Introduction to Cyber Security

UNIT–I:

Introduction to Cyber security- Cyber security objectives**,** Cyber security roles**,** Differences between Information Security & Cyber security, **Cyber security Principles-**Confidentiality, integrity, &availability Authentication & non- repudiation.

Cyber Security Introduction - Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

The term cyber security refers to techniques and practices designed to protect digital data.

The data that is stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

Cyber is related to the technology which contains systems, network and programs or data.

Whereas security related to the protection which includes systems security, network• security and application and information security.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

Cyber attacks can be extremely expensive for businesses to endure.

In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.

Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.

Regulations such as GDPR are forcing organizations into taking better care of the• personal data they hold.

Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack.

But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Fundamental Goals of Cyber Security

The majority of the business operations run on the internet exposing their data and resources to various cyber threats. Since the data and system resources are the pillars upon which the organization operates, it goes without saying that a threat to these entities is indeed a threat to the organization itself.

A threat can be anywhere between a minor bug in a code to a complex cloud hijacking liability. Risk assessment and estimation of the cost of reconstruction help the organization to stay prepared and to look ahead for potential losses.

Thus knowing and formulating the goals of cybersecurity specific to every organization is crucial in protecting the valuable data.

Cybersecurity is a practice formulated for the protection of sensitive information on the internet and on devices safeguarding them from attack, destruction, or unauthorized access.

The goal of cybersecurity is to ensure a risk-free and secure environment for keeping the data, network and devices guarded against cyber threats. Let us learn more about the Goals of cybersecurity.

What are the goals of Cyber Security?

The ultimate goal of cyber security is to protect the information from being stolen or compromised. To achieve this we look at 3 fundamental goals of cyber security.

1. Protecting the Confidentiality of data

2. Preserving the Integrity of data

3. Restricting the Availability of data only to authorized users

Here are few steps to maintain these goals

1. Classifying the assets based on their importance and priority. The most important ones are kept secure at all times.

2. Pinning down potential threats.

3. Determining the method of security guards for each threat

4. Monitoring any breaching activities and managing data at rest and data in motion.

5. Iterative maintenance and responding to any issues involved.

6. Updating policies to handle risk, based on the previous assessments.

All of the above aspects can be fit into 3 significant goals known as the “CIA Triad”. So let us jump right in and get started with the CIA concepts in the below section.

What Are the Different Roles in Cyber Security?

“Organizations are still working hard to accurately define the expectations of cyber security roles and how those roles fit into the bigger organizational picture,” said Backherms.

The specific job responsibilities for any given cyber security role can also depend on the size and resources of the employer. “At a smaller or mid-size firm, you might end up being a ‘jack of all trades,’ while at a larger firm you’re more likely to have specialists,” said Champion.

Cyber security professionals can benefit from starting as generalists and then specializing in an area of interest or strength, according to Champion. These areas can include:

- Application security
- Data loss prevention
- Forensics
- Incident response
- Network security

Security architecture

Threat intelligence

Vulnerability management

Differences between Information Security & Cyber security:

The terms Cyber Security and Information Security are often used interchangeably. As they both are responsible for the security and protecting the computer system from threats and information breaches and often Cyber security and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously. If we talk about data security it's all about securing the data from malicious users and threats. Now another question is what is the difference between Data and Information? So one important point is that "not every data can be information" data can be informed if it is interpreted in a context and given meaning. for example "100798" is data and if we know that it's the date of birth of a person then it is information because it has some meaning. so information means data that has some meaning.

Examples and Inclusion of Cyber Security are as follows:

Network Security

Application Security

Cloud Security

Critical Infrastructure

Examples and inclusion of Information Security are as follows:

Procedural Controls

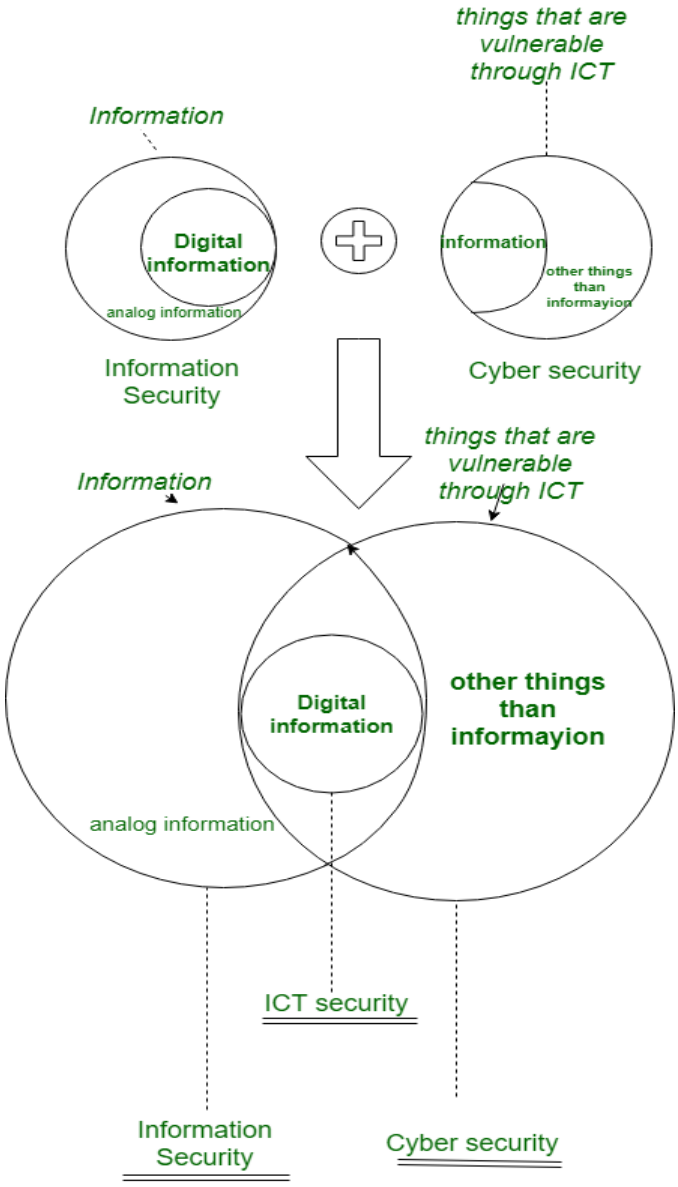
Access Controls

Technical Controls

Compliance Controls

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.

Diagrams are given below to represent the difference between Information Security and Cybersecurity.



In the above diagram, **ICT** refers to Information and communications technology (ICT) which is an extensional term for information technology (IT) that defines the role of unified communications and the integration of telecommunications (basically digital communication security).

What is the CIA Triad?

The CIA Triad is a security model developed to ensure the 3 goals of cybersecurity, which are Confidentiality, Integrity, and Availability of data and the network.

1. Confidentiality

Keeping the sensitive data private and accessible to only authorized users.

2. Integrity

Designed to protect the data from unauthorized access and ensure its reliability, completeness and correctness.

3. Availability

Authorized users can have access to system resources and data as and when they need it.

Goals of CIA Triad

1. Confidentiality

The central idea behind the term confidentiality in the CIA Triad. The CIA Triad ensures that the data is only accessible by genuine authorized users. It helps in preventing disclosure to unintended parties who might exploit the privacy of the user.

Methods to ensure Confidentiality are :

- Encryption of raw data
- Using biometrics for authentication
- Two way or multifactor authentication
- Let us say you work as a security engineer for a renowned financial firm with many competitors across the globe. An anonymous entity is trying to access the company's trade secrets. You must make sure that the confidential information is not accessible to any unauthorized outsiders.
- Hence you implement Firewall and intrusion detection systems. This is a typical example of holding the confidentiality of your company.

2. Integrity

- Integrity is making sure the data is unaltered during the time of transmission and ensuring it reaches the end-user in the correct form. It maintains the consistency and reliability of data.

Methods to ensure Integrity are :

- Making use of user access control to restrict unauthorized modification of files.

- Setting up backups to restore data during any system failure.
- Version control systems help to identify any modification by tracing the logs.

Now being the same security engineer of the same financial firm, you have to ensure that users are not destroying the data that the company holds.

Some users may accidentally or intentionally alter the database and corrupt the data to cause loss to the firm.

You need to ensure that the backups are in place for implementation during such emergencies.

You may use File Integrity Monitors(FIM) and hashing functions to make sure the data is un-tampered and safe.

3. Availability

The last component of the CIA Triad – Availability helps in delivering resources as and when requested by the user without any intervention like Denial of Service warnings.

Methods to ensure Availability are :

1. Installing firewalls, proxy servers during downtime.
2. Locating backups at geographically isolated locations.

Lastly, consider your task this time is to ensure the website of your firm is functioning properly 24/7 without any hindrance.

Organizations that deal with financial transactions cannot take any chances to face downtime as it will cause huge losses, hold the customers' assets at stake and reduce trust in the organization.

During such times, when the server crashes you need to have a second one that you replace the services and keep the site up and running.

Tools for Achieving CIA Goals

1. Tools for Confidentiality

a. Encryption – It is the process of transforming plain data into unreadable cipher data using an encryption key.

b. Access Control – It has rules and policies to limit access to the resources by checking the credentials of users.

c. Authentication – It is the confirmation of the user's identity for providing access to the resources.

d. Authorisation – Verifies the user's access level and either grant or refuses resource access.

e. Physical Security – It is required to keep the information available and improve the robustness of the system during hardware failures. It secures business-sensitive information, trade secrets, and customer information.

2. Tools for Integrity

a. Backups – These are duplicate archives of original data.

b. Checksums – It is a computational function that maps the contents of the data to a numerical value to check whether the data is the same before and after the transaction.

c. Error-correcting codes – Method for controlling errors during and unreliable data transfer over noisy channels.

3. Tools for Availability

a. Physical protection – Safeguarding the data against physical challenges like fire or theft.

b. Computational Redundancy – Makes the system fault-tolerant and protects against accidental modification.

To achieve and maintain these goals, good cybersecurity has to consider the following points:

- A business-specific plan which establishes threats and risk.
- Policies and procedures for execution when business is under threat.
- Security training among employees to create awareness.
- Set security milestones.
- Consult an expert for advice.

UNIT–II:

Information Security (IS) within Lifecycle Management-Lifecycle management landscape, Security architecture processes, Security architecture tools, Intermediate lifecycle management concepts, **Risks & Vulnerabilities-**Basics of risk management**,** Operational threat environments**,** Classes of attacks

Information Security (IS) within Lifecycle Management

Across all sectors of IT, projects are often managed through a lifecycle model, where a product goes through a cycle of improvement and upkeep with no endpoint. This is true for information security as much as any other IT sector.

The information security lifecycle serves as a core guide for daily operations for security professionals. Understanding the lifecycle model for information security planning gives professionals a guide that ensures continuous, evolutionary progress within a company's information security.

In this guide, we'll answer an essential question: what are the steps of the information security program lifecycle?

Foundations: Security policy and standards

Before we dive into the steps of the information lifecycle, we first need to discuss which core elements are needed.

An information security program lifecycle depends on a solid foundation. The foundation is the set of company policies and procedures upon which the security team will base its lifecycle process.

Clear and thorough policies and standards are essential core components of information security. Taking the time to put clear standards in place:

- Sets clear expectations: Policies and procedures create a clear framework that security teams can refer back to when analyzing and evaluating both existing systems and new systems. Instead of comparing systems and processes to a nebulous goal, they have a firm set of policies and standards for comparison.
- Creates cohesion: Many information security projects may operate separately on individual problem areas. Clear policies and procedures create a baseline that all teams can work from, which helps to minimize conflicting solutions and updates.
- Streamlines improvements: Detailed policies and standards establish a baseline that teams can refer back to when developing and evaluating systems and solutions, minimizing the need for back and forth between teams. This means that security teams can work more efficiently

through the information security lifecycle. Depending on the policies and procedures your company has laid out, your information lifecycle may have a radically different foundation than another company's. However, despite these different foundations, company information security lifecycles tend to follow a similar step-by-step process. This process is outlined in detail in the following sections.

Step 1: Identify

- The first step in the information security program lifecycle is to identify what items need to be protected. In an information security protocol, you can't protect what you don't know about. For this reason, identification is a key first step to ensuring the cycle covers all aspects of a network.
- Identification primarily involves mapping the network you're working on. This should start at a high level then drill down to more granular details. This information helps your information security team understand the assets within a system and how they are related, as well as the resources currently available for information security protocols. Some of the key items the identification stage looks at include the following:
- The number of servers, routers, and other assets available
- The locations of physical assets
- The types of operating systems running on the network
- The number and type of applications and software running on systems
- The reach and importance of applications and software for each department
- The status of each computer and mobile device on the network
- Which assets are a top priority for your company
- The current infrastructure of security systems

Gathering this information involves performing an audit of the company's systems. Audits will typically start with a general overview and assessment of current tools and platforms. However, this audit should also involve interviews and internal discussions. Conversations with security professionals, IT staff, and individuals from other departments will help create a more thorough understanding of current systems, their interrelationships, their purpose within the company, and their importance within various departments. Additionally, external resources are often used during audits to provide an unbiased look at your company's posture, adding another layer to the information gathered in the audit.

Once the audit is complete, the information security team will have a thorough picture of the company's information security posture as it exists. This data is typically written up into a document and stored for later use and reference in the information security lifecycle.

Step 2: Assess

Once the information security team has thoroughly mapped out the organization's existing technology through the identification process, it’s time for the assessment phase. In the assessment step, security professionals take the information gathered from the identification process and perform a security assessment on all assets. This assessment process is one of the most extensive steps in the information

security lifecycle and covers several areas, including process and system reviews, server reviews, and vulnerability assessments.

1. Process and system reviews

The first part of the assessment step is to review the current structure of the business. In this review, security professionals will look into the structures outlined during the identification process and collect more information to identify vulnerabilities. This can be a monumental task, especially for large enterprises, so it’s generally recommended to use one or more of the following methods during this phase of the assessment process:

- Focus on essential assets first: One way to handle the assessment process is to prioritize based on asset importance. Start the assessment process by focusing on assets that are the most vulnerable and the most critical to your organization's functionality. This will help identify the most important improvements early on so the security team can implement these improvements more quickly.
- Review from top to bottom:Another way to handle the assessment process is to work from high-level systems and drill down from there. By analyzing systems from the most general to the most detailed, security professionals can identify larger, more systemic problems first.
- Look for flags:Finally, the information security team may have identified red flags and concerns during the identification process. This includes outdated software versions, obsolete hardware, and feedback from employees. Teams can take these issues into account when performing the assessment process, as these flags can help identify smaller vulnerabilities early on in the assessment process.

When performing these assessments, information security teams continue collecting information about the resources analyzed. Some of the information the team may collect includes details about applications, how they're configured, where components are located, and how the application is used within the business. All of this data helps to develop thorough vulnerability assessments.

2. Server reviews

During the assessment process, teams will also conduct internal reviews of each server, including configurations and settings. The team will compare the server settings to policies and standards to ensure compliance, especially in the following areas:

- Password and user account policies
- User IDs, administrator accounts, and groups
- Web server configurations
- Log protocols and access
- Relationships to other servers
  Like with the process and system reviews, teams will collect detailed information about each server, including problems and configuration settings. All of this information is needed to perform vulnerability assessments and evaluate servers and processes for potential updates.

3. Vulnerability assessments

Once the security team is done consulting and collecting information, they perform vulnerability assessments on each system. Vulnerability assessments utilize risk-management practices to create thorough analyses of each system's current and future risks.

During the vulnerability assessment process, security teams will generally focus the most effort on essential assets and areas where they flagged potential risk factors. During the vulnerability assessment, the team identifies all items of concern and asks essential risk-management questions, including:

- What level of risk is tolerable for each system?
- How prepared is each system for handling existing threats?
- How versatile is the system for handling new threats?
- Is data secured in the event of a natural disaster?
- What countermeasures exist for each device and service?
- What is the business impact of the system going down?
- Does the current security structure comply with industry, local, and federal regulations?
- Once each vulnerability assessment is complete, the team documents the results for reference later in the information security lifecycle.

Step 3: Design

After the security team assesses all systems, it's time to use the information they collected to design solutions and countermeasures. Based on the specific vulnerabilities and issues they identified in the assessment step, the information security team will brainstorm ways to resolve specific problems, including cybersecurity threats, security products, and information security culture and processes. Some specific factors teams will consider during the design phase include the following:

Security layering: Design teams will consider security layering an essential part of the design. In this design protocol, multiple layers of defense protect each system, starting with general protective measures like firewalls and narrowing down to detailed security measures like multi-factor authentication procedures. Security designers should ensure that each system is protected by multiple security layers, especially critical systems.

Compliance: Another consideration in design is compliance with mandatory obligations at the industry, local, and federal levels. Security structures developed during the design process should comply with any standards and legislation that apply to the company.

Continuity: Business continuity is the ability of a business to maintain or recover service after an interruption or disaster. Your security team should design systems and processes with integrated backups and redundancies to ensure the company can quickly resume normal operation after the event.

Area of effect: For each potential alteration, design teams need to consider what systems will be affected by the change. Some changes may have limited effect, while others may create more widespread change that affects multiple systems.

Effectiveness: Finally, teams handling system designs need to consider any trade-offs between security and effectiveness. Maximum security may be the safest option, but the cost of achieving it may be prohibitive both in resources and in productivity lost to introduced inefficiencies.

Once the team has developed potential ways to resolve specific issues, they will analyze each solution in detail and create individual plans and blueprints for each change. These blueprints will include system configuration alterations, process changes, tools, and other factors, as well as how they will resolve the issue. The blueprint will also present an analysis of the effects of these changes, including procedural alterations, impacts on adjacent systems, and costs of implementation.

When the team finalizes their blueprints, they deliver their solutions to management and leadership, who make the final decision on a go-forward plan for each individual issue.

Step 4: Implement

After the design of a solution is approved, the next step in the information lifecycle is implementation. In this step of the process, the team creates an implementation plan for the solution and begins deployment. This implementation plan typically includes the following steps:

Develop a change plan: Working off the blueprints developed in the design phase, the security team creates a step-by-step change plan. When possible, they focus on the most important areas first, then work down toward the least vulnerable areas. The change plan should also account for any personnel training needed to implement new procedures or policies.

Create team roles: After developing a plan, the team assigns roles and responsibilities for individuals involved in implementing the changes. These individuals will likely include project managers, IT leaders, training teams, and any other specialists related to the changes being made.

Acquire resources: Next, your team acquires the tools needed to implement the proposed changes. These may include security programs, network hardware, and software needed for implementing and maintaining the proposed changes.

Test changes: Once they've acquired the necessary resources, the team performs tests to ensure the new resources work as expected. If any unexpected issues arise, they adjust the change plan as needed.

Implement changes: After tests have validated desired results, and any alterations to the change plan have been finalized, the security team rolls out the new changes according to the plan. They also perform regular assessments and reviews during the implementation phase and make adjustments in the event of delays.

Of course, the implementation phase should also include any internal processes the company requires for major changes. These may include change management controls and quality assurance reviews.

Step 5: Protect

This step is closely related to the design and implementation steps but covers a slightly different scope. The goal of the protection step, also called the mitigation phase, is to validate your security measures to ensure systems match your established security policies and standards.

In this phase, information security planning teams review the system as a whole, combined with any new changes added during previous steps. This involves the following:

Policies and standards: The security team ensures new and existing systems meet or exceed established security policies and standards.

Security levels: The team checks that individual systems have an appropriate level of security for their importance. For example, core systems will have greater security than less critical systems.

Implementation verification: The team and stakeholders will verify that all new measures have been correctly implemented. This involves assessing each change compared to the goals established during the design and implementation phases.

Once the systems and changes have been evaluated, the protect phase may involve repeating the design and implementation phases to correct errors or target areas that were missed in the original assessment phase.

Step 6: Monitor

The final step of the information security lifecycle is the monitoring phase. In this phase, the information security team monitors the system and any changes put in place. While security measures implemented today may protect against vulnerabilities, there is no guarantee that they will remain secure in the future. The goal of the monitoring phase is twofold: to ensure that strengthened security remains in place and to identify new vulnerabilities as they arise.

The monitoring phase requires the security team to update and implement monitoring processes as needed to measure the status of new and existing systems across the network. Establishing this process involves analyzing a few key areas:

Monitoring methods: Monitoring and verifying network systems is essential, but the question is how to monitor these systems. Network intrusions can be monitored through event logging and other security systems, but it's just as important to ensure that the network systems continue to maintain correct configurations. Vulnerabilities can be introduced when new applications or patches are installed, so regular examination of configurations is key to ensuring that servers, routers, and applications remain compliant with a company's security policies and standards. The security team can monitor these configurations manually or with the assistance of compliance monitoring tools.

Monitoring frequency: Another key question is how often a system should be monitored. Your team can determine the frequency based on the value of each individual resource. While every system needs to be checked regularly for vulnerabilities, core systems should be checked more often than less valuable systems. This value-based monitoring ensures that the right amount of attention is paid to each resource.

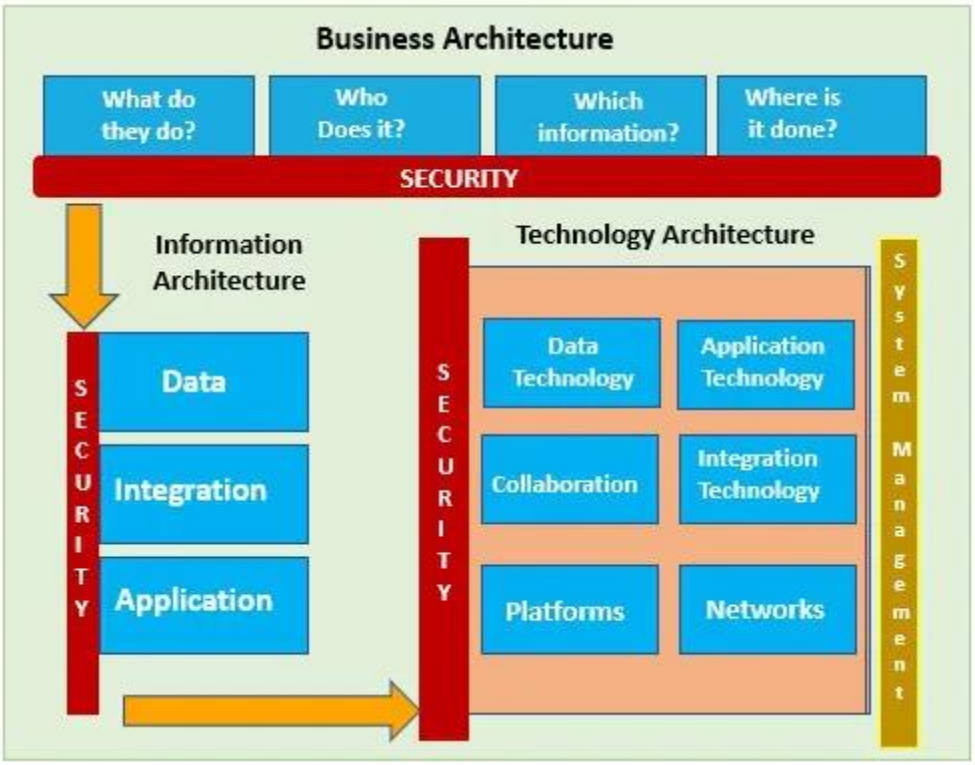
Monitoring measurements: Monitoring must also involve measurements that communicate data into a quantifiable format. Quantifiable data allows the team to compare metrics from day to day across the enterprise. This makes it easier to visualize security and allows for easier identification of deficiencies. A quality monitoring protocol will allow information security professionals to maintain visualization of security systems as a whole, informing them when a critical error arises. On top of establishing a monitoring protocol, the monitoring phase also involves keeping abreast of new developments in the cybersecurity landscape. New threats arise every day, and best practices in information security are constantly evolving. With a combination of quality monitoring and cybersecurity awareness, information security professionals can determine the best time to restart the information security lifecycle over again.

Introduction to Security Architecture

Security architecture is defined as the architectural design that includes all the threats and potential risks which can be present in the environment or that particular scenario. This also includes the security controls and the use of security controls. For the security architecture, the proper documentation is done that include all the security specifications and include all the detailed information about the architecture. The organization uses for their system, and it is mainly used because the architecture is affordable and cost-effective and can be used easily by the organization.

Security Architecture with Diagram

This is defined as the part of enterprise architecture that is particularly design for addressing the information system and fulfill the security requirements of the organization. The system architecture system has a role that it meets the security requirements and also helps to protect the company operating environment. It is beneficial for the company as it includes other activities like risk management activities that require continuous improvement, and security architecture helps to meet the organization requirements. It defines proper polices, rules and regulations that need to reinforce in the organization and provide proper information about them. The architecture is also used for allocating the controls for technical security so that the information system of the organization can be maintained properly. As the same can be followed in a whole organization, it helps to define common regulations and standards for every employee so that everyone can follow the rules and maintain data integrity and security in the organization.



In the above diagram, the high-level design of the system architecture is shown. The abstraction is given here.

Components of Security Architecture

For making the security architecture important, there are certain components that are involved in the design. The components are people, process and the tools. All these components combine helps to protect the organization assets. After defining the components, the next step is to make the policy and the reinforcement technique for the policies. After the other important steps are the method procedural for the implementation of security architecture and how the architecture will get enforced. By this, the overall design and architecture are designed for the organization that will protect them throughout their business operations. For a proper security architecture, some of the components are briefly discussed:

1. Guidance

The policies and procedures that act as the guidance should be design and implement properly. The policies should include the documentation that includes the objectives and goals for designing the architecture, standards, policies, rules and regulations for the organization, identification of scope and function, identification of other security policies.

2. Identity Management

It is the type of system that include the organization processes, technologies and policies that directly help users to gain access to the online applications and other network resources. For the organization, the proper responsibilities and roles need to be clearly stated, and individual tasks need to be designed for the employees.

3. Inclusion & Exclusion

The other components are the inclusion and exclusion that include the security of elements of the organization in which company resources are protected. The company resources include web resources, e-mail servers, private HR data and other reporting system information. The access should be grant to authorized users only so that the privacy and integrity can be maintained in the organization.

4. Access and Border Control

The organization should develop an architecture that is able to control the access to the business resources and can use the layer system for providing access to the company employees. Only authorized users should gain complete access to the system, and the rest should be provided with limited access of the system.

5. Validation of Architecture

As the technology advances, the company need to renew the policies and laws as per the changes, and continuous effort is needed by the organization in this change. For that, the continuous monitoring is required, and according to that, proper changes can be made in the architecture.

6. Training

As for the organization, to maintain the privacy and integrity, the security architecture system is very important. AS there is a continuous change in the system, it becomes important that the employee should know about the changes and proper training is given to them so that they can use the system and protect the company assets and elements.

7. Technology

To reinforce the security architecture, the software and hardware used for making the architecture become very crucial for the organization. Because of continuous change in technology, there is a requirement of continuous change in the system so that the system can be up to date and help to make the system secure and private.

Benefits of Using the Security Architecture

Some of the benefits are mentioned below.

Help to protect the important company assets from the outside and provide security to the important resources to the organization. The architecture provides the limited access to the user so that the confidential data can be kept secure and safe.

The architecture defines the common policies and standards that can be used by the every employee of the company and also define common rules so that no one face any difficulty to use the system. It helps the organization to reach their goal and easily conduct their business operations smoothly.

The other benefit is risk management activities covered by the architecture as the risk management activity requires continuous assistance and also need continuous improvement, the security architecture act as a better solution for them.

Every technology-driven business process is exposed to security and privacy threats. Sophisticated technologies are capable of combating cybersecurity attacks, but these aren't enough: organizations must ensure that business processes, policies, and workforce behavior minimize or mitigate these risks.

Because this path is neither easy nor clear, companies adopt frameworks that help guide towards information security (InfoSec) best practices. This is where information security management systems come into play—let's take a look.

What is an ISMS?

An information security management system (ISMS) is a framework of policies and controls that manage security and risks systematically and across your entire enterprise—information security. These security controls can follow common security standards or be more focused on your industry.

For example, ISO 27001 is a set of specifications detailing how to create, manage, and implement ISMS policies and controls. The ISO doesn't mandate specific actions; instead, it provides guideline on developing appropriate ISMS strategies.

The framework for ISMS is usually focused on risk assessment and risk management. Think of it as a structured approach to the balanced tradeoff between risk mitigation and the cost (risk) incurred.

Organizations operating in tightly regulated industry verticals, such as healthcare or finance, may require a broad scope of security activities and risk mitigation strategies.

(Consider InfoSec management within your overall IT security policy.)

Continuous improvement in information security

While ISMS is designed to establish holistic information security management capabilities, digital transformation requires organizations to adopt ongoing improvements and evolution of their security policies and controls.

The structure and boundaries defined by an ISMS may apply only for a limited time frame and the workforce may struggle to adopt them in the initial stages. The challenge for organizations is to evolve these security control mechanisms as their risks, culture, and resources change.

According to ISO 27001, ISMS implementation follows a Plan-Do-Check-Act (PCDA) model for continuous improvement in ISM processes:

Plan. Identify the problems and collect useful information to evaluate security risk. Define the policies and processes that can be used to address problem root causes. Develop methods to establish continuous improvement in information security management capabilities.

Do. Implement the devised security policies and procedures. The implementation follows the ISO standards, but actual implementation is based on the resources available to your company.

Check. Monitor the effectiveness of ISMS policies and controls. Evaluate tangible outcomes as well as behavioral aspects associated with the ISM processes.

Act. Focus on continuous improvement. Document the results, share knowledge, and use a feedback loop to address future iterations of the PCDA model implementation of ISMS policies and controls.

Popular ISMS frameworks

ISO 27001 is a leader in information security, but other frameworks offer valuable guidance as well. These other frameworks often borrow from ISO 27001 or other industry-specific guidelines.

- ITIL, the widely adopted service management framework, has a dedicated component called Information Security Management (ISM). The goal of ISM is to align IT and business security to ensure InfoSec is effectively managed in all activities.

- COBIT, another IT-focused framework, spends significant time on how asset management and configuration management are foundational to information security as well as nearly every other ITSM function—even those unrelated to InfoSec.

ISMS security controls

ISMS security controls span multiple domains of information security as specified in the ISO 27001 standard. The catalog contains practical guidelines with the following objectives:

Information security policies. An overall direction and support help establish appropriate security policies. The security policy is unique to your company, devised in context of your changing business and security needs.

Organization of information security. This addresses threats and risks within the corporate network, including cyberattacks from external entities, inside threats, system malfunctions, and data loss.

Asset management. This component covers organizational assets within and beyond the corporate IT network., which may involve the exchange of sensitive business information.

Human resource security. Policies and controls pertaining to your personnel, activities, and human errors, including measures to reduce risk from insider threats and workforce training to reduce unintentional security lapses.

Physical and environmental security. These guidelines cover security measures to protect physical IT hardware from damage, loss, or unauthorized access. While many organizations are taking advantage of digital transformation and maintaining sensitive information in secure cloud networks off-premise, security of physical devices used to access that information must be considered.

Communications and operations management. Systems must be operated with respect and maintenance to security policies and controls. Daily IT operations, such as service provisioning and problem management, should follow IT security policies and ISMS controls.

Access control. This policy domain deals with limiting access to authorized personnel and monitoring network traffic for anomalous behavior. Access permissions relate to both digital and physical mediums of technology. The roles and responsibilities of individuals should be well defined, with access to business information available only when necessary.

Information system acquisition, development, and maintenance. Security best practices should be maintained across the entire lifecycle of the IT system, including the phases of acquisition, development, and maintenance.

Information security and incident management. Identify and resolve IT issues in ways that minimize the impact to end users. In complex network infrastructure environments, advanced

technology solutions may be required to identify insightful incident metrics and proactively mitigate potential issues.

Business continuity management. Avoid interruptions to business processes whenever possible. Ideally, any disaster situation is followed immediately by recovery and procedures to minimize damage.

Compliance. Security requirements must be enforced per regulatory bodies.

Cryptography. Among the most important and effective controls to protect sensitive information, it is not a silver bullet on its own. Therefore, ISMS govern how cryptographic controls are enforced and managed.

Supplier relationships. Third-party vendors and business partners may require access to the network and sensitive customer data. It may not be possible to enforce security controls on some suppliers. However, adequate controls should be adopted to mitigate potential risks through IT security policies and contractual obligations.

These components and domains offer general best practices towards InfoSec success. Though these may vary subtly from one framework to another, considering and aligning with these domains will provide much in the way of information security.

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH RISK MANAGEMENT

this chapter describes the fundamental concepts associated with managing information security risk across an organization including: (i) the components of risk management; (ii) the multitiered risk management approach; (iii) risk management at Tier 1 (organization level); (iv) risk management at Tier 2 (mission/business process level); (v) risk management at Tier 3 (information system level); (vi) risk related to trust and trustworthiness; (vii) the effects of organizational culture on risk; and (viii) the relationships among key risk management concepts.

2.1 COMPONENTS OF RISK MANAGEMENT

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization—from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the organization's missions/business functions. Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organizationwide activity that addresses risk from the strategic level to the tactical level, ensuring that riskbased decision making is integrated into every aspect of the organization.13 The following sections briefly describe each of the four risk management components.

The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. Establishing a realistic and credible risk frame requires that organizations identify: (i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses). The risk framing component and the associated risk management strategy also include any strategic-level decisions on how risk to organizational operations and assets, individuals, other organizations, and the Nation, is to be managed by senior leaders/executives.

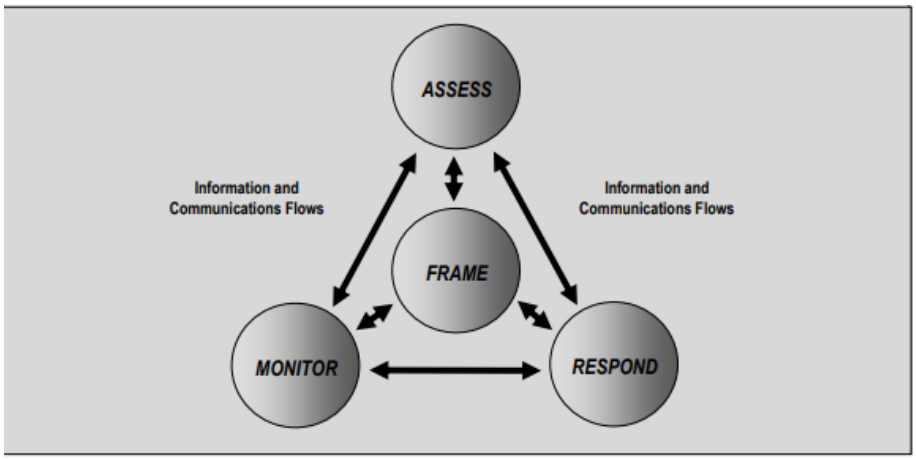
The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations;14 (iii) the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring). To support the risk assessment component, organizations identify: (i) the tools, techniques, and methodologies that are used to assess risk; (ii) the assumptions related to risk assessments; (iii) the constraints that may affect risk assessments; (iv) roles and responsibilities; (v) how risk assessment information is collected, processed, and communicated throughout organizations; (vi) how risk assessments are conducted within organizations; (vii) the frequency of risk assessments; and (viii) how threat information is obtained (i.e., sources and methods).

The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of risk assessments. The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action. To support the risk response component, organizations describe the types of risk responses that can be implemented (i.e., accepting, avoiding, mitigating, sharing, or transferring risk). Organizations also identify the tools, techniques, and methodologies used to develop courses of action for responding to risk, how courses of action are evaluated, and how risk responses are communicated across organizations and as appropriate, to external entities (e.g., external service providers, supply chain partners).

The fourth component of risk management addresses how organizations monitor risk over time. The purpose of the risk monitoring component is to: (i) verify that planned risk response measures are implemented and information security requirements derived from/traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied; (ii) determine the ongoing effectiveness of risk response measures following implementation; and (iii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate.To support the risk monitoring component, organizations describe how compliance is verified and how the ongoing effectiveness of risk responses is determined (e.g., the types of tools, techniques, and methodologies used to determine the sufficiency/correctness of risk responses and if risk mitigation measures are implemented correctly, operating as intended, and producing the desired effect with regard to reducing risk). In addition, organizations describe how changes that may impact the ongoing effectiveness of risk responses are monitored.

As indicated in the four components of risk management described above, organizations also consider external risk relationships, as appropriate. Organizations identify external entities with which there is an actual or potential risk relationship (i.e., organizations which could impose risks on, transfer risks to, or communicate risks to other organizations, as well as those to which organizations could impose, transfer, or communicate risks). External risk relationships include, for example, suppliers, customers or served populations, mission/business partners, and/or service providers. For organizations dealing with advanced persistent threats (i.e., a long-term pattern of targeted, sophisticated attacks) the risk posed by external partners (especially suppliers in the supply chain) may become more pronounced. Organizations establish practices for sharing riskrelated information (e.g., threat and vulnerability information) with external entities, including those with which the organizations have a risk relationship as well as those which could supply or receive risk-related information (e.g., Information Sharing and Analysis Centers [ISAC], Computer Emergency Response Teams [CERT]).

Figure 1 illustrates the risk management process and the information and communications flows among components. The black arrows represent the primary flows within the risk management process with risk framing informing all the sequential step-by-step set of activities moving from risk assessment to risk response to risk monitoring. For example, one of the primary outputs from the risk framing component is a description of the sources and methods that organizations use in acquiring threat information (e.g., open source, classified intelligence community reports). The output regarding threat information is a primary input to the risk assessment component and is communicated accordingly to that component. Another example is illustrated in the primary output from the risk assessment component—that is, a determination of risk. The output from the risk assessment component is communicated to the risk response component and is received as a primary input for that component. Another primary input to the risk response component is an output from the risk framing component—the risk management strategy that defines how the organization should respond to risk. Together, these inputs, along with any additional inputs, are used by decision makers when selecting among potential courses of action for risk responses.



Operational threat environments

Why Does the Threat Environment Matter?

A cyber threat is an attempt to damage or disrupt a computer network or system. Cyber threats can become a reality if there are vulnerabilities present within a network, hardware, or software, which allow an attacker to reduce a system's information assurance. Most cybersecurity guidance addresses access control, configurations, and accountability, but businesses cannot determine risk or know where to invest in security until they know the threat landscape facing their organization.

Where to Start

First,

understand and prevent common vulnerabilities. Leverage community repositories, such as the National Vulnerability Database (https://nvd.nist.gov/), to ensure that known vulnerabilities are addressed. This requires that some form of asset management exists in your business.

Second,

determine what cyber events you organization monitors. If information technology and incident response activities are outsourced, insist that the service providers supply threat, incident, and activity reports from network traffic in a format that works for your staff. The National Institute of Standards and Technology (NIST) Cybersecurity Framework and special publications (e.g. NIST SP 800-30) provide a common language for understanding, managing, and expressing cyber risk. Industries may also offer specific security guidance, controls, or threat models

Third,

ensure that a business impact assessment is complete and up to date. Do you know what your critical business functions are? Do your threats have the capabilities to disrupt them? What are your contingency plans and procedures?

Fourth,

create or become an active member in an industry or regional information sharing and analysis organization (ISAO) to crowd source security. Lastly, continuously use what already exists to counter and monitor threats. DHS offers several programs enabling industry to protect and defend critical infrastructure and provide opportunities to share threat intelligence: Enhanced Cybersecurity Services (ECS)¬ Critical Infrastructure Information¬ Sharing and Collaboration Program (CISCP)

About the C3 Voluntary Program

The Critical Infrastructure Cyber Community (C3) Voluntary Program is a public-private partnership led by DHS to help align critical infrastructure owners and operators with existing resources to assist the use

of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. All of these programs, tips, and resources, can be found on the C3 Voluntary Program

What is Operational Cyber Threat Intelligence and How to Use It

Organizations of all sizes are building security teams to deploy network solutions and address threats. A key component to the success of these initiatives is access to up-to-date cyber threat intelligence.

This blog describes the significance of operational threat intelligence for organizations. Don't forget to look at the other blog posts where we talk about tactical, technical, and strategic cyber threat intelligence.

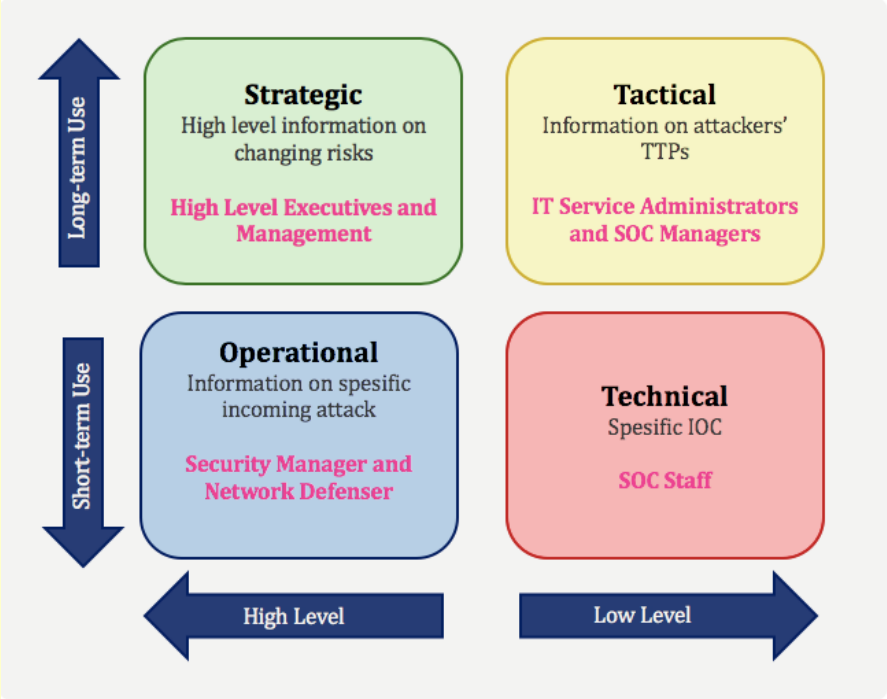
What is Cyber Threat Intelligence (CTI)?

CTI, by definition, is a form of threat intelligence that can be used to understand current or future threats better.

Collecting, analyzing, and classifying cyber threat information is used for providing firms with an actionable vision to identify, measure and rank vulnerabilities and mitigate cyber risks. Better knowledge about cyber CTI gives the latest threat trends on the cyber threat landscape. For your cybersecurity strategy to be effective, you must understand the different types of cyber information.

What are the Types of Cyber Threat Intelligence?

Threat intelligence falls into four categories within the framework of applicable information: Strategic, Tactical, Operational, and Technical. For these four types of intelligence, data collection, analysis, and consumption of intelligence differ. SOCRadar generates intelligence at different levels with the information it collects and ensures the best use of information.



- *Strategic Cyber Intelligence:* The audience does not need technical knowledge. High-level information on changing risks. High-level information on risk-based intelligence is used by high-level decision-makers (Executives and management). Whitepapers, policy documents, and publications are examples of strategic cyber intelligence.
- *Operational Cyber Intelligence*: Actionable information about specific incoming attacks. They are infiltrating hacker chat rooms to anticipate the incoming attacks.
- *Tactical Cyber Intelligence*: Details of threat actor tactics, techniques, and procedures (TTPs).
- *Technical Cyber Intelligence:* Technical threat indicators such as specific IOC for SOC Staff.

What is Operational Cyber Threat Intelligence?

Operational CTI aims to answer "how" and "where" at the operational level. Detected threat actor TTPs explain "how." How should the organization understand the extent of a breach and prepare a defense policy?

CTI helps organizations proactively pursue threat hunting before the compromise or after recovering the beginning of the incident. As a result, to better respond, you should know where to skim/scan. Tactical and Operational CTI's features can overlap, but the main difference is Tactical CTI is more automated.

Operational CTI focuses on attack knowledge, which provides detailed insights into factors such as nature, motivation, timing, and attack methods. Ideally, information is collected through penetration from hacker chat rooms or online discussions, which is difficult to obtain.

Operational CTI provides a coherent framework to analyze and prioritize potential threats and vulnerabilities in the organization's threat environment, thereby linking the possibility and impact of cyber attacks to their strategic implications.

Who Uses Operational CTI, Why, and How?

Operational CTI scope is Industry/Sector, Partners, Suppliers, Competitors, Customers, etc. OCT users in any firm include various personnel related to security such as malware analysts, incident responders/teams, network defenders, host analysts, etc. Technical background crucial for using Operational CTI. They use threat hunting procedures for counterintelligence. And they also use Operational CTI to provide warning intelligence.

Operational CTI Use Case: Threat Hunting

Threat hunting for operational users uses CTI to proactively search for evidence of threat actor activity, leveraging all relevant IOCs. A hypothesis based on the hunter's intuition, or one or two seemingly unrelated pieces of evidence, is often the starting point for threat hunting. The hunter uses the CTI to explore the theory's details further, either confirming it or moving on to the next issue. Successful Threat Hunting is nearly impossible without a specialized and reliable CTI.

What are the Difficulties in Collecting Operational Intelligence:

- Threats usually communicate over encrypted or private chat rooms, and access to these channels is not easy.
- It is not easy to manually gather relevant intelligence from vast data of chat rooms or other communication channels.
- Threat groups may use confusing and ambiguous language so that no one can understand their conversation.

What are the common types of cyber security attacks?

Cyber attacks are increasingly common, and some of the more advanced attacks can be launched without human intervention with the advent of network-based ransomware worms.

Definition of Cyber Attack: A cyber attack is when there is a deliberate and malicious attempt to breach the information system of an individual or organization.

While there is usually an economic goal, some recent attacks show the destruction of data as a goal. Malicious actors often look for ransom or other kinds of economic gain, but attacks can be perpetrated with an array of motives, including political activism purposes.

Top 10 common types of cyber security attacks

- Malware
- Phishing
- Man-in-the-Middle (MitM) Attacks
- Denial-of-Service (DOS) Attack
- SQL Injections
- Zero-day Exploit
- Password Attack
- Cross-site Scripting
- Rootkits
- Internet of Things (IoT) Attacks

Malware

The term “malware” encompasses various types of attacks including spyware, viruses, and worms. Malware uses a vulnerability to breach a network when a user clicks a “planted” dangerous link or email attachment, which is used to install malicious software inside the system.

Malware and malicious files inside a computer system can:

- Deny access to the critical components of the network
- Obtain information by retrieving data from the hard drive
- Disrupt the system or even render it inoperable

Malware is so common that there is a large variety of modus operandi. The most common types being:

- **Viruses**—these infect applications attaching themselves to the initialization sequence. The virus replicates itself, infecting other code in the computer system. Viruses can also attach themselves to executable code or associate themselves with a file by creating a virus file with the same name but with an .exe extension, thus creating a decoy which carries the virus.
- **Trojans**—a program hiding inside a useful program with malicious purposes. Unlike viruses, a trojan doesn't replicate itself and it is commonly used to establish a backdoor to be exploited by attackers.
- **Worms**—unlike viruses, they don't attack the host, being self-contained programs that propagate across networks and computers. Worms are often installed through email attachments, sending a copy of themselves to every contact in the infected computer email list. They are commonly used to overload an email server and achieve a denial-of-service attack.
- **Ransomware**—a type of malware that denies access to the victim data, threatening to publish or delete it unless a ransom is paid. Advanced ransomware uses cryptoviral extortion, encrypting the victim's data so that it is impossible to decrypt without the decryption key.
- **Spyware**—a type of program installed to collect information about users, their systems or browsing habits, sending the data to a remote user. The attacker can then use the information for blackmailing purposes or download and install other malicious programs from the web.

Phishing

Phishing attacks are extremely common and involve sending mass amounts of fraudulent emails to unsuspecting users, disguised as coming from a reliable source. The fraudulent emails often have the appearance of being legitimate, but link the recipient to a malicious file or script designed to grant

attackers access to your device to control it or gather recon, install malicious scripts/files, or to extract data such as user information, financial info, and more.

Phishing attacks can also take place via social networks and other online communities, via direct messages from other users with a hidden intent. Phishers often leverage social engineering and other public information sources to collect info about your work, interests, and activities—giving attackers an edge in convincing you they're not who they say.

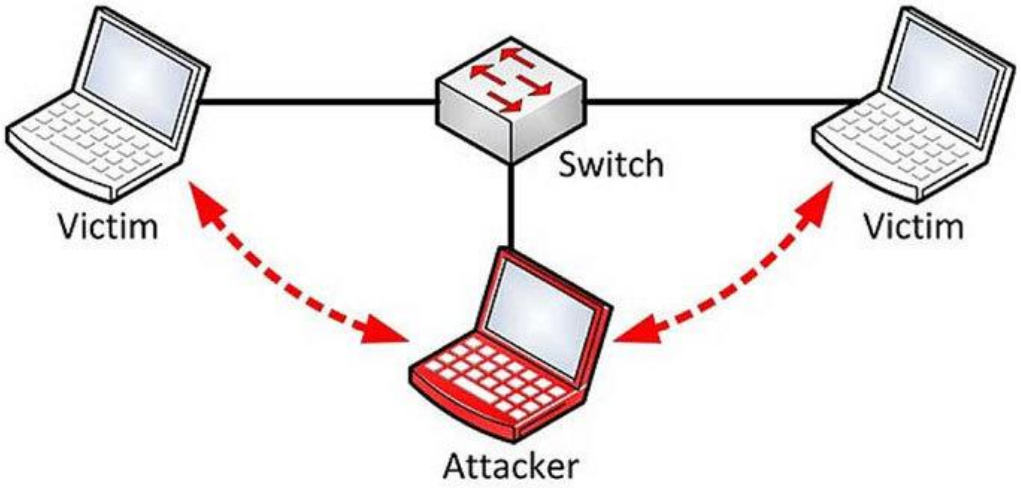
There are several different types of phishing attacks, including:

- **Spear Phishing**—targeted attacks directed at specific companies and/or individuals.
- **Whaling**—attacks targeting senior executives and stakeholders within an organization.
- **Pharming**—leverages DNS cache poisoning to capture user credentials through a fake login landing page.

Phishing attacks can also take place via phone call (voice phishing) and via text message (SMS phishing). This post highlights additional details about phishing attacks—how to spot them and how to prevent them.

Man-in-the-Middle (MitM) Attacks

Occurs when an attacker intercepts a two-party transaction, inserting themselves in the middle. From there, cyber attackers can steal and manipulate data by interrupting traffic.



This type of attack usually exploits security vulnerabilities in a network, such as an unsecured public WiFi, to insert themselves between a visitor's device and the network. The problem with this kind of attack is that it is very difficult to detect, as the victim thinks the information is going to a legitimate destination. Phishing or malware attacks are often leveraged to carry out a MitM attack.

Denial-of-Service (DOS) Attack

DoS attacks work by flooding systems, servers, and/or networks with traffic to overload resources and bandwidth. The result is rendering the system unable to process and fulfill legitimate requests. In addition to denial-of-service (DoS) attacks, there are also distributed denial-of-service (DDoS) attacks.

DoS attacks saturate a system's resources with the goal of impeding response to service requests. On the other hand, a DDoS attack is launched from several infected host machines with the goal of achieving service denial and taking a system offline, thus paving the way for another attack to enter the network/environment.

The most common types of DoS and DDoS attacks are the TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack, and botnets.

SQL Injections

This occurs when an attacker inserts malicious code into a server using server query language (SQL) forcing the server to deliver protected information. This type of attack usually involves submitting malicious code into an unprotected website comment or search box. Secure coding practices such as using prepared statements with parameterized queries is an effective way to prevent SQL injections.

When a SQL command uses a parameter instead of inserting the values directly, it can allow the backend to run malicious queries. Moreover, the SQL interpreter uses the parameter only as data, without executing it as a code. Learn more about how secure coding practices can prevent SQL injection here.

Zero-day Exploit

A Zero-day Exploit refers to exploiting a network vulnerability when it is new and recently announced — before a patch is released and/or implemented. Zero-day attackers jump at the disclosed vulnerability in the small window of time where no solution/preventative measures exist. Thus, preventing zero-day attacks requires constant monitoring, proactive detection, and agile threat management practices.

Password Attack

Passwords are the most widespread method of authenticating access to a secure information system, making them an attractive target for cyber attackers. By accessing a person's password, an attacker can gain entry to confidential or critical data and systems, including the ability to manipulate and control said data/systems.

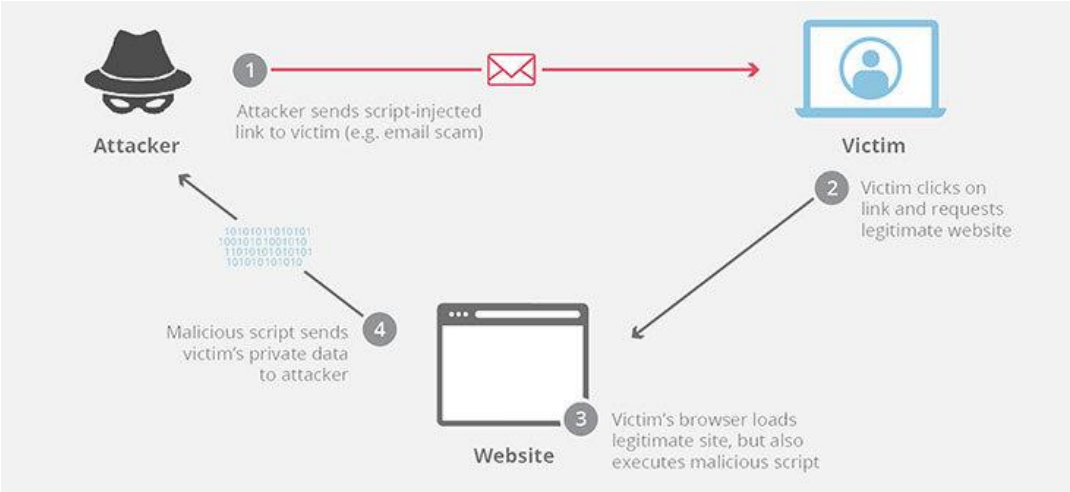
Password attackers use a myriad of methods to identify an individual password, including using social engineering, gaining access to a password database, testing the network connection to obtain unencrypted passwords, or simply by guessing.

The last method mentioned is executed in a systematic manner known as a "brute-force attack." A brute-force attack employs a program to try all the possible variants and combinations of information to guess the password.

Another common method is the dictionary attack, when the attacker uses a list of common passwords to attempt to gain access to a user's computer and network. Account lockout best practices and two-factor authentication are very useful at preventing a password attack. Account lockout features can freeze the account out after a number of invalid password attempts and two-factor authentication adds an additional layer of security, requiring the user logging in to enter a secondary code only available on their 2FA device(s).

Cross-site Scripting

A cross-site scripting attack sends malicious scripts into content from reliable websites. The malicious code joins the dynamic content that is sent to the victim's browser. Usually, this malicious code consists of Javascript code executed by the victim's browser, but can include Flash, HTML, and XSS.



Additional information about cross-site scripting attacks can be found here.

Rootkits

Rootkits are installed inside legitimate software, where they can gain remote control and administration-level access over a system. The attacker then uses the rootkit to steal passwords, keys, credentials, and retrieve critical data.

Since rootkits hide in legitimate software, once you allow the program to make changes in your OS, the rootkit installs itself in the system (host, computer, server, etc.) and remains dormant until the attacker

activates it or it’s triggered through a persistence mechanism. Rootkits are commonly spread through email attachments and downloads from insecure websites.

Internet of Things (IoT) Attacks

While internet connectivity across almost every imaginable device creates convenience and ease for individuals, it also presents a growing—almost unlimited—number of access points for attackers to exploit and wreak havoc. The interconnectedness of things makes it possible for attackers to breach an entry point and use it as a gate to exploit other devices in the network.

IoT attacks are becoming more popular due to the rapid growth of IoT devices and (in general) low priority given to embedded security in these devices and their operating systems. In one IoT attack case, a Vegas casino was attacked and the hacker gained entry via an internet-connected thermometer inside one of the casino’s fishtanks.

Best practices to help prevent an IoT attack include updating the OS and keeping a strong password for every IoT device on your network, and changing passwords often.

Incident Response-

Incident categories**,** Incident response Incident recovery, and **Operational security protection**: Digital and data assets, ports and protocols, Protection technologies, Identity and access Management, configuration management.

UNIT-1

1.Cyber security objectives

The ultimate goal of cyber security is to protect the information from being stolen or compromised. To achieve this we look at 3 fundamental goals of cybersecurity.

1. Protecting the Confidentiality of data

2. Preserving the Integrity of data

3. Restricting the Availability of data only to authorized users

1. Confidentiality

The central idea behind the term confidentiality in the CIA Triad. The CIA Triad ensures that the data is only accessible by genuine authorized users. It helps in preventing disclosure to unintended parties who might exploit the privacy of the user.

Methods to ensure Confidentiality are :

1. Encryption of raw data
2. Using biometrics for authentication
3. Two way or multifactor authentication

   Let us say you work as a security engineer for a renowned financial firm with many competitors across the globe. An anonymous entity is trying to access the company's trade secrets. You must make sure that the confidential information is not accessible to any unauthorized outsiders.

   Hence you implement Firewall and intrusion detection systems. This is a typical example of holding the confidentiality of your company.

2. Integrity

Integrity is making sure the data is unaltered during the time of transmission and ensuring it reaches the end-user in the correct form. It maintains the consistency and reliability of data.

Methods to ensure Integrity are :

1. Making use of user access control to restrict unauthorized modification of files.
2. Setting up backups to restore data during any system failure.
3. Version control systems help to identify any modification by tracing the logs.

Now being the same security engineer of the same financial firm, you have to ensure that users are not destroying the data that the company holds.

Some users may accidentally or intentionally alter the database and corrupt the data to cause loss to the firm.

You need to ensure that the backups are in place for implementation during such emergencies.

You may use File Integrity Monitors(FIM) and hashing functions to make sure the data is un-tampered and safe.

3. Availability

The last component of the CIA Triad – Availability helps in delivering resources as and when requested by the user without any intervention like Denial of Service warnings.

Methods to ensure Availability are :

1. Installing firewalls, proxy servers during downtime.
2. Locating backups at geographically isolated locations.

Lastly, consider your task this time is to ensure the website of your firm is functioning properly 24/7 without any hindrance.

Organizations that deal with financial transactions cannot take any chances to face downtime as it will cause huge losses, hold the customers' assets at stake and reduce trust in the organization.

During such times, when the server crashes you need to have a second one that you replace the services and keep the site up and running.

2.Different Job Roles In Cyber Security

Cyber security is a vital area in this advanced world. With a surge of cyber attacks nowadays, ensuring the safety of your and your clients data has become a must-have for all companies. There are many different types of cyber security jobs available, some more technical than others. Often, you will need to have a few years of specialized education or training under your belt before you can apply for these positions, but even entry level jobs in the cyber security industry are still very lucrative.

There are many job titles and which are discussed below:

1. **Security Specialist –**
   Security specialist are the people who are responsible for their organizations security. They check the systems and the connections for any security vulnerability. The onset of cloud trend has boosted this role as a security specialist is required to assess the cloud systems regularly.

2. **Incident Responder –**
   Incident responders are people who not only detect the threats but also respond to them. These people help the organization and its employees to stay prepared and act when the security is breached.

3. **Security Administrator –**
   Security administrators are the most essential personnel. Their tasks include roles of multiple titles. They set up proper security guidelines for the flow of data and also are responsible for installing firewalls and malware blockers.

1. **Vulnerability Assessor –**
   Vulnerability assessor or vulnerable assessment analyst are people who run multiple tests on the systems. Their main aim is to find the critical flaws in the security system while also prioritizing things that affect the organization the most.

2. **Cryptographer –**
   Cryptographers are the people who use cryptography techniques to encrypt and decrypt the data keeping it hidden from irrelevant parties. They are very essential and are more in demand.

3. **Security Manager –** Security managers supervise the rest of the team. They take important decisions and oversee the whole team's work.

4.

5. **Security Architect –** As the name suggests security architect are people who design the security structure. They also test out the security and respond to threats.

6. **Security Analyst –** Security analysts analyze the systems and patch the loop holes. They often work together with the rest of the team of IT specialist and developers.

7. **Security Auditor –** Security auditor are the people who are tasked with finding the breach in the system first before anyone else does. They check whether the currently installed firewalls and other security measures are working properly or not.

8. **Forensic Expert –** Forensic expert are people who trace back the hacks and breaches. They investigate cyberattacks or any other illegal activity taking place online. They try to revive any damaged or encrypted data related to the crime.

9. **Penetration Tester –** Penetration testers are people who are allowed to hack the system and try to find a way in. They act like hackers trying to attack the security system.

10. **Security Consultant –** Security consultant are people who assess the systems and suggest new improvements while pointing out the flaws. These people generally work as freelancers to develop a security plan.

11. **Security Engineer –** Security engineers patch, maintain and remove stuffs on the system. They work directly on the system and are responsible for the modification of the system.

Difference between Cyber Security and Information Security

- Last Updated : 07 Jul, 2022

The terms **Cyber Security** and **Information Security** are often used interchangeably. As they both are responsible for the security and protecting the computer system from threats and information breaches and often Cyber security and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously. If we talk about data security it's all about securing the data from malicious users and threats. Now another question is what is the difference between Data and Information? So one important point is that "not every data can be information" data can be informed if it is interpreted in a context and given meaning. for example **"100798"** is data and if we know that it's the date of birth of a person then it is information because it has some meaning. so information means data that has some meaning.

Examples and Inclusion of Cyber Security are as follows:

- Network Security
- Application Security
- Cloud Security
- Critical Infrastructure

Examples and inclusion of Information Security are as follows:

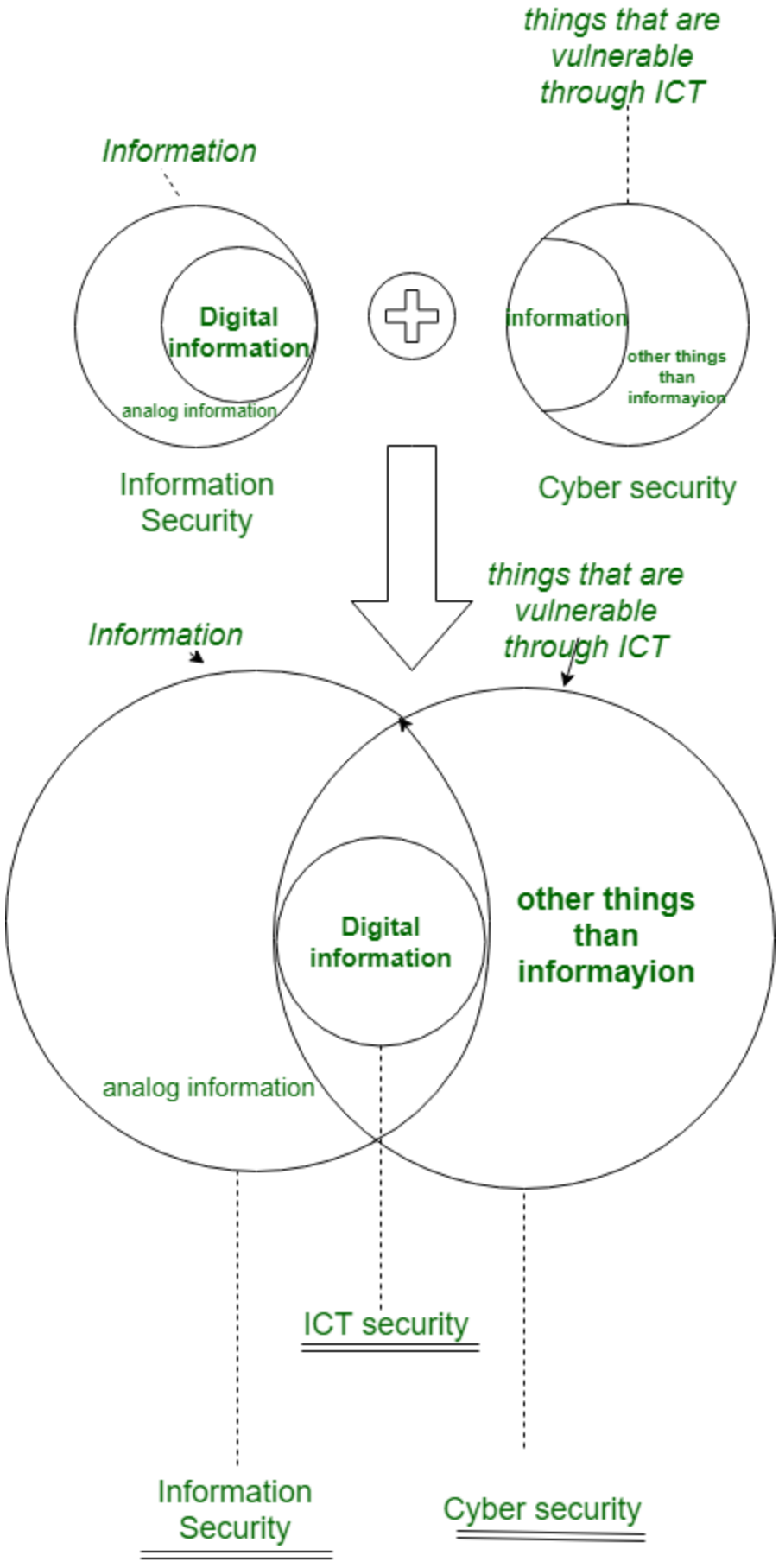
- Procedural Controls
- Access Controls
- Technical Controls
- Compliance Controls

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity,

Parameters	CYBER SECURITY	INFORMATION SECURITY
		and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and

Parameters	CYBER SECURITY	INFORMATION SECURITY
		availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.

Diagrams are given below to represent the difference between *Information Security* and *Cybersecurity*.


things that are vulnerable through ICT
Information
Digital information
analog information
information
other things than informayion
Information Security
Cyber security
things that are vulnerable through ICT
Information
Digital information
other things than informayion
analog information
ICT security
Information Security
Cyber security

In the above diagram, **ICT** refers to Information and communications technology (ICT) which is an extensional term for information technology (IT) that defines the role of unified communications and the integration of telecommunications (basically digital communication security).

Cyber security Principles

The purpose of the cyber security principles is **to provide strategic guidance on how an organisation can protect their systems and data from cyber threats**. These cyber security principles are grouped into four key activities: govern, protect, detect and respond. Govern: Identifying and managing security risks.

What is the CIA triad?

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. Although elements of the triad are three of the most foundational and crucial cybersecurity needs, experts believe the CIA triad needs an upgrade to stay effective.

In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Confidentiality, integrity, availability

The following is a breakdown of the three key concepts that form the CIA triad:

- **Confidentiality** is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.

- **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
- **Availability** means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

The three CIA triad principles

Why is the CIA triad important?

With each letter representing a foundational principle in cybersecurity, the importance of the CIA triad security model speaks for itself. Confidentiality, integrity and availability together are considered the three most important concepts within information security.

Considering these three principles together within the framework of the "triad" can help guide the development of security policies for organizations. When evaluating needs and use cases for potential new products and technologies, the triad helps organizations ask focused questions about how value is being provided in those three key areas.

Thinking of the CIA triad's three concepts together as an interconnected system, rather than as independent concepts, can help organizations understand the relationships between the three.

What are examples of the CIA triad?

Here are examples of the various management practices and technologies that comprise the CIA triad. While many CIA triad cybersecurity strategies implement these technologies and practices, this list is by no means exhaustive.

Confidentiality

Sometimes safeguarding data confidentiality involves special training for those privy to sensitive documents. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods to prevent users from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure confidentiality is requiring an account number or routing number when banking online. Data encryption is another common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication (2FA) is becoming the norm. Other options include Biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, such as storing only on air-gapped computers, disconnected storage devices or, for highly sensitive information, in hard-copy form only.

Integrity

These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem. In addition, organizations must put in some means

to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash.

Data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state. Furthermore, digital signatures can be used to provide effective nonrepudiation measures, meaning evidence of logins, messages sent, electronic document viewing and sending cannot be denied.

Availability

This is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a properly functioning operating system (OS) environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important tactics. Redundancy, failover, RAID -- even high-availability clusters -- can mitigate serious consequences when hardware issues do occur.

Fast and adaptive disaster recovery is essential for the worst-case scenarios; that capacity relies on the existence of a comprehensive DR plan. Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data blocked by malicious denial-of-service (DoS) attacks and network intrusions.

Special challenges for the CIA triad

Big data poses challenges to the CIA paradigm because of the sheer volume of information that organizations need safeguarded, the multiplicity of sources that data comes from and the variety of formats in which it exists. Duplicate data sets and disaster recovery plans can multiply the already-high costs. Furthermore,

because the main concern of big data is collecting and making some kind of useful interpretation of all this information, responsible data oversight is often lacking. Whistleblower Edward Snowden brought that problem to the public forum when he reported on the National Security Agency's collection of massive volumes of American citizens' personal data.

Internet of things privacy protects the information of individuals from exposure in an IoT environment. Almost any physical or logical entity or object can be given a unique identifier and the ability to communicate autonomously over the internet or a similar network. The data transmitted by a given endpoint might not cause any privacy issues on its own. However, when even fragmented data from multiple endpoints is gathered, collated and analyzed, it can yield sensitive information.

Internet of things security is also challenging because IoT consists of so many internet-enabled devices other than computers, which often go unpatched and are often configured with default or weak passwords. Unless adequately protected, IoT could be used as a separate attack vector or part of a thingbot.

As more and more products are developed with the capacity to be networked, it's important to routinely consider security in product development.

Best practices for implementing the CIA triad

In implementing the CIA triad, an organization should follow a general set of best practices. Some best practices, divided by each of the three subjects, include:

Confidentiality

- Data should be handled based on the organization's required privacy.
- Data should be encrypted using 2FA.
- Keep access control lists and other file permissions up to date.

Integrity

- Ensure employees are knowledgeable about compliance and regulatory requirements to minimize human error.
- Use backup and recovery software.
- To ensure integrity, use version control, access control, security control, data logs and checksums.

Availability

- Use preventive measures such as redundancy, failover and RAID. Ensure systems and applications stay updated.
- Use network or server monitoring systems.
- Ensure a data recovery and business continuity (BC) plan is in place in case of data loss.

History of the CIA triad

The concept of the CIA triad formed over time and does not have a single creator. Confidentiality may have first been proposed as early as 1976 in a study by the U.S. Air Force. Likewise, the concept of integrity was explored in a 1987 paper titled "A Comparison of Commercial and Military Computer Security Policies" written by David Clark and David Wilson. The paper recognized that commercial computing had a need for accounting records and data correctness. Even though it is not as easy to find an initial source, the concept of availability became more widespread one year later in 1988.

By 1998, people saw the three concepts together as the CIA triad.

what is authentication in cyber security?

Authentication is **the process of determining whether someone or something is, in fact, who or what it says it is**. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

What is an example of authentication?

In computing, authentication is the process of verifying the identity of a person or device. A common example is **entering a username and password when you log in to a website**.

non- repudiation.

Definition(s):

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

What is non-repudiation with example?

Nonrepudiation is **the property of agreeing to adhere to an obligation**. More specifically, it is the inability to refute responsibility. For example, if you take a pen and sign a (legal) contract your signature is a non repudiation device.

UNIT -2

Information Security (IS) within Lifecycle Management

What is information security simple definition?

Information security **protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction**. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

What is meaning of life cycle management?

IT system life-cycle management is **the administration of a system from provisioning, through operations, to retirement**. Every IT system, resource, and workload has a life cycle. Life-cycle management lets you: Reliably create systems in an automated and scalable manner.

What is information lifecycle management (ILM)?

Information lifecycle management (ILM) is a comprehensive approach to managing an organization's data and associated metadata, starting with its creation and acquisition through when it becomes obsolete and is deleted. An effective ILM strategy can help lower storage and data management costs, as well as reduce the security, compliance and legal risks that come with failing to maintain full control over organizational data.

Unlike earlier approaches to data storage management, ILM deals with all aspects of data throughout its life span, rather than focusing only on one facet of data management. For example, hierarchical storage management is concerned only with automating storage processes and not with how data is transformed or used. ILM addresses how data is utilized and many other issues. In addition, ILM enables more complex criteria for storage management than systems that rely only on basic metrics, such as data age or access frequency.

The traditional data lifecycle

How information lifecycle management works

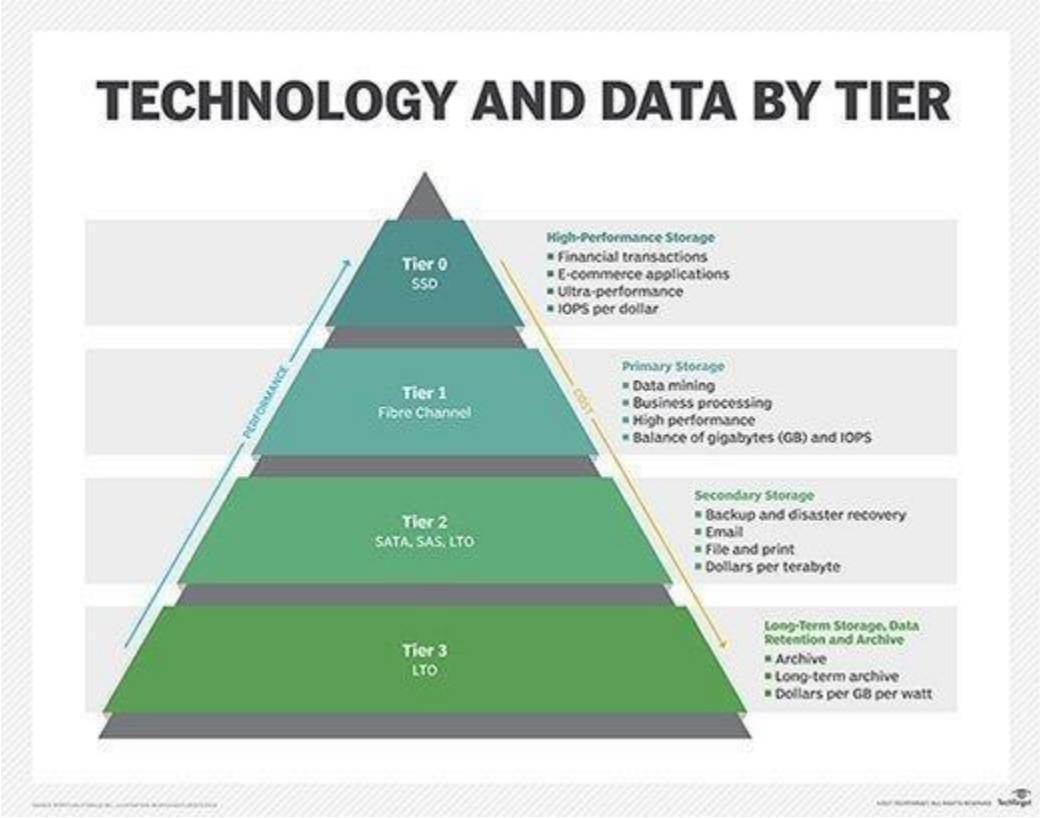
Information lifecycle management takes a policy-based approach to handling data, providing a centralized, consistent strategy for managing the entire data lifecycle. ILM also facilitates automation and storage tiering. In this way, data can be automatically migrated from one storage tier or format to another based on the applicable policies. As a rule, newer data and data that must be accessed more frequently are stored on faster, more expensive storage media, while less-critical data is stored on slower and cheaper media.

The ILM approach enables IT teams to specify different policies for different types of data throughout its life span. ILM takes into account that data declines in value at different rates, with some types of data retaining its value much longer than other types. In some cases, ILM might also incorporate path management

capabilities, which make it easier to retrieve stored data by tracking where it is in the storage cycle.

To be effective, however, ILM needs to be an organization-wide effort, involving procedures and practices, as well as applications and technology platforms. That ability to better track and retrieve information provides a key benefit for IT, the legal team and the business when faced with e-discovery requests, according to consultancy Deloitte.

Deloitte also noted that ILM can introduce "management rigor and controls" of information for the entire business.



Information lifecycle management facilitates automation and storage tiering.

Information lifecycle management vs. data lifecycle management

ILM is commonly confused with data lifecycle management (DLM). In fact, the two terms are often used interchangeably; however, they're not the same thing. One way to look at ILM is as a more complex subset of DLM.

So, while DLM products deal with general attributes of files, such as their type, size and age, ILM provides more complex capabilities.

Think of DLM as being concerned with data sets as a whole. However, ILM focuses on what's inside those data sets, such as the information in document files. For example, a DLM product would enable a user to search for a certain file type of a certain age, but an ILM product would enable the user to search through multiple file types for instances of a specific piece of information, such as a customer number and, subsequently, the data associated with that customer account.

The type of control that ILM can provide has become increasingly important as more regulations have been enacted. The European Union's General Data Protection Regulation (GDPR), for example, guarantees an individual's right to be forgotten, and the California Consumer Privacy Act specifies that an individual has the right to know about the personal information that a business collects and how that information is used and shared. An ILM product can help locate the individual's personal data, but a DLM product cannot.

What are the phases of the information lifecycle?

The ILM process is often described in terms of the phases, or stages, that data passes through as part of the information lifecycle. Different resources often define these phases in different ways, although many of them are usually close in concept. The following seven phases provide a general overview of what happens with data during its lifecycle:

1. **Capture data.** Organizations continuously create data and collect data from external sources. That data might be generated manually or automatically. Data sources can include social media, industrial internet of things (IoT), corporate collateral, user-generated content, customer input, sales records or a wide range of other sources.
2. **Store data.** Organizations that create and collect data must find ways to effectively store that data. They might store the data in file, block or object storage systems. They might use different types of storage media and configurations, such as network-attached storage or storage area networks. They might store their data on premises, in the cloud or a combination of both.
3. **Manage data.** It's not enough to simply store data. Organizations must also be able to effectively manage that data. They must ensure the data's security, availability and compliance with corporate, industry and government regulations. They might also classify the data, compress or deduplicate the data, or implement a system for monitoring their data and storage systems.
4. **Transform data.** Few organizations simply capture and store data without transforming it in various ways to make it easier to access and understand. As part of this process, they might cleanse, filter, aggregate, enrich, merge or, in some other way, modify the data to meet their business needs.
5. **Use data.** The purpose of capturing, storing and transforming data is to ensure that users and applications have the data they need to conduct business and carry out their assigned tasks. During this phase, users might view, modify, share or collaborate on data. They might also analyze data or use it to generate reports.
6. **Archive data.** Once data is no longer needed on a daily basis, it is often archived in case it's required for future business needs or to meet regulatory or legal requirements. Organizations typically use slower and cheaper storage systems because data access requirements are minimal. Although archiving data can be an important phase in the ILM process, not all data needs to be archived. For example, data collected by IoT devices might

need to be retained only if anomalies have been discovered or only until it has been aggregated and analyzed.

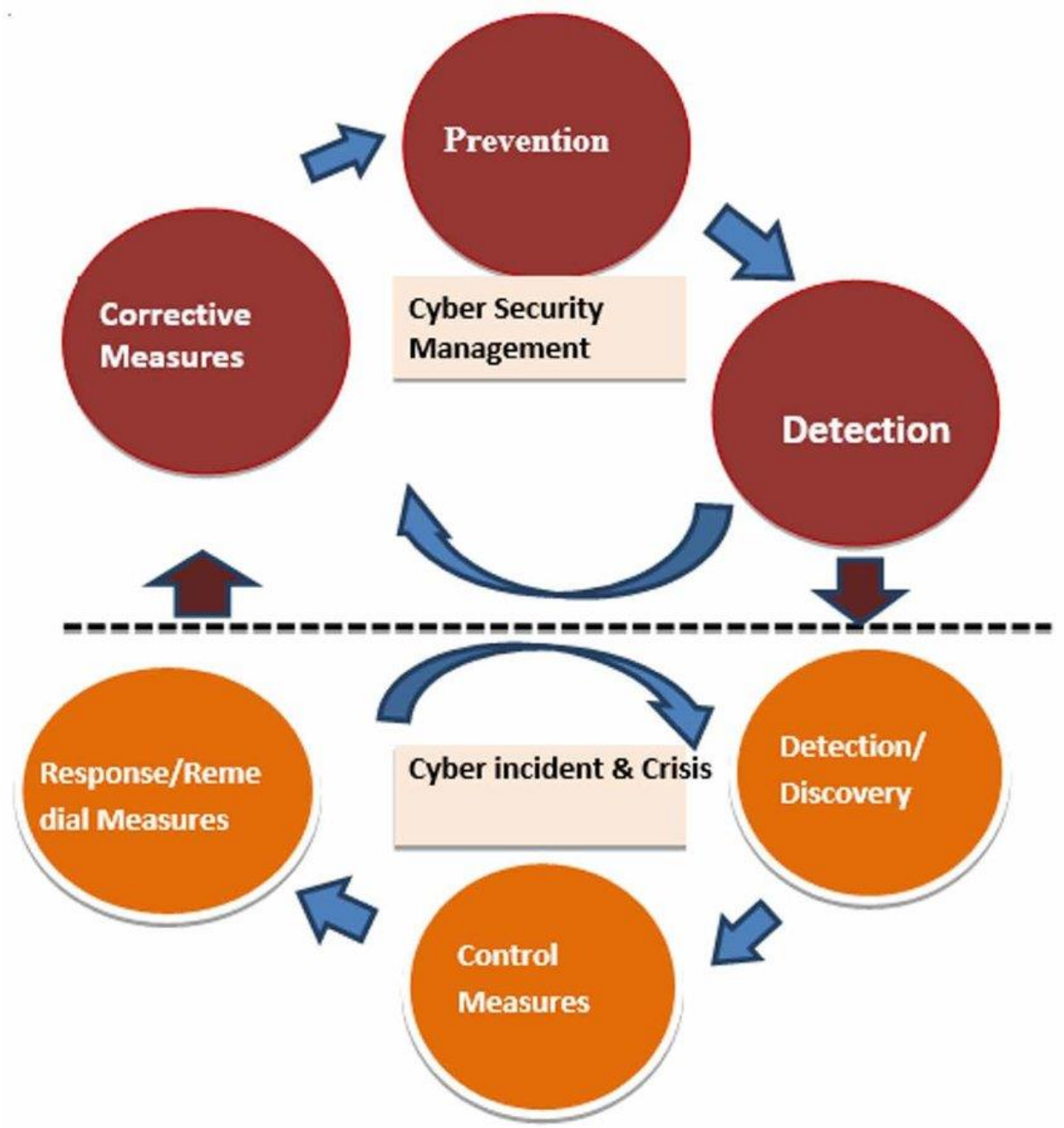
7. **Destroy data.** When an organization is certain that the data is no longer needed and it's not subject to regulatory or legal requirements, it is considered to be at the end of its useful life and can be deleted. The destruction phase is an important step in the ILM process because it reduces the amount of data that has to be stored and the organization's potential liability. All data maintenance and storage come with overhead and costs, even if the data is not needed, so the sooner that data can be safely deleted, the better. In addition, if data is not deleted in a timely manner, it can make it more difficult to work with the current data and make informed business decisions based on that fresh data.

Stages of the content management lifecycle

Although data typically passes through all seven stages, this process should not be thought of as a strictly linear flow of information. For example, data creation and collection are ongoing operations that can occur as some of the data passes through other phases. In addition, data might be transformed before it is stored, after it is stored or both before and after. Meanwhile, data use might come right after data is stored, right after it's transformed or both. Data might even be used after it has been archived.

The only phase that consistently follows a linear pattern is the last phase, in which data is deleted.

Lifecycle management landscape



Prevention is **the key to reducing the risk of a data breach**. By investing in cybersecurity software, using a VPN, and being aware of common attack methods, individuals and organizations can deter hackers and keep their data private.

Example:

- Train your staff. ...
- Keep your software and systems fully up to date. ...
- Ensure Endpoint Protection. ...
- Install a Firewall. ...
- Backup your data. ...
- Control access to your systems. ...
- Wifi Security.

cyber security management

Cybersecurity management is an area of information technology that organizations and businesses use to protect and secure sensitive information from cybercriminals or any unwanted guests.

What is corrective cyber security?

Corrective security controls include **technical, physical, and administrative measures that are implemented to restore the systems or resources to their previous state after a security incident or an unauthorized activity**.

What is detection in cyber security?

Threat detection is **the practice of analyzing the entirety of a security ecosystem to identify any malicious activity that could compromise the network**. If a threat is detected, then mitigation efforts must be enacted to properly neutralize the threat before it can exploit any present vulnerabilities.

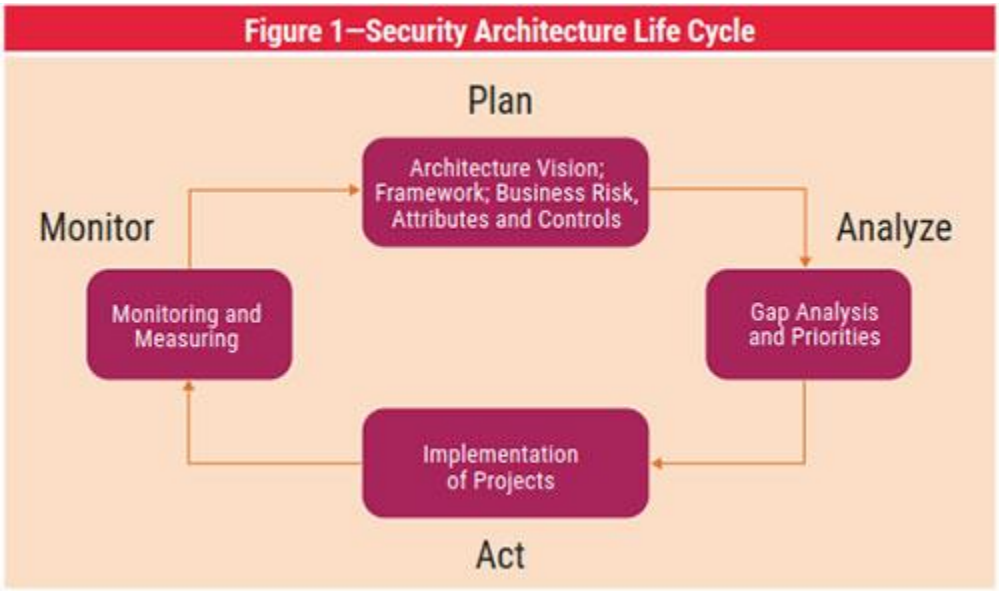
A cyber crisis is **when an IT system fails and becomes unavailable, potentially resulting in serious disturbance to your organisation**. Normal business processes are not enough to mitigate such consequences.

What are the types of response process in cyber security incidents?

This article reviews the steps in the SANS incident response process, including **preparation, identification, containment, and eradication**. An incident response plan is a documented, systematic process that defines how your organization should deal with a cybersecurity incident.

Incident is: Situation that might be, or could lead to, a disruption, loss, emergency or crisis. Crisis is: A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organization and requires urgent action.

Security architecture processes



Security architecture tools

Security architecture forms the foundation of a good cyber security strategy. It is **a type of security design composed of multiple components, including the tools, processes, and technologies used to protect your business from external threats**.

Introduction to Security Architecture

Security architecture is defined as the architectural design that includes all the threats and potential risks which can be present in the environment or

that particular scenario. This also includes the security controls and the use of security controls. For the security architecture, the proper documentation is done that include all the security specifications and include all the detailed information about the architecture. The organization uses for their system, and it is mainly used because the architecture is affordable and cost-effective and can be used easily by the organization.

Security Architecture with Diagram

This is defined as the part of enterprise architecture that is particularly design for addressing the information system and fulfill the security requirements of the organization. The system architecture system has a role that it meets the security requirements and also helps to protect the company operating environment. It is beneficial for the company as it includes other activities like risk management activities that require continuous improvement, and security architecture helps to meet the organization requirements. It defines proper polices, rules and regulations that need to reinforce in the organization and provide proper information about them. The architecture is also used for allocating the controls for

technical security so that the information system of the organization can be maintained properly. As the same can be followed in a whole organization, it helps to define common regulations and standards for every employee so that everyone can follow the rules and maintain data integrity and security in the organization.

In the above diagram, the high-level design of the system architecture is shown. The abstraction is given here.

Components of Security Architecture

For making the security architecture important, there are certain components that are involved in the design. The components are people, process and the tools. All these components combine helps to protect the organization assets. After defining the components, the next step is to make the policy and the reinforcement technique for the policies. After the other important steps are the method procedural for the implementation of security architecture and how the architecture will get enforced. By this, the

overall design and architecture are designed for the organization that will protect them throughout their business operations. For a proper security architecture, some of the components are briefly discussed:

1. Guidance

The policies and procedures that act as the guidance should be design and implement properly. The policies should include the documentation that includes the objectives and goals for designing the architecture, standards, policies, rules and regulations for the organization, identification of scope and function, identification of other security policies.

2. Identity Management

It is the type of system that include the organization processes, technologies and policies that directly help users to gain access to the online applications and other network resources. For the organization, the proper responsibilities and roles need to be clearly stated, and individual tasks need to be designed for the employees.

3. Inclusion & Exclusion

The other components are the inclusion and exclusion that include the security of elements of the organization in which company resources are protected. The company resources include web resources, e-mail servers, private HR data and other reporting system information. The access should be grant to authorized users only so that the privacy and integrity can be maintained in the organization.

4. Access and Border Control

The organization should develop an architecture that is able to control the access to the business resources and can use the layer system for providing access to the company employees. Only authorized users should gain complete access to the system, and the rest should be provided with limited access of the system.

5. Validation of Architecture

As the technology advances, the company need to renew the policies and laws as per the changes, and continuous effort is needed by the

organization in this change. For that, the continuous monitoring is required, and according to that, proper changes can be made in the architecture.

6. Training

As for the organization, to maintain the privacy and integrity, the security architecture system is very important. AS there is a continuous change in the system, it becomes important that the employee should know about the changes and proper training is given to them so that they can use the system and protect the company assets and elements.

7. Technology

To reinforce the security architecture, the software and hardware used for making the architecture become very crucial for the organization. Because of continuous change in technology, there is a requirement of continuous change in the system so that the system can be up to date and help to make the system secure and private.

Benefits of Using the Security Architecture

Some of the benefits are mentioned below.

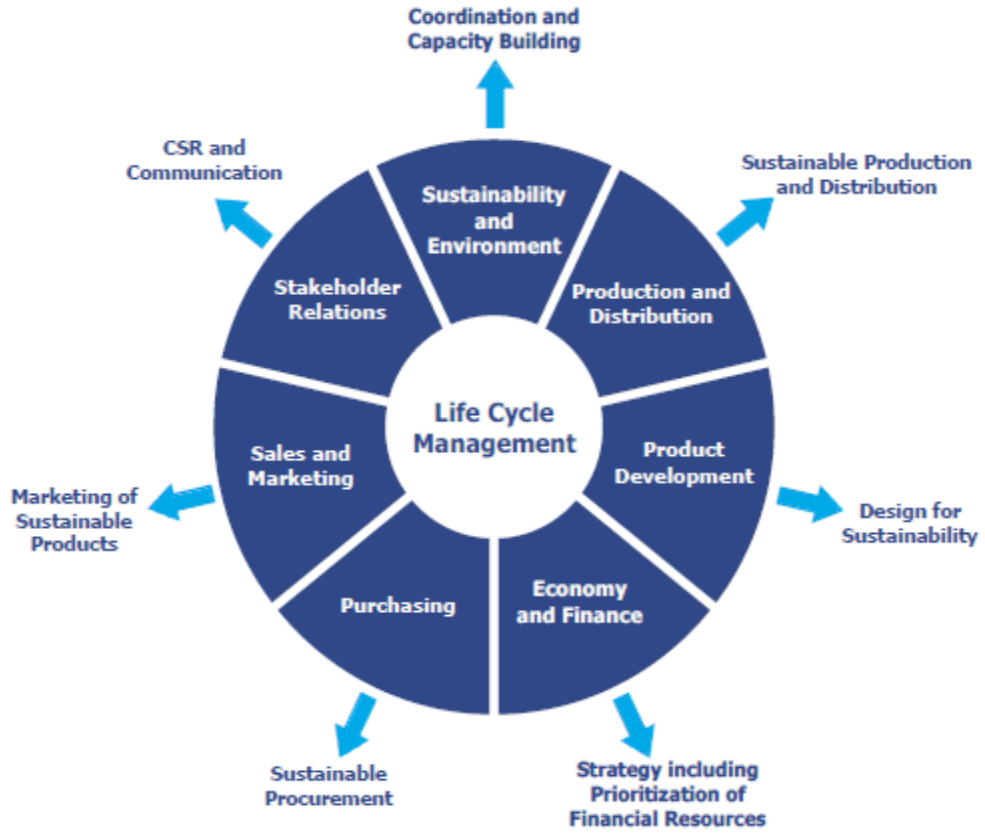
- Help to protect the important company assets from the outside and provide security to the important resources to the organization. The architecture provides the limited access to the user so that the confidential data can be kept secure and safe.
- The architecture defines the common policies and standards that can be used by the every employee of the company and also define common rules so that no one face any difficulty to use the system. It helps the organization to reach their goal and easily conduct their business operations smoothly.
- The other benefit is risk management activities covered by the architecture as the risk management activity requires continuous assistance and also need continuous improvement, the security architecture act as a better solution for them.

Conclusion

Security architecture is a type of enterprise architecture and is very important for the organization to protect the company resources from the outside world. A strong security architecture is used by the organization to

main security and data integrity in the system, and the policies and rules defined by the system are followed by the employee of an organization.

Intermediate lifecycle management concepts



Risks & Vulnerabilities

A threat exploits a vulnerability and can damage or destroy an asset. Vulnerability refers to a weakness in your hardware, software, or procedures. (In other words, it's a way hackers could easily find their way into your system.) And **risk refers to the potential for lost, damaged, or destroyed assets**.

Basics of risk management

There are five basic steps that are taken to manage risk; these steps are referred to as the risk management process. It begins with **identifying risks, goes on to**

analyze risks, then the risk is prioritized, a solution is implemented, and finally, the risk is monitored.

Operational threat environments

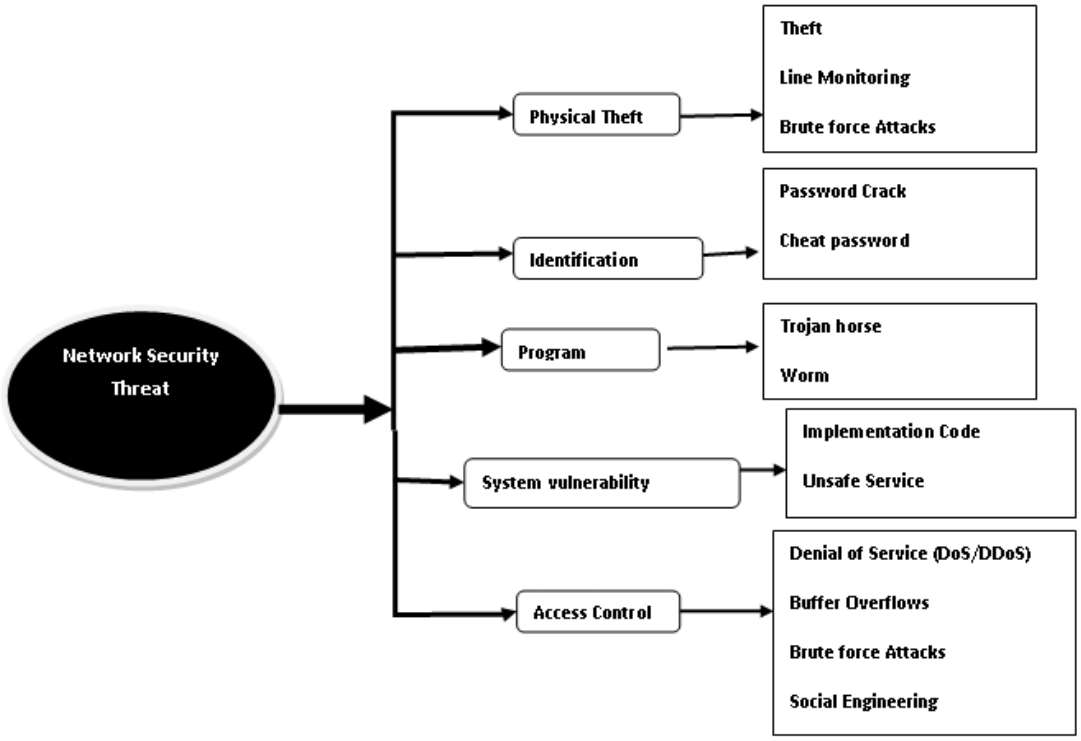
What is operational threat environment in cyber security?

The cyber threat environment is **the online space where cyber threat actors conduct malicious cyber threat activity.**

Classes of attacks

Malware.

- Phishing.
- Man-in-the-Middle (MitM) Attacks.
- Denial-of-Service (DOS) Attack.
- SQL Injections.
- Zero-day Exploit.
- Password Attack.
- Cross-site Scripting.



UNIT-3

1.What is an incident response plan?

An incident response plan is a set of tools and procedures that your security team can use to identify, eliminate, and recover from cyber security threats. It is designed to help your team respond quickly and uniformly against any type of external threat.

Incident response plans ensure that responses are as effective as possible. These plans are necessary to minimize damage caused by threats, including data loss, abuse of resources, and the loss of customer trust.

Incident response planning typically includes:

The organization's incident response strategy and how it supports business **objectives**

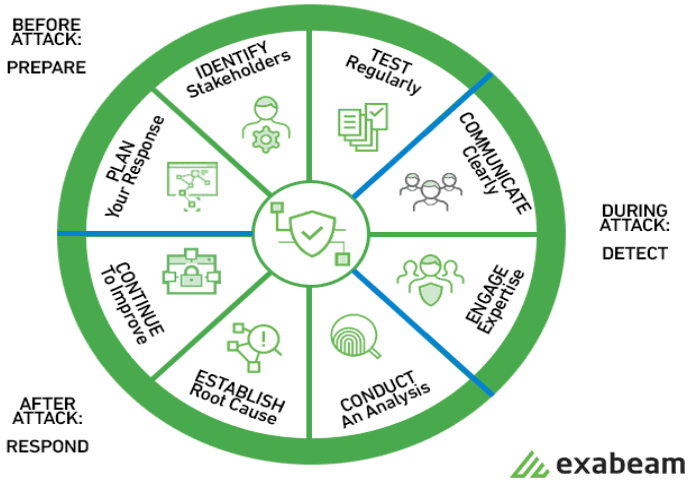
Roles and responsibilities involved in incident response

Procedures for each phase of the incident response process

Communication procedures within the incident response team, with the rest of the organization, and external stakeholders

How to learn from previous incidents to improve the organization's security posture

An incident response plan forms the basis of your incident response cycle:



6 steps of incident response

1. Preparation

At the preparation stage, you should review and codify the underlying security policy that informs your incident response plan. Perform a risk assessment and prioritize security issues, identify which are the most sensitive assets, and by extension, which are the critical security incidents the team should focus on. Create a communication plan, and prepare documentation that clearly and briefly states the roles, responsibilities, and processes.

Planning is not enough — you must also recruit members to the Cyber Incident Response Team (CIRT), train them, ensure they have access to all relevant systems, and the tools and technologies they need to identify and respond to incidents.

2. Identification

The team should be able to effectively detect deviations from normal operations in organizational systems and identify if those deviations represent actual security incidents.

When a potential incident is discovered, the team should immediately collect additional evidence, decide on the type and severity of the incident, and document everything they are doing. Documentation should answer “Who, What, Where, Why, and How” questions to allow the attackers to be prosecuted in court at a later stage.

3. Containment

Once the team identifies a security incident, the immediate goal is to contain the incident and prevent further damage from occurring. This involves:

Short-term containment — this can be as simple as isolating a network segment that is under attack or taking down production servers that have been hacked and are diverting traffic to backup servers.

Long-term containment — applying temporary fixes to affected systems to allow them to be used in production, while rebuilding clean systems, preparing to bring them online in the recovery stage.

4. Eradication

The team must identify the root cause of the attack, remove malware or threats, and prevent similar attacks in the future. For example, if a weak authentication mechanism was the entry point for the attack, it should be replaced with strong authentication; if vulnerability was exploited, it should be immediately patched.

5. Recovery

The team brings affected production systems back online carefully, to ensure another incident doesn’t take place. Important decisions at this stage are from which time and date to restore operations, how to test and verify that affected systems are back to normal and how long to monitor the systems to ensure activity is back to normal.

6. Lessons Learned

This phase should be performed no later than two weeks from the end of the incident, to ensure the information is fresh in the team's mind. The purpose of this phase is to complete documentation that could not be prepared during the response process and investigate the incident further to identify its full scope, how it was contained and eradicated, what was done to recover the attacked systems, areas where the response team was effective, and areas that require improvement.

2.Incident categories in cyber security

Security incidents indicate the failure of security measures or the breach of organizations' systems or data. This includes any event that threatens the integrity, availability, or confidentiality of information — or represents a violation or threat of violation to a law, security policy or procedure, or acceptable use policies. Causes of security incidents include anything from perimeter breaches and external attacks to insider threats or negligence.

Incidents usually require an IT administrator to take action. Incident response (IR) is an organized process by which organizations identify, triage, investigate scope, and direct mitigation or recovery from security incidents.

Types of security incidents

Security incidents can occur via a broad range of threat vectors. Here are a few of the most common cyber security threats and vulnerabilities:

Brute force attacks – Attackers use brute force methods to breach networks, systems, or services, which they can then degrade or destroy. For example, attackers use software that tests multiple passwords to guess the correct one. Another example is a distributed denial-of-service (DDoS) attack, which overwhelms the target system and causes it to deny access to users.

Email – attacks executed through an email message or attachments. Viruses posing as documents trick users into downloading an attachment and then take

control of the host. Email can also be abused via phishing. An attacker may request sensitive information or link to a website that appears legitimate, tricking the recipient into complying.

Web – attacks executed on websites or web-based applications. This could be via drive-by downloads from watering hole attacks, malicious scripts, popup alerts or supposedly legitimate user-initiated downloads. Beyond this lies the host of OWASP-based application vulnerabilities and misconfigurations. (Remember the Panama Papers? Application security matters!)

Loss or theft of equipment – A company device like a laptop or Smartphone is lost or stolen. Over 40 percent of small business owners, healthcare centers, and senior executives of all industries attribute their latest security incident to employee negligence or accidental loss, according to a 2018 study.

External/removable media – attacks executed using removable media like a flash drive or CD, or a peripheral device. Using removable media from an unidentified source can spread malware. One study revealed that users plug up to half of USB sticks found in office parking lots into their computers, enabling malware infection. (One supposes this is why many Macs no longer have USB drives.)

3.ports and protocols

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

What is a port number?

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices.

What are the different port numbers?

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol, are:

Ports 20 and 21: File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.

Port 22: Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.

Port 25: Simple Mail Transfer Protocol (SMTP). SMTP is used for email.

Port 53: Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.

Port 80: Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.

Port 123: Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption.

Port 179: Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.

Port 443: HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.

Port 500: Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.

Port 3389: Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

4.DIGITAL ASSETS

A digital asset is anything that exists in a digital format that has value. The number of digital assets on the internet is rapidly growing because the sheer number of digital devices we use—especially smart phones—is also growing exponentially.

Popular types of digital assets include the following:

PDFs

Videos

Images

Logos

Mobile apps

Spreadsheets

Emails

Websites

Blockchain-based assets

There are three key components that a digital asset must have to be considered a digital asset. Here's what they are:

It must have value.

It must be in a digital format.

It must be accessible, searchable, and distributable.

Companies often use many digital assets for different purposes, such as marketing, legal, sales, and tech initiatives.

The Importance of Digital Assets

Digital assets are important because they provide value to a company or individual. Investors are also becoming more interested in digital assets.

Digital assets are the heart of a company's brand and help them fuel online engagement. They can also be sold independently, meaning that a company can claim expenses and even make tax deductions regarding their digital assets. As the world is becoming more digital, owners of digital assets must treat them how they would treat physical assets.

While digital assets are receiving more attention, there's limited control over them due to a lack of regulation. Well, that's mostly because digital assets are still not widely understood by the government.

Potential Security Threats Regarding Digital Assets

Since digital assets are inherently valuable, they are more attractive in the eyes of a cybercriminal. For example, crypto investors must safeguard their assets, avoid scams, and take other cybersecurity measures to keep hackers at bay.

Phishing Attacks

Phishing attacks are a widely used attack method threat actors use to steal user data. These **types of attacks** have been prevalent for several years, and even though internet users today are more aware of phishing, cybercriminals have learned to target unsuspecting victims.

Phishing starts with a malicious email or email attachment that tricks you into downloading malware onto your device. For example, a cybercriminal may steal your username and password for a digital wallet platform where you store your crypto assets.

Ransomware

Another common cyberattack is a ransomware attack. This type of malware encrypts your data, making it impossible to access it until you pay the cybercriminal a costly fee. A cybercriminal may encrypt one of your digital assets and refuse to give you access to it until you pay up.

Data Breaches

Data breaches are fairly common, and they can target your digital assets. A data breach occurs when an unauthorized individual gains access to your asset, copies it, transmits it, or views it without your knowledge. Ledger, a well-known company that creates wallets for digital assets, once experienced a data breach that impacted roughly one million accounts.

5.What is IAM? Identity and Access Management Definitions

IAM is a framework of policies, processes, and technologies that enable organizations to manage digital identities and control user access to critical corporate information. By assigning users with specific roles and ensuring they have the right level of access to corporate resources and networks, IAM improves security and user experience, enables better business outcomes, and increases the viability of mobile and remote working and cloud adoption.

How Identity and Access Management Boosts Security

The core objective of an IAM platform is to assign one digital identity to each individual or a device. From there, the solution maintains, modifies, and monitors access levels and privileges through each user's access life cycle.

The core responsibilities of an IAM system are to:

Verify and authenticate individuals based on their roles and contextual information such as geography, time of day, or (trusted) networks

Capture and record user login events

Manage and grant visibility of the business's user identity database

Manage the assignment and removal of users' access privileges

Enable system administrators to manage and restrict user access while monitoring changes in user privileges

What is IAM Composed Of?

An IAM solution consists of various components and systems. The most commonly deployed include:

1. Single Sign-On

Single sign-on (SSO) is a form of access control that enables users to authenticate with multiple software applications or systems using just one login and one set of credentials. The application or site that the user attempts to access relies on a trusted third party to verify that the user is who they say they are, resulting in:

Enhanced user experience

Reduced password fatigue

Simplified password management

Minimized security risks for customers, partners, and vendors

Limited credential usage

Improvedidentityprotection

2. Multi-Factor Authentication

Multi-factor authentication verifies a user's identity with requirements to enter multiple credentials and provide various factors:

Something the user knows: a password

Something the user has: a token or code sent to the user via email or SMS, to a hardware token generator, or to an authenticator application installed on the user's smartphone

Something specific to the user, such as biometric information

3. Privileged Access Management

Privileged access management protects businesses from both cyber and insider attacks by assigning higher permission levels to accounts with access to critical corporate resources and administrator-level controls. These accounts are typically high-value targets for cybercriminals and, as such, high risk for organizations.

4. Risk-Based Authentication

When a user attempts to log in to an application, a risk-based authentication solution looks at contextual features such as their current device, IP address, location, or network to assess the risk level.

Based on this, it will decide whether to allow the user access to the application, prompt them to submit an additional authentication factor, or deny them access. This helps businesses immediately identify potential security risks, gain deeper insight into user context, and increase security with additional authentication factors.

5. Data Governance

Data governance is the process that enables businesses to manage the availability, integrity, security, and usability of their data. This includes the use of data policies and standards around data usage to ensure that data is consistent, trustworthy, and does not get misused. Data governance is important within an IAM solution as artificial intelligence and machine learning tools rely on businesses having quality data.

6. Federated Identity Management

Federated identity management is an authentication-sharing process whereby businesses share digital identities with trusted partners. This enables users to use the services of multiple partners using the same account or credentials. Single sign-on is an example of this process in practice.

7. Zero-Trust

A Zero-Trust approach moves businesses away from the traditional idea of trusting everyone or everything that is connected to a network or behind a firewall. This view is no longer acceptable, given the adoption of the cloud and mobile devices extending the workplace beyond the four walls of the office and enabling people to work from anywhere. IAM is crucial in this approach, as it allows businesses to constantly assess and verify the people accessing their resources.

Benefits of Using an Identity and Access Management System:
We will learn about the various organizational benefits in this section. These are listed below –

Reducerisk

You'll have more user control, which means you'll be less vulnerable to internal and external data breaches. When hackers utilize the user credential as a crucial technique to obtain access to the business network and resources, this is critical.

Secureaccess

When your company grows, you will have additional employees, customers, contractors, partners, etc. Your company's risk will increase at the same time, and you will have higher efficiency and production overall. IAM allows you to expand your business without compromising on security at the moment.

MeetingCompliance

A good IAM system can help a company meet its compliance requirements as well as meet the rapidly expanding data protection regulations.

MinimizeHelpDeskRequests

IAM looks into the user's needs and then resets the password and the help desk will help them automate the same. Getting the authentication requires the user to

verify their identity without bothering the system administrator as they need to focus on other things in the business, which gives more profit to the business.

6.Configuration Management?

Security configuration management is a process that involves adjusting the default settings of an information system in order to increase security and mitigate risk.

Security configuration management identifies misconfigurations of a system's default settings. Misconfigurations can lead to a host of problems, including poor system performance, noncompliance, inconsistencies and security vulnerabilities.

In routers or operating systems, for example, manufacturers often set the default configurations with predefined passwords or pre-installed applications. Accepting easily exploitable default settings can make it easy for attackers to gain unauthorized access to an organization's data and has the potential to cause catastrophic data loss.

Specialized configuration management tools allow security teams to understand what's changing in their key assets and detect a breach early. These tools typically perform the following tasks:

Classify and manage systems

Modify base configurations

Roll out new settings to applicable systems

Automate patches and updates

Identify problematic and noncompliant configurations

Access and apply remediation

Security configuration management has four phases

Planning.

This step involves developing policies and procedures for incorporating security configuration management into existing IT and other security programs, then disseminating this guidance throughout the organization.

Identifying and implementing configurations.

Creating, reviewing, approving and implementing a secure baseline configuration for the system is critical. The approach may address configuration settings, software loads, patch levels, the physical or logical arrangement of data, security control implementation and documentation.

Controlling configuration changes.

Organizations ensure that changes are formally analyzed for their impact on security — and later tested and approved prior to implementation. Organizations may employ a variety of restrictions on making changes to limit unauthorized or undocumented updates to the system.

Monitoring.

This phase identifies previously undiscovered or undocumented system components, misconfigurations, vulnerabilities and unauthorized changes — all of which can expose organizations to increased risk. Automated tools help organizations to efficiently identify when the system is not consistent with the approved baseline configuration and when remediation actions are necessary.

Security configuration management tools can address these challenges, providing a number of advantages for businesses.

Automation and visibility. Without a security configuration management tool, it’s nearly impossible to maintain secure configurations across servers, routers,

firewalls and switches. The right tool automatically brings misconfigurations into alignment while providing real-time visibility.

Heightened compliance. Security configuration management tools monitor an organization's compliance with both internal and external standards. This reduces the time to identify noncompliance, which helps avoid incurring costly penalties and fees.

Lower risk and faster recovery. Tools detect and quickly correct misconfigurations, thereby reducing organizational risk. This enables organizations to provide a higher level of service and faster recovery, since the correct configuration is documented and automated.

UNIT-4

1. Vulnerability management ?

A. Vulnerability management is a term that describes the various processes, tools, and strategies of identifying, evaluating, treating, and reporting on security vulnerabilities and misconfigurations within an organization's software and systems. In other words, it allows you to monitor your company's digital environment to identify potential risks, for an up-to-the-minute picture of your current security status.

What is considered vulnerability?

Any means by which an external threat actor can gain unauthorized access or privileged control to an application, service, endpoint, or server is considered vulnerability. Tangible examples include communication ports open to the internet, insecure configurations of either software or OSs, methods by which to gain privileged access through approved interaction with a given application or OS, and a susceptibility to allow malware to infect a system.

Security vulnerabilities

In broad terms, a vulnerability is a weakness—a flaw that can be exploited. In computer science, a security vulnerability is essentially the same thing. Security vulnerabilities are targeted by threat actors. These attackers attempt to find and exploit vulnerabilities to access restricted systems.

Vulnerability scanner

Identifying vulnerabilities throughout your systems, networks, and application requires specific tools. A vulnerability scanner is a program that is designed to move through your digital systems and discover any potential weaknesses, making vulnerability management possible.

Risk-based vulnerability management

An extension of vulnerability management, risk-based vulnerability management programs are designed to address the weaknesses inherent in digital systems, including software, hardware, and infrastructure. Risk-based vulnerability

management uses machine learning to extend vulnerability management beyond traditional IT assets, incorporating cloud infrastructure, IoT devices, web apps, and more. This allows businesses access to relevant insights across their entire attack surface.

Risk-based vulnerability management also allows for more accurate, risk-based prioritization. Your company can focus first on identifying and repairing the weaknesses that are most likely to result in a breach, leaving less-critical vulnerabilities for later.

Stages of vulnerability Management Process:

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

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

  Strong vulnerability management programs see each process (and any sub-processes) as a continual lifecycle designed to help improve security and reduce organizational risk found in the network environment. Strong programs see this as being a daily process rather than quarterly or annually.

2. Security Logs and Alerts in cyber security?

A. Alerting sends real-time alert messages that arrive as Simple Network Management Protocol (SNMP) traps from devices managed by a central management solution. An SNMP trap is a type of SNMP Protocol Data Unit (PDU) that acts as an unrequested message, notifying the network management system about a security event that requires attention. The message appears immediately on the management dashboard.

Logging is the collection of all entries contained in a device(s) log that an admin can view locally or through the central management solution as System Logging Protocol (Syslog) messages. These are extremely valuable for security breach investigations that require historical logs.

Logs are also essential when identifying operational trends, establishing baselines, and supporting internal audits. Sometimes, effective logging is the main reason a security incident has a low impact rather than a more damaging one. IT security can react before a severe data breach occurs when they detect it early.

Cyber Security Alerting & Logging (In 6 Steps)

The following six steps are essential to improving your corporate network security by maximising the benefits of security alerting and logging.

1. Understand ISO 27001 Compliance

ISO/IEC 27001:2013, also known as ISO 27001, is the international standard for information security. It establishes the specification for an Information Security Management System (ISMS).

ISO 27001 takes a best-practice approach that helps organisations manage their information security by addressing people, processes, and technology. ISO 27001 certifications are recognised globally and indicate that your ISMS operates with information security best practices.

Part of ISO 27000's information security standards is ISO 27001, a framework that aids organisations in establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving an ISMS.

2. Define Your Overall Alerting and Logging Policy

If it doesn't already, your organisation should have a defined strategy for alerting and monitoring. Your strategy should be based on business needs and risk assessment data regarding securing business services and assets.

The strategy should include regular device monitoring and logging events such as the following:

- Authentication and access to devices and services
- User activity and permissions changes
- Monitoring and logging of network communications to critical applications and services
- Malware, phishing and ransomware vulnerabilities

Your organization should also determine how to best collect and analyse your log data. Such analysis will enable your security team to detect and respond to security events. It also allows them to automate the majority of detection and remediation actions.

As your policies evolve, they will include additional ways to learn from security incidents. Your security team can refine alerting and logging to monitor your network better.

Alerting is defined by severity levels. For instance, when an interface goes down, that takes a higher priority than when an admin exits the global configuration. Using Cisco as a model, there are eight alert levels that IT security teams can use to set up and view real-time alerts:

- 0. Emergency
- 1. Alert
- 2. Critical
- 3. Error
- 4. Warning
- 5. Notice
- 6. Informational
- 7. Debug

With this model, the lower the alert number, the more important the message is. Emergency (0), Alert (1) and Critical (2) can indicate a security issue or that

something such as a device running out of memory, a process has crashed, or an interface has gone down.

3. Define Specific Devices and Services That Should Alert

Device alerting and logging to a centralised management solution should include all devices accessing the network, including endpoint devices such as mobile phones, laptops and tablets that are more often targeted by cybercriminals.

Be sure the following devices are included in your alerting and logging policies:

- Bring Your Own Device (BYOD)
- Business-critical applications
- Cloud Services
- Desktops
- Firewalls
- Internet of Things (IoT) devices
- Intrusion Prevention System (IPS) devices
- Intrusion Detection System (IDS) devices
- Laptops
- Mobile phones
- Routers
- Servers
- Switches
- Tablets

4. Define Security Events That Should be Alerted and Logged

Your security team must decide which security-related event types should be logged and at which alerting level. Many logs can be generated for events, processes, and applications (including successes and failures). Part of your event log monitoring and audit plan will include which events you want to configure to better detect these issues.

Some of the typical events include the following:

- Access privilege changes
- Antivirus and malware events
- Attempt to install a service or application
- Failed login attempts
- Firewall events

- Local user account creation
- Locked user accounts
- Scheduled tasks
- Services stopped, started, or disabled
- Software update events
- Time changes

5. Choose a Centralised Management Solution

Centralised network management software (NMS) solution allows for the early detection of network issues such as down devices or poor WAN performance. These alerts and logs report directly to the system and provide the automation and analytics needed to manage the system with ease.

A modern NMS solution can also aggregate all your security alerts into a 'single pane of glass', providing your security team with a centralised point for all potential security-related issues.

While there are many vendors of NMS, SolarWinds is a prime example of affordable and robust IT infrastructure management software. Solar Winds Security Event Manager monitors and manages the security of any IT environment, whether it operates on-premises, in the cloud, or in a hybrid model.

Some of SolarWinds security features include the following:

- **Access Rights Management** – Manage and audit access rights across the entire IT infrastructure.
- **Security Event Management** – Improve security posture and demonstrate compliance using a ready-to-use, affordable event management and security solution.
- **Server Configuration Monitoring** – Detect and compare configuration changes to network databases, servers, and applications.
- **Patch Management** – Patch management software efficiently addresses software vulnerabilities.

6. Testing of Real-Time Alerting and Historical Logging

Once your IT security team has configured all devices per the alerting and monitoring policies, they should conduct regular tests to ensure that those configurations are alerting correctly and that the alerts are reporting to the centralised management solution.

Likewise, IT security should check if Syslog logging is functioning correctly to ensure all devices on the network are logging to your centralised NMS. If they are not, you won't be able to troubleshoot past security events and compliance guidelines properly.

Conclusion

In conclusion, monitoring, logging, and alerting are vital for IT security teams to identify activity patterns and security root causes on their network. When a security incident occurs, properly logged, real-time alert information is crucial to determine the source and the extent of the breach.

Regular logging is also required to better understand security incidents during an active investigation as well as the post-mortem analysis of the event.

3. Network traffic Analysis in cyber security?

A Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues. Common use cases for NTA include:

- Collecting a real-time and historical record of what's happening on your network
- Detecting malware such as ransom ware activity
- Detecting the use of vulnerable protocols and ciphers
- Troubleshooting a slow network
- Improving internal visibility and eliminating blind spots

Implementing a solution that can continuously monitor network traffic gives you the insight you need to optimize network performance, minimize your attack surface, enhance security, and improve the management of your resources. However, knowing how to monitor network traffic is not enough. It's important

to also consider the data sources for your network monitoring tool; two of the most common are flow data (acquired from devices like routers) and packet data (from SPAN, mirror ports, and network TAPs).

The key benefits of network traffic analysis:

With the "it's not if, it's when" mindset regarding cyber attacks today, it can feel overwhelming for security professionals to ensure that as much of an organization's environment is covered as possible. The network is a critical element of their attack surface; gaining visibility into their network data provides one more area they can detect attacks and stop them early. Benefits of NTA include:

- Improved visibility into devices connecting to your network (e.g. IoT devices, healthcare visitors)
- Meet compliance requirements
- Troubleshoot operational and security issues
- Respond to investigations faster with rich detail and additional network context

A key step of setting up NTA is ensuring you're collecting data from the right sources. Flow data is great if you are looking for traffic volumes and mapping the journey of a network packet from its origin to its destination.

Packet data extracted from network packets can help network managers understand how users are implementing/operating applications, track usage on WAN links, and monitor for suspicious malware or other security incidents.

The importance of network traffic analysis:

- Keeping a close eye on your network perimeter is always good practice. Even with strong firewalls in place, mistakes can happen and rogue traffic could get through. Users could also leverage methods such as tunneling, external anonymizers, and VPNs to get around firewall rules.
- Additionally, the rise of ransom ware as a common attack type in recent years makes network traffic monitoring even more critical. A network monitoring

solution should be able to detect activity indicative of ransom ware attacks via insecure protocols.

- Remote Desktop Protocol (RDP) is another commonly targeted application. Make sure you block any inbound connection attempts on your firewall. Monitoring traffic inside your firewalls allows you to validate rules, gain valuable insight, and can also be used as a source of network traffic-based alerts.

  Watch out for any suspicious activity associated with management protocols such as Telnet. Because Telnet is an unencrypted protocol, session traffic will reveal command line interface (CLI) command sequences appropriate for the make and model of the device. CLI strings may reveal login procedures, presentation of user credentials, commands to display boot or running configuration, copying files, and more. Be sure to check your network data for any devices running unencrypted management protocols, such as:
  - Telnet
  - Hypertext Transport Protocol (HTTP, port 80)
  - Simple Network Management Protocol (SNMP, ports 161/162)
  - Cisco Smart Install (SMI port 4786)

What is the purpose of analyzing and monitoring network traffic?

Many operational and security issues can be investigated by implementing network traffic analysis at both the network edge and the network core. With the traffic analysis tool, you can spot things like large downloads, streaming or suspicious inbound or outbound traffic. Make sure you start off by monitoring the internal interfaces of firewalls, which will allow you to track activity back to specific clients or users.

NTA also provides an organization with more visibility into threats on their networks, beyond the endpoint. With the rise in mobile devices, IoT devices, smart TV's, etc., you need something with more intelligence than just the logs from firewalls. Firewall logs are also problematic when a network is under attack. You may find that they are inaccessible due to resource load on the firewall or that they've been overwritten (or sometimes even modified by hackers), resulting in the loss of vital forensic information.

Some of the use cases for analyzing and monitoring network traffic include:

- Detection of ransomware activity
- Monitoring data exfiltration/internet activity
- Monitor access to files on file servers or MSSQL databases
- Track a user's activity on the network, though User Forensics reporting
- Provide an inventory of what devices, servers and services are running on the network
- Highlight and identity root cause of bandwidth peaks on the network
- Provide real-time dashboards focusing on network and user activity
- Generate network activity reports for management and auditors for any time period.

What to look for in a network traffic analysis and monitoring solution

Not all tools for monitoring network traffic are the same. Generally, they can be broken down into two types: flow-based tools and deep packet inspection (DPI) tools. Within these tools you'll have options for software agents, storing historical data, and intrusion detection systems. When evaluating which solution is right for your organization, consider these five things:

- **Availability of flow-enabled devices:**
  Do you have flow-enabled devices on your network capable of generating the flows required by a NTA tool that only accepts flows like Cisco Net flow? DPI tools accept raw traffic, found on every network via any managed switch, and are vendor independent. Network switches and routers do not require any special modules or support, just traffic from a SPAN or port mirror from any managed switch.

- **The data source:** Flow data and packet data come from different sources, and not all NTA tools collect both. Be sure to look through your network traffic and decide which pieces are critical, and then compare capabilities against the tools to ensure everything you need is covered.

- **The points on the network:** Consider whether the tool uses agent-based software or agent-free. Also be careful not to monitor too many data sources right out the gate. Instead, be strategic in picking locations where data converges, such as internet gateways or VLANs associated with critical servers.

- **Real-time data vs. historical data:** Historical data is critical to analyzing past events, but some tools for monitoring network traffic don't retain that data as time goes on. Also check whether the tool is priced based on the amount of data you want to store. Have a clear understanding of which data you care about most to find the option best suited to your needs and budget.

- **Full packet capture, cost and complexity:** Some DPI tools capture and retain all packets, resulting in expensive appliances, increased storage costs, and much training/expertise to operate. Others do more of the 'heavy lifting,' capturing full packets but extracting only the critical detail and metadata for each protocol. This metadata extraction results in a huge data reduction but still has readable, actionable detail that's ideal for both network and security teams.

4. What is packet capture and analysis?

A. Packet Capture Definition

Packet capture is a networking practice involving the interception of data packets travelling over a network. Once the packets are captured, they can be stored by IT teams for further analysis. The inspection of these packets allows IT teams to identify issues and solve network problems affecting daily operations.

What is packet capture used for?

Packet capturing helps to analyze networks, manage network traffic, and identify network performance issues. It allows IT teams to detect intrusion attempts, security issues, network misuse, packet loss, and network congestion. It enables network managers to capture data packets directly from the computer network. The process is known as packet sniffing.

IT teams prefer using packet monitor to perform crucial tasks, such as:

- Monitoring WAN utilization
- Monitoring bandwidth and traffic volume
- Tracking network usage
- Isolating compromised systems
- Demonstrating compliance
- Detecting suspicious content

Importances of packet capture monitoring?

Packet capture enables teams to deal with complex network issues with ease and efficiency. Management of organizations' networks is daunting. It involves checking client IP addresses, DNS servers, and more following the standard tests to identify the root cause of the issues.

Here's when the packet capture system greatly helps. A packet monitoring tool can collect and such analyze packet data and handle complex network issues quickly. It provides in-depth packet information as source and destination of IP addresses, time of capture, protocol information, and more.

Advantages of packet capture:

Enhance your organization's security:

Packet analysis helps in identifying security flaws, breaches, and more. It can detect intrusions, security incidents, and sudden spikes in network traffic.

Identify data leaks: Packet analysis and monitoring help IT teams to understand data leakage points and identify the root cause of the issues.

Locate packet loss: Packet capture monitoring enables IT teams to retrieve stolen, lost, or exfiltrated data packets by providing a series of events.

Improve network troubleshooting: Packet capture monitoring provides full visibility into network resources that help network teams improve troubleshooting efforts.

5. What are Monitoring Tools and Appliances in cyber security?

A. Cyber security software is a must for ensuring business and individuals security and privacy. It is a method to protect networks, systems and applications from cyber-attacks. It helps to avoid unauthorized data access, cyber attacks and identify stealing. Application, information , operational and network security, Disaster recovery are different parts of cyber security. They are required to maintain

systems protected from various cyber threats like Ransomware, malware, social engineering and phishing.

List of Top 10 Cyber Security Monitoring Tools

1. SolarWinds Security Event Manager –

- Ideally well suited for small to large businesses.
- It is a network and host intrusion detection system.
- It performs real time monitoring, response, and reporting of security threats.
- Some of its features are highly indexed log search capabilities, cloud based, scalable, threat intelligence is continuously updated, security information and event manager, log correlation, and log event archival, comprehensive set of integrated tools

2. Intruder

- It is ideal for small to large businesses.
- It is one of the most popular cloud-based network vulnerability scanners which helps to identify cybersecurity weaknesses in exposed systems.
- Some of its features are 9,000 security vulnerabilities, unlimited scans on demand, unlimited user accounts, check for web application flaws such as SQL injection and cross site scripting, emerging threats advanced notifications, smart recon, network view and PCI ASV scans are supported.

3. Syxsense

- It is ideal for small to large businesses.
- It provides security scanning, patch management and remediation on one console from the cloud and allows IT and security teams to stop breaches.
- Some of its features are security scanner by scanning authorization issues, security implementation, and antivirus status, automatically deploy OS and 3rd party patches including Windows 10 updates, blocks communication from an infected device to the Internet, isolation of endpoint and kill malicious processes.

4. Acunetix

- It is used by small businesses, enterprise customers, Web professionals and pen testers.
- It secures websites, web applications and APIs.
- It has vulnerability management capability and both on premises and on demand deployment options are available.
- Some of its features are advanced macro recording technology to scan complex multi-level forms, password protected areas of the website, assessment for the severity of issue and actionable insights, functionalities of scheduling and prioritizing full/incremental scans.

5. NetSparker

- Ideal for small to large businesses.
- It is an application security solution.
- Some of its features are assistance in writing secure code to developers, comprehensive scanning , detection of vulnerabilities, combined signature and behaviour-based testing, unique dynamic and interactive scan to find more actual vulnerabilities.

6. Vipre

- It offers solutions for individuals as well as organizations.
- It provides all inclusive packages and scalable pricing, unparalleled protection with AI, fully integrated to deploy and manage, email encryption capabilities.

7. LifeLock

- It is ideal for small to large businesses.
- It is used to monitor and identify theft and associated threats. Norton 360 LifeLock is all in one identity protection solution.
- Some of its features are dark web monitoring, id verification monitoring, fictitious identity monitoring, device security, cloud backup for windows, virus protection, parental control, ad tracker blocker, alert of crimes committed in your name and has a privacy monitor.

8. Bit defender total security

- Ideal for small and large enterprises.
- It provides online privacy, multi-layer ransomware protection and remediation, network threat protection, complete real time data protection, advanced threat defence, web attack prevention, anti-fraud and rescue mode.

9. Malwarebytes

- Ideal for small and large businesses.
- It offers cyber security solutions which protect against malware, ransomware, malicious websites etc. it supports windows, Android, iOS, Chromebook devices . Some of its features are anomaly detection, behaviour matching, application hardening , clean up of infected devices, shut down attack vendors from every angle, multilayer protection with endpoint detection, threat prevention in real time.

10. Mimecast

- Ideal for small to large businesses.
- It is a cloud-based platform to provide email security and cyber resiliency.
- It has multiple products and services like email security, threat protection, information protection ,web security and cloud archiving.
- Some of its features are email security with threat protection from spear phishing, ransomware, impersonation and other targeted attacks, automated content control, data loss prevention, web security by blocking inappropriate websites and protection against malicious web activity and malware, it has cloud archiving feature to secure emails, files and data.

UNIT-5

1. WHAT IS A BACKDOOR ATTACK?

A. The backdoor attack is a type of malware that is used to get unauthorized access to a website by the cybercriminals. The cybercriminals spread the malware in the system through unsecured points of entry, such as outdated plug-ins or input fields. The malware is entered in the system through the backdoor and it makes it ways to the company's sensitive data including customer personally identifiable information.

Smaller and middle-sized businesses are usually attacked by the backdoor attack as they have fewer resources to close off entry points and identify successful attacks. SMBs often lack resources like budget and security experts to prevent and mitigate attacks. In backdoor attacks, the business usually remains unaware of the attack as the name suggests the attack is made from the backdoor.

Types of Backdoors:

Backdoors can come in various different forms. A few of the most common types include:

- **Trojans**: Most backdoor malware is designed to slip past an organization's defenses, providing an attacker with a foothold on a company's systems. For this reason, they are commonly trojans, which pretend to be a benign or desirable file while containing malicious functionality, such as supporting remote access to an infected computer.
- **Built-in Backdoors**: Device manufacturers may include backdoors in the form of default accounts, undocumented remote access systems, and similar features. While these systems are typically only intended for the use of the manufacturer, they are often designed to be impossible to disable and no backdoor remains secret forever, exposing these security holes to attackers.
- **Web Shells:** A web shell is a web page designed to take user input and execute it within the system terminal. These backdoors are commonly installed by system

and network administrators to make it easier to remotely access and manage corporate systems.

- **Supply Chain Exploits:** Web applications and other software often incorporate third-party libraries and code. An attacker may incorporate backdoor code into a library in the hope that it will be used in corporate applications, providing backdoor access to systems running the software.

How to Prevent a Backdoor Attack:

Some best practices for protecting against exploitation of backdoors include:

- **Changing Default Credentials:** Default accounts are some of the most common types of backdoors. When setting up a new device, disable the default accounts if possible, and, if not, change the password to something other than the default setting.
- **Deploying Endpoint Security Solutions:** Backdoors are commonly implemented as trojan malware. An endpoint security solution may detect and block known malware or identify novel threats based on unusual behavior.
- **Monitoring Network Traffic:** Backdoors are designed to provide remote access to systems via alternative means that bypass authentication systems. Monitoring for unusual network traffic may enable the detection of these covert channels.
- **Scanning Web Applications:** Backdoors may be deployed as web shells or integrated into third-party libraries or plugins. Regular vulnerability scanning can help to identify these backdoors in an organization's web infrastructure.

2. WHAT IS A DIGITAL SIGNATURE?

A. A digital signature is a type of electronic signature. It is a mathematical technique used to authenticate the data exchanged over the internet like emails,

digital documents, card transactions, etc. It sorts of creates a unique virtual fingerprint that represents the identity of the sender and protects the information in the digital document.

It is commonly used for financial transactions, software distributions, and other areas where it is imperative to ensure that there is no breach of data or any forgery. It is very popular with email users where email content becomes the part of the digital signature. It increases the transparency of online transactions and develops trust between the parties involved.

Application of Digital Signature

The important reason to implement digital signature to communication is:

- Authentication
- Non-repudiation
- Integrity

Authentication

Authentication is a process which verifies the identity of a user who wants to access the system. In the digital signature, authentication helps to authenticate the sources of messages.

Non-repudiation

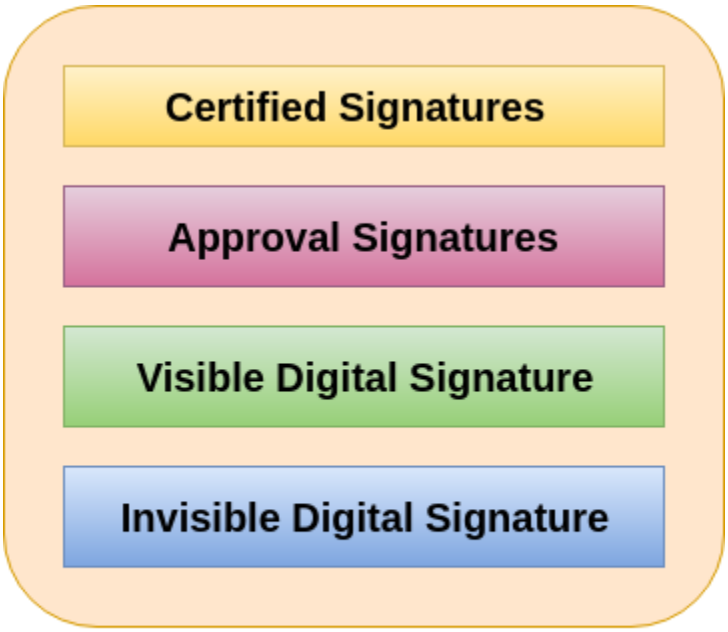
Non-repudiation means assurance of something that cannot be denied. It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or in a file or the sending of a message that they originated.

Integrity

Integrity ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.

Types of Digital Signature

Different document processing platform supports different types of digital signature. They are described below:



Types of Digital Signature

Certified Signatures

The certified digital signature documents display a unique blue ribbon across the top of the document. The certified signature contains the name of the document signer and the certificate issuer which indicate the authorship and authenticity of the document.

Approval Signatures

The approval digital signatures on a document can be used in the organization's business workflow. They help to optimize the organization's approval procedure. The procedure involves capturing approvals made by us and other individuals and embedding them within the PDF document. The approval signatures to include details such as an image of our physical signature, location, date, and official seal.

Visible Digital Signature

The visible digital signature allows a user to sign a single document digitally. This signature appears on a document in the same way as signatures are signed on a physical document.

Invisible Digital Signature

The invisible digital signatures carry a visual indication of a blue ribbon within a document in the taskbar. We can use invisible digital signatures when we do not have or do not want to display our signature but need to provide the authenticity of the document, its integrity, and its origin.

3. What is Metasploit in cyber security?

A. Introduction to Metasploit:

- Metasploit is one of the open source software.
- It is one of the most powerful tool used for testing purpose.
- It comes in two versions: commercial and free.
- If you want to perform practical concept on Metasploit, we need to install "kali distribution"- It is a part of OS or one of the version of kali operating system which has the metasploit community version embedded in it along with other ethical hacking tools.
- Kali distribution is mainly used for vulnerable testing and penetrating testing.
- But if you want to install metasploit on separate tool you can do so on systems that runs on LINUX, WINDOWS &MACOS.
- Metasploit can be used with either command prompt & with web UI.

REX:

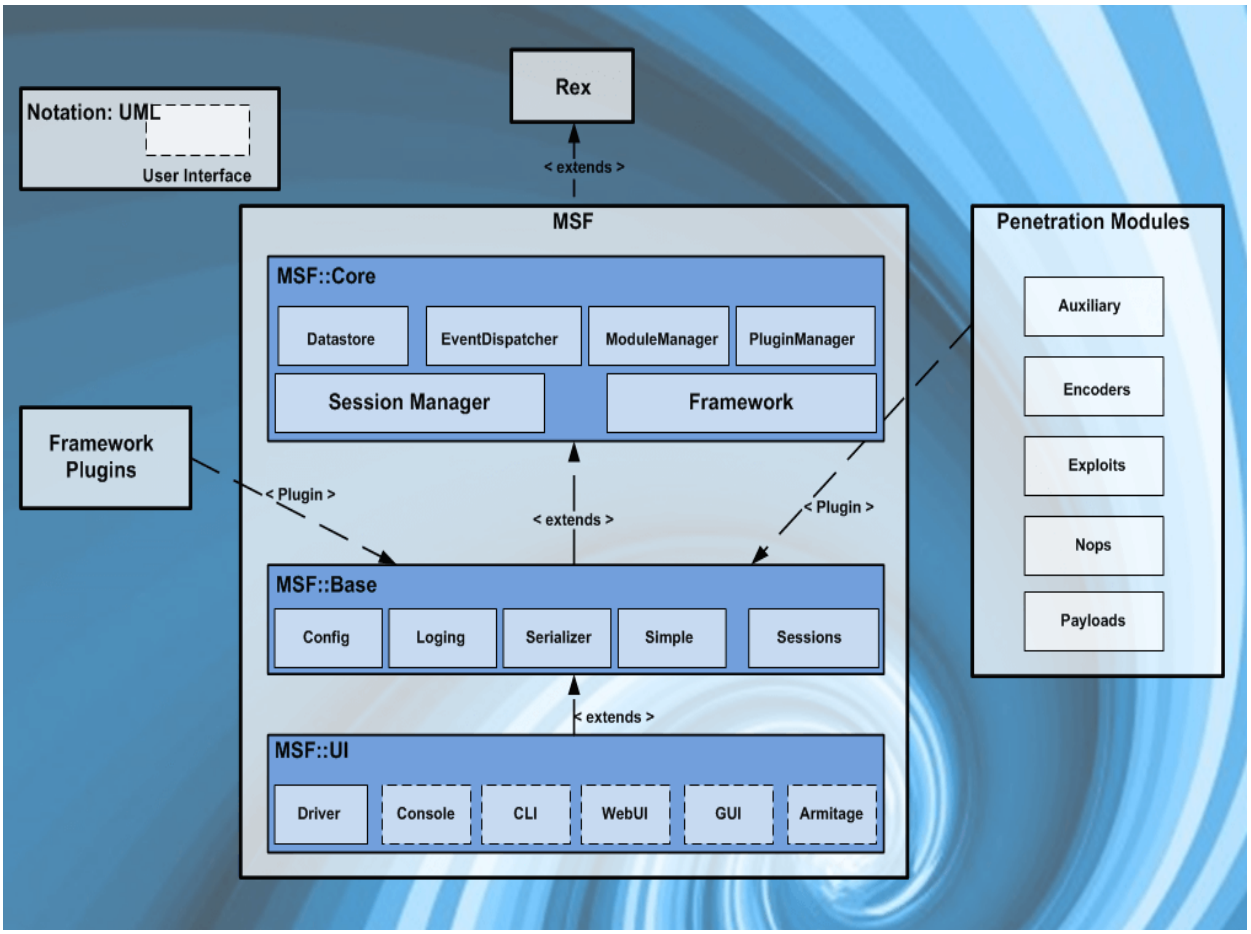
It handles all core functions like setup, sockets, connections and formatting. It is a library about Metasploit Frame work.

MSF CORE:

Heart of Metasploit, provide basic API and Actual core that describes the frame work.

Based on MSF there are 3 different things:

i. MSF CORE: Through which all the API Module will work.
ii. MSF BASE: Through which they can handle all the API Events.
iii. MSF UI: Through which all the users can access Metasploit tools.



Penetration Modules:

1. **Auxiliary:** An exploit work without payload.
2. **Encoders:** Ensures payloads transfer to destination security.
3. **Exploits:** A module working o payload/users payload.
4. **Nops(No operations Generator):** Makes the payload size consistent.
5. **Payloads:** A code that run remotely ,create and run time with various components
6. **Plugin:** Works directly with with API and Penetration Module.

Datastore: central configuration that lets testers define how Metasploit components behave. It also enables setting dynamic parameters and variables and reuse them between modules and payloads. Metasploit has a global datastore and a specific datastore for each module.

4. What is a DMZ Network?

A. In computer security, a DMZ Network (sometimes referred to as a "demilitarized zone") functions as a sub network containing an organization's exposed, outward-facing services. It acts as the exposed point to an untrusted networks, commonly the Internet.

The goal of a DMZ is to add an extra layer of security to an organization's local area network. A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ, while the rest of the organization's network is safe behind a firewall.

When implemented properly, a DMZ Network gives organizations extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

Purpose of a DMZ

The DMZ network is there to protect the hosts that have the most vulnerabilities. DMZ hosts mostly involve services that extend to the users that are outside of the local area network. The increased potential for attacks makes it necessary for them to be placed into the monitored subnetwork. This will protect the rest of the network if they end up getting compromised.

Hosts in the DMZ have access permissions to other services within the internal network and this access is tightly controlled due to the fact that the data that is passed through the DMZ is not as secure.

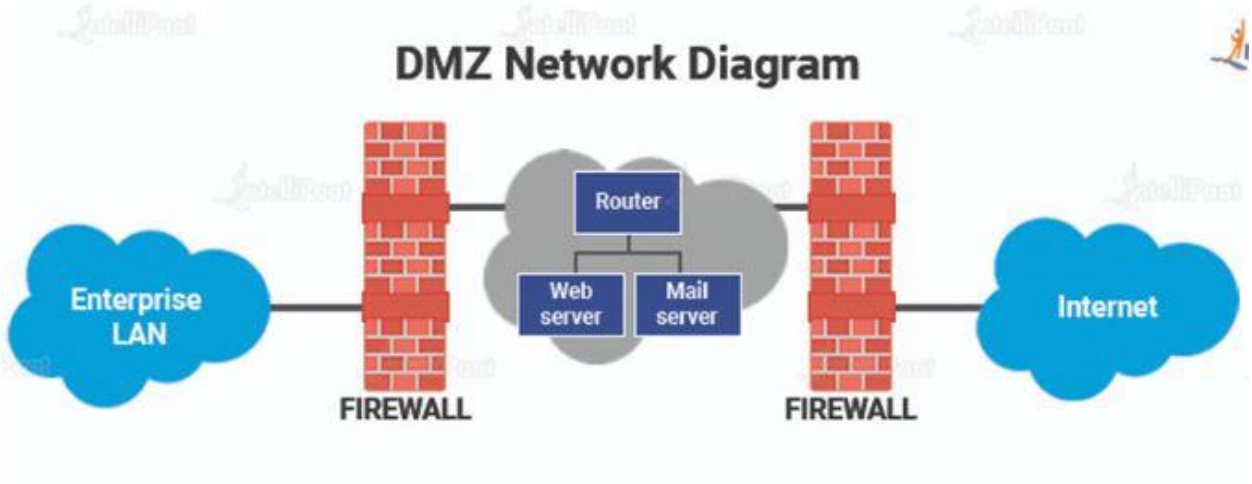
To help expand the protected border zone, the communications between the DMZ hosts and the external network are restricted. This enables the hosts in the protected network to communicate with the internal and external network, while the firewall takes care of the separation and management of all the traffic that is shared between the DMZ and the internal network.

An additional firewall typically protects the DMZ from exposure to everything on the external network. Here are some uses of DMZ in some of the most common services accessible to users on communicating from an external network:

- **Web Servers –** Web servers that maintain communication with an internal database server may need to be placed into a DMZ for the safety of the internal database, which often stores sensitive information. The web servers can then interact through an application firewall or directly with the internal database server, while still having DMZ protections.
- **Mail Servers –** Emails and user databases that contain personal messages and login credentials are usually stored on servers that do not have direct access to the internet. An email server can be built or set up inside the DMZ for interaction with and access to the email database without exposing it to potentially harmful traffic.

- **FTP Servers:** FTP servers can host critical content on the website of an organization, and allow direct interaction with files. Due to this, FTP servers should always be partially isolated from the internal systems that are critical.

Architecture of DMZ:



There are several ways a network can be built using a DMZ. The two primary methods of achieving this are a single firewall (or a three-legged model) or dual firewalls.

1. **Single Firewall**

Using a single firewall with a minimum of 3 network interfaces is a modest approach to network architecture. The DMZ is placed inside this firewall. The connection to the external network device is made from the ISP. The second device connects the internal network and the third network device handles the connections within the DMZ.

- **Dual Firewall**

Using two firewalls is a more secure method to create a DMZ. The first firewall is referred to as the frontend firewall and is built to only allow traffic that is headed

towards the DMZ. The second firewall or the backend firewall is only in charge of the traffic that travels to the internal network from the DMZ.

To further increase the level of protection, firewalls that are built by separate vendors are used as there are fewer possibilities of having the same security vulnerabilities. It is a more effective, but more costly scheme to be implemented across a large network.

DMZ Network Benefits:

Implementing a DMZ enables an organization to define multiple different levels and zones of trust within its network. This provides a number of benefits to an organization, including:

- **Protection of Internet-Facing Systems:** Email servers, web applications, and other Internet-facing systems need access to sensitive data, meaning that they must be protected against attack. Placing these systems on the DMZ enables them to be accessible to the public Internet while still being protected by the external firewall.
- **Protection of Internal Systems:** Some systems on the DMZ (such as FTP servers) pose a threat to the systems within an organization's network. Placing these systems on a DMZ ensures that another layer of security inspection exists between these systems and the organization's internal network.
- **Limited Lateral Movement:** Cyber attackers commonly exploit a system to gain a foothold on a network, then expand their access from that foothold. Since the most vulnerable and exploitable systems are located on the DMZ, it is more difficult to use them as a foothold to gain access to and exploit the internal protected network.
- **Preventing Network Scanning:** Attackers commonly scan organizations' networks to identify computers and software that may be vulnerable to exploitation. Implementing a DMZ structures the network so that only systems that are intended to be Internet-facing are actually visible and scannable from the public Internet.

5. Brief study on Hardening of operating system.

A. System hardening is the process of securing a server or computer system by minimizing its attack surface, or surface of vulnerability, and potential attack vectors. It's a form of cyber attack protection that involves closing system loopholes that cyber attackers frequently use to exploit the system and gain access to users' sensitive data.

Part of the system hardening elimination process involves deleting or disabling needless system applications, permissions, ports, user accounts, and other features so that attackers have fewer opportunities to gain access to a mission-critical or critical-infrastructure computer system's sensitive information.

But at its core, system hardening is a method for protecting a system against attacks perpetrated by cybercriminals. It involves securing a computer system's software mainly but also its firmware and other system elements to reduce vulnerabilities and a potential compromise of the entire system.

What are the types of system hardening?

System hardening involves securing not only a computer's software applications, including the operating system, but also its firmware, databases, networks, and other critical elements of a given computer system that an attacker could exploit.

There are five main types of system hardening:

- Server hardening
- Software application hardening
- Operating system hardening
- Database hardening
- Network hardening

Server hardening:

Server hardening is a general system hardening process that involves securing the data, ports, components, functions, and permissions of a server using advanced security measures at the hardware, firmware, and software layers.

These general server security measures include, but are not limited to:

- Keeping a server's operating system patched and updated
- Regularly updating third-party software essential to the operation of the server and removing third-party software that doesn't conform to established cybersecurity standards
- Using strong and more complex passwords and developing strong password policies for users
- Locking user accounts if a certain number of failed login attempts are registered and removing needless accounts
- Disabling USB ports at boot.
- Implementing multi-factor authentication

Software application hardening:

Software application hardening, or just application hardening, involves updating or implementing additional security measures to protect both standard and third-party applications installed on your server.

Unlike server hardening, which focuses more broadly on securing the entire server system by design, application hardening focuses on the server's applications, specifically, including, for example, a spreadsheet program, a web browser, or a custom software application used for a variety of reasons.

At a basic level, application hardening involves updating existing or implementing new application code to further secure a server and implementing additional software-based security measures.

Examples of application hardening include, but are not limited to:

- Patching standard and third-party applications automatically
- Using firewalls
- Using antivirus, malware, and spyware protection applications
- Using software-based data encryption
- Using CPUs that support Intel Software Guard Extensions (SGX)

Operating system hardening:

Operating system hardening involves patching and implementing advanced security measures to secure a server's operating system (OS). One of the best ways to achieve a hardened state for the operating system is to have updates, patches, and service packs installed automatically.

OS hardening is like application hardening in that the OS is technically a form of software. But unlike application hardening's focus on securing standard and third-party applications, OS hardening secures the base software that gives permissions to those applications to do certain things on your server.

Other examples of operating system hardening include:

- Removing unnecessary drivers
- Encrypting the HDD or SSD that stores and hosts your OS
- Enabling and configuring Secure Boot
- Limiting and authenticating system access permissions

Database hardening:

Database hardening involves securing both the contents of a digital database and the database management system (DBMS), which is the database application users interact with to store and analyze information within a database.

Database hardening mainly involves three processes:

1. Controlling for and limiting user privileges and access
2. Disabling unnecessary database services and functions

3. Securing or encrypting database information and resources

   Types of Database hardening techniques include:

- Restricting administrators and administrative privileges and functions
- Encrypting in-transit and at-rest database information
- Adhering to a role-based access control (RBAC) policy
- Regularly updating and patching database software, or the DBMS

Network hardening:

Network hardening involves securing the basic communication infrastructure of multiple servers and computer systems operating within a given network.

Two of the main ways that network hardening is achieved are through establishing an intrusion prevention system or intrusion detection system, which are usually software-based. These applications automatically monitor and report suspicious activity in a given network and help administrators prevent unauthorized access to the network.

Network hardening techniques include properly configuring and securing network firewalls, auditing network rules and network access privileges, disabling certain network protocols and unused or unnecessary network ports,