**SDLC Cycle:**

**Maintenance:**

**1. Dangers to each of the six different levels of security:**

-Physical: destruction of the system or unauthorized access to the system

-In the network: unauthorized access to data and attempts to disrupt service

-Application: code flaws, authentication bypasses, and other vulnerabilities

unauthorized access to the file's data or modification of the file's contents User: passwords that are simple or easily guessed social engineering

-Procedural: Insufficient security training for users and a lack of appropriate procedures for managing the system

**2. Backup method:**

We recommend combining backups that are kept locally and in the cloud. To create local backups, we can make use of an external drive or a NAS (networking attached storage) device. When it comes to cloud backups, I recommend making use of either Amazon Web Services or Google Compute Engine.

Redundancy is achieved by utilizing a combination of different backup strategies, in this case local as well as cloud-based, in the event that one of the backup strategies proves ineffective. In the event that the external hard drive that was used for the local backup becomes corrupted, for instance, the cloud-based backup can be utilized to successfully restore the data. In a similar vein, the local backup can be utilized in the event that the cloud-based backup service is unavailable.

**3. Maintenance plan**:

**In-house:**

The product can be modified to suit the requirements of the company, which is a definite plus.

-The staff in information technology is already familiar with the processes and procedures of the company. -There is the potential for greater cost efficiency in the long run.

**Cons:** It is more difficult to scale up or down according to requirements. It requires a larger initial investment.

**-Outsourced:**

**Advantages:** It is possible to be more flexible and scalable.

It is not necessary to make a large investment right away, and it may be cheaper in the long run.

**Cons:** It's possible that it won't be able to be adapted to the particular requirements of the company.

It's possible that the IT staff isn't familiar with the company's procedures and systems. This could end up being more expensive in the long run.

**Security risks:**

**1. Dangers to each of the six different levels of security:**

-Physical: destruction of the system or unauthorized access to the system

-In the network: unauthorized access to data and attempts to disrupt service

-Application: code flaws, authentication bypasses, and other vulnerabilities

unauthorized access to the file's data or modification of the file's contents User: passwords that are simple or easily guessed social engineering

-Procedural: insufficient security training for users and a lack of appropriate procedures for managing the system

**2. For the method of backup, We recommend using a combination of local and cloud storage:**

To create local backups, we can make use of an external drive or a NAS (networking attached storage) device. When it comes to cloud backups, We recommend making use of either Amazon Web Services or Google Compute Engine.

Redundancy is achieved by utilizing a combination of different backup strategies, in this case local as well as cloud-based, in the event that one of the backup strategies proves ineffective. In the event that the external hard drive that was used for the local backup becomes corrupted, for instance, the cloud-based backup can be utilized to successfully restore the data. In a similar vein, the local backup can be utilized in the event that the cloud-based backup service is unavailable.

**3. Maintenance plan:**

**In-house:**

**Pros**

-Are able to be adapted to the particular requirements of the organization.

-Members of the IT staff are already familiar with the company's various procedures and systems.

-May end up being less expensive than other options in the long run.

**Cons:**

-Requires a larger up-front investment

- It is more difficult to scale up or down depending on the requirements.

**Outsourcing:**

**Pros:**

-Has the potential to be more adaptable and scalable.

-Does not require a large up-front investment.

-It's possible that the costs will be lower for the Cons.

-Won't necessarily be adapted to meet the precise requirements of the organization.

-There is a possibility that the IT staff is not familiar with the company's various systems and procedures.

-Could end up costing more money in the long run.

**Cost feasibility:**

**Phase 1:** Step one is to identify where our entry points are located. It is imperative that we first and foremost identify the potential entry points into our network that could be exploited by cybercriminals. These are the areas of your network in which we need complete visibility, free of any obstructions.

If determining the location of the access point to our network is Step 1A, then determining what criminals are doing outside of these access points is Step 1B. If we are aware of what is happening outside the confines of our security perimeter, then we will be in a better position to ward off any potential attacks.

For instance, if we notice that a particular IP address is scanning our network for open ports, we can easily eliminate the threat by blocking that IP address and preventing it from entering our network in the first place. This will prevent the threat from occurring in the first place.

**Phase 2:** We would characterize the normal flow of traffic.

If we are not familiar with the normal behavior of traffic on our network, it will be impossible for us to identify the characteristics of traffic that point to an imminent attack because we will not be able to differentiate between normal behavior and suspicious behavior.

Think about how fundamentally important this vision is in light of the collaborative relationship we share with the person who oversees our medical care. Our doctor will not approach our care in the same way that he or she treats his or her other patients. Instead, he or she will customize his or her approach to best meet our needs. After all, the way in which our body functions and reacts is not going to be identical to that of the person who is seated next to us in the waiting room. With the assistance of our medical history and baseline vitals, our physician will be better able to make decisions that are in your best interest.

In the same vein, we should never stop monitoring the traffic on our network in order to determine what kinds of activities are typical and what kinds of activities are not typical. Establish a benchmark for the average amount of traffic that moves across our network.

**Phase 3:** At this level, we are responsible for ensuring that all of the traffic and data are recorded by utilizing security tools that are immune to hacking. It is absolutely necessary to take the necessary precautions to ensure that none of our devices can be hacked in order to keep the reliability of our network intact. If we want to know exactly what is happening across all layers of our network, which is especially important in relation to the capture of data, we need to have complete network visibility.

In order to conceal data loss and other network security vulnerabilities, hackers are able to gain access to switches and reprogramme their SPAN ports once they have gained access to the switches. Network TAPS, on the other hand, are a physical security device that cannot be broken into or hacked in any way. They cannot have any concessions made to them.

If we had security cameras installed outside of our building and those cameras only worked part of the time or if someone had the ability to block the lenses of those cameras, we probably wouldn't feel very safe even if we had those cameras. As a result we would be okay with putting our visibility at risk both within and outside of our network.

**Phase 4:** The fourth phase teaches us how to make the most of our firewalls.

There are many different types of firewalls that are available on the market today. Some examples of these include application firewalls, web application firewalls, and traditional firewalls.

The installation of firewalls is the essential first step in the process of preventing malicious software such as hackers, viruses, and worms from entering a system. However, we can't count on them to be our only line of defense, so don't rely on them. A firewall is a sensitive device that can be attacked or flooded, and in order for it to do its job correctly, it also needs to have the precise configuration settings put into it. This is because a firewall is a sensitive device that can be attacked or flooded.

**Phase 5:** At this level, our network should be segmented according to the different areas that need to be monitored.

There is no such thing as two networks that are completely identical.

There are many different types of firewalls that are available on the market today. Some examples of these include application firewalls, web application firewalls, and traditional firewalls.

The installation of firewalls is the essential first step in the process of preventing malicious software such as hackers, viruses, and worms from entering a system. However, we can't count on them to be our only line of defense, so don't rely on them. A firewall is a sensitive device that can be attacked or flooded, and in order for it to do its job correctly, it also needs to have the precise configuration settings put into it. This is because a firewall is a sensitive device that can be attacked or flooded. When it comes to the proper way to organize your network, there is no one structure that can accommodate everything that needs to be done. The diagnostic process, in conjunction with the specifications of our network, should be used to determine the approach that will be taken to achieve this goal. First, divide the total area into percentages, and then deploy network TAPS in the areas that fall within those percentages to determine the locations at which visibility is required. For example, the following information pertaining to the traffic can be indicated by our diagnostics:

• Email accounts for 40 percent of all communication.

• Twenty percent of the total is made up of applications for businesses

• 25 percent Video • 10 percent Applications That Don't Fit Any Other Category

Voice over Internet Protocol (VoIP) accounts for 25% of all calls.

• Browsing the Internet: 30%

In this specific setting, it is absolutely necessary for us to maintain visibility over the activity that is taking place on our email server.

If we deploy network TAPS in layers of the network that are essential to its operation and that are located outside of our security perimeter, you will have a greater degree of control over potential problems with the network's security.

**Phase 6:** Innovative Equipment for an Increase in Safety is the Focus.

The following are some examples of implementations that are considered "next level":

Proxy servers; data capture or forensics boxes; intrusion prevention/detection systems; SSL decryption devices; and more.

Even though many businesses have already invested a significant amount of money into purchasing these applications and gadgets, the success of these products is still dependent on first resolving the five levels that came before them. If our network was developed from the ground up with security in mind, you will have a significantly better chance of fending off attacks and the plethora of other security problems that could put your network in jeopardy.

**BEGINNING AT THE BOTTOM AND WORKING UPWARDS:**

When compared to a full backup, this method is both quicker and more cost-effective because it only backs up the files that have been modified since the last time a backup was made of the entire system. A full backup will only copy over the data that has been altered since the last time it was copied over (when the previous backup was made). The creation of incremental backups is a simple and straightforward process. At the P1 point (let's say, at midnight on Tuesday), a backup of files that have been modified or that have been created since the last full backup is performed; at the P2 point (let's say, at midnight on Wednesday), a backup of files that have been modified or that have been created since the last full backup is performed;... at the Pn point (let's say, at midnight on Friday), the cycle is closed, and the next full backup is created. An initial backup point PO is determined by selecting the time at which a full backup was first created (say, Monday midnight).

When compared to other methodologies, this one is a great deal more cost-effective in terms of the utilization of resources and storage space, the amount of time, and the volume of data that is transferred. If, on the other hand, you need to restore data from a backup, the process of doing so will take place in stages, beginning with points Pn-1...P2, P1, and P0 and progressing all the way up to the most recent full backup. P0 is the point at which the most recent full backup was created. This suggests that it is possible to retrieve data up to the point of the most recent complete backup.

Because components of the files that are being updated are backed up, the binary patches method, which was developed by software developers, functions in a manner that is comparable to how it was originally intended. On the other hand, a distinct comparison foundation is utilized here (blocks for the delta methods and bits of information for this one).

However, one thing that should be kept in mind is that neither of these methods is used on its own; rather, they are utilized in conjunction with either a differential or an incremental backup. This is the case because neither method can create a full backup without the other.

When it is used for RAID1 at the hardware level or when it is used to build a mirror, the technology of mirroring is sometimes referred to as a backup option. This is because both of these applications involve mirroring in some way. It is merely a copy of the files, and any modified files that have accumulated over a given period of time are not saved or organized in any way.