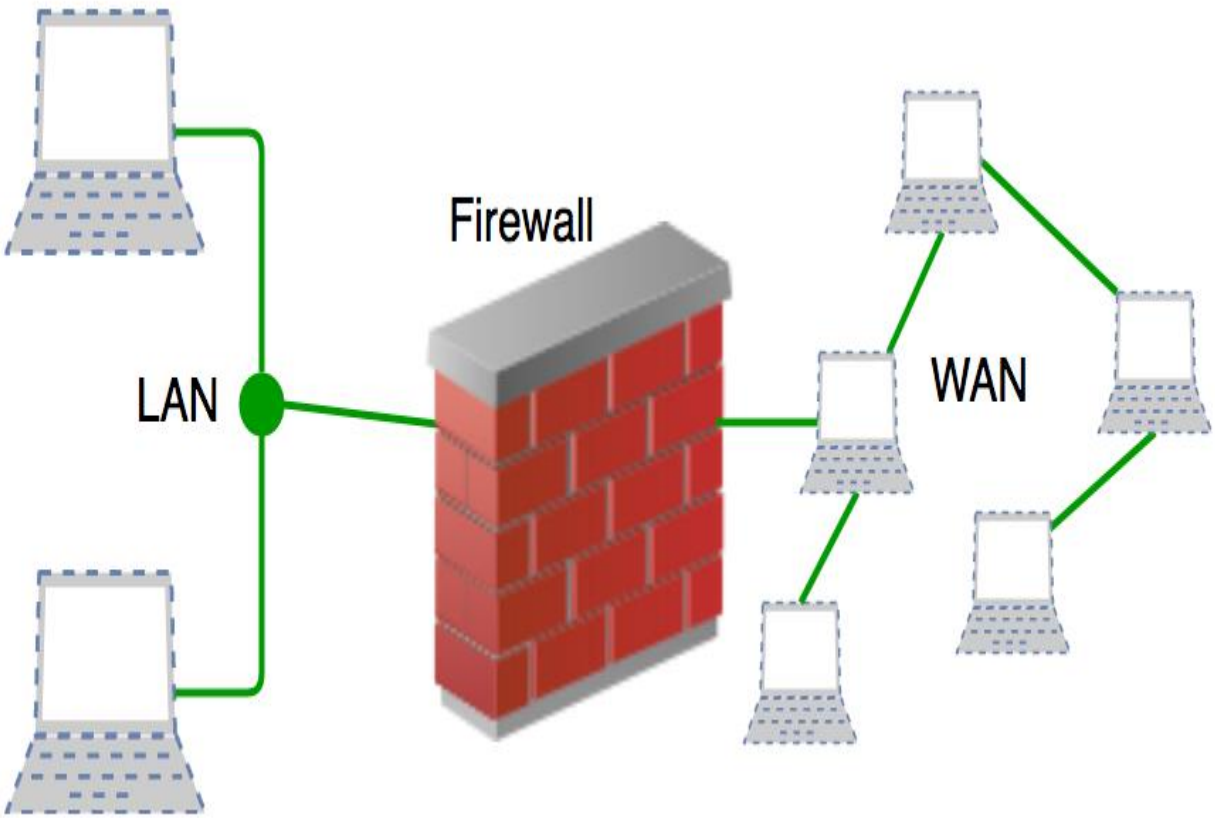
UNIT 5:

Tools & Technologies

Firewalls:-

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic. **Accept :** allow the traffic **Reject :** block the traffic but reply with an "unreachable error" **Drop :** block the traffic with no reply A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced. Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How does Firewall work?

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet. **Default policy:** It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Generation of Firewall

Firewalls can be categorized based on their generation.

1. **First Generation- Packet Filtering Firewall:** Packet filtering firewall is used to control network access by monitoring outgoing and incoming

packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be filtered according to the following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for the internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.
5. **Second Generation- Stateful Inspection Firewall:** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.
6. **Third Generation- Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules. *Note: Application layer firewalls can also be used as Network Address Translator(NAT).*

7. **Next Generation Firewalls (NGFW):** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

What is Magic Firewall?

"Magic Firewall" is a term used to describe a security feature provided by the web hosting and security company Cloudflare. It is a cloud-based firewall that provides protection against a wide range of security threats, including DDoS attacks, SQL injections, cross-site scripting (XSS), and other types of attacks that target web applications.

The Magic Firewall works by analyzing traffic to a website and using a set of predefined rules to identify and block malicious traffic. The rules are based on threat intelligence from a variety of sources, including the company's own threat intelligence network, and can be customized by website owners to meet their specific security needs.

The Magic Firewall is considered "magic" because it is designed to work seamlessly and invisibly to website visitors, without any noticeable impact on website performance. It is also easy to set up and manage, and can be accessed through Cloudflare's web-based control panel.

Overall, the Magic Firewall is a powerful security tool that provides website owners with an additional layer of protection against a variety of security threats.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system.

Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Advantages of using Firewall

1. **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.
2. **Prevention of malware and other threats:** Malware and other threat prevention: Firewalls can be set up to block traffic linked to known malware or other security concerns, assisting in the defense against these kinds of attacks.
3. **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
4. **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity. This information is essential for identifying and looking into security problems and other kinds of shady behavior.
5. **Regulation compliance:** Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.
6. **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Disadvantages of using Firewall

1. **Complexity:** Setting up and keeping up a firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of users and devices.
2. **Limited Visibility:** Firewalls may not be able to identify or stop security risks that operate at other levels, such as the application or endpoint level, because they can only observe and manage traffic at the network level.
3. **False sense of security:** Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.
4. **Limited adaptability:** Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.
5. **Performance impact:** Network performance can be significantly impacted by firewalls, particularly if they are set up to analyze or manage a lot of traffic.
6. **Limited scalability:** Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.
7. **Limited VPN support:** Some firewalls might not allow complex VPN features like split tunneling, which could restrict the experience of a remote worker.
8. **Cost:** Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

Real-Time Applications of Firewall

1. **Corporate networks:** Many businesses employ firewalls to guard against unwanted access and other security risks on their corporate networks. These firewalls can be set up to only permit authorized users to access particular resources or services and to prevent traffic from particular IP addresses or networks.
2. **Government organizations:** Government organizations frequently employ firewalls to safeguard sensitive data and to adhere to rules like HIPAA or PCI-DSS. They might make use of cutting-edge firewalls like Next-

generation firewalls (NGFW), which can detect and stop intrusions as well as manage access to particular data and apps.

3. **Service providers:** Firewalls are used by service providers to safeguard their networks and the data of their clients, including ISPs, cloud service providers, and hosting firms. They might make use of firewalls that accommodate enormous volumes of traffic and support advanced features such as VPN and load balancing.
4. **Small enterprises:** Small firms may use firewalls to separate their internal networks, restrict access to specific resources or applications, and defend their networks from external threats.
5. **Networks at home:** To guard against unwanted access and other security risks, many home users employ firewalls. A firewall that many routers have built in can be set up to block incoming traffic and restrict access to the network.
6. **Industrial Control Systems (ICS):** Firewalls are used to safeguard industrial control systems against illegal access and cyberattacks in many vital infrastructures, including power plants, water treatment facilities, and transportation systems.

IDS :-

Intrusion Detection Systems and firewalls are both cybersecurity solutions that can be deployed to protect an endpoint or network. However, they differ significantly in their purposes.

An IDS is a passive monitoring device that detects potential threats and generates alerts, enabling security operations center (SOC) analysts or incident responders to investigate and respond to the potential incident. An IDS provides no actual protection to the endpoint or network. A firewall, on the other hand, is designed to act as a protective system. It performs analysis of the metadata of network packets and allows or blocks traffic

based upon predefined rules. This creates a boundary over which certain types of traffic or protocols cannot pass.

Since a firewall is an active protective device, it is more like an Intrusion Prevention System (IPS) than an IDS. An IPS is like an IDS but actively blocks identified threats instead of simply raising an alert. This complements the functionality of a firewall, and many next-generation firewalls (NGFWs) have integrated IDS/IPS functionality. This enables them to both enforce the predefined filtering rules (firewalls) and detect and respond to more sophisticated cyber threats (IDS/IPS). Learn more about the IPS vs IDS debate here.

Selecting an IDS Solution

An IDS is a valuable component of any organization's cybersecurity deployment. A simple firewall provides the foundation for network security, but many advanced threats can slip past it. An IDS adds an additional line of defense, making it more difficult for an attacker to gain access to an organization's network undetected.

When selecting an IDS solution, it is important to carefully consider the deployment scenario. In some cases, an IDS may be the best choice for the job, while, in others, the integrated protection of an IPS may be a better option. Using a NGFW that has built-in IDS/IPS functionality provides an integrated solution, simplifying threat detection and security management.

Check Point has many years of experience in developing IDS and IPS systems that provide a high level of threat detection with very low error rates, enabling SOC analysts and incident responders to easily identify true threats. To see our NGFWs, with integrated IDS/IPS functionality, in action, request a demonstration or simply contact us with any questions. Furthermore, you're welcome to learn about preventing attacks on IoT networks and devices in this webinar.

Antiviras:-

What is an antivirus product? Do I need one?
Detect and prevent malicious software and viruses on your computer or laptop.

An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop.

Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them. Your devices can become infected by inadvertently downloading malware that's in an attachment linked to a dubious email, or hidden on a USB drive, or even by simply visiting a dodgy website.

Once it's on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it completely. For this reason it's important that you always use antivirus software, and keep it up to date to protect your data and devices.

How do antivirus products work?

Antivirus products work by detecting, quarantining and/or deleting malicious code, to prevent malware from causing damage to your device. Modern antivirus products update themselves automatically, to provide protection against the latest viruses and other types of malware.

Which antivirus product should I use?

Antivirus software is often included for free within the operating systems that run Windows and Apple computers. **If you make sure that this built-in antivirus is switched on, you'll instantly be safer**.

New computers often come with a trial version of a separate antivirus product installed (such as McAfee, Norton and Avast). You should note that:

- when the trial version expires, you'll have to pay (or register) to continue using it
- separate antivirus products won't always work alongside the built-in antivirus software and could even stop it from working completely
- with so many products available you may want to carry out your own research to find out which is right for you

---

How do I use my antivirus product?

1. When you first install (or switch on) your antivirus product, run a **full scan** to make sure your computer is free of all known malware.
2. Make sure your antivirus software is set to automatically scan all new files, such as those downloaded from the internet or stored on a USB stick, external hard drive, SD card, or other type of removable media.

3. Make sure your antivirus software is set to receive updates automatically.

We've also created more detailed advice on protecting your PCs and laptops from viruses and other kinds of malicious software.

Do I need antivirus products on my smartphone and tablet?

No, provided that you only install apps and software from official stores such as Google Play and the Apple App Store. You should also set your apps (and the tablet/smartphone itself) to update automatically. For more information, read our blog covering antivirus for mobile phones.

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 analysis tools that are leveraged to collect, parse, and analyze the data written to log files. 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.

Ensuring effective log analysis with log analyzers

Effective log analysis requires the use of modern log analysis concepts, tooling, and practices. The following tactics can increase the effectiveness of an organization's log analysis strategy, simplify the process for incident response, and improve application quality.

Real-time log analysis

Real-time log analysis refers to the process of collecting and aggregating log event information in a manner that is readable by humans, thereby providing insight into an application in *real time*. With the assistance of a log aggregator and analysis software, a DevOps team will have several distinct advantages when their logs are analyzed in this way.

When log analysis is performed in real-time, development teams are alerted to potential problems within their applications at the earliest possible moment. This enables them to be as proactive as possible, thereby limiting the impact that an incident has on the end users. The types of incidents that previously went unreported and undetected by the DevOps team will now have the team's attention in a matter of minutes. This provides the necessary framework for increasing application availability and reliability.

In addition to notifying the development team of application issues nearly instantly, real-time log file analysis provides developers with critical context that enables them to resolve incidents quickly and completely. This limits the amount of downtime experienced by the customer while also adding to the likelihood that the issue will be thoroughly resolved.

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:

- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- PCI DSS V3.1 (Parts 10 and 11)
- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

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

Event logging for all of these systems and applications can generate a high volume of data, with significant expense and resources required to handle logs effectively. Cyber security experts should determine the most important logs for consistent monitoring and leverage automated or software-based log analysis methods to save time and resources.

Log analysis in Linux

The Linux operating system offers several unique features that make it popular among its dedicated user base. In addition to being free to use, thanks to an open-source development model with a large and supportive community, Linux automatically generates and saves log files that make it easy for server administrators to monitor important events that take place on the server, in the kernel, or any of the active services or applications.

Log analysis is a crucial activity for server administrators who value a proactive approach to IT. By tracking and monitoring Linux log files, administrators can keep tabs on server performance, discover errors, detect potential threats to security and privacy issues and even anticipate future problems before they ever occur. Linux keeps four types of logs that system administrators can review and analyze:

- **Application logs** - Linux creates log files that track the behavior of several applications. Application logs contain records of events, errors, warnings, and other messages that come from applications.
- **Event logs** - the purpose of an event log is to record events that take place during the execution of a system. Event logs provide an audit trail, enabling system administrators to understand how the system is behaving and diagnose potential problems.

- **Service logs** - The Linux OS creates a log file called /var/log/daemon.log which tracks important background services that have no graphical output. Logging is especially useful for services that lack a user interface, as there are few other methods for users to check the activities and performance of the service.
- **System logs** - System log files contain events that are logged by the operating system components. This includes things like device changes, events, updates to device drivers and other operations. In Linux, the file /var/log/Syslog contains most of the typical system activity logs. Users can analyze these logs to discover things like non-kernel boot errors, system start-up messages, and application errors.

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 state that it's in.

To illustrate this point, imagine that you have a web app. As users navigate the app, log events are generated with each page request. Request data can provide meaningful insights, but the painstaking and tedious process of combing through massive log files on individual web servers would be too much for human beings to handle productively. Instead, these log events should be consumed by a log analyzer that centralizes all log data for all instances of the application. This enables human beings to digest the log data more efficiently and completely, allowing team members to readily evaluate the overall health of the application at any given time.

Glancing at individual requests on a single web server may not provide much insight into how the application as a whole is performing. But when thousands of requests are aggregated and utilized to create visualizations, you get a much clearer picture for evaluating the state of the application. For example, are a significant number of requests resulting in 404s? Are requests to pages that have historically responded in a reasonable time frame experiencing latency? Centralized log collection and analysis allow you to answer these questions.

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.

Improved root cause analysis

The increased visibility provided by log analyzers allows DevOps folks to get to the root cause of application problems in the shortest time frame possible.

In the context of application troubleshooting, root cause analysis refers to the process of identifying the central cause of an application issue during incident response. When dealing with application issues of any complexity, log files are almost always a focal point. But, as is often the case, raw logs also contain a plethora of information that has no relevance to the issue at hand. This sort of information (or noise) in log files can make it difficult to isolate information related to a particular incident.

In the realm of root cause analysis, log analyzers provide critical tooling designed to empower development and operations personnel to sift through the noise and dig into the relevant data. This includes:

- Alerts notify the correct staff of an issue at the earliest possible moment in time. In addition to leading to a faster resolution simply by starting the process of analysis sooner, alerting often helps incident response personnel connect the dots between the problem and its cause by providing an exact time frame for when the issue surfaced.
- Visualizations represent log entries in a manner that provides context for the data being collected. In the process of root cause analysis, it is not uncommon for an alarming trend to accompany the incident. Visualizations that depict such trends can prove extremely useful in helping staff develop hypotheses that bring them closer to identifying the root cause of the problem.
- Search and filter functionality for centralized log data help reduce the time it takes to isolate instances of a particular incident to begin deciphering its underlying cause.

Log data is big data

The single biggest data set that IT can use for monitoring, planning, and optimization is log data. After all, logs are what the IT infrastructure generates while it is going about its business. Log data is generally the most detailed data available for analyzing the state of the business systems, whether it be for operations, application management, or security. Best of all, the log data is being generated whether it is being collected or not. But to use it, some non-trivial additional infrastructure has to be put in place. And with that still, first-generation log management tools did run into problems scaling to the required amount of data, even before the data explosion we have seen over the last couple of years took off.

Key Management:-

In cryptography, it is a very tedious task to distribute the public and private keys between sender and receiver. If the key is known to the third party (forger/eavesdropper) then the whole security mechanism becomes worthless. So, there comes the need to secure the exchange of keys.

There are two aspects for Key Management:

1. Distribution of public keys.
2. Use of public-key encryption to distribute secrets.

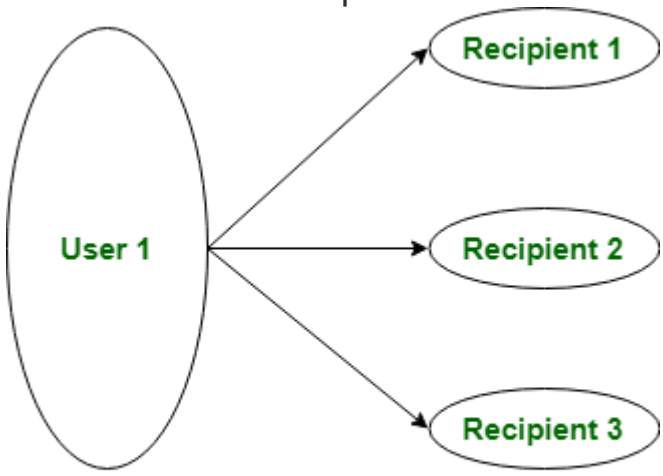
Distribution of Public Key:
The public key can be distributed in four ways:

1. Public announcement
2. Publicly available directory
3. Public-key authority
4. Public-key certificates.

These are explained as following below:

1. Public Announcement: Here the public key is broadcasted to everyone. The major weakness of this method is a forgery. Anyone can

create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.



Public Key Announcement

2. Publicly Available Directory: In this type, the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}. Directories can be accessed electronically still vulnerable to forgery or tampering.
3. Public Key Authority: It is similar to the directory but, improves security by tightening control over the distribution of keys from the directory. It requires users to know the public key for the directory. Whenever the keys are needed, real-time access to the directory is made by the user to obtain any desired public key securely.
4. Public Certification: This time authority provides a certificate (which binds an identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied by some other info such as period of validity, rights of use, etc. All of this content is signed by the private key of the certificate authority and it can be verified by anyone possessing the authority's public key.
First sender and receiver both request CA for a certificate which contains a public key and other information and then they can exchange these certificates and can start communication.

What is Network Infrastructure Security?

Network Infrastructure Security, typically applied to enterprise IT environments, is a process of protecting the underlying networking infrastructure by installing preventative measures to deny unauthorized access, modification, deletion, and theft of resources and data. These security measures can include access control, application security, firewalls, virtual private networks (VPN), behavioral analytics, intrusion prevention systems, and wireless security.

How does Network Infrastructure Security work?

Network Infrastructure Security requires a holistic approach to ongoing processes and practices to ensure that the underlying infrastructure remains protected. The Cybersecurity and Infrastructure Security Agency (CISA) recommends considering several approaches when addressing what methods to implement.

- **Segment and segregate networks and functions -** Particular attention should be paid to the overall infrastructure layout. Proper segmentation

and segregation is an effective security mechanisms to limit potential intruder exploits from propagating into other parts of the internal network. Using hardware such as routers can separate networks creating boundaries that filter broadcast traffic. These micro-segments can then further restrict traffic or even be shut down when attacks are detected. Virtual separation is similar in design as physically separating a network with routers but without the required hardware.

- **Limit unnecessary lateral communications -** Not to be overlooked is the peer-to-peer communications within a network. Unfiltered communication between peers could allow intruders to move about freely from computer to computer. This affords attackers the opportunity to establish persistence in the target network by embedding backdoors or installing applications.
- **Harden network devices -** Hardening network devices is a primary way to enhance network infrastructure security. It is advised to adhere to industry standards and best practices regarding network encryption, available services, securing access, strong passwords, protecting routers, restricting physical access, backing up configurations, and periodically testing security settings.
- **Secure access to infrastructure devices -** Administrative privileges are granted to allow certain trusted users access to resources. To ensure the authenticity of the users by implementing multi-factor authentication (MFA), managing privileged access, and managing administrative credentials.

- **Perform out-of-band (OoB) network management -** OoB management implements dedicated communications paths to manage network devices remotely. This strengthens network security by separating user traffic from management traffic.
- **Validate integrity of hardware and software -** Gray market products threaten IT infrastructure by allowing a vector for an attack into a network. Illegitimate products can be pre-loaded with malicious software waiting to be introduced into an unsuspecting network. Organizations should regularly perform integrity checks on their devices and software.

Why is Network Infrastructure Security important?

The greatest threat to network infrastructure security is from hackers and malicious applications that attack and attempt to gain control over the routing infrastructure. Network infrastructure components include all the devices needed for network communications, including routers, firewalls, switches, servers, load-balancers, intrusion detection systems (IDS), domain name systems (DNS), and storage systems. Each of these systems presents an entry point to hackers who want to place malicious software on target networks.

- **Gateway Risk:** Hackers who gain access to a gateway router can monitor, modify, and deny traffic in and out of the network.

- **Infiltration Risk:** Gaining more control from the internal routing and switching devices, a hacker can monitor, modify, and deny traffic between key hosts inside the network and exploit the trusted relationships between internal hosts to move laterally to other hosts.

Although there is any number of damaging attacks that hackers can inflict on a network, securing and defending the routing infrastructure should be of primary importance in preventing deep system infiltration.

What are the benefits of Network Infrastructure Security?

Network infrastructure security, when implemented well, provides several key benefits to a business's network.

- **Improved resource sharing saves on costs:** Due to protection, resources on the network can be utilized by multiple users without threat, ultimately reducing the cost of operations.
- **Shared site licenses:** Security ensures that site licenses would be cheaper than licensing every machine.
- **File sharing improves productivity:** Users can securely share files across the internal network.
- **Internal communications are secure:** Internal email and chat systems will be protected from prying eyes.

- **Compartmentalization and secure files:** User files and data are now protected from each other, compared with using machines that multiple users share.
- **Data protection:** Data backup to local servers is simple and secure, protecting vital intellectual property.

What are the different types of Network Infrastructure Security?

A variety of approaches to network infrastructure security exist, it is best to adhere to multiple approaches to broaden network defense.

- **Access Control:** The prevention of unauthorized users and devices from accessing the network.
- **Application Security:** Security measures are placed on hardware and software to lock down potential vulnerabilities.
- **Firewalls:** Gatekeeping devices that can allow or prevent specific traffic from entering or leaving the network.
- **Virtual Private Networks (VPN):** VPNs encrypt connections between endpoints creating a secure “tunnel” of communications over the internet.
- **Behavioral Analytics:** These tools automatically detect network activity that deviates from usual activities.

- **Wireless Security:** Wireless networks are less secure than hardwired networks, and with the proliferation of new mobile devices and apps, there are ever-increasing vectors for network infiltration.

****Security Infrastructure: Detail Report****

1. Public Key Infrastructure (PKI):

- PKI is a framework used to manage the creation, distribution, and revocation of digital certificates and encryption keys. It ensures secure communication and authentication in a networked environment.

- Components: Certificate Authority (CA), Registration Authority (RA), Certificate Revocation Lists (CRLs), and end-user devices with public-private key pairs.

- Use Cases: SSL/TLS certificates for secure websites, digital signatures, secure email encryption, VPN authentication.

2. **Virtual Private Network (VPN):**

- A VPN creates a secure encrypted tunnel over an untrusted network (e.g., the internet) to protect data transmitted between remote locations or individuals.

- Types: Site-to-Site VPN for connecting multiple networks, Remote Access VPN for individual users.

- Encryption Protocols: IPSec, SSL/TLS.

- Use Cases: Secure remote access to corporate resources, connecting branch offices securely.

3. **Network Scanners:**

- Network scanners are used to identify vulnerabilities and potential security threats in a network by scanning and analyzing devices, ports, and services.

- Types: Active Scanners (send packets to target systems) and Passive Scanners (listen to network traffic).

- Use Cases: Vulnerability assessments, penetration testing, network inventory management.

4. **Digital Forensics:**

- Digital forensics involves the collection, preservation, analysis, and presentation of digital evidence for legal or investigative purposes.

- Process: Identification, acquisition, examination, analysis, and reporting.

- Tools: EnCase, FTK (Forensic Toolkit), Autopsy, Sleuth Kit.

- Use Cases: Investigating cybercrimes, data breaches, intellectual property theft.

5. **Security Audits:**

- Security audits assess an organization's security policies, controls, and practices to identify weaknesses and ensure compliance with security standards and regulations.

- Types: Internal audits performed by the organization's own team, External audits by third-party security firms.

- Use Cases: Identifying security gaps, evaluating the effectiveness of security measures, regulatory compliance checks.

6. **Asset Classification and Risk Analysis:**

- Asset classification categorizes information and resources based on their importance and sensitivity to prioritize security measures.

- Risk analysis identifies and assesses potential threats and vulnerabilities, determining the likelihood and impact of security incidents.

- Risk Management: Implementing controls and mitigation strategies to reduce risk.

- Use Cases: Identifying critical assets, understanding potential threats and their impact, developing risk treatment plans.

In conclusion, a comprehensive security infrastructure encompasses multiple components such as PKI, VPN, network scanners, digital forensics, security audits, asset classification, and risk analysis. These elements work together to protect an organization's assets, data, and networks from various security threats and ensure the confidentiality, integrity, and availability of critical information. Regular security assessments and risk management practices are vital for maintaining a strong security posture in today's ever-evolving threat landscape.

Audit Trails:-

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. This bulletin focuses on audit trails as a technical control and discusses the benefits and objectives of audit trails, the types of audit trails, and some common implementation issues.

An audit trail is a series of records of computer events, about an operating system, an application, or user activities. A computer system may have several audit trails, each devoted to a particular type of activity. Auditing is a review and analysis of management, operational, and technical controls. The auditor can obtain valuable information about activity on a computer system from the audit trail. Audit trails improve

the auditability of the computer system.

Audit trails may be used as either a support for regular system operations or a kind of insurance policy or as both of these. As insurance, audit trails are maintained but are not used unless needed, such as after a system outage. As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems.

BENEFITS AND OBJECTIVES

Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events (actions that happen on a computer system), intrusion detection, and problem analysis.

Individual Accountability

Audit trails are a technical mechanism that help managers maintain individual accountability. By advising users that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.

For example, audit trails can be used in concert with access controls to identify and provide information about users suspected of improper modification of data (e.g., introducing errors into a database). An audit trail may record "before" and "after" versions of records. (Depending upon the size of the file and the capabilities of the audit logging tools, this may be very resource-intensive.) Comparisons can then be made between the actual changes made to records and what was expected. This can help management determine if errors were made by the user, by the system or application software, or by some other source.

Audit trails work in concert with logical access controls, which restrict use of system resources. Granting users access to particular resources usually means that they need that access to accomplish their job. Authorized access, of course, can be misused, which is where audit trail

analysis is useful. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis is used to examine their actions. For example, consider a personnel office in which users have access to those personnel records for which they are responsible. Audit trails can reveal that an individual is printing far more records than the average user, which could indicate the selling of personal data. Another example may be an engineer who is using a computer for the design of a new product. Audit trail analysis could reveal that an outgoing modem was used extensively by the engineer the week before quitting. This could be used to investigate whether proprietary data files were sent to an unauthorized party.

Reconstruction of Events

Audit trails can also be used to reconstruct events after a problem has occurred. Damage can be more easily assessed by reviewing audit trails of system activity to pinpoint how, when, and why normal operations ceased. Audit trail analysis can often distinguish between operator-induced errors (during which the system may have performed exactly as instructed) or system-created errors (e.g., arising from a poorly tested piece of replacement code). If, for example, a system fails or the integrity of a file (either program or data) is questioned, an analysis of the audit trail can reconstruct the series of steps taken by the system, the users, and the application. Knowledge of the conditions that existed at the time of, for example, a system crash, can be useful in avoiding future outages. Additionally, if a technical problem occurs (e.g., the corruption of a data file) audit trails can aid in the recovery process (e.g., by using the record of changes made to reconstruct the file).

Intrusion Detection

Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access. If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Although normally thought of as a real-time effort, intrusions can be detected in real time, by examining audit records as they are created (or through the use of other kinds of warning flags/notices), or after the fact (e.g., by examining audit records in a batch process).

Real-time intrusion detection is primarily aimed at outsiders attempting to gain unauthorized access to the system. It may also be used to detect changes in the system's performance indicative of, for example, a virus or worm attack (forms of malicious code). There may be difficulties in implementing real-time auditing, including unacceptable system performance.

After-the-fact identification may indicate that unauthorized access was attempted (or was successful). Attention can then be given to damage assessment or reviewing controls that were attacked.

Problem Analysis

Audit trails may also be used as on-line tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring. If a system or application is deemed to be critical to an organization's business or mission, real-time auditing may be implemented to monitor the status of these processes (although, as noted above, there can be difficulties with real-time analysis). An analysis of the audit trails may be able to verify that the system operated normally (i.e., that an error may have resulted from operator error, as opposed to a system-originated error). Such use of audit trails may be complemented by system performance logs. For example, a significant increase in the use of system resources (e.g., disk file space or outgoing modem use) could indicate a security problem.

AUDIT TRAILS AND LOGS

A system can maintain several different audit trails concurrently. There are typically two kinds of audit records, (1) an event-oriented log and (2) a record of every keystroke, often called keystroke monitoring. Event-based logs usually contain records describing system events, application events, or user events.

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result.

Date and time can help determine if the user was a masquerader or the actual person specified.

Keystroke Monitoring

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. Examples of keystroke monitoring would include viewing characters as they are typed by users, reading users' electronic mail, and viewing other recorded information typed by users. (See the CSL Bulletin of March 1993, for guidance on the legality of keystroke monitoring.)

Some forms of routine system maintenance may record user keystrokes. This could constitute keystroke monitoring if the keystrokes are preserved along with the user identification so that an administrator could determine the keystrokes entered by specific users. Keystroke monitoring is conducted in an effort to protect systems and data from intruders who access the systems without authority or in excess of their assigned authority. Monitoring keystrokes typed by intruders can help administrators assess and repair damage caused by intruders.

Audit Events

System audit records are generally used to monitor and fine-tune system performance. Application audit trails may be used to discern flaws in applications, or violations of security policy committed within an application. User audits records are generally used to hold individuals accountable for their actions. An analysis of user audit records may expose a variety of security violations, which might range from simple browsing to attempts to plant Trojan horses or gain unauthorized privileges.

The system itself enforces certain aspects of policy (particularly system-specific policy) such as access to files and access to the system itself. Monitoring the alteration of systems configuration files that implement the policy is important. If special accesses (e.g., security administrator access) have to be used to alter configuration files, the system should generate audit records whenever these accesses are used.

Sometimes a finer level of detail than system audit trails is required. Application audit trails can provide this greater level of recorded detail. If an application is critical, it can be desirable to record not only who invoked the application, but certain details specific to each use. For example, consider an e-mail application. It may be desirable to record who sent mail, as well as to whom they sent mail and the length of messages. Another example would be that of a database application. It may be useful to record who accessed what database as well as the individual rows or columns of a table that were read (or changed or deleted), instead of just recording the execution of the database program.

A user audit trail monitors and logs user activity in a system or application by recording events initiated by the user (e.g., access of a file, record or field, use of a modem).

Flexibility is a critical feature of audit trails. Ideally (from a security point of view), a system administrator would have the ability to monitor all system and user activity, but could choose to log only certain functions at the system level, and within certain applications. The decision of how much to log and how much to review should be a function of application/data sensitivity and should be decided by each functional manager/application owner with guidance from the system administrator and the computer security manager/officer, weighing the costs and benefits of the logging. Audit logging can have privacy implications; users should be aware of applicable privacy laws, regulations, and policies that may apply in such situations.

System-Level Audit Trails

If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke). System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.

Application-Level Audit Trails

System-level audit trails may not be able to track and log events within applications, or may not be able to provide the level of detail needed by application or data owners, the system administrator, or the computer security manager. In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports. Some applications may be sensitive enough from a data availability,
confidentiality, and/or integrity perspective that a "before" and "after" picture of each modified record (or the data element(s) changed within a record) should be captured by the audit trail.

User Audit Trails

User audit trails can usually log:

- all commands directly initiated by the user;
- all identification and authentication attempts; and
- files and resources accessed.

It is most useful if options and parameters are also recorded from commands. It is much more useful to know that a user tried to delete a log file (e.g., to hide unauthorized actions) than to know the user merely issued the delete command, possibly for a personal data file.

IMPLEMENTATION ISSUES

Audit trail data requires protection, since the data should be available for use when needed and is not useful if it is not accurate. Also, the best planned and implemented audit trail is of limited value without timely review of the logged data. Audit trails may be reviewed periodically, as needed (often triggered by occurrence of a security event), automatically in real-time, or in some combination of these. System managers and administrators, with guidance from computer security personnel, should determine how long audit trail data will be maintained -- either on the system or in archive files.

Following are examples of implementation issues that may have to be

addressed when using audit trails.

Protecting Audit Trail Data

Access to on-line audit logs should be strictly controlled. Computer security managers and system administrators or managers should have access for review purposes; however, security and/or administration personnel who maintain logical access functions may have no need for access to audit logs.

It is particularly important to ensure the integrity of audit trail data against modification. One way to do this is to use digital signatures. Another way is to use write-once devices. The audit trail files need to be protected since, for example, intruders may try to "cover their tracks" by modifying audit trail records. Audit trail records should be protected by strong access controls to help prevent unauthorized access. The integrity of audit trail information may be particularly important when legal issues arise, such as when audit trails are used as legal evidence. (This may, for example, require daily printing and signing of the logs.) Questions of such legal issues should be directed to the cognizant legal counsel.

The confidentiality of audit trail information may also be protected, for example, if the audit trail is recording information about users that may be disclosure-sensitive such as transaction data containing personal information (e.g., "before" and "after" records of modification to income tax data). Strong access controls and encryption can be particularly effective in preserving confidentiality.

Review of Audit Trails

Audit trails can be used to review what occurred after an event, for periodic reviews, and for real-time analysis. Reviewers should know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like. Audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.

Audit Trail Review After an Event. Following a known system or application software problem, a known violation of existing requirements by a user, or

some unexplained system or user problem, the appropriate system-level or application-level administrator should review the audit trails. Review by the application/data owner would normally involve a separate report, based upon audit trail data, to determine if their resources are being misused.

Periodic Review of Audit Trail Data. Application owners, data owners, system administrators, data processing function managers, and computer security managers should determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities. This determination should have a direct correlation to the frequency of periodic reviews of audit trail data.

Real-Time Audit Analysis. Traditionally, audit trails are analyzed in a batch mode at regular intervals (e.g., daily). Audit records are archived during that interval for later analysis. Audit analysis tools can also be used in a real-time, or near real-time fashion. Such intrusion detection tools are based on audit reduction, attack signature, and variance techniques. Manual review of audit records in real-time is almost never feasible on large multiuser systems due to the volume of records generated. However, it might be possible to view all records associated with a particular user or application, and view them in real time. (This is similar to keystroke monitoring, though, and may be legally restricted.)

Tools for Audit Trail Analysis

Many types of tools have been developed to help to reduce the amount of information contained in audit records, as well as to distill useful information from the raw data. Especially on larger systems, audit trail software can create very large files, which can be extremely difficult to analyze manually.

The use of automated tools is likely to be the difference between unused audit trail data and a robust program. Some of the types of tools include:

Audit reduction tools are preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. (This alone may cut in half the number of records in the

audit trail.) These tools generally remove records generated by specified classes of events, such as records generated by nightly backups might be removed.

Trends/variance-detection tools look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations. For example, if a user typically logs in at 9 a.m., but appears at 4:30 a.m. one morning, this may indicate a security problem that may need to be investigated.

Attack signature-detection tools look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed log-in attempts.

COST CONSIDERATIONS

Audit trails involve many costs. First, some system overhead is incurred recording the audit trail. Additional system overhead will be incurred storing and processing the records. The more detailed the records, the more overhead is required. Another cost involves human and machine time required to do the analysis. This can be minimized by using tools to perform most of the analysis. Many simple analyzers can be constructed quickly (and cheaply) from system utilities, but they are limited to audit reduction and identifying particularly sensitive events. More complex tools that identify trends or sequences of events are slowly becoming available as off-the-shelf software. (If complex tools are not available for a system, development may be prohibitively expensive. Some intrusion detection systems, for example, have taken years to develop.)

The final cost of audit trails is the cost of investigating anomalous events. If the system is identifying too many events as suspicious, administrators may spend undue time reconstructing events and questioning personnel.

FOR MORE INFORMATION

This bulletin summarizes a chapter in NIST Special Publication 800-12, Introduction to Computer Security: The NIST Handbook. The handbook is available electronically at: http://csrc.nist.gov/nistpubs/800-12 in

WordPerfect 6.1, MS Word, and PostScript formats. You can also order the handbook from the Government Printing Office at (202) 512-1800, stock number SN003-003-03374-0, price $18.00.

Reporting in Security Management: Security Policies, Procedures, and International Standards.

Effective reporting is a crucial aspect of security management, as it enables organizations to communicate and document their security policies, procedures, and adherence to international standards. Let's delve into each of these elements:

1. **Security Policies:**

- Security policies are high-level documents that outline an organization's overall approach to security, providing guidance on protecting critical assets and ensuring compliance with relevant laws and regulations.

- Types of Policies: Acceptable Use Policy (AUP), Information Security Policy, Access Control Policy, Incident Response Policy, etc.

- Content: Policies should clearly define the roles and responsibilities of individuals, acceptable and unacceptable behavior, and consequences for policy violations.

- Reporting Aspect: The policy should specify the reporting mechanisms for security incidents, breaches, and potential vulnerabilities.

2. **Security Procedures:**

- Security procedures are detailed step-by-step instructions that support and implement security policies. They provide guidelines on how specific security tasks should be performed.

- Examples: Incident response procedures, password management procedures, data backup and recovery procedures, etc.

- Reporting Aspect: Procedures should include reporting requirements for different security incidents, the chain of communication, and escalation procedures.

3. **International Standards:**

- International standards provide organizations with best practices and guidelines for information security. Complying with these standards can enhance an organization's security posture and facilitate international business.

- Examples: ISO/IEC 27001 (Information Security Management System), ISO/IEC 27002 (Code of Practice for Information Security Controls), NIST Cybersecurity Framework, GDPR (General Data Protection Regulation), etc.

- Reporting Aspect: Organizations need to document their efforts to adhere to these standards and undergo audits and assessments to demonstrate compliance.

4. **Reporting Mechanisms:**

- Incident Reporting: Establishing clear and accessible channels for reporting security incidents to appropriate personnel or teams, such as a Security Operations Center (SOC) or IT security department.

- Compliance Reporting: Regularly reporting on adherence to security policies, procedures, and international standards to internal stakeholders, management, and external regulatory bodies.

- Metrics and Key Performance Indicators (KPIs): Tracking and reporting on security-related metrics to assess the effectiveness of security measures and identify areas for improvement.

5. **Documentation and Record-Keeping:**

- Maintaining comprehensive documentation of security policies, procedures, compliance efforts, and incident reports is essential for transparency and accountability.

- Incident Records: Recording details of security incidents, including the incident's nature, response actions taken, and lessons learned.

- Audits and Assessments: Documenting audit results, findings, and action plans to address identified gaps.

In summary, reporting plays a pivotal role in security management. It ensures that security policies, procedures, and compliance efforts are effectively communicated, recorded, and reviewed. Reporting also facilitates continuous improvement in an organization's security posture, enabling proactive identification and mitigation of security risks and incidents. Adhering to international standards helps organizations align with best practices and demonstrate their commitment to information security to stakeholders and customers.