LAB CYBER
Cybersecurity made easy

CompTIA Security+

COMPTIA SECURITY+

SYO - 701 Exam Study Guide

Table of Contents

Section 1 -

Summarize Fundamental Security Concepts

Section 2 -

Explaining Threat Actors And Threat Vectors

Section 3 -

Explain Cryptographic Solutions

Section 4 -

Implement Identity and Access Management

Section 5 -

Secure Enterprise Network Architecture

Section 6 -

Secure Cloud Network Architecture

Section 7 -

Explain Resiliency and Site Security Concepts

Section 8 -

Explain Vulnerability Management

Section 9 -

Evaluate Network Security Capabilities

Section 10 -

Assess Endpoint Security Capabilities

Section 11 -

Enhance Application Security Capabilities

Section 12 -

Explain Incident Response and Monitoring Concepts

Section 13 -

Section 13 - Analyze Indicators of Malicious Activity

Section 14 -

Summarize Security Governance Concepts

Section 15 -

Explain Risk Management

Section 16 -

Summarize Data Protection and Compliance Concepts

SECTION 1 -

SUMMARIZE FUNDAMENTAL SECURITY CONCEPTS

1.1 Introduction To Information Security

Information security is based on the cia and dad triads. information and cyber security professionals strive to accomplish the cia triad.

- **Confidentiality** - Data is accessed by only those with the right permit and can be achieved with the use of encryption, passwords, biometrics, 2fa and so on.
- **Integrity** - This ensures that data has not been tampered or altered in any way with the use of hashing, checksums etc
- **Availability** - Data and resources are available to be accessed or shared at all times. This can be achieved with network access, server and data availability.

Black hat hackers and cyber criminals aim for the dad triad.

- **Disclosure** - Hwwwwere data is accessed by non-authorized users with the use of trojans, brute force attacks and theft
- **Alteration** - This means data has been compromised or tampered with. This can be attained by malware, viruses and attacks like sql injection.
- **Deniability** - This means data is not made available to those who need it with the use of attacks like dos and ddos as well as ransomware.

Non-repudiation - means a subject cannot deny something such as creating, modifying or sending a resource.

1.2 Cybersecurity Framework

Information security and cyber tasks can be classified as five functions following the framework developed by the national institute of standards and technology (nist).

The Nist Framework Has 5 Parts

- **Identify** - Evaluate Risks, Threats & Vulnerabilities And Recommend Security Controls To Mitigate Them.
- **Protect** - Procure/Develop, Install, Operate And Decommission It Hardware & Software Assets With Security As An Embedded Requirement At Every Stage.
- **Detect** - Perform Ongoing Proactive Monitoring To Ensure That Security Controls Are Effective And Capable Of Protection Against New Types Of Threats.
- **Respond** - Identify, Analyze, Contain And Eradicate Threats To Systems And Data Security
- **Recover** - Implement Cyber Security Resilience To Restore Systems And Data If Other Controls Are Unable To Prevent Attacks

1.3 Gap Analysis

Gap analysis is a process that identifies how an organization's security systems deviate from those required or recommended by a framework. This will be performed when first adopting a framework or when meeting a new industry or legal compliance requirement. The analysis might be repeated every few years to meet compliance requirements or to validate any changes.

For each section of the framework, a gap analysis report will provide an overall score, a detailed list of missing or poorly configured controls associated with that section, and recommendations for remediation.

While some or all work involved in gap analysis could be performed by the internal security team, a gap analysis is likely to involve third-party consultants. Frameworks and compliance requirements from regulations and legislation can be complex enough to require a specialist. Advice and feedback from an external party can alert the internal security team to oversights and to new trends and changes in best practice.

1.4 Control Objectives

Controls are tactics or strategies that proactively minimize risk by reducing or eliminating:

- A vulnerability
- The likelihood that a threat actor will exploit a vulnerability
- The impact of an exploit

Countermeasures are controls implemented to address a **specific** threat.

Controls can be measured by

- **Functionality -** what the control does
- **Effectiveness -** how well a control works (consistency, reliability, timely)
- **Assurance -** a measure of confidence that intended security controls are effective in their application
- Cost-Benefit

Control objectives refer to a statement of a desired result that should be achieved by implementing a control or set of controls.

Defense-in-depth

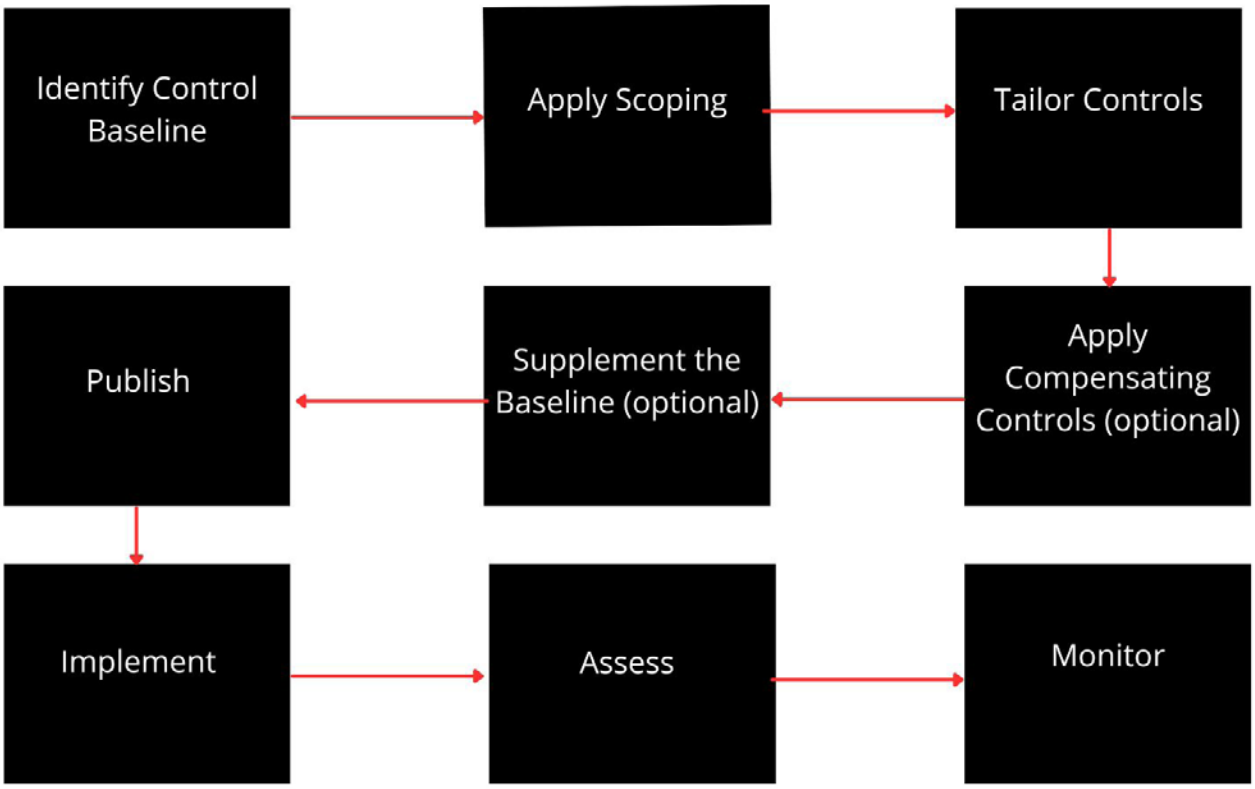
Design and implementation of multiple overlapping layers of diverse controls. Controls should maintain independence and not be subject to the cascading effect.

Security Control Baselines

these express the minimum standards for a given environment

Fine-Tuning Controls

- **Scoping -** Eliminating unnecessary baseline recommendations that are not applicable
- **Tailoring -** Customizing baseline recommendations to align with objectives
- **Compensating -** Substituting a recommended baseline control with a similar control
- **Supplementing -** Adding to the baseline recommendations



1.5 Security Control Categories

A Security Control Is Something Designed To Give A System Or Digital Asset The Properties Of Cia & Non-Repudiation.

There Are Three Main Security Control Categories

- **Technical -** Implemented As A System Such As Firewalls, Anti-Malware And Os Access Control. They Can Also Be Referred To As Logical Controls.
- **Operational -** Implemented Primarily By People Rather Than Systems E.G Security Guards And Training Programs
- **Managerial -** These Controls Give Oversight Of The Information System E.G Risk Identification Tools Or Security Policies.

1.6 Security Control Functional Types

- **Preventive -** These Controls Act To Eliminate Or Reduce The Likelihood That An Attack Can Succeed E.G Acls, Anti-Malware. Directives And Standard Operating Procedures (Sops) Can Be Regarded As Administrative Versions Of Preventative Controls.
- **Detective -** These Controls May Not Deter Access But Will Identify And Record Any Attempted Or Successful Intrusion E.G Logs & Audits

- **Corrective -** These Controls Act To Eliminate Or Reduce The Impact Of An Intrusion Event E.G Backups And Patch Management.
- **Physical -** These Include Alarms, Security Cameras And Guards And Can Be Used To Deter Physical Access To Premises And Hardware
- **Deterrent -** These Controls Can Psychologically Discourage An Attacker From Attempting An Intrusion E.G Signs And Warnings Of Legal Penalties.
- **Compensating -** These Controls Serve As A Substitute For A Principal Control By A Security Standard And Affords The Same (Or Better) Level Of Protection But Uses A Different Methodology Or Technology.

1.7 Security Roles & Responsibilities

Security Professionals Must Be Competent In A Wide Range Of Disciplines From Network To Application Design And Procurement Of Security Resources.

- Participate In Risk Assessments
- Source, Install And Configure Security Devices And Software
- Set Up And Maintain Document Access Control
- Monitor Audit Logs And Review User Privileges
- Manage Security-Related Incident Response And Reporting
- Create And Test Business Continuity And Disaster Recovery Plans
- Participate In Security Training And Education Programs

A security policy is a formalized statement that defines how security will be implemented within an organization and can contain multiple individual policies.

Overall internal responsibility might be allocated to a dedicated department run by a director of security, chief security officer or chief information security officer

Managers may have responsibility for a domain such as building control, ict or even accounting.

Security Operations Center (Soc) - This Is A Location Where Security Professionals Monitor And Protect Critical Information Assets Across Other Business Functions Such As Finance, Operations And Marketing. Typically Employed By Larger Corporations Such As Government Agencies Or A Healthcare Company.

Devsecops - Devops is a cultural shift within an organization to encourage much more collaboration between developers and system admins. Devsecops extends the boundary to security specialists reflecting the principle that security is a primary consideration at every stage of software development **(known as shift left)**

Incident Response - A Dedicated Cyber Incident Response Team (Cirt) / Computer Security Incident Response Team (Csirt) / Computer Emergency Response Team (Cert) As A Single Point-Of-Contact For The Notification Of Security Incidents.

SECTION 2 -

EXPLAINING THREAT ACTORS AND THREAT VECTORS

2.1 Vulnerability, Threat And Risk

Vulnerability - This Is A Weakness That Could Be Triggered Accidentally Or Exploited Intentionally To Cause A Security Breach. Threats Can Exist Even When There Are No Vulnerabilities.

Threats Can Exist Without Risks But A Risk Needs An Associated Threat To Exist

The Path Or Tool Used By A Malicious Threat Actor Can Be Referred To As The Attack Vector.

Risks Are Often Measured Based On The **Probability** That An Event Might Occur As Well As The Impact Of The Event On The Business.

Threat Assessment Is The Combination Of A Threat Actor's **Intentions** To Harm Combined With An Assessment Of That Actor's **Capability** To Carry Out Those Intentions.

Risk Assessment Involves Identification Of Security Risks Through The Analysis Of Assets, Threats And Vulnerabilities, Including Their Impacts And Likelihood.

Risks Are Event Focused (The Database Server Goes Down) While Threats Focus On Intentions (A Hacker Wants To Take Down The Database Server)

Risks Are Event Focused (The Database Server Goes Down) While Threats Focus On Intentions (A Hacker Wants To Take Down The Database Server)

2.2 Attributes Of Threat Actors

Location - An external threat or actor is one that has no account or authorized access to the target system. such threats must use malware and or social engineering to infiltrate the security system. Conversely, an internal or insider threat actor is one that has been granted permissions on the system and typically means either an employee or a third party contractor.

Intent/motivation - Intent describes what an attacker hopes to achieve from the attack while motivation is the reason for perpetuating the attack.motivation could be driven by greed, curiosity or grievance.

Threats can either be structured or unstructured. A criminal gang attempting to steal financial data is a structured targeted threat while a script kiddie launching a series of spam emails is unstructured and opportunistic.

Level of sophistication/capability - the technical abilities and resources/funding the adversary possesses must also be considered. capability refers to a threat actor's ability to craft novel exploit techniques and tools.

2.3 Threat Actors

- **Script kiddie -** Use hacker tools without necessarily understanding how they work or have the ability to craft new attacks.
- **Black hats -** Very skilled and have financial interests
- **White hat -** Hack systems and networks with full authorization typically to discover vulnerabilities and test current security setup.
- **Gray hats -** Are very skilled and typically employ black hat tactics for white hat objectives
- **Hacktivists ** -** Hacking for a cause. they might attempt to obtain and release confidential information to the public or deface a website. (anonymous, wikileaks)
- **State actors & advanced persistent threats -** The term atp was coined to understand the behavior underpinning modern types of cyber adversaries. it refers to the ongoing ability of an adversary to compromise network security and maintain access by using a variety of tools and techniques.
- **Criminal syndicates -** Criminal syndicates can operate across the internet from different jurisdictions than its victim, increasing the complexity of prosecution.
- **Insider threats -** These include, compromised employees, disgruntled employee (ex,) second streamer, spy/saboteur, shadow it, unintentional

2.4 Attack Surface & Attack Vectors

Attack Surface - This refers to all the points at which a malicious threat actor could try to exploit a vulnerability. The attack surface for an external actor is and should be far smaller than that for an insider threat. Minimizing the attack surface means restricting access so that only a few known endpoints, protocols/ports and services are permitted.

The attack vector is the path that a threat actor uses to gain access to a secure system and can include

- Direct Access
- Removable Media
- Email
- Remote & Wireless
- Supply Chain
- Web & Social Media
- Cloud

2.5 Vulnerable Software & Network Vectors

Vulnerable software is one that contains a flaw in its code or design that can be exploited to circumvent access control or to crash the process.

Unsupported systems & applications - An unsupported system is one whose vendor no longer develops updates or patches for it.

One strategy for dealing with unsupported apps that cannot be replaced is to try to isolate them from other systems. The idea is to reduce opportunities for a threat actor to access the vulnerable app and run exploit code. Using isolation as a substitute for patch management is an example of a compensating control.

Network Vectors - An exploit technique for any given software vulnerability can be classed as either remote or local.

- Remote means the vulnerability can be exploited by sending code to the target over a network.
- Local means that the exploit code must be executed from an authenticated session on the computer.

An unsecure network is one that lacks the attributes of CIA while a secure network uses an access control framework and cryptographic solutions to identify, authenticate, authorize and audit network users, hosts and traffic.

Some specific threat vectors associated with unsecure networks are:

- **Direct Access -** Getting physical access to an unlocked workstation, stealing a PC or maybe using a boot disk to install malicious tools.
- **Wired Network -** A threat actor attaches an unauthorized device to a physical network port and is able to launch eavesdropping or DoS attacks.
- **Remote & Wireless Network -** The attacker either obtains credentials for a remote access or wireless connection to the network or cracks the security protocols used for authentication
- **Cloud Access -** The attacker is likely to target the accounts used to develop services in the cloud or manage cloud systems. They may also try to attack the cloud service provider (CSP) as a way of accessing the victim system.

- **Bluetooth Network -** The threat actor exploits a vulnerability or misconfiguration to transmit a malicious file to a user's device over the Bluetooth personal area wireless networking protocol.
- **Default Credentials -** The attacker gains control of a network device or app because it has been left configured with a default password
- **Open Service Port -** The threat actor is able to establish an unauthenticated connection to a logical TCP or UDP network port

2.6 Lure-Based & Message-Based Vectors

This is something superficially attractive that causes its target to want it even though it may be concealing something dangerous.

In cybersecurity terms, when the target opens the file bait, it delivers a malicious payload hook that will typically give the threat actor control over the system or perform service disruption

- **Removable Device -** The attacker conceals malware on a USB thumb drive or memory card and tries to trick employees into connecting the media to a PC or smartphone typically through a drop attack.
- **Executable File -** The threat actor conceals exploit code in a program file (Trojan Malware).
- **Document Files -** Malware is concealed by embedding it in word processing and PDF format files.
- **Image Files -** The exploit code is concealed in an image file that targets a vulnerability in browser or document editing software.

Message-Based Vectors

- **Email -** The attacker sends a malicious file attachment via email that allows attachments (phishing).
- Short Message Service (SMS)
- **Instant Messaging -** Most apps for this are more secure than SMS because they use encryption but they can still contain software vulnerabilities.
- **Web & Social Media -** Malware may be concealed in files attached to posts or presented as downloads.

The most powerful exploits are zero-click which means that simply receiving an attachment or viewing an image on a webpage can trigger the exploit.

2.7 Third Party Risks

Vendor Management Is The Process Of Choosing Supplier Companies And Evaluating The Risks Inherent In Relying On A Third Party Product Or Service.

Within Vendor Management, System Integration Refers To The Process Of Using Components From Multiple Vendors To Implement A Business Workflow.

There Are Two Main Data Risks When Using Third Parties

- Vendor May Need To Be Granted Access To Your Data
- The Vendor May Have To Be Used To Host The Data Or The Data Backups

Data Storage

The Following Precautions Should Be Taken:

- Ensure The Same Protections For Data As Though It Were Stored On-Premises.
- Monitor And Audit Third-Party Access To The Data
- Evaluate Compliance Impacts From Storing Personal Data On A Third-Party System

2.8 Intro To Social Engineering

This is the exploitation of human emotions and interactions to extract valuable information. more dangerous than traditional methods of hacking as it relies on human error which is subjective & less predictable than software/hardware vulnerabilities.

Social engineering relies heavily on human emotions such as fear, curiosity, excitement, anger and guilt.

Phishing - Relies on creating a sense of excitement or panic in the target using emails.

Spear phishing - A phishing attack against a very specific individual or organization

Angler phishing - A phishing attack directed specifically at social media users

Whaling - A phishing attack targeted at senior executives of an organization

Tailgating - The attacker without access authorization closely follows an authorized person in a reserved area

Vishing - Relies on creating a sense of excitement or panic in the target using a phone call

Smishing - Relies on creating a sense of excitement or panic in the target using a text message

Hoaxes - The hacker impersonates an employee or angry customer

Baiting - Dropping infected usb drives in the parking lot to influence employees.

Piggybacking - An attacker enters a secure building with the permission of an employee

Shoulder Surfing - Obtaining sensitive information by spying

Dumpster Diving - Obtaining sensitive information by going through the company trash

Credential Darvesting - Using phishing emails and spamming campaigns to gather information which can then be sold.

Pharming - Redirecting victims to a malicious website using dns cache poisoning.

Watering Hole Attack - An attack that aims to compromise a specific group of end-users by infecting existing websites or creating a new one that will attract them.

Typo Squatting / url Hijacking - Hackers register misspelled domain names of popular websites hoping to capture sensitive information. e.g facbook.com. instagarm.com

Influence Campaigns - A major program launched by an adversary with a high level of capability such as a nation-state actor or terrorist group. the goal is to shift public opinion on some topic and when deployed along with espionage, disinformation/fake news and hacking, it can be characterized as hybrid warfare.

SECTION 3 -

EXPLAIN CRYPTOGRAPHIC SOLUTIONS

3.1 Introduction To Cryptography And Hashing

Cryptography Is A Secure Communication Technique That Allows Only The Sender And Receiver Of A Message To View It.

Plaintext - An Unencrypted Message

Ciphertext - An Encrypted Message

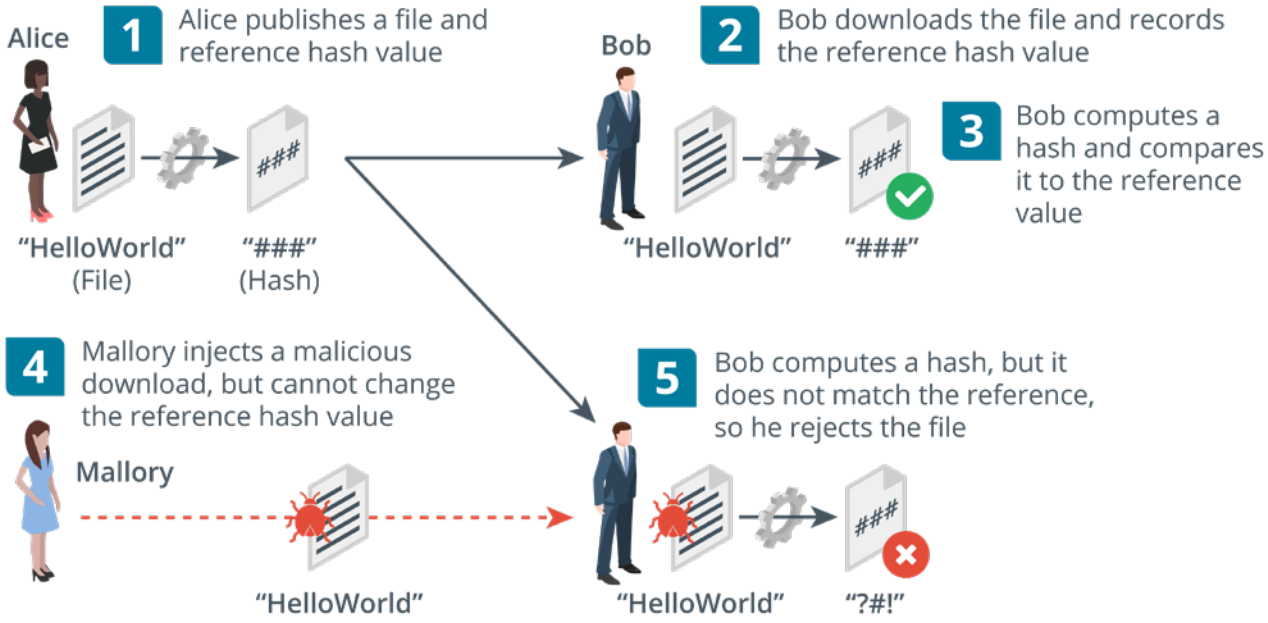
Cipher - The Process (Algorithm) Used To Encrypt And Decrypt A Message

Cryptanalysis - The Art Of Cracking Cryptographic Systems

There Are Three Main Types Of Cryptographic Algorithms:

- Hashing Algorithms
- Symmetric Encryption Cipher
- Asymmetric Encryption Cipher

Hashing Algorithms - The Simplest Type Of Cryptographic Operation And Produces A Fixed Length String From An Input Plaintext That Can Be Of Any Length. A **Hashing Collision** Occurs When Two Different Plain Texts Produce The Exact Same Hash Value. Encryption Algorithms Must Demonstrate Collision Avoidance.



Hashing Algorithms

- **Secure Hash Algorithm (Sha) -** Considered To Be The Strongest Algorithm With The Most Popular Being The Sha-256 Which Produces A 256-Bit Digest.
- Message Direct Algorithm #5 (Md5) - Produces A 128-Bit Digest

Birthday Attack - A Brute Force Attack Aimed At Exploiting Collisions In Hash Functions. Could Be Used For Forging A Digital Signature

3.2 Encryption

An encryption algorithm is a type of cryptographic process that encodes data so that it can be recovered or decrypted.

The use of a key, with the encryption cipher ensures that decryption can only be performed by authorized persons.

A substitution cipher involves replacing units in the plaintext with different ciphertext. e.g rot13 rotates each letter 13 places so a becomes n

The ciphertext “uryyb jbeyq” means “hello world”

In contrast to substitution ciphers, the units in a transposition cipher stay the same in plaintext and ciphertext but their order is changed according to some mechanism.

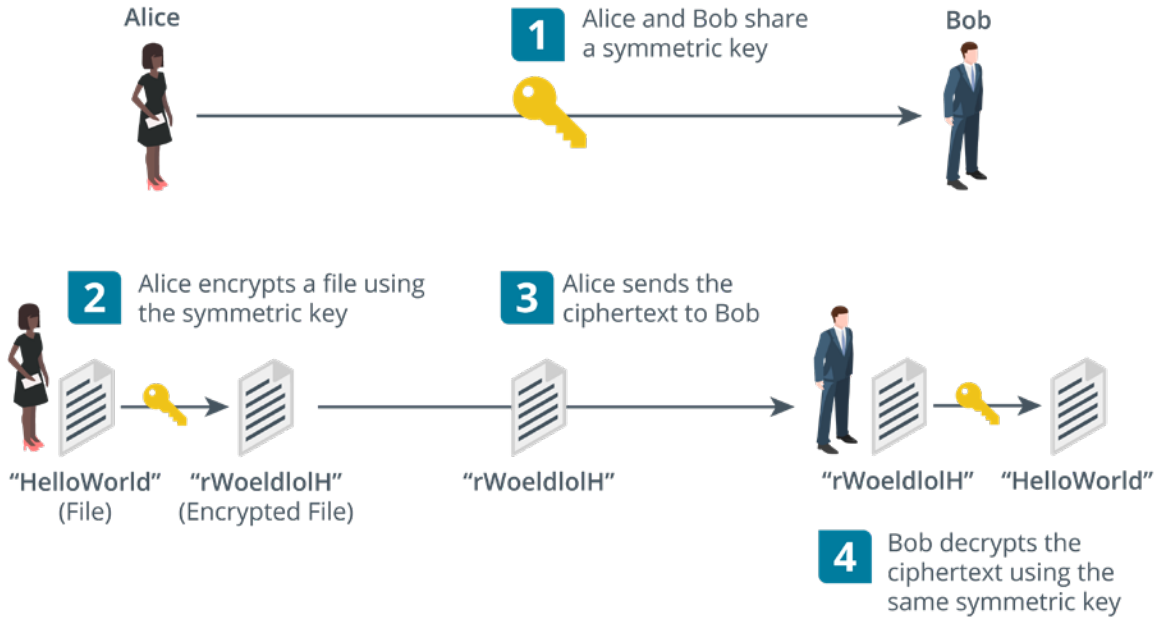
Consider the ciphertext “hloolelwrd”

h l o o l

e l w r d

The letters are simply written as columns and the rows are concatenated.

symmetric encryption - here both encryption and decryption are performed by the same secret key and can be used for confidentiality. It is very fast and is used for bulk encryption of large amounts of data but can be vulnerable if the key is stolen.

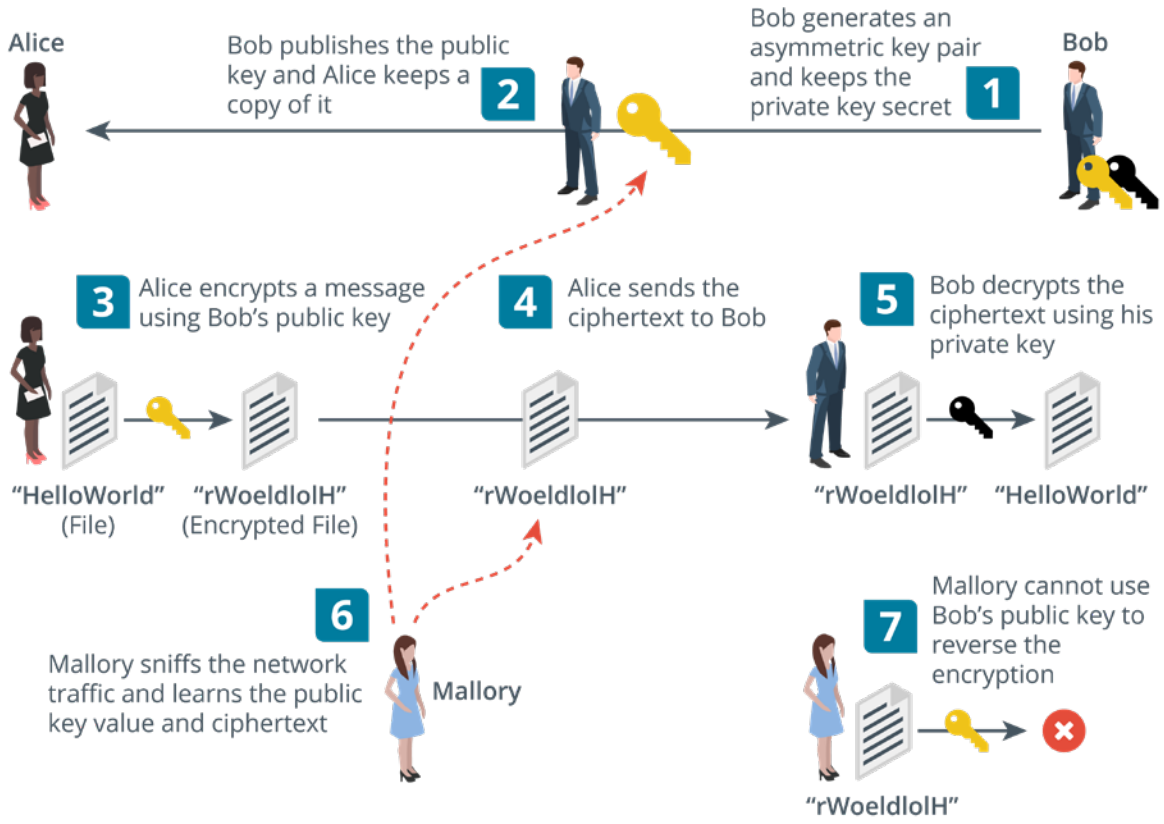


There are two types - Stream ciphers & block ciphers

Stream cipher - The plaintext is combined with a separate randomly generated message calculated from the key and an initialization vector (iv). each byte or bit of data is encrypted one at a time.

Block cipher - The plaintext is divided into equal-size blocks (usually 128-bit). if there is not enough data in the plaintext, it is padded to the correct size. e.g, a 1200-bit plaintext would be padded with an extra 80 bits to fit into 10 x 128-bit blocks.

Asymmetric Encryption - Here both encryption and decryption are performed by two different but related public and private keys in a key pair. Each key is capable of reversing the operation of its pair and they are linked in such a way as to make it impossible to derive one from the other.



Can Be Used To Prove Identity As The Holder Of The Private Key Cannot Be Impersonated By Anyone Else.

The Major Drawback Of This Encryption Is That It Involves Substantial Computing Resources.

Mostly Used For Authentication And Non-Repudiation And For Key Agreement And Exchange.

Asymmetric Encryption Is Often Referred To As Public Key Cryptography And The Products Are Based On The Rsa Algorithm.

Ron Rivest, Adi Shamir And Leonard Adleman Published The Rsa Cipher In 1977.

3.3 Cryptographic Modes Of Operation & Cipher Suites

A Mode Of Operation Is A Means Of Using A Cipher Within A Product To Achieve A Security Goal Such As Confidentiality Or Integrity.

Public Key Cryptography Can Authenticate A Sender While Hashing Can Prove Integrity.

Both Can Be Combined To Authenticate A Sender And Prove The Integrity Of A Message And This Usage Is Called A **Digital Signature**.

Symmetric Encryption Can Encrypt And Decrypt Large Amounts Of Data But It's Difficult To Distribute The Secret Key Securely.

Asymmetric (Pkc) Encryption Can Distribute The Key Easily But Cannot Be Used For Large Amounts Of Data.

Digital Certificates - Public Keys Are Used And Are Freely Available But How Can Anyone Trust The Identity Of The Person Or Server Issuing A Public Key?

A Third Party Known As A **Certificate Authority** (Ca) Can Validate The Owner Of The Public Key By Issuing The Subject With A Certificate.

The Process Of Issuing And Verifying Certificates Is Called **Public Key Infrastructure (Pki)**

Cipher Suite - This Is The Combination Of Ciphers Supported And Is Made Up Of

- **Signature Algorithm -** Used To Assert The Identity Of The Server's Public Key And Facilitate Authentication
- **Key Exchange/Agreement Algorithm -** Used By The Client And Server To Derive The Same Bulk Encryption Symmetric Key.

3.4 Cryptographic Use Cases

Cryptography supporting authentication & non-repudiation - a single hash function, symmetric or asymmetric cipher is called a cryptographic primitive. a complete cryptographic system or product is likely to use multiple cryptographic primitives such as within a cipher suite.

Authentication & non-repudiation depend on the recipient not being able to encrypt the message or the recipient would be able to impersonate the sender. Basically the recipient must be able to use the cryptographic process to decrypt authentication and integrity data but not to encrypt it.

Cryptography supporting confidentiality - cryptography removes the need to store data in secure media as even if the ciphertext is stolen, the threat actor will not be able to understand or change what has been stolen.

Cryptography supporting integrity & resiliency - integrity is proved by hashing algorithms which allow two parties to derive the same checksum and show that a message or data has not been tampered with. Cryptography can be used to design highly resilient control systems and secure computer code.

A developer can make tampering more difficult through obfuscation which is the art of making a message difficult to understand. Cryptography is a very effective way of obfuscating code but it also means the computer might not be able to understand and execute the code.

3.5 Longevity, Salting , Stretching & Other Types Of Cryptographic Technologies

Longevity - This Refers To The Measure Of Confidence That People Have In A Given Cipher. In Another Sense, It Is The Consideration Of How Long Data Must Be Kept Secure.

Salting - Passwords Stored As Hashes Are Vulnerable To Brute Force And Dictionary Attacks. A Password Hash Cannot Be Decrypted As They Are One-Way. However, An Attacker Can Generate Hashes To Try And Find A Match For The Captured Password Hash Through A Brute Force Or Dictionary Attack.

A Brute Force Attack Will Run Through A Combination Of Letters, Numbers And Symbols While A Dictionary Attack Creates Hashes Of Common Words And Phrases.

Both Attacks Can Be Slowed Down By Adding A Salt Value When Creating The Hash.

(Salt + Password) * Sha = Hash

The Salt Is Not Kept Secret Because Any System Verifying The Hash Must Know The Value Of The Salt But It's Presence Means That An Attacker Cannot Use Pre-Computed Tables Of Hashes.

Key Stretching - This Takes A Key That's Generated From A User Password Plus A Random Salt Value And Repeatedly Converts It To A Longer And More Random Key. This Means The Attacker Will Have To Do Extra Processing For Each Possible Key Value Thus Make The Attack Even Slower.

This Can Be Performed By Using A Particular Software Library To Hash And Save Passwords When They Are Created. The **Password-Based Key Derivation Function 2 (Pbkdf2)** Is Widely Used For This Purpose.

Homomorphic Encryption - This Is The Conversion Of Data Into Ciphertext That Can Be Analyzed And Worked With As If It Were Still In Its Original Form.

It Enables Complex Mathematical Operations To Be Performed On Encrypted Data Without Compromising The Encryption.

Blockchain - This is a concept in which an expanding list of transactional records is secured using cryptography. Each record is referred to as a block and is run through a hash function. The hash value of the previous block in the chain is added to the hash calculation of the next block and thus ensures that each successive block is cryptographically linked.

Steganography - This is a technique for obscuring the presence of a message such as hiding a message in a picture. the container document or file is called the covertext.

3.6 Certificates, Pkis, Ras & Csrs

Public & Private Key Usage

When you want others to send you confidential messages, you give them your public key to encrypt the message and then you decrypt the message with your private key.

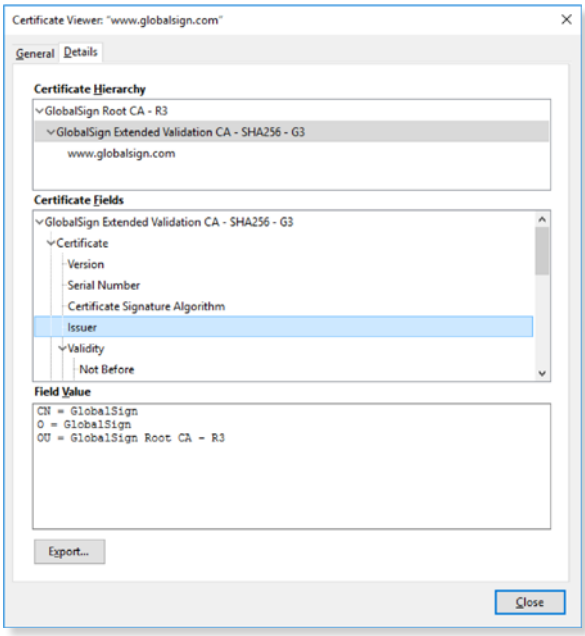
When You Want To Authenticate Yourself To Others, You Create A Signature And Sign It Using Your Private Key To Encrypt It. You Give Others Your Public Key To Decrypt The Signature.

Certificate Authority - This Is The Entity Responsible For Issuing And Guaranteeing Certificates.

Pki Trust Models Include:

- **Single Ca -** A Single Ca Issues Certificates To Users And The Users Trust Certificates By That Ca Exclusively. If The Ca Is Compromised, The Entire Pki Collapses
- **Hierarchical (Intermediate Ca) -** A Single Ca Called The Root Issues Certificates To Several Intermediate Cas. The Intermediate Cas Issue Certificates To Subjects (Leaf Or End Entities). Each Leaf Certificate Can Be Traced Back To The Root Ca Along The Certification Path And This Is Referred To As A Certificate Chain Or Chain Of Trust. The Root Is Still A Single Point Of Failure But It Can Be Taken Offline As Most Of The Regular Ca Activities Are Handled By The Intermediate Ca Servers.

- **Online Versus Offline Cas -** An online ca is one that is available to accept and process certificate signing requests and management tasks. Because of the high risk posed by a compromised root ca, a secure configuration will involve making the root an offline ca meaning it is disconnected from any network and only brought back online to add or update intermediate cas.



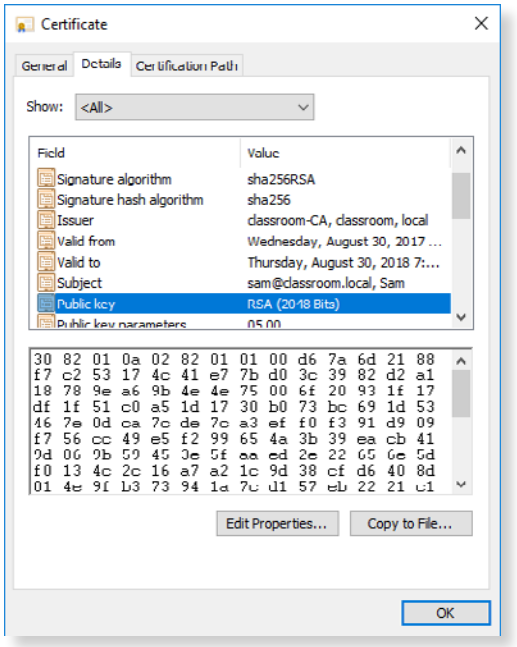
Registration authorities and CSRS - registration is the process by which end users create an account with the CA and become authorized to request certificates.

When A Subject Wants To Obtain A Certificate, It Completes A Certificate Signing Request (Csr) And Submits It To The Ca.

The CA Reviews The Certificate And Checks That The Information Is Valid. If The Request Is Accepted, The CA Signs The Certificate And Sends It To The Subject.

3.7 Digital Certificates

A Digital Certificate Is Essentially A Wrapper For A Subject's Public Key. As Well As The Public Key, It Contains Information About The Subject And The Certificate's Issuer.

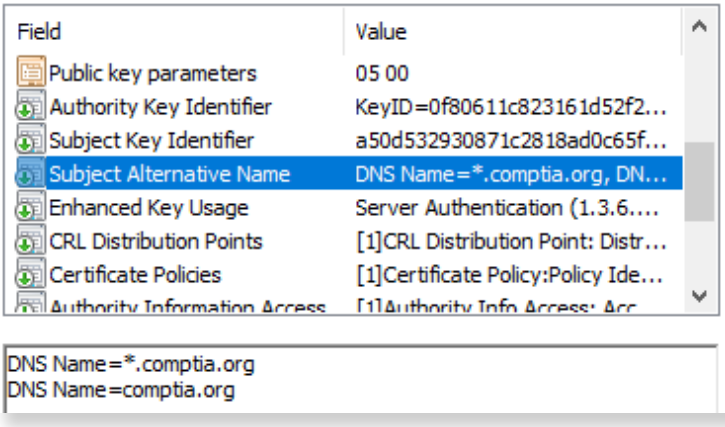


Field	Usage
Serial number	A number uniquely identifying the certificate within the domain of its CA.
Signature algorithm	The algorithm used by the CA to sign the certificate.
Issuer	The name of the CA.
Valid from/to	Date and time during which the certificate is valid.
Subject	The name of the certificate holder, expressed as a distinguished name (DN). Within this, the common name (CN) part should usually match either the fully qualified domain name (FQDN) of the server or a user email address.
Public key	Public key and algorithm used by the certificate holder.
Extensions	V3 certificates can be defined with extended attributes, such as friendly subject or issuer names, contact email addresses, and intended key usage.
Subject alternative name (SAN)	This extension field is the preferred mechanism to identify the DNS name or names by which a host is identified.

When Certificates Were First Introduced, The Common Name (Cn) Attribute Was Used To Identify The Fqdn By Which The Server Is Accessed.

The **Subject Alternative Name (San)** Extension Field Is Structured To Represent Different Types Of Identifiers Including Domain Names.

A **Wildcard** Domain Such As *.Comptia.Org Means That The Certificate Issued To The Parent Domain Will Be Accepted As Valid For All Subdomains.



Eku Field - Can Have The Following Values

- Server Authentication
- Client Authentication
- Code Signing
- Email Protection

Other Certificate Types Include:

- Machine/Computer Certificates
- Email/User Certificates
- Code Signing Certificates
- Root Certificate
- Self-Signed Certificates

Web Server Certificate Types Include:

- Domain Validation (Dv) - Proves The Ownership Of A Particular Domain
- Extended Validation (Ev) - Subjecting To A Process That Requires More Rigorous Checks On The Subject's Legal Identity And Control Over The Domain.

3.8 Key Management

This Refers To Operational Considerations For The Various Stages In A Key's Life Cycle And Can Be **Centralized** Meaning One Admin Controls The Process Or **Decentralized** In Which Each User Is Responsible For His Or Her Keys.

Key Life Cycle

- Key Generation
- Certificate Generation
- Storage
- Revocation
- Expiration And Renewal

If The Key Used To Decrypt Data Is Lost Or Damaged, Encrypted Data Cannot Be Recovered Unless A Backup Of The Key Exists. However Making Too Many Backups Can Make It More Difficult To Keep The Key Secure.

Escrow Means That Something Is Held Independently Which In Terms Of Key Management, Means A Third Party Is Trusted To Store The Key Securely.

3.9 Certificate Management

When You Are Renewing A Certificate, It Is Possible To Use The Existing Key Referred To Specifically As **Key Renewal** Or Generate A New Key In Which Case, The Certificate Is **Rekeyed.**

Certificates Are Issued With A Limited Duration Set By The Ca Policy For The Certificate Type E.G A Root Certificate Might Have A 10 Year Expiry Date While A Web Server Certificate Might Be Issued For 1 Year Only.

A Certificate May Be Revoked Or Suspended. A Revoked Certificate Is No Longer Valid And Cannot Be Reinstated While A Suspended Certificate Can Be Re-Enabled.

A Certificate May Be Revoked Or Suspended For A Variety Of Reasons Such As The Private Key Compromise, Business Closure Or A User Leaving The Company. These Reasons Are Codified Under

- Unspecified
- Key Compromise
- Ca Compromise
- Superseded
- Cessation Of Operation

A Suspended Key Is Given The Code **Certificate Hold**

SECTION 4 -

IMPLEMENT IDENTITY AND ACCESS MANAGEMENT

4.1 Identity Access Management

Covers The Authentication & Authorization Aspects Of A System And How Privileged Users Are Managed.

There Are Four Phases Involved In IAM

- Identity - Supply Identification Information
- Authenticate - Identity Information Is Verified
- Authorize - Allows Actions Based On Verified Identification
- Audit - Keeps Track Of Actions Performed With The Identification

Identity & Access Threats

- Spoofing
- Identity Theft
- Keylogging
- Escalation Of Privilege
- Information Leakage

IM Tools & Techniques

- Identity Manager
- Fraud Analytics
- Multi Factor Authentication

Am Tools & Techniques

- Single Sign On
- Behavior Analytics
- Role Based Approach

4.2 Authentication Factors, Design And Attributes

Authentication Factors

- **Something You Know -** This Includes Passwords, Passphrases Or Pins. A **Knowledge Factor** Is Also Used For Account Reset Mechanisms.
- **Something You Have -** An **Ownership Factor** Means That The Account Holder Possesses Something That No One Else Does Such As A Smart Card, Hardware Token Or Smartphone.

- **Something You Are/Do -** A **Biometric Factor** Uses Either Physiological Identifiers Like Fingerprints Or Behavioral Identifiers Such As The Way Someone Walks And Talks.

Multi Factor Authentication - This Combines The Use Of More Than One Authentication Factor And Can Either Be 2factor Or 3 Factor Authentication.

Multifactor authentication requires a combination of different technologies. for example, requiring a pin along with a date of birth isn't multifactor.

Authentication Attributes

Compared to the authentication factors, an authentication attribute is either a non-unique property or a factor that cannot be used independently.

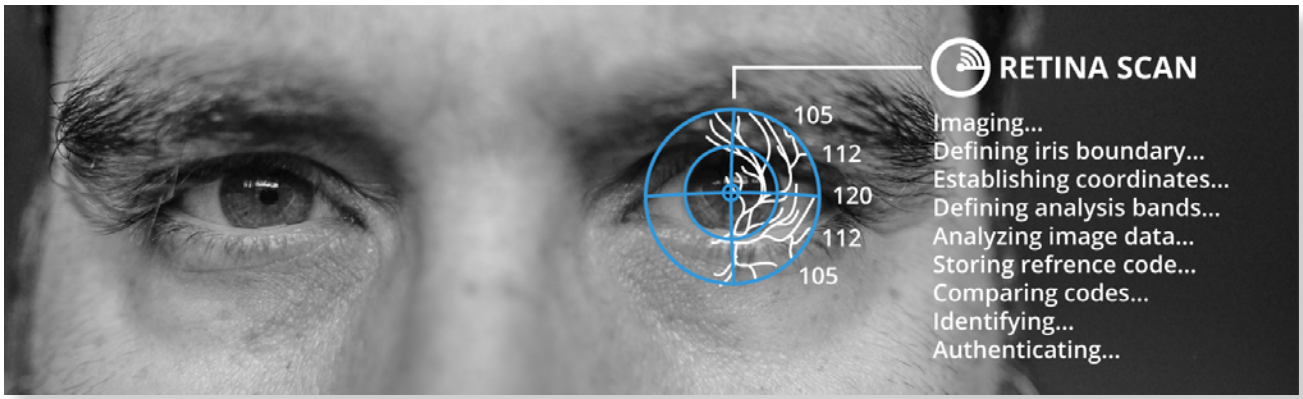
- **Somewhere you are -** This could be a geographic location measured using a device's location service or ip address. This isn't used as a primary authentication factor but may be used as a continuous authentication mechanism.
- **Something you can do -** Behavioral characteristics such as the way you walk or hold your smartphone can be used to identify you to a considerable degree of activity.
- **Something you exhibit -** This also refers to a behavioral-based authentication and authorization with specific emphasis on personality traits such as the way you use smartphone apps or web search engines.
- **Someone you know -** This uses a web of trust model where new users are vouched for by existing users.

4.3 Biometric Authentication

The first step is enrollment and the chosen biometric is scanned by a biometric reader and converted to binary information. The biometric template is kept in the authentication server database and when a user wants to access a resource, they are scanned and the scan is compared to the template to determine if access will be granted or denied.

- **False rejection rate (FRR) -** Where a legitimate user is not recognized. also referred to as a type 1 error or false non-match rate (FNMR).
- **False acceptance rate (FAR) -** Where an interloper is accepted. also referred to as type 2 error or false match rate (FMR)
- **Crossover error rate (CER) -** The point at which FRR and FAR meet. the lower the CER, the more efficient and reliable the technology.

Fingerprint & facial recognition - Fingerprint recognition is the most widely used as it's inexpensive and non-intrusive. facial recognition records multiple factors about the size and shape of the face



Facial Recognition

- **Retinal Scan -** An Infrared Light Is Shone Into The Eye To Identify The Pattern Of Blood Vessels. It Is Very Accurate, Secure But Also Quite Expensive
- **Iris Scan -** Matches Patterns On The Surface Of The Eye Using Near-Infrared Imaging And Is Less Intrusive Than Retinal Scan.

Behavioral Technology - A Template Is Created By Analyzing A Behavior Such As Typing Or Walking.

- **Voice Recognition -** Relatively Cheap But Subject To Impersonation And Background Noise
- **Gait Analysis -** Human Movement
- **Signature Recognition -** Records The User Applying Their Signature (Stroke, Speed And Pressure Of The Stylus)
- **Typing -** Matches The Speed And Pattern Of A User's Input Of A Passphrase

Continuous Authentication Verifies That The User Who Logged On Is Still Operating The Device.

4.4 Password Concepts

Password Length - Enforces a minimum length for passwords.

Password Complexity - Enforces password complexity rules

Password Aging - Forces the user to select a new password after a set period

Password Reuse and History - Prevents the selection of a password that has been used already.

Under the most recent NIST guidelines:

Complexity rules should not be enforced and the only restriction should be to block common passwords.

Aging policies should not be enforced. Users should be able to select if and when a password should be changed

Password hints should not be used.

Password Managers - These are used to mitigate poor credential management practices that are hard to control.

The main risks involved are selection of a weak master password, compromise of the vendor's cloud storage or systems and impersonation attacks designed to trick the manager into filling a password to a spoofed site.

4.5 Authorization Solutions - Part 1

An Important Consideration When Designing A Security System Is To Determine How Users Receive Rights Or Permissions.

The Different Models Are Referred To As Access Control Schemes.

Discretionary Access Control (Dac) - It Is Very Flexible But Also The Easiest To Compromise As It's Vulnerable To Insider Threats And Abuse Of Compromised Accounts.

This Is Based On The Primacy Of The Resource Owner And This Means The Owner Has Full Control Over The Resource And Can Decide Who To Grant Rights To.

Role-Based Access Control (Rbac) - Rbac Can Be Partially Implemented Through The Use Of Security Group Accounts.

This Adds An Extra Degree Of Centralized Control To The Dac Model Where Users Are Not Granted Rights Explicitly (Assigned Directly) But Rather Implicitly (Through Being Assigned A Role)

File System Permissions (Linux) - In Linux, There Are Three Basic Permissions:

- **Read(R) -** The Ability To Access And View The File
- **Write(W) -** The Ability To Modify The File
- **Execute(X) -** The Ability To Run A Script Or Program Or Perform A Task On That Directory.

These Permissions Can Be Applied In The Context Of The Owner User(U), A Group Account(G) And All Other Users/World(O).

D Rwx R-X R-X Home

The String Above Shows That For The Directory(D), The Owner Has Read, Write And Execute Permissions While The Group Context And Others Have Read And Execute Permissions

The Chmod Command Is Used To Modify Permissions And Can Be Used Either In Symbolic Or Absolute Mode.

In Symbolic Mode, The Command Works As Follows:

Chmod G+W, O-X Home

The Effect Of This Command Is To Append Write Permission To The Group Context And Remove Execute Permission From The Other Context.

By Contrast, The Command Can Also Be Used To Replace Existing Permissions.

Chmod U=Rwx, G=Rx, O=Rx Home

D rwx r-x r-x home

In absolute mode, permissions are assigned using octal notation where r=4, w=2 and x=1

Chmod 755 home

Mandatory access control (mac) - this is based on the idea of security clearance levels (labels) instead of acls. In a hierarchical one, subjects are only permitted to access objects at their own clearance level or below.

Attribute-based access control (abac) - this is the most fine-grained type of access control mode and it is capable of making access decisions based on a combination of subject and object attributes plus any system-wide attributes.

This system can monitor the number of events or alerts associated with a user account or track resources to ensure they are consistent in terms of timing of requests.

Rule-based access control - this is a term that can refer to any sort of access control model where access control policies are determined by system-enforced rules rather than system users.

As such rbac, abac and mac are all examples of rule-based (or non-discretionary) access control.

4.6 Authorization Solutions - Part 2

Directory services - Directory services are the principal means of providing privilege management and authorization on an enterprise network as well as storing information about users, security groups and services.

The types of attributes, what information they contain and the way object types are defined through attributes is described by the directory schema.

Cn - common name ou - organizational unit c - country dc - domain component

E.G the distinguished name of a web server operated by widget in the uk might be:

Cn = widgetweb, ou = marketing, o = widget, c= uk, dc = widget, dc = foo

Federation - Federation means that the company trusts accounts created and managed by a different network.

This is the notion that a network needs to be accessible to more than just a well-defined group of employees. In business, a company might need to make parts of its network open to partners, suppliers and customers.

Cloud versus on-premises requirements - Where a company needs to make use of cloud services or share resources with business partner networks, authorization and authentication design comes with more constraints and additional requirements.

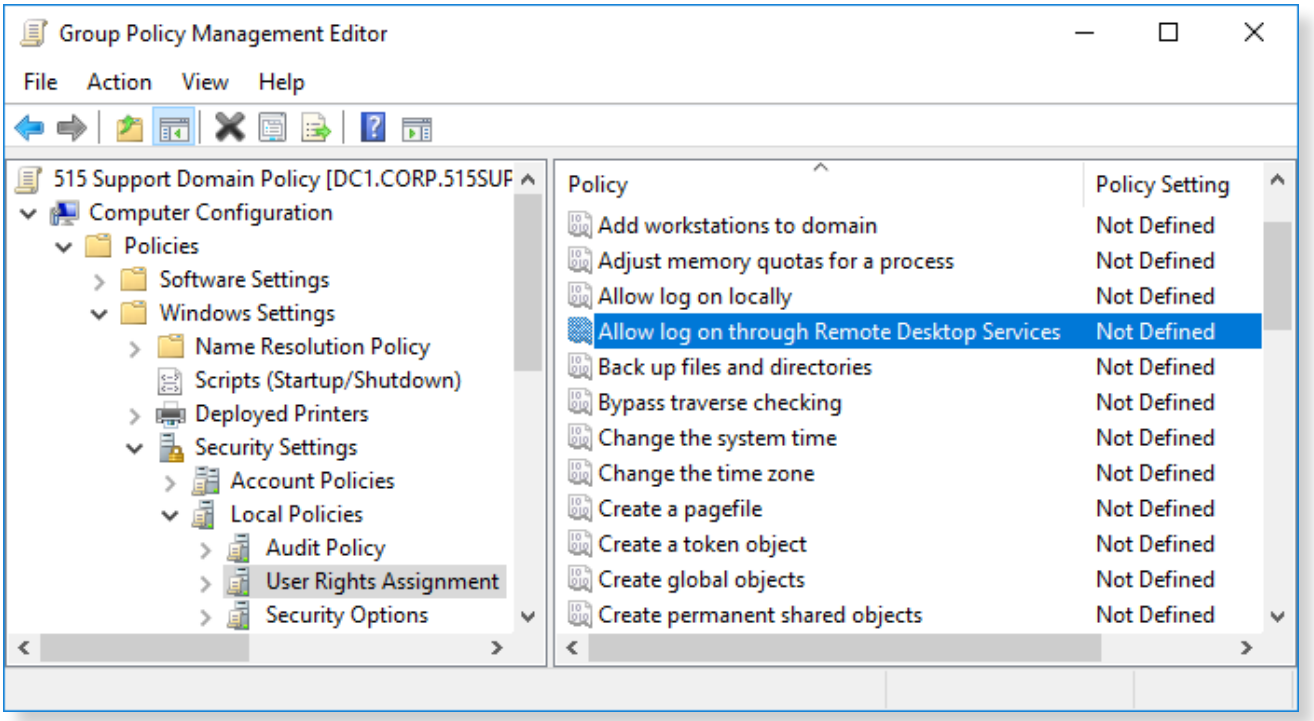
Oauth and openid connect - Many public clouds use application programming interfaces (apis) based on representational state transfer (rest) rather than soap.

Authentication and authorization for a restful api is often implemented using the open authorization (oauth) protocol. Oauth is designed to facilitate sharing of information within a user profile between sites.

4.7 Account Attributes & Access Policies

A user account is defined by a unique security identifier (sid), a name and a credential. Each account is associated with a profile which can be defined with custom identity attributes describing the user, such as full name, email address, contact number etc.

Each account can be assigned permissions over files and other network resources. These permissions might be assigned directly to the account or inherited through membership of a security group or role. On a windows active directory network, access policies can be configured via group policy objects (gpos)



Location-Based Policies - A User Or Device Can Have A Logical Network Location Identified By An Ip Address Which Can Be Used As An Account Restriction Mechanism.

The Geographical Location Of A User Or Device Can Be Calculated Using A Geographical Mechanism.

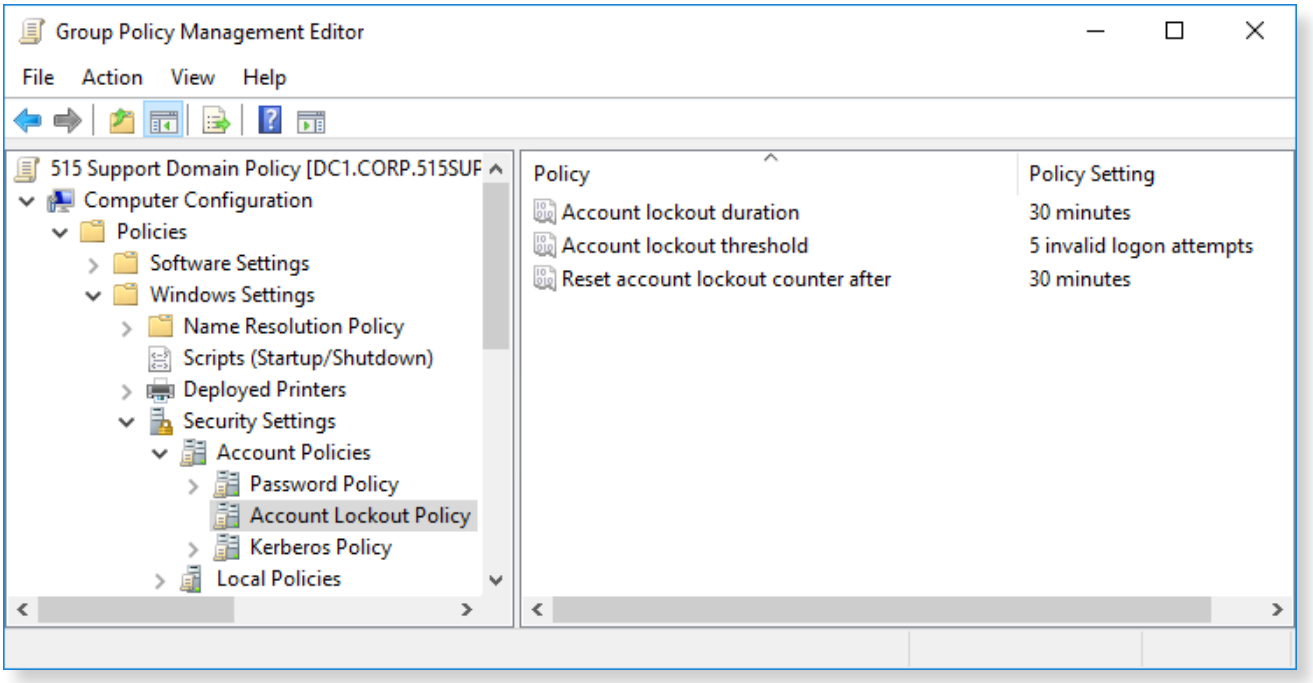
Geofencing Refers To Accepting Or Rejecting Access Requests Based On Location.

Time-Based Restrictions - There Are Three Main Types Of Time-Based Policies.

- A Time Of Day Policy Established Authorized Logon Hours For An Account
- A Time-Based Login Policy Established The Maximum Amount Of Time An Account May Be Logged In For
- An Impossible Travel Time/Risky Login Policy Tracks The Location Of Logon Events Over Time.

Account & Usage Audits - Accounting And Auditing Processes Are Used To Detect Whether An Account Has Been Compromised Or Is Being Misused. Usage Auditing Means Configuring The Security Log To Record Key Indicators And Then Reviewing The Logs For Suspicious Activity.

Account Lockout & Disablement - If Account Misuse Is Detected Or Suspected, The Account Can Be Manually Disabled By Setting An Account Property. An Account Lockout Means That Login Is Prevented For A Period



4.8 Privileged Access Management

A privileged account is one that can make significant configuration changes to a host, such as installing software or disabling a firewall or other security system. Privileged accounts also have the right to manage network appliances, application servers, and databases.

Privileged Access Management (PAM) refers to policies, procedures and technical controls to prevent compromise of privileged accounts.

It is a good idea to restrict the number of administrative accounts as much as possible. The more accounts there are, the more likely it is that one of them will be compromised. On the other hand, you do not want administrators to share accounts or to use default accounts, as that compromises accountability.

To protect privileged account credentials, it is important not to sign in on untrusted workstations. A **secure administrative workstation (SAW)** is a computer with a very low attack surface running the minimum possible apps.

Traditional administrator accounts have standing permissions. **Just-in-time (JIT)** permissions means that an account's elevated privileges are not assigned at log-in. Instead, the permissions must be explicitly requested and are only granted for a limited period. This is referred to as zero standing privileges (ZSP).

There are three main models for implementing this

- **Temporary Elevation -** Means that the account gains administrative rights for a limited period. The User Account Control (UAC) feature of Windows and the sudo command in Linux use this concept.
- **Password Vaulting/Brokering -** The privileged account must be "checked out" from a repository and is made available for a limited amount of time. The administrator must log a justification for using the privileges.
- **Ephemeral Credentials -** Means the system generates or enables an account to use to perform the administrative task and then destroys or disables it once the task has been performed. Temporary or ephemeral membership of security groups or roles can serve a similar purpose.

4.9 Local, Network & Remote Authentication

This involves a complex architecture of components but the following three scenarios are typical:

Windows Authentication

- **Windows local sign-in --** the Local Security Authority (LSA) compares the submitted credential to a hash stored in the Security Accounts Manager (SAM) database.
- **Windows network sign-in --** the LSA can pass the credentials for authentication to a network service either Kerberos or NT LAN Manager (NTLM) authentication.
- **Remote sign-in --** if the user's device is not connected to the local network, authentication can take place over some type of virtual private network (VPN) or web portal.

Linux Authentication -Local user account names are stored in **/etc/passwd**. When a user logs in to a local interactive shell, the password is checked against a hash stored in /etc/shadow.

A pluggable authentication module (PAM) is a package for enabling different authentication providers.

Single Sign-On (SSO) - This system allows the user to authenticate once to a local device and be authenticated to compatible application servers without having to enter credentials again.

In Windows, SSO is provided by the Kerberos framework.

4.10 Kerberos Authentication & Authorization

Kerberos is a single sign-on network authentication and authorization protocol used on many networks notably as implemented by Microsoft's Active Directory (AD) service.

Kerberos Authentication - This protocol is made up of 3 parts

- KDC (Authentication Service)
- Principal
- Application Server

SECTION 5 -

SECURE ENTERPRISE NETWORK ARCHITECTURE

5.1 Secure Network Designs

Switches - forward frames between nodes in a cabled network.

They work at layer 2 of the osi model and make forwarding messages based on the hardware or media access control (mac) address of attached nodes.

They can establish network segments that either map directly to the underlying cabling or to logical segments created in the switch configuration as virtual lans (vlans)

Wireless access points - provide a bridge between a cabled network and wireless clients or stations. They also work at layer 2 of the osi model.

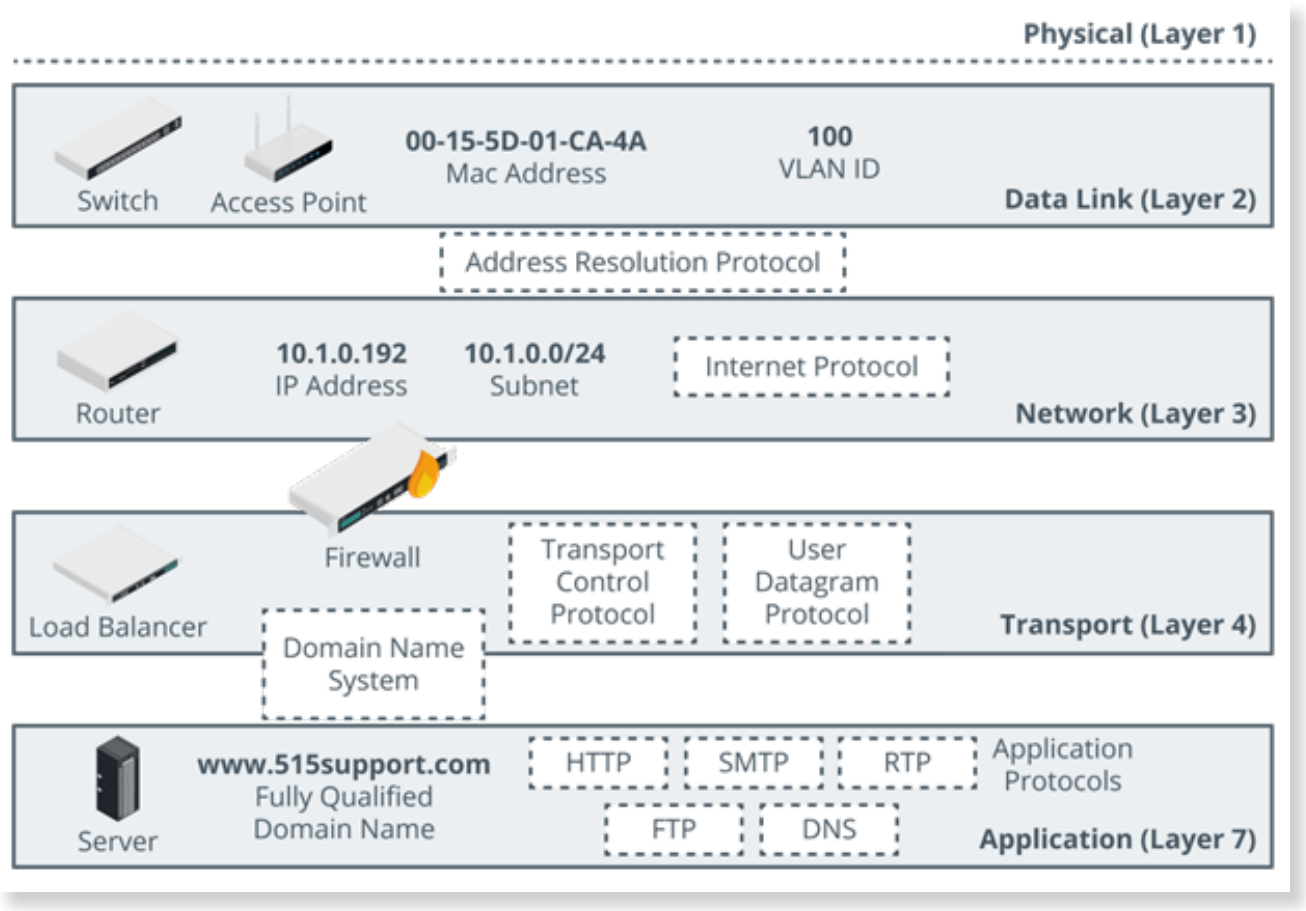
Load balancers - distribute traffic between network segments or servers to optimize performance. They work at layer 4 of the osi model or higher

Routers - forward packets around an internetwork, making forward decisions based on ip addresses. They work at layer 3 of the osi model. They can apply logical ip subnet addresses to segments within a network.

Firewalls - they apply an access control list (acl) to filter traffic passing in or out of a network segment. They can work at layer 3 of the osi model or higher.

Domain name system (dns) servers - host name records and perform name resolution to allow applications and users to address hosts and services using fully qualified domain names (fqdns) rather than ip addresses.

Dns works at layer 7 of the osi model.



5.2 Network Segmentation, Topology & Dmzs

A Network Segment Is One Where All The Hosts Attached To The Segment Can Use Local (Layer 2) Forwarding To Communicate Freely With One Another.

Segregation Means That The Hosts In One Segment Are Restricted In The Way They Communicate With Hosts In Other Segments.

Freely Means That No Network Appliances Or Policies Are Preventing Communications.

A Network Topology Is A Description Of How A Computer Network Is Physically Or Logically Organized.

The Main Building Block Of A Topology Is A Zone Which Is An Area Of The Network Where The Security Configuration Is The Same For All Hosts Within It.

Zones Can Be Segregated With Vlans While The Traffic Between Them Can Be Controlled Using A Security Device, Typically A Firewall.

Network Zones

- **Intranet (Private Network) -** This Is A Network Of Trusted Hosts Owned And Controlled By The Organization.
- **Extranet -** This Is A Network Of Semi-Trusted Hosts Typically Representing Business Parties, Suppliers Or Customers.
- **Internet/Guest -** This Is A Zone Permitting Anonymous Access By Untrusted Hosts Over The Internet.

Demilitarized Zones (Dmzs) - The Most Important Distinction Between Different Security Zones Is Whether A Host Is Internet-Facing.

An Internet-Facing Host Accepts Inbound Connections From And Makes Connections To Hosts On The Internet.

Such Hosts Are Placed In A Dmz (Perimeter Or Edge Network). In A Dmz, External Clients Are Allowed To Access Data On Private Systems Such As Web Servers Without Compromising The Security Of The Internal Network As A Whole.

Triple-Homed Firewall - A Dmz Can Also Be Established Using One Router/Firewall Appliance With Three Network Interfaces, Referred To As Triple-Homed.

- One Interface Is The Dmz
- The Second Is The Public One
- The Third Connects To The Lan

East-West Traffic - Traffic That Goes To And From A Data Center Is Referred To As **North-South**. This Traffic Represents Clients Outside The Data Center Making Requests.

However In Data Centers That Support Cloud Services, Most Traffic Is Actually Between Servers Within That Data Center And This Traffic Is Referred To As **East-West** Traffic.

Zero Trust - This Is Based On The Idea That Perimeter Security Is Unlikely To Be Robust Enough. As Such In A Zero Trust Model, Continuous Authentication And Conditional Access Are Used To Mitigate Threats.

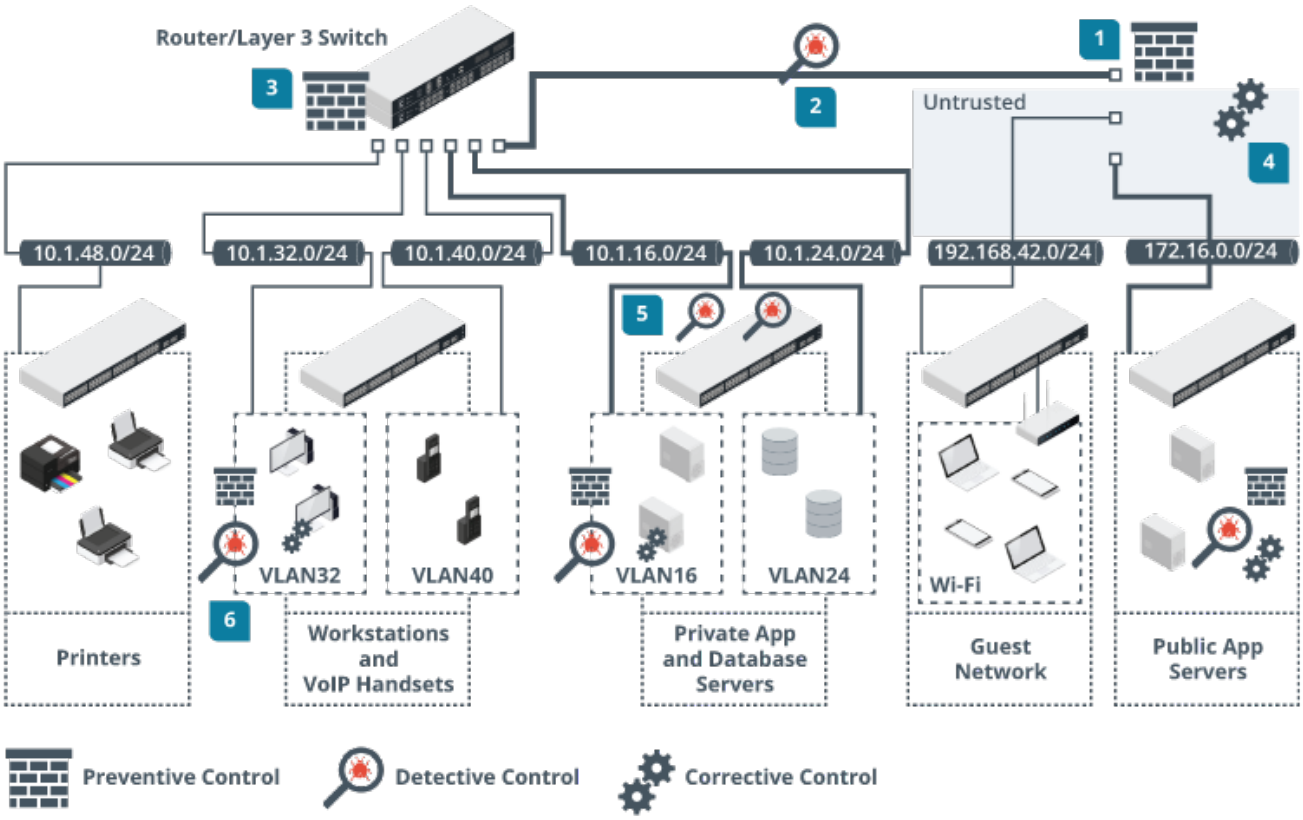
Zero Trust Also Uses A Technique Called **Microsegmentation**. This Is A Security Process That Is Capable Of Applying Policies To A Single Node As Though It Was In A Zone Of Its Own.

5.3 Device Placement & Attributes

The process of choosing the type and placement of security controls to ensure the goals of the CIA triad and compliance with any framework requirements.

The selection of effective controls is governed by the principle of defense in depth.

- **Preventive Controls** - Are often placed at the border of a network segment or zone. Preventive controls such as firewalls enforce security policies on traffic entering and exiting the segment, ensuring confidentiality and integrity. A load balancer control ensures high availability for access to the zone.
- **Detective Controls** - Might be placed within the perimeter to monitor traffic exchanged between hosts within the segment. This provides alerting of malicious traffic that has evaded perimeter controls.
- **Preventive, Detective & Corrective Controls** - Might be installed on hosts as a layer of endpoint protection in addition to the network infrastructure controls.



Attributes determine the precise way in which a device can be placed within the network topology

A **passive security control** is one that does not require any sort of client or agent configuration or host data transfer to operate.

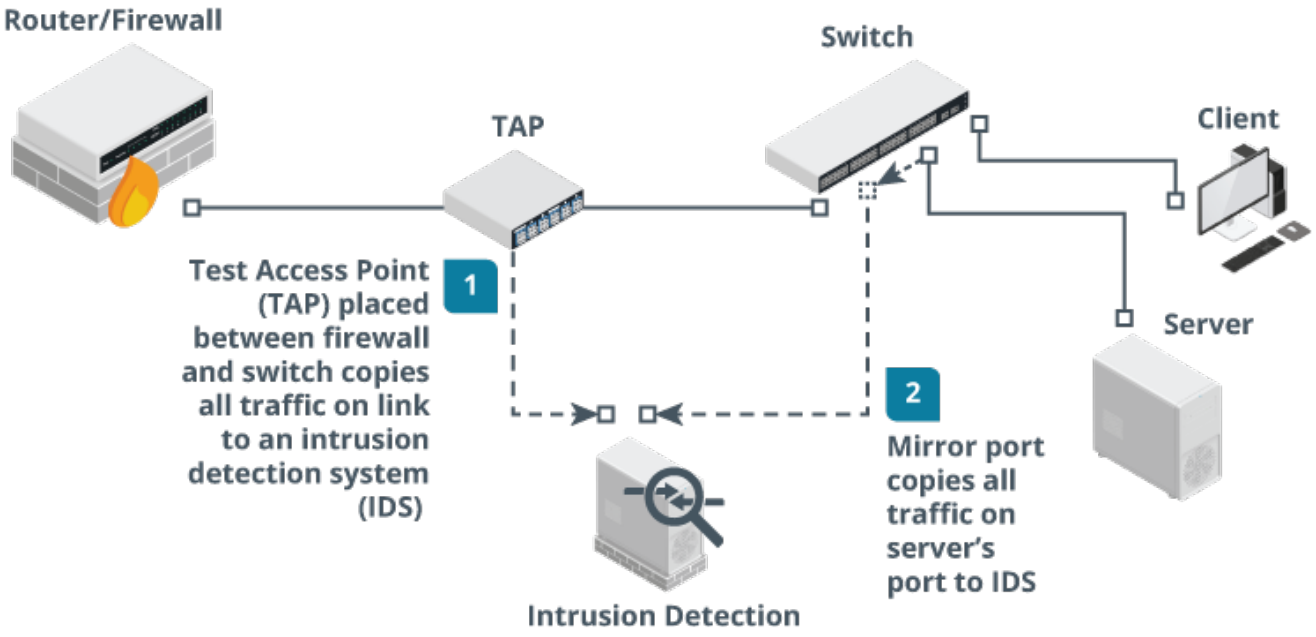
An **active security control** that performs scanning must be configured with credentials and access permissions and exchange data with target hosts. An active control that performs filtering requires hosts to be explicitly configured to use the control. This might mean installing agent software on the host, or configuring network settings to use the control as a gateway.

Inline vs Monitor

A device that is deployed inline becomes part of the cable path. No changes in the IP or routing topology are required. The device's interfaces are not configured with MAC or IP addresses.

SPAN (Switched Port Analyzer)/Mirror Port - This means that the sensor is attached to a specially configured monitor port on a switch that receives copies of frames addressed to nominated access ports (or all the other ports). This method is not completely reliable. Frames with errors will not be mirrored and frames may be dropped under heavy load

Test Access Point (TAP) - This is a box with ports for incoming and outgoing network cabling and an inductor or optical splitter that physically copies the signal from the cabling to a monitor port. Unlike SPAN every single frame is copied or received.



Fail-Open versus Fail-Closed

A security device could enter a failure state for a number of reasons. There could be a power or hardware fault, an irreconcilable policy violation, or a configuration error. Hardware failure can be caused by power surges, overheating, and physical damage.

Software failure can occur because of bugs, security vulnerabilities, and compatibility issues. Configuration issues can be caused by human errors such as inattention, fatigue, or lack of training.

When a device fails, it can be configured to fail-open or fail-closed

- Fail-open means that network or host access is preserved. This mode prioritizes availability over confidentiality and integrity.
- Fail-closed means that access is blocked. This mode prioritizes confidentiality and integrity over availability.

5.4 Device Placement & Attributes

Man-In-The-Middle & Layer 2 Attacks - Most Attacks At Layer 1 And 2 Of The Osi Model Are Typically Focused On Information Gathering Through Network Mapping And Eavesdropping.

A MITM can also be performed on this layer due to the lack of security.

MAC cloning or **MACaddress spoofing -** Changes the hardware address of an adapter to an arbitrary one either by overriding the original address in software via os commands or with the use of packet crafting software.

Arp Poisoning Attack - Arp poisoning attack uses a packet crafter such as ettercap to broadcast unsolicited arp reply packets.

Because arp has no security mechanism, the receiving devices trust this communication and update their mac:ip address cache table with the spoofed address.

MAC flooding attacks - Where arp poisoning is directed at hosts, mac flooding is used to attack a switch.

The idea here is to exhaust the memory used to store the switch's mac address table which is used by the switch to determine which port to use to forward unicast traffic to its correct destination.

Overwhelming the table can cause the switch to stop trying to apply mac-based forwarding and simply flood unicast traffic out of all ports.

Router / Switch Security

- **Physical Port Security -** Access to physical switch ports and hardware should be restricted to authorized staff by using a secure server room or lockable hardware cabinets.
- **Mac Limiting/Filtering -** Configuring mac filtering on a switch means defining which mac addresses are allowed to connect to a particular port by creating a list of valid mac addresses. mac limiting involves specifying a limit to the number of permitted addresses that can connect to a port.
- **Dhcp Snooping -** Dynamic host configuration protocol is one that allows a server to assign an ip address to a client when it connects to a network. dhcp snooping inspects this traffic arriving on access ports to ensure that a host is not trying to spoof its mac address. with dhcp snooping, only dhcp messages from ports configured as trusted are allowed.
- **Network Access Control -** Nac products can extend the scope of authentication to allow admins to devise policies or profiles describing a minimum security configuration that devices must meet to be granted network access. This is called a health policy.
- **Route Security -** A successful attack against route security enables the attacker to redirect traffic from its intended destination. routes between networks and subnets can be configured manually, but most routers automatically discover routes by communicating with each other.

routing is subject to numerous vulnerabilities

- **Spoofed Routing Information (Route Injection) -** Traffic is misdirected to a monitoring port (sniffing) or continuously looped around the network causing dos.
- **Source Routing -** This uses an option in the ip header to pre-determine the route a packet will take through the network. This can be used to spoof ip addresses and bypass router/firewall filters.
- **Software Exploits In The Underlying Operating System -** Cisco devices typically use the internetwork operating system (ios) which suffer from fewer exploitable vulnerabilities than full network operating systems.

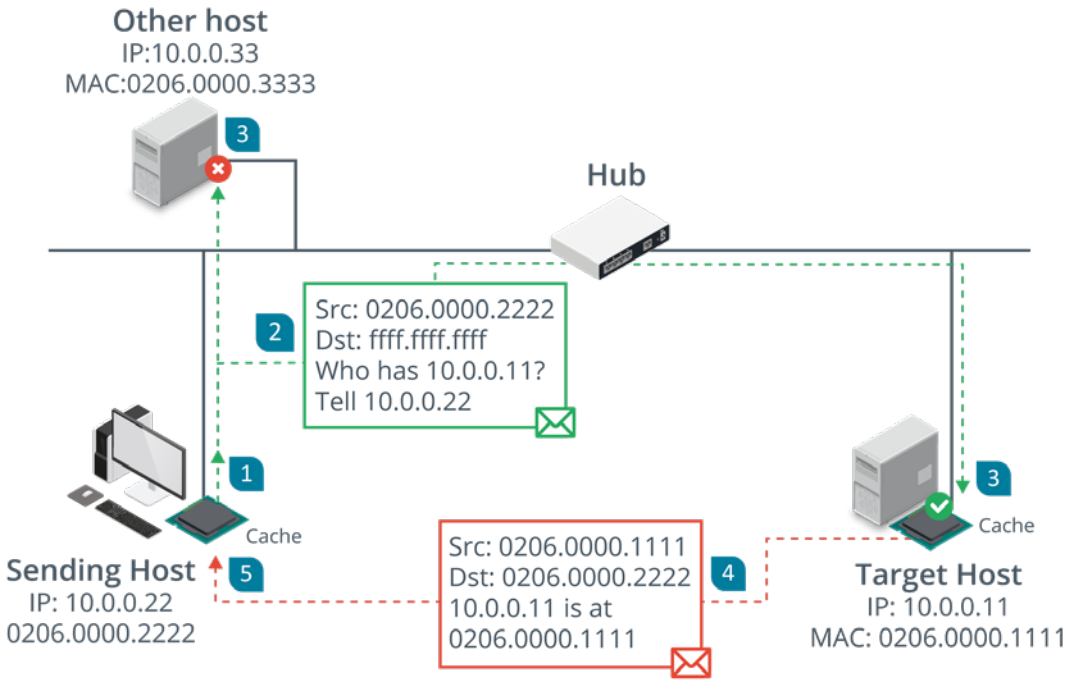
5.5 Routing & Switching Protocols

Layer 3 Forwarding Or Routing Occurs Between Both Logically And Physically Defined Networks. A Single Network Divided Into Multiple Logical Broadcast Domains Is Said To Be Subnetted.

At Layer 3, Nodes Are Identified By Ip Addresses.

Address Resolution Protocol (Arp) - This Maps A Mac Address To An Ip Address.

Normally A Device That Needs To Send A Packet To An Ip Address But Does Not Know The Receiving Device's Mac Address Broadcasts Will Broadcast An Arp Request Packet And The Device With The Matching Ip Responds With An Arp Reply.



Internet Protocol (Ip)

This Provides The Addressing Mechanism For Logical Networks And Subnets.

172.16.1.101/16

The /16 Prefix Indicates That The First Half Of The Address (172.16.0.0) Is The Network Id While The Remainder Uniquely Identifies A Host On That Network. Networks Also Use 128-Bit Ipv6 Addressing.

2001:Db8::Abc:0:Def0:1234

The First 64-Bits Contain Network Information While The Last Are Fixed As The Host's Interface Id.

A Route To A Network Can Be Configured Statically But Most Networks Use Routing Protocols To Transmit New And Updated Routes Between Routers.

Some Common Routing Protocols Include

- Border Gateway Protocol (Bgp)
- Open Shortest Path First (Ospf)
- Enhanced Interior Gateway Routing Protocol (Eigrp)
- Routing Information Protocol (Rip)

5.6 Using Secure Protocols

Secure protocols have places in many parts of your network and infrastructure. Security professionals need to be able to recommend the right protocol for each of the following scenarios:

- Voice and video rely on a number of common protocols. Videoconferencing tools often rely on HTTPS, but secure versions of the Session Initiation Protocol (SIP) and the Real-time Transport Protocol (RTP) exist in the form of SIPS and SRTP, which are also used to ensure that communications traffic remains secure.
- A secure version of the Network Time Protocol (NTP) exists and is called NTS, but NTS has not been widely adopted. Like many other protocols you will learn about in this chapter, NTS relies on TLS. Unlike other protocols, NTS does not protect the time data. Instead, it focuses on authentication to make sure that the time information is from a trusted server and has not been changed in transit.
- Email and web traffic relies on a number of secure options, including HTTPS, IMAPS, POPS, and security protocols like Domain-based Message Authentication Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) as covered earlier in this chapter.
- File Transfer Protocol (FTP) has largely been replaced by a combination of HTTPS file transfers and SFTP or FTPS, depending on organizational preferences and needs.
- Directory services like LDAP can be moved to LDAPS, a secure version of LDAP.

- Remote access technologies—including shell access, which was once accomplished via telnet and is now almost exclusively done via SSH—can also be secured. Microsoft's RDP is encrypted by default, but other remote access tools may use other protocols, including HTTPS, to ensure that their traffic is not exposed.
- Domain name resolution remains a security challenge, with multiple efforts over time that have had limited impact on DNS protocol security, including DNSSEC and DNS reputation lists.
- Routing and switching protocol security can be complex, with protocols like Border Gateway Protocol (BGP) lacking built-in security features. Therefore, attacks such as BGP hijacking attacks and other routing attacks remain possible. Organizations cannot rely on a secure protocol in many cases and need to design around this lack.
- Network address allocation using DHCP does not offer a secure protocol, and network protection against DHCP attacks relies on detection and response rather than a secure protocol.
- Subscription services such as cloud tools and similar services frequently leverage HTTPS but may also provide other secure protocols for their specific use cases. The wide variety of possible subscriptions and types of services means that these services must be assessed individually with an architecture and design review, as well as data flow reviews all being part of best practices to secure subscription service traffic if options are available.

5.7 Attack Surface

The network attack surface refers to all the points at which a threat actor could gain access to hosts and services.

Using the OSI model we can analyze the potential attack surface:

- **Layer 1/2 -** Allows the attacker to connect to wall ports or wireless networks and communicate with hosts within the same broadcast domain
- **Layer 3 -** Allows the attacker to obtain a valid network address possibly by spoofing and communicate with hosts in other zones
- **Layer 4/7 -** Allows the attacker to establish connections to TCP or UDP ports and communicate with application layer protocols and services.

Each layer requires its own type of security controls to prevent, detect, and correct attacks. Provisioning multiple control categories and functions to enforce multiple layers of protection is referred to as **defense in depth.**

Security controls deployed to the network perimeter are designed to prevent external hosts from launching attacks at any network layer. The division of the private network into segregated zones is designed to mitigate risks from internal hosts that have either been compromised or that have been connected without authorization.

Typical weaknesses in a network include:

- Single points of failure
- Complex dependencies
- Availability over confidentiality and integrity
- Lack of documentation
- Over dependence on perimeter security

5.8 Firewalls

Packet Filtering Firewalls - These are the earliest type of firewalls and are configured by specifying a group of rules called an access control list (acl).

Each rule defines a specific type of data packet and the appropriate action to take when a packet matches the rule. an action can either be to deny or to accept the packet.

This firewall can inspect the headers of ip packets meaning that the rules can be based on the information found in those headers.in certain cases, the firewall can control only inbound or both inbound and outbound traffic and this is often referred to as **ingress** and **egress** traffic or filtering.

A basic packet filtering firewall is stateless meaning that it does not preserve any information about network sessions. The least processing effort is required for this but it can be vulnerable to attacks that are spread over a sequence of packets.

Stateful Inspection Firewalls - This type of firewall can track information about the session established between two hosts and the session data is stored in a state table.

When a packet arrives, the firewall checks it to confirm that it belongs to an existing connection and if it does then the firewall would allow the traffic to pass unmonitored to conserve processing effort.

Stateful inspection can occur at two layers: transport and application.

Transport Layer (Osi Layer 4) - Here, the firewall examines the tcp three-way handshake to distinguish new from established connections.

syn > syn/ack > ack

Any deviations from this sequence can be dropped as malicious flooding or session hijacking attempts.

Application Layer (Osi Layer 7) - This type of firewall can inspect the contents of packets at the application layer and one key feature is to verify the application protocol matches the port e.g http web traffic will use port 80.

Ip Tables - Iptables s a command on linux that allows admins to edit the rules enforced by the linux kernel firewall.

Iptables works with chains which apply to the different types of traffic such as the input chain for traffic destined for the local host. Each chain has a default policy set to drop or allow traffic that does not match a rule.

The rules in this example will drop any traffic from the specific host 10.1.0.192 and allow icmp echo requests (pings), dns and http/https traffic either from the local subnet (10.1.0.0/24) or from any network (0.0.0.0/0)

```
Chain INPUT (policy DROP)

# target prot opt source   destination

1 DROP  all -- 10.1.0.192  0.0.0.0/0

2 ACCEPT icmp -- 10.10.0.0/24 0.0.0.0/0 icmptype 8

3 ACCEPT udp -- 0.0.0.0/0  0.0.0.0/0  udp dpt:53

4 ACCEPT tcp -- 0.0.0.0/0  0.0.0.0/0  tcp dpt:53

5 ACCEPT tcp -- 10.1.0.0/24 0.0.0.0/0  tcp dpt:80

6 ACCEPT tcp -- 10.1.0.0/24 0.0.0.0/0  tcp dpt:443

7 ACCEPT all -- 0.0.0.0/0  0.0.0.0/0  ctstate RELATED,ESTABLISHED
```

5.9 Firewall Implementation

Firewall Appliances - This Is A Stand-Alone Firewall Deployed To Monitor Traffic Passing Into And Out Of A Network Zone. It Can Be Deployed In Two Ways:

- **Routed (Layer 3) -** The Firewall Performs Forwarding Between Subnets
- **Bridged (Layer 2) -** The Firewall Inspects Traffic Between Two Nodes Such As A Router And A Switch.

Application-Based Firewalls

- **Host-Based (Personal) -** Implemented As A Software Application Running On A Single Host Designed To Protect The Host Only.
- **Application Firewall -** Software Designed To Run On A Server To Protect A Particular Application Only
- **Network Operating System (Nos) Firewall -** A Software Based Firewall Running Under A Network Server Os Such As Windows Or Linux.

Proxies And Gateways - A Firewall That Performs Application Layer Filtering Is Likely To Be Implemented As A Proxy.

Proxy Servers Can Either Be Non-Transparent Or Transparent.

- Non-Transparent Means The Client Must Be Configured With The Proxy Server Address And Port Number To Use It
- Transparent (Forced Or Intercepting) Intercepts Client Traffic Without The Client Having To Be Reconfigured

Reverse Proxy Servers - These Provide For Protocol-Specific Inbound Traffic.

A Reverse Proxy Can Be Deployed On The Network Edge And Configured To Listen For Client Requests From A Public Network

5.10 Remote Access Architecture

Most Remote Access Is Implemented As A Virtual Private Network (Vpn) Running Over The Internet But It Can Be More Difficult To Ensure The Security Of Remote Workstations And Servers Than Those On The Lan. A Vpn Can Also Be Deployed In A Site-To-Site Model To Connect Two Or More Private Networks And Is Typically Configured To Operate Automatically

Openvpn - This Is An Open Source Example Of A Tls Vpn. Openvpn Can Work In Tap (Bridged) Mode To Tunnel Layer 2 Frames Or In Tun (Routed) Mode To Forward Ip Packets.

Another Option Is Microsoft's Secure Sockets Tunneling Protocol (Sstp) Which Works By Tunneling Point-To-Point Protocol (Ppp) Layer 2 Frames Over A Tls Session.

Internet Protocol Security (Ipsec) - Tls Is Applied At The Application Level Either By Using A Separate Secure Port Or By Using Commands In The Application Protocol To Negotiate A Secure Connection.

Ipsec Operates At The Network Layer (Layer 3) So It Can Operate Without Having To Configure Specific Application Support.

Authentication Header (Ah) - This Performs A Cryptographic Hash On The Whole Packet Including The Ip Header Plus A Shared Secret Key And Adds This Hmac In Its Header As Integrity Check Value (Icv)

The Recipient Performs The Same Function On The Packet And Key And Should Derive The Same Value To Confirm That The Packet Has Not Been Modified.

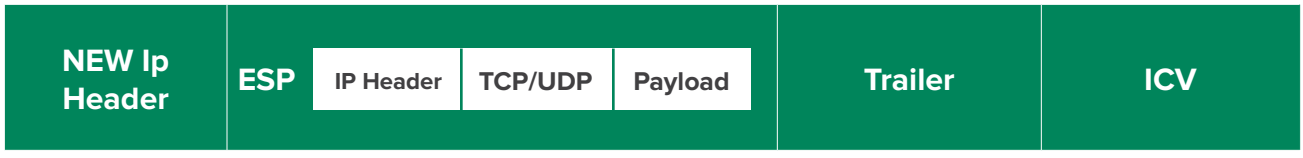
Encapsulation Security Payload (Esp) - This Provides Confidentiality And/Or Authentication And Integrity. It Can Be Used To Encrypt The Packet Rather Than Simply Calculating An Hmac.

Esp Attaches Three Fields To The Packet: A Header, A Trailer (Providing Padding For The Cryptographic Function) And An Icv.

Ipsec Transport And Tunnel Modes - Ipsec Can Be Used In Two Modes:

- **Transport Mode -** This Mode Is Used To Secure Communications Between Hosts On A Private Network. Here The Ip Header For Each Packet Is Not Encrypted, Just The Payload Data. If Ah Is Used In This Mode, It Can Provide Integrity For The Ip Header.

- **Tunnel Mode -** This Mode Is Used For Communications Between Vpn Gateways Across An Unsecure Network And Is Also Referred To As Router Implementation. With Esp, The Whole Ip Packet (Header And Payload) Is Encrypted And Encapsulated As A Datagram With A New Ip Header.



Internet Key Exchange (Ike) - Ipsec's Encryption And Hashing Functions Depend On A Shared Secret. The Secret Must Be Communicated To Both Hosts And The Hosts Must Confirm One Another's Identity (Mutual Authentication) Otherwise The Connection Is Vulnerable To Mitm And Spoofing Attacks. The Ike Protocol Handles Authentication And Key Exchange Referred To As Security Associations (Sa).

Ike Negotiations Take Place Over Two Phases:

Phase 1 Establishes The Identity Of The Two Hosts And Performs Key Agreement Using The Dh Algorithm To Create A Secure Channel. Digital Certificates And Pre-Shared Key Are Used For Authenticating Hosts.

Phase 2 Uses The Secure Channel Created In Phase 1 To Establish Which Ciphers And Key Sizes Will Be Used With Ah And/Or Esp In The Ipsec Session.

Vpn Client Configuration - To Configure A Vpn Client, You May Need To Install The Client Software If The Vpn Type Is Not Natively Supported By The Os.

Always-On Vpn - This Means That The Computer Establishes The Vpn Whenever An Internet Connection Over A Trusted Network Is Detected, Using The User's Cached Credentials To Authenticate.

When A Client Connected To A Remote Access Vpn Tries To Access Other Sites On The Internet, There Are Two Ways To Manage The Connection:

Split Tunnel - The Client Accesses The Internet Directly Using Its "Native" Ip Configuration And Dns Servers.

Full Tunnel - Internet Access Is Mediated By The Corporate Network, Which Will Alter The Client's Ip Address And Dns Servers And May Use A Proxy.

Full Tunnel Offers Better Security But The Network Address Translations And Dns Operations Required May Cause Problems With Some Websites Especially Cloud Services.

Out-Of-Band Management - Remote Management Methods Can Be Described As Either In-Band Or Out-Of-Band (Oob).

An **In-Band** Management Link Is One That Shares Traffic With Other Communications On The "Production" Network While A Serial Console Or Modem Port On A Router Is A Physically **Out-Of-Band** Management Method.

Secure Shell - This Is The Principal Means Of Obtaining Secure Remote Access To A Command Line Terminal. Mostly Used For Remote Administration And Secure File Transfer (Sftp).

Ssh Servers Are Identified By A Public/Private Key Pair (The Host Key).

SECTION 6 -

SECURE CLOUD NETWORK ARCHITECTURE

6.1 Cloud Deployment Models

Public (multi-tenant) - A service offered over the internet by cloud service providers (csps) to cloud consumers

Hosted Private - Hosted by a third party for the exclusive use of an organization. Better performance but more expensive than public.

Private - Cloud infrastructure that is completely private and owned by the organization. Geared more towards banks and governmental services where security and privacy is of utmost importance.

Community - Several organizations share the costs of either a hosted private or fully private cloud.

Cloud Service Models - Cloud services can also be differentiated on the level of complexity and pre-configuration provided (sometimes referred to as anything as a service xaas)

Most common implementations are infrastructure, software and platform.

Infrastructure As A Service (IAAS) - It resources (servers, load balancers and san) are provided here. Examples include amazon elastic compute cloud, oracle cloud and microsoft azure virtual machines.

Software As A Service (SAAS) - Provisioning of software applications and can be purchased on a pay-as-you-go or lease arrangement. Examples are microsoft 365, salesforce and adobe creative cloud.

Platform As A Service (PAAS) - Provides resources somewhere between saas and iaas. A typical paas solution would provide servers and storage network infrastructure and also a web-application or database platform on top.

Examples include oracle database, microsoft azure sql database and google app engine.

Security As A Service

- **Consultants -** Can Be Used For Framework Analysis Or For More Specific Projects.
- **Managed Security Services Provider (Mssp) -** Fully Outsourcing Responsibility For Information Assurance To A Third Party. Can Be Expensive But A Good Fit For An Sme That Has No In-House Security Capability.
- **Security As A Service (Secaas) -** Can Mean A Lot Of Things But Typically Means Implementing A Particular Security Control Such As Malware Scanning In The Cloud. Examples Include Cloudflare, Mandiant/Fireeye And Sonicwall.

6.2 Responsibility Matrix

The shared responsibility model describes the balance of responsibility between a customer and a cloud service provider (CSP) for implementing security in a cloud platform.

The division of responsibility becomes more or less complicated based on whether the service model is SaaS, PaaS, or IaaS. For example, in a SaaS model, the CSP performs the operating system configuration and control as part of the service offering.

In contrast, operating system security is shared between the CSP and the customer in an IaaS model.

A **responsibility matrix** sets out these duties in a clear table.

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and Accountability	●	●	●	●	●	✓	✓
Client and end-point Protection	●	●	●	◪	◪	✓	✓
Identity and access Management	●	●	◪	◪	◪	✓	✓
Application-level Controls	●	●	◪	◪	◪	✓	✓
Network Controls	●	◪	●	●	●	✓	✓
Host Infrastructure	●	◪	●	●	●	✓	
Physical Security	●	●	●	●	●		

● Cloud customer ● Cloud provider

6.3 Cloud Security Solutions

Cloud computing is also a means of transferring risk and as such it is important to identify which risks are being transferred and what responsibilities both the company and service provider will undertake.

A company will always still be held liable for legal and regulatory consequences in case of a security breach though the service provider could be sued for the breach.

The company will also need to consider the legal implications of using a csp if its servers are located in a different country.

Application security in the cloud refers both to the software development process and to the identify and access management (iam) features designed to ensure authorized use of applications.

Cloud provides resources abstracted from physical hardware via one or more layers of virtualization and the compute component provides process and system memory (ram) resources as required for a particular workload.

High availability - one of the benefits of using the cloud is the potential for providing services that are resilient to failures at different levels.

In terms of storage performance, high availability (ha) refers to storage provisioned with a guarantee of 99.99% Uptime or better and the csp typically uses redundancy to make multiple disk controllers and storage devices available to a pool of storage resources.

Replication - data replication allows businesses to copy data to where it can be utilized most effectively and the cloud may be used as a central storage area.

The terms hot and cold storage refer to how quickly data is retrieved and hot storage is quicker but also more expensive to manage.

- **Local replication -** Replicates data within a single data center in the region where the storage account was created.
- **Regional replication -** Replicates data across multiple data centers within one or two regions.
- **Geo-redundant storage (grs) -** Replicates data to a secondary region that is distant from the primary region. This safeguards data in the event of a regional outage or a disaster.
- **Virtual private clouds (vpcs) -** each customer can create one or more vpcs attached to their account. By default, a vpc is isolated from other csp accounts and from other vpcs operating in the same account.

Each subnet within a vpc can either be private or public. For external connectivity that isn't appropriate for public.

Routing can be configured between subnets in a vpc and between vpcs in the same

account or with vpcs belonging to different accounts.

Configuring additional vpcs rather than subnets within a vpc allows for a greater degree of segmentation between instances.

A vpc endpoint is a means of publishing a service that is accessible by instances in other vpcs using only the aws internal network and private ip addresses. There are two types - gateway and interface

- **Cloud firewall security -** Filtering decisions can be made based on packet headers and payload contents at various layers
- **Network layer 3 -** The firewall accepts/denies connections based on the ip addresses or address ranges and tcp/udp port numbers (actually contained in layer 4 headers but the functionality is still always described as layer 3 filtering).
- **Transport layer 4 -** The firewall can store connection states and use rules to allow established traffic.
- **Application layer 7 -** The firewall can parse application protocol headers and payloads and make decisions based on their contents.

Firewalls in the cloud can be implemented in several ways to suit different purposes.

- As software running on an instance
- As a service at the virtualization layer to filter traffic between vpc subnets and instances. This equates to an on-premises network firewall.

Cloud access security brokers (casb) -CASBs provide you with visibility into how clients and other network nodes are using cloud services.

- Enable single sign-on authentication and enforces access controls and authorizations from the enterprise network to the cloud provider
- Scan for malware and rouge devices
- Monitor and audit user and resource activity
- Mitigate data exfiltration

Casbs are implemented in one of three ways:

- **Forward proxy -** positioned at the client network edge that forwards user traffic to the cloud network
- **Reverse proxy -** positioned at the cloud network edge and directs traffic to cloud services
- api

6.4 - Infrastructure As Code Concepts

Service-Oriented Architecture (Soa) - This Conceives Of Atomic Services Closely Mapped To Business Workflows. Each Service Takes Defined Inputs And Produces Defined Outputs.

Service Functions Are Self-Contained, Do Not Rely On The State Of Other Services And Expose Clear Input/Output (I/O) Interfaces.

Microservices - Microservice-Based Development Shares Many Similarities With Agile Software Project Management And The Processes Of Continuous Delivery And Deployment.

The Main Difference From Soa Is That While Soa Allows A Service To Be Built From Other Services, Each Microservice Should Be Capable Of Being Developed, Tested And Deployed Independently (Highly Decoupled)

Services Integration - Service Integration Refers To Ways Of Making These Decoupled Services Work Together To Perform A Workflow. Where Soa Used The Concept Of An Enterprise Service Bus, Microservices Integration And Cloud Services/Virtualization, Integration Generally Is Very Often Implemented Using **Orchestration** Tools.

Automation Focuses On Making A Single Discrete Task Easily Repeatable While Orchestration Performs A Sequence Of Automated Tasks.

Cloud Orchestration Platforms Connect To And Provide Administration, Management And Orchestration For Many Popular Cloud Platforms And Services.

Application Programming Interfaces (Api) - Soa, Microservices, Service Integration, Automation And Orchestration All Depend On Apis

- **Simple Object Access Protocol (Soap) -** Uses Xml Format Messaging And Has A Number Of Extensions In The Form Of Web Services Standards That Support Common Features Such As Authentication, Transport Security And Asynchronous Messaging.
- **Representational State Transfer (Rest) -** A Much Looser Architectural Framework Also Referred To As Restful Api. Soap Requests Must Be Sent In Correctly Formatted Xml Document While Rest Requests Can Be Submitted As An Http Operation.

Serverless architecture - This is a modern design pattern for service delivery and is strongly associated with modern web applications - netflix.

billing is based on execution time rather than hourly charges and this type of service provision is also called function as a service (FAAS).

Serverless architecture eliminates the need to manage physical or virtual server instances so there is no need for software and patches or file system security monitoring.

Infrastructure as code - An approach to infrastructure management where automation and orchestration fully replace manual configuration is referred to as infrastructure as code (IAC)

The main objective of iac is to eliminate snowflake systems which are basically systems that

are different from others and this can happen when there is a lack of consistency in terms of patch updates and stability issues.

By rejecting manual configuration of any kind, iac ensures idempotence which means making the same call with the same parameters will always produce the same result.

Iac means using carefully developed and tested scripts and orchestration runbooks to generate consistent builds.

Fog & Edge Computing - Traditional data center architecture sensors are quite likely to have low bandwidth and higher latency WAN links to data networks.

Fog computing developed by cisco addresses this by placing fog node processing resources close to the physical location for the iot sensors. The sensors communicate with the fog node using wi-fi or 4g/5g and the fog node prioritizes traffic, analyzes and remediates alertable conditions.

Edge Computing Is A Broader Concept Partially Developed From Fog Computing.

- Edge Devices Collect And Depend Upon Data For Their Operation.
- Edge Gateways Perform Some Pre-Processing Of Data To And From Edge Devices To Enable Prioritization.
- Fog Nodes Can Be Incorporated As A Data Processing Layer Positioned Closed To The Edge Gateways.
- The Cloud Or Data Center Layer Provides The Main Storage And Processing Resources Plus Distribution And Aggregation Of Data Between Sites.

Instead of depending on a cluster of clouds for computing and data storage, edge computing leverages local computing (routers, PCs, smartphones) to produce shorter response time as the data is processed locally.

6.5 Zero Trust

This is a security framework requiring all subjects, assets and workflows to be authenticated, authorized and continuously validated before being granted or keeping access to the data or application.

Zero Trust View

- **No Implicit Zone Trust -** Assets should always act as though an attacker was present in the enterprise network
- Devices on the network cannot be owned or configured by users
- Assume all network connections are insecure

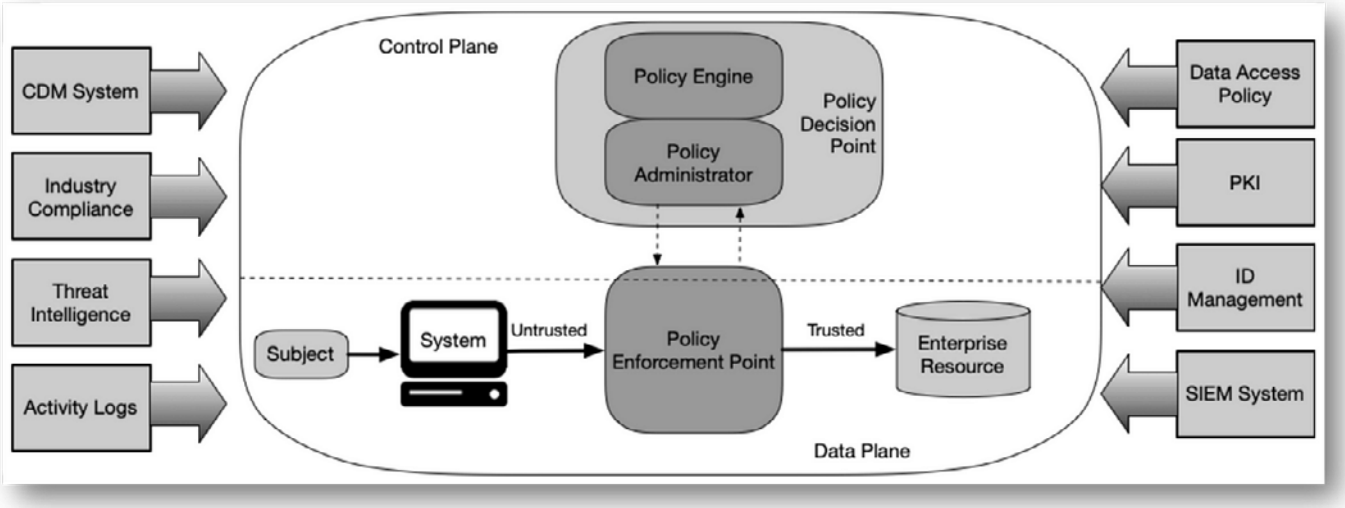
Zero Trust Core Principles (NIST SP800-207)

- **Continuous Verification -** Always verify access all the time
- **Access Limitation -** Access to resources are granted strictly on a per-session basis

- **Limit the "Blast Radius" -** Minimize the impact of a breach
- **Automate -** Automate context, collection and response for credentials, workloads, threat intelligence and endpoints

Control & Data Planes

- **Control Plane -** Used by infrastructure components to maintain and configure assets, access control and communication security.
- **Data Plane -** Used for communication between software components.



Zero Trust Architecture

Zero Trust Logical Components

- **Policy Decision Point (PDP) -** The gatekeeper and is made up of the policy engine and policy administrator.
- **Policy Engine (PE) -** is responsible for granting access to a resource
- **Policy Administrator (PA) -** generates any session-specific authentication token or credential used to access an enterprise resource.
- **Policy Enforcement Point (PEP) -** is responsible for enabling, monitoring and terminating connections between a subject and an enterprise resource.

Zero Trust Disadvantages

- Can be complex and expensive
- Slows down application performance
- Hampers employee productivity

6.6 Embedded Systems

This Is A Complete System Designed To Perform A Specific Dedicated Function.

These Systems Can Be A Microcontroller In A Small Device Or Could Be As Large And Complex As The Network Of Control Devices Managing A Water Treatment Plant.

Embedded Systems Are Characterized As Static Environments While A Pc Is A Dynamic Environment Because Both Software And Hardware Changes Can Be Made By The User.

Embedded Systems Are Usually Constrained By:

- Processor Capability
- System Memory
- Persistent Storage
- Cost
- Power (Battery)
- Authentication Technologies
- Cryptographic Identification
- Network And Range Constraints

Raspberry Pi And Arduino Are Examples Of Soc Boards Initially Devised As Educational Tools But Now Widely Used For Industrial Applications And Hacking.

Field Programmable Gate Array (Fpga) - As Many Embedded Systems Perform Simple And Repetitive Operations, It Is More Efficient To Design The Hardware Controller To Perform Only The Instructions Needed.

An Example Of This Is The Application-Specific Integrated Circuits (Asics) Used In Ethernet Switches But They Can Be Quite Expensive And Work Only For A Single Application.

An Fpga Solves The Problem Because The Structure Is Not Fully Set At The Time Of Manufacture Giving The End Customer The Ability To Configure The Programming Logic Of The Device To Run A Specific Application.

Operational Technology (Ot) Networks - These Are Cabled Networks For Industrial Applications And Typically Use Either Serial Data Protocols Or Industrial Ethernet.

Industrial Ethernet Is Optimized For Real-Time And Deterministic Transfers.

Cellular Networks - A Cellular Network Enables Long-Distance Communication Over The Same System That Supports Mobile And Smartphones.

Also Known As Baseband Radio And There Are Two Main Radio Technologies:

- **Narrowband-Iot (Nb-Iot) -** This Refers To Low-Power Version Of The Long Term Evolution (Lte) Or 4g Cellular Standard.
- **Lte Machine Type Communication (Lte-M) -** This Is Another Low-Power System But Supports Higher Bandwidth (Up To About 1 Mbps)

Any Lte-Based Cellular Radio Uses A Subscriber Identity Module (Sim) Card As An Identifier. The Sim Is Issued By A Cellular Provider With Roaming To Allow The Use Of Other Supplier's Tower Relays.

6.7 Industrial Control Systems & Internet Of Things

Industrial Systems Have Different Priorities To It Systems And Tend To Prioritize Availability And Integrity Over Confidentiality (Reversing The Cia Triad As The Aic Triad)

Workflow And Process Automation Systems - Industrial Control Systems (Icss) Provide Mechanisms For Workflow And Process Automation And These Systems Control Machinery Used In Critical Infrastructure Like Power And Water Suppliers And Health Services.

An Ics Comprises Plant Devices And Equipment With Embedded PLCs.

Supervisory Control And Data Acquisition (SCADA) - A SCADA System Takes The Place Of A Server In Large Scale Multiple-Site Icss. Scada Typically Run As Software On Ordinary Computers, Gathering Data From And Managing Plant Devices And Equipment With Embedded Plcs Referred To As Field Devices.

Ics/Scada Applications - These Types Of Systems Are Used Within Many Sectors Of Industry

- Power Generation And Distribution
- Mining And Refining Raw Materials
- Fabrication And Manufacturing
- Logistics
- Site And Building Management Systems

Internet Of Things (IoT) - This Is Used To Describe A Global Network Of Appliances And Personal Devices That Have Been Equipped With Sensors, Software And Network Connectivity.

SECTION 7 -

EXPLAIN RESILIENCY AND SITE SECURITY CONCEPTS

7.1 Backup Strategies & Storage

Backups & Retention Policies - As Backups Take Up Space, There Is The Need For Storage Management Routines While Also Giving Adequate Coverage Of The Required Window.

The Recovery Window Is Determined By The Recovery Point Objective (Rpo) Which Is Determined Through Business Continuity Planning.

Backup Types

- Full includes all files and directories while incremental and differential check the status of the archive attribute before including a file. The archive attribute is set whenever the file is modified so the backup software knows which files have been changed and need to be copied.
- Incremental makes a backup of all new files as well as files modified since the last backup while differential makes a backup of all new and modified files since the last full backup. Incremental backups save backup time but can be more time-consuming when the system must be restored. The system is restored first from the last full backup set and then from each incremental backup that has subsequently occurred.

Snapshots And Images - Snapshots Are Used For Open Files That Are Being Used All The Time Because Copy-Based Mechanisms Are Not Able To Backup Open Files.

In Windows, Snapshots Are Provided For On Ntfs By The Volume Shadow Copy Service (Vss).

Backup Storage Issues - Backups Require Cia As Well And Must Be Secured At All Times. Natural Disasters Such As Fires And Earthquakes Must Also Be Accounted For.

Distance Consideration Is A Calculation Of How Far Offsite Backups Need To Be Kept Given Different Disaster Scenarios However They Mustn't Be Too Far To Slow Down A Recovery Operation.

The 3-2-1 Rule States That You Should Have 4 Copies Of Your Data Across Two Media Types With One Copy Held Offline And Offsite.

Backup Media Types

- Disk
- **Network attached storage (nas) -** An appliance that is a specially configured type of server that makes raid storage available over common network protocols
- **Tape -** Very cost effective and can be transported offsite but slow compared to disk-based solutions especially for restore operations
- San & cloud

Restoration order - If a site suffers an uncontrolled outage, ideally processing should be switched to an alternate site. However, if an alternate processing site is not available, then the main site must be brought back online as quickly as possible to minimize service disruption.

A complex facility such as a data center or campus network must be reconstituted according to a carefully designed order of restoration.

- Enable and test power delivery systems (grid power, ups, secondary generators and so on)
- Enable and test switch infrastructure then routing appliances and systems
- Enable and test network security appliances (firewalls, ids)
- Enable and test critical network servers (dhcp. dns, ntp and directory services)
- Enable and test back-end and middleware (databases). verify data integrity
- Enable and test front-end applications
- Enable client workstations and devices and client browser access.

Non-persistence

- **Snapshot/revert to known state -** A saved system state that can be reapplied to the instance.
- Rollback to known configuration
- **Live boot media -** An instance that boots from read-only storage to memory rather than being installed on a local read/write hard disk.

When provisioning a new or replacement instance automatically, the automation system may use one of two types of mastering instructions.

- **Master image -** the “gold copy” of a server instance with the os applications and patches all installed and configured.
- **Automated build from a template -** similar to a master image and is the build instructions for an instance. rather than storing a master image, the software may build and provision an instance according to the template instructions.

7.2 Implementing Redundancy Strategies

High Availability - A Key Property Of Any Resilient System And Is Typically Measured Over A Period Of One Year.

The Maximum Tolerable Downtime (Mtd) Metric Expresses The Availability Requirement For A Particular Business Function.

High Availability Also Means That A System Is Able To Cope With Rapid Growth In Demand.

Scalability Is The Capacity To Increase Resources To Meet Demands With Similar Cost Ratios

- To Scale Out Is To Add More Resources In Parallel With Existing Resources
- To Scale Up Is To Increase The Power Of Existing Resources.

Elasticity Refers To The System's Ability To Handle These Changes On Demand In Real Time.

Fault Tolerance & Redundancy - A System That Can Experience Failures And Continue To Provide The Same Or Nearly The Same Level Of Service Is Said To Be **Fault Tolerant.**

Fault Tolerance Is Often Achieved By Provisioning **Redundancy** For Critical Components And Single Points Of Failure.

Power Redundancy

- Dual Power Supplies
- Managed Power Distribution Units (Pdus)
- Battery Backups And Upss
- Generators

A Ups Is Always Required To Protect Against Any Interruption As A Backup Generator Cannot Be Brought Online Fast Enough To Respond To A Power Failure.

Network Redundancy - Network Interface Card (Nic) Teaming Means The Server Is Installed With Multiple Nics Or Nics With Multiple Ports Or Both. Each Port Is Connected To Separate Network Cabling.

For Example Four 1gb Ports Gives An Overall Bandwidth Of 4gb So If One Port Goes Down, 3gb Of Bandwidth Will Still Be Provided.

Switching & Routing - Network Cabling Should Be Designed To Allow For Multiple Paths Between The Various Switches And Routers So That During A Failure Of One Part Of The Network, The Rest Remains Operational.

Load Balancers - Nic Teaming Provides Load Balancing At The Adapter Level, Load Balancing And Clustering Can Also Be Provisioned At A Service Level.

- A Load Balancing Switch Distributes Workloads Between Available Servers.
- A Load Balancing Cluster Enables Multiple Redundant Servers To Share Data And Session Information To Maintain A Consistent Service If There Is Failover From One Server To Another.

Disk Redundancy - Redundant Array Of Independent Disks (Raid) - Here Many Disks Can Act As Backups For Each Other To Increase Reliability And Fault Tolerance.

There Are Several Raid Levels Numbered 0 To 6

RAID Level	Fault Tolerance
Level 1	Mirroring means that data is written to two disks simultaneously, providing redundancy (if one disk fails, there is a copy of data on the other). The main drawback is that storage efficiency is only 50%.
Level 5	Striping with parity means that data is written across three or more disks, but additional information (parity) is calculated. This allows the volume to continue if one disk is lost. This solution has better storage efficiency than RAID 1.
Level 6	Double parity, or level 5 with an additional parity stripe, allows the volume to continue when two devices have been lost.
Nested (0+1, 1+0, or 5+0)	Nesting RAID sets generally improves performance or redundancy.For example, some nested RAID solutions can support the failure ofmore than one disk.

Geographical Redundancy & Replication - Data Replication Can Be Applied In Many Contexts:

- **Storage Area Networks -** Redundancy Can Be Provided Within The San And Replication Can Also Take Place Between Sans Using Wan Links.
- Database
- **Virtual Machine -** The Same Vm Instance Can Be Deployed In Multiple Locations. This Can Be Achieved By Replicating The Vm's Disk Image And Configuration Settings.

Geographical Dispersal Refers To Data Replicating Hot And Warm Sites That Are Physically Distant From One Another. This Means That Data Is Protected Against A Natural Disaster Wiping Out Storage At One Of The Sites.

Asynchronous & Synchronous Replication

- Synchronous Replication Is Designed To Write Data To All Replicas Simultaneously Therefore All Replicas Should Always Have The Same Data All The Time.
- Asynchronous Replication Writes Data To The Primary Storage First And Then Copies Data To The Replicas Scheduled Intervals. It Isn't A Good Choice For A Solution That Requires Data In Multiple Locations To Be Consistent

7.3 Cyber Security Resilient Strategies

Configuration management - Configuration management ensures that each component of ict infrastructure is in a trusted state that has not diverged from its documented properties.

Change control and change management reduce the risk that changes to these components could cause service disruption.

Asset management - An asset management process tracks all the organization's critical systems, components, devices and other objects of value in an inventory.

An asset management database can be configured to store as much or as little information as it deemed necessary though typical data would be type, model, serial number, asset id, location, user(s), value and service information.

Asset identification & standard naming conventions - Tangible assets can be identified using a barcode label or frequency id (rfid) tag attached to the device. the rfid tag is a chip programmed with asset data and can help to also track the location of the device making theft more difficult.

A standard naming convention for hardware and digital assets such as accounts and virtual machines makes the environment more consistent. This means errors are easier to spot and it's easier to automate through scripting.

The naming strategy should allow admins to identify the type and function of any particular resource or location at any point in the network directory.

Change control & change management - A change control process can be used to request and approve changes in a planned and controlled way. change requests are usually generated when

- Something needs to be corrected
- When something changes
- Where there is room for improvement in a process or system currently in place.

In a formal change management process, the need or reasons for change and the procedure for implementing the change is captured in a request for change (rfc) document and submitted for approval.

The implementation of changes should be carefully planned, with consideration for how the change will affect dependent components.

For major changes, a trial change should be attempted first and every change should be accompanied by a rollback plan so the change can be reversed if it has a negative impact.

Site resiliency - An alternate processing site might always be available and in use while a recovery site might take longer to set up or only be used in an emergency.

- A hot site can failover almost immediately.
- A warm site could be similar but with the requirement that the latest data set will need to be loaded.
- A cold site takes longer to set up and could be an empty building waiting to

have whatever equipment that is needed to be installed in it.

Diversity and defense in depth - layered security is typically seen as improving cybersecurity resiliency because it provides defense in depth (multiple security controls).

Allied with defense in depth is the concept of security through diversity. Technology diversity refers to a mix of oss, applications, coding languages and so on while control diversity means that the layers of controls should combine different classes of technical and administrative controls with the range of control functions to prevent, detect, correct and deter.

Vendor diversity - As well as deploying multiple types of controls, there are also advantages in leveraging vendor diversity.

While single vendor solutions provide interoperability and can reduce training and support costs, it does have several disadvantages.

- Not obtaining best-in-class performance
- Less complex attack surface.
- Less innovation

Deception and disruption strategies

Active defense means an engagement with the adversary and can mean the deployment of decoy assets to act as lures or bait.

A honey **pot** is a system set up to attract threat actors, with the intention of analyzing attack strategies and tools to provide early warnings of attack attempts. it could also be used to detect internal fraud, snooping and malpractice.

A honeynet is an entire decoy network.

On a production network, a honeypot is more likely to be located in a dmz, or on an isolated segment on the private network if the honeypot is seeking to draw out insider threats.

A honeypot or honeynet can be combined with the concept of a **honeyfile** which is convincingly useful but actually fake data.

Some examples of disruption strategies include:

- Using bogus dns entries to list multiple non-existent hosts
- Configuring a web server with multiple decoy directories
- Using port triggering or spoofing to return fake telemetry data when a host detects port scanning activity. This will result in multiple ports being falsely reported as open.
- Using a dns sinkhole to route suspect traffic to a different network such as a honeynet.

7.4 - Physical Security Controls

Physical access controls - These are security measures that restrict and monitor access to specific physical areas or assets. They can control access to buildings, server rooms, data centers, finance or legal areas and so on.

Physical access controls depend on the same access control fundamentals as network or os security:

- **Authentication -** Create lists of approved people
- **Authorization -** Create barriers around a resource so access to it is controlled through defined entry and exit points
- **Accounting -** Keep a record of when entry/exit points are used and detect security breaches.

Site layout, fencing & lighting - Given constraints of cost and existing infrastructure, try to plan the site using the following principles

- Locate secure zones
- Use a demilitarized zone design for the physical space and position public access areas so that guests do not pass near secure zones.
- Use signage and warnings to enforce the idea that security is tightly controlled.
- Entry points to secure zones should be discreet. Do not allow an intruder the opportunity to inspect security mechanisms.
- Try to minimize traffic having to pass between zones. The flow should be "in and out" rather than "across and between"
- Give high traffic public areas high visibility
- In secure zones, do not display screens facing toward pathways or windows. Alternatively use one-way glass so that no one can look in through windows.

Gateways and locks - in order to secure a gateway, it must be fitted with a lock. Lock types can be categorized as follows:

- **Physical -** A conventional lock that prevents the door handle from being operated without the use of a key.
- **Electronic -** Rather than a key, the lock is operated by entering a pin on an electronic keypad. This type of lock is also referred to as cipher, combination or keyless.
- **Biometric -** A lock may be integrated with biometric scanner

Physical attacks against smart cards and usb - smart cards used to bypass electronic locks can be vulnerable to cloning and skimming attacks.

- **Card cloning -** Making one or more copies of an existing card. A lost or stolen card with no cryptographic protections can be physically duplicated.
- **Skimming -** Refers to using a counterfeit card to capture card details which are then used to program a duplicate.

Malicious usb charging cables and plugs are also a widespread problem. A usb data blocker can provide mitigation against “juice-jacking” attacks by preventing any sort of data transfer when the smartphone is connected to a charge point.

Alarm systems & sensors

there are five main types of alarms

- **Circuit -** A circuit-based alarm sounds when the circuit is opened or closed depending on the type of alarm. Could be caused by a door or window opening or by a fence being cut.
- **Motion detection -** A motion-based alarm is linked to a detector triggered by any movement within an area.
- **Noise detection -** An alarm triggered by sounds picked up by a microphone.
- **Proximity -** Rfid tags and readers can be used to track the movement of tagged objects within an area.
- **Duress -** This type of alarm is triggered manually by staff if they come under threat.

Security guards & cameras - Surveillance is typically a second layer of security designed to improve the resilience of perimeter gateways.

Security guards can be placed in front of secure and important zones and can act as a very effective intrusion detection and deterrence mechanism but can be expensive.

Cctv is a cheaper means of providing surveillance than using security guards.

The other big advantage is that movement and access can also be recorded but the main drawback is that response times are longer and security may be compromised if not enough staff are present to monitor the camera feeds.

Reception personnel & id badges - A very important aspect of surveillance is the challenge policy and can be quite effective against social engineering attacks.

An access list can be held at the reception area for each secure area to determine who is allowed to enter.

Reception areas for high-security zones might be staffed by at least two people at all times

7.5 - physical host security controls

Secure Areas - A secure area is designed to store critical assets with a higher level of access protection than general office areas. The most vulnerable point of the network infrastructure will be the communications or server room.

Air gap/ dmz - An air gapped host is one that is not physically connected to any network. Such a host would normally have stringent physical access controls.

An air gap within a secure area serves the same function as a dmz. As well as being disconnected from any network, the physical space around the host makes it easier to detect unauthorized attempts to approach the asset.

Protected Distribution & Faraday Cages - A physically secure cabled network is referred to as protected cable distribution or as a protected distribution system (pds). There are two main risks:

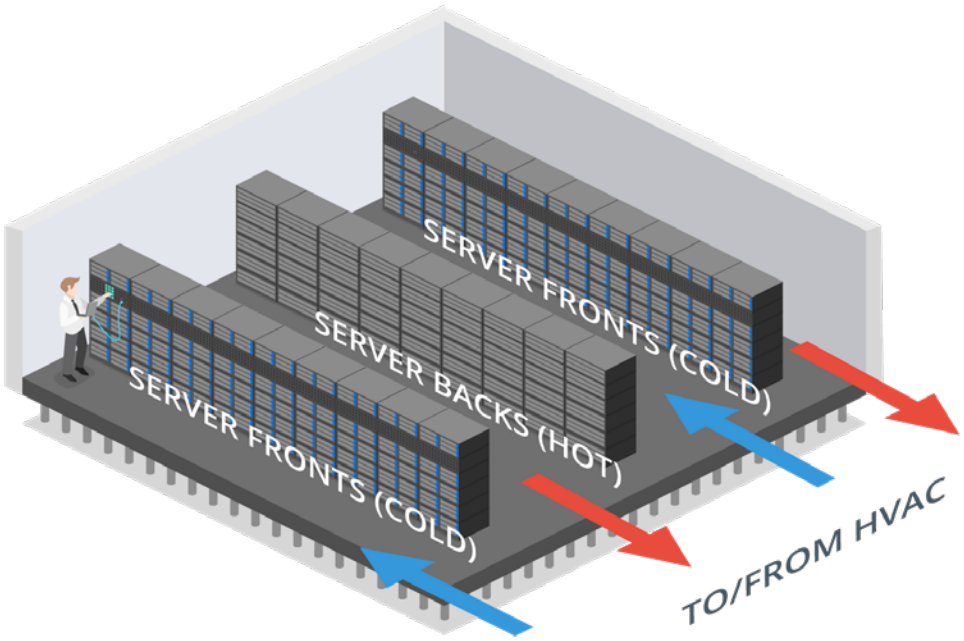
- An attacker could eavesdrop using a tap
- An attacker could cut the cable (dos)

Heating, Ventilation & Air Conditioning - Environmental controls mitigate the loss of availability through mechanical issues with equipment such as overheating.

For computer rooms and data centers, the environment is typically kept at a temperature of about 20-22 degrees centigrade and relative humidity of 50%.

Hot and Cold Aisles - A server room or data center should be designed in such a way as to maximize air flow across the server or racks.

The servers are placed back-to-back not front-to-back so that the warm exhaust from one bank of servers is not forming the air intake for another bank. This is referred to as a hot/cold aisle arrangement.



Fire detection & suppression - Fire suppression systems work on the basis of the fire triangle. This triangle works on the principle that a fire requires heat, oxygen and fuel to ignite and burn so removing any one of them will suppress the fire.

Overhead sprinklers may also be installed but there is the risk of a burst pipe and accidental triggering as well as the damage it could cause in the event of an actual fire.

Secure data destruction - Physical security controls also need to take account of the disposal phase of the data life cycle. Media sanitization and remnant removal refer to erasing data from hard drives, flash drives and tape media before they are disposed of.

There are several physical destruction options:

- Burning
- Shredding and pulping
- Pulverization
- **Degaussing -** Exposing a hard disk to a powerful electromagnet disrupts the magnetic pattern that stores the data.

Data Sanitization Tools - The standard method of sanitizing an hdd is called overwriting. This can be performed using the driver's firmware tools or a utility program.

The most basic type of overwriting is called zero filling which just sets each bit to zero. Single pass zero filling can leave patterns that can be read with specialist tools.

Secure Erase (SE) - Since 2001, the sata and serial attached scsi (sas) specifications have included a secure erase (se) command. This command can be invoked using a drive/array utility or the hdparm linux utility. On hdds, this performs a single pass of zero-filling.

Instant Secure Erase (ISE) - Hdds and ssds that are self-encrypting drives (seds) support another option invoking a sanitize command set in sata and sas standards from 2012 to perform a crypto ease. Drive vendors implement this as ise. With an ise, all data on the drive is encrypted using media encryption key (mek) and when the erase command is issued, the mek is erased rendering the data unrecoverable.

SECTION 8

EXPLAIN VULNERABILITY MANAGEMENT

8.1 Vulnerability Discover

A zero-day vulnerability refers to a vulnerability that is actively being exploited by attackers before the vendor has had an opportunity to develop and release a patch or fix for it.

A bug bounty program is an incentive program that compensates participants for discovering and ethically reporting the bugs or vulnerabilities. The program could be Open or Closed.

Ethical Disclosure - This is the practice of publishing information related to a vulnerability or finding in order to inform users so they can make informed decisions.

- **Full Disclosure -** Making all details public without regard to additional harm that may be caused to others including exploitation by adversaries.
- **Responsible Disclosure -** Making enough information known so that informed decisions can be made while not releasing sensitive details that could be useful to an adversary.

CVE Program - This is an international community driven effort to catalog hardware and software vulnerabilities for public access.

The CVSS is an open framework for communicating the characteristics and severity of hardware and software vulnerabilities.

There are five ratings - None, low, medium, high and critical.

The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

8.2 Weak host & Network configurations

Using the default manufacturer settings is an example of weak configuration. The root account or the default admin account typically has no restrictions set over system access and can have an extremely serious impact if an attacker gains control of it.

Open Permissions - This refers to provisioning data files or applications without differentiating access rights for user groups. This can lead to permitting unauthenticated guests to view confidential data or allowing write access to read only files. servers must operate with at least some open ports but security best practice dictates that these should be restricted to only necessary services.

Weak encryption - this can arise from the following:

- the key is generated from a simple password making it easy to brute-force
- the algorithm or cipher used for the encryption has known weaknesses
- the key is not distributed securely and can easily fall into the attacker's hands.
- **Errors -** weakly configured applications may display unformatted error messages under certain conditions and can provide threat actors with valuable information.

8.3 Evaluation Scope

Evaluation target or scope refers to the product, system, or service being analyzed for potential security vulnerabilities.

The target is the focus of a specific evaluation process, where it is subjected to rigorous testing and analysis to identify any possible weaknesses or vulnerabilities in its design, implementation, or operation

For application vulnerabilities, the target would refer to a specific software application.

The primary goal of the evaluation is to mitigate risk, improve the application's security posture, and ensure compliance with relevant security standards or regulations.

Security Testing	Conducting vulnerability assessments and penetration testing to identify potential weaknesses, vulnerabilities or misconfigurations
Documentation Review	Reviewing documentation such as design specifications, architecture diagrams, security policies and procedures
Secure Code Analysis	Analyzing source code to identify potential security vulnerabilities or coding errors to uncover issues related to input validation and coding standards.
Cryptographic Analysis	Assessing cryptographic mechanisms
Compliance Verification	Verifying compliance with standards specified by relevant regulations, frameworks or security certifications
Security Architecture	Evaluating security architecture and design to identify potential weaknesses or gaps in security controls

8.4 Overflows, Resource Exhaustion, Memory Leaks & Race Conditions

Buffer overflow - A buffer is an area of memory reserved by the application to store working data. the attacker passes data that deliberately overfills the buffer. One of the most common vulnerabilities is stack overflow.

Integer overflow - An integer is a whole number and integers are used as a valid data type with fixed lower and upper bounds. an integer flow attack causes the target software to calculate a value that exceeds these bounds and can even cause a positive number to become negative.

Eternal blue is an example of an attack that uses vulnerabilities in integer overflow to gain system privileges on a windows host.

Null pointer dereferencing & race conditions - in c/c++ programming, a pointer is a variable that stores a memory location rather than a value. attempting to read/write that memory address via the pointer is called **dereferencing**.

If the memory location is invalid or null this can create a **null pointer dereference** and cause the process to crash and in other cases might allow the threat actor to run arbitrary code.

A **race condition** is a way of engineering a null pointer dereference exception.

This occurs when the outcome from an execution process is directly dependent on the order and timing of certain events and those events fail to execute in the order and timing intended by the developer.

Memory leaks & resource exhaustion - A process should release its block of memory used when it no longer requires it but if it doesn't, it can lead to memory leaks. such a situation can lead to less memory available for other applications and could lead to a system crash.

Resources refer to cpu time, system memory, fixed disk capacity & network utilization. a malicious process could spawn multiple looping threads to use cpu time or write thousands of files to disk.

Dll injection & driver manipulation - Dll (dynamic link library) is a binary package that implements some sort of standard functionality such as establishing a network connection or performing cryptography.

The main process of a software application is likely to load several DLLS during the normal course of operations.

DLL injection is a vulnerability where the OS allows one process to attach to another and a malware can force a legitimate process to load a malicious link library.

To perform dll injection, the malware must already be operating with sufficient privileges and evade detection by anti-virus software.

Avoiding detection is done through a process called **code refactoring** where the code performs the same function by using different methods (variable types and control blocks).

Pass the hash attack - pth is the process of harvesting an account's cached credentials when the user is logged into a single sign-on (sso) system so the attacker can use the credentials on other systems.

If the attacker can obtain the hash of the user password, it is possible to use it (without cracking) to authenticate to network protocols that accept ntlm (windows new technology lan manager) hashes as authentication credentials.

8.5 Sideloading, Rooting & Jailbreaking

Mobile devices introduce unique security vulnerabilities related to their operation, specialized software, ubiquity, and ability to store and collect vast amounts of personal and professional data.

- **Rooting -** Associated with Android devices and typically involves using custom firmware
- **Jailbreaking -** Associated with iOS and is accomplished by booting the device with a patched kernel
- **Carrier Unlocking -** For either iOS or Android and it means removing the restrictions that lock a device to a single carrier.

Rooting or jailbreaking mobile devices involves subverting the security measures on the device to gain super administrative access to it but also has the side effect of permanently disabling certain security features

Sideloading - This is the practice of installing applications from sources other than the official app store of the platform such as the Play store or App store..

Additionally, apps that require excessive access permissions can raise significant security and privacy concerns.

App permissions should align with the app's purpose. Apps with excessive permissions may access sensitive user data without a legitimate need, including personal information, corporate data, contacts, call logs, location data, or device identifiers.

Granting unnecessary permissions to apps increases the device's attack surface and the potential for security vulnerabilities.

8.6 Threat Research Sources

Threat Research Is A Counterintelligence Gathering Effort In Which Security Companies And Researchers Attempt To Discover The Tactics, Techniques And Procedures (Ttps) Of Modern Cyber Adversaries.

Another Primary Source Of Threat Intelligence Is The Deep Web.

The Deep Web Is Any Part Of The World Wide Web That Is Not Indexed By A Search Engine E.G Registration Pages, Unlinked Pages And Pages That Block Search Indexing.

8.7 Threat Intelligence Providers

The outputs from the primary research undertaken by security solutions providers can take three main forms.

Behavioral threat research - Narrative commentary describing examples of attacks and TTPs gathered through primary research sources.

Reputational threat intelligence - List of ip addresses and domains associated with malicious behavior

Threat data - Computer data that can correlate events observed on a customer's own networks and logs with known TTP and threat actor indicators.

Threat data can be packaged as feeds that integrate with a security information and event management (SIEM) platform.

These feeds are usually described as cyber threat intelligence (cti) data.

Threat intelligence platforms and feeds are supplied as one of four different commercial models

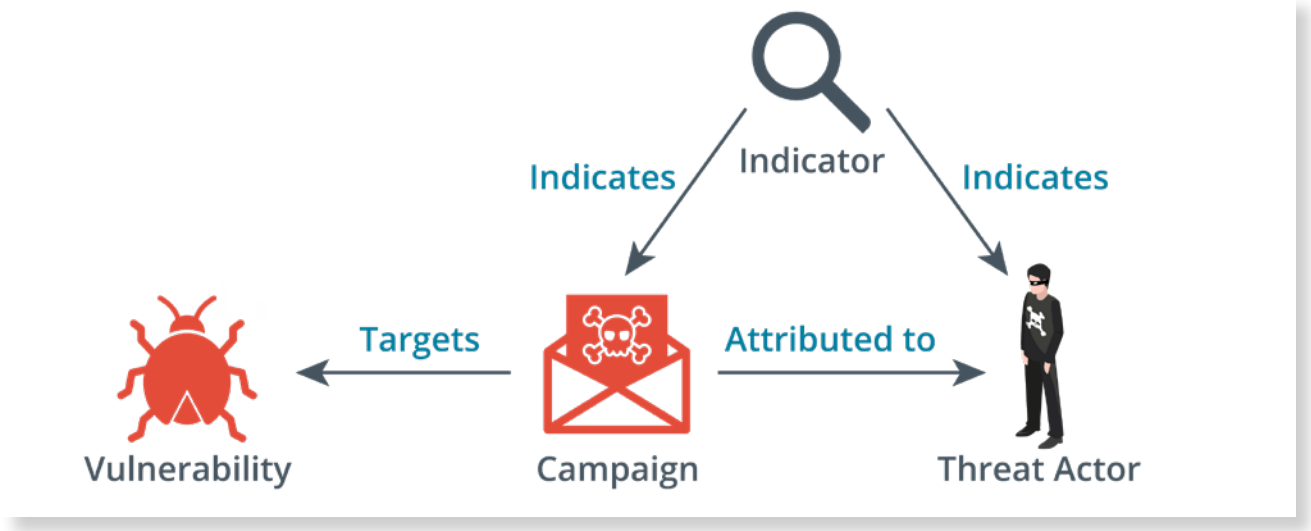
- **Closed/proprietary -** The threat research and cti data is made available as a paid subscription to a commercial threat intelligence platform.
- **Vendor websites -** This is proprietary threat intelligence that is not provided at a cost but is provided as a general benefit to customers e.g microsoft's security intelligence blog.
- **Public/private information sharing centers -** In many critical industries, **information sharing and analysis centers (isacs)** have been set up to share threat intelligence and promote best practice.

- **Open source intelligence (OSINT) -** Some companies operate threat intelligence services on an open-source basis earning income from consultancy
- **Other threat intelligence research resources include -** Academic journals, conferences, request for comments (RFC) and social media

8.8 Threat Data Feeds

There Are Various Ways That A Threat Data Feed Can Be Implemented.

Structured Threat Information Expression (Stix) - Describes Standard Terminology For Iocs And Ways Of Indicating Relationships Between Them.



Trusted automated exchange of indicator information (taxii) - Protocol provides a means for transmitting cti data between servers and clients.

Automated indicator sharing (ais) - Is a service offered by the dhs for companies to participate in threat intelligence sharing. ais is based on the stix and taxii standards and protocols.

Threat map - A threat map is an animated graphic showing the source, target and type of attacks detected by a cti platform.

File/code repositories - such a repository holds signatures of known malware code.

Vulnerability databases & feeds - Another source of threat intelligence is identifying vulnerabilities in os, software applications and firmware code. vulnerability databases include the common vulnerabilities and exposure (CVE).

Artificial Intelligence - Ai is the science of creating machine systems that can simulate or demonstrate a similar general intelligence capability to humans.

Predictive analysis - This refers to when a system can anticipate an attack and possibly identify the threat actor before the attack is fully realized.

8.9 Vulnerability Response & Remediation

Vulnerability scanning - This is an automated activity that relies on a database of known vulnerabilities such as the CVE.

Web app vulnerability scanners are specialized automated tools designed to identify vulnerabilities such as XSS and SQL injection attacks in websites and other web-based applications.

This category of tools is frequently referred to as the Dynamic Application Security Testing (DAST) tools.

True Positive	False Positive	True Negative	False Negative
Normal or xpected activity is correctly identified	Normal or xpected activity is incorrectly identified as abnormal	Abnormal or unexpected activity is correctly identified	Abnormal or unexpected activity is incorrectly identified as normal or expected
GOOD	PROBLEMATIC	GOOD	DANGEROUS

Vulnerability Scanning & Assessments

- **System Configuration -** Identify issues related to security configurations, compliance and nonconformance.
- **Vulnerability Assessment -** Identify host attributes and known Common Vulnerabilities and Exposures (CVE)
- **Penetration Testing -** Evaluate the security of a target by identifying and providing proof of concept of flaws and vulnerabilities by performing compromise exploitation.

Vulnerability Analysis - This focuses on analyzing the results gotten from vulnerability scans and assessments to determine the level of risk associated with each identified vulnerability.

Very useful for prioritizing vulnerabilities.

Vulnerability Severity Levels

- **High -** This can also be critical levels and such vulnerabilities have the potential to cause significant damage and require immediate attention.
- **Medium -** Could result in adverse consequences eventually and should be prioritized based on their potential impact on the organization.
- **Low -** Have limited impact and should be remediated as part of ongoing vulnerability management efforts.

Patch Management - This is the process of identifying, acquiring, installing and verifying patches (updates)

The time from when an exploit first becomes active to the time it becomes insignificant is known as the **Window of Vulnerability.**

Patch Classifications

CRITICAL	DEFINITION	DRIVERS	FEATURE PACKS
Fixes for critical non- security related issues.	Updates to virus and definition files	For software components that control or regulate a	Provides new product functionality for the next product release
SECURITY	**SERVICE PACKS**	**UPDATE ROLLUPS**	**UPDATES**
Provides a fix for a product- specific, security-related vulnerability	Provides a cumulative set of security updates, hotfixes and design change or features	Provides a cumulative set of security updates, hot fixes and updates in one package	Provides fixes that address non-critical, non-security bugs

Patch Management Challenges

- Unintentional consequences
- Roll-back issues
- Prioritization, timing and testing
- Approach - manual, automated, hybrid?
- Access to unmanaged mobile or remote devices

SECTION 9

EVALUATE NETWORK SECURITY CAPABILITIES

9.1 Bench Marks & Secure Configuration Guides

Although frameworks provide a "high-level" view of how to plan its services, they generally don't provide detailed implementation guidance.

At a system level, the deployment of servers and applications is covered by benchmarks and secure configuration guides.

Center For Internet Security (CIS)

A non profit organization that publishes the well-known (the cis critical security controls).

They also produce benchmarks for different aspects of cybersecurity e.g benchmarks for compliance with it frameworks include pci dss and iso 27000.

There are also product-focused benchmarks such as windows desktop, windows server, macos and web & email servers.

Os/Network Appliance Platform/ Vendor-Specific Guides

Operating System (Os) Best Practice Configuration Lists The Settings And Controls That Should Be Applied For A Computing Platform To Work In Defined Roles Such As Workstation, Server, Network Switch/Router Etc.

Most Vendors Will Provide Guides, Templates And Tools For Configuring And Validating The Deployment Of Network Appliances And Operating Systems And These Configurations Will Vary Not Only By Vendor But By Device And Version As Well.

- Department Of Defense Cyber Exchange Provides Security Technical Implementation Guides (Stigs) With Hardening Guidelines For A Variety Of Software And Hardware Solutions.
- National Checklist Program (Ncp) By Nist Provides Checklists And Benchmarks For A Variety Of Operating Systems And Applications.

Application Servers

Most Application Architectures Use A Client/Server Model Which Means Part Of The Application Is A Client Software Program Installed And Run On Separate Hardware To The Server Application Code.

Attacks Can Therefore Be Directed At The Client, Server Or The Network Channel Between Them.

Open Web Application Security Project (Owasp)

A Non Profit Online Community That Publishes Several Secure Application Development Resources Such As The Owasp Top 10 That Lists The Most Critical Application Security Risks.

9.2 Hardening Concepts

Network equipment, software, and operating systems use default settings from the developer or manufacturer which attempt to balance ease of use with security. Unfortunately these default configurations are an attractive target for attackers as they usually include well-documented credentials, allow simple passwords and use insecure protocols which increase the likelihood of successful cyberattacks. Therefore, it's crucial to change these default settings to improve security.

Hardening refers to the methods used to improve a device's security by changing its default configuration. There are various ways for hardening switches, routers, server hardware and operating systems.

Switches & Routers

- Change default credentials
- Disable unnecessary services and interfaces
- Use secure management protocols such as SSH and HTTPS instead of Telnet or HTTP
- Implement Access Control Lists
- Configure port security
- Enforce strong password policies

Server Hardware and Operating Systems

- Change default credentials
- Disable unnecessary services
- Apply security patches and updates
- Use firewalls and intrusion detection systems
- Secure configuration
- Enable logging and monitoring
- Use Antivirus and Antimalware solutions
- Enforce physical security

9.3- Wi-Fi Authentication Methods

Wi-Fi Authentication Comes In Three Types - Open, Personal And Enterprise.

Within The Personal Category, There Are Two Methods:

- Pre-Shared Key Authentication (Psk)
- Simultaneous Authentication Of Equals (Sae)

WPA2 pre-shared key authentication - In wpa2, pre-shared key (PSK) authentication uses a passphrase to generate the key for encryption.

The passphrase length is typically between 8 and 63 ascii characters and is then converted to a 256-bit HMAC value.

Wpa3 personal authentication - Wpa3 also uses a passphrase like wpa2 but it changes the method by which this secret is used to agree on session keys. this scheme is called password authenticated key exchange (PAKE)

Wi-fi protected setup (wps) - This is a feature of both WPA and WPA2 that allows enrollment in a wireless network based on an 8-digit pin.

It is vulnerable to brute force attacks and is set to be replaced by the easy connect method in wpa3 which uses quick response (qr) codes of each device.

Open authentication and captive portals - Open authentication means that the client is not required to authenticate however it can be combined with a secondary authentication mechanism via a browser.

When the client launches the browser, the client is redirected to a **captive portal** or splash page where they will be able to authenticate to the hotspot provider's network.

Enterprise/ieee 802.1x authentication - When a wireless station requests to join the network, its credentials are passed to an aaa server on the wired network for validation.

Once authenticated, the aaa server transmits a master key (mk) to the station and then both of them will derive the same pairwise master key (pmk) from the mk.

Extensible authentication protocol (eap) - This defines a framework for negotiating authentication mechanisms rather than the details of the mechanisms themselves.

Eap implementations can include smart cards, one-time passwords and biometric identifiers.

Peap, eap-ttls and eap-fast - in protected extensible authentication protocol (peap), an encrypted tunnel is established between the supplicant and authentication server but only a server-side public key certificate is required.

Eap with flexible authentication via secure tunneling (eap-fast) - is also similar to peap but instead of a server side certificate, it uses a protected access credential (pac) which is generated for each user from the authentication server's master key.

Radius federation - most implementations of eap use a radius server to validate the authentication credentials for each user.

Radius federation means that multiple organizations allow access to one another's users by joining their radius servers into a radius hierarchy or mesh.

Rogue access points & evil twins - a rogue access point is one that has been installed on the network without authorization.

A rogue wap masquerading as a legitimate one is called an evil twin. an evil twin might have a similar ssid as the real one or the attacker might use some dos technique to overcome the legitimate wap.

A rogue hardware WAP can be identified through physical inspections. there are also various wi-fi analyzers that can detect rogue waps including inssider and kismet

Disassociation and replay attacks - a

disassociation attack exploits the lack of encryption in management frame traffic to send spoofed frames.

One type of disassociation attack injects management frames that spoof the mac address of a single victim causing it to be disconnected from the network.

Another variant broadcasts spoofed frames to disconnect all stations.

Jamming Attacks - A Wi-Fi Jamming Attack Can Be Performed By Setting Up A Wap With A Stronger Signal.

The Only Way To Defeat This Attack Is To Either Locate The Offending Radio Source And Disable It Or To Boost The Signal From The Legitimate Equipment.

9.4 Network Access Control

Network Access Control (NAC)not only authenticates users and devices before allowing them access to the network but also checks and enforces compliance with established security policies. By evaluating the operating system version, patch level, antivirus status, or the presence of specific security software, NAC ensures that devices meet a minimum set of security standards before being granted network access.

NAC also can restrict access based on user profile, device type, location, and other attributes, to ensure users and devices can only access the resources necessary to complete their duties. NAC plays a crucial role in identifying and quarantining suspicious or noncompliant devices.

NAC and virtual local area networks (VLANs) work together to improve and automate network security. One of the primary ways NAC integrates with VLAN protections is through dynamic VLAN assignment. Dynamic VLAN assignment is a NAC feature that assigns a VLAN to a device based on the user's identity attributes, device type, device location, or health check results.

Agent vs Agentless Configurations

NAC can enforce security policies using agent-based and agentless methods.

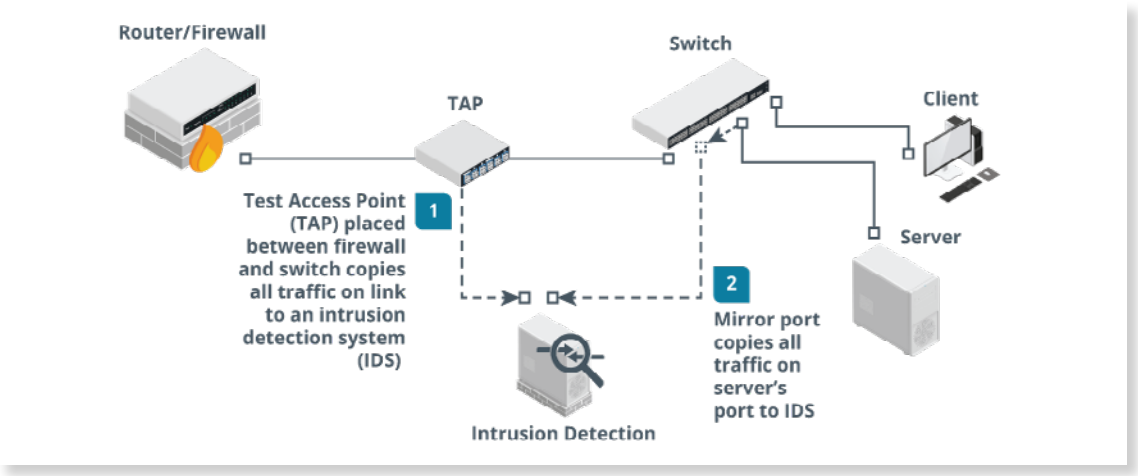
In an agent-based approach, a software agent is installed on the devices that connect to the network. This agent communicates with the NAC platform, providing detailed information about the device's status and compliance level. An agent-based NAC implementation can enable features such as automatic remediation, where the NAC agent can perform actions like updating software or disabling specific settings to bring a device into compliance with mandatory security configurations.

In contrast, an agentless NAC approach uses port-based network access control or network scans to evaluate devices. For example, agentless NAC may use DHCP fingerprinting to identify the type and configuration of a device when it connects, or it might perform a network scan to detect open ports or active services.

9.5 Network Security Monitoring

Network-based intrusion detection systems - An ids is a means of using software tools to provide real-time analysis of either network traffic or system and application logs. a network-based ids captures traffic via a packet sniffer referred to as a sensor. when traffic matches a detection signature, it raises an alert but will not block the source host.

Taps & port mirrors - Typically the packet capture sensor is placed inside a firewall or close to an important server and the idea is to identify malicious traffic that has managed to get past the firewall. depending on network size and resources, one or just a few sensors will be deployed to monitor key assets and network paths.



Network-based intrusion prevention systems (IPS) - An ips provides an active response to any network threat.

Typical responses to a threat can include blocking the attacker's ip address (shunning), throttling the bandwidth to attacking hosts and applying complex firewall filters.

Next generation firewall (NGFW) - HGFW is a product that combines application-aware filtering with user account-based filtering and the ability to act as an ips.

Unified threat management (UTM) - This refers to a security product that centralizes many types of security controls - firewall, antimalware, spam filtering, vpn etc into a single appliance. The downside is that this creates a single point of failure that can affect the entire network. they can also struggle with latency issues if they are subject to too much network activity.

Content/url filter - A firewall typically has to sustain high loads of traffic which can increase latency and even cause network outages. a solution is to treat security solutions for server traffic differently from that of user traffic.

A Content Filter Is Designed To Apply A Number Of User-Focused Filtering Rules Such As Applying Time-Based Restrictions To Browsing.

Content Filters Are Now Implemented As A Class Of Product Called Secure Web Gateway (Swg) Which Can Also Integrate Filtering With The Functionality Of Data Loss Prevention.

Host-Based Ids - A Host-Based Ids (Hids) Captures Information From A Single Host. The Core Ability Is To Capture And Analyze Log Files But More Sophisticated Systems Can Also Monitor Os Kernel Files, Monitor Ports And Network Interfaces.

One Other Core Feature Is File Integrity Monitoring (Fim). Fim Software Will Audit Key System Files To Make Sure They Match The Authorized Versions.

Web Application Firewall (Waf) - A Waf Is Designed To Specifically Protect Software Running On Web Servers And Their Back-End Databases From Code Injection And Dos Attacks.

They Use Application-Aware Processing Rules To Filter Traffic And Perform Application-Specific Intrusion Detection.

9.6 Web Filtering

Its primary function is to block users from accessing malicious or inappropriate websites, thereby protecting the network from potential threats.

Web filters analyze web traffic, often in real time, and can restrict access based on various criteria such as URL, IP address, content category, or even specific keywords.

Agent-Based Web Filtering

Agent-based web filtering involves installing a software agent on desktop computers, laptops, and mobile devices. The agents enforce compliance with the organization's web filtering policies.

Agents communicate with a centralized management server to retrieve filtering policies and rules and then apply them locally on the device.

Centralized Web Filtering

A centralized proxy server plays a crucial role in web content filtering by acting as an intermediary between end users and the Internet.

When an organization routes Internet traffic through a centralized proxy server, it can effectively control and monitor all inbound and outbound web content.

The primary role of the proxy in web content filtering is to analyze web requests from users and determine whether to permit or deny access based on established policies.

Centralized Web Filtering Techniques

- **URL Scanning -** Where the proxy server examines the URLs requested by users.
- **Content Categorization -** Classifies websites into categories
- **Block Rules -** Uses the proxy server to implement block rules based on various factors such as the website's URL, domain, IP address and even specific keywords within the web content.
- **Reputation-Based Filtering -** This leverages continually updated databases that score websites based on their observed behavior and history.

SECTION 10

ASSESS ENDPOINT SECURITY CAPABILITIES

10.1 Endpoint Security

Hardening - This Is The Process Of Putting An Os Or Application In A Secure Configuration However Hardening Must Be Balanced Against The Access Requirements And Usability In A Particular Situation.

The Essential Principle Is Of Least Functionality Meaning The System Should Run Only The Protocols And Services Required By Legit Users And No More.

Interfaces, Services And Application Service Ports Not In Use Should Be Disabled.

Patch Management - On Residential And Small Networks, Hosts Can Be Configured To Auto-Update Either By The Windows Update Process Or In Linux With The Commands Yum-Cron Or Apt Unattended-Upgrades Depending On The Package Manager Used By The Distribution.

Patches Can Become Incompatible With A Particular Application And Cause Availability Issues. Update Repositories Can Also Be Infected With Malware That Can Then Be Spread Via Automatic Updates.

Antivirus (A-V)/ Anti-Malware - First Generation Of Antivirus Scanned For Only Viruses But Today They Can Perform Generalized Malware Detection.

While A-V Software Remains Important, Signature-Based Detection Is Widely Regarded To Be Insufficient For The Prevention Of Data Breaches.

Hardening - This Is The Process Of Putting An Os Or Application In A Secure Configuration However Hardening Must Be Balanced Against The Access Requirements And Usability In A Particular Situation.

The Essential Principle Is Of Least Functionality Meaning The System Should Run Only The Protocols And Services Required By Legit Users And No More.

Interfaces, Services And Application Service Ports Not In Use Should Be Disabled.

Patch Management - On Residential And Small Networks, Hosts Can Be Configured To Auto-Update Either By The Windows Update Process Or In Linux With The Commands Yum-Cron Or Apt Unattended-Upgrades Depending On The Package Manager Used By The Distribution.

Patches Can Become Incompatible With A Particular Application And Cause Availability Issues. Update Repositories Can Also Be Infected With Malware That Can Then Be Spread Via Automatic Updates.

Host-Based Intrusion Detection/Prevention (Hids/Hips) - Hids Provide Threat Detection Via Logs And File System Monitoring. Other Products May Also Monitor Ports And Network Interfaces And Process Data And Logs Generated By Specific Applications Such As Http Or Ftp.

Endpoint Protection Platform (Epp) - An Epp Is A Single Agent Performing Multiple Security Tasks, Including Malware/Intrusion Detection And Prevention But Also Other Features Such As Firewall, Web Content Filtering And File/Message Encryption.

Sandboxing - This Is A Technique That Isolates An Untrusted Host Or App In A Segregated Environment To Conduct Tests. Sandbox Offers More Than Traditional Anti-Malware Solutions Because You Can Apply A Variety Of Different Environments To The Sandbox Instead Of Just Relying On How The Malware Might Exist In Your Current Configuration.

10.2 Segmentation

This is the division of an enterprise into security zones based on function, performance and security requirements.

Security zones are enforced by firewall ingress and egress access control lists

Security Zones

- **Untrusted -** The organization has no control
- **Screened Subnet -** Has connections to both trusted and untrusted networks
- **Trusted -** The organization has complete control
- **Enclave -** Is a restricted network within a trusted network
- **Air Gapped -** Does not connect to any untrusted network
- **Physically Isolated -** Does not connect to any other network
- **Wireless -** Supports wireless transmissions
- **VPN -** Designed to facilitate secure communications over a public circuit

Micro-Segmentation - This is a method of creating zones within data centers and cloud environments to isolate workloads from one another and secure them individually.

It allows for the implementation of a zero trust protect surface environments.

A protect surface is made up of the network's most critical and valuable data, assets and applications.

North-South traffic is one that flows into and out of a data center or cloud while East-West refers to traffic within a data center or cloud.

Isolation - This is when zones, devices, sessions or even components need to be segregated so as not to cause harm or be harmed.

Virtualization - creates multiple environments from a single physical hardware system.

Logical - A VLAN divides a single existing network into multiple logical network segments which can be restricted.

10.3 Mobile Device Management

Mobile Device Deployment Models Include

- **Bring Your Own Device (BYOD) -** The Mobile Device Is Owned By The Employee And Will Have To Meet Whatever Security Profile Is Required. It's The Most Common Model For Employees But Poses The Most Difficulties For Security Managers.
- **Corporate Owned Business Only (COBO) -** The Device Is Owned By The Company And May Only Be Used For Company Business.
- **Corporate Owned, Personally-Enabled (COPE) -** The Employee May Use It To Access Personal Email ,Social Media Accounts And For Some Personal Web Browsing.
- **Choose Your Own Device (CYOD) -** Very Similar To Cope Except That Here, The Employee Is Given A Choice Of Device From A List.
- **Enterprise Mobility Management (EMM) -** This Is A Class Of Management Software Designed To Apply Security Policies To The Use Of Mobile Devices And Apps In An Enterprise.
- **Mobile Device Management (Mdm) -** Sets Device Policies For Authentication, Feature Use (Camera And Microphone) And Connectivity. Mdm Also Allows Device Resets And Remote Wipes.
- **Mobile Application Management (Mam) -** Sets Policies For Apps That Can Process Corporate Data And Prevents Data Transfer To Personal Apps.

Ios in the enterprise - In apple's ios ecosystem, third-party developers can create apps using apple's software development kit available only on macos.

Corporate control over ios devices and distribution of corporate and b2b apps is facilitated by participating in the device enrollment program, the volume purchase program and the developer enterprise program.W

Android in the enterprise - Android is open source meaning there is more scope for vendor-specific versions and the app model is far more relaxed.

The sdk is available on linux, windows and macos.

Mobile access control systems - If a threat actor is able to gain access to a smartphone, they might be able to gain access to plenty of confidential data as well as cached passwords for email, social media etc.

Smartphone authentication - Access control can be implemented by configuring a screen lock that can be bypassed using a password, pin or swipe pattern. Some devices also support biometrics like fingerprint readers.

Screen lock - The screen lock can also be configured with a lockout policy. For example, the device can be locked out for a period of time after a certain number of incorrect password attempts.

Context-aware authentication - Smartphones now allow users to disable screen locks when the device detects it is in a trusted location (home) however an enterprise may seek more stringent access controls to prevent misuse of a device.

For example, even if a device has been unlocked, the user might need to reauthenticate in order to access the corporate workspace.

Remote wipe - If the phone is stolen, it can be set to factory defaults or cleared of any personal data with the use of the remote wipe feature. it can also be triggered by several incorrect password attempts.

In theory, the thief could prevent the remote wipe by ensuring the phone cannot connect to the network then hacking the phone and disabling its security.

Full device encryption & external media - in ios, there are various levels of encryption:

- All user data on the device is always encrypted but the key is stored on the device. It's this key that is deleted in a remote wipe to ensure the data is inaccessible.
- Email data and any apps using the "data protection" option are subject to a second round of encryption using a key derived from the user's credential.

Location services - location services make use of two systems:

- **Global positioning system (gps) -** Means of determining the device's latitude and longitude based on information received from satellites via a gps sensor.
- **Indoor positioning system (ips) -** Works out a device's location by triangulating its proximity to other radio sources such as cell towers and wi-fi access points.

Geofencing and camera /microphone enforcement - Geofencing is the practice of creating a virtual boundary based on real-world geography and can be a useful tool for controlling the use of camera or video functions or applying context-aware authentication.

GPS tagging - This is the process of adding geographical identification metadata such as latitude and longitude, photographs, sms messages, video and so on.

GPS tagging is highly sensitive personal information and potentially confidential organizational data also.

Content management - Containerization allows the employer to manage and maintain the portion of the device that interfaces with the corporate network. a container can also enforce storage segmentation where the container will be associated with a directory.

rooting & jailbreaking

- **Rooting -** Associated with android devices and typically involves using custom firmware
- **Jailbreaking -** Associated with ios and is accomplished by booting the device with a patched kernel
- **Carrier unlocking -** For either ios or android and it means removing the restrictions that lock a device to a single carrier.

Rooting or jailbreaking mobile devices involves subverting the security measures on the device to gain super administrative access to it but also has the side effect of permanently disabling certain security features.

10.4 Secure Mobile Device Connections

Personal area networks (pans) - These enable connectivity between a mobile device and peripherals. Ad hoc (peer-to-peer) networks between mobile devices or between mobile devices and other computing devices can also be established

For corporate security, these peer-to-peer functions should generally be disabled.

Ad hoc wi-fi and wi-fi direct - An ad hoc network involves a set of wireless stations establishing peer-to-peer connections with one another rather than using an access point.

Wi-fi directly allows one-to-one connections between stations though one of them will serve as a soft access point.

Tethering and hotspots - A smartphone can share its internet connection with other devices via wi-fi making it a hotspot.

Where the connection is shared by connecting the smartphone to a pc via usb or bluetooth, it can be referred to as tethering.

Bluetooth connection methods

- **Device discovery -** Allows the device to connect to any other bluetooth devices nearby.
- **Authentication & authorization -** Use of a simple passkey to “pair” connecting devices
- Malware

Bluetooth connection methods - Discoverable devices are vulnerable to **bluejacking,** where the spammer sends unsolicited messages to the device.

Bluesnarfing refers to using an exploit in bluetooth to steal information from someone else’s phone.

Infrared & rfid connection methods - infrared has been used for pan but it’s use in modern smartphones and wearable technology focuses on two other uses:

- **Ir blaster -** This allows the device to interact with an ir receiver and operate a device such as a tv as though it were the remote control.
- **Ip sensor -** These are used as proximity sensors and to measure health information (heart rate & blood oxygen levels).

Radio frequency id (rfid) is a means of encoding information into passive tags which can easily be attached to devices, clothing and almost anything else.

Skimming involves using a fraudulent rfid reader to read the signals from a contactless bank card

Microwave radio connection methods - Microwave radio is used as a backhaul link from a cell tower to the service provider’s network and these links are important to 5g where many relays are required and provisioning fiber optic cable backhaul can be difficult.

A microwave link can be provisioned in two modes:

- **Point-to-point (p2p) -** Microwave uses high gain antennas to link two sites and each antenna is pointed directly at the other. It’s very difficult to eavesdrop on the signal as an intercepting antenna would have to be positioned within the direct path.
- **Point-to-multipoint (p2m) -** Microwave uses smaller sectoral antennas each covering a separate quadrant. P2m links multiple sites to a single hub and this can be cost-efficient in high density urban areas.

SECTION 11

ENHANCE APPLICATION SECURITY CAPABILITIES

11.1 Dns Security, Directory Services & Snmp

DNS Security – To Ensure Dns Security On A Private Network, Local Dns Servers Should Only Accept Recursive Queries From Local Authenticated Hosts And Not From The Internet.

Clients Should Be Restricted To Using Authorized Resolvers To Perform Name Resolution. **Dns Footprinting** Means Obtaining Information About A Private Network By Using Its Dns Server To Perform A Zone Transfer (All The Records In A Domain) To A Rogue Dns.

DNS Security Extensions (DNSSEC) – These Help To Mitigate Against Spoofing And Poisoning Attacks By Providing A Validation Process For Dns Responses.

Secure Directory Services – A Network Directory Lists The Subjects (Users, Computers And Services) And Objects (Directories And Files) Available On The Network Plus The Permissions Subjects Have Over Objects.

Most Directory Services Are Based On The Lightweight Directory Access Protocol (Ldap) Running Over Port 389.

Authentication Referred To As Binding To The Server Can Be Implemented By:

- **No Authentication -** Anonymous Access Is Granted
- **Simple Bind -** The Client Must Supply Its Distinguished Name And Password In Plaintext
- **Simple Authentication And Security Layer (Sasl) -** The Client And Server Negotiate The Use Of A Supported Authentication Mechanism Such As Kerberos.
- **Ldap Secure (Ldaps) -** The Server Is Installed With A Digital Certificate Which It Uses To Setup A Secure Tunnel For The User Credential Exchange. Ldaps Use Port 636.

Generally Two Levels Of Access To The Directory Can Be Granted Which Are Read-Only Access (Query) And Read/Write Access (Update) And Is Implemented Using An Access Control Policy.

Time Synchronization - Many Network Applications Are Time Dependent And Time Critical. The **Network Time Protocol (Ntp)** Provides A Transport Over Which To Synchronize These Time Dependent Applications

Ntp Works Over Udp On Port 123.

Ntp Has Historically Lacked Any Sort Of Security Mechanism But There Are Moves To Create A Security Extension For The Protocol Called **Network Time Security**.

Simple Network Management Protocol (Snmp) Security - This Is A Widely Used Framework For Management And Monitoring And Consists Of An Snmp Monitor And Agents. The Agent Is A Process (Software Or Firmware) Running On A Switch, Router, Server Or Other Snmp-Compatible Network Device.

This Agent Maintains A Database Called A Management Information Base (Mib) That Holds Statistics Relating To The Activity Of The Device. The Agent Is Also Capable Of Initiating A Trap Operation Where It Informs The Management System Of A Notable Event Like Port Failure.

11.2 Secure Application Operations Protocols

HTTP enables clients to request resources from an HTTP server. The server acknowledges the request and responds with the data or an error message.

HTTP is a **stateless** protocol which means the server preserves no information about the client during a session.

Transport Layer Security - Secure Sockets Layer (SSL) was developed by Netscape in the 1990s to address the lack of security in HTTP and was quickly adopted as a standard named Transport Layer Security (TLS).

To implement TLS, a server is assigned a digital certificate signed by some trusted CA. The certificate proves the identity of the server and validates the server's public/private key pair.

The server uses its key pair and the TLS protocol to agree mutually supported ciphers with the client and negotiate an encrypted communications session.

SSL/TLS Version - A server can provide support for legacy clients meaning a TLS 1.2 server could be configured to allow clients to downgrade to TLS 1.1 or 1.0

TLS 1.3 was approved in 2018 and the ability to perform downgrade attacks was mitigated by preventing the use of unsecure features and algorithms from previous versions.

Cipher Suites - This is a set of algorithms supported by both the client and server to perform the different encryption and hashing operations required by the protocol.

Prior to TLS 1.3, a cipher suite would be written like this

ECDHE-RSA-AES128-GCM-SHA256

This means that the server can use Elliptic Curve Diffie-Hellman Ephemeral mode for a session key agreement, RSA signatures, 128-bit AES-GCM (Galois Counter Mode) for symmetric bulk encryption and 256-bit SHA for HMAC functions.

TLS 1.3 uses simplified and shortened suites

TLS_AES_256_GCM_SHA384

Only ephemeral key agreement is supported in 1.3 and the signature type is supplied in the certificate so the cipher suite only lists the bulk encryption key strength and mode of operation (AES_256_GCM) plus the cryptographic hash algorithm (SHA384).

11.3 File Transfer, Email & Video Services

FTP - File Transfer Protocol is the most popular protocol for transferring files across networks because it is very efficient and has wide cross-platform support but has no security mechanism.

SSH FTP (SFTP) & FTP over SSL (FTPS) - SFTP addresses the lack of security by encrypting the authentication and data transfer between client and server. SFTP uses port 22.

Explicit TLS (FTPES) - Use the AUTH TLS command to upgrade and insecure connection established on port 21 to a secure one.

Implicit TLS (FTPS) - Negotiates an SSL/TLS tunnel before the exchange of any FTP commands. This mode uses the secure port 990 for the control connection.

Email Services: These use two types of protocols:

- The Simple Mail Transfer Protocol (SMTP) which specifies how mail is sent from one system to another.
- A mailbox protocol stores messages for users and allows them to download them to client computers or manage them on the server.

Secure SMTP (SMTPS) - communications can be secured using TLS and there are two ways to do this:

- **STARTTLS -** This command will upgrade an existing unsecure connection to use TLS. Also referred to as explicit TLC or opportunistic TLS.
- **SMTPS -** This establishes the secure connection before any SMTP commands are exchanged. Also referred to as implicit TLS.

Typical SMTP configurations use the following ports and secure services:

- **Port 25 -** Used for message relay between SMTP servers or Message Transfer Agents (MTA)
- **Port 587 -** Used by mail clients to submit messages for delivery by an SMTP server
- **Port 465 -** Some providers and mail clients use this port for message submission over implicit TLS (SMTPS)

Secure POP (POP3S) - The Post Office Protocol v3 is a mailbox protocol designed to store the messages delivered by SMTP on a server.

Secure IMAP (IMAPS) - The Internet Message Access Protocol v4 (IMAP4) supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously.

Secure/Multipurpose Internet Mail Extensions (S/MIME) - Is a means of applying both authentication and confidentiality on a per-message basis.

11.4 Email Security

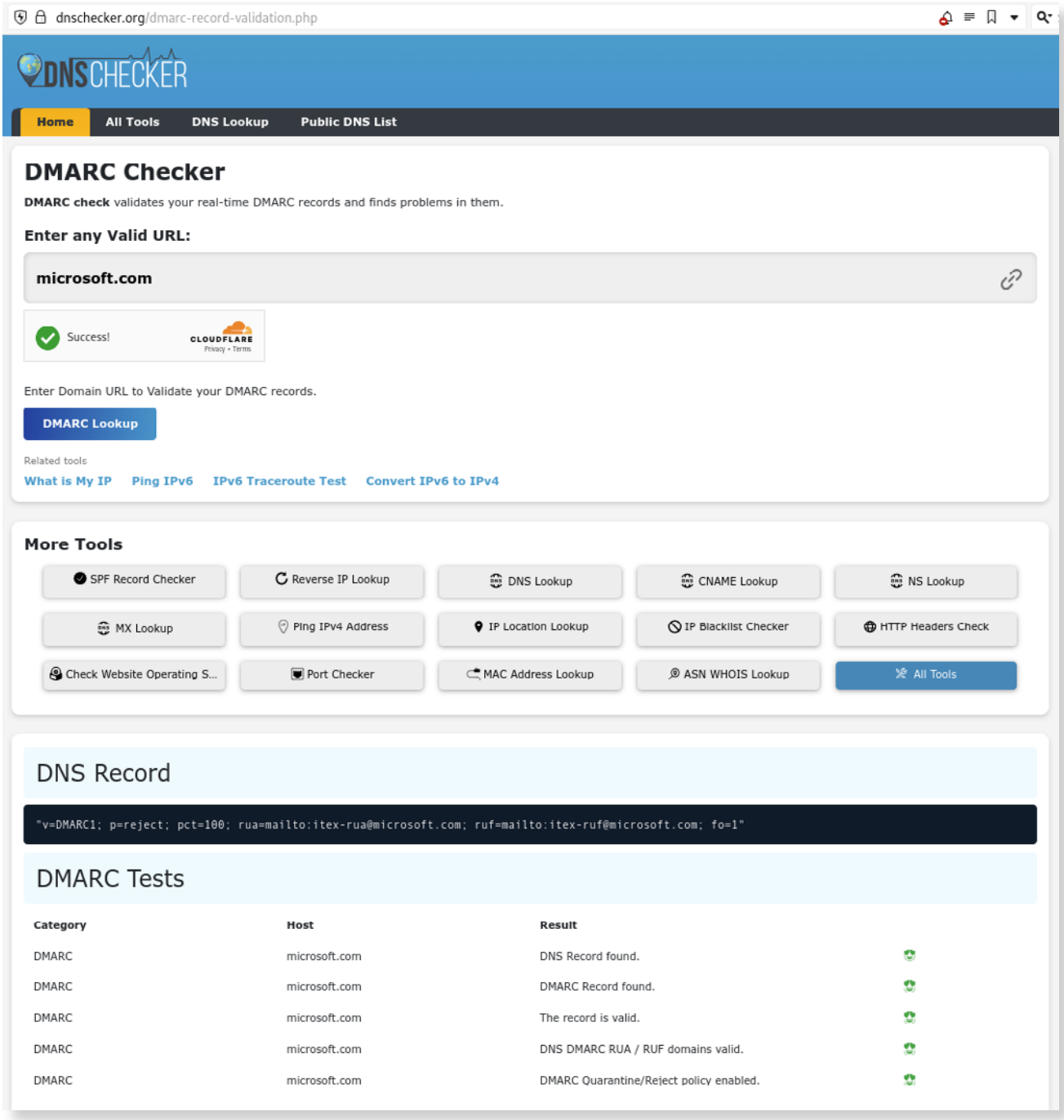
Sender Policy Framework (SPF) - Is an email authentication method that helps detect and prevent sender address forgery commonly used in phishing and spam emails.

SPF works by verifying the sender's IP address against a list of authorized sending IP addresses published in the DNS TXT records of the email sender's domain.

DomainKeys Identified Mail (DKIM) - Leverages encryption features to enable email verification by allowing the sender to sign emails using a digital signature, The receiving email server uses a DKIM record in the sender's DNS record to verify the signature and the email's integrity.

Domain-based Message Authentication, Reporting & Conformance (DMARC) - Uses the results of SPF and DKIM checks to define rules for handling messages, such as moving messages to quarantine or spam, rejecting them outright or tagging the message.

An email gateway - Is the control point for all incoming and outgoing email traffic. It acts as a gatekeeper, scrutinizing all emails to remove potential threats before they reach inboxes. Email gateways utilize several security measures, including anti-spam filters, antivirus scanners, and sophisticated threat detection algorithms to identify phishing attempts, malicious URLs, and harmful attachments.



The combined use of SPF, DKIM, and DMARC significantly enhances email security by making it much more difficult for attackers to impersonate trusted domains, which is one of the most common tactics used in phishing and spam attacks.

11.5 Secure Coding Techniques

Input Validation - Malicious Input Could Be Crafted To Perform An Overflow Attack Or Some Type Of Script Or Sql Injection Attack.

To Mitigate This, There Should Be Routines To Check User Input And Anything That Does Not Conform To What Is Required Must Be Rejected.

Normalization And Output Encoding - Normalization Means That A String Is Stripped Of Illegal Characters Or Substrings And Converted To The Accepted Character Set. This Ensures That The String Is In A Format That Can Be Processed Correctly By The Input Validation Routines.

Output Encoding Means That A String Is Re-Encoded Safely For The Context In Which It Is Being Used.

Server-Side Versus Client-Side Validation - A Web Application Can Be Designed To Perform Code Execution And Input Validation Locally (On The Client) Or Remotely (On The Server).

The Main Issue With Client-Side Validation Is That The Client Will Always Be More Vulnerable To Some Sort Of Malware Interfering With The Validation Process.

Main Issue With Server-Side Validation Is That It Can Be Time-Consuming As It May Involve Multiple Transactions Between The Server And Client.

Client-Side Validation Is Usually Restricted To Informing The User That There Is Some Sort Of Problem With The Input Before Submitting It To The Server. Relying On Client-Side Validation Only Is Poor Programming Practice.

Web Application Security In Response Headers

A Number Of Security Options Can Be Set In The Response Header

- **Http Strict Transport (Hsts) -** Forces Browser To Connect Using Https Only, Mitigating Downgrade Attacks Such As Ssl Stripping.
- **Content Security Policy (Csp)** - Mitigates Clickjacking, Script Injection And Other Client-Side Attacks.
- **Cache Control -** Sets Whether The Browser Can Cache Responses. Preventing Caching Of Data Protects Confidential And Personal Information Where The Client Device Might Be Shared By Multiple Users.

Data Exposure And Memory Management - Data Exposure Is A Fault That Allows Privileged Information Such As A Password Or Personal Data To Be Read Without Being Subject To The Appropriate Access Controls.

A Well-Written Application Must Be Able To Handle Errors And Exceptions Gracefully. Ideally The Programmer Should Have Written A **Structured Exception Handler (Seh)** To Dictate What The Application Should Then Do.

The Error Must Not Reveal Any Platform Information Or Inner Workings Of The Code To An Attacker.

Secure Code Usage - A Program May Make Use Of Existing Code In The Following Ways:

- **Code Reuse -** Using A Block Of Code From Elsewhere In The Same Application Or From Another Application To Perform A Different Function.
- **Third-Party Library -** Using A Binary Package (Such As A Dynamic Link Library) That Implements Some Sort Of Standard Functionality Such As Establishing A Network Connection.
- **Software Development Kit (Sdk) -** Using Sample Code Or Libraries Of Pre-Built Functions From The Programming Environment Used To Create The Software.
- **Stored Procedures -** Using A Pre-Built Function To Perform A Database Query.

Unreachable code and dead code

Unreachable code is a part of application source code that can never be executed (if ... then conditional logic that is never called because the conditions are never met).

Dead code s executed but has no effect on the program flow (a calculation is performed but the result is never stored as a variable or used to evaluate a condition).

Static code analysis - this is performed against the application code before it is packaged as an executable process. The software will scan the source code for signatures of known issues.

Human analysis of software source code is described as a manual code review. It is important that the code be reviewed by developers other than the original coders to try to identify oversights, mistaken assumptions or a lack of experience.

Dynamic code analysis - static code review will not reveal any vulnerabilities that exist in the runtime environment. dynamic analysis means that the application is tested under real world conditions using a staging environment.

Fuzzing is a means of testing that an application‘s input validation routines work well. fuzzing will deliberately generate large amounts of invalid or random data and record the responses made by the application.

Associated with fuzzing is the concept of stress testing an application to see how an application performs under extreme performance or usage scenarios.

Finally, the fuzzer needs some means of detecting an application crash and recording which input sequence generated the crash.

SECTION 12 -

EXPLAIN INCIDENT RESPONSE AND MONITORING CONCEPTS

12.1 - Incident Response Process

This is a set of policies and procedures that are used to identify, contain, and eliminate cyberattacks. The goal is to allow an organization to quickly detect and stop attacks, minimize damage and prevent future attacks of the same type.

Principal stages in incident response life cycle

- **Preparation -** Makes the system resilient to attack. this includes: hardening systems, writing policies and procedures,and creating incident response resources and procedures
- **Identification** - Determine whether an incident has taken place, assess how severe it might be and then notify the appropriate personnel.
- **Containment -** Limits the scope and magnitude of the incident. The main aim of incident response is to secure data while limiting the immediate impact on customers and business partners.
- **Eradication -** Once the incident is contained, the vulnerability/issue is removed and the affected systems are restored to a secure state.
- **Recovery -** The restored system is then reintegrated back into the business process that it supports
- **Lessons learned -** Analyze the incident and responses to identify whether procedures or systems could be improved. It is also imperative to document the incident.

12.2 Cyber Incident Response Team

Preparing For Incident Response Means Establishing The Policies And Procedures For Dealing With Security Breaches And The Personnel And Resources To Implement Those Policies.

First Task Is To Define And Categorize Types Of Incidents. In Order To Identify And Manage Incidents, You Should Develop Some Method Of Reporting, Categorizing And Prioritizing Them.

An Incident Response Team Can Be Referred To As A Cyber Incident Response Team (Cirt), Computer Security Incident Response Team (Csirt) Or Computer Emergency Response Team (Cert).

For Major Incidents, Expertise From Other Business Divisions Might Be Needed

- **Legal -** The Incident Can Be Evaluated From The Perspective Of Compliance With Laws And Industry Regulations.
- **Human Resources (Hr) -** Incident Prevention And Remediation Actions May Affect Employee Contracts, Employment Law And So On.
- **Marketing -** The Team Is Likely To Require Marketing Or Public Relations Input So Any Negative Publicity From A Serious Incident Can Be Managed.

Incident Response Policies Should Establish Clear Lines Of Communication Both For Reporting Incidents And For Notifying Affected Parties.

Status And Event Details Should Be Circulated On A Need-To-Know Basis And Only To Trusted Parties Identified On A Call List.

Trusted Parties Might Include Both Internal And External Stakeholders.

Obligations To Report The Attack Must Be Carefully Considered And It May Be Necessary To Inform Affected Parties During Or Immediately After The Incident So That They Can Perform Their Own Remediation E.G " Change Your Passwords Immediately "

12.3 Incident Response Plan

This Lists The Procedures, Contacts And Resources Available To Responders For Various Incident Categories.

A **Playbook** Is A Data-Driven Standard Operating Procedure (Sop) To Assist Junior Analysts In Detecting And Responding To Specific Cyberthreat Scenarios.

One Challenge In Incident Management Is To Allocate Resources Efficiently And There Are Several Factors That Can Affect This Process.

- **Data Integrity -** The Most Important Factor In Prioritizing Incidents
- **Downtime -** An Incident Can Either Degrade Or Interrupt The Availability Of An Asset Or System.
- **Economic/Publicity -** Both Data Integrity And Downtime Will Have Important Economic Effects. Short-Term Might Involve Lost Business Opportunity While Long-Term May Involve Damage To Reputation And Marketing Standing.
- **Scope -** Refers To The Number Of Affected Systems In An Incident
- **Detection Time -** Research Has Shown That More Than Half Of Data Breaches Are Not Detected For Weeks Or Months. This Demonstrates That Systems Used To Search For Intrusions Must Be Thorough.
- **Recovery Time -** Some Incidents Require Lengthy Remediation As The System Changes Required Are Complex To Implement.

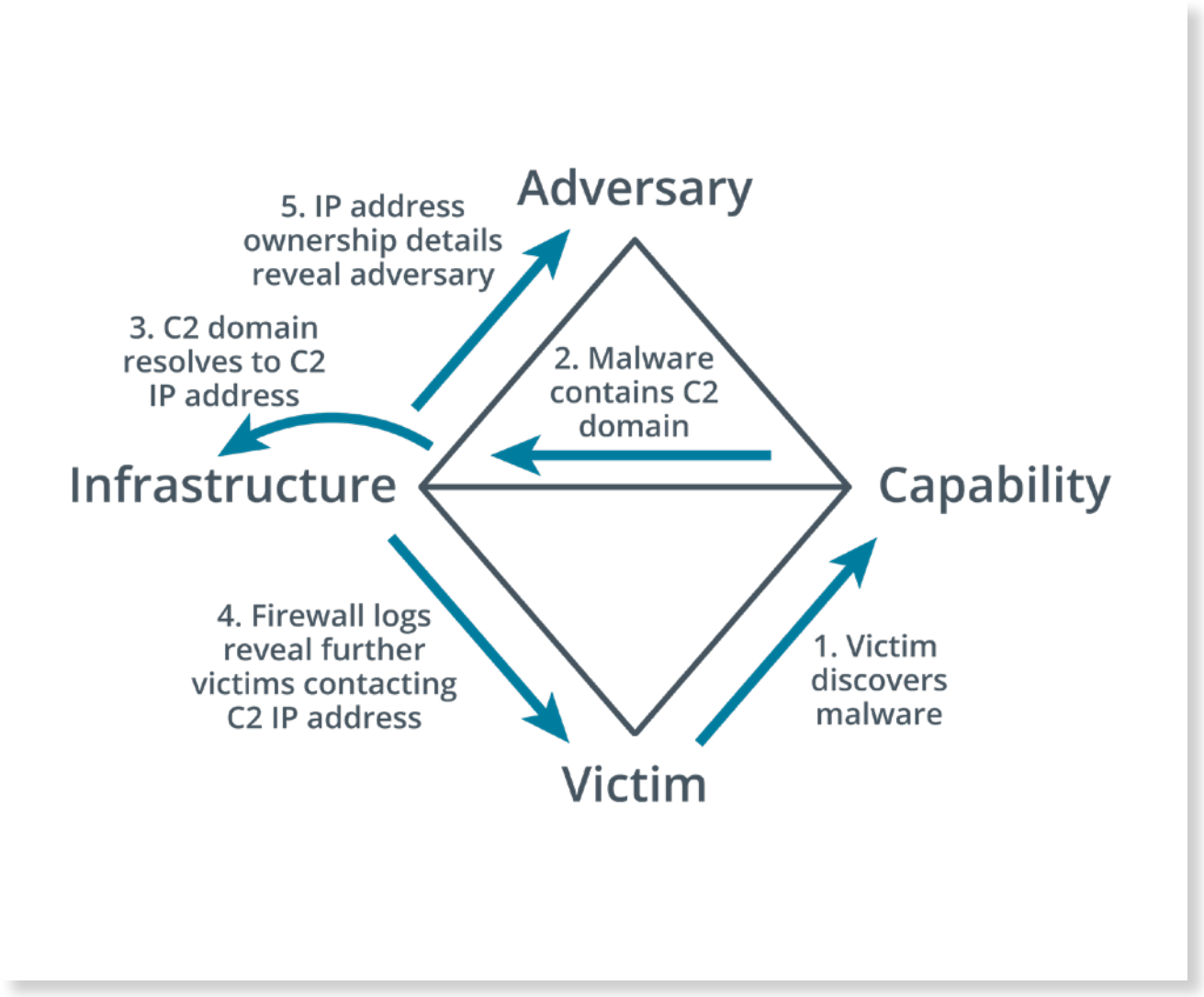
A Key Tool For Threat Research Is A Framework To Use To Describe The Stages Of An Attack And These Stages Are Referred To As A **Cyber Kill Chain**.

Mitre Att&Ck - An Alternative To The Kill Chain Is The Mitre Corporation's Adversarial Tactics, Techniques And Common Knowledge

It Provides Access To A Database Of Known Ttps And Tags Each Technique With A Unique Id And Places It In One Or More Tactic Categories Such As Initial Access , Persistence Or Command & Control.

Diamond Model Of Intrusion Analysis - This Suggests A Framework To Analyze An Intrusion Event (E) By Exploring The Relationships Between Four Core Features: Adversary, Capability, Infrastructure And Victim.

Each Event May Also Be Described By Meta-Features Such As Date/Time, Kill Chain Phase Etc.



12.4 Incident Response Exercises, Recovery And Retention Policy

Identification - This Is The Process Of Collating Events And Determining Whether Any Of Them Should Be Managed As Incidents Or As Possible Precursors To An Incident.

- **Tabletop -** Least Costly Where The Facilitator Presents A Scenario And The Responders Explain What Action They Would Take To Identify, Contain And Eradicate The Threat. Flashcards Are Used In Place Of Computer Systems.
- **Walkthroughs -** Similar To Tabletop Except Here The Responders Demonstrate What Actions They Would Take In Response Such As Running Scans And Analyzing Sample Files.
- **Simulations -** A Team Based Exercise Where The Red Team Attempts An Intrusion, The Blue Team Operates Response And Recovery Controls And The White Team Moderates And Evaluates The Exercise.

Disaster recovery plan - Also called the emergency response plan. This is a document meant to minimize the effects of a disaster or disruption. meant for short term events and implemented during the event itself.

Business continuity plan - Identifies how business processes should deal with both minor and disaster-level disruption. a continuity plan ensures that business processes can still function during an incident even if at a limited scale.

Continuity of operation planning (COOP) - This terminology is used for government facilities but is functionally similar to business continuity planning. In some definitions, coop refers specifically to backup methods of performing mission functions without IT support.

Retention policy - a retention policy for historic logs and data captures sets the period of which these are retained. indicators of a breach might be discovered only months after the breach and this would not be possible without the retention policy to keep logs and other digital evidence.

Training On Specific Incident Response Scenarios Can Use Three Forms

- **Tabletop -** Least Costly Where The Facilitator Presents A Scenario And The Responders Explain What Action They Would Take To Identify, Contain And Eradicate The Threat. Flashcards Are Used In Place Of Computer Systems.
- **Walkthroughs -** Similar To Tabletop Except Here The Responders Demonstrate What Actions They Would Take In Response Such As Running Scans And Analyzing Sample Files.
- **Simulations -** A Team Based Exercise Where The Red Team Attempts An Intrusion, The Blue Team Operates Response And Recovery Controls And The White Team Moderates And Evaluates The Exercise.

Disaster recovery plan - also called the emergency response plan. This is a document meant to minimize the effects of a disaster or disruption. meant for short term events and implemented during the event itself.

Business continuity plan - identifies how business processes should deal with both minor and disaster-level disruption. a continuity plan ensures that business processes can still function during an incident even if at a limited scale.

Continuity of operation planning (COOP) - this terminology is used for government facilities but is functionally similar to business continuity planning. In some definitions, coop refers specifically to backup methods of performing mission functions without IT support.

Retention policy - a retention policy for historic logs and data captures sets the period of which these are retained. indicators of a breach might be discovered only months after the breach and this would not be possible without the retention policy to keep logs and other digital evidence.

12.5 Incident Identification

Training On Specific Incident Response Scenarios Can Use Three Forms

- Using Logs, Error Messages And Ids/Firewall Alerts
- Comparing Deviations To Established Metrics To Recognize Incidents And Their Scopes
- Manual Or Physical Inspections Of Site, Premises, Networks And Hosts
- Notification By An Employee, Customer Or Supplier
- Public Reporting Of New Vulnerabilities

Correlation - This Means Interpreting The Relationship Between Individual Data Points To Diagnose Incidents Of Significance To The Security Team.

A SIEM (Security Information And Event Management System) Correlation Rule Is A Statement That Matches Certain Conditions.

These Rules Use Logical Expressions Such As And And Or And Operators (==, <,>, In)

A Single-User Logon Failure Might Not Raise An Alert However Multiple Failed Logins For The Same Account Over A Short Period Of Time Should Raise One.

Error.Logonfailure > 3 And Logonfailure.Alice And Duration < 10 Minutes

One of the biggest challenges in operating a SIEM is tuning the system sensitivity to reduce false positive indicators being reported as an event.

The correlation rules are likely to assign a criticality level to each match.

Trend analysis - This is the process of detecting patterns or indicators within a data set over a time series and using those patterns to make predictions about future events.

- Frequency-based trend analysis establishes a baseline for a metric such as number of errors per hour of the day. if the frequency exceeds the threshold for the baseline, then an alert is raised.
- **Volume-based trend analysis -** this can be based on logs growing much faster than usual. This analysis can also be based on network traffic and endpoint disk usage.
- Statistical deviation analysis can show when a data point should be treated as suspicious. For example, a data point that appears outside the two clusters for standard and admin users might indicate some suspicious activity by that account.

Logging platforms - Log data from network appliances and hosts can be aggregated by a siem either by installing a local agent to collect the data or by using a forwarding system to transmit logs directly to the siem server.

Syslog - Provides an open format, protocol and server software for logging event messages and it's used by a very wide range of host types.

A syslog message comprises a pri code, a header containing a timestamp and host name and a message part. usually uses UDP port 514

- Rsyslog uses the same configuration file syntax but can work over tcp and use a secure connection.
- Syslog-ng uses a different configuration file syntax but can also use tcp/secure communications and more advanced options for message filtering.

In linux, rather than writing events to syslog-format text files, logs from processes are written to a binary-format called **journald**.

Events captured by journald can be forwarded to syslog and to view events in journald directly, you can use **journalct** command to print the entire journal log.

System & security logs - The five main categories of windows event logs are:

- **Application** - Events generated by applications and services
- **Security** - Audit events such as a failed logon or denied access to a file
- **System -** Events generated by the os and its services such as storage volume health checks
- **Setup -** Events generated during the windows installation
- **Forwarded Events -** Events that are sent to the local log from other hosts.

Network logs can be generated from routers, firewalls, switches and access points.

Authentication attempts for each host are likely to be written to the security log.

DNS event logs may be logged by a dns server while web servers are typically configured to log http traffic that encounters an error or traffic that matches some predefined rule set.

The status code of a response can reveal something about both the request and the server's behavior.

- Codes in the 400 range indicate client-based errors
- Codes in the 500 range indicate server-based errors
- "403" may indicate that the server is rejecting a client's attempts to access resources they are not authorized to.
- "502" (bad gateway) response could indicate that communications between the target server and its upstream server are being blocked or the upstream server is down.

Dump files - A system memory dump creates an image file that can be analyzed to identify the processes that are running, the contents of temporary file systems, registry data, network connections and more.

It can also be a means of accessing data that is encrypted when stored on a mass storage device.

Metadata - This the properties of data as it is created by an application stored on media or transmitted over a network. Metadata sources are useful during an investigation as they can establish timeline questions as well as containing other types of evidence.

File - File metadata is stored as attributes. The file system tracks when a file was created, accessed and modified. The acl attached to a file showing its permissions also represents another type of attribute.

Web - when a client requests a resource from a web server, the server returns the resource plus headers setting or describing its properties. headers describe the type of data returned.

Email - An email's internet header contains address information for the recipient and sender plus details of the servers handling transmission of the message between them.

Mobile - Phone metadata comprises call detail records (CDRs) of incoming, outgoing and attempted calls and sms text time, duration and the opposite party's number. meta data will also record data transfer volumes and the location history of the device can be tracked by the list of cell towers it has used to connect to the network.

Netflow/ipfix - A flow collector is a means of recording metadata and statistics about network traffic rather than recording each frame.

Flow analysis tools can provide features such as:

- Highlighting trends and patterns in traffic generated by particular applications, hosts and ports.
- Alerting based on detection of anomalies or custom triggers
- Identification of traffic patterns revealing rouge user behavior or malware in transit

12.6 Digital Forensics Documentation

Digital Forensics Is The Practice Of Collecting Evidence From Computer Systems To A Standard That Will Be Accepted In A Court Of Law.

Prosecuting External Threat Sources Can Be Difficult As The Threat Actor May Be In A Different Country Or Have Taken Effective Steps To Disguise Their Location.

Like Dna Or Fingerprints, Digital Evidence Is Latent Meaning That The Evidence Cannot Be Seen With The Naked Eye; Rather It Must Be Interpreted Using A Machine Or Process.

Due Process - Term Used In Us And Uk Common Law That Requires That People Only Be Convicted Of Crimes Following The Fair Application Of The Laws Of The Land.

The First Response Period Following Detection And Notification Is Often Critical. To Gather Evidence Successfully, It‘s Vital That Staff Do Not Panic Or Act In A Way That Would Compromise The Investigation.

Legal Hold - This Refers To The Fact That Information That May Be Relevant To A Court Case Must Be Preserved. This Means That Computer Systems May Be Taken As Evidence With All The Obvious Disruption To A Network That Entails.

Chain Of Custody - This Documentation Reinforces The Integrity And Proper Handling Of Evidence From Collection, To Analysis, To Storage And Finally To Presentation. It Is Meant To Protect An Organization Against Accusations That Evidence Has Been Tampered With During A Trial.

Digital Forensics Reports - A Report Summarizes The Significant Contents Of The Digital Data And The Conclusions From The Investigator‘s Analysis.

- Analysis Must Be Performed Without Bias. Conclusions And Opinions Should Be Formed Only From The Direct Evidence Under Analysis.

- Analysis Methods Must Be Repeatable By Third Parties With Access To The Same Evidence
- Ideally, The Evidence Must Not Be Changed Or Manipulated.

E-Discovery - This Is A Means Of Filtering The Relevant Evidence Produced From All The Data Gathered By A Forensic Examination And Storing It In A Database In A Format Such That It Can Be Used As Evidence In A Trial.

Some Of The Functions Of E-Discovery Suites Are:

- **Identify And De -** Duplicate Files And Metadata
- **Search -** Allows Investigators To Locate Files Of Interest To The Case.
- **Tags -** Apply Standardized Keywords Or Labels To Files And Metadata To Help Organize The Evidence.
- **Security -** At All Points Evidence Must Be Shown To Have Stored, Transmitted And Analyzed Without Tampering.
- **Disclosure -** An Important Part Of The Trial Procedure Is That Evidence Is Made Available To Both Plaintiff And Defendant.

Video and witness interviews - The first phase of a forensics investigation is to document the scene by taking photographs and ideally audio and video.

As well as digital evidence, an investigator should interview witnesses to establish what they were doing at the scene and whether they observed any suspicious behavior or activity.

Timelines - A very important part of a forensic investigation will involve tying events to specific times to establish a consistent and verifiable narrative. This visual representation of events in a chronological order is called a timeline.

Operating systems and files use a variety of methods to identify the time at which something occurred but the benchmark time is coordinated universal time (utc).

Local time will be offset from UTC by several hours and this local time offset may also vary if a seasonal daylight saving time is in place.

NTFSuses utc “internally“ but many OS and file systems record timestamps as the local system time and when collecting evidence, it is vital to establish how a timestamp is calculated and note the offset between the local system time and utc.

Event logs and network traffic - An investigation may also obtain the event logs for one or more network appliances and/or server hosts. network captures might provide valuable evidence.

For forensics, data records that are not supported by physical evidence (data drive) must meet many tests to be admissible in court. if the records were captured by a SIEM, it must demonstrate accuracy and integrity.

The intelligence gathered from a digital forensic activity can be used in two different ways:

- **Counterintelligence -** Identification and analysis of specific adversary tactics, techniques and procedures (TTPS) provides information on how to configure and audit systems so they are better able to capture evidence of attempted and successful intrusions.
- **Strategic Intelligence -** Data that has been analyzed to produce actionable insights. These insights are used to inform risk management and security control provisioning to build mature cybersecurity capabilities.

12.7 Digital Forensics Evidence Acquisition

Acquisition is the process of obtaining a forensically clean copy of data from a device held as evidence. if the system is not owned by the organization then the seizure could be challenged legally (BYOD)

Data acquisition is also more complicated when capturing evidence from a digital scene compared to a physical one (evidence may be lost due to system glitches or loss of power).

Data acquisition usually proceeds by using a tool to make an image from the data held on the target device. the image can be acquired from either volatile or nonvolatile storage.

Digital acquisition and order of volatility - the general principle is to capture evidence in the order of volatility from more volatile to less volatile.

According to the ISOC, the order is as follows

- Cpu registers and cache memory
- Contents of ram including routing table, arp cache, kernel statistics
- Data on persistent mass storage devices like hard drives, usbs
- Remote logging and monitoring data
- Physical configuration and network topology
- Archival media and printed documents

Digital forensics software include:

- Encase forensic is a digital forensics case management product. contains workflow templates showing the key steps in diverse types of investigation.
- The forensic toolkit (ftk) from accessdata. a commercial investigation suite designed to run on windows server.
- **The sleuth kit -** an open source collection of command line tools and programming libraries for disk imaging and file analysis. autopsy is the gui that sits on top of the kit and is accessed through a web browser.
- **Winhex -** a commercial tool for forensic recovery and analysis of binary data, with support for a range of file systems and memory dump types.
- The volatility framework which is widely used for system memory analysis.

Disk image acquisition refers to acquiring data from non-volatile storage. it could also be referred to as device acquisition meaning the ssd storage in a smartphone or media player.

There are three device states for persistent storage acquisition

Live acquisition - Means copying the data while the host is still running. this may capture more evidence or more data for analysis and reduce the impact on overall services. however the data on the actual disks will have changed so this method may not produce legally acceptable evidence.

Static acquisition by shutting down the host - runs the risk that the malware will detect the shut-down process and perform anti-forensics to try and remove traces of itself.

Static acquisition by pulling the plug - This means disconnecting the power at the wall socket. This will likely preserve the storage device in a forensically clean state but there is the risk of corrupting data.

Whichever method is chosen, it is important to document the steps taken and supply a

timeline of all actions.

Preservation and integrity of evidence - It is vital that the evidence collected at the crime scene conform to a valid timeline. recording the whole process establishes **provenance** of the evidence as deriving directly from the crime scene.

To obtain a clean forensic image from a non-volatile storage, you need to ensure nothing you do alters the data or metadata on the source disk or file system. A **write blocker** can ensure this by preventing any data from being changed by filtering write commands.

The host devices and media taken from the crime scene should be labeled, bagged and sealed using tamper-evident bags. bags should have anti-static shielding to reduce the possibility that data will be damaged or corrupted on the electronic media by electrostatic discharge.

The evidence should be stored in a secure facility.

Acquisition of other data types includes:

- **Network -** Packet captures and traffic flows can contain evidence. most networks will come from a SIEM.
- **Cache -** Software cache can be acquired as part of a disk image. the contents of hardware cache are generally not recoverable.
- **Artifacts and data recovery -** Artifact refers to any type of data that is not part of the mainstream data structures of an os. Data recovery refers to analyzing a disk for file fragments that might represent deleted or overwritten files. The process of recovering them is referred to as carving.
- **Snapshot -** Is a live acquisition image of a persistent disk and may be the only means of acquiring data from a virtual machine or cloud process.
- **Firmware -** Is usually implemented as flash memory. Some types like the pc firmware can potentially be extracted from the device or from the system memory using an imaging utility.

12.8 Data Sources

Incident investigation often requires analysis of several data sources in order to draw a defensible conclusion.

- Vulnerability Scans
- Log files
- SIME dashboards
- Metadata
- Packet capture

Log Analysis and Response Tools

- Security Information Event Management (SIEM) is an automation tool for real-time data capture, event correlation, analysis and reporting
- Threat Intelligence Platform (TIP) is an automation tool that combines multiple threat intelligence feeds and integrates with existing SIEM solutions
- User & Entity Behavior Analytics (UEBA) - is an automation tool that models human and machine behavior to identify normal and abnormal behavior.
- Security Orchestration, Automation and Response (SOAR) is an automation tool that responds to alerts and takes remediation steps.

Packet Capture - This is the process of intercepting and logging traffic for analysis.

- A protocol analyzer (sniffer) is a tool used to capture and analyze network packets
- A port mirror captures network traffic from one or several ports of a switch and forwards a copy of the traffic to an analysis device
- A network TAP is a dedicated hardware device that is inserted between network devices and makes copies of the traffic and forwards to an analysis device.

Packet Capture Modes

- **Normal -** The network interface card (NIC) only captures frames intended for the interface (filtering by MAC address)
- **Promiscuous -** The NIC accepts any frame it captures even if it was not the intended recipient
- **Unfiltered -** Packet capture regardless of data elements
- **Filtered -** Packet capture limited to specific data elements

SECTION 13 -

ANALYZE INDICATORS OF MALICIOUS ACTIVITY

13.1 Malware Classification

Some Malware Classifications Such As Trojan, Virus And Worm Focus On The Vector Used By The Malware. The Vector Is The Method By Which The Malware Executes On A Computer And Potentially Spreads To Other Network Hosts.

The Following Categories Describe Some Types Of Malware According To Vector:

- **Viruses & Worms -** Spread Without Any Authorization From The User By Being Concealed Within The Executable Code Of Another Process.
- **Trojan -** Malware Concealed Within An Installer Package For Software That Appears To Be Legitimate
- **Potentially Unwanted Programs/Applications (Pups/Puas) -** These Are Software Installed Alongside A Package Selected By The User. Unlike A Trojan, Their Presence Isn't Necessarily Malicious. They Are Sometimes Referred To As Grayware.

Other Classifications Are Based On The Payload Delivered By The Malware. The Payload Is The Action Performed By The Malware

Examples Of Payload Classification Include:

- Spyware
- Rootkit
- Remote Access Trojan (Rat)
- Ransomware

13.2 Computer Viruses

This Is A Type Of Malware Designed To Replicate And Spread From Computer To Computer Usually By “Infecting” Executable Applications Or Program Code.

The Following Categories Describe Some Types Of Malware According To Vector:

- **Non-Resident/File Infector -** The Virus Is Contained Within A Host Executable File And Runs With The Host Process. The Virus Will Try To Infect Other Process Images On Persistent Storage And Perform Other Payload Actions.
- **Memory Resident -** When The Host File Is Executed, The Virus Creates A New Process For Itself In Memory. The Malicious Process Remains In The Memory Even If The Host Process Is Terminated.
- **Boot -** The Virus Code Is Written To The Disk Boot Sector And Executes As A Memory Resident Process When The Os Starts.
- **Script And Macro Viruses -** The Malware Uses The Programming Features Available In Local Scripting Engines For The Os And/Or Browser Such As Powershell, Javascript, Microsoft Office Documents Or Pdf Documents With Javascript Enabled.

The Term **Multipartite** Is Used For Viruses That Use Multiple Vectors And **Polymorphic** For Viruses That Can Dynamically Change Or Obfuscate Their Code To Evade Detection. Viruses Must Infect A Host File Or Media. An Infected File Can Be Distributed Through Any Normal Means - On A Disk, On A Network, A Download From A Website Or Email Attachment.

13.3 Computer Worms & Fileless Malware

Computer Worms - this is a memory resident malware that can run without user intervention and replicate over network resources. viruses need the user to perform an action but worms can execute by exploiting a vulnerability in a process and replicate themselves.

Worms can rapidly consume network bandwidth as the worm replicates and they may be able to crash an operating system or server application. worms can also carry a payload that may perform some other malicious action.

Fileless malware - as security controls got more advanced so did malware and this new sophisticated modern type of malware is often referred to as fileless.

The Following Categories Describe Some Types Of Malware According To Vector:

- Fileless Malware Do Not Write Their Code To Disk. The Malware Uses Memory Resident Techniques To Run Its Own Process Within A Host Process Or Dynamic Link Library (Dll). The Malware May Change Registry Values To Achieve Persistence.
- Fileless Malware Uses Lightweight Shellcode To Achieve A Backdoor Mechanism On The Host. The Shellcode Is Easy To Recompile In An Obfuscated Form To Evade Detection By Scanners. It Is Then Able To Download Additional Packages Or Payloads To Achieve The Actor's Objectives.
- Fileless Malware May Use "Live Off The Land" Techniques Rather Than Compiled Executables To Evade Detection. This Means That The Malware Code Uses Legitimate System Scripting Tools Like Powershell To Execute Payload Actions.

13.4 Spyware, Keyloggers, Rootkits, Backdoors, Ransomware & Logic Bombs

Spyware - This is malware that can perform adware-like tracking but also monitor local application activity, take screenshots and activate recording devices.

Adware - Grayware that performs browser reconfigurations such as allowing cookies, changing default search engines, adding bookmarks and so on.

Tracking cookies - Can be used to record pages visited, the user's ip address and various other metadata.

Keylogger - Spyware that actively attempts to steal confidential information by recording keystrokes.

Backdoors & rats - A backdoor provides remote user admin control over a host and bypasses any authentication method. A remote access trojan is a backdoor malware that mimics the functionality of legitimate remote control programs but is designed specifically to operate covertly. a group of bots under the same control of the same malware are referred to as a botnet and can be manipulated by the herder program.

Rootkits - This malware is designed to provide continued privileged access to a computer while actively hiding its presence. it may be able to use an exploit to escalate privileges after installation.software processes can run in one of several "rings".

- Ring 0 is the most privileged and provides direct access to hardware
- Ring 3 is where user-mode processes run
- Ring 1 or 2 is where drivers and i/o processes may run.

Ransomware - This type of malware tries to extort money from the victim by encrypting the victim's files and demanding payment. ransomware uses payment methods such as wire transfer or cryptocurrency.

Logic bombs - Logic bombs are not always malware code. a typical example is a disgruntled admin who leaves a scripted trap that runs in the event his or her account is disabled or deleted. anti-malware software is unlikely to detect this kind of script and this type of trap is also referred to as a mine.

13.5 Malware Indicators & Process Analysis

There Are Multiple Indicators Of Malware:

- Antivirus Notifications
- Sandbox Execution
- Resource Consumption - Can Be Detected Using Task Manager Or Top Linux Utility.
- File System

Because shellcode is easy to obfuscate, it can easily evade signature-based a-v products. Threat hunting and security monitoring must use behavioral-based techniques to identify infections.

Along with observing how a process interacts with the file system, network activity is one of the most reliable ways to identify malware.

13.6 Password Attacks

Plain text/ unencrypted attacks - an attack that exploits unencrypted password storage such as those used in protocols like http, pap and telnet.

Online attacks - The threat actor interacts directly with the authentication service using either a database of known passwords or a list of passwords that have been cracked online. This attack can be prevented with the use of strong passwords and restricting the number of login attempts within a specified period of time.

Password spraying - A horizontal brute force attack where the attacker uses a common password (123456) and tries it with multiple usernames.

Offline attacks - An offline attack means the attacker has gotten access to a database of password hashes e.g %systemroot%\system32\config\sam or %systemroot%\ntds\ntds.dit (the active directory credential store)

Brute force attack - Attempts every possible combination in the output space in order to match a captured hash and guess the plaintext that generated it. the more the characters used in the plaintext password, the more difficult it would be to crack.

Rainbow table attack - A refined dictionary attack where the attacker uses a precomputed lookup table of all possible passwords and their matching hashes.

Hybrid attack - Uses a combination of brute force and dictionary attacks.

Password crackers - There are some windows tools including cain and l0phtcrack but the majority of password crackers like hashcat run primarily on linux.

Password managers can be implemented with a hardware token or as a software app:

- **Password Key** - Usb tokens for connecting to pcs and smartphones.
- **Password Vault -** Software based password manager typically using a cloud service to allow access from any device.

13.7 Tactics, Techniques & Procedures

A Tactic, Technique Or Procedure (Ttp) Is A Generalized Statement Of Adversary Behavior. Ttps Categorize Behaviors In Terms Of Campaign Strategy And Approach (**Tactics**), Generalized Attack Vectors (**Techniques**) And Specific Intrusion Tools And Methods (**Procedures**).

An **Indicator Of Compromise** (Ioc) Is A Residual Sign That An Asset Or Network Has Been Successfully Attacked. In Other Words, An Ioc Is Evidence Of A Ttp.

Examples Of Iocs Include

- Unauthorized Software And Files
- Suspicious Emails
- Suspicious Registry And File System Changes
- Unknown Port And Protocol Usage
- Excessive Bandwidth Usage
- Rouge Hardware
- Service Disruption And Defacement
- Suspicious Or Unauthorized Account Usage

Strictly Speaking An Ioc Is Evidence Of An Attack That Was Successful. The Term Indicator Of Attack (Ioa) Is Sometimes Also Used For Evidence Of An Intrusion Attempt In Progress.

13.8 Privilege Escalation & Error Handling

Application Attack - This Attacks A Vulnerability In An Os Or Application And A Vulnerability Refers To A Design Flaw That Can Cause The Application Security System To Be Circumvented Or To Crash. The Purpose Of This Attack Is To Allow The Attacker To Run His/Her Own Code On The System And This Is Referred To As **Arbitrary Code Execution**.

Where The Code Is Transmitted From One Computer To Another, This Is Referred To As Remote Code Execution.

Privilege Escalation - A Design Flaw That Allows A Normal User Or Threat Actor To Suddenly Gain Extended Capabilities Or Privileges On A System.

- **Vertical Privilege Escalation -** The User Or Application Is Able To Gain Access To Functionality Or Data That Shouldn't Be Available To Them.
- **Horizontal Privilege Escalation -** The User Or Application Is Able To Access Data Or Functionality Intended For Another User.

Error Handling - An Application Attack May Cause An Error Message. As Such Applications In The Event Of An Error Should Not Reveal Configuration Or Platform Details That Can Help The Attacker.

Improper Input Handling - Good Programming Practice Dictates That Any Input Accepted By A Program Or Software Must Be Tested To Ensure That It Is Valid. Most Application Attacks Work By Passing Invalid Or Maliciously Constructed Data To The Vulnerable Process.

13.9 Uniform Resource Locator Analysis & Percent Encoding

Uniform Resource Locator Analysis - Besides Pointing To The Host Or Service Location On The Internet, A Url Can Encode Some Action Or Data To Submit To The Server Host. This Is A Common Vector For Malicious Activity.

Http Methods - It Is Important To Understand How Http Operates.

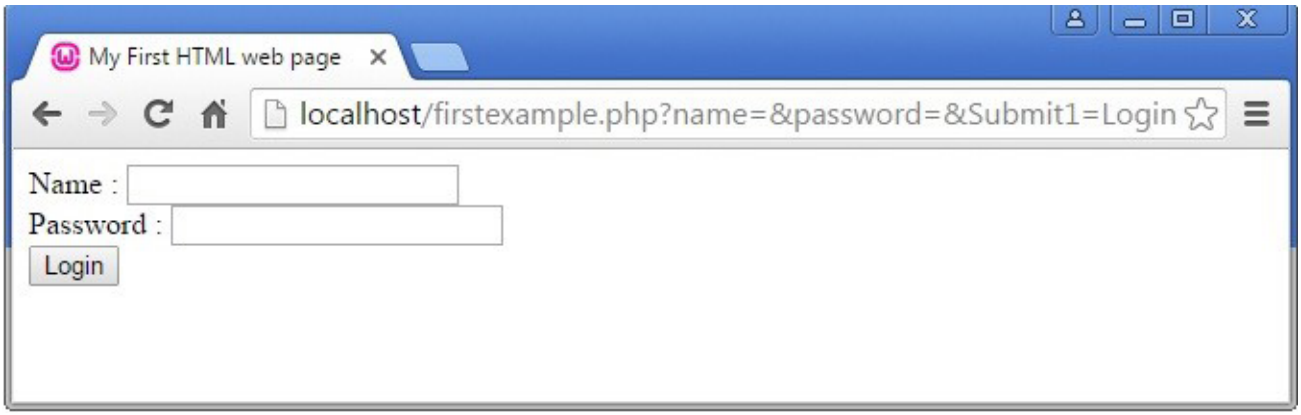
- An Http Session Starts With A Client (Web Browser) Making A Request To An Http Server.
- The Connection Establishes A Tcp Connection
- The Connection Can Be Used For Multiple Requests Or A Client Can Start New Tcp Connections For Different Requests.

A Request Typically Contains A Method, Resource (Url Path), Version Number, Headers And Body. The Principal Method Is Get But Other Methods Include:

- **Post -** Send Data To The Server For Processing By The Requested Resource
- **Put -** Create Or Replace The Resource. Delete Can Be Used To Remove The Resource
- **Head -** Retrieve The Headers For A Resource Only (Not The Body)

Data Can Be Submitted To The Server Using A Post Or Put Method And The Http Headers And Body Or By Encoding The Data Within The Url Used To Access The Resource.

Data Submitted Via A Url Is Delimited By The ? Character Which Follows The Resource Path And Query Parameters Are Usually Formatted As One Or More Name=Value Pairs, With Ampersands Delimiting Each Pair.



Percent Encoding - A Url Can Contain Only Unreserved And Reserved Characters From The Ascii Set. Reserved Ascii Characters Are Used As Delimiters Within The Url Syntax.

Reserved Characters **: / ? # [ ] @ ! $ & ' ( ) * + , ; =**

There Are Also Unsafe Characters Which Cannot Be Used In A Url. Control Characters Such As Null String Termination, Carriage Return, Line Feed, End Of File And Tab Are Unsafe.

Character	Percent Encoding
null	%00
space	%20
CR (Carriage Return)	%0D
LF (Line Feed)	%0A
+	%2B
%	%25
/	%2F
\	%5C
.	%2E
?	%3F
"	%22
'	%27
<	%3C
>	%3E
&	%26
|	%7C

13.10 Api & Replay Attacks, Cross-Site Request Forgery, Clickjacking & Ssl Strip Attacks

Application Programming Interface Attacks - Web Applications And Cloud Services Implement Application Program Interfaces (Apis) To Allow Consumers To Automate Services.

If The Api Isn't Secure, Threat Actors Can Easily Take Advantage Of It To Compromise The Services And Data Stored On The Web Application. Api Calls Over Plain Http Are Not Secure And Could Easily Be Modified By A Third Party.

Some Other Common Attacks Against Apis Include

- Ineffective Secrets Management, Allowing Threat Actors To Discover An Api Key And Perform Any Action Authorized To That Key.
- Lack Of Input Validation Allowing The Threat Actor To Insert Arbitrary Parameters Into Api Methods And Queries. This Is Often Referred To As Allowing Unsanitized Input.
- Error Messages Revealing Clues To A Potential Adversary. (Username/Password)
- Denial Of Service (Dos) By Bombarding The Api With Bogus Calls.

Replay Attacks - Session Management Enables Web Applications To Uniquely Identify A User Across A Number Of Different Actions And Requests.

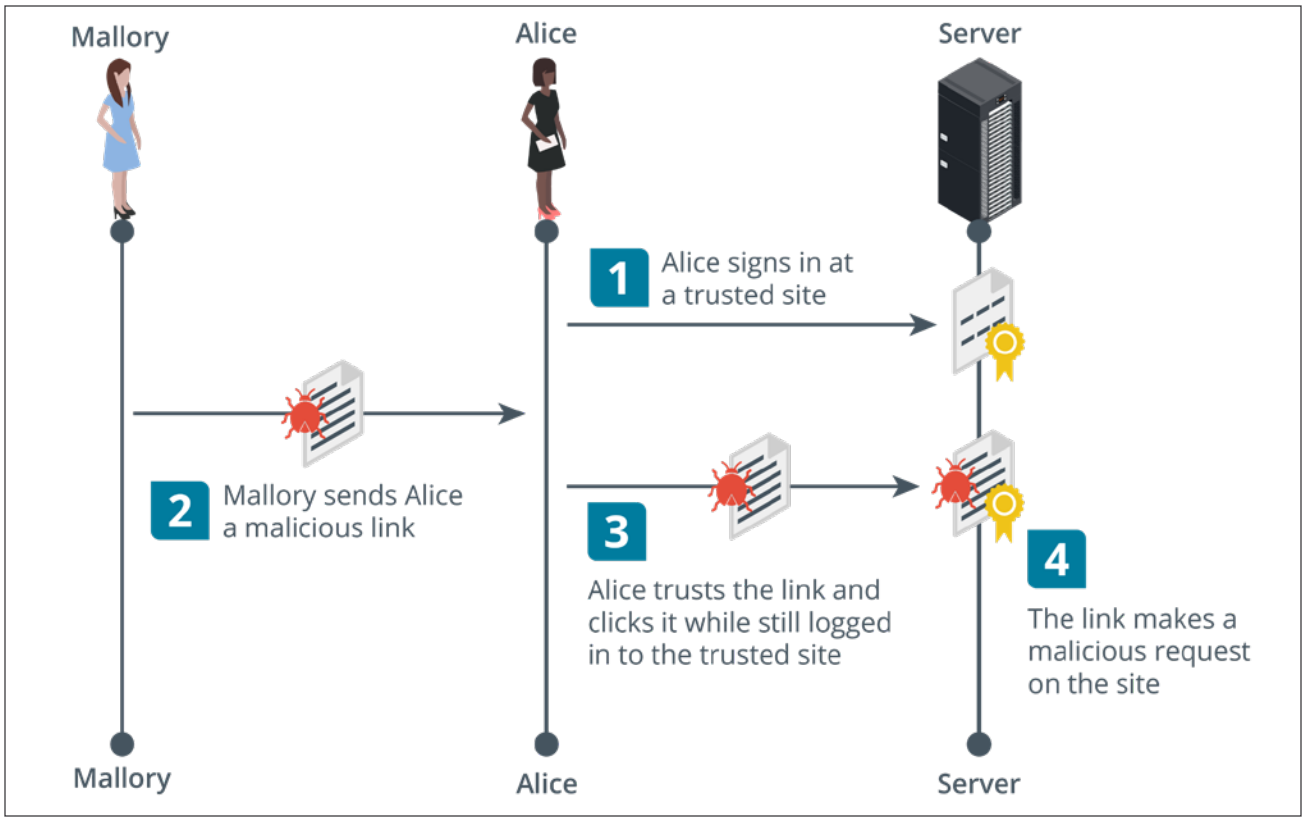
To Establish A Session, The Server Normally Gives The Client Some Type Of Token And A Replay Attack Works By Sniffing Or Guessing The Token Value And Then Submitting It To Re-Establish The Session Illegitimately.

Http By Default Is A Stateless Protocol Meaning The Server Preserves No Information About The Client But **Cookies** Allow For The Preservation Of Data.

A Cookie Has A Name, Value And Optional Security And Expiry Attributes. Cookies Can Either Be Persistent And Non-Persistent.

Cross-Site Request Forgery - A Client-Side Or Cross-Site Request Forgery (Csrf Or Xsrf) Can Exploit Applications That Use Cookies To Authenticate Users And Track Sessions.

In Order To Work, The Attacker Must Convince The Victim To Start A Session With The Target Site. The Attacker Must Then Pass An Http Request To The Victim's Browser That Spoofs An Action On The Target Site Such As Changing A Password Or An Email Address.



If The Target Site Assumes The Browser Is Authenticated Because There Is A Valid Session Cookie, It Will Accept The Attacker's Input As Genuine.

This Is Also Referred To As A Confused Deputy Attack.

Clickjacking - This Is An Attack Where What The User Sees And Trusts As A Web Application With Some Sort Of Login Page Or Form Contains A Malicious Layer Or Invisible Iframe That Allows An Attacker To Intercept Or Redirect User Input.

Clickjacking Can Be Launched Using Any Type Of Compromise That Allows The Adversary To Run Arbitrary Code As A Script. It Can Be Mitigated By Using Http Response Headers That Instruct The Browser Not To Open Frames From Different Origins

Ssl Strip - This Is Launched Against Clients On A Local Network As They Try To Make Connections To Websites. The Threat Actor First Performs A Mitm Attack Via Arp Poisoning To Masquerade As The Default Gateway.

When A Client Requests An Http Site That Redirects To An Https Site In An Unsafe Way, The Sslstrip Utility Proxies The Request And Response, Serving The Client The Http Site With An Unencrypted Login Form Thus Capturing Any User Credentials.

13.11 Injection Attacks

XML and LDAP injection attacks - an injection attack can target other types of protocols where the application takes user input to construct a query, filter or document.

Extensible markup language (xml) injection - xml is used by apps for authentication and authorizations and for other types of data exchange and uploading.

Lightweight directory access protocol (ldap) injection - ldap is another example of query language. ldap is specifically used to read and write network directory databases. a threat actor could exploit either unauthenticated access or a vulnerability in a client app to submit arbitrary ldap queries. This could allow accounts to be created or deleted or for the attacker to change authorizations and privileges.

For example a web form could construct a query from authenticating the valid credentials for bob and pa$$w0rd like this:

(& (username = bob)(password = pa$$w0rd))

If the form input is not sanitized, the threat actor could bypass the password check by entering a valid username plus an ldap filter string

(& (username = bob)(&))

Directory traversal & command injection attacks - directory traversal is another type of injection attack performed against a web server.

The threat actor submits a request for a file outside the web server's root directory by submitting a path to navigate to the parent directory (../)

The threat actor might use a **canonicalization** attack to disguise the nature of the malicious input.

Canonicalization refers to the way the server converts between different methods by which a resource (file path or url) may be represented and submitted to the simplest method used by the server to process the input.

Server-side request forgery (SSRF) - SSRF causes the server application to process an arbitrary request that targets another service either on the same host or a different one.

It exploits both the lack of authentication between the internal servers and services and weak input validation allowing the attacker to submit unsanitized requests or api parameters.

SECTION 14 -

SUMMARIZE SECURITY GOVERNANCE CONCEPTS

14.1 Regulations, Standards & Legislation

Key Frameworks, Benchmarks And Configuration Guides May Be Used To Demonstrate Compliance With A Country's Legal Requirements.

Due Diligence Is A Legal Term Meaning That Responsible Persons Have Not Been Negligent In Discharging Their Duties.

- Sarbanes-Oxley Act (Sox) Mandates The Implementation Of Risk Assessments, Internal Controls And Audit Procedures.
- The Computer Security Act (1987) Requires Federal Agencies To Develop Security Policies For Computer Systems That Process Confidential Information.
- In 2002, The Federal Information Security Management Act (Fisma) Was Introduced To Govern The Security Of Data Processed By Federal Government Agencies.

Some Regulations Have Specific Cybersecurity Control Requirements While Others Simply Mandate "Best Practice" As Represented By A Particular Industry Or International Framework.

Personal Data And General Data Protection Regulation (GDPR)

This legislation focuses on information security as it affects privacy or personal data.

GDPR means that personal data cannot be collected, processed or retained without the individual's informed consent.

Compliance issues are complicated by the fact that laws derive from different sources e.g gdpr does not apply to american data subjects but it does apply to american companies that collect or process the personal data of people in eu countries.

National, Territory Or State Laws

In the US there are federal laws such as the gramm-leach-bliley act (GLBA) for financial services and the health insurance portability and accountability act (HIPAA).

14.2 ISO and Cloud Frameworks

Iso 27k - The International Organization For Standardization (Iso) Has Produced A Cybersecurity Framework In Conjunction With The International Electrotechnical Commission (Iec).

Unlike The Nist Framework, The Iso 27001 Must Be Purchased. The Iso 27001 Is Part Of An Overall 27000 Series Of Information Security Standards Also Known As 27k.

There Are 3 Main Versions Of The Iso 27k

- **27002 -** Security Controls
- **27017 & 27018 -** Cloud Security
- **27701 -** Personal Data & Privacy

Iso 31k - This Is An Overall Framework For Enterprise Risk Management (Erm). Erm Considers Risks And Opportunities Beyond Cybersecurity By Including Financial, Customer Service And Legal Liability Factors.

Cloud Security Alliance (Csa) - The Not-For-Profit Organization Produces Various Resources To Assist Cloud Service Providers (Csp) In Setting Up And Delivering Secure Cloud Platforms.

Security Guidance - A Best Practice Summary Analyzing The Unique Challenges Of Cloud Environments And How On-Premises Controls Can Be Adapted To Them.

Enterprise Reference Architecture - Best Practice Methodology And Tools For Csps To Use In Architecting Cloud Solutions.

Cloud Controls Matrix - Lists Specific Controls And Assessment Guidelines That Should Be Implemented By Csps.

Statements On Standards For Attestation Engagements (SSAE) - the SSAE are audit specifications developed by the american institute of certified public accountants (aicpa). These audits are designed to assure consumers that service providers (notably cloud providers) meet professional standards.

Within Ssae No. 18, There Are Several Levels Of Reporting:

Service Organization Control (Soc2) - Soc2 Evaluates The Internal Controls Implemented

By The Service Provider To Ensure Compliance With Trust Services Criteria (Tsc) When Storing And Processing Customer Data.

An Soc Type 1 Report Assesses The System Design, While A Type 2 Report Assesses The Ongoing Effectiveness Of The Security Architecture Over A Period Of 6-12 Months.

Soc2 Reports Are Highly Detailed And Designed To Be Restricted.

Soc 3 - A Less Detailed Report Certifying Compliance With Soc2. They Can Be Freely Distributed.

14.3 Governance Structure

Enterprise Governance - This is a system that holds to account, directs and controls all entities involved in an organization.

Governance is useful in identifying roles and responsibilities.

A role is a specific position or job title that an individual occupies within an organization. Stewardship is the responsible oversight and protection of something entrusted to one's care. Responsibility refers to the specific duties or tasks that an individual is expected to fulfill within a given role.

Board of Directors

- Determine the desired future state of information/cyber security and provide funding.
- Exercise Due Care (providing the standard of care that a prudent person would have provided under the same conditions.)
- A fiduciary is a person or organization who holds a position of trust
- They also provide oversight and authorization of organizational activities.

Executive Management Duties

- Make decisions to achieve strategic goals and objectives
- Manage risks to an acceptable risk and also comply with applicable laws and regulations.
- Manage resources and the budget efficiently
- Evaluate performance measures
- Implement oversight process

Information Security Steering Committee

- Make decisions to achieve information security strategic goals and objectives
- Set a cybersecurity budget, authorize risk decisions and report to the board of committee.
- They provide an effective communication channel for ensuring the alignment of the security program and business objectives.

Chief Information Security Officer (CISO) - Interprets strategic decisions and is ultimately responsible for the success or failure of the information security program.

Supporting roles include Information Assurance Officer/Manager (IAO/IAM), Information Security Officer (ISO)

Complimentary Organization Roles

- **Privacy Officer -** Responsible for developing and implementing all aspects of the privacy program.
- **Compliance Officer -** Responsible for identifying all applicable regulatory and contractual requirements.
- **Physical Security Officer -** Responsible for ensuring that appropriate physical security procedures are implemented
- **Internal Audit -** Responsible for providing independent and objective assurance services.

Functional Roles

- **Owners -** Responsible for oversight and decisions related to access control and protection.
- **Custodians -** Responsible for advising, managing and monitoring data protection controls.
- **Users -** Responsible for treating data in accordance with security policies and objectives.

14.4 Governance Documents

These are used to communicate direction, expectations and rules.

They are typically derived from the information security strategy which is also derived from the desired future state.

Policies

- These codify the high-level requirements for securing information assets and ensure CIA
- They should be approved and authorized by the organization's highest governing body
- Modifications should be minor over extended periods of time

Standards, Baselines & Guidelines

- Standards serve as precise specifications for the implementation of policy and dictate mandatory requirements.
- Baselines are the aggregate of standards for a specific category or grouping such as a platform, device type or location
- Guidelines assist in helping to understand and conform to a standard. Guidelines are not mandatory.

Procedures - Procedures are instructions for how to carry out an action. They focus on discrete actions or steps with a specific starting and ending point.

- **Simple Step -** Lists sequential actions. There is no decision making
- **Hierarchical -** Organizes the instructions in a hierarchical structure where each level is nested within the one above it.
- **Graphic -** Presents in pictorial or symbol form.
- **Flowchart -** Is used to communicate a process and when decision making is required.

Plan - This is a detailed strategy or tactic for doing or achieving something.

The function of the plan is to provide instructions and guidance on how to execute or respond to a situation within a certain timeframe usually with defined stages and with designated resources.

Acceptable Use Policy (AUP) - This details user community obligations pertaining to Information and information systems. It contains rules that specifically pertain to acceptable behavior and actions that are prohibited.

It's a teaching document that develops security awareness and must be written in a way that is easy to understand.

Non-disclosure Agreement (NDA) - Establishes data ownership and the reason why the data is being provided.

It's primarily used to prevent data disclosure and prevents forfeiture of patent rights.

Acceptable Use Policy Agreement - When a user signs it, they acknowledge that they understand and agree to abide by the AUP including violation sanctions up to and including termination.

Agreement should be executed prior to being granted access to information and information systems.

14.5 Change Management

The objective is to drastically minimize the risk and impact a change can have on business operations.

Types of Changes

- **Standard -** Occurs frequently, is low risk and has a pre-established procedure with documented tasks for completion (updates, patch management)
- **Normal -** Not standard but also not an emergency. Can be approved by the change control board (change of anti-malware product)
- **Major -** May have significant financial implications and could be high risk. May require multiple levels of management approval (change to new Operating system)
- **Emergency -** This is one that must be assessed and implemented without prior authorization to quickly resolve a major incident (switch to a backup server)

Configuration Management KPIs - Key Performance Indicators (KPIs) are business metrics used to measure performance in relation to strategic goals and objectives.

- **Successful Changes -** The higher the better
- **Backlog of Changes -** Changes not yet completed and should not grow over time
- **Emergency Changes -** It should not trend upward

14.6 Configuration Management

This is a set of practices designed to ensure that Configuration Items (CI) are deployed in a consistent state and stay that way through their frame. The primary goal is to minimize risk and ensure the configuration of services are known, good and trusted.

Configuration Management Elements

- **Configuration Item (CI) -**This is an aggregation of information system components and treated as a single entity throughout the configuration management process.
- **Baseline Configuration (BC) -** A set of specifications for a CI that has been reviewed and agreed upon and can be changed only through change control procedures.

Automated Provisioning - This is the ability to deploy information technology (IT) or operational technology (OT) systems and services using predefined automated procedures without requiring human intervention.

The primary goal is to reduce or eliminate manual dependencies and human error.

Provisioning Processes

- **Demand -** Generated Resource Allocation - is the automatic provisioning and deprovisioning of resources based upon demand.
- **Idempotence -** Is a principle that every time an automated configuration script is run, the same exact result is produced.
- **Immutable System -** Immutability is the principle that resources should not be changed, only created and destroyed (replace not fix).
- **Infrastructure as Code -** Is using code to manage configurations and automate provisioning of infrastructure. Supports Idempotence.

14.7 Scripting, Automation & Orchestration

Scripting - This is a set of instructions (interactive/non-interactive) used to automate a sequence of repetitive tasks.

Usually written in a scripting language which means they are interpreted and not compiled (the scripts are read and executed line-by-line by the processor at runtime).

Scripting Tools

- **Python -** Interpreted, open-source programming language with an extensive available library.
- **PowerShell -** Microsoft automation and configuration management framework
- **Bash -** Linux | Unix shell command line interface (CLI) and scripting language.
- **Macro -** An automated input sequence that imitates keystrokes or mouse actions.

Adversarial Scripting

- **Python -** Very easy to learn and is used for writing attack code and tools
- **PowerShell -** Can be used to direct the execution of a local script, retrieve and execute remote resources using various network protocols and encode payloads.
- **Bash -** Can be used to direct the execution of a local script, retrieve and execute remote resources using various network protocols and automate tasks on a LINUX/UNIX platform
- **Macro -** A macro virus can infect a software program and trigger a set of actions when the program is opened or run.

Automation - This is the execution of tasks without human intervention.

The goals are to eliminate manual dependencies and human error, improve quality of service, increase agility and reduce risk. Typically requires significant investment.

Orchestration - Orchestration is the coordination and management of multiple computer systems, applications and/or services, stringing together multiple tasks in order to execute a larger workflow or process.

SECTION 15 - EXPLAIN RISK MANAGEMENT

15.1 Risk management process

Risk management involves all processes from assessing the risk to managing it.

- **Identify Assets -** Humans, data, emails, hardware (scoping)
- **Identify Vulnerabilities -** Weak passwords, unpatched systems
- **Identify Exploits & Threats -** Hackers, natural disasters
- **Determine Safeguards & Countermeasures -** Security policies, backups, patches, updates etc
- Determine which risks are acceptable or not

Enterprise risk management - Risk management is treated very differently in companies of different sizes and compliance requirements. most companies will institute enterprise risk management (erm) policies and procedures based on frameworks such as nist's rmf

Risk Types

- External
- Internal
- Multiparty (Supply Chain Attack)
- Intellectual Property (Ip) Theft
- Software Compliance/Licensing
- Legacy Systems

Quantitative risk assessment - This aims to assign concrete values to each risk factor:

- **Single loss expectancy (sle) -** The amount that would be lost in a single occurrence of the risk factor. it's calculated by multiplying the value of the asset by an exposure factor (ef). ef is the percentage of the asset value that would be lost.
- **Annualized loss expectancy (ale) -** The amount that would be lost over the course of a year. done by multiplying the sle by the annualized rate of occurrence (aro)

It's important to realize that the value of an asset isn't just about its material value but also the damage its compromise could cost the company (e.g a server is worth more than its cost).

Qualitative risk assessment - Seeks out people's opinions of which risk factors are significant. assets and risks may be placed in categories such as high, medium or low value and critical, high, medium or low probability respectively.

Risk Factor	Impact	ARO	Cost Of Control	Overall Risk
Legacy Windows Clients	⚠	✖	⚠	✖
untrained Staff	✔	⚠	✔	⚠
No Antivirus Software	⚠	✖	⚠	✖

15.2 Risk Controls

Risk Mitigation - This is the most common method of handling risk and typically involves the use of countermeasure or safe guards. The likelihood of the risk occurring must be reduced to the absolute minimum.

Risk Avoidance - The cost of the risk involved is too high and must be avoided. Mitigation means the risk probabilities are reduced to the maximum while avoidance means the risk is eliminated completely

Risk Transference - This involves assigning or transferring the risk to another entity or organization. In other words, the risk is outsourced because the organization cannot mitigate the risk on it's own due to cost.

Risk Acceptance - The cost of mitigating the risk outweighs the cost of losing the asset. Risk can also be accepted when there isn't a better solution.

Risk Appetite & Residual Risk - Where risk acceptance has the scope of a single system, risk appetite has a project or institution-wide scope and is typically constrained by regulation and compliance. Where inherent risks are the risks before security controls have been applied, residual risks are those carried over after the controls have been applied.

Control risk is a measure of how much less effective a security control has become over time e.G antivirus.

Risk Register - A document showing the results of risk assessments in a comprehensible format.

Business Impacts and Risk Value

	Risk Criticality	Overall Projected Loss	Critical Systems Downtime	Non-Critical Systems Downtime	Data Leak	Brand Damage	Compliance	Calculated Value
5	Critical	>50 M	>30 min	>24 Hrs	Highly sensitive PII for more than 5 people	Re-branding, loss of major accounts	Major (Ex. License loss)	$100 M
4	High	5-50 M	Up to 30 min	5-24 Hrs	Detailed PII for multiple people	Major damage sustained for years	Fines >$200k, investigation impacting business	$50 M
3	Medium	500k-5 M	None	1-5 Hrs	General PII for multiple people or senstive PII for up to 5	Moderate reputational damage	Fines $200k-2 M, investigation not impacting business	$5 M
2	Low	50k-500k	None	Up to 1 Hr	None	Minor	Fines <$10k	$500k
1	Very Low	<50k	None	None	None	None	None	$5k

15.3 Business Impact Analysis

Business Impact Analysis (BIA) - This is the process of assessing what losses might occur for a range of threat scenarios.

Where BIA identifies risks, the business continuity plan (BCP) identifies controls and processes that enable an organization to maintain critical workflows in the face of an incident.

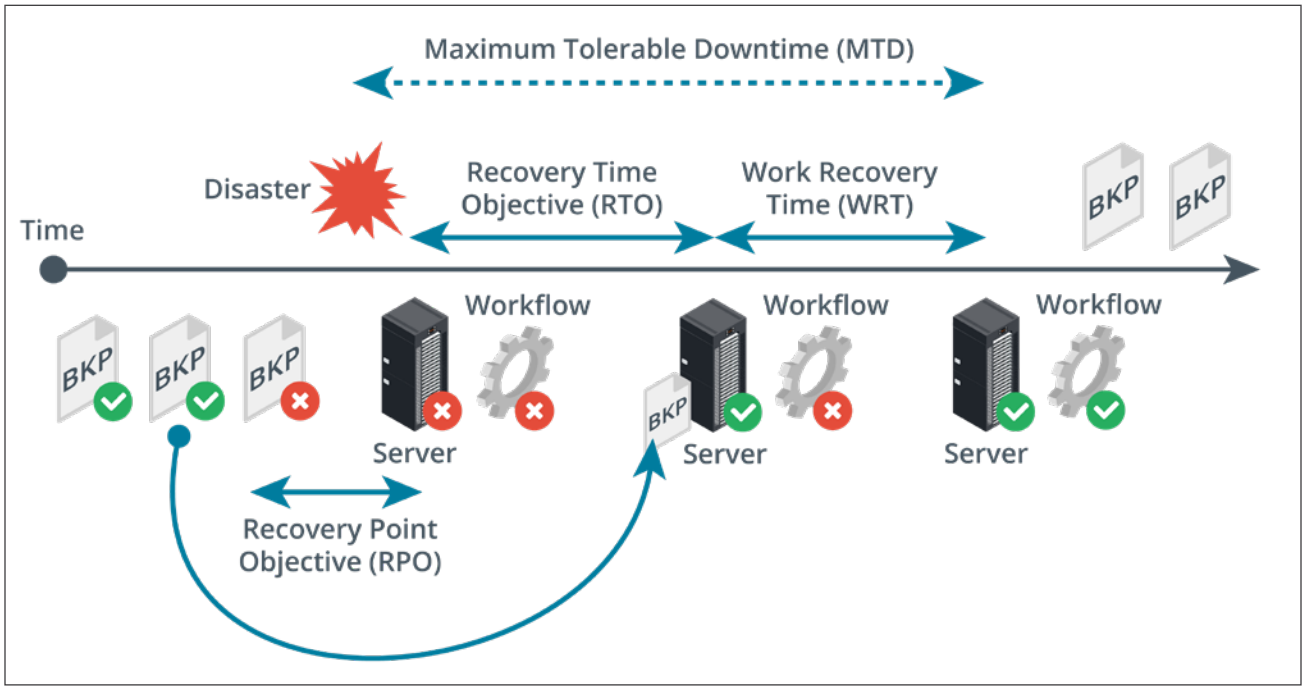
Mission Essential Function (MEF) - This is one that cannot be deferred. the business must be able to perform the function as close to continually as possible.

Maximum Tolerable Downtime (MTD) - The maximum amount of time a business can be down before it can no longer recover in a reasonable time or manner.

Recovery Time Objective (RTO) - The targeted amount of time to recover business operations after a disaster.

Work Recovery Time (WRT) - Following systems recovery, there may be additional work to reintegrate different systems, test overall functionality and brief system users on any changes.

Recovery Point Objective (RPO) - Refers to the maximum amount of data that can be lost after recovery from a disaster before the loss exceeds what is tolerable to an organization.



Identification of critical systems - Asset types include:

- People
- Tangible assets
- Intangible assets (ideas, reputation, brand)
- Procedures (supply chains, critical procedures)

Single points of failure - A spof is an asset that causes the entire workflow to collapse if it is damaged or unavailable. Can be mitigated by provisioning redundant components.

Mean time to failure (mttf) and **mean time between failures (mtbf)** represent the expected lifetime of a product. Mttf should be used for non-repairable assets for example, a hard drive can be described with an mttf while a server with mtbf.

- Calculation for mtbf is the total time divided by the number of failures. For example 10 devices that run for 50 hours and two of them fail, the mtbf is 250.
- Calculation for mttf for the same test is the total time divided by number of devices so 50 hours/failure.

Mean time to repair (mttr) is a measure of the time taken to correct a fault so that the system is restored to full operation. This metric is important for determining the overall rto.

Disasters

- **Internal Vs External -** Internal Could Be System Faults Or Malicious/Accidental Act By An Employee
- **Person-Made -** War, Terrorism, Pollution
- **Environmental -** Natural Disaster

A Site Risk Assessment Should Be Conducted To Identify Risks From These Factors.

Disaster Recovery Plans

- Identify Scenarios For Natural And Non-Natural Disasters And Options For Protecting Systems
- Identify Tasks, Resources And Responsibilities For Responding To A Disaster
- Train Staff In The Disaster Planning Procedures And How To React Well To Change.

Functional Recovery Plans

- Walkthroughs, Workshops And Seminars
- **Tabletop Exercises -** Staff “Ghost” The Same Procedures As They Would In A Disaster Without Actually Creating Disaster Conditions.
- **Functional Exercises -** Action Based Sessions Where Employees Can Validate The Drp By Performing Scenario-Based Activities In A Simulated Environment
- **Full-Scale Exercises -** Action Based Sessions That Reflect Real Situations. Held On Site And Uses Real Equipment And Real Personnel.

15.4 Third-Party Risk Management & Security Agreements

A root of trust is only trustworthy if the vendor has implemented it properly. Anyone with time and resources to modify the computer's firmware could create some sort of backdoor access.

For a tpm to be trustworthy, the supply chain of chip manufacturers, firmware authors and the administrative staff responsible for providing the computing device to the user must all be trustworthy.

When assessing suppliers for risk, it is helpful to distinguish two types of relationship

- **Vendor -** This means a supplier of commodity goods and services possibly with some level of customization and direct support.
- **Business partner -** This implies a closer relationship where two companies share quite closely aligned business goals.

End of life systems - When a manufacturer discontinues the sales of a product, it enters an **end of life (eol)** phase in which support and availability of spares and updates become more limited.

An end of service life (eosl) system is one that is no longer supported by its developer or vendor.

Windows versions are given five years of mainstream support and five years of extended support (during which only security updates are provided).

Organizational security agreements - It is important to remember that although one can outsource virtually any service to a third party, one cannot outsource legal accountability for these services.

Issues of security risk awareness, shared duties and contractual responsibilities can be set out in a formal legal agreement.

Memorandum of understanding (mou) - A preliminary agreement to express an intent to work together. They are usually intended to be relatively informal and not contract binding.

Business partnership agreement (bpa) - The most common model of this in it are the agreements between large companies and their resellers and solution providers.

Nondisclosure agreement (NDA) - Used between companies and employees/contractors/ other companies as a legal basis for protecting information assets.

Service level agreement (SLA) - A contractual agreement describing the terms under which a service is provided.

Measurement systems analysis (MSA) - A means of evaluating the data collection and statistical methods used by a quality management process to ensure they are robust.

15.5 Audit & Assurance

Information security assessment - This is the process of determining how effectively the entity being evaluated meets the specific security requirements.

- **Examination -** is the process of interviewing, reviewing, inspecting, studying and observing to facilitate understanding, comparing standards or to obtain evidence (audit)
- **Testing -** is the process of exercising objects under specified conditions to compare actual and expected behaviors (pen testing)

Assurance -This is the measure of confidence that intended controls, plans and processes are effective in their application.

The objective of an audit is to provide independent assurance based on evidence.

Audit plan - This is a high-level description of audit work to be performed in a specific time frame.

The plan may include objectives, resource requirements and reporting expectations. The final audience for the audit results is either an executive or board audit committee.

Audit focus

- **Compliance -** Meeting laws, regulations and industry standards.
- **Security & privacy -** Attaining required levels of cia and privacy
- **Internal controls -** Evaluation of the design of the controls and assessment of the operational effectiveness and efficiency of the controls
- **Alignment -** Assure alignment with organizational and control objectives.

Sampling - This is used to infer characteristics about a population based upon the characteristics of a sample of that population.

Evidence sampling is applying a procedure to less than 100% of the population.

Audit examination opinions

- **Unqualified -** Rendered when the auditor does not have any significant reservations (clean report)
- **Qualified -** Rendered when there are minor deviations or scope limitations.
- **Adverse -** Rendered when the target is not in conformance with the control objectives or when the evidence is misleading or misstated.
- **Disclaimer -** This means the auditor was not able to render an opinion due to certain/ named circumstances

Audit framework - This is a structured and systematic approach used by auditors to plan, execute and report on an audit engagement. They are typically developed by auditing standards-setting bodies.

- Isaca cobit 5
- Aicpa (ssae18)

Ssae 18 soc versions

- Soc1 is a report of controls relevant to user entities financial statements
- Soc2 is based upon trust services principles (tsp) reports on controls intended to mitigate risk related to security, cia and privacy
- Soc 3 is similar to soc2 but does not detail testing performed and is designed for public distribution.

15.6 PenTest Attack Life Cycle

- **Reconnaissance -** Is typically followed by an initial exploitation phase where a software tool is used to gain some sort of access to the target's network.
- **Persistence -** this is the tester's ability to reconnect to the compromised host and use it as a remote access tool (rat) or backdoor.
- **Privilege escalation -** The tester attempts to map out the internal network and discover the services running on it.
- **Lateral movement -** Gaining control over other hosts and usually involves executing the attack or scripting tools such as powershell.
- **Pivoting -** If a pen tester achieves a foothold on a perimeter server, a pivot allows them to bypass a network boundary and compromise servers on an inside network.
- **Actions on objectives -** For a threat actor, this means stealing data while for a tester it would be a matter of the scope definition.
- **Cleanup -** For an attacker, this means removing evidence of the attack while for a pen tester, this means removing any backdoors or tools and ensuring the system is not less secure than its pre-engagement state.

SECTION 16 -

SUMMARIZE DATA PROTECTION AND COMPLIANCE CONCEPTS

16.1 Privacy & Sensitive Data Concepts

The value of an information asset can be determined by how much damage its compromise would cause the company.

It is important to consider how sensitive data must be secured not just at rest but also in transit.

Information life cycle management

- Creation/collection
- Distribution/use
- Retention
- Disposal

Data roles & responsibilities - A data governance policy describes the security controls that will be applied to protect data at each stage of its life cycle.

Data owner - A senior executive role with ultimate responsibility for maintaining the cia of the information asset. The owner also typically chooses a steward and custodian and directs their actions and sets the budget and resource allocation for controls.

Data steward - Primarily responsible for data quality. Ensuring data is labeled and identified with appropriate metadata and that it is stored in a secure format

Data custodian - This role handles managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption and backup measures.

Data privacy officer (dpo) - This role is responsible for oversight of any personally identifiable information (pii) assets managed by the company.

In the context of legislation and regulations protecting personal privacy, the following two institutional roles are important

Data controller - The entity responsible for determining why and how data is stored, collected and used for ensuring that these purposes and means are lawful. The controller has ultimate responsibility for privacy breaches and is not permitted to transfer that responsibility.

Data processor - An entity engaged by the data controller to assist with technical collection, storage or analysis tasks. A data processor follows the instructions of a data controller with regard to collection or processing.

Data classifications - Data can be classified based on the degree of confidentiality required.

- **Public (unclassified) -** no restrictions and can be viewed by the public. Poses no real risk to the company.
- **Confidential (secret) -** Highly sensitive information to be viewed only by authorized people and possibly by trusted parties under an nda.
- **Critical (top secret) -** Extremely valuable information and viewing is severely restricted.

Data can also be classified based on the kind of information asset.

- **Proprietary/intellectual property (ip) -** Information created and owned by the company typically about the products they make.
- **Private/personal data -** Information that relates to an individual identity.
- **Sensitive -** Refers to company data that could cause serious harm or embarrassment if it is leaked to the public. Sensitive personal data includes political opinions, sexual orientation, health records , tax records etc.

Data types

Personally identifiable information (pii) - This is data that can be used to identify, contact or locate an individual such as a social security number.

An ip address can also be used to locate an individual and could be considered to be a type of pii.

Customer data -This can be institutional information but also personal information about the customer's employees such as sales and technical support contacts.

Financial information -This refers to data held about bank and investment accounts plus tax returns and even credit/debit cards. The payment card industry data security standard (pci dss) defines the safe handling and storage of this information.

Government data - Government agencies have complex data collection and processing requirements. The data may sometimes be shared with companies for analysis under very strict agreements to preserve security and privacy.

Data retention -This refers to backing up and archiving information assets in order to comply with business policies and applicable laws and regulations.

16.2 Data Sovereignty, Privacy Breaches & Data Sharing

Data sovereignty & geographical considerations - Some states and nations may respect data more or less than others and likewise some nations may disapprove of the nature and content of certain data.

Data sovereignty refers to a jurisdiction preventing or restricting processing and storage from taking place on systems that do not physically reside within that jurisdiction. For example gdpr protections are extended to any eu citizen while they are within the eu borders.

Geographic access requirements fall into two different scenarios

- Storage locations might have to be carefully selected to mitigate data sovereignty issues. Most cloud providers allow choice of data centers for processing and storage, ensuring that information is not illegally transferred from a particular privacy jurisdiction without consent.
- Employees needing access from multiple geographic locations. Cloud-based file and database services can apply constraint-based access controls to validate the user's geographic location before authorizing access.

A data breach occurs when information is read, modified or deleted without authorization.

Notification & escalation - Responses to a data breach must be configured so the appropriate personnel are notified immediately of the breach.

The first responders might be able to handle the incident if its a minor issue however in more serious cases, the case may need to be escalated to a more senior manager.

In certain cases, a timescale might also be applied. For example with gdpr, all affected individuals must be informed of the breach within 72 hours after the breach occurred.

Data sharing & privacy terms of agreement

- **Service level agreement (sla) -** A contractual agreement setting out the detailed terms under which a service is provided.
- **Interconnection security agreement (isa) -** ISAS set out a security risk awareness process and commits the agency and supplier to implementing security controls.
- **Nondisclosure agreement (nda) -** This is a legal basis for protecting information assets.

- **Data sharing and use agreement -** Personal data can only be collected for a specific purpose but data sets can be subject to deidentification to remove personal data. However there are risks of re identification if combined with other data sources. A data sharing and use agreement is a legal means of preventing this risk. It can specify terms for the way a data set can be analyzed and proscribe the use of re identification techniques.

16.3 Privacy And Data Controls

Data can be described as being in one of three states:

- **Data at rest -** Data is in some sort of persistent storage media. This data can be encrypted and acls can also be applied to it
- **Data in transit -** This is the state when data is transmitted over a network. In this state it can be protected by a transport encryption protocol such as tls or ipsec.
- **Data in use/processing -** This is the state when data is present in volatile memory such as the ram cache. Trusted execution environment (tee) mechanisms e.G intel software guard extensions are able to encrypt the data as it exists in memory.

Data protection against exfiltration

- All sensitive data is encrypted at rest
- Create and maintain offsite backups of data
- Ensure that systems storing or transmitting sensitive data are implementing access controls.
- Restrict the types of network channels that attackers can use to transfer data from the network to the outside.
- Train users about document confidentiality and the use of encryption to store and transmit data securely.

Data exfiltration - Data exfiltration can take place via a wide variety of mechanisms:

- Copying the data to removable media such as usb drive or smartphone
- Using a network protocol such as ftp, http or email
- Communicating it orally over a phone or even with the use of text messaging.

Data loss prevention

Dlp products automate the discovery and classification of data types and enforce rules so that data is not viewed or transferred without proper authorization.

- **Policy server -** to configure classification, confidentiality and privacy rules and policies, log incidents and compile reports
- **Endpoint agents -** to enforce policy on client computers even when they are not connected to the network
- **Network agents -** to scan communications at network borders and interface with web and messaging servers to enforce policy.

Remediation is the action the dlp software takes when it detects a policy violation.

- Alert only
- **Block -** The user is prevented from copying the original file but retains access to it. User may not alerted to the policy violation but it will be logged as an incident by the management engine.
- **Quarantine** - Access to the original file is denied to the user.
- **Tombstone -** The original file is quarantined and replaced with one describing the policy violation and how the user can release it again.

Privacy enhancing technologies - data minimization is the principle that data should only be processed and stored if that is necessary to perform the purpose for which it is collected.

Data minimization affects the data retention policy and its necessary to track how long a data point has been stored for and whether continued retention is necessary for a legitimate processing function.

Pseudo-anonymization modifies identifying information so that reidentification depends on an alternate data source which must be kept separate. With access to the alternated data, pseudo-anonymization methods are reversible.

Database identification methods

Data masking - Can mean that all or part of the contents of a field are redacted by substituting all character strings with “x”.

Tokenization - Means that all or part of data in a field is replaced with a randomly generated token. The token is stored with the original value on a token server or vault separate to the production database. It’s often used as a substitute for encryption.

Aggregation/binding - Another identification technique is to generalize the data such as substituting a specific age with a broader age band.

Hashing & salting - A cryptographic hash produces a fixed-length string from arbitrary-length plaintext data using an algorithm such as sha. If the function is secure, it should not be possible to match the hash back to a plaintext. A salt is an additional value stored with the hashed data field. The purpose of salt is to frustrate attempts to crack the hashes.

16.4 Privacy Principles

Privacy - This is the right of an individual to control the use of their personal information.

Data minimization approach limits data collection to only what is required to fulfill a specific purpose.

Privacy Statement - This describes how an organization collects, uses, shares and protects personal information collected from individuals.

Right to be Forgotten - This pertains to an individual’s right to have their personal information removed or deleted from online platforms, search engine results or other publicly accessible sources.

It is not an absolute right and needs to be balanced against other rights such as freedom of expression, public interest or legal obligations.

Privacy Enhancing Technologies

- **Data Masking -** A technique used to protect sensitive data by replacing it with fictional or deidentified data
- **Tokenization -** A technique used to desensitize data by replacing the original data with an unrelated value of the same length and format.
- **Anonymization -** Is the process in which individually identifiable data is altered in a way it can no longer be traced back to the original owner
- **Pseudo-Anonymization -** Is a method to substitute identifiable data with a reversible consistent value

Privacy Management Components

- **Privacy Program -** Privacy statement, tools for data mapping, executive sponsorship and privacy impact assessment
- **Operations -** Cookie compliance, privacy enhancing technologies, reporting and assessment and consent mechanisms
- **Incident and Breach Response -** Incident prevention, detection, management, notification triggers and reporting obligations.

16.5 Compliance Monitoring

Compliance - This means acting in accordance with applicable rules, laws, policies and obligations.

Organizations are responsible for complying with all local, state, federal and union laws and regulations, international treaties as well as contractual obligations.

Jurisdiction - This is the power or right of a legal or political body to exercise their authority over a person, subject or territory.

Consequences of Non-Compliance

- Fines & Sanctions
- Loss of License
- Reputational Damage
- Contractual Impact
- Resource Utilization

Compliance Monitoring - This is the active process of evaluating activities and behaviors to verify compliance and identify any deviations or non-compliant actions.

Monitoring activities include:

- Manual Inspections
- Audits
- Data Analysis
- Automated Systems
- Specialized Tools

Automated Compliance Monitoring - This utilizes automated tools to monitor and assess compliance.

Automated systems can analyze large volumes of data in real time to identify compliance breaches and also generate alerts when specific conditions or thresholds are met.

16.6 Education, Training & Awareness

Security	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Object	Understanding	Skill	Behavior
Method	Discussion, Seminar, Reading	Lecture, case study, hands-on	Interactive vedio, posters, games
Measure	Essay	Problem solving	True/false,multiple choice
Impact	Long-term	Intermediate	Shorts-terms

16.7 Personnel Policies

- Acceptable use policy (aup)
- Code of conduct and social media analysis
- Use of personally owned devices in the workplace
- Clean desk policy

User and role-based training - Appropriate security awareness training needs to be delivered to employees at all levels including end users, technical staff and executives.

- Overview of the organization's security policies
- Data handling
- Password & account management
- Awareness of social engineering and phishing

Diversity of training techniques - Using a diversity of training techniques helps to improve engagement and retention.

- Phishing campaigns
- Capture the flag - Usually used in ethical hacker training programs and gamified competitions.
- Computer-based training and gamification