintenance of the storage device equipment.

3. The cloud: You could subscribe to a cloud storage service, like Amazon Web Services (AWS). The cost of this service will depend on the amount of storage space you need, so you may need to be more selective about what data you back up. You will have access to your backup data as long as you have access to your account. One of the benefits of using a cloud storage service is that your data is safe in the event of a storage device failure or if you experience an extreme situation such as a fire or theft.

Are They Really Gone? This is a multiple choice question. Once you have selected an option, select the submit button below You‘ve logged into your laptop but it contains some photos belonging to the previous user, who no longer works at @Apollo. Your line manager asks you to delete them. You drag the photos into the recycle bin, open the recycle bin, select them and click _Delete‘ once again. That should do it! Do you think the photos are really gone from the laptop?

- Yes, the photos can no longer be retrieved
- **No, the photos are just inaccessible from the operating system**

Explanation: When you move a file to the recycle bin and delete it permanently, the file is only inaccessible from the operating system. Anyone with the right forensic tools could still recover the file due to a magnetic trace left on the hard drive.

How Do You Delete Your Data Permanently?

Have you ever had to delete data or get rid of a hard drive? If so, did you take any precautions to safeguard the data to keep it from falling into the wrong hands?

What you should do to ensure you delete your files securely and permanently.

1. To erase data so that it is no longer recoverable, it must be overwritten with ones and zeroes multiple times, using tools specifically designed to do just that. SDelete from Microsoft claims to have the ability to remove sensitive files completely. Shred for Linux and Secure Empty Trash for Mac OS X claim to provide a similar service.

2. The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device. Many criminals have taken advantage of files thought to be impenetrable or irrecoverable! Don't forget about data that may be stored online in the cloud. These copies will also need to be deleted.

Terms of Service

You have been asked to set up an online photo storage and sharing account to be used for creative collaboration with the design department and other teams at @Apollo. When signing up, you are prompted to sign a service agreement with the provider. You don't think too much about it and agree to all the terms without reading them. This is a multiple choice question. Once you have selected an option, select the submit button below You have just signed a Terms of Service agreement. But do you know what this is? Consider the following options and choose the one you think best describes a Terms of Service agreement.

Select the correct answer

- A contract outlining the services that you expect to receive from the service provider and how you will use their service
- An informal arrangement that sets out the rules of the relationship between you, the service provider and others who use the service
- **A legally binding contract that governs the rules of the relationship between you, the service provider and others who use the service**

Understand the Terms The Terms of Service will include a number of sections, from user rights and responsibilities to disclaimers and account modification terms.

- The data use policy outlines how the service provider will collect, use and share your data.
- The privacy settings allow you to control who sees information about you and who can access your profile or account data.
- The security policy outlines what the company is doing to secure the data it obtains from you.

What Are You Agreeing To? You have successfully created the @Apollo account and agreed to the Terms of Service of the online photo sharing company. But do you really know what you have signed up for? Let's take a closer look.

The Data Use Policy The data use policy of the company you used to set up the account states that for any content you publish: *"you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings)"*. What does this statement really mean? **Select the correct answer**

- You no longer own your content and the photo sharing company can re-use any of your content but only in specific circumstances
- **You own your content but the photo sharing company can re-use any of your content for any purposes**
- You own your content and the photo sharing company has to get permission to re-use your content

Privacy Settings

As you didn't set the privacy settings before you accepted the terms, default settings were applied. Which of the following do you think is more likely?

Select the correct answer

- No one will be able to see information about you and access your profile until you change the preferences in privacy settings
- **Anyone will be able to see information about you and access your profile until you change the privacy settings**

Before You Sign Up What factors should you consider before you sign up to an online service?

- Have you read the Terms of Service?
- What are your rights regarding your data?
- Can you request a copy of your data?
- What can the provider do with the data you upload?
- What happens to your data when you close your account?

Protect Your Data You must always take appropriate action to protect your data and safeguard your account. Thinking back to the Terms of Service examples outlined above, what can you do to protect yourself when you enter into an agreement with an online service provider? What can you do to safeguard your account and protect your data? Ans: To protect your data and safeguard your account, you should:

always read the Terms of Service when registering for a new service and decide whether the service is worth waiving your rights to your data for

select your privacy settings rather than accepting the default

limit the group of people you share content with

review the service provider's security policy to understand what they are doing to protect your data

change your passwords periodically, use a complex password and two factor authentication to secure your account.

Safeguarding Your Online Privacy Two Factor Authentication

Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentications to add an extra layer of security for account logins. Besides your username and password or personal identification number (PIN), two factor authentication requires a second token to verify your identity. This may be a:

- physical object such as a credit card, mobile phone or fob
- biometric scan such as a fingerprint or facial and voice recognition
- verification code sent via SMS or email.

Be careful! Even with two factor authentications, hackers can still gain access to online accounts through phishing attacks, malware and social engineering.

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.

- You are looking forward to registering for Cisco's 'Cybersecurity Essentials,' the next course in this series, to help you develop your career. But you must be logged into the eLearning portal to do so.
- You can't remember your login details, but that's OK. The portal gives you the option of logging in using your credentials from a social media website such as Facebook or via another account such as Google.
- So instead of having to reset your login details, you log into the eLearning portal using your existing social media accounts and register for your next course with ease. You can't wait to get started!

Social Sharing You decide to update your new job position on your social networks. When doing so, one of the sites asks you to update your profile information to ensure you receive the content that you really don't want to miss! You take a look at the missing fields. Which ones do you fill in? Remember, answering correctly will improve your privacy settings, so think carefully about the information you want to share online.

Select the two correct answers

- **Name of the organization**
- Email address
- Your colleagues' names and contact information
- Your manager's name and contact information
- **Your profile picture**
- Date of birth
- Mobile phone number

Explanation: You've shared just the right amount of information and boosted your online privacy settings. Click the icon in the top right-hand corner to check your progress. In order to safeguard your privacy on social media, it's important to share as little personal information as possible. You should also check your social media settings so that only people you know can see your activities or engage in conversations with you. The more information you share online, the easier it is for someone to create a profile about you and take advantage of you, both online and offline.

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:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab or private window
- **Safari**: Private browsing

When private mode is enabled, cookies — files saved to your device to indicate what websites you've visited — are disabled. Therefore, any temporary internet files are removed and your browsing history is deleted when you close the window or program. This may help to prevent others from gathering information about your online activities and trying to entice you to buy something with targeted ads. Even with private browsing enabled and cookies disabled, companies are constantly developing new ways of fingerprinting users in order to track their online behavior. For example, some intermediary devices, like routers, can gather information about a user's web surfing history.

Scenario 1

Do you know what information is safe to share on social media sites? It's surprising what people post on social media without thinking! Which of the following do you think poses a risk if posted on social media? **Select three correct answers**

Explanation: Photos showing bank details or valuable goods and vacation information always put you at risk, and especially when you've previously given clues about where you live, or where you are going to visit. Always stop and think about what you are about to post — would you tell it to a complete stranger?!

Scenario 2

When creating a new account in an online service, what password do you use? Is it secure? In your own words, describe what a password manager application is, how they work and why they are beneficial. If you have used a password manager before, outline a few details and share your experience.

Explanation: Password manager applications can protect passwords by saving them in a secure encrypted form. They enable random passwords to be generated and managed easily, averting the need for users to have the same password for multiple accounts, which presents a security risk.

Scenario 3 Connecting to an open Wi-Fi hotspot can make your system and data vulnerable to an attack. @Apollo 's Sales Manager is traveling to meet a client. She forgot to download the contract from @Apollo 's server to bring to the meeting with her. The train has an open Wi-Fi network. She contacts you to ask what she should do. What would you advise?

- **She should access the train's open Wi-Fi network and connect to the @Apollo servers using the VPN connection on her work laptop.**
- She should wait until she arrives at the client 's office and ask for the access code to their Wi-Fi network, then access @Apollo 's service directly on her work laptop.

- She should use the 4G connection on her phone to find an alternative open Wi-Fi network.
- She should forget about the contract for the meeting and catch up on other online work using the train ‘s open Wi-Fi to access the https websites she needs.

Explanation: The Sales Manager can use the VPN connection on her laptop to create a secure, encrypted channel back to @Apollo, on top of the untrusted open Wi-Fi network. This way, all the traffic from her laptop will be securely transferred over the secure VPN tunnel.

Scenario 4 Are you aware of the risks that come when downloading a trial version of a program? A designer at @Apollo needs to install some image manipulation software. The mainstream application is really expensive, and it’s only needed for one small piece of a one-off project. The Design Manager says this would not be a cost-effective purchase and says to install an alternative free application instead — the manager doesn‘t mind if it‘s from an untrusted source as they feels the risks are low. Should the designer take the manager ‘s advice? Select the correct answer

- **No, the designer should check with a member of the IT team before installing any applications from a non-trusted source.**
- Yes, the Design Manager feels the risk is low so that must be right!
- Of course, the designer has been given an instruction by their manager so it‘s fine to install the free application. It will save the company some money!
- No, the designer should purchase the trusted application from the mainstream software provider and pay for it using their own money.

Scenario 5 Have you ever had a warning message telling you to download a diagnostics program that will make your computer safe? You should be aware of the risks.

DAY-4/2

Protecting Your Devices and Network You've just been issued with a new laptop at @Apollo and are getting ready to set it up. What steps would you take to secure it before use? **Write your thoughts** Ans: To make your device safe and secure, you should:

- turn the firewall on
- install antivirus and antispyware
- manage your operating system and browser
- set up password protection.

Protecting Your Computing Devices Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it's important to protect the security of your devices.

1. Turn the Firewall On: You should use at least one type of firewall (either a software firewall or a hardware firewall on a router) to protect your device from unauthorized access. The firewall should be turned on and constantly updated to prevent hackers from accessing your personal or organization data.

2. Install Antivirus and Antispyware: Malicious software, such as viruses and spyware, are designed to gain unauthorized access to your computer and your data. Once installed, viruses can destroy your data and slow down your computer. They can even take over your computer and broadcast spam emails using your account. Spyware can monitor your online activities, collect your personal information or produce unwanted pop-up ads on your web browser while you are online. To prevent this, you should only ever download software from trusted websites. However, you should always use antivirus software to provide another layer of protection. This software, which often includes antispyware, is designed to scan your computer and incoming email for viruses and delete them. Keeping your software up to date will protect your computer from any new malicious software that emerges.

3. Manage your Operating System and Browser: Hackers are always trying to take advantage of vulnerabilities that may exist in your operating system (such as Microsoft Windows or macOS) or web browser (such as Google Chrome or Apple Safari). Therefore, to protect your computer and your data, you should set the security settings on your computer and browser to medium level or higher. You should also regularly update your computer's operating system, including your web browser, and download and install the latest software patches and security updates from the vendors.

4. Set Up Password Protection: All of your computing devices, including PCs, laptops, tablets and smartphones, should be password protected to prevent unauthorized access. Any stored information, especially sensitive or confidential data, should be encrypted. You should only store necessary information on your mobile device, in case it is stolen or lost. Remember, if any one of your devices is compromised, the criminals may be able to access all of your data through your cloud storage service provider, such as iCloud or Google Drive. IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most IoT devices have their original software. If vulnerabilities are found in the software, the IoT device is likely to be vulnerable. And to make the problem worse, IoT devices require Internet access, most often relying on your local network. The result is that when IoT devices are compromised, they allow hackers access to your local network and data. The best way to protect yourself from this scenario is to set up any IoT devices on an isolated network. Check out Shodan, a web-based IoT device scanner that helps you identify any vulnerable devices on the Internet.

Wireless Network Security at Home Wireless networks allow Wi-Fi enabled devices, such as laptops and tablets, to connect to the network by way of a preset network identifier, known as the service set identifier (SSID). Although a wireless router can be configured so that it doesn't broadcast the SSID, this should not be considered adequate

security for a wireless network. Hackers will be aware of the preset SSID and default password. Therefore, these details should be changed to prevent intruders from entering your home wireless network. Furthermore, you should encrypt wireless communication by enabling wireless security and the WPA2 encryption feature on your wireless router. But be aware, even with WPA2 encryption enabled, a wireless network can still be vulnerable.

The discovery of a security flaw in the WPA2 protocol in 2017. This vulnerability can be exploited by key reinstallation attacks (KRACKs) by intruders. In simple terms, attackers break the encryption between a wireless router and a wireless device, giving them access to network data. This flaw affects all modern, protected Wi-Fi networks. To mitigate this situation, you should:

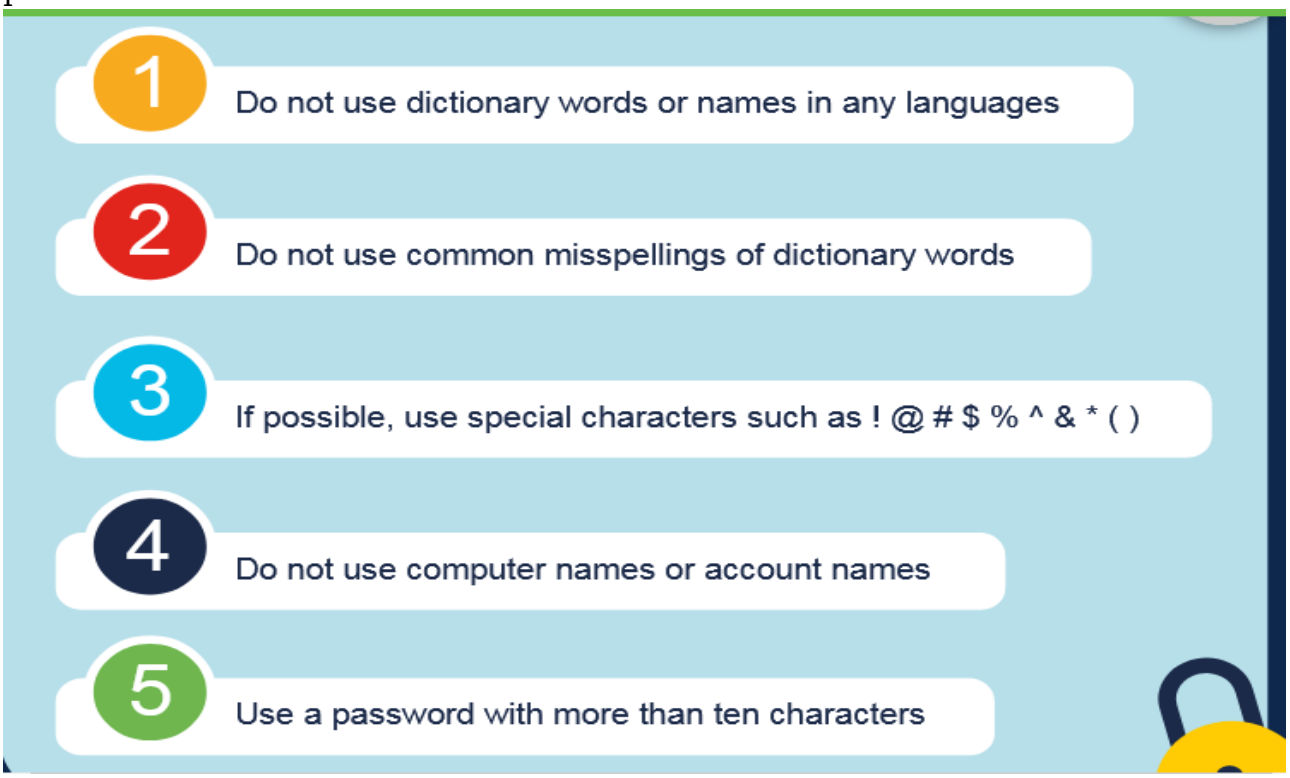
- update all wireless capable devices such as routers, laptops and mobile devices, as soon as security updates become available
- use a wired connection for any devices with a wired network interface card (NIC)
- use a trusted virtual private network (VPN) service when accessing a wireless network.

Public Wi-Fi Risks When you are away from home, you can access your online information and surf the Internet via public wireless networks or Wi-Fi hotspots. However, there are some risks involved, which mean that it is best not to access or send any personal information when using public Wi-Fi. You should always verify that your device isn't configured with file and media sharing and that it requires user authentication with encryption. You should also use an encrypted VPN service to prevent others from intercepting your information (known as eavesdropping) over a public wireless network. This service gives you secure access to the Internet, by encrypting the connection between your device and the VPN server. Even if hackers intercept a data transmission in an encrypted VPN tunnel, they will not be able to decipher it. Don't forget that the Bluetooth wireless protocol, found on many smartphones and tablets, can also be exploited by hackers to eavesdrop, establish remote access controls, distribute malware and drain batteries! Therefore, my top tip is to keep Bluetooth turned off when you aren't using it.

Password Security You've logged into your new laptop and it has prompted you to change your network password. You already struggle to remember the few passwords you use for your personal accounts online. You ask one of your colleagues for their advice. They tell you to use one of the passwords you use for your personal accounts — that's what they do! They keep their personal passwords written down at the back of their diary, just in case they forget them.

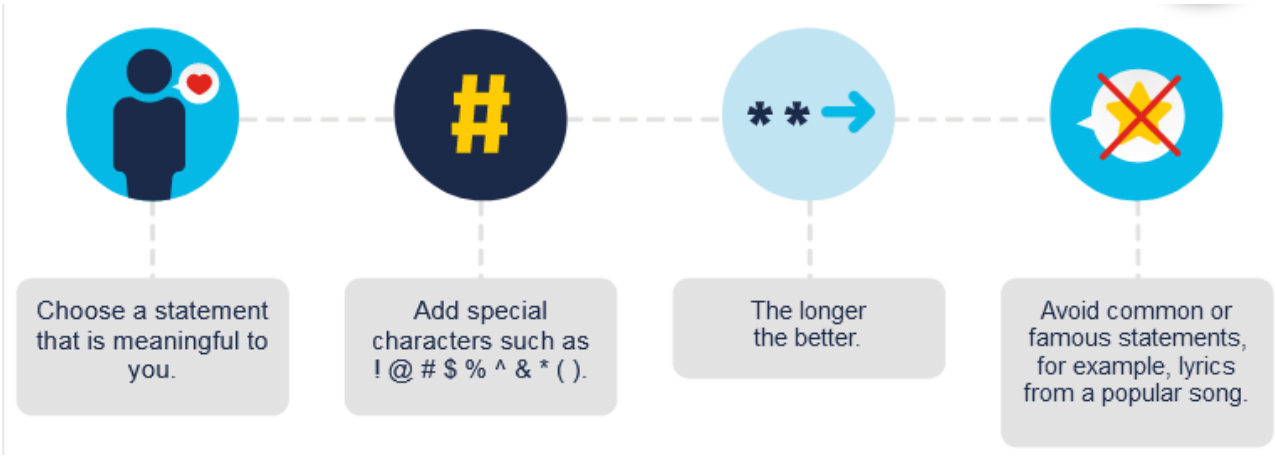
How would you rate your colleague's attitude to password security on a scale of 1 (bad practice) to 5 (good practice)? Ans: Bad Practice: identified that your colleague is advocating bad password practice and improved your privacy settings. Check your progress by clicking on the icon in the top right-hand corner of your screen. It's important that all of your online accounts have a unique password. Using the same passwords leaves you and your data vulnerable to cybercriminals. And if it becomes too much to remember all of these passwords, you should use a password manager. This tool stores and encrypts all of your passwords and helps you log into your accounts automatically

A Strong Password Here are a few simple tips to help you when choosing a strong password.



Using a Passphrase

In order to prevent unauthorized access to your devices, you should consider using passphrases instead of passwords. A passphrase generally takes the form of a sentence (_Acat th@tlov3sd0gs.‘), making it easier for you to remember. And because it‘s longer than a typical password, it‘s less vulnerable to dictionary or brute-force attacks. **Here are a few tips for creating a good passphrase.**



Password Guidelines

The United States National Institute of Standards and Technology (NIST) has published improved password requirements. NIST standards are intended for government applications but can serve as a standard for other sectors as well. These guidelines aim to place responsibility for user verification on service providers and ensure a better experience for users overall. They state:

- Passwords should be at least eight characters, but no more than 64 characters.
- Common, easily guessed passwords, such as password or abc123 should not be used.

- There should be no composition rules, such as having to include lower and uppercase letters and numbers.
- Users should be able to see the password when typing, to help improve accuracy.
- All printing characters and spaces should be allowed.
- There should be no password hints.
- There should be no password expiration period.
- There should be no knowledge-based authentication, such as having to provide answers to secret questions or verify transaction history.

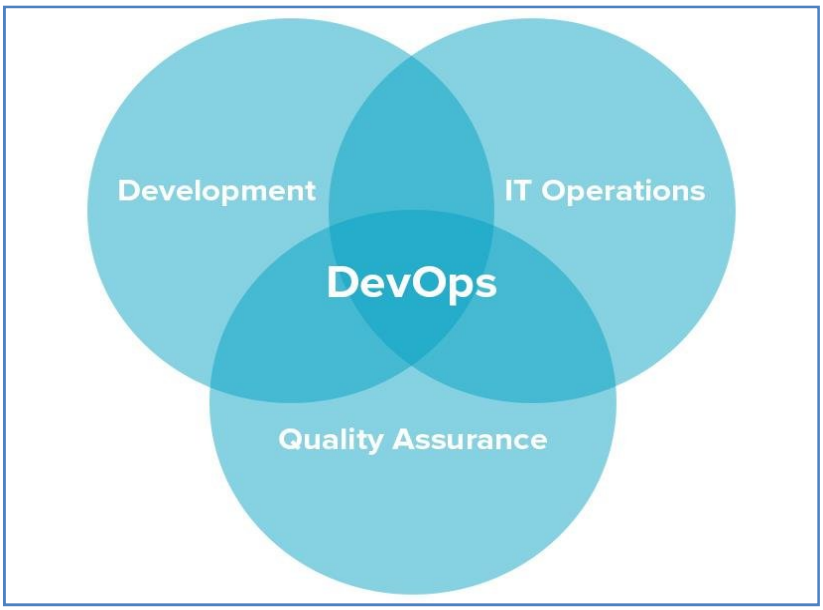
Course: Cyber Security **Code: 20CS54I**

WEEK-12: DAY-1: Session-2

- **DevOps and Security Challenges**
- **Understand the Core Principles and Patterns behind DevOps**
- **Recognize how DevOps works and identify keys to success**

DevOps and Security Challenges:

- DevOps is a software development approach that utilizes the Agile methodology to integrate and streamline the development and operations process. The result is a faster and more efficient development process.
- The downside of DevOps is that the fast pace it promotes doesn't cover security. The solution is to include security protocols and practices across the DevOps pipeline.
- DevOps security (DevSecOps) is an approach to cybersecurity that focuses on application development and development operations (DevOps). It combines three phrases:
  1. Development
  2. Operations
  3. Security



- The goal of DevOps security is to remove barriers between an organization's software development and its IT operations. Namely, it calls for speed and intense, fast communication and collaboration. It is essentially a philosophy that covers developers' code and its subsequent need to work (and grow) properly with the organization's employees and customers.
- The core of the DevOps security philosophy is **continuous deployment.** Development and IT teams work closely and rapidly to add to and fix software. This means, for example, adding new features and troubleshooting bugs so that they can be continuously released in fast cycles without causing disruptions. It enables teams, other employees, and customers to continue interacting with software without interruption.
- In short, business operations are continuous and don't face unnecessary interruptions.

Why is DevOps Security Needed?

- Security is one of the critical areas of concern for developers. Developers often rely heavily on Software Development Kits (SDKs) or at least on other frameworks or individual programs. But third-party code can represent a serious security vulnerability in these cases. As far as a developer is concerned, their organization doesn't necessarily know whether they've been addressed before.

DevOps Security Challenges:

- DevOps has become the standard of software development in the past years. Introducing DevOps security presents its own set of challenges, as explained below.

i) Faster development process

- The fast pace of a DevOps process can lead to an increase in coding mistakes, which could result in undetected bugs and errors. Attackers look for coding mistakes they can exploit to gain access to digital assets.

ii) Serverless computing

- The term refers to a cloud computing model where the cloud provider manages the infrastructure resources. The cloud platform also manages the security of the applications hosted in it. Migrating to a serverless computing environment presents some challenges for organizations. When migrating applications or data to the cloud, you can't always be sure how the platform's security work until deployment. Another concern is the exposure of sensitive data during migration.

iii) Collaboration challenges

- DevOps requires the collaboration of two different teams: development and operations. Considering that they are used to working in a siloed way, unifying their processes can be challenging. Undefined roles and policies can lead to gaps in security.

iv) The interconnectedness of the DevOps process

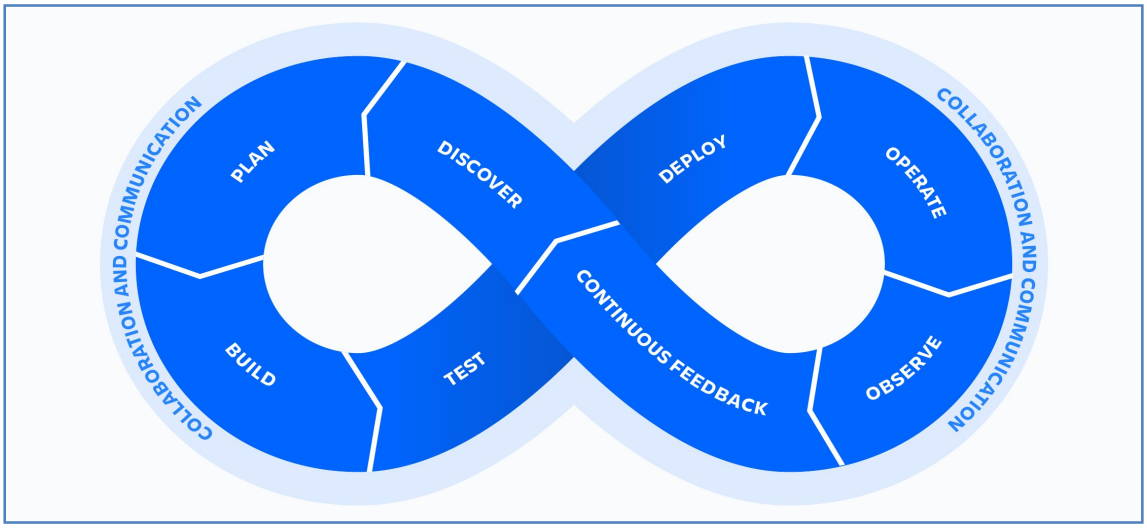
- One of the characteristics of DevOps is that requires the constant collaboration of the teams. This highly interconnected environment allows for the exchange of privileged information. Teams share account credentials, tokens, and SSH keys. Systems such as applications, containers, and microservices also share passwords and tokens. A common pitfall of DevOps environments is poor secrets management. This provides a path for attackers to disrupt operations, and steal information.

v) Implementing security in CI/CD

- In a traditional siloed development environment, security has always come at the end of the pipeline. Typically, a security team performs security testing after the development stage, before sending the application into production.
- Integrating security into the pipeline can be challenging. By nature, security teams tend to take their time to secure every part of the code, which in turn clashes with the fast pace of the DevOps process. Security risks can arise during the integration stage until the DevOps model is fully implemented and running.

Understand the Core Principles and Patterns behind DevOps:

- In 2010 Damon Edwards and John Willis came up with the CAMS model to showcase the key values of DevOps. A CAM is an acronym that stands for Culture, Automation, Measurement, and Sharing.
- DevOps is more than just development and operations teams working together. It's more than tools and practices. DevOps is a mindset, a cultural shift, where teams adopt new ways of working.



- A DevOps culture means developers get closer to the user by gaining a better understanding of user requirements and needs. Operations teams get involved in the development process and add maintenance requirements and customer needs. It means adhering to the following key principles that help DevOps teams deliver applications and services at a faster pace and higher quality than organizations using the traditional software development model.

Collaboration

- The key premise behind DevOps is collaboration. Development and operations teams coalesce into a functional team that communicates, shares feedback, and collaborates throughout the entire development and deployment cycle. Often, this means development and operations teams merge into a single team that works across the entire application lifecycle.
- The members of a DevOps team are responsible for ensuring quality deliverables across each facet of the product. This leads to more 'full stack' development, where teams own the complete backend-to-frontend responsibilities of a feature or product. Teams will own a feature or project throughout the complete lifecycle from idea to delivery. This enhanced level of investment and attachment from the team leads to higher quality output.

Automation

- An essential practice of DevOps is to automate as much of the software development lifecycle as possible. This gives developers more time to write code and develop new features. Automation is a key element of a CI/CD pipeline and helps to reduce human errors and increase team productivity. With automated processes, teams achieve continuous improvement with short iteration times, which allows them to quickly respond to customer feedback.

Continuous Improvement

- Continuous improvement was established as a staple of agile practices, as well as lean manufacturing and Improvement. It's the practice of focusing on experimentation, minimizing

waste, and optimizing for speed, cost, and ease of delivery. Continuous improvement is also tied to continuous delivery, allowing DevOps teams to continuously push updates that improve the efficiency of software systems. The constant pipeline of new releases means teams consistently push code changes that eliminate waste, improve development efficiency, and bring more customer value.

Customer-centric action

- DevOps teams use short feedback loops with customers and end users to develop products and services centered on user needs. DevOps practices enable rapid collection and response to user feedback through use of real-time live monitoring and rapid deployment. Teams get immediate visibility into how live users interact with a software system and use that insight to develop further improvements.

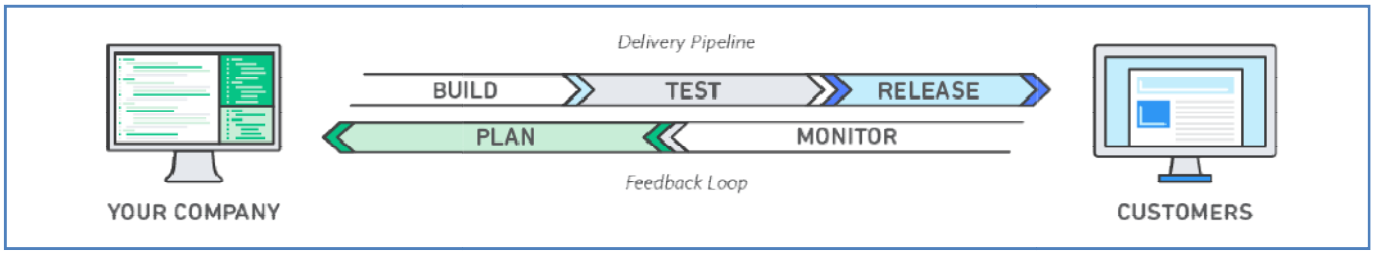
Create with the end in mind

- This principle involves understanding the needs of customers and creating products or services that solve real problems. Teams shouldn't 'build in a bubble', or create software based on assumptions about how consumers will use the software. Rather, DevOps teams should have a holistic understanding of the product, from creation to implementation.

Recognize how DevOps works and identify keys to success:

DevOps Model Defined:

- DevOps is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes. This speed enables organizations to better serve their customers and compete more effectively in the market.



How DevOps Works:

- Under a DevOps model, development and operations teams are no longer "siloed." Sometimes, these two teams are merged into a single team where the engineers work across the entire application lifecycle, from development and test to deployment to operations, and develop a range of skills not limited to a single function.
- In some DevOps models, quality assurance and security teams may also become more tightly integrated with development and operations and throughout the application lifecycle. When security is the focus of everyone on a DevOps team, this is sometimes referred to as DevSecOps.
- These teams use practices to automate processes that historically have been manual and slow. They use a technology stack and tooling which help them operate and evolve applications quickly and reliably. These tools also help engineers independently accomplish tasks (for example, deploying code or provisioning infrastructure) that normally would have required help from other teams, and this further increases a team's velocity.

Here, then, are 5 key characteristics of successful DevOps deployments:

1) Respect the organization's culture

- The most fundamental success factor for DevOps deployment is the organization's people, and the way that they work together. DevOps is a fundamental change in the way the organization functions. Unfortunately, it is considerably more difficult to bring about cultural change in an organization than it is to adopt a handful of new software practices.
- A collaborative and respectful culture must be created across the company's entire IT organization - with Development (Dev) and Operations (Ops) collaborating productively together. A fundamental philosophy of DevOps is that developers, operations staff, and support teams must see one other as important stakeholders and actively seek to work together.

2) Take small steps

- Moving to a DevOps organization is easier and meets with much less resistance if it is implemented through 'baby steps': with simpler and more frequent deployments, rather than one large change, which is always much harder to adapt to. Smaller deployments are easier to test, and carry a much smaller risk.

3) Use system orchestration to get the benefits of automation

- While implementing DevOps, companies must be aware of creating new potential silos as they implement domain-specific deploys. A central coordination service is needed that provides end-to-end visibility of the way the different aspects of the network system is deployed while allowing each domain to manage itself autonomously to reduce management complexity and functional duplication. Multi-domain system orchestration enables services to be managed and manipulated from end-to-end, from a central point and at a high level of abstraction.

4) Accommodate legacy systems where necessary

- Large enterprises, particularly in sensitive sectors such as financial services and healthcare, for example, often have complex legacy infrastructure constraints.
- Implementing DevOps on one business practice might impact another application, or have legal ramifications. These organizations must think about new ways to incorporate the DevOps mentality into their standard processes.
- Enterprises like these must be pragmatic about legacy systems: heterogeneity is a fact of network life. Such organizations might consider what Gartner refers to as 'bimodal IT' - balancing the need to maintain legacy processes in some areas, while automating where possible to achieve both IT agility and stability.

5) Adopt a DevOps toolkit and then do it themselves

- The DevOps toolkit that an enterprise chooses is the enabler to develop new, virtualized services quickly, customize them and differentiate them. Rather than outsourcing to big integrators to the extent that they might find themselves dependent on them, enterprises must choose a toolkit that empowers them to take control after having someone take them through the initial startup and training.

Basics of cloud computing:

- Cloud Computing is an emerging style of IT delivery in which applications, data and IT resources rapidly provisioned and provided as standardized offerings to users over the web in a flexible pricing model.
- "The National Institute of Standards and Technology (NIST) defines cloud computing as a "pay-per-use model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- "The National Institute of Standards and Technology (NIST) defines cloud computing as a "pay-per-use model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Why is cloud computing necessary?

- Cost Reduction
- Universal Access
- Software Updates
- Application Alternatives
- Potential and cost Effective
- Flexibility

- Users can scale services to fit their needs, customize applications and access cloud services from anywhere with an internet connection.

Introduction to key cloud services (Compute, storage, networking):

- Fundamentally the term "compute" refers to physical servers comprised of the processing, memory, and storage required to run an operating system such as Microsoft Windows or Linux, and some virtualized networking capability.

Compute Services

The components of a compute server include the following:

- **Processor or Central Processing Unit (CPU)** – the CPU is the brains of the computer and carries out the instructions of computer programs
- **Memory or Random Access Memory (RAM)** – within a computer memory is very high-speed storage for data stored on an integrated circuit chip
- **Storage** – the storage location for the operating system files (and optionally data). This is typically a local disk stored within the computer or a network disk attached using a block protocol such as iSCSI
- **Network** – physical network interface cards (NICs) to support connectivity with other servers

- When used in cloud computing, the operating system software that is installed directly on the server is generally a hypervisor that provides a hardware abstraction layer onto which additional operating systems can be run as virtual machines (VMs) or "instances". This technique is known as hardware virtualization.

Storage as a Services(Staas)

- Storage as a service defines a business model where a large company will rent spaceon their storage infrastructure to a small company or an individual who lack thebudget to compensate for it on their own.
- The main advantage of StaaS is an enterprise in cost savings.
- The storage is rented by the provider using either accost -per-data-transferred or cost-per-gigabyte-stored model.
- The users need not to compensate for infrastructure, they just pay for how much data they transferred and saved on the server of the provider.

- If there is any loss of data, the client can get the lost data from provider of the service.
- Examples: web e-mail providers such as yahoo, Gmail, hot mail, sites like flickr, Picasa,YouTube, facebook.

Network as a service

What is cloud networking?

- **Cloud networking** is a type of IT infrastructure in which some or all of an organization's network capabilities and resources are hosted in a public or private cloud platform, managed in-house or by a service provider, and available on demand.
- Companies can either use on-premises cloud networking resources to build a private cloud network or use cloud-based networking resources in the public cloud, or a hybrid cloud combination of both. These network resources can include virtual routers, firewalls, and bandwidth and network management software, with other tools and functions available as required.

Why cloud networking?

- Businesses today turn to the cloud to drive agility, deliver differentiation, accelerate time-to-market, and increase scale. The cloud model has become the standard approach to build and deliver applications for the modern enterprise.
- Cloud networking has also played a critical role in the way organizations address their growing infrastructure needs, regional expansions, and redundancy plans. Many organizations are adopting a multi-data center strategy and leveraging multiple clouds from multiple cloud service providers (CSPs).

Benefits of cloud networking

- Most organizations have become a patchwork of on-premises technologies, public cloud services, legacy applications and systems, and emerging technologies — a complex situation that contributes to a weak security posture and results in inadequate governance, visibility, and manageability across fragmented networks.
- A **Virtual Cloud Network is VMware's vision of the future of networking**. It is an architectural approach (not a product) built in software at global scale from **edge-to-edge**, that's able to deliver consistent, pervasive connectivity and security for apps and data wherever they reside, independent of underlying physical infrastructure.
- Whether your workloads are on premises or in the cloud, the same network and security stack can be used to provide connectivity, security, and visibility
- It is also the kind of next-generation networking service consumption technology that IT is increasingly adopting to provide the digital fabric that helps unify a hyper-distributed world.

What is network virtualization?

- Network Virtualization (NV) refers to abstracting network resources that were traditionally delivered in hardware to software. NV can combine multiple physical networks to one virtual, software-based network, or it can divide one physical network into separate, independent virtual networks.
- Network virtualization software allows network administrators to move virtual machines across different domains without reconfiguring the network. The software creates a network overlay that can run separate virtual network layers on top of the same physical network fabric.

Why network virtualization?

- Network virtualization is rewriting the rules for the way services are delivered, from the software-defined data center (SDDC), to the cloud, to the edge. This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized. Modern networks must keep up with the demands for cloud-hosted, distributed apps, and the increasing threats of cybercriminals while delivering the speed and agility you need for faster time to market for your applications. With network virtualization, you can forget about spending days or weeks provisioning the infrastructure to support a new application. Apps can be deployed or

updated in minutes for rapid time to value.

How does network virtualization work?

- Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network. It makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane. Physical network resources, such as switching, routing, firewalling, load balancing, virtual private networks (VPNs), and more, are pooled, delivered in software, and require only Internet Protocol (IP) packet forwarding from the underlying physical network.
- Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and "attached" to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application. When a workload is moved to another host, network services and security policies move with it. And when new workloads are created to scale an application, necessary policies are dynamically applied to these new workloads, providing greater policy consistency and network agility.

Benefits of network virtualization

- Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud. Here are some of the key benefits of network virtualization:
  - Reduce network provisioning time from weeks to minutes
  - Achieve greater operational efficiency by automating manual processes
  - Place and move workloads independently of physical topology
  - Improve network security within the data center

Network Virtualization Example

- One example of network virtualization is virtual LAN (VLAN). A VLAN is a subsection of a local area network (LAN) created with software that combines network devices into one group, regardless of physical location. VLANs can improve the speed and performance of busy networks and simplify changes or additions to the network.
- Another example is network overlays. There are various overlay technologies. One industry-standard technology is called virtual extensible local area network (VXLAN). VXLAN provides a framework for overlaying virtualized layer 2 networks over layer 3 networks, defining both an encapsulation mechanism and a control plane. Another is generic network virtualization encapsulation (GENEVE), which takes the same concepts but makes them more extensible by being flexible to multiple control plane mechanisms.
- VMware NSX Data Center – Network Virtualization Platform
- VMware NSX Data Center is a network virtualization platform that delivers networking and security components like firewalling, switching, and routing that are defined and consumed in software. NSX takes an architectural approach built on scale-out network virtualization that delivers consistent, pervasive connectivity and security for apps and data wherever they reside, independent of underlying physical infrastructure.

Cloud delivery models

List and explain various types of cloud.

Types of Clouds: Basic Cloud Types

i. Public Clouds

ii. Private Clouds

iii. Hybrid Clouds

i) Public Clouds:

Figure 2: Public Cloud

- Public clouds are open to use by the general users.
- Public clouds survive ahead of the firewall of an industry, entirely hosted and supervised by vendors such as Amazon, MS and Google.
- Works on Pay-as-you-go criterion.
- Users do not have the power of resources management.
- Every task is supervised, software updated, and security patches installed by the third party.

Private Clouds:

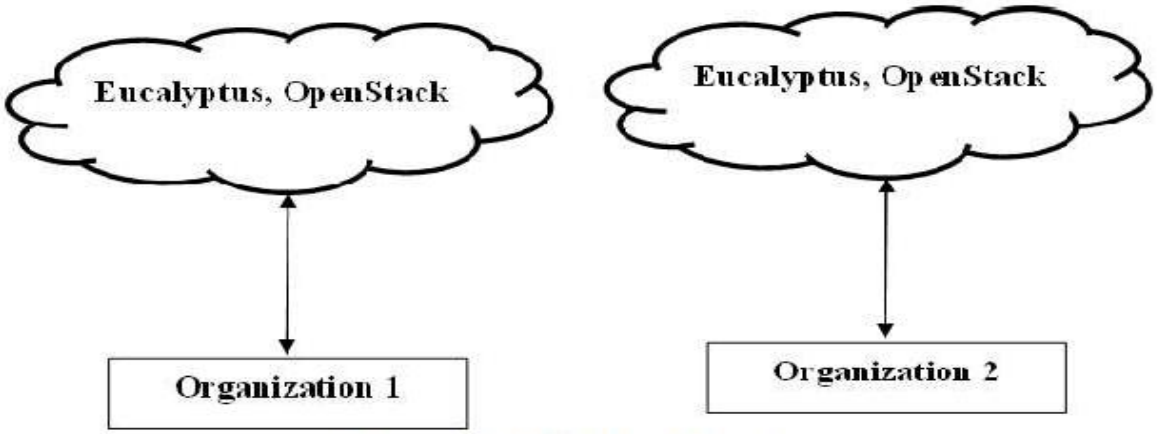


Figure 3: Private Cloud

- Private clouds exist within the firewall of an organization.
- Private clouds are entirely supervised by an enterprise.
- Possess all qualities of a public cloud with the additional responsibility of managing underlying IT infrastructure.
- It is used by the industries who have invested in their IT infrastructure massively.
- It is most suited for applications with strict security need, follow some rules or designed for regulatory tasks.

Hybrid Clouds:

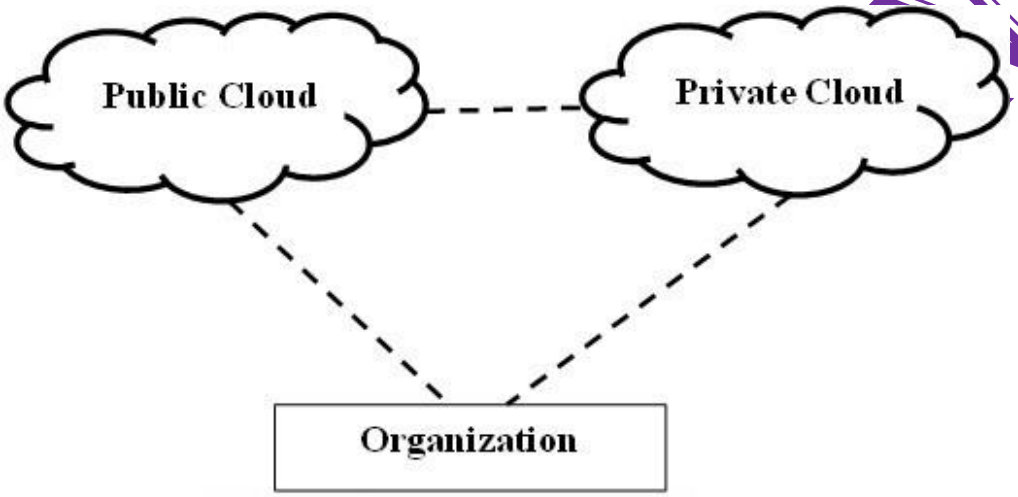


Figure 4: Hybrid Cloud

- Hybrid clouds consists of external as well as internal providers.
- It is a blend of Public as well as Private Clouds.
- Here, secure and complex applications are supervised by an organization and unsecured apps are managed by the third party vendors.
- They have distinct identity and are surrounded by standard technology.
- It enables data and application portability.
- Hybrid clouds are mainly used in Cloud bursting.

IV. Community Cloud:

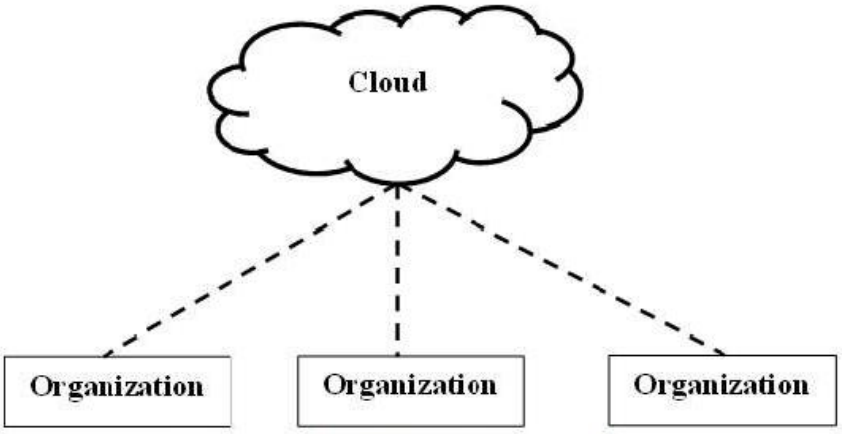


Figure 5: Community Cloud

- Community Cloud is implemented when several businesses have similar requirements and perspectives to share. These are accessible to members of a particular community, but are not available to the general public. Examples include branches of the educational organizations and government, military and industry suppliers and partners.
- These are mainly useful when the customers distribute special needs or there is a necessity for general services. By creating the virtual data centre from instances of virtual machines deployed on user machines (which are underutilized), another form of Community Cloud can be established. Thus, a Community Cloud is a kind of Private Cloud, but goes beyond a business or an organization.

Compare public cloud verses private cloud.

Sl. No.	Type	Public Cloud	Private Cloud
1	**Infrastructure Owner**	The owner of the infrastructure is the cloud provider or third party.	The owner of the infrastructure is an enterprise
2	**Cost**	The cost is less.	The cost is high.
3	**Scalability**	Scalability is on demand and unlimited.	Scalability is limited to the infrastructure installed.
4	**Security**	Concern regarding data security.	Security is high.
5	**Performance**	The performance is hard to attain for unpredictable environments.	The performance is guaranteed.
6	**Control and Management**	The public cloud manipulates the virtual machines which result in less management burden.	The private cloud has a high level of control over the resources which requires extra expertise to manage them.

IaaS v/s PaaS v/s SaaS

Explain application as a Service (SaaS) with a neat diagram and also list its isadvantages.

- Application as a Service can also be called as Software as a Service, which is simply written SaaS. In SaaS, customers rent software hosted by the vendor. This service is defined as a distribution model where the applications are hosted by a service provider or a vendor and made accessible to users over the internet. Software as a Service is similar to Application Service Provider (ASP) where a provider hosts available applications or software for the users and delivers those over the web.
- The merits of the model which includes this service are global accessibility, easy administration, compatibility, that is, all customers can use the same software version. With SaaS, tasks such as application or software deployment, maintenance, and keeping it working correctly from testing, managing patches, observing performance, etc., will be managed by the provider.
- In simple words, it can be understood as a provider hosts software or centrally located application, and can be made available for easy access to customers over the network, that is, internet on the basis of payment.

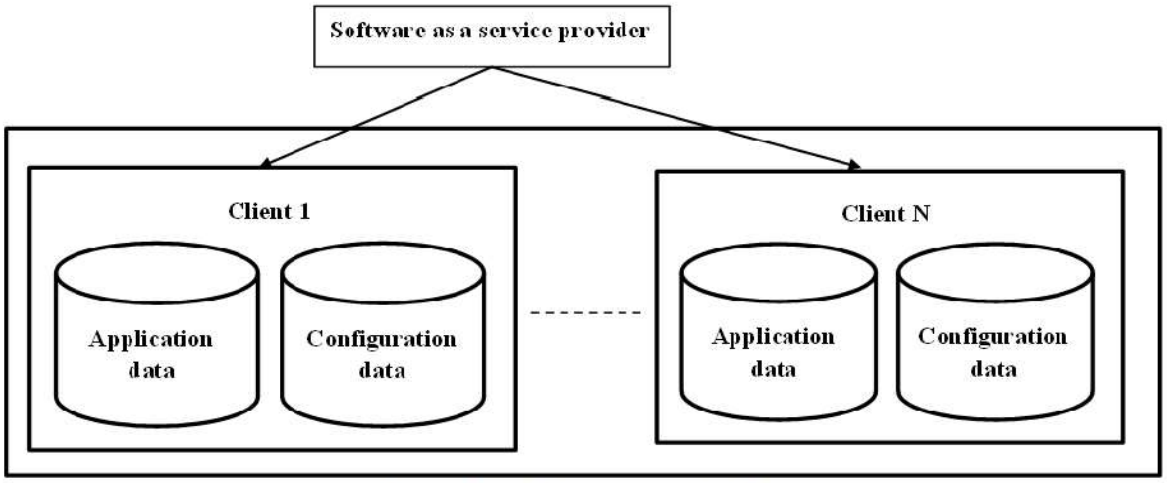


Figure 8: Software as a Service

Disadvantages of SaaS

1. Security is a major concern since the whole data will be in Cloud.
2. Switching between different SaaS vendors is a little bit challenging as it may involve a slow and difficult process of transferring very big data files through the internet.
3. Internet connection is mandatory.
4. Software as a Service model is not apt for the applications which demand response time in milliseconds.

12. (a) Explain Application /Software as a Service.
(b) What are the advantages and disadvantages of SaaS?

(a) Application as a service is also called as Software as a service(SaaS).

- In SaaS Customers rent s/w hosted by the vendors. This is defined as a software distribution model where the applications arehosted by a service provider and made accessible to the users over the internet.

(b) Advantages of SaaS:

- The service model SaaS facilitates the enterprises that all locations are using the application of the correct version.
- SaaS also increases the accessibility of application to global localities.
  - customization
  - security
  - web reliability
  - more bandwidth
- SaaS involves less maintenance of set-up, installation, monitoring of software.

Disadvantages of SaaS:

- Security is a major concern since the whole data will be in the cloud Internet connection is mandatory
- Switching different SaaS vendors is a little bit challenging as it may involve a slow and difficult process of transferring very big data files through internet
- Software as a service (SaaS) model is not apt for applications which demand for response time in milliseconds

Describe the importance of Platform as a service (PaaS).

- Paas provides hardware,storage,operating systems & network capacity on a charge basis over the network internet.
- It includes services for application development and deployment.
- PaaS is a verified model for running applications without the difficulty of maintaining software and hardware infrastructure at your own company.
- It allows users to create web applications very quickly, without bothering about the cost and complexity of buying and also managing the related hardware/software.
- PaaS is used to build multi-tenant applications.
- The developer's duty is simply to write the code by using the services provided by PaaS and the PaaS provider will take care of uploading that code and making it available to the users through the internet.

Advantages of IaaS cloud computing layer

There are the following advantages of IaaS computing layer -

1. Shared infrastructure

- IaaS allows multiple users to share the same physical infrastructure.

2. Web access to the resources

- Iaas allows IT users to access resources over the internet.

3. Pay-as-per-use model

- IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

4. Focus on the core business

- IaaS providers focus on the organization's core business rather than on IT infrastructure.

5. On-demand scalability

- On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

Disadvantages of IaaS cloud computing layer

1. Security

- Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.

2. Maintenance & Upgrade

- Although IaaS service providers maintain the software, but they do not upgrade the software for some organizations.

3. Interoperability issues

- It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problem related to vendor lock-in.

Some important point about IaaS cloud computing layer

- IaaS cloud computing platform cannot replace the traditional hosting method, but it provides more than that, and each resource which are used are predictable as per the usage.
- IaaS cloud computing platform may not eliminate the need for an in-house IT department. It will be needed to monitor or control the IaaS setup. IT salary expenditure might not reduce significantly, but other IT expenses can be reduced.
- Breakdowns at the IaaS cloud computing platform vendor's can bring your business to the halt stage. Assess the IaaS cloud computing platform vendor's stability and finances. Make sure that SLAs (i.e., Service Level Agreement) provide backups for data, hardware, network, and application failures. Image portability and third-party support is a plus point.
- The IaaS cloud computing platform vendor can get access to your sensitive data. So, engage with credible companies or organizations. Study their security policies and precautions.

Introduction to cloud vendors(Azure,AWS, GCP)

- A cloud service provider is an information technology (IT) company that provides its customers with computing resources over the internet and delivers them on-demand.
- Cloud computing is like your water/ electricity bill; you **only pay for what you use**. In this way cloud vendors provide Pay-as-you-go Model for cloud users.
- Cloud Service providers (CSP) offers various services such as Software as a Service**,** Platform as a service**,** Infrastructure as a service**,** network services**,** business applications**,** mobile applications**,** and infrastructure in the cloud.
- The cloud service providers host these services in a data center, and users can access these services through cloud provider companies using an Internet connection.
- CSPs are well-suited for organizations and individuals who don't want the responsibility of installing software, hardware or network resources and maintaining them until the end of their life cycles.

There are the following Cloud Service Providers Companies –

1. Amazon Web Services (AWS)
2. Microsoft Azure
3. Google Cloud Platform (GCP)
4. IBM Cloud Services
5. VMware Cloud
6. Oracle cloud
7. Red Hat
8. DigitalOcean
9. Rackspace
10. Alibaba Cloud

Amazon Web Services (AWS)

- Amazon Web Services is a **secure cloud service platform** provided by **Amazon** company.
- AWS started its life as an internal cloud offering by 2006,
- AWS is the most mature cloud platform offering a wide range of services to practically everyone: individual developers, large enterprises, and even governments.
- It offers various services such as database storage, computing power, content delivery, Relational Database, Simple Email, Simple Queue, and other functionality to increase the organization's growth.
- It had evolved into a publicly available cloud platform with services like Amazon S3 cloud storage and elastic compute cloud (EC2). serve millions of users.
- **Features of AWS**
- AWS provides various powerful features for building scalable, cost-effective, enterprise applications. Some important features of AWSis given below-
- AWS is **scalable** because it has an ability to scale the computing resources up or down according to the organization's demand.

- AWS is cost-effective as it works on a pay-as-you-go pricing model.
- It provides various flexible storage options.
- It offers various security services such as infrastructure security, data encryption, monitoring & logging, identity & access control, penetration testing, and DDoS attacks.
- It can efficiently manage and secure Windows workloads.

Prominent AWS customers include:

- Expedia
- Netflix
- Coinbase
- Formula 1
- Coca Cola
- Intuit
- Airbnb
- Lyft
- Coursera
- Food and Drug Administration (FDA)

2. Microsoft Azure

- Microsoft Azureis also known as **Windows Azure**. It supports various operating systems, databases, programming languages, frameworks that allow IT professionals to easily build, deploy, and manage applications through a worldwide network. It also allows users to create different groups for related utilities.

- Microsoft Azure is the second-largest cloud platform. Debuting in 2010, Azure has evolved into a cloud platform with more than 200 products and services. Today, it is among the fastest-growing cloud platforms.
- As Microsoft offers Azure, it provides a wide array of services tailored particularly for Microsoft-centric enterprises—making the switch to a cloud or a hybrid-cloud environment smooth for many organizations.
- In use by more than 95% of For une 500 companies, Microsoft Azure has a proven track record in catering to enterprise users.
- Importantly, Azure is not limited to Windows-based services. It also supports open-source languages, technologies, and platforms, giving anyone the freedom to build and support any application.

Features of Microsoft Azure

- Microsoft Azure provides **scalable**, **flexible**, and **cost-effective**
- It allows developers to quickly manage applications and websites.
- It managed each resource individually.

- Its IaaS infrastructure allows us to launch a general-purpose virtual machine in different platforms such as Windows and Linux.
- It offers a **Content Delivery System (CDS)** for delivering the Images, videos, audios, and applications.

Well-known Azure customers include:

- DAIMLER AG
- McKesson Group
- Asos
- Center of Disease Control (CDC) – US
- National Health Service (NHS) – UK
- HSBC
- Starbucks
- Walgreens
- 3M
- HP
- Mitsubishi Electric
- Renault
- eBay, Samsung, Rolls-Royce

3. Google Cloud Platform(GCP)

- Google cloud platform is a product of **Google**. It consists of a set of physical devices, such as computers, hard disk drives, and virtual machines. It also helps organizations to simplify the migration process.

beginning in 2010, the Google Cloud Platform currently offers over 100

- Available to the general public services spanning computing, networking, big data, and more. Today GCP consists of services including Google Workspace, enterprise Android, and Chrome OS.

- Compared to AWS and Azure, GCP is the smallest of the Big 3 cloud providers. Yet it offers a robust set of cloud services to power and support any kind of application.
- Notable GCP customers include:
  - Toyota
  - Unilever
  - Nintendo
  - Spotify
  - The Home Depot
  - Target

- Twitter
- Paypal
- UPS

Features of Google Cloud

- Google cloud includes various **big data services** such as Google BigQuery, Google CloudDataproc, Google CloudDatalab, and Google Cloud Pub/Sub.
- It provides various services related to **networking**, including Google Virtual Private Cloud (VPC), Content Delivery Network, Google Cloud Load Balancing, Google Cloud Interconnect, and Google Cloud DNS.
- It offers various **scalable** and **high-performance**
- GCP provides various **serverless services** such as Messaging, Data Warehouse, Database, Compute, Storage, Data Processing, and Machine learning (ML)
- It provides a free cloud shell environment with Boost Mode.

How to choose a cloud service provider

Organizations evaluating potential cloud partners should consider the following factors:

- **Cost.** The cost is usually based on a per-use utility model, but all subscription details and provider-specific variations must be reviewed. Cost is often considered one of the main reasons to adopt a cloud service platform.
- **Tools and features.** An overall assessment of a provider's features, including data management and security features, is important to ensure it meets current and future IT needs.
- **Physical location of the servers**. Server location may be an important factor for sensitive data, which must meet data storage regulations.
- **Reliability.** Reliability is crucial if customers' data must be accessible. For example, a typical cloud storage provider's SLA specifies precise levels of service -- such as 99.9% uptime -- and the recourse or compensation the user is entitled to should the provider fail to deliver the service as described. However, it's important to understand the fine print in SLAs, because some providers discount outages of less than 10 minutes, which may be too long for some businesses.
- **Security.**Cloud security should top the list of cloud service provider considerations. Organizations such as the Cloud Security Alliance offer certification to cloud providers that meet its criteria.
- **Business strategy.** An organization's business requirements should align with the offerings and technical capabilities of a potential cloud provider to meet both current and long-term enterprise goals.

How to choose a cloud service provider

- There are many factors to consider when choosing a CSP. Let’s take a look at the most common angles.
- **Regions and availability**
- When choosing a cloud provider, the first thing to consider is its supported regions and availability. These directly impact the performance of your cloud, due to factors like latency and compliance requirements, especially when dealing with data.
- As of September 2021, here’s where the Big 3 stand:
- **Amazon Web Service** has 25 geographic regions with 81 availability zones. 218+ edge locations, and 12 Regional Edge Caches.
- **Microsoft Azure** runs 60+ regions with a minimum of three availability zones in each region with more than 116 edge locations (Points of Presence).
- **Google Cloud Platform** has 27 cloud regions with 82 zones and 146 edge locations.

- Common services
- AWS and Azure have the largest service catalogs by offering more than 200+ services. GCP currently offers around 100+ services. A general breakdown of services is:
- AWS has the largest catalog of services.
- Azure is a close second with an impressive set of AI, ML, and analytics services.
- Google Cloud Platform comes in third place for the number of services offered.
- In this section, let's take a look at the common service offerings of each cloud platform.
- **Compute Services**

SERVICE	AWS	AZURE	GCP
VM (Compute Instance)	EC2 (Elastic Compute)	Azure Virtual Machine	Google Compute Engine

Database & Storage Services

SERVICE	AWS	AZURE	GCP
RDBMS (Multiple Database Types – SQL, MySQL, etc..)	AWS RDS	Azure SQL/ Database for MySQL/PostgreSQL	Cloud SQL
File Storage	Elastic File System	Azure File Storage	Google Filestore

Networking

SERVICE	AWS	AZURE	GCP
Virtual Network	Virtual Private Cloud (VPC)	Virtual Network (Vnet)	Virtual Private Cloud (VPC)
Load Balancing	Elastic Load Balancer	Azure Load Balancer	Google Cloud Load Balancing

Pricing

The pricing of the cloud platform depends on many factors:

- Customer requirements
- Usage
- The services used

AWS vs Azure vs GCP: pros & cons

AWS	
Pros	**Cons**
• Most services available, from networking to robotics • Most mature • Considered the gold standard in cloud reliability and security • More compute capacity vs Azure & GCP • All major software vendors make their programs available on AWS	• Dev/Enterprise support must be purchased • Can overwhelm newcomers with the sheer number of services and options • Comparatively limited options for hybrid cloud
MICROSOFT AZURE	
Pros	**Cons**
• Easy integration and migrations for existing Microsoft services • Many services available, including best-in-class AI, ML, and analytics services • Relatively cheaper for most services vs AWS & GCP • Great support for hybrid cloud strategies	• Fewer service offerings vs AWS • Particularly geared towards enterprise customers
GCP	
Pros	**Cons**
• Plays nicely with other Google service and products • Excellent support for containerized workloads • Global fiber network	• Limited services vs AWS & Azure • Limited support for enterprise use cases

- All three platforms offer competitive pricing plans with additional cost management options—reserved instances, budgets, and resource optimization—available to all users.
- The consensus in the IT community is that Microsoft Azure has the lowest on-demand pricing while Amazon tends to come somewhere around the middle.
- However, there is a clear advantage when enterprise customers already using Microsoft services (Windows, active directory, MS SQL, etc.) move to Azure as it is significantly cheaper than other cloud providers.

The 14 Cloud Security Principles explained

- Cloud security is an essential part of today's cyber security landscape. With hybrid working now the norm, many organisations are relying on Cloud services to access data from home or the office.
- But whenever organisations adopt technological solutions such as this, they must acknowledge the risks that come with it. Indeed, Cloud computing can increase the risk of data breaches and regulatory non-compliance, as well as introducing other vulnerabilities.
- To mitigate these risks, the NCSC (National Cyber Security Centre) created the Cloud Security Principles, which outline 14 guidelines for protecting information stored online.

1. Data in transit protection

- **What the NCSC says**: User data transiting networks should be adequately protected against tampering and eavesdropping.
- **How you can achieve it**: There are many ways you can bolster your network security, such as auditing and mapping your infrastructure to look for vulnerabilities. This might include spotting misconfigured firewalls or physical security threats.
- You should also make sure firmware and software are up to date, check that default passwords have been changed and secure your physical premises.
- Additionally, you should consider encrypting data or using VPNs where possible. Encryption can greatly reduce the risk of data being compromised in transit, but it will also make sharing data more complex and will require significant resources.
- Meanwhile, VPNs protect remote users by extending your organisation's private network across a public network. This enables employees to send and receive data as if their computer was directly connected to your organisation's network.

2. Asset protection and resilience

- **What the NCSC says**: User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
- **How you can achieve it**: The NCSC breaks down this principle into six parts: physical location and legal jurisdiction, data centre security, data at rest protection, data sanitisation, equipment disposal, and physical resilience and availability.
- Physical location and legal jurisdiction is relevant if you are subject to laws such as the GDPR (General Data Protection Regulation), which contain strict rules on data depending on its location.
- To determine this, you must identify the locations at which your data is stored, processed and managed, and consider how this affects your compliance with relevant legislation.
- Similarly, you should consider whether the legal jurisdiction within which the Cloud service provider operates applies to you.
- Data centre security refers to the controls you have implemented to protect the physical locations in which data is stored. This should cover the threat of unauthorised access, tampering, theft and reconfiguration of systems.
- Data at rest protection refers to the security of information stored in the Cloud, and data sanitation refers to the process of supplying resources, transferring them and having users return them when no longer needed.
- Equipment disposal requires organisations to securely delete or discard information at the end of its lifecycle. Physical records should be shredded, while digital documents and other relevant information – such as credentials and configuring information – should be wiped from hard drives.
- Finally, physical resilience and availability refers to an organisation's ability to function in the event of failures, security incidents and cyber attacks.

3. Separation between users

- **What the NCSC says**: A malicious or compromised user of the service should not be able to affect the service or data of another.
- **How you can achieve it**: Factors that affect user separation include where the separation controls are implemented, who the organisation shares the service with and the level of assurance available in the implementation of separation controls.
- As such, organisations must understand the types of user that they share the Cloud service with and implement appropriate tools. This might include virtualisation technologies or other software that can separate users.
- Whenever organisations use such tools, they must also conduct regular penetration tests on their infrastructure and web applications to look for vulnerabilities.

4. Governance framework

- **What the NCSC says**: The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.
- **How you can achieve it**: Organisations should begin by appointing a board representative (or a person with the direct delegated authority) to take responsibility for the security of the Cloud service. This will typically be the chief information officer, chief security officer or someone with a similar title.
- Next, they should document a framework for security governance containing policies addressing key aspects of information security.
- The organisation must also implement processes to identify and ensure compliance with relevant legal and regulatory requirements.

5. Operational security

- **What the NCSC says**: The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.
- **How you can achieve it**: There are four things to consider here, the first of which is configuration and change management. This means ensuring that changes to the system have been properly tested and authorised.
- The second thing to consider is vulnerability management, which involves identifying and mitigating security issues in constituent components.
- Third, you must implement protective monitoring, which enables you to detect cyber attacks and unauthorised activity on the service.
- Finally, you must create an incident management system to ensure that you can respond to incidents and recover a secure, available service.

6. Personnel security

- **What the NCSC says**: Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.
- **How you can achieve it**: Service providers must conduct security screening for employees and provide regular security training.
- This should include explanations of the security responsibilities associated with specific roles and the ways in which the organisation screens and manages personnel within privileged roles.
- BS7858 outlines a basic standard for personnel screening, and organisations are advised to follow its guidelines.

7. Secure development

- **What the NCSC says**: Services should be designed and developed to identify and mitigate threats to their security. Those that aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.
- **How you can achieve it**: Organisations must create an ISO 27001 secure development policy to ensure that development is carried out in line with industry good practice.
- They should also regularly monitor new and evolving threats, taking appropriate steps to adjust their service accordingly.
- Additionally, organisations should implement configuration management processes to guarantee the integrity of the solution through development, testing and deployment.

8. Supply chain security

- **What the NCSC says**: The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.
- **How you can achieve it**: If your organisation relies on third-party products and services, you must understand how your information is shared with and accessible to those partners and how it flows through their supply chain.
- You must also review the service provider's procurement processes, looking at the security requirements it places on third-party suppliers. Similarly, you must understand how the service provider manages third-party security risks and the ways it enforces the security requirements of its suppliers.
- Finally, you should review how the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

9. Secure user management

- **What the NCSC says**: Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.
- **How you can achieve it**: There are two things you must address here. First, users must be properly authenticated before they are allowed to perform management activities, report faults or request changes to the service.
- These changes can be performed through a service management web portal or by telephone/email.
- Second, you must implement role-based access controls within management interfaces to prevent users from making unauthorised changes that could affect the service.
- This step also protects management interfaces in the event that an employee's account is compromised by criminal hackers.

10. Identity and authentication

- **What the NCSC says**: All access to service interfaces should be constrained to authenticated and authorised individuals.
- **How you can achieve it**: This principle requires a series of technical solutions. First, you should implement two-factor authentication to strengthen the login process.
- By doing this, you protect employees' accounts in the event that their password is compromised, because an attacker will still need the hardware or software token.
- You should also obtain a TLS client certificate, which will provide strong cryptographic protection, and implement identity federation with your existing identity provider.

11. External interface protection

- **What the NCSC says**: All external or less trusted interfaces of the service should be identified and

appropriately defended.

- **How you can achieve it**: You must first understand the physical and logical interfaces from which your information is available and how access to your data is controlled.
- Once you have this information, you must implement measures to ensure that the service identifies and authenticates users to an appropriate level over those interfaces. This includes the Internet, community networks and private networks.

12. Secure service administration

- **What the NCSC says**: Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.
- **How you can achieve it**: To begin, you must understand which service administration model is being used by.
- Next, you should assess the risks associated with that administration model. The NCSC outlines those risks on its website. If you cannot determine which service administration model is used, you should refer to the risks associated with the *Direct service administration* approach.

13. Audit information for users

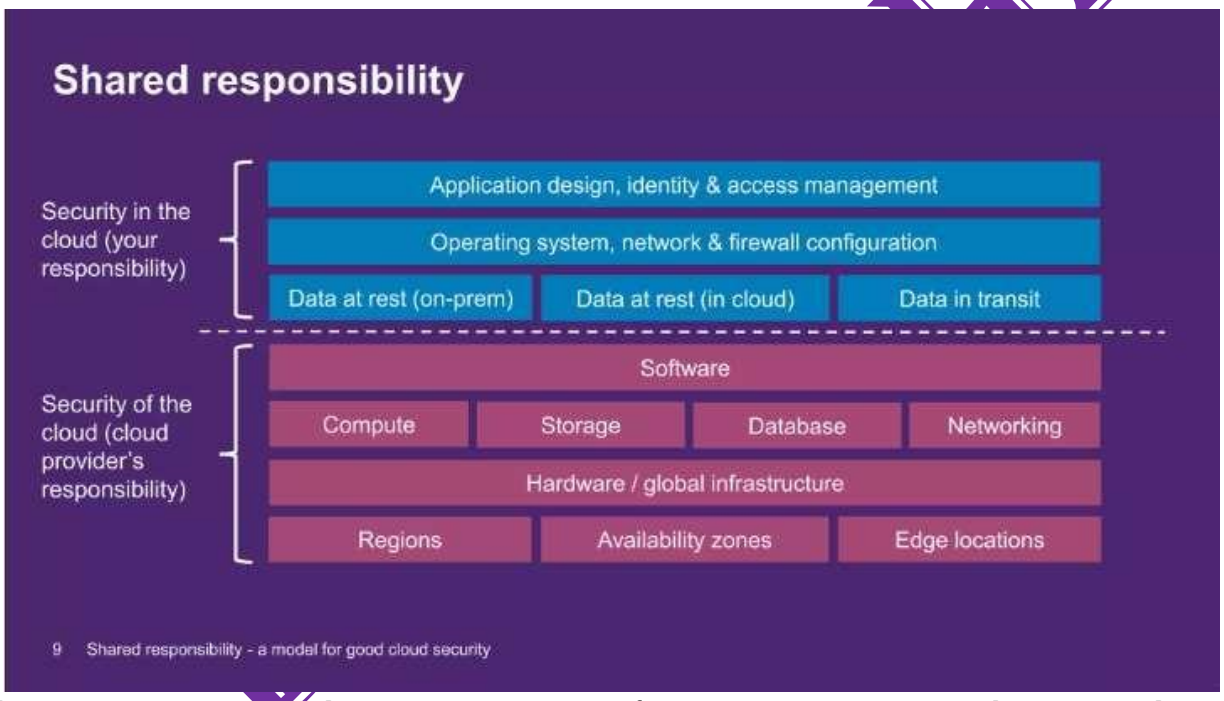
- **What the NCSC says**: You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.
- **How you can achieve it**: This principle refers to the way in which you will receive audit information rather than what you will do with it.
- As such, your requirements relate to the processes related to receiving the information. This means establishing how and when audit information will be provided, including the format of the data, and the data retention period associated with it.
- The NCSC splits this into three potential scenarios: the service provider might not offer any audit information, it might provide some information (perhaps as a result of negotiation) or it might make specific information available.
- For the audit information to be useful, you must insist on receiving complete, specific details. If you don't, you will face regulatory compliance issues and could be at greater risk of security incidents.

14. Secure use of the service

- **What the NCSC says**: The security of Cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.
- **How you can achieve it**: Your responsibilities here are subject to the deployment models you use, the features of those services and the scenario in which you intend to use the service.
- For example, with infrastructure- and platform-as-a-service offerings, the organisation is responsible for significant aspects of their security, including the installation and configuration of an operating system, the deployment of applications and their maintenance.
- The NCSC provides a guide for organisations configuring infrastructure-as-a-service securely.
- Separately, it recommends that organisations identify the security requirements related to its use of service and educate staff on how to use and manage that service securely.

Shared Responsibility Model:

- The **Shared Responsibility Model** is a security and compliance framework that outlines the responsibilities of **cloud service providers (CSPs)** and **customers** for securing every aspect of the cloud environment, including hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights.
- In its simplest terms, the Shared Responsibility Model dictates that the cloud provider—such as Amazon Web Service (AWS), Microsoft Azure, or Google Cloud Platform (GCP)—must monitor and respond to security threats related to the cloud itself and its underlying infrastructure. Meanwhile, end users, including individuals and companies, are responsible for protecting data and other assets they store in any cloud environment.



- When an enterprise runs and manages its own IT infrastructure on premises, within its own data center, the enterprise -- and its IT staff, managers and employees -- is responsible for the security of that infrastructure, as well as the applications and data that run on it. When an organization moves to a public cloud computing model, it hands off some, but not all, of these IT security responsibilities to its cloud provider. Each party -- the cloud provider and cloud user -- is accountable for different aspects of security and must work together to ensure full coverage.
- While the responsibility for security in a public cloud is shared between the provider and the customer, it's important to understand how the responsibilities are distributed depending on the provider and the specific cloud model.
- The type of cloud service model -- infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) -- dictates who is responsible for which security tasks. According to the Cloud Standards Customer Council, an advocacy group for cloud users, users' responsibilities generally increase as they move from SaaS to PaaS to IaaS.

Amaznon's AWS Shared Responsibility Model

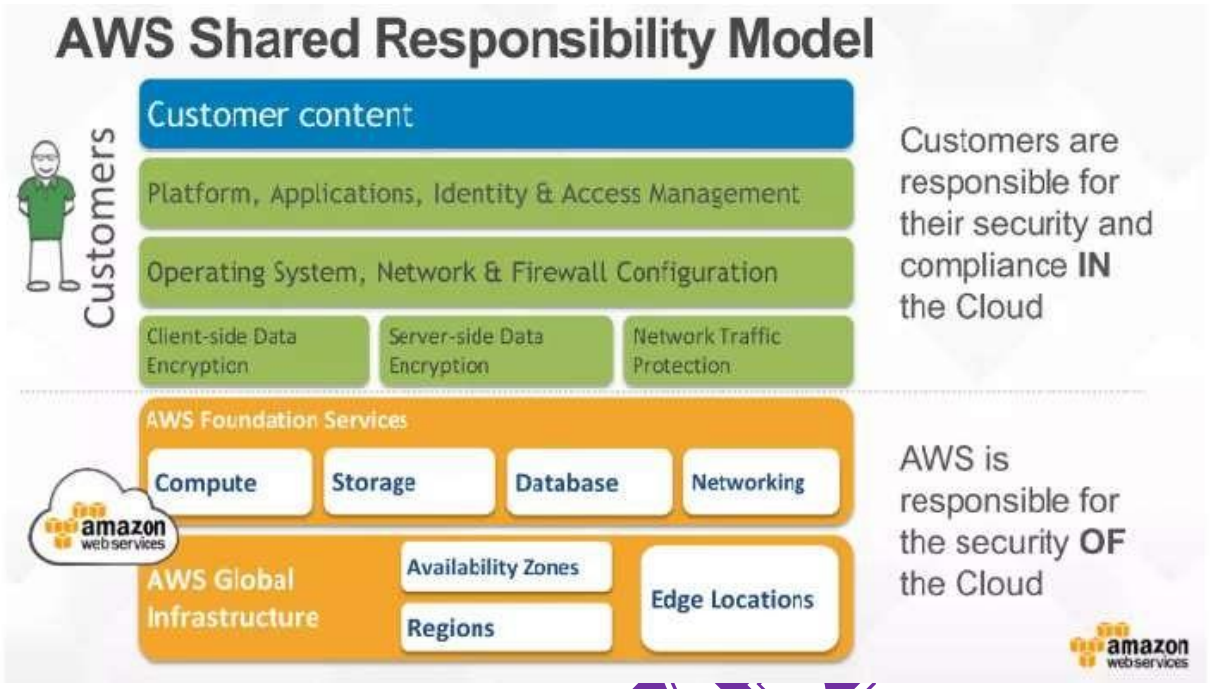


Fig:The cloud service provider's and user's security responsibilities vary depending on whether they're using the IaaS, PaaS or SaaS model.

The cloud service provider's and user's security responsibilities vary depending on whether they're using the IaaS, PaaS or SaaS model.

- **IaaS.** The cloud provider is responsible for services and storage -- the basic cloud infrastructure components such as virtualization layer, disks and networks.
- The provider is also responsible for the physical security of the data centers that house its infrastructure. IaaS users, on the other hand, are generally responsible for the security of the OS and software stack required to run their applications, as well as their data.
- **PaaS.** When the provider supplies a more comprehensive platform, the provider assumes greater responsibility that extends to the platform applications and OSes.

- For example, the provider ensures that user subscriptions and login credentials are secure, but the user is still responsible for the security of any code or data -- or other content -- produced on the platform.
- **SaaS.** The provider is responsible for almost every aspect of security, from the underlying infrastructure to the service application, such as an HR or finance tool, to the data the application produces.
- Users still bear some security responsibilities such as protecting login credentials from phishing or social engineering attacks.

The customer's typical cloud security responsibilities

In general terms, a cloud customer is always responsible for configurations and settings that are under their direct control, including the following:

- **Data.** A user must ensure that any data created on or uploaded to the cloud is properly secured. This can include the user's creation of authorizations to access the data, as well as the use of encryption to protect the data from unauthorized access.
- **Applications.** If a user placed a workload into a cloud VM, the user is still fully responsible for securing that workload. This can include creating secure (hardened) code through proper design, testing and patching; configuring and maintaining proper identity and access management (IAM); and securing any integrations -- the security of connected systems such as local databases or other workloads.
- **Credentials.** Users control the IAM environment such as login mechanisms, single sign-on, certificates, encryption keys, passwords and any multifactor authentication items.
- **Configurations.** The process of provisioning a cloud environment includes a significant amount of user control through configuration settings. Any cloud instances must be configured in a secure manner using the provider's tools and options.
- **Outside connections.** Beyond the cloud, the user is still responsible for anything in the business that connects to the cloud such as traditional local data center infrastructure and applications.

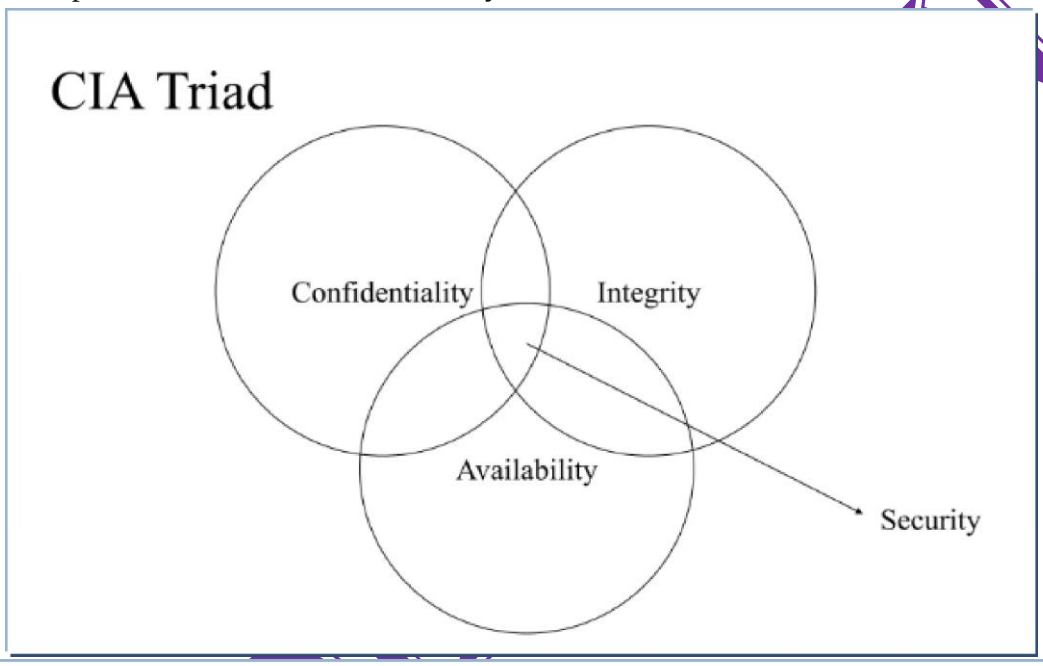
The provider's typical cloud security responsibilities

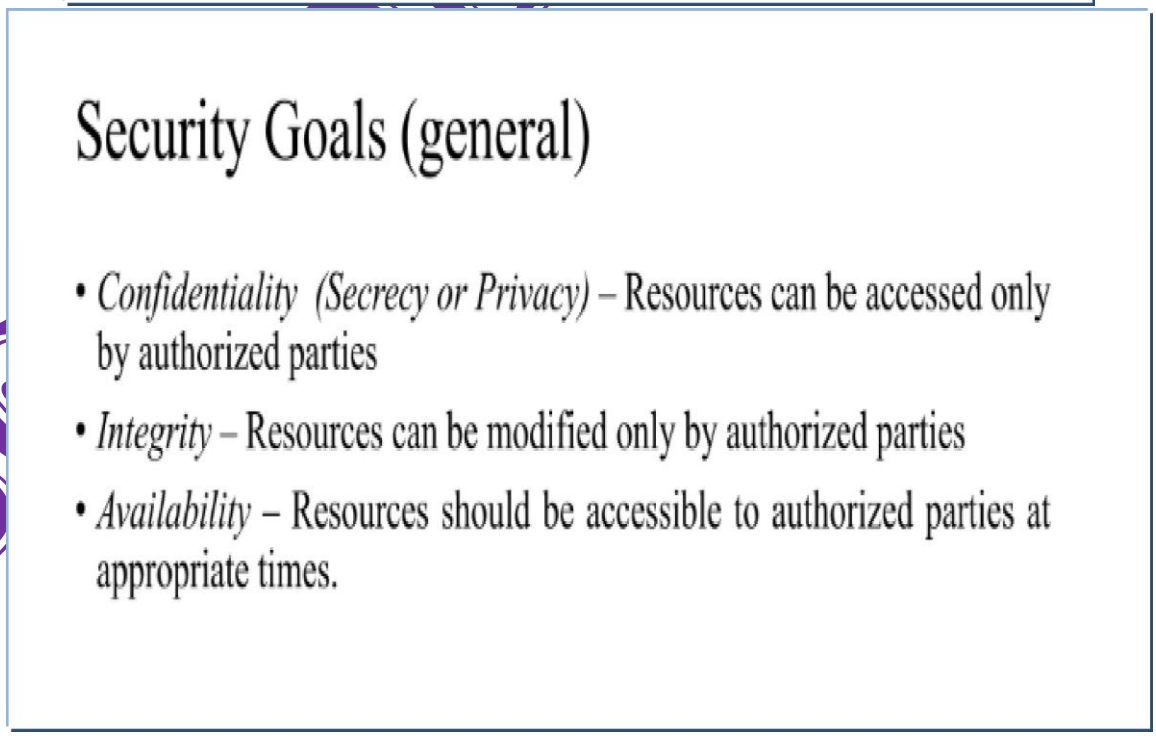
Public clouds present a vast and complex infrastructure, and cloud providers will always be completely responsible for that infrastructure, including the following components:

- **Physical layer.** The provider manages and protects the elements of its physical infrastructure. This includes servers, storage, network gear and other hardware as well as facilities. An infrastructure typically includes various resilient architectures such as redundancy and failover, as well as redundant power and network carrier connectivity. Infrastructure management also frequently includes backup, restoration and disaster recovery implementations.
- **Virtualization layer.** Public clouds are fundamentally do-it-yourself environments where users can provision and use as many resources and services as they wish. But such flexibility demands a high level of virtualization, automation and orchestration within the provider's infrastructure. The provider is responsible for implementing and maintaining this virtualization/abstraction layer as well as its various APIs, which serve as the means of user access and interaction with the infrastructure.
- **Provider services.** Cloud providers typically offer a range of dedicated or pre-built services such as databases, caches, firewalls, serverless computing, machine learning and big data processing. These pre-built services can be provisioned and used by customers but are completely implemented and managed by the cloud providers -- including any OSes and applications needed to run those services.

Principle of least privilege :

- The principle of least privilege (PoLP) stipulates that users should be granted the least privileges they need to carry out their role, and is arguably one of the most important principals of data security.
- PoLP helps to minimize the attack surface – limiting the amount of damage that can be caused were an attacker to gain access to a set of credentials. Likewise, PoLP helps to protect against both negligent and malicious insiders.
- As Governments across the globe introduce their own stringent data privacy regulations, a failure to adequately restrict access to personal data could result in costly lawsuits and fines.





Tips for implementing Least Privilege in the cloud

Assigning the appropriate access controls requires some initial housekeeping, which includes locating your critical assets, and removing any redundant data and accounts. When implementing the principal of least privilege in the cloud, ideally, you should use a single Identify Access Management (IAM) solution, and a single solution for monitoring permissions. Your chosen auditing solution should be able to aggregate and correlate event logs from multiple cloud platforms, as well as hybrid environments.

1. Discover & classify your sensitive data

- Perhaps the best place to start would be to ensure that we know exactly what sensitive data we have, and where it is located. Most popular cloud platforms provide data classification capabilities out-of-the-box, including AWS, Azure and Google Cloud. However, for multi-cloud or hybrid environments, there are third-party solutions which will scan your local and remote repositories and automatically discover and classify sensitive data as it is found. Some solutions can also classify sensitive data at the point of creation. It's always good practice you make sure that any redundant data is removed before attempting to implement PoLP. Establishing a profound understanding of what data you have makes the process of assigning access rights considerably easier.

2. Implement Role-Based Access Control (RBAC)

- A common technique that is used to simplify the process of setting up PoLP is Role-Based Access Control (RBAC). As opposed to trying to assign access rights to specific individuals, you can define a comprehensive set of roles, each with their respective privileges, and assign users to these roles on an ad-hoc basis. While RBAC is arguably less granular than assigning access rights on a per-user basis, it is generally more secure as it is less prone to error. Most popular cloud platforms provide role-based access control, including AWS, Azure and Google Cloud.

3. Identify and remove inactive user accounts

- You will need to ensure that any inactive user accounts are identified and removed before implementing PoLP. Since inactive user accounts are rarely monitored, hackers often target them as it enables them to gain persistent access to the network with less risk of getting caught.

4. Monitor privileged accounts in real-time

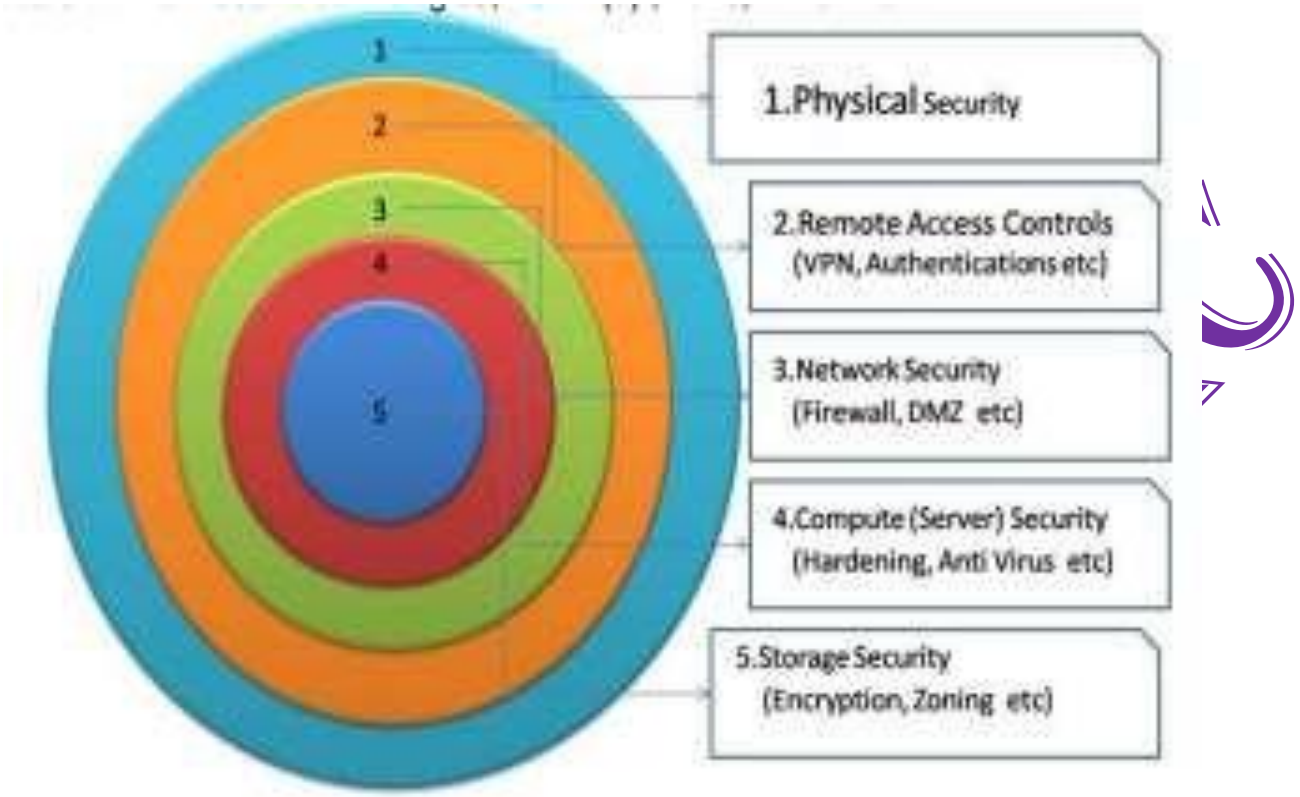
- You will need to ensure that you have as much visibility as possible into who is already accessing what data, and when. Most real-time auditing solutions use machine learning techniques to monitor user behavior and establish usage patterns which can be tested against in order to identify anomalies. Once you have an understanding of each user's behavioral patterns, you can use this information as a guide to determine what data each user should have access to.

5. Implement dynamic access controls and Just In Time (JIT) access

- Of course, there are times when a user may need access to assets which they don't normally need access to. For obvious reasons, we cannot simply grant access to a user just because they ask for it. There needs to be a formal process to determine the legitimacy of their request.

Defense in depth

- Defense-in-depth represents the use of multiplesecurity defenses to help mitigate the risk of security threats, if one component of the defense is being compromised.
- An example, could be an antivirus software installed on individual VM when there is already a virus protection on the firewalls within the same environment.
- Different security products from multiple vendors may be deployed to defend different potential vulnerable resources within the network.



ADVANTAGES OF APPROACH

- Multilayered cloud security approach
- Minimizes the risk of security breach even other components of the system get compromised.
- Compete CIA triad assurance for critical enterprise business information and applications.
- Provides additional time to detect and respond to the attacks.
- Can handle higher velocity and different varieties of attacks.
- Crucial data storage is at the deepest layer to provide stronger protection.
- Includes all the areas of possible security vulnerabilities even with the virtualized components.
- Complete security solution for cloud computing, well suited for all types of deployment models of cloud.
- Use of best practice security mechanisms in the different areas of concerns.
- Meets all the requirements of the SLAs and other legal issues.
- Performance management and focus on the availability of the cloud resources and services.
- Less overheads on the client sites so to avoid throughput issues.
- The overall cost of the approach is higher, but can be optimized.

Defense in Depth (DiD) refers to an information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within.

Threat actors, diagrams & trust boundaries

- **Threat Actor:** "A **threat actor**, also called a **malicious actor**, is an entity that is partially or wholly responsible for a security incident that impacts – or has the potential to impact – an organization's security."
- A threat actor – compared to a hacker or attacker – does not necessarily have any technical skill sets.
- They are a person or organization with malicious intent and a mission to compromise an organization's security or data. This could be anything from physical destruction to simply copying sensitive information.
- **Hacker:** A hacker can "hack" his or her way through the security levels of a computer system or network.
- **Attacker:**A **cyberattack** is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices.

- A Hackers and attackers are technical personas or organizations intentionally targeting technology to create an incident and, hopefully (for them, not you), a breach. They can be solo individuals, groups, or even nation-states with goals and missions to destabilize a business, government, to disseminate information, or for financial gain.
- **Assets** – a resource of value. May be tangible or intangible. Usually referred to a 'Object'.
- **Threat** – Undesired act that potentially occurs causing compromise or damage of an asset.
- **Threat Agent** – Something/someone that makes the threat materialize. Usually referred to as 'Subject'
- Vulnerability – Weakness that makes an attack possible.
- **Attack –** Act of malicious threat agent. Also known as Exploit.
- **Safeguard (Countermeasure)** – address vulnerabilities (not threats directly);
- For example – Application Design, Writing Secure Code, deploy with least privilege
- Probability – the potential chance of a threat being realized by an attack on an asset
- Impact – Outcome of the materialized threat.

Four main types of threat actors that you may need to worry about:

- Organized crime or independent criminals, interested primarily in making money.
- Hacktivists, interested primarily in discrediting you by releasing stolen data, committing acts of vandalism, or disrupting your business.
- Inside attackers, usually interested in discrediting you or making money.
- State actors, who may be interested in stealing secrets or disrupting your business.

Cloud asset management

- Cloud asset management is the process used to control an organization's cloud infrastructure and the application data within the cloud.
- Many organizations use a variety of cloud-based applications to store and manage their digital assets.
- With a collection of cloud-based asset sources, CAM helps organize assets to avoid operational hiccups and security concerns.
- Incorporating the use of cloud asset management practices provides an organization with visibility and easy control over the digital assets within the company cloud.
- Optimizing an organization's asset cloud allows users to efficiently access company data when necessary and provides a method to effectively monitor internal assets and maintain data security.

Why is asset management important?

- From physical products to digital company data, asset management is a critical component of any organization.
- For one, asset management is necessary for complete visibility and control over various assets.
- Fully comprehending the who, what, and where's of an asset inventory helps streamline operations and allows multiple users to access data whenever and wherever.
- Not to mention, it's easy to mishandle company assets without proper management, allowing data to fall into the wrong hands or become swept under the rug. Assets that fall into the wrong hands, especially digital ones, can also cause costly customer debacles and security concerns that can significantly impact overall operations — or invite cybercriminals to your virtual front door.

The Key Benefits of Cloud Asset Management

- Cloud asset management provides businesses with the ability to make better decisions, supported by valuable data.
- When you align the long-term integrity of your cloud infrastructure (visibility, accuracy, and reliability) with your cloud management objectives, you build a stronger cloud framework, with minimized risks.
- Here are three of the main benefits of cloud asset management:

1. Cloud Inventory Accuracy

- A key advantage of cloud asset management is the ability to gain greater visibility over your cloud asset inventory. Cloud asset management systems can gather in-depth inventory information that can be used to make educated decisions about managing your assets in the most cost-effective manner possible.
- Not only does this encourage your enterprise to make the most of your existing infrastructure, but it also targets extra or unnecessary spending. By minimizing risk, and steering clear of cloud projects that would prove fruitless, you can avoid wasting valuable finances. Similarly, greater visibility of your inventory can help you target exactly where improvements can be made.
- An accurate cloud asset inventory ensures your enterprise can optimize these measures with confidence, based on reliable data instead of guesswork.

2. Automation

- Cloud asset management uses automated processing to instantly manage the discovery of your assets and provides real-time, up-to-date inventory information. Not only can automation reduce the time-consuming process of trawling through large amounts of data, but it also removes human error from cloud asset management – boosting the accuracy of your cloud management processes.
- Additionally, automation enables your enterprise to become self-serving, placing control of your cloud estate

back in your hands. By using a system that enables your employees to service your cloud infrastructure, you remove the unnecessary interference of your cloud provider. This provides you with greater transparency and visibility over your cloud expenses. For example, it can help you automatically track your cloud costs, and identify extraneous or unnecessary cloud spending that can be changed as required.

3. Security Assurance

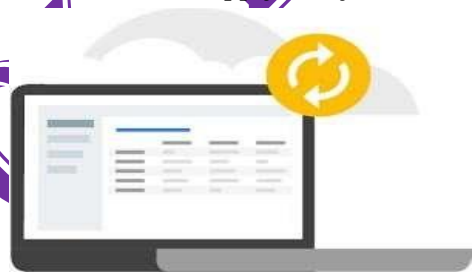
- Cloud asset management firms up your cloud security package – enabling you to keep track of your critical security measures with actionable assessments of potential risks and threats to your cloud infrastructure. Automated systems can fix vulnerabilities upon detection, without human intervention – ensuring your business is not left with critical security gaps.
- Additionally, cloud asset management systems identify non-compliant cloud resources and shift them back into compliance immediately. Considering cloud compliance is one of the most vital legal requirements of cloud technology, it's important to have rigorous security and compliance checkpoints in place. Cloud asset management enables this, by automatically processing regulatory reviews of your cloud estate.

Identity & Access management in the cloud

- Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage Google Cloud resources centrally. For enterprises with complex organizational structures, hundreds of workgroups, and many projects, IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes.

Simplicity first

- We recognize that an organization's internal structure and policies can get complex fast. Projects, workgroups, and managing who has authorization to do what all change dynamically. IAM is designed with simplicity in mind: a clean, universal interface lets you manage access control across all Google Cloud resources consistently. So you learn it once, then apply everywhere.

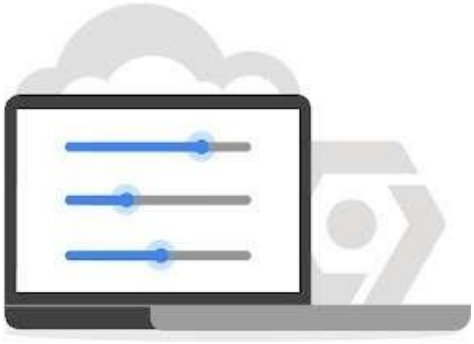


The right roles

- IAM provides tools to manage resource permissions with minimum fuss and high automation. Map job functions within your company to groups and roles. Users get access only to what they need to get the job done, and admins can easily grant default permissions to entire groups of users.

Smart access control

- Permissions management can be a time-consuming task. Recommender helps admins remove unwanted access to Google Cloud resources by using machine learning to make smart access control recommendations. With Recommender, security teams can automatically detect overly permissive access and rightsize them based on similar users in the organization and their access patterns.



Get granular with context-aware access

- IAM enables you to grant access to cloud resources at fine-grained levels, well beyond project-level access. Create more granular access control policies to resources based on attributes like device security status, IP address, resource type, and date/time. These policies help ensure that the appropriate security controls are in place when granting access to cloud resources.

Streamline compliance with a built-in audit trail

- A full audit trail history of permissions authorization, removal, and delegation gets surfaced automatically for your admins. IAM lets you focus on business policies around your resources and makes compliance easy.

Enterprise identity made easy

- Leverage Cloud Identity, Google Cloud's built-in managed identity to easily create or sync user accounts across applications and projects. It's easy to provision and manage users and groups, set up single sign-on, and configure two-factor authentication (2FA) directly from the Google Admin Console. You also get access to the Google Cloud Organization, which enables you to centrally manage projects via Resource Manager.

Workforce Identity Federation

- Workforce Identity Federation lets you use an external identity provider (IdP) to authenticate and authorize a workforce—a group of users, such as employees, partners, and contractors—using IAM, so that the users can access Google Cloud services. Workforce Identity Federation uses an identity federation approach instead of directory synchronization, eliminating the need to maintain separate identities across multiple platforms.

Introduction to IAM

- Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations.
- Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication and privileged access management.
- These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.
- IAM systems can be deployed on premises, provided by a third-party vendor through a cloud-based subscription model or deployed in a hybrid model.
- On a fundamental level, IAM encompasses the following components:
  - how individuals are identified in a system (understand the difference between identity management and authentication);
  - how roles are identified in a system and how they are assigned to individuals;
  - adding, removing and updating individuals and their roles in a system;
  - assigning levels of access to individuals or groups of individuals; and
  - protecting the sensitive data within the system and securing the system itself.

Why is IAM important?

- Businesses leaders and IT departments are under increased regulatory and organizational pressure to protect access to corporate resources. As a result, they can no longer rely on manual and error-prone processes to assign and track user privileges. IAM automates these tasks and enables granular access control and auditing of all corporate assets on premises and in the cloud.
- IAM, which has an ever-increasing list of features
- Including biometrics,
- behaviour analytics and AI is well suited to the rigors of the new security landscape.
- For example, IAM's tight control of resource access in highly distributed and dynamic environments aligns with the industry's transition from firewalls to zero-trust models and with the security requirements of IoT.
- For more information on the future of IoT security, check out this video.
- While IT professionals might think IAM is for larger organizations with bigger budgets, in reality, the technology is accessible for companies of all sizes.

Basic components of IAM

- An IAM framework enables IT to control user access to critical information within their organizations. IAM products offer role-based access control, which lets system administrators regulate access to systems or networks based on the roles of individual users within the enterprise.
- In this context, access is the ability of an individual user to perform a specific task, such as view, create or modify a file. Roles are defined according to job, authority and responsibility within the enterprise.
- IAM systems should do the following: capture and record user login information, manage the enterprise database of user identities, and orchestrate the assignment and removal of access privileges.
- That means systems used for IAM should provide a centralized directory service with oversight and visibility into all aspects of the company user base.
- Digital identities are not just for humans; IAM can manage the digital identities of devices and applications to help establish trust.
- In the cloud, IAM can be handled by authentication as a service or identity as a service (IDaaS). In both cases, a third-party service provider takes on the burden of authenticating and registering users, as well as managing their information. Read more about these cloud-based IAM options.

Benefits of IAM

IAM technologies can be used to initiate, capture, record and manage user identities and their related access permissions in an automated manner. An organization gains the following IAM benefits:

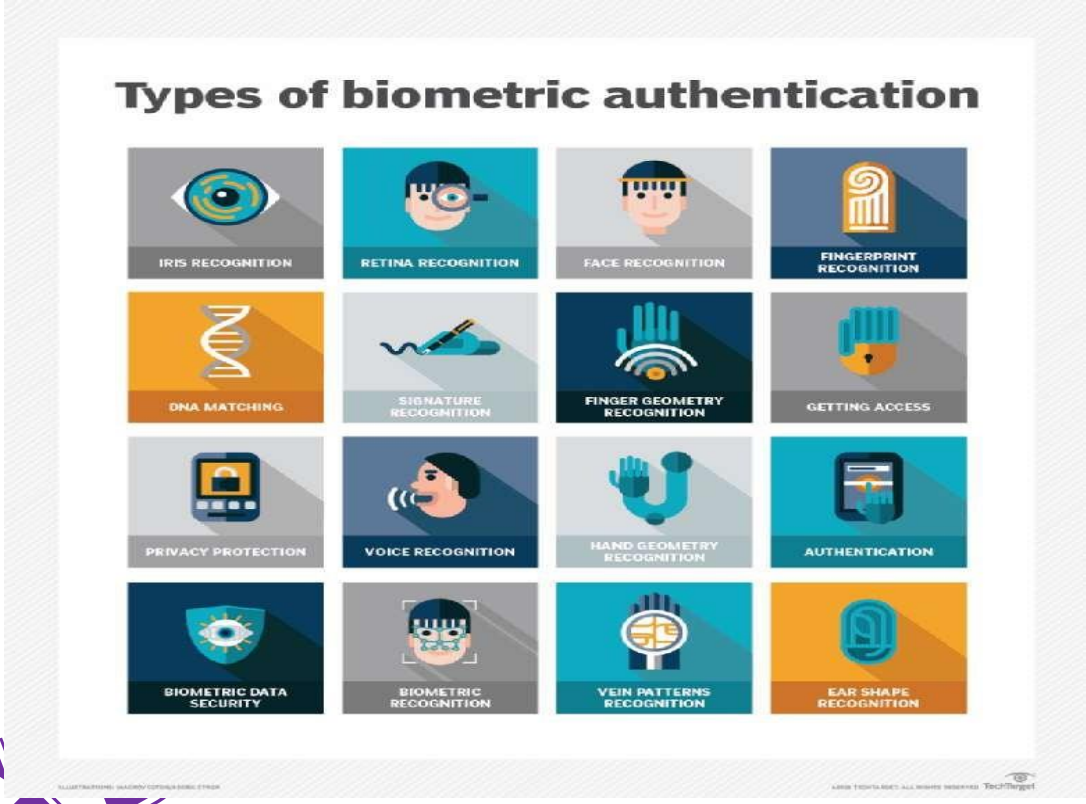
- Access privileges are granted according to policy, and all individuals and services are properly authenticated, authorized and audited.
- Companies that properly manage identities have greater control of user access, which reduces the risk of internal and external data breaches.
- Automating IAM systems allows businesses to operate more efficiently by decreasing the effort, time and money that would be required to manually manage access to their networks.
- In terms of security, the use of an IAM framework can make it easier to enforce policies around user authentication, validation and privileges, and address issues regarding privilege creep.
- IAM systems help companies better comply with government regulations by allowing

Types of digital authentication

- With IAM, enterprises can implement a range of digital authentication methods to prove digital identity and authorize access to corporate resources.
- **Unique passwords.** The most common type of digital authentication is the unique password. To make passwords more secure, some organizations require longer or complex passwords that require a combination of letters, symbols and numbers. Unless users can automatically gather their collection of passwords behind a single sign-on entry point, they typically find remembering unique passwords onerous.
- **Pre-shared key (PSK).** PSK is another type of digital authentication where the password is shared among users authorized to access the same resources -- think of a branch office Wi-Fi password. This type of authentication is less secure than individual passwords.
- A concern with shared passwords like PSK is that frequently changing them can be cumbersome.
- **Behavioral authentication.** When dealing with highly sensitive information and systems, organizations can use behavioral authentication to get far more granular and analyze keystroke dynamics or mouse-use characteristics. By applying artificial intelligence, a trend in IAM systems, organizations can quickly recognize if user or machine behavior falls outside of the norm and can automatically lock down systems.
- **Biometrics.** Modern IAM systems use biometrics for more precise authentication. For instance, they collect a

range of biometric characteristics, including fingerprints, irises, faces, palms, gaits, voices and, in some cases, DNA. Biometrics and behavior-based analytics have been found to be more effective than passwords.

- When collecting and using biometric characteristics, companies must consider the ethics in the following areas:
  - data security (accessing, using and storing biometric data);
  - transparency (implementing easy-to-understand disclosures);
  - optionality (providing customers a choice to opt in or out); and
  - biometric data privacy (understanding what constitutes private data and having rules around sharing with partners.
- One danger in relying heavily on biometrics is if a company's biometric data is hacked, then recovery is difficult, as users can't swap out facial recognition or fingerprints like they can passwords or other non-biometric information.
- Another critical technical challenge of biometrics is that it can be expensive to implement at scale, with software, hardware and training costs to consider.



Implementing IAM in the enterprise

- Before any IAM system is rolled out into the enterprise, businesses need to identify who within the organization will play a lead role in developing, enacting and enforcing identity and access policies. IAM impacts every department and every type of user (employee, contractor, partner, supplier, customer, etc.), so it's essential the IAM team comprises a mix of corporate functions.
- IT professionals implementing an IAM system largely on-premises and largely for employees should become familiar with the OSA IAM design pattern for identity management, SP-010. The pattern lays out the architecture of how various roles interact with IAM components as well as the systems that rely on IAM. Policy enforcement and policy decisions are separated from one another, as they are dealt with by different elements within the IAM framework.

1. Make a list of usage, including applications, services, components and other elements users will interact with. This list will help validate that usage assumptions are correct and will be instrumental in selecting the features needed from an IAM product or service.
2. Understand how the organization's environments, such as cloud-based applications and on-premises applications, link together. These systems might need a specific type of federation (Security Assertion Markup Language OpenID Connect, for instance).
3. Know the specific areas of IAM most important to the business. Answering the following questions will help:
    a. Is multifactor authentication needed?
    b. Do customers and employees need to be supported in the same system?
    c. Are automated provisioning and deprovisioning required?
    d. What standards need to be supported?

Implementations should be carried out with IAM best practices in mind, including documenting expectations and responsibilities for IAM success. Businesses also should make sure to centralize security and critical systems around identity. Perhaps most important, organizations should create a process they can use to evaluate the efficacy of current IAM controls.

Introduction to Federal Identity Management

- The term "identity management" is relatively new, the concept is not. In fact, the underlying processes have been in use for many generations in an offline environment. Passports, driver's licenses, and employee ID cards are all components of what might be referred to as identity management systems – i.e., they are credentials issued by an entity for the purpose of identifying individuals, and they are used by such individuals to validate their identity in order to enter into a transaction with a third party.
- While there are many different approaches to identity management, it essentially involves two fundamental processes:
- the process of identifying a person and issuing an identity credential to reflect that identity ("identification"), and
- the process of later verifying that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person ("authentication").
- Once an individual's identity is successfully authenticated, a third process, referred to as "authorization," is used by the business relying on the authenticated identity to determine what rights and privileges are accorded to such person – e.g., whether such person should be granted access to a website, a database, a bar, an airport boarding area, etc.
- A simple and familiar example of these processes can be seen in the case of an employee who logs into his or her employer's network using a user ID and password.
- Before a company allows a person to access its internal network, that person must be properly identified in a manner appropriate for the transaction (e.g., as an employee with certain authority), and then that identity must be authenticated at the time of each transaction. Employees are identified by their employer, and issued an identity credential consisting of a unique identifier (typically a User ID) which is linked to other relevant information attributes stored on the company's computer system. A secret (in this case, a password), is then used to link the employee to the identity credential. Thereafter, when the employee wants to remotely access the company's network, he or she can be authenticated by using the password in an authentication protocol. The authentication protocol allows the employee to demonstrate to the employer that he or she has or knows the secret, and thus, is the person previously identified
- A key characteristic of some existing offline identity documents (such as a passport or driver's license) is that

their use is not limited to transactions with the entities that issued them. Rather, they are often accepted by third parties (such as airport security, a bank, or a bartender) when proof of certain aspects of one's identity is required. This characteristic is critical for the identity credentials needed for e-commerce. Such an approach, whereby a business or government agency relies on an identification process performed, and identity information provided, by one of several possible unrelated third parties is sometimes referred to as a federated identity model. Under such a model, a single identity credential can be used with numerous organizations that had no involvement with the original issuance of the credential. The challenge is to import a similar approach to the digital online environment. That is, to create secure, reliable and trustworthy digital identity credentials that can be used across different ecosystems and entities. This allows individuals to use the same identity credential to sign on to the networks of more than one business in order to conduct transactions.

IAM Best Practices

Identity and Access Management (IAM) has become an essential element of security plans for many organizations. To reap the most security benefits, it is imperative that companies ensure that their IAM tools and processes are set up correctly. In this article, we will share 11 identity and access management best practices your company should adopt to establish a strong security posture. By the end of this article, you'll know the next steps to take to incorporate **IAM best practices** into your security strategy.

1. Adopt a Zero Trust Approach to Security

Many companies have applications, platforms, and tools that are designed with implicit trust features. Implicit trust means that if users have access to your network or log in to a tool, the system "remembers" them and doesn't always prompt the user to verify their identity again. These lax access permissions can pose a major risk to your organization's security stance if an unauthorized entity gains access to your system via a remembered credential.

2. Identify and Protect High-Value Data

Protecting your most valuable data involves limiting who can access it as much as possible—but, to limit access, you first need to know where your most valuable data is stored and how it is used.

3. Enforce a Strong Password Policy

Your IAM technologies are only as strong as the identity management best practices and policies that support them. If your team is leveraging single sign-on (SSO) tools, it's critical that each user's password is strong, unique, and difficult to guess to support password and IAM best practices. Passwords must be complex enough to deter cyberattacks, frequently changed, and not used for multiple sign-on requirements.

4. Use Multi-Factor Authentication (MFA)

User authentication is an essential component of effective identity and access management best practices. After all, if you can't guarantee a user is who they claim to be, you may be putting your data at risk and unintentionally allowing access to an unauthorized user.

MFA tools often use a combination of these methods to authenticate identity:

- Biometric authentication (e.g., fingerprints or facial recognition)
- Possession authentication (e.g., sending a one-time password to a user's personal device)
- Knowledge authentication (e.g., answering security questions)
- User location or time data

5. Automate Workflows

IAM tools offer IT teams many opportunities to use automation to make your organization more secure. Automation reduces manual errors, streamlines workflows, and supports compliance and governance needs.

6. Adopt The Principle of Least Privilege

One of the most common roles and permissions best practices is applying the principle of least privilege. IAM least privilege encourages organizations to restrict access and permissions as much as possible, without interfering with

users' daily workflows.

7. Enforce Just-in-Time Access Where Appropriate

In some circumstances, the principle of least privilege doesn't provide the necessary flexibility that certain situations require. For instance, a help desk associate may need temporary elevation of privileges to troubleshoot a customer's urgent ticket. One way to enforce identity and access management best practices, yet still support the principle of least privilege without compromising user experience, is by leveraging just-in-time access.

8. Leverage Both Role-Based Access Control and Attribute-Based Access Control Policies

Using role-based access control (RBAC) and attribute-based access control (ABAC) together can facilitate robust user access management best practices.

9. Regularly Audit Access to Resources

Even with strong policies around access control, over-provisioning remains a problem for many organizations. Auditing is one of the fundamental IAM best practices to build into your overall IAM strategy to maintain the principle of least privilege.

10. Centralize Log Collection

Many IAM tools automatically generate logs, and these logs are valuable tools to help your team meet compliance requirements, audit usage, and strengthen IAM policies. However, not all teams think to centralize where they store their logs.

11. Adopt IAM Solutions That Work With Existing Tools Using the right tools can make applying identity and access management industry best practices much easier for your organization. There's no need to force a round peg into a square hole; instead of making IAM solutions fit your existing tech stack, search for the right solutions that already support your existing tools and applications.

IAM ADUIT LOGS

1) Create an IAM Policy

Make sure the IAM process is clearly defined and a crucial part of your organizational security policy. Creating an IAM policy document is strongly recommended for the following reasons:

- Meet compliance requirements
- Manage user access and authorization
- Define access to stakeholders who can help make a robust IAM policy
- Robust incident response

Moreover, it's more important to review the policy document at regular intervals to ensure that the right practices are updated and followed on time.

2) Develop and Streamline Procedure

It's not done with creating a policy, and you see desired results only if implemented properly. For that, you need to develop a procedure involving all stakeholders in the IAM process and define roles.

The streamlined procedure should have the list of stakeholders with assigned responsibilities and actions they are accountable for.

3) Access Review

In any organization, users, roles, and responsibilities keep changing. In such a scenario, it's important to review access and authorizations given to different users. To ensure the right access is given, formulate a user access review process.

Keep reviewing that at different intervals to avoid discrepancies. Policy-Based Access Control (PBAC) is one means to execute the user access review process.

4) Appropriate Privileges

This is the crucial point that defines the robustness of an IAM system. Despite being known, this is often ignored. It's very important to see the user access remains limited to 'particular' job requirements and not further. It's recommended to follow the Least Privileged Account principle, which calls for setting maximum limitations possible to the resources.

If special privileges have to be given, make sure to revoke them immediately after the temporary period set for its usage ends.

5) Segregating Responsibilities

This is one crucial aspect that can avoid possible risks in the very first step. Segregating duties among people keeps them limited to their respective functions, and none gets complete access. In case of critical tasks, break them into smaller ones and assign them to multiple people. This keeps every process and its associated security functions independent from others.

In case one of any breach to a process, the threat scope remains limited to that particular process, leaving the rest of the system.

6) Generic Accounts

Generic accounts are required in every organization to execute regular and common activities like training and testing. But keeping them idle can lead to security risks. Never assign admin rights to generic accounts and make sure to delete the unused ones.

It's important to see they are bound by strong passwords to avoid breaches through default settings. Privileged Access Management (PAM) and PBAC can offer full control over generic accounts.

7) Delete/Disable Idle Accounts

It's important to keep your IAM system clean, secure and updated. Delete any unused user account (generic or important ones) lying idle. Leaving them is like allowing them to grow further and welcome threats through them.

Delete inactive users lying individually and in groups. Make sure users are only present in their relevant groups. Conduct a regular review of group policies and delete exposed login details.

8) Document Everything

Back to where we started. We started with documenting policy for its effective implementation. But it's important to document everything in implementation too. This forms as a trial for future implementations and helps comply with rules every time.

Documentation is key to the IAM audit process, where you need to share administration activities, policies, and usage documented. Moreover, the documentation process gives a better understanding of the entire IAM system, helping you find ways to improve it further.

Intro to AWS/Azure clint and Web Portal

What is AWS client?

- AWS Client VPN is **a fully-managed remote access VPN solution used by your remote workforce to securely access resources within both AWS and your on-premises network**. Fully elastic, it automatically scales up, or down, based on demand.

- When migrating applications to AWS, your users access them the same way before, during, and after the move. AWS Client VPN, including the software client, supports the OpenVPN protocol.

Benefits

Advanced authentication

- Many organizations require multi-factor authentication (MFA) and federated authentication from their VPN solution. AWS Client VPN supports these and other authentication methods.

Elastic

- Traditional on-premises VPN services are limited by the capacity of the hardware that runs them. AWS Client VPN is a pay-as-you-go cloud VPN service that elastically scales up or down based on user demand.

Remote access

- Unlike on-premises VPN services, AWS Client VPN allows users to connect to AWS and on-premises networks using a single VPN connection

Fully managed

- AWS Client VPN automatically takes care of deployment, capacity provisioning, and service updates — while you monitor all connections from a single console.

AWS Client VPN use cases

Quickly scale remote access

- Unexpected events can require many of your employees to work remotely. This creates a spike in VPN connections and traffic that can reduce performance or availability for your users. AWS Client VPN is elastic, and automatically scales up to handle peak demand. When the spike has passed, it scales down so you are not paying for unused capacity.

Access applications during migration

- AWS Client VPN provides users with secure access to applications both on premises and in AWS. This is helpful during a cloud migration when applications move from on-premises locations to the cloud. With AWS Client VPN, users don't have to change the way they access their applications during or after migration.

Integrate with your authentication and MDM systems

- AWS Client VPN supports authentication with Microsoft Active Directory using AWS Directory Services, Certificate-based authentication, and Federated Authentication using SAML-2.0 to facilitate these scenarios when using the AWS provided OpenVPN Client software. AWS Client VPN works with Mobile Device Management (MDM) solutions to reject devices that do not comply with the your policies.

Securely connecting IoT devices

Create encrypted connections between IoT devices and Amazon Virtual Private Cloud (VPC) resources using certificate-based authentication.

In this tutorial you will create a Client VPN endpoint that does the following:

- Provides all clients with access to a single VPC.
- Provides all clients with access to the internet.
- Uses mutual authentication.

The following diagram represents the configuration of your VPC and Client VPN endpoint after you've completed this tutorial.

Steps

- Prerequisites
- Step 1: Generate server and client certificates and keys
- Step 2: Create a Client VPN endpoint
- Step 3: Associate a target network
- Step 4: Add an authorization rule for the VPC
- Step 5: Provide access to the internet
- Step 6: Verify security group requirements
- Step 7: Download the Client VPN endpoint configuration file
- Step 8: Connect to the Client VPN endpoint

What is Azure?

Azure Cloud is an ever-expanding set of services that help your organization meet your current and future business challenges. Azure gives you the freedom to build, manage and deploy applications across a vast global network using the tools and frameworks of your choice.

What does Azure provide?

With Azure, you have everything you need to build your next great solution. The following table lists the many benefits that Azure provides for ease of invoicing with Objective.

Be ready for the future: Microsoft's constant innovation supports your growth today and your product vision for tomorrow.

Build on Your Terms: You have options. With a commitment to open-source and support for all languages and frameworks, you can build as you wish and deploy wherever you want.

Operate the hybrid seamlessly: on-premises, in the cloud, and on edge--we'll meet you where you are. Integrate and manage your environment with tools and services designed for hybrid cloud solutions.

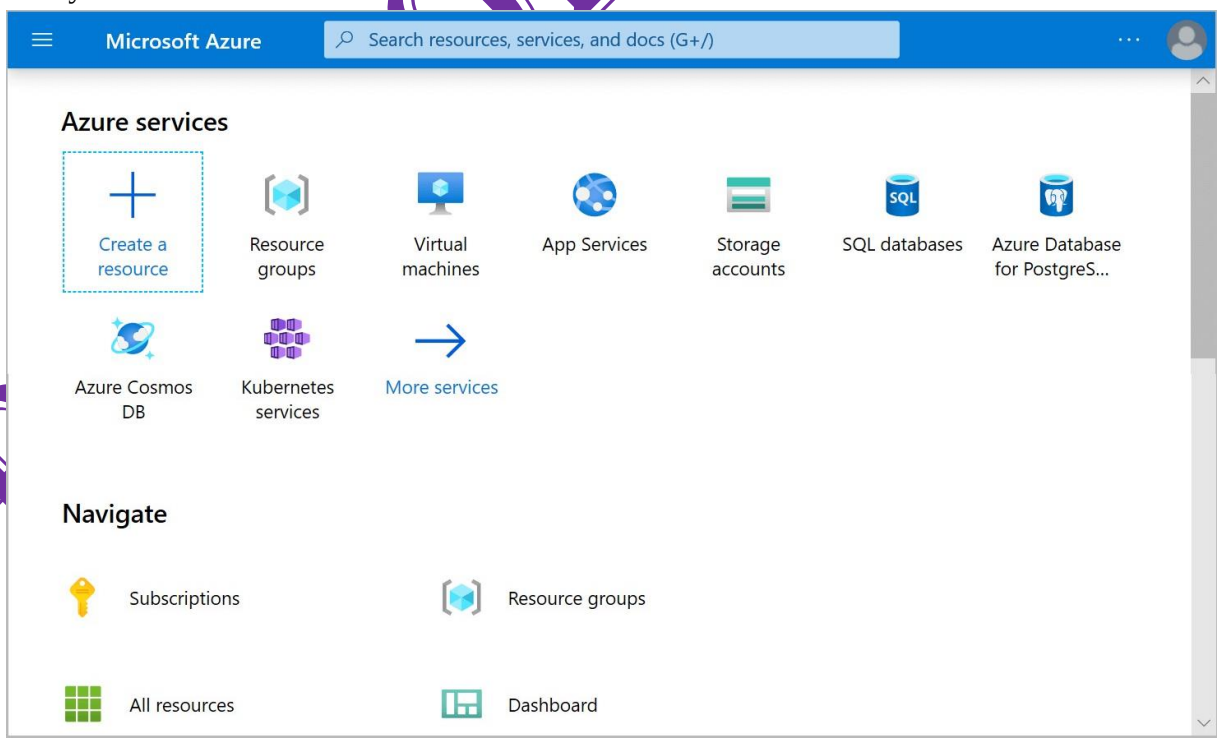
Trust your cloud: Get security from the ground up, backed by a team of experts, and proactive compliance trusted by enterprises, governments, and startups.

What is Azure Portal?

Azure Portal is a web-based, integrated console that provides an alternative to command-line tools. With the Azure Portal, you can manage your Azure subscription using the graphical user interface. You can do this:

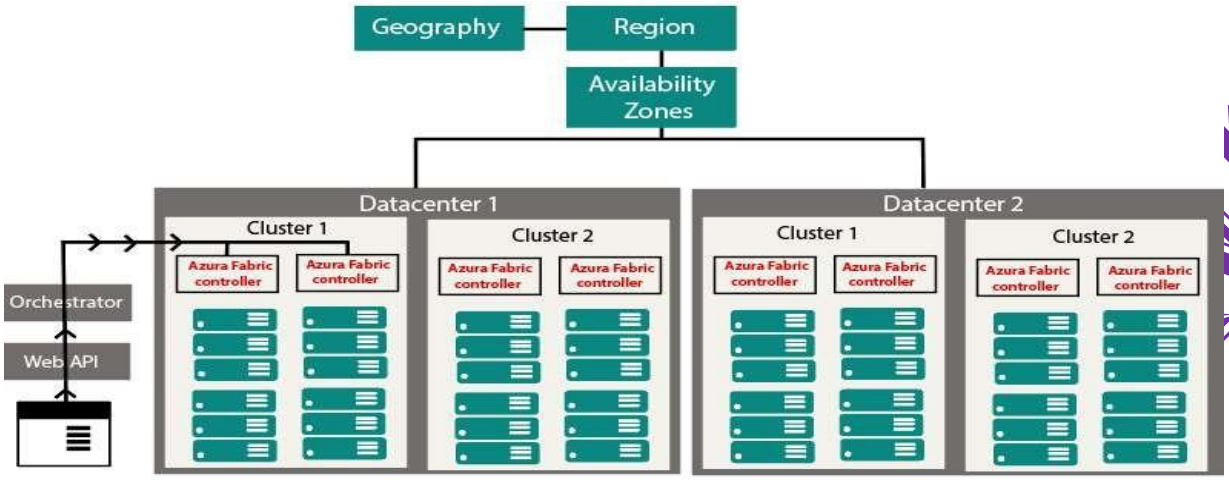
- Build, manage and monitor everything from simple web apps to complex cloud deployments.
- Create custom dashboards for an organized view of resources.
- Configure accessibility options for the optimum experience.

The Azure Portal is designed for flexibility and constant availability. It maintains a presence in each Azure datacenter. This configuration makes the Azure portal resilient to isolated datacenter failures and prevents network slowdowns by being closer to users. The Azure Portal is constantly updated, and maintenance activities do not require any downtime.



How Azure works

It is essential to understand the internal workings of Azure so that we can design our applications on Azure effectively with high availability, data residency, resilience, etc.



Microsoft Azure is completely based on the concept of virtualization. So, similar to other virtualized data center, it also contains *racks*. Each rack has a separate power unit and network switch, and also each rack is integrated with a software called *Fabric-Controller*. This *Fabric-controller* is a distributed application, which is responsible for managing and monitoring servers within the rack. In case of any server failure, the Fabric-controller recognizes it and recovers it. And Each of these Fabric-Controller is, in turn, connected to a piece of software called *Orchestrator*. This *Orchestrator* includes web-services, Rest API to create, update, and delete resources.

When a request is made by the user either using PowerShell or Azure portal. First, it will go to the Orchestrator, where it will fundamentally do three things:

1. Authenticate the User
2. It will Authorize the user, i.e., it will check whether the user is allowed to do the requested task.
3. It will look into the database for the availability of space based on the resources and pass the request to an appropriate Azure Fabric controller to execute the request.

Combinations of racks form a cluster. We have multiple clusters within a data center, and we can have multiple Data Centers within an Availability zone, multiple Availability zones within a Region, and multiple Regions within a Geography.

- **Geographies:** It is a discrete market, typically contains two or more regions, that preserves data residency and compliance boundaries.
- **Azure regions:** A region is a collection of data centers deployed within a defined perimeter and interconnected through a dedicated regional low-latency network.
- **Availability Zones:** These are the physically separated location within an Azure region. Each one of them is made up of one or more data centers, independent configuration.

Azure covers more global regions than any other cloud provider, which offers the scalability needed to bring applications and users closer around the world. It is globally available in 50 regions around the world. Due to its availability over many regions, it helps in preserving data residency and offers comprehensive compliance and flexible options to the customers.

Vulnerability management:

- It is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their "attack surface."

Vulnerability management process:

Every new vulnerability introduces risk to the organization. So, a defined process is often used to provide organizations with a way to identify and address vulnerabilities quickly and continually. At a high level, 6 processes make up vulnerability management—each with their own subprocesses and tasks.

- Discover: You can't secure what you're unaware of. The first process involves taking an inventory of all assets across the environment, identifying details including operating system, services, applications, and configurations to identify vulnerabilities. This usually includes both a network scan and an authenticated agent-based system scan. Discovery should be performed regularly on an automated schedule.
- Prioritize: Second, discovered assets need to be categorized into groups and assigned a risk-based prioritization based on criticality to the organization.
- Assess: Third is establishing a risk baseline for your point of reference as vulnerabilities are remediated and risk is eliminated. Assessments provide an ongoing baseline over time.
- Remediate: Fourth, based on risk prioritization, vulnerabilities should be fixed (whether via patching or reconfiguration). Controls should be in place so that that remediation is completed successfully and progress can be documented.
- Verify: Fifth, validation of remediation is accomplished through additional scans and/or IT reporting.
- Report: Finally, IT, executives, and the C-suite all have need to understand the current state of risk around vulnerabilities. IT needs tactical reporting on vulnerabilities identified and remediated (by comparing the most recent scan with the previous one), executives need a summary of the current state of vulnerability (think red/yellow/green type reporting), and the C-suite needs something high-level like simple risk scores across parts of the business.

Discovering cloud misconfigurations:

- Companies are increasingly moving their IT operations to IaaS (infrastructure-as-a-service) solutions. Gartner estimates that by 2022, about 60% of business entities will be leveraging cloud-managed offerings, doubling the recorded use in 2018.
- Cloud offerings like Amazon Web Services (AWS) are generally secure. But since IaaS uses a shared security model, there's a great chance of data security issues, including cybersecurity and workload concerns. Misconfigurations when migrating to cloud-native environments can inadvertently lead to cybersecurity loopholes.
- Misconfiguration isn't just a theoretical cloud computing concern. McAfee's enterprise security research shows that the typical enterprise experiences approximately 3,500 incidents monthly. From the study, 90% of businesses reported that they'd experienced IaaS security issues.
- Therefore, getting it right with cloud migration configuration can significantly reduce future IaaS security issues and boost your digital transformation.

Cloud Misconfiguration – A Major Security Threat

- Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption. These cyber threats come in the form of security breaches, external hackers, ransomware, malware, or insider threats that use vulnerabilities to access your network.

- The NSA considers cloud misconfiguration a leading vulnerability in a cloud environment. While these risks are often less sophisticated, the issues' prevalence is generally through the roof.
- Misconfiguration is a cloud computing problem because multi-cloud environments can be quite complicated, and it can be tough to detect and manually remediate mistakes. According to a Gartner survey, these issues cause 80% of all data security breaches, and until 2025, up to 99% of cloud environment failures will be attributed to human errors.
- This is tricky, considering there's no one-time remedy for cloud misconfiguration issues like cloud leaks. However, it would help to implement security procedures at the build stage. So, DevOps and security teams must work collaboratively.

Common Cloud Misconfigurations and Their Solutions

- Let's take a deep dive into the most common cloud misconfigurations that you'll likely have to deal with when migrating to a cloud environment.

1. Unrestricted Inbound Ports

- All ports open to the internet can be potentially problematic. Cloud services mostly use high-number UDP or TCP ports to prevent exposure risks, but determined hackers can still sniff them out. Obfuscation can be helpful, but it's insufficient by itself.
- When migrating to a multi-cloud environment, make sure you know the full range of open ports and then restrict or lock down those that aren't strictly necessary.

2. Unrestricted Outbound Ports

- These ports create opportunities for security events like data exfiltration, lateral movement, and internal network scans once there's a system compromise. Granting outbound access to RDP or SSH is a common cloud misconfiguration. Application servers seldom have to SSH to other network servers, so it's unnecessary to use open outbound ports for SSH.
- Make sure you limit the outbound port access and use the least privilege principle to restrict outbound communications.

3. "Secrets" Management

- This configuration issue can be damaging to your organization. Securing secrets like API keys, passwords, encryption keys, and admin credentials is essential. But most companies openly avail these through compromised servers, poorly configured cloud buckets, HTML code, and GitHub repositories. This is as risky as leaving your home's deadbolt key taped to your front door.
- You can beat this by maintaining an inventory of all your company secrets in the cloud and regularly evaluating how they're secured. Otherwise, threat actors could easily breach your systems, access your data, and overrun your cloud resources to effect irreversible damage.
- You may also use secret management solutions and services like Hashicorp Vault, AWS Secrets Manager, Azure Key Vault, and AWS Parameter Store.

4. Disabled Monitoring and Logging

- Surprisingly, most organizations fail to configure, enable, or review the telemetry data and logs offered by public clouds, which can be sophisticated. It would help to have someone responsible for regular reviews and flagging security-related incidents.
- This valuable tip isn't only limited to IaaS public clouds. You'll also get the same information from storage-as-a-service vendors, which you must also review regularly. A maintenance alert or update bulletin could leave your organization with profound security implications, but it won't help if there's no one paying attention.

5. ICMP Left Open

- The ICMP (Internet Control Message Protocol) reports network device errors, but it's a common target for threat actors. This happens because while the protocol can display if your server is responsive and online, cybercriminals can also use it to pinpoint an attack.
- Furthermore, it's also an attack vector for denial-of-service (DDoS) and many types of malware. A ping flood or ping sweep can overwhelm your servers with ICMP messages. While it's a dated attack strategy, it's still effective. So make sure your cloud configuration blocks ICMP.

6. Insecure Automated Backups

- Insider threats to your cloud environment are an ever-present cybersecurity risk. According to McAfee, about 92% of business organizations have workers' credentials being sold on the darknet. One section where insider threats can be particularly damaging is when you fail to secure automated cloud data backup properly.
- You may have protected your master data, but poorly configured backups will inadvertently remain vulnerable and exposed to insider threats.
- When migrating to the cloud, ensure your backups are encrypted whether at rest or in transit. Also, verify the permissions to restrict access to the backups.

7. Storage Access

- Most cloud users believe that "authenticated users" only cover those already authenticated within the relevant apps or organizations regarding storage buckets. Unfortunately, this isn't the case.
- "Authenticated users" refers to any person with AWS authentication, essentially any AWS client. Due to this misunderstanding, alongside the resulting control settings misconfiguration, you may have your storage objects wholly exposed to public access. Be especially cautious when setting storage object access to grant it to only the people within your organization.

8. Lack of Validation

- This cloud configuration error is a meta-issue: most organizations don't create and implement systems for identifying misconfigurations whenever they occur. Whether an outside auditor or internal resource, you need someone to verify that permissions and services are correctly configured and deployed.
- Create a schedule that ensures validation occurs like clockwork because mistakes are inevitable as the cloud environment evolves. You also need a rigorous process of auditing cloud configurations periodically. Otherwise, you may leave a security loophole that cybercriminals can exploit.

9. Unlimited Access to Non-HTTPS/HTTP Ports

- Web servers are made to host web services and websites to the internet, alongside other services like RDP or SSH for databases or management. However, you must block these from accessing every part of the internet.
- Improperly configured ports can open your cloud infrastructure up to malicious actors looking to brute force or exploit the authentication. When opening these ports to the web, ensure you limit them to accept traffic from specific addresses, such as your office.

10. Overly Permissive Access to Virtual Machines, Containers, and Hosts

- Would you connect a virtual or physical server in your data center directly to the internet without protecting it using a firewall or filter? You likely wouldn't, but people do exactly this in their cloud infrastructures all the time.
- Some of the most common examples include:
  - Enabling legacy protocols and ports like FTP on cloud hosts

- Legacy protocols and ports like rexec, rsh, and telnet in physical serves that have been made virtual and moved to the cloud
- Exposing etcd (port 2379) for Kubernetes clusters to the public internet

- You can avoid this cloud configuration mistake by securing important ports and disabling (or at the very least locking down) legacy, insecure protocols in your cloud environment the same way you would treat your on-premise data center.

11. Enabling Too Many Cloud Access Permissions

- A major benefit of cloud computing is its ease of scalability. However, this simplicity of expansion is not without its downsides. As cloud environments grow larger and more complex, administrators rapidly lose oversight of system controls.
- Lack of visibility makes it harder for admins to review permissions and restrict access. They may also find it easier to enable default permission settings for all users to avoid dealing with an influx of access requests.
- Unnecessary permissions greatly increase the risk of insider threats, which could result in cloud leaks and data breaches.
- Organizations should seek to adopt the emerging Secure Access Service Edge (SASE) architecture, which enables more efficient cloud security, including the use of Cloud Access Service Brokers (CASBs) and Cloud Security Posture Management (CSPM) solutions to manage user permissions in multi-cloud environments.

12. Subdomain Hijacking (AKA Dangling DNS)

- A common cause of this type of cyberattack is when an organization deletes a subdomain from its virtual host (e.g. AWS, Azure, Github, etc.) but forgets to delete the its associated records from the Domain Name System (DNS).
- Once the attacker discovers the unused subdomain, they can re-register it via the hosting platform and route users to their own malicious web pages.
- Such hijacking could result in malware injections or phishing attacks to unsuspecting users and can cause severe reputational damage to the original subdomain owner.
- To avoid subdomain hijacking, organizations should always remember to delete DNS records for all domains and subdomains that are no longer in use.
- 13. Misconfigurations Specific to Your Cloud Provider(s)
- While misconfigurations like open ports and overly permissive access are applicable to all cloud providers, many misconfigurations exist that are more specific to the service(s) you're using. For example, default public access settings for S3 buckets is a well-known AWS flaw.
- Organizations should research cloud misconfigurations specific to their cloud service provider(s).

Remediating vulnerabilities:

- It is always important to remember that the end-game of vulnerability management is remediation. One of the important KPIs of a vulnerability management program is how many high-risk vulnerabilities are removed or neutralized before critical systems and assets are compromised.

Why is Vulnerability Remediation Important?

- Customers, partners, employees and regulators expect companies to put in place policies and processes that continuously and effectively protect data from accidental or malicious loss and exposure. There is also zero tolerance for system disruptions or slowdowns. In short, meeting vulnerability

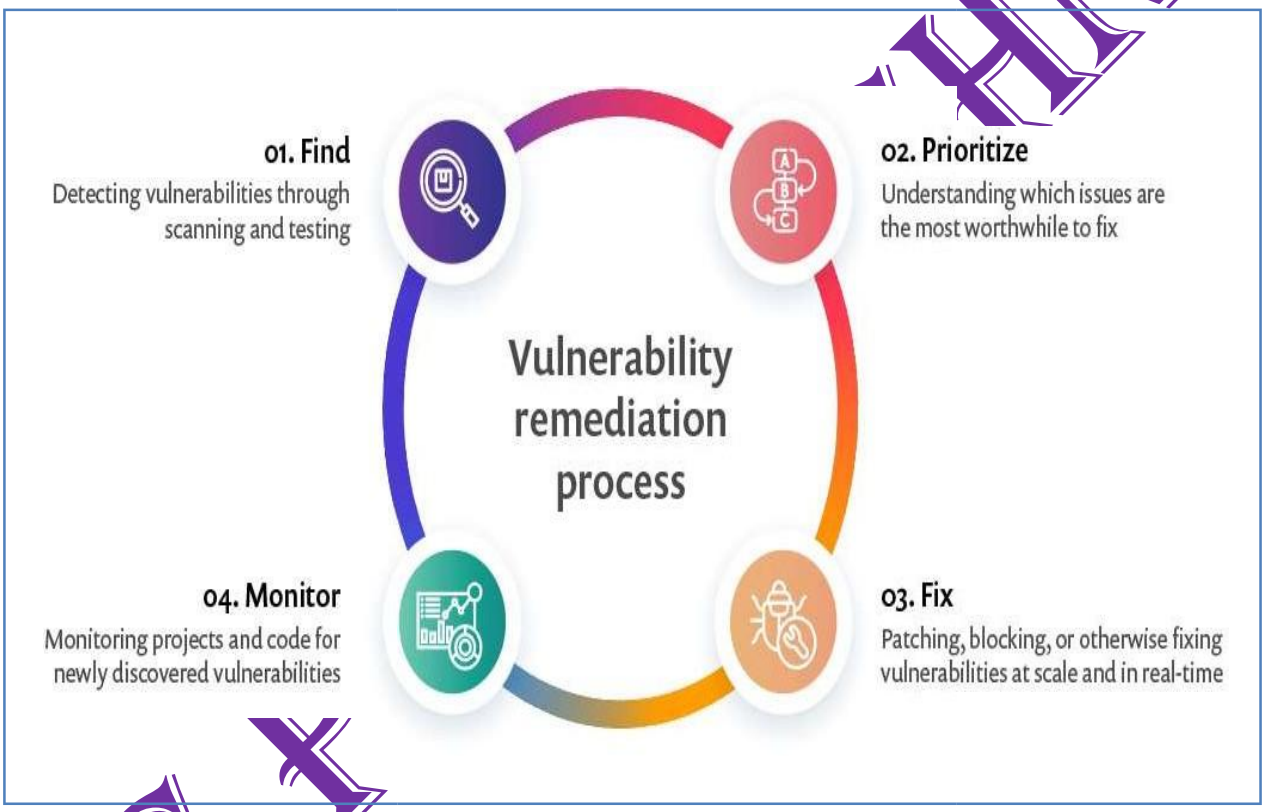
remediation challenges has become a business-critical activity.

What is the Vulnerability Remediation Process?

- The vulnerability remediation process is a workflow that fixes or neutralizes detected weaknesses. It includes 4 steps: finding vulnerabilities through scanning and testing, prioritising, fixing and monitoring vulnerabilities.

4 steps of vulnerability remediation process

1. **Find:** Detecting vulnerabilities through scanning and testing
2. **Prioritize:** Understanding which vulnerabilities pose a real and significant risk
3. **Fix:** Patching, blocking, or otherwise fixing vulnerabilities at scale and in real-time
4. **Monitor:** Automatically monitor projects and code for newly discovered vulnerabilities, with real-time alerts and notifications via all the relevant channels



1. Finding Vulnerabilities

- Security vulnerabilities are known coding flaws or system misconfigurations that can be exploited to compromise an application, service, library, container, or function and all its related assets. The active exploit seeks to shut down or disrupt performance, exfiltrate data, hijack compute resources, and so on. Systems and assets that are laterally accessible to the compromised component are also at risk.
- The first step of the vulnerability remediation process, therefore, is to scan for and find security vulnerabilities. Mature vulnerability management programs implement a shift-left DevSecOps approach in which vulnerability scanning takes place throughout a secure SDLC (software development life cycle). In order not to slow down the CI/CD pipeline, automated vulnerability testing tools are deployed in development, testing, and production environments. These may include:
  - **Software Composition Analysis** (SCA) tools
  - **Open source vulnerability scanners**
  - White-box static application security (**SAST**) tools

- Black-box dynamic application security tools (**DAST**)

- Special attention needs to be paid to **container security**. It is important to scan for security vulnerabilities in container images as well as in running container instances, with all their linkages. It is also important to ensure that third-party container images are from trusted sources only. **Kubernetes security** also raises a unique set of vulnerability scanning challenges. If a cluster is breached, every service and machine in the network is at risk.

2. Prioritizing Vulnerabilities

- The next step in the vulnerability remediation process is prioritizing vulnerability remediation.
- No matter which approach your company takes to security risk management, not every detected vulnerability poses the same level of risk. It is always a tradeoff among a variety of considerations such as severity, fixability, coverage, and compliance. With risk-based, context-aware prioritization, the vulnerability remediation team can focus its limited resources on the issues that matter the most.
- Good likelihood that 80% plus of discovered vulnerabilities are false-positives. another 18% are low-risk and then the last 2% are really things that you need to fix.

3. Fixing Vulnerabilities

- The third step in the vulnerability remediation process is to fix the weakness.
- In many cases, removing vulnerable software involves deploying an upgrade or a patch, as recommended by the vendor of the affected software. However, patch deployment can be challenging in and of itself. Testing and rolling out patches and upgrades can consume considerable time and resources. Business-critical systems may have to be shut down during the deployment process. And there is always the risk that the patch will have unforeseen impact on the application itself or its dependencies.
- There may be less risky ways to fix a weakness, or to at least buy time while a patch is being prepared for deployments. For example, you can update risky system, platform, or service configurations. Similarly, you can disable a vulnerable process or function, or remove a vulnerable component, that is not actually in use.

4. Monitoring Vulnerabilities

- Just like the rest of the SDLC, the security vulnerability remediation process is continuous. To facilitate this loop, you need to have monitoring in place. The tool(s) you use to do this need to automatically monitor projects and code for newly discovered vulnerabilities, with real-time alerts and notifications via all the relevant channels.
- Ideally, the monitoring tool will also provide contextualized prioritization, helping with both steps 1 and 2 of the vulnerability remediation process (**find** and **prioritize**). Otherwise, developers or AppSec teams receiving notifications will quickly become burned out by an influx of low-priority vulnerabilities. It's important that teams are not overwhelmed by noise, which can delay them from handling important, high-priority vulnerabilities that need prompt remediation.

Tracking open vulnerabilities using cloud native tools:

- All three of the major cloud providers offer a vulnerability scanning solution as part of their cloud services. Let's see what is provided by these first-party solutions.

AWS Vulnerability Scanning

- Amazon Inspector is a vulnerability management service that continuously scans AWS workloads for vulnerabilities. It automatically detects and scans Amazon EC2 instances and container images in Amazon Elastic Container Registry (Amazon ECR), identifying software vulnerabilities and accidental network exposure.
- Amazon Inspector creates a "finding" when it identifies software vulnerabilities or network issues. These

findings describe the vulnerability, identify affected resources, assess the severity of the vulnerability, and provide remediation guidance. You can use the Amazon Inspector console to review findings in your Amazon account, or view findings within other AWS services.

Azure Vulnerability Scanning

- Microsoft provides Defender Vulnerability Management, a solution that provides asset visibility, assessment, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and networked devices. It can be used to secure resources in the Azure cloud and elsewhere.
- By leveraging Microsoft's extensive threat intelligence database, Defender Vulnerability Management automatically assesses the business and device environment and performs breach forecasting. It can quickly and consistently prioritize and assign risk scores to vulnerabilities in a company's most valuable assets, including both software vulnerabilities and misconfigurations, and provides actionable remediation advice to mitigate the impact.

Google Cloud Platform (GCP) Vulnerability Scanning

Google provides the Security Command Center, which offers three key vulnerability scanning features:

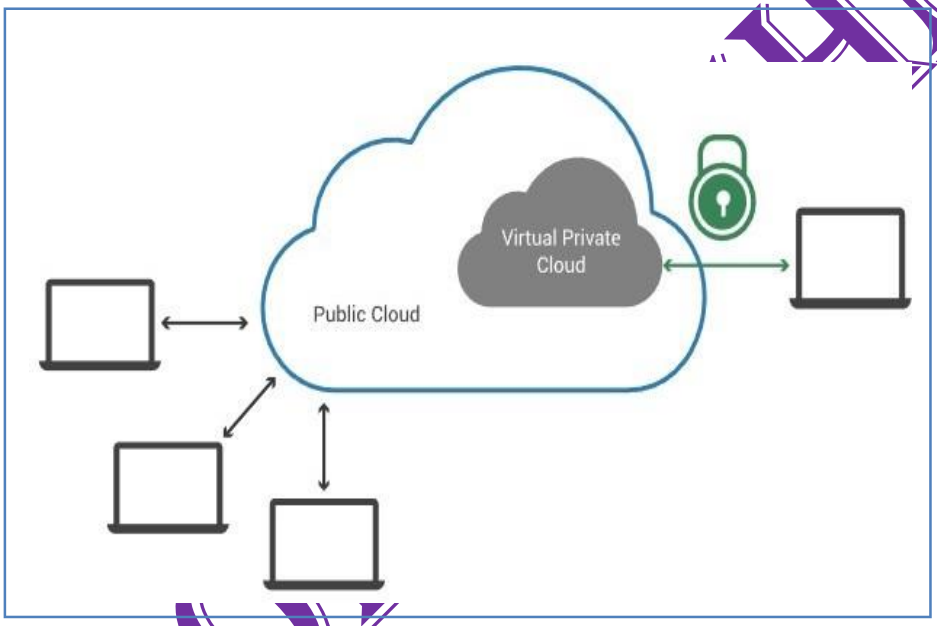
- Continuously monitors container images to identify suspicious changes and remote access attempts. The service can detect common container runtime attacks.
- Monitors cloud logs for your organization's Google services and detects threats using detection logic and threat intelligence feeds from Google.
- Scans web applications running on Google App Engine, Google Compute Engine, or Google Kubernetes Engine (GKE). The service can scrape application URLs, execute user input, and test for vulnerabilities such as legacy libraries, mixed content, and cross-site scripting (XSS).

Network security and Security groups:

- Cloud-based infrastructure requires a similar level of security as an organization's on-prem environment. Cloud network security is a foundational layer of cloud security and is vital to protecting the data, applications, and IT resources deployed within enterprise cloud environments as well as the traffic flowing between cloud deployments and the enterprise's intranet and on-prem data centers.
- On-prem enterprise networks use network security solutions for advanced threat prevention, to restrict access to corporate systems, enforce security policies, and perform internal segmentation of corporate networks. Cloud network security provides similar enterprise-grade protection to cloud infrastructure and networks.
- Network Security Groups(NSGs)
- Network security groups (NSGs) determine the inbound and outbound traffic to and from your CDP environment. That is, you should use security group settings to allow users from your organization access to CDP(Cloudera Data Platform) resources.
- You have two options:
  - Use your existing security groups (recommended for production)
  - Have CDP create new security groups
- You should verify the security group limits in your Azure account to ensure that you can create security groups for CDP.

Virtual Private Clouds (VPC):

- A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider.
- VPCs combine the scalability and convenience of public cloud computing with the data isolation of private cloud computing.
- Imagine a public cloud as a crowded restaurant, and a virtual private cloud as a reserved table in that crowded restaurant. Even though the restaurant is full of people, a table with a "Reserved" sign on it can only be accessed by the party who made the reservation. Similarly, a public cloud is crowded with various cloud customers accessing computing resources – but a VPC reserves some of those resources for use by only one customer.



How a virtual private cloud works

- In a virtual private cloud model, the public infrastructure-as-a-service (IaaS) provider is responsible for ensuring that each private cloud customer's data remains isolated from every other customer's data both in transit and inside the cloud provider's network. This can be accomplished through the use of security policies requiring some -- or all -- of the following elements: encryption, tunneling, private IP addressing or allocating a unique virtual local area network (VLAN) to each customer.
- A virtual private cloud user can define and directly manage network components, including IP addresses, subnets, network gateways and access control policies.

Benefits and challenges of virtual private clouds

- As mentioned above, one of the biggest benefits of VPCs is that they enable an enterprise to tap into some of the benefits of private clouds, such as more granular network control, while still using off-premises, public cloud resources in a highly scalable, pay-as-you-go model.
- Another benefit of VPCs is enabling a hybrid cloud deployment. An enterprise can use a VPC as an extension of its own data center without dealing with the complexities of building an on-premises private cloud.
- Despite the benefits of VPCs, they can also introduce some challenges. For example, an enterprise might face some complexity when configuring, managing and monitoring its virtual private network (VPN).

- In addition, while VPCs offer an isolated environment within a public cloud in which workloads can run, they are still hosted outside an enterprise's own data center. This means that businesses in highly regulated industries with strict compliance requirements might face limitations on which kinds of applications and data they can place in a VPC.
- Before it commits to a VPC, an enterprise should also verify that all of the resources and services it wants to use from its chosen public cloud provider are available via that provider's VPC.

Virtual private cloud providers

- Most leading public IaaS providers, including Amazon Web Services (AWS), Microsoft Azure and Google, offer VPC and virtual network services.

WAF in Cloud:

- A regular **web application firewall (WAF)** provides security by operating through an application or service, blocking service calls, inputs and outputs that do not meet the policy of a firewall, i.e. set of rules to a HTTP conversation. WAFs do not require modification of application source code.
- The rules to blocking an attack can be customized depending on the role in protecting websites that WAFs need to have. This is considered an evolving information security technology, more powerful than a standard network firewall, or a regular intrusion detection system.

- Today, WAF products are deeply integrated with network technologies such as load balancing and — cloud.
- Cloud-based WAFs, thus, utilize all advantages of WAFs and share that threat detection information among all tenants of the service, which improves results and speeds up detection rates.
- The whole community learns from an attack to any website sharing a single cloud-based WAF service. Plus, cloud based WAF technology is:
  - elastic
  - scalable
  - fast
  - easy to set-up
  - offered as pay-as-you-grow service

- sharing back reports

- **By using cloud-based WAFs, clients need not make any software or hardware changes and tunings to their system**, and can successfully protect their websites from threats, by applying custom rules and deciding on the aggressiveness of the protection.
- This service is used and considered ideal by anyone from financial institutions to mid-sized businesses and trading platforms, to government bodies, e-commerce vendors, and so on. They all pick WAF as protection against top vulnerabilities such as:
  - identity theft
  - access to confidential/unauthorized data
  - falsified transactions
  - injection flaws (such as SQL injection)
  - broken authentication session
  - cross-site scripting (XSS flaws)
  - sensitive data exposure
  - forged requests to access functionality
  - forged HTTP requests to a vulnerable web application
  - vulnerable component exploit
  - unvalidated redirects and forwards
- With cloud space opening up and bringing full virtualization of OS, of storage, of software, platform, and infrastructure, more applications need to be developed for the cloud (while most are not) and remain secure on the cloud.
- With WAF in the cloud, traffic is being redirected to traffic scrubbing and protecting proxy farm of WAFs. Cloud-based WAF service providers will often include a full threat analysis, exception handling policies, as well as continuous monitoring of their service.

Incident Response

- An **event** is an observed change to the normal behavior of a system, environment, process, workflow or person. Examples: router ACLs were updated, firewall policy was pushed.
-
- An **alert** is a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action. Examples: the events above sent to on-call personnel.
-
- An **incident** is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business. Examples: attacker posts company credentials online, attacker steals customer credit card database, worm spreads through network.

What is Incident Response?

- Incident response (IR) is the steps used to prepare for, detect, contain, and recover from a data breach.Incident response is the methodology an organization uses to respond to and manage a cyber-attack.
- An incident response aims to reduce this damage and recover as quickly as possible.

- An incident response plan is a document that outlines an organization's procedures, steps, and responsibilities of its incident response program.
- It is a document that spells out the actions that need to be taken to minimise the damage and protect your business data during the attack.

Why is Incident Response Important?

- As the cyberattacks increase in scale and frequency, incident response plans become more vital to a company's cyber defenses.

Who is the Incident Response Team?

- The company should look to their "Computer Incident Response Team (CIRT)" to lead incident response efforts. This team is comprised of experts from upper-level management. Incident response should also be supported by HR, legal, and PR or communications.

Six key steps to a response plan:

1,Preparation:

- Developing policies and procedures to follow in the event of a cyber-breach.
- This will include determining the exact composition of the response team and the triggers to alert internal partners.
- Key to this process is effective training to respond to a breach and documentation to record actions taken for later review.

2.Identification:

- This is the process of detecting a breach and enabling a quick, focused response. IT security teams identify breaches using various threat intelligence streams, intrusion detection systems, and firewalls.
- Some people don't understand what threat intelligence is but it's critical to protecting your company.
- Threat intelligence professionals analyze current cyber threat trends, common tactics used by specific groups, and keep your company one step ahead.

3.Containment:

- One of the first steps after identification is to contain the damage and prevent further penetration.
- This can be accomplished by taking specific sub-networks offline and relying on system backups to maintain operations.
- Your company will likely remain in a state of emergency until the breach is contained.

4.Eradication:

- This stage involves neutralizing the threat and restoring internal systems to as close to their previous state as possible.
- This can involve secondary monitoring to ensure that affected systems are no longer vulnerable to subsequent attack.

5.Recovery:

- Security teams need to validate that all affected systems are no longer compromised and can be returned to working condition.
- This also requires setting timelines to fully restore operations and continued monitoring for any abnormal network activity.
- At this stage, it becomes possible to calculate the cost of the breach and subsequent damage.

6.Lessons Learned:

- One of the most important and often overlooked stages.

- During this stage, the incident response team and partners meet to determine how to improve future efforts.
- This can involve evaluating current policies and procedures, as well specific decisions the team made during the incident.
- Final analysis should be condensed into a report and used for future training.
- Forcepoint can help your team analyze previous incidents and help improve your response procedures.
- Protecting your organization requires a determined effort to constantly learn and harden your network against malicious actors.

A Cyber Incident Response Plan is important because it helps the business to:

1. Identify the breach correctly.
2. Contain the attack, control the damage and perhaps thwart the cyber criminals in their attempt to steal data.
3. Protect customer data and other sensitive information as far as possible.
4. Patch the vulnerabilities that allowed the attack to happen in the first place.
5. Recover from the attack with minimal damage and/or regulatory implications.
6. Assess the lessons learned and implement them to enhance/improve the Cyber Incident Response Plan further.

What Does a Cyber Incident Response Plan Include?

A cyber incident response plan example should outline (amongst other things depending on the organisational context) the key steps your company will take in the event of a cyberattack. Your plan should include the following:

- A description of your company's incident response team and their roles and responsibilities.
- An overview of the company's incident response process.
- The steps that will be taken to contain the attack and prevent it from spreading.
- How information will be shared within the company and with external parties.
- The procedures for restoring systems and data.
- The contact information for key personnel.

Log Analysis

What is log analysis?

Log analysis is the process of reviewing, interpreting and understanding computer-generated records called logs.

Key takeaways

- Log analysis functions manipulate data to help users organize and extract information from the logs.
- Organizations that effectively monitor their cyber security with log analysis can make their network assets more difficult to attack.
- Log analysis is a crucial activity for server administrators who value a proactive approach to IT.
- With Sumo Logic's cloud-native platform, organizations and DevOps teams can aggregate and centralize event logs from applications and their infrastructure components throughout private, public and hybrid cloud environments.

What is a log analyzer?

- Log analyzers provide functionality that helps developers and operations personnel monitor their applications as well as visualize log data in formats that help contextualize the data. This, in turn, enables the development team to gain insight into issues within their applications and identify opportunities for improvement. When referencing a log analyzer, we're referring to software designed for use in log management and log analysis.

Log analysis offers many benefits, but these benefits cannot be realized if the processes for log management and log file analysis are not optimized for the task. Development teams can achieve this level of optimization through the use of log analyzers.

How do you analyze logs?

- One of the traditional ways to analyze logs was to export the files and open them in Microsoft Excel. This time-consuming process has been abandoned, as tools like **Sumo Logic** have entered the market. With Sumo Logic, you can integrate with several different environments using IIS web servers, NGINX, and others. With free trials available to test out their log analysis tooling at no risk, the time has never been better to see how log analyzers can help improve your strategies for log analysis and the processes described above.

Log analysis functions and methods

- Log analysis functions manipulate data to help users organize and extract information from the logs. Here are just a few of the most common methodologies for log analysis.
- **Normalization**
  Normalization is a data management technique wherein parts of a message are converted to the same format. The process of centralizing and indexing log data should include a normalization step where attributes from log entries across applications are standardized and expressed in the same format.
- **Pattern recognition**
  Machine learning applications can now be implemented with log analysis software to compare incoming messages with a pattern book and distinguish between "interesting" and "uninteresting" log messages. Such a system might discard routine log entries, but send an alert when an abnormal entry is detected.
- **Classification and tagging**
  As part of our log analysis, we may want to group log entries that are of the same type. We may want to track all of the errors of a certain type across applications, or we may want to filter the data in different ways.
- **Correlation analysis**
  When an event happens, it is likely to be reflected in logs from several different sources. Correlation analysis is the analytical process of gathering log information from a variety of systems and discovering the log entries from each system that connects to the known event.

How to perform log analysis

- Logs provide visibility into the health and performance of an application and infrastructure stack, enabling developer teams and system administrators to easily diagnose and rectify issues. Here's our basic five-step process for managing logs with log analysis software:

1. **Instrument and collect** - install a collector to collect data from any part of your stack. Log files may be streamed to a log collector through an active network, or they may be stored in files for later review.
2. **Centralize and index** - integrate data from all log sources into a centralized platform to streamline the search and analysis process. Indexing makes logs searchable, so security and IT personnel can quickly find the information they need.
3. **Search and analyze** - Analysis techniques such as pattern recognition, normalization, tagging, and correlation analysis can be implemented either manually or using native machine learning.
4. **Monitor and alert** - With machine learning and analytics, IT organizations can implement real-time, automated log monitoring that generates alerts when certain conditions are met. Automation can enable the continuous monitoring of large volumes of logs that cover a variety of systems and applications.
5. **Report and dashboard** - Streamlined reports and dashboarding are key features of log analysis software. Customized reusable dashboards can also be used to ensure that access to confidential security logs and metrics is provided to employees on a need-to-know basis.

Log analysis in cyber security

- Organizations that wish to enhance their capabilities in cyber security must develop capabilities in log analysis that can help them actively identify and respond to cyber threats. Organizations that effectively monitor their cyber security with log analysis can make their network assets more difficult to attack. Cyber security monitoring can also reduce the frequency and severity of cyber-attacks, promote earlier response to threats and help organizations meet compliance requirements for cyber security, including:
- The first step to an effective cyber security monitoring program is to identify business applications and technical infrastructure where event logging should be enabled. Use this list as a starting point for determining what types of logs your organization should be monitoring:
- System logs
    - System activity logs
    - Endpoint logs
    - Application logs
    - Authentication logs
    - Physical security logs
- Networking logs
    - Email logs
    - Firewall logs
    - VPN logs
    - Netflow logs
- Technical logs
    - HTTP proxy logs
    - DNS, DHCP and FTP logs
    - AppFlow logs
    - Web and SQL server logs
- Cyber security monitoring logs
    - Malware protection software logs
    - Network intrusion detection system (NIDS) logs
    - Network intrusion prevention system (NIPS) logs
    - Data loss protection (DLP) logs

Centralized log collection & analysis

- Log events are generated all the time in any application built with visibility and observability in mind. As end users utilize the application, they are creating log events that need to be captured and evaluated for the DevOps team to understand how their application is being used and the
- In addition, it's important to know that the analysis of log events isn't just useful for responding to incidents that are detrimental to the health of the application. It can also help organizations keep tabs on how customers are interacting with their applications. For example, you can track which sources refer to the most users and which browsers and devices are used most frequently. This information can help organizations fine-tune their applications to help provide end users with the greatest value and user experience moving forward. It is much easier to gather this information when log data is contextualized through centralized log collections and intuitive visualizations – and the easiest way to do this is to use log analysis tools such as the one provided by Sumo Logic.

Key metrics (MTTD & MTTR)

- While there are dozens of metrics available to determine success, here are two key cybersecurity performance indicators every organization should monitor MTTD & MTTR.

What is MTTD and MTTR?

- The two measurements and their role in the cyber security industry:
  - Mean Time to Detect (MTTD): Your MTTD is the average time it takes to discover a security threat or incident.
  - Mean Time to Respond (MTTR): Your MTTR measures the average time it takes to control and remediate a threat.
- Your MTTD and MTTR depend on a number of factors, including the size and complexity of your network, the size and expertise of your IT staff, your industry, and more. And different companies measure things in different ways. There are no industry-standard approaches to measuring MTTD and MTTR, so granular comparisons between organizations can be problematic apples-vs-oranges affairs.

Why is it important to measure your security operations effectiveness?

- As they say, what gets measured gets managed, which is why security teams are very well aware that MTTD and MTTR are some of the most important metrics to follow.
- Measuring the effectiveness of your security operations will help you focus your efforts on areas where improvements will provide the highest gains.
- Last but not least, displaying your progress can help you prove the value of your program to your board.
- Best strategies to drive down your MTTD and MTTR
- Reducing MTTD and MTTR is the primary goal of a resilient security operations program, which starts with applying a series of techniques, including:

• Understanding cyber attacks

- TTPs is an acronym that everyone in the industry should be familiar with – tactics, techniques and procedures – but not everyone understands how they aid counterintelligence and cyber security operations. TTPs define how threat actors orchestrate and manage attacks. Knowing these patterns and behaviours allows Analysts to strengthen alerting, identify additional vectors of attack, and provide invaluable support to the investigative process by understanding likely compromised hosts, contextualising events and aiding in the identification of appropriate mitigation processes.

• Optimising your incident response plan

- The key to success in a cyber security incident extends beyond the tools you leverage in your environment. Having a solid IR plan will ensure your business is prepared to respond in the event of an incident. Go beyond the implementation of policy and identify your most sensitive assets, define which critical security events your teams should focus on and get buy-in from management to ensure you are prepared for security breaches.

- Implementation of policy and identify your most sensitive assets, define which critical security events your teams should focus on and get buy-in from management to ensure you are prepared for security breaches.

• Know normal

- Taking the time to understand what is normal will make the abnormal stick out. This will enable Analysts to catch changes in network and endpoint activity that could indicate a security breach. It has the added benefit of allowing Analysts to fine-tune technologies and decrease alert fatigue.

• Streamlining decision making

- Security Orchestration, Automation and Response (SOAR) tools allow security teams to connect disparate systems into one centralised point of authority. This enables security teams to make faster and more efficient decisions. SOAR can be used to escalate alerts, provide additional context and notify the right people and tools to neutralise and remediate incidents.

• Use machine learning to enhance threat hunting

- Develop a comprehensive methodology to simulate threat actor activity within your environment. Test these hypotheses against collected data and leverage technology to automate those searches.

• Conducting regular Offensive Security assessments

- From vulnerability scanning to Penetration Testing, these tests are designed to simulate threat actors breaching an environment. Frequent testing results in a stronger security posture, as Incident Response plans and technologies are further refined and improved.

• Performing regular Security Awareness Training (SAT and Phishing Campaigns)

- People are frequently the weakest security link and the biggest factor in driving down your MTTD and MTTR. Security Awareness Training can never be a "one and done", to be successful it needs to be an ongoing process.

- For any organization to protect itself from cyberattacks and data breaches, it's critical to discover and respond to cyber threats as quickly as possible.
- According to the SANS 2019 Incident Response survey, 52.6% of organizations had an MTTD of less than 24 hours, while 81.4% had an MTTD of 30 days or less.
- Once an incident is detected, 67% of organizations report an MTTR of less than 24 hours, with that number increasing to 95.8% when measuring an MTTR of less than 30 days. However, according to the Verizon Data Breach Investigations Report, 56% of breaches took months or longer to discover at all. That's an incredible amount of time for the bad guys to be inside of your perimeter while preparing to exfiltrate your data.

How to Improve MTTD and MTTR

- Measuring and improving MTTD and MTTR is easier said than done. The fact is that many businesses work with IT teams that are stretched thin and often lack cybersecurity expertise. Meanwhile, they face ever-more

sophisticated attacks stemming from well-funded criminal networks or malicious nation-state actors. That said, there are a number of things every organization can do to drive down its MTTD and MTTR.

Start with a plan: Create an incident response plan in advance of potential attacks to identify and define stakeholder responsibilities so the entire team knows what to do when an attack occurs. This plan can define your processes and services used to detect these threats. As you get a few incidents under your belt, review your plan to look for areas for improvement that can reduce MTTD and MTTR.

Conduct regular cybersecurity training: Cybersecurity isn't simply an IT issue—people are frequently the weakest link. Employees may facilitate a compromise by clicking malicious emails or links that install ransomware, viruses, and other malware. In addition, non-technical company leaders may not grasp the risk of cyberattacks, which keeps them from providing sufficient budget and resources IT needs to be effective. The more educated the entire company becomes about cybersecurity, the more prepared it will be to both prevent and respond to attacks. To be effective, education is an ongoing process rather than "one and done."

Level up to Reduce MTTD and MTTR

A security operations center (SOC) such as the Arctic Wolf SOC-as-a-service can extend the capabilities of your IT team by providing 24/7, real-time monitoring of your on-premise and cloud resources. This will help you see if, when, and where an attack occurs, vastly reducing your MTTD. Meanwhile, Arctic Wolf's Concierge Security™ Team can help reduce MTTR by providing expert advice to help navigate incident response.

Data protection in the cloud

Data In Transit vs. Data At Rest

Definition of Data In Transit vs. Data At Rest

- Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. Data protection in transit is the protection of this data while it's traveling from network to network or being transferred from a local storage device to a cloud storage device – wherever data is moving, effective data protection measures for in transit data are critical as data is often considered less secure while in motion.
- Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data at rest is sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion. The risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state.
- Protecting sensitive data both in transit and at rest is imperative for modern enterprises as attackers find increasingly innovative ways to compromise systems and steal data.

The Role of Encryption In Data Protection In Transit and At Rest

- Data can be exposed to risks both in transit and at rest and requires protection in both states. As such, there are multiple different approaches to protecting data in transit and at rest. Encryption plays a major role in data protection and is a popular tool for securing data both in transit and at rest. For protecting data in transit, enterprises often choose to encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc) to protect the contents of data in transit. For protecting data at rest, enterprises can simply encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself.

Best Practices for Data Protection In Transit and At Rest

Unprotected data, whether in transit or at rest, leaves enterprises vulnerable to attack, but there are effective security measures that offer robust data protection across endpoints and networks to protect data in both states. As mentioned above, one of the most effective data protection methods for both data in transit and data at rest is data encryption.

In addition to encryption, best practices for robust data protection for data in transit and data at rest include:

- Implement robust network security controls to help protect data in transit. Network security solutions like firewalls and network access control will help secure the networks used to transmit data against malware attacks or intrusions.
- Don't rely on reactive security to protect your valuable company data. Instead, use proactive security measures that identify at-risk data and implement effective data protection for data in transit and at rest.
- Choose data protection solutions with policies that enable user prompting, blocking, or automatic encryption for sensitive data in transit, such as when files are attached to an email message or moved to cloud storage, removable drives, or transferred elsewhere.
- Create policies for systematically categorizing and classifying all company data, no matter where it resides, in order to ensure that the appropriate data protection measures are applied while data remains at rest and triggered when data classified as at-risk is accessed, used, or transferred.

Finally, if you utilize a public, private, or hybrid cloud provider for storing data or applications, carefully evaluate cloud vendors based on the security measures they offer – but don't rely on the cloud service to secure your data. Who has access to your data, how is it encrypted, and how often your data is backed up are all imperative questions to ask.

While data in transit and data at rest may have slightly different risk profiles, the inherent risk hinges primarily on the sensitivity and value of your data; attackers will attempt to gain access to valuable data whether it's in motion, at rest, or actively in use, depending on which state is easiest to breach. That's why a proactive approach including classifying and categorizing data coupled with content, user, and context-aware security protocols is the safest and most effective way to protect your most sensitive data in every state.

Frequently Asked Questions

What is the difference between data at rest and data in transit?

- The difference between data at rest and data in transit is simply whether the data is currently stationary or moving to a new location. Data at rest is safely stored on an internal or external storage device.
- Data in transit, also known as data in motion, is data that is being transferred between locations over a private network or the Internet. The data is vulnerable while it is being transmitted. Data can be intercepted and compromised as it travels across the network where it is out of a user's direct control. For this reason, data should be encrypted when in transit. Encryption makes the data unreadable if it falls into the hands of unauthorized users.

What is an example of data in transit?

- An example of data in transit is information transferred between a remote user's mobile device and a cloud-based application. If the data is transmitted in plaintext and not encrypted, it can be compromised by malicious actors. Valuable or sensitive in-transit data should always be encrypted.

Is data encrypted in transit and at rest?

- Data may or may not be encrypted when it is in transit and at rest. Encryption is not a native characteristic of data in either an in-transit or at-rest state. Encryption protects data from unauthorized use and can be implemented on data in transit or at rest. Affording valuable data extra protection through encryption is always a good idea, whether it's at rest or in transit. It is critically important to encrypt sensitive data in transit when it is potentially exposed to unknown entities.

What are some data at rest examples?

Data at rest is information that is currently not moving between two points and is safely stored on a computer or device. As soon as a user attempts to transfer any of these items over the network, they become data in transit. Examples of data at rest include:

- Spreadsheet files stored on your laptop's hard drive
- Videos stored on your iPhone or Android device
- Employment records stored in corporate HR applications
- Sales information that is stored in company databases

Cloud data storage - AWS EBS, S3 / Azure SAS

- Cloud data storage - AWS EBS, S3 / Azure SAS
- **Cloud data storage - AWS EBS**
- Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
- You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage.
- Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.
- Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances.
- Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use block storage.
- Amazon EBS volumes are placed in a specific Availability Zone where they are automatically replicated to protect you from the failure of a single component.
- All EBS volume types offer durable snapshot capabilities and are designed for 99.999% availability.

- Amazon EBS provides a range of options that allow you to optimize storage performance and cost for your workload.
- These options are divided into two major categories:
- **SSD-backed storage for transactional workloads**, such as databases and boot volumes (performance depends primarily on IOPS).
- **HDD-backed storage for throughput intensive workloads**, such as MapReduce and log processing (performance depends primarily on MB/s).
- We recommend Amazon EBS for data that must be quickly accessible and requires long-term persistence.
- **Cloud data storage - AWS S3**

- Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance.
- Customers of all sizes and industries can store and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps. With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements.

Azure SAS

Azure shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:

- What resources the client may access.
- What permissions they have to those resources.
- How long the SAS is valid.

Types of shared access signatures

Azure Storage supports three types of shared access signatures:

- User delegation SAS
- Service SAS
- Account SAS

User delegation SAS

A user delegation SAS is secured with Azure Active Directory (Azure AD) credentials and also by the permissions specified for the SAS. A user delegation SAS applies to Blob storage only.

For more information about the user delegation SAS, see Create a user delegation SAS (REST API).

Service SAS

A service SAS is secured with the storage account key. A service SAS delegates access to a resource in only one of the Azure Storage services: Blob storage, Queue storage, Table storage, or Azure Files.

For more information about the service SAS, see Create a service SAS (REST API).

Account SAS

An account SAS is secured with the storage account key. An account SAS delegates access to resources in one or more of the storage services. All of the operations available via a service or user delegation SAS are also available via an account SAS.

You can also delegate access to the following:

- Service-level operations (For example, the **Get/Set Service Properties** and **Get Service Stats** operations).

- Read, write, and delete operations that aren't permitted with a service SAS.

A shared access signature can take one of the following two forms:

- **Ad hoc SAS**. When you create an ad hoc SAS, the start time, expiry time, and permissions are specified in the SAS URI. Any type of SAS can be an ad hoc SAS.

- **Service SAS with stored access policy**. A stored access policy is defined on a resource container, which can be a blob container, table, queue, or file share. The stored access policy can be used to manage constraints for one or more service shared access signatures. When you associate a service SAS with a stored access policy, the SAS inherits the constraints—the start time, expiry time, and permissions—defined for the stored access policy.

How a shared access signature works

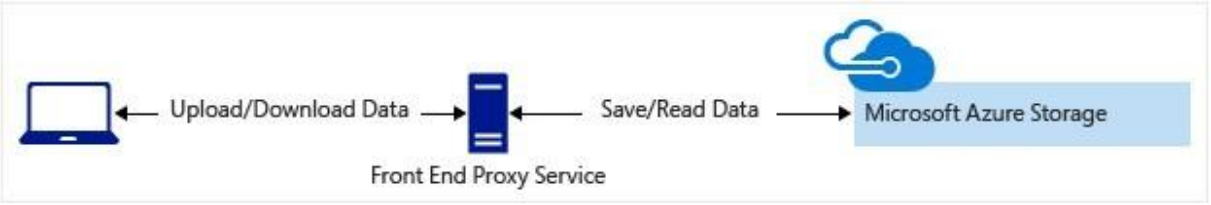
- A shared access signature is a signed URI that points to one or more storage resources. The URI includes a token that contains a special set of query parameters. The token indicates how the resources may be accessed by the client. One of the query parameters, the signature, is constructed from the SAS parameters and signed with the key that was used to create the SAS. This signature is used by Azure Storage to authorize access to the storage resource.
- **Note**
- It's not possible to audit the generation of SAS tokens. Any user that has privileges to generate a SAS token, either by using the account key, or via an Azure role assignment, can do so without the knowledge of the owner of the storage account. Be careful to restrict permissions that allow users to generate SAS tokens. To prevent users from generating a SAS that is signed with the account key for blob and queue workloads, you can disallow Shared Key access to the storage account. For more information, see Prevent authorization with Shared Key.
- **SAS signature and authorization**
- You can sign a SAS token with a user delegation key or with a storage account key (Shared Key).
- ***Signing a SAS token with a user delegation key***
- You can sign a SAS token by using a *user delegation key* that was created using Azure Active Directory (Azure AD) credentials. A user delegation SAS is signed with the user delegation key.
- To get the key, and then create the SAS, an Azure AD security principal must be assigned an Azure role that includes the Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey action. For more information, see Create a user delegation SAS (REST API).

When to use a shared access signature

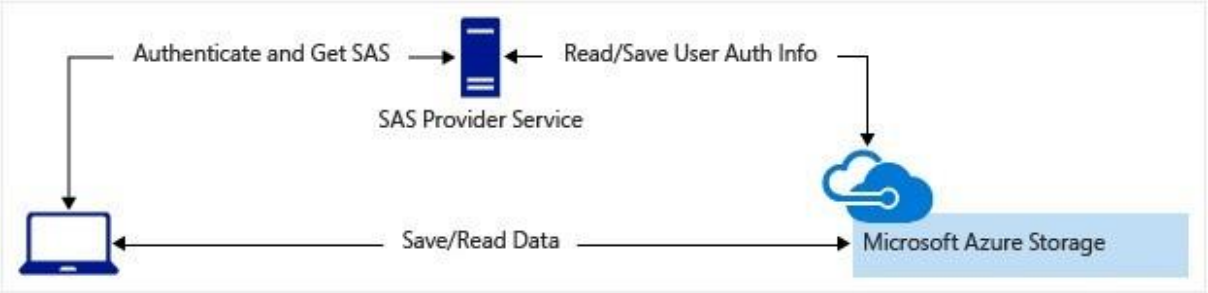
Use a SAS to give secure access to resources in your storage account to any client who does not otherwise have permissions to those resources.

A common scenario where a SAS is useful is a service where users read and write their own data to your storage account. In a scenario where a storage account stores user data, there are two typical design patterns:

1. Clients upload and download data via a front-end proxy service, which performs authentication. This front-end proxy service allows the validation of business rules. But for large amounts of data, or high-volume transactions, creating a service that can scale to match demand may be expensive or difficult.



2. A lightweight service authenticates the client as needed and then generates a SAS. Once the client application receives the SAS, it can access storage account resources directly. Access permissions are defined by the SAS and for the interval allowed by the SAS. The SAS mitigates the need for routing all data through the front-end proxy service.



Many real-world services may use a hybrid of these two approaches. For example, some data might be processed and validated via the front-end proxy. Other data is saved and/or read directly using SAS.

Additionally, a SAS is required to authorize access to the source object in a copy operation in certain scenarios:

- When you copy a blob to another blob that resides in a different storage account.
  You can optionally use a SAS to authorize access to the destination blob as well.
- When you copy a file to another file that resides in a different storage account.
  You can optionally use a SAS to authorize access to the destination file as well.
- When you copy a blob to a file, or a file to a blob.
  You must use a SAS even if the source and destination objects reside within the same storage account.

Secrets Management

Why Secrets Management is Important

Passwords and keys are some of the most broadly used and important tools your organization has for authenticating applications and users and providing them with access to sensitive systems, services, and information. Because secrets have to be transmitted securely, secrets management must account for and mitigate the risks to these secrets, both in transit and at rest.

Secrets can include:

- User or auto-generated passwords
- API and other application keys/credentials (including within containers)
- SSH Keys
- Database and other system-to-system passwords.
- Private certificates for secure communication, transmitting and receiving of data (TLS, SSL etc.)
- Private encryption keys for systems like PGP
- RSA and other one-time password devices

Challenges to Secrets Management

As the IT ecosystem increases in complexity and the number and diversity of secrets explodes, it becomes increasingly difficult to securely store, transmit, and audit secrets.

Common risks to secrets and some considerations include:

- Incomplete visibility and awareness:
- Hardcoded/embedded credentials
- Privileged credentials and the cloud
- DevOps tools
- Third-party vendor accounts/remote access solutions
- Manual secrets management processes
- Best Practices & Solutions for Secrets Management