UNIT V

SECURITY ASSESSMENT

In today's world, everyone is going digital because they want to keep up with society and technology. Even small shop vendors are now keeping online payment, and small-scale businesses too are going digital. During lockdown there were cases of data breach in different organizations which caused them heavy losses.

Now, this breach happens because criminals, famously known as the black hat hackers break into computer networks with malicious intentions and release malware that destroys files, steal passwords, and other crucial details of the organizations. This is when Cyber Security Monitoring comes into the picture. This monitoring detects threats and data breaches before it gets escalated to serious security issues.

What is Cyber Security Monitoring?

Cyber Security Monitoring is automation process of continuously observing the behavior on an organization’s network or we can say keeping an eye on the traffic of an organization’s network which are intended to harm its data (data breach) and making cyber threats, if this happens it will send the alert to the security incident and event management (SIEM) system. We will talk about SIEM in more detail further.

Why Security Monitoring is Important?

Today just using cybersecurity tools are not efficient or effective like they were in the previous time. Now you have to take some advance tactics or steps to keep the organization safe from attacks and data breaches. Previously when any data breach occurs then an organization have to bear loss.Nowadays, even if the organization’s website or application is not available to users (showing some server-side error) the organization has to bear the loss because it hurts its reputation. The main importance of security monitoring is to preserve the following aspects:

- Reputation
- Privacy of User Data
- Availability
- Misuse of Organization Service

There are many methods used by an attacker to make the website or application unavailable to the user by using method like DDoS attacks, injecting malicious code or commands, etc.

- **DDoS**

DDos stands for Distributed Denial of Service. In this attack, an attacker sent large number of packets or we can say a request which is made continuously until an error of 5xx (range from 500-599 stands for server-side error) occurs which also results in unavailability of resources provided by the organization.

- **Injecting Malicious Code or Command**

When an attacker is injecting malicious code or command on different input field or URL endpoint then it can harm the privacy of user's data. By identifying these kinds of commands or code and block them is suggested.So, to prevent these types of malicious attack security monitoring is configured and done to prevent, block or reject these types of requests.

How does Cyber Security Threat Monitoring Work?

Cyber Security Threat Monitoring gives us the ability of real-time spectating on the network and helps us to identify unusual or malicious behavior on the network. This will help the cyber security or IT team to take prevention steps before the occurrence of the attack incident.

The unknown packet which comes into the organization's network, by the help of the security protocols it will be stored in the company's database so that the professionals can analyze the packet and if it is harmful, they will triage it and will take actions accordingly and send the alert to the IT team. For a better understanding, consider two main types of monitoring:

- Endpoint Monitoring
- Network Monitoring

1. Endpoint Monitoring

Endpoints are the devices connected to a network like laptops, desktop, smartphones, cell-phones and IOT (Internet of Things) devices.

Endpoint monitoring consist of analyzing the behavior of the devices connected to a specific network and analyze their behavior. It will help IT team to detect threat and they can take prevention measures when the behavior malicious, unusual or suspicious.

2. Network Monitoring

Network is the connection between different devices to communicate and share information

and assets.

Network Monitoring entails keeping an eye (tracking) and analyzing the network from which it will respond on the basis of the result network monitoring gets during monitoring. If the network components are not properly working means like component being overloaded, keeps crashing, slow etc. all that can lead to certain cyber threats and makes the system vulnerable.

There are many diagnostic tools which will keep diagnosing the components and keeps the logs of the result and if there is any disturbance or threat it will automatically notify the IT team instantly via many medium. From this the IT team can fix the error or problem.

Importance of Cybersecurity Monitoring

As I already mentioned the pandemic gives a vast or rapid increase in the cyber-attacks. So, to prevent the organization from these kinds of cyber-attacks the organization have to monitor the network and packets which are being thrown toward the network and prevent any casualty from happening.

1. Minimize Data Breach

Continuously monitoring of the network will help to detect any threat before the occurrence of the event and the organization can prevent these kinds of attacks from affecting the information that the company holds of their users and employees. So, doing continuous security monitoring will help effectively.

2. Improve your Time to Respond to Attacks

Most organizations take security measures to prevent cyber threats and attacks, but what if the bad guys somehow successfully attacked the organization, then the organization must be ready to respond to the attack and fix it as soon as it is detected. Because the assets of the organization must be available to its user 24 x 7.

3. Address Security Vulnerability

Every system has loop holes (vulnerability). Address Security Vulnerability means to address or find the vulnerability the network has. Vulnerability is hunted and fix before any bad guy can find and exploit it. This category also includes keeping all the protocols and firewalls up to date. Even many organizations organize Bug Hunting program.

In bug hunting program the organization invites ethical hackers to ethically hack the system and make a report of the vulnerability so the organization can confirm the vulnerability and fix it, they also provide bounties, swags or hall of fame according to the severity of the vulnerability.

4. Compliance with Standards and Regulations

The most basic and fundamental term of cybersecurity is Confidentiality, Integrity and Availability (CIA Triad). An organization is required to meet these set of rules for the possession of data. If even a single requirement is not met then it will increase the chances of vulnerability existence in the network which will also harm the reputation of the organization. So, by continuous cybersecurity monitoring will help to fix these kinds of problems.

5. Reduce Downtime

Reduce down time means being ensure that organization's network is fully functional and handle all operations Because networks downtime can harm the organization's reputation and even financially. And if organization face any threats they should respond and fix it as soon as possible. So, continuous cybersecurity monitoring will decrease the chances of getting the sever or the network down.

6. Nature of Threats has Changed

Cyber criminals are getting smarter and sharper day by day. They are always trying to get through the defense which any organization sets up for their network. Day by day cyber criminals are bringing up new attack, trick and tactics to perform their malicious activity. Best way to tackle these kinds of problems is by continuously monitoring the network.

7. Rise in Remote Work

Because of the pandemic everybody starts doing work from home (WFH). For that company had started using cloud services to provide the essentials to their employees. But this causes a problem that is to do the access control so that an unauthorized person cannot get access to the data even if he tries.

But then also this can lead to unauthorized access because there is always a way. So, it's a good move to monitor the traffic and detect the threat or any unauthorized user trying to access should be blacklisted or blocked.

8. Increase Productivity of the Employee

Employee plays an important role in any organization. Making the employee productive, that is the thing every organization wants. Focusing on the IT infrastructure will boost the productivity of the employee, because well-structured and secured network will help employees to focus on their core skills and job even can do their work faster.

This can be done by keeping a security expert who will handle all the technical responsibilities will be great. So, this will boost the productivity of all the employees.

Security Monitoring Tools

IT team cannot be available for 24 x 7 to keep an eye on the traffic so that's why automation monitoring tools are used which will directly sends the alert to IT team if any unusual activity or threat is monitored. There are even some tools which will automatically perform certain steps if the programmed condition is met. There are many tools that are used for security monitoring tools, some are as follows

1. ARGUS (Audit Record Generation and Utilization System)

ARGUS stands for Audit Record Generation and Utilization System. It is one of the best open-source network monitoring tools available online. It is used to analyze the traffic of the network. It is one of the most efficient tools available. It does in-depth analysis of the traffic.

2. Nagios

Nagios is used to monitor hosts, networks and system and send alerts accordingly if any unusual behavior occurs. The user has the choice to setup the message they want to receive for any condition. It monitors most of the services like HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), ICMP (Internet Control Message Protocol) and many more.

3. P0F

It is streamlined and efficient because it generated no additional traffic. It is used to detect the operating system with the hosts it interacts with. Many more tools are also there for the work like this but those tools create name lookups, assorted queries, probes, etc. P0f is best for these kinds of works because it is light, faster but it is not easy to learn for a newbie.

4. Splunk

Splunk is like a multitasking tool because it is for designed for both real time analysis and historical data searches. It has very user-friendly interface. Splunk is a paid app. It also has its free version but with limited features and use. This is worth of penny app. Cybersecurity professionals always recommend this app to the client who has decent budget. Big organizations most of time buys premium plan. It is really fantastic app.

5. OSSEC

OSSEC stand for Open source HIDS Security. HIDS is Host based intrusion detection system. OSSEC is a free and an open-source host-based intrusion detection system. It continuously monitors most of the source devices trying to communicate or access. It performs log analysis, rootkit detection, time-based alerting, etc. The users are very much contributing in the modification, suggestion and all that so that it can be much better. It is available for different platforms like Windows, Linux, macOS, BSD, VMWare ESX, etc.

Effective Steps for Cyber Security Monitoring

An organization should always be careful about the traffic which is going through their network because if it comes out to be a malicious packet then it will cost the organization its reputation and its money. So, precaution is better than cure. An organization should focus on its networks traffic by taking some effective and efficient steps.

1. SIEM Tools and Software Solutions

A Security Information and Event Management platform plays an important role in any organization for cybersecurity monitoring. Security Incident and Event Management is field where software and services are combined security information management and security event management. The work of Security Information and Event Management is to monitor and analyze log data efficiently then combine all the monitoring logs in one place to make the analyzing or further assessment easy. This will help the IT team to revise the logs and fix or even they can be prepared for further possible cyber threats.

Some of the best security information and event management tools are as follows:

A. SolarWinds Security Event Manager

It is one the fast-growing tool in the market Some of its key feature (according to Solar

Winds official website) is as follows

- Centralized log collection and normalization
- Automated threat detection and response
- Built-in file integrity model
- Built-in dashboard and user interface
- Simple and affordable pricing

B. Datadog Security Monitoring

It is a cloud-native monitoring and management system which contains real-time security monitoring and log management. It is a paid tool. But it has awesome features.

Some of the key features are as follows (according to the official website of Datadog):

- Simplify complexity with end-to-end, unified visibility
- Automatic detect security threats and misconfigurations in real time.
- Setup in minutes with 350+ detection rules and 500+ integration.
- Response to threats faster with a low maintenance
- Cost effective SIEM

C. Graylog

It is a log management package which includes a SIEM service extension that is available in both free and paid version and even for cloud option. Graylog comes with pre-configured search templates, virtualization, intuitive alert and correlation customization and investigation workflows. These all features make the work easy.

Some of the key-features are as follows (according to the official website of Graylog):

- Compliance Alerting
- Incident Investigation
- S.O.A.R (Security orchestration, automation and Response) Integration
- Archiving
- Threat Intelligence Feed

2. Trained Experts

All the tools we discussed before will do their work properly but this is not enough. A trained expert is important in the team. The person who understands the infrastructure will be much easier for them because the expert will know where to look and for what to look. But an experienced expert is much means those who have knowledge, understanding and ability to identify the threat and fix it as soon as possible. The expert will also know how to make the system much faster for the response to the attack means improving the speed when a cyber threat occurs.

3. Trained Employees

Trained employees play a vital role as same a trained expert plays in an organization for its security. It is important factor to educate or train the employee or the staff about that how to protect the organization from malicious and abrupt attack the attacker might tries to perform on the organization. A well-trained employee will know the symptoms, effects or precautions that should be taken against some cyber-attacks. They will also understand the importance of cybersecurity in the organization.

4. Managed Services

Managed services are the most important factor because an attacker can exploit the services which are not required. By setting the strong protocols and metric will help in improving security. An organization should use or enable only the required services because it will reduce the risks effectively. Some services can help the organization manage or monitor the services running on their network and system. A small mistake in managing the services can lead to a huge reputation or financial loss of a company.

Challenges in Implementing Continuous Security Monitoring

Implementing Continuous Security Monitoring is the most crucial and important part of cyber security. A Continuous Security Monitoring plan helps in monitoring the behavior of the network so the organization can do security controls in an effective manner.

1. Identifying Critical Assets

Many organizations contain lots of data of their users which are also very important data and by the coming time it will be increasing continuously. The challenge comes here is setting a proper Continuous Security Monitoring (CSM) plan so it can find the critical assets of the organization. Every department of an organization should categorize their department according to the level of criticality like low, medium, high, etc. With all this process it should also be considered how often these assets are been scanned, analyzed and retained.

2. Keep an Eye on Endpoint Activity

Tracking an endpoint is very much important and it’s challenging too. The endpoint is not just limited to PCs. If the stakeholder feels they can add whatever device they want like smartphone, printer and even wearables too. So, the continuous security monitoring system plan of the organization should be as accurate as possible otherwise it can cause lots of

damage to the organization. Using hybrid passive and real-time monitoring with an always-on active scanner will be a very efficient way to keep tracking.

3. Choosing Correct Tools Collection

Identifying that which tools will be best for continuous security monitoring is also a big challenge. Proper tools are required which can take action when there is any casualty or even handle them by themselves by matching some condition programmed by the IT team. So, it is important to choose the correct tools which can be programmed for certain condition, analyze the logs and packets without anyone's interaction, record the log for further analysis, should be able to do real time monitoring.

Attack Detection Through Proper Security Monitoring

The security monitoring plan should be planned in such a manner that the automation tools can identify and can take action to any attack by itself, then it will be considered as proper attack detection through security monitoring. It is also one of the important aspects of security monitoring.

Even if the expert is there the monitoring plan should filter the unusual traffic and display it to the expert. The security monitoring plan should be capable of sending the alerts to the IT team if any unusual activity is spotted. Some of the basic points on which attackers can be detected are as follows:

IP Address

If the server is receiving continuous request of large packet from a single IP address and in very short period of time. Then we can the security monitoring system blocks the request form that IP address for a fixed amount of time (configured by the organization according to their requirement). This will let the server to cool down and simultaneously keep the resources available to other users.

By Same Pattern Packets

If the same pattern of packets is incoming from different IP addresses continuously in a short period of time. Then those packets can be considered malicious and rejected or blocked which is decided by the organization.

Accessing Restricted Files or URL

If any user is trying to access the restricted file which is placed on the server but not intended for the end user then that user will get blocked or rejected.

By Identifying Specific Keywords or Character

Here let's take an example of XSS (Cross Side Scripting). XSS attack is based on scripting language and scripting language used '>' greater than, '<' less than, "()" parentheses, etc. and if user is using these types of symbols in an input field like name, contact no, etc., then we can say that the end user is an attacker.

Security Monitoring Best Practices

Identify Assets and Events which Needed to be Logged and Monitored

The strange events should be logged (recorded) and monitored. It gives two advantages. First is that if any data compromise occurs, the investigation team can find the attacker. Second is, the security team will analyze the event which is recorded to find the vulnerability and fix it.

Establish Active Monitoring, Alerting and Incident Response Plan

So, here all organization cannot put team for blocking for rejecting every single, same type of event which can harm system so to fix this, three steps are followed

Active Monitoring

Active monitoring is continuously monitoring the traffics using a SIEM (Security Information and Event Management) tool. The work of SIEM is to automate the process of monitoring. There are many SIEM tools available in the market which is been used by many organizations like Splunk enterprise security, IBM Security QRadar SIEM, etc.

Incident Response

In incident response, the organization will preconfigure the SIEM tool, that which packet (request) should be accepted, rejected or blocked (blacklist) and it is decided on the basis of the structure or pattern of packet (request). Incident response are also done manually. If any big incident happens then the security professional creates a plan and takes instant decision to overcome the incident, this whole scenario is known as incident response.

Alerting

Alerting is used to send alert notifications to the user or admin whose ID is configured. Basically, alerting is used when certain actions are made like if someone is trying to upload any malicious file, trying to brute force admin panel password, etc.

Define the Need for Log and Monitoring

By using log, security team can improve the security as per the log content. By using monitoring, the best advantage is automation means even if there is no interaction of any security professional monitoring can block, reject or blacklist any request.

Keep Monitoring Plan, Firewall and Protocols Up-to-date

It is extremely essential to keep monitoring plan, firewall and protocols up-to-date because if any attacker gets the version of any service and if it is not at the latest version then the attacker can exploit that service and harm the organization. The update contains the latest bug fixes which makes system more secure.

Conclusion

Cyber security monitoring is the first thing that an organization should setup so their system will be safe. Cyber security monitoring is and will be the most crucial and important part of cyber security field and only cybersecurity security monitoring can be used to prevent most of the attacks.