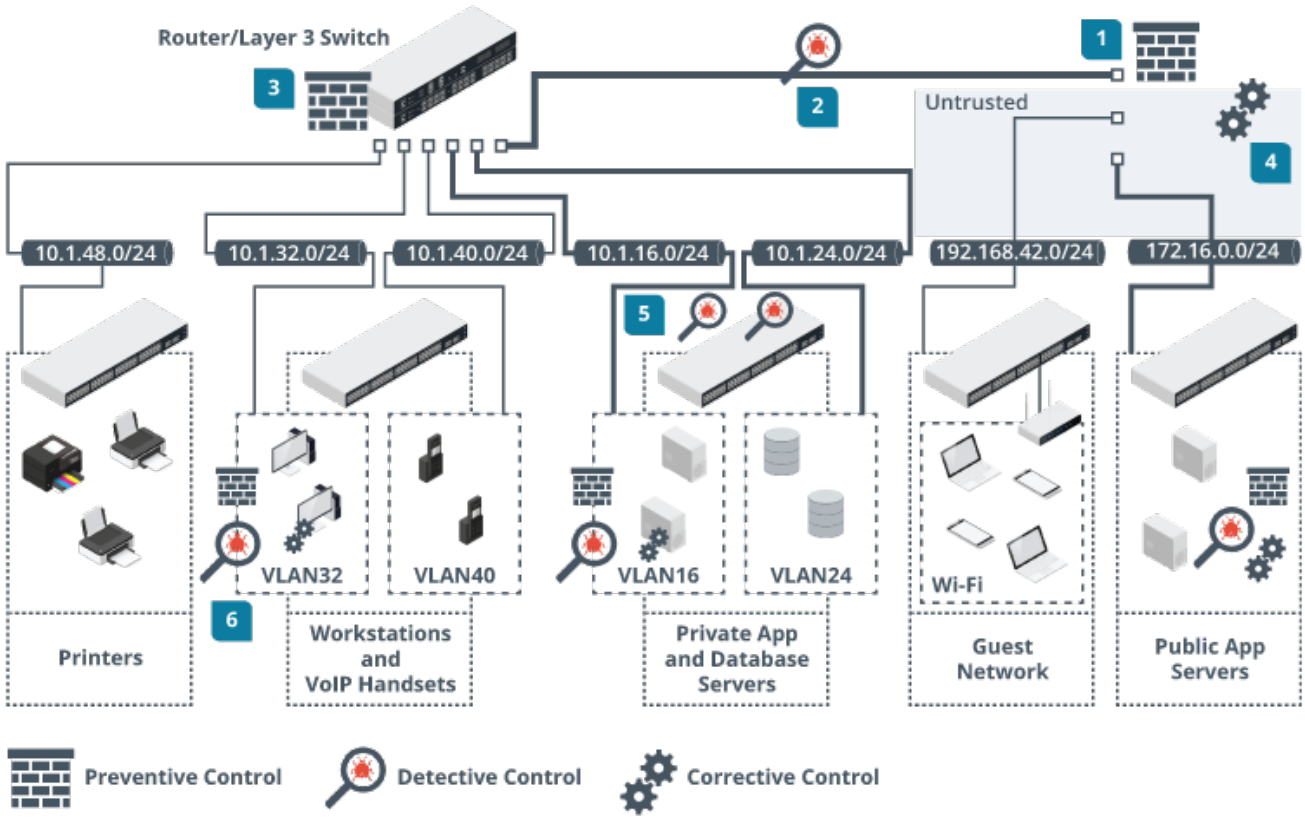
5.3 Device Placement & Attributes

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.

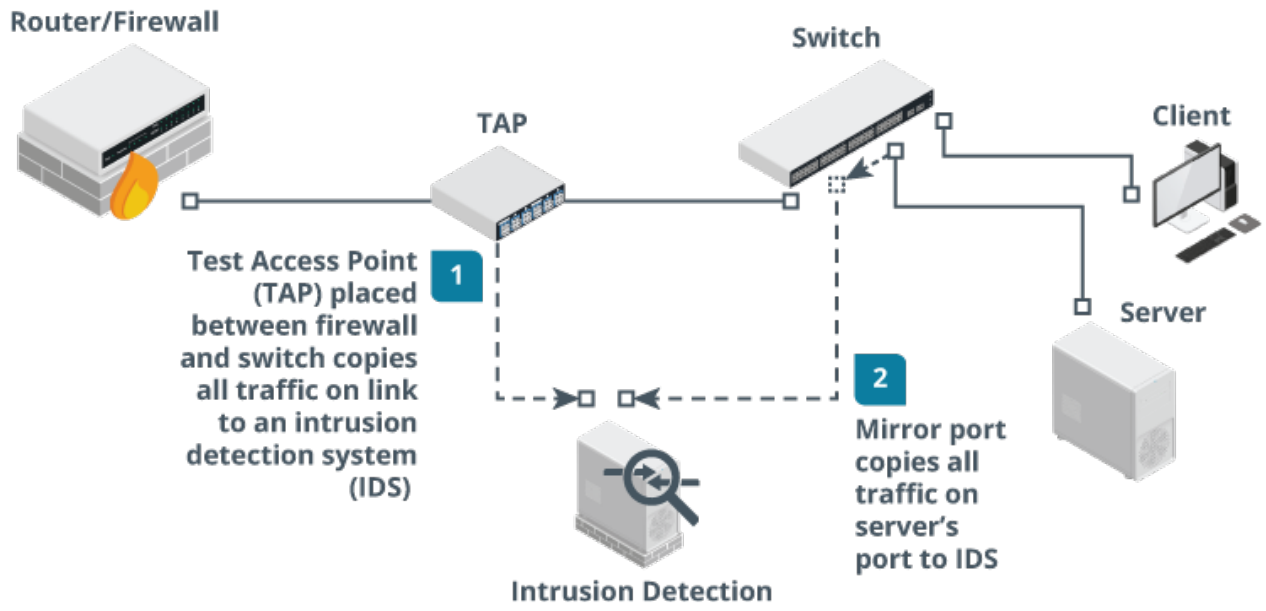
An **active security control** that performs scanning must be configured with credentials and access permissions and exchange data with target hosts. An active control that performs filtering requires hosts to be explicitly configured to use the control. This might mean installing agent software on the 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

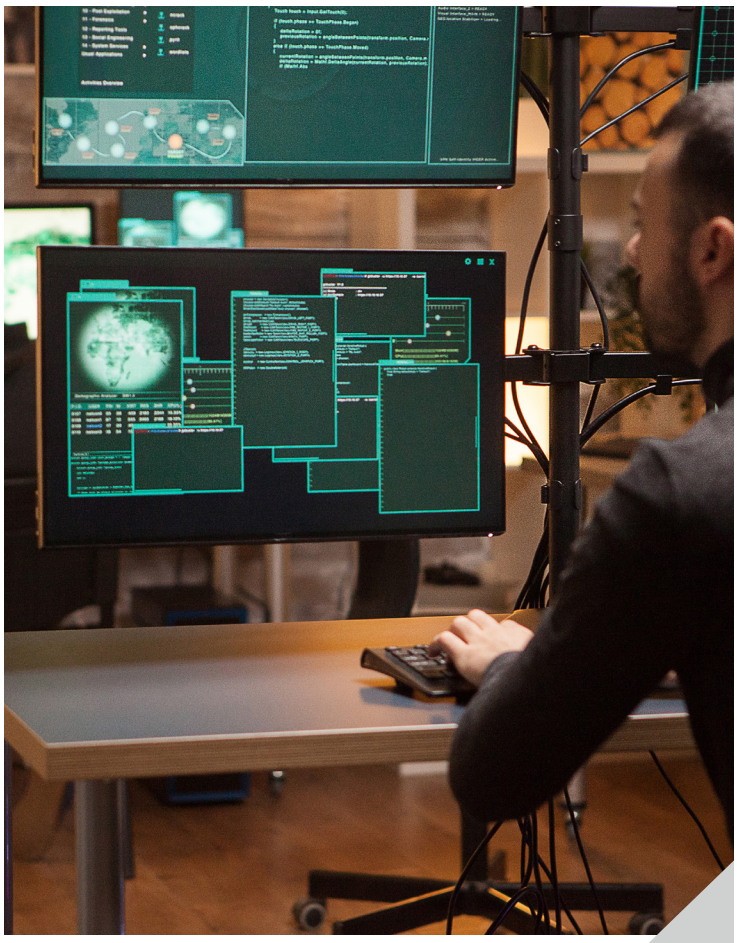
Man-In-The-Middle & Layer 2 Attacks - Most Attacks At Layer 1 And 2 Of The Osi Model Are Typically Focused On Information Gathering Through Network Mapping And Eavesdropping.

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.

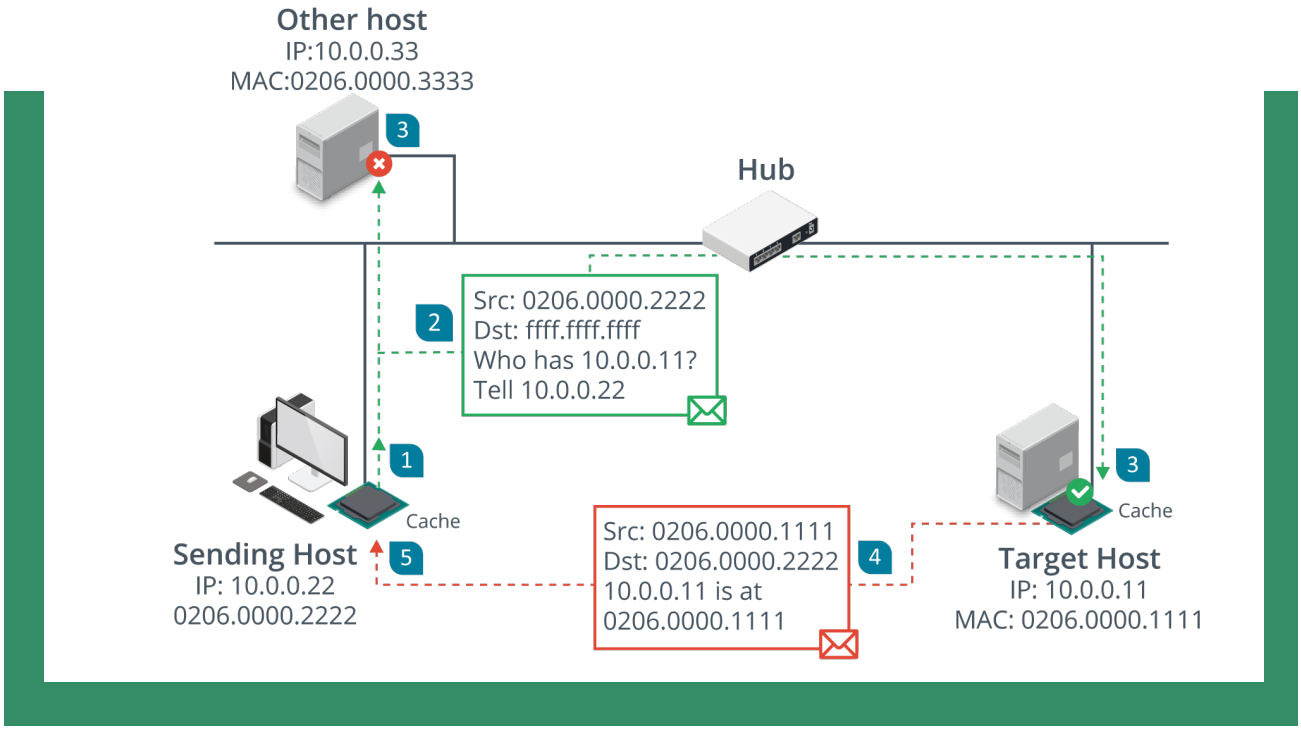
5.5 Routing & Switching Protocols

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 is 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

Open VPN - 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.

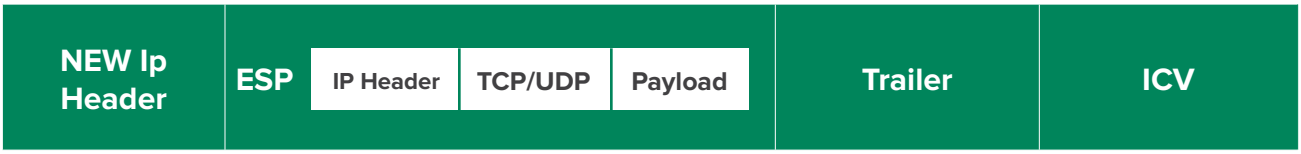
Encapsulation Security Payload (ESP) - this provides confidentiality and/or authentication and integrity. it can be used to encrypt the packet rather than simply calculating an HMAC.

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 DNS 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.

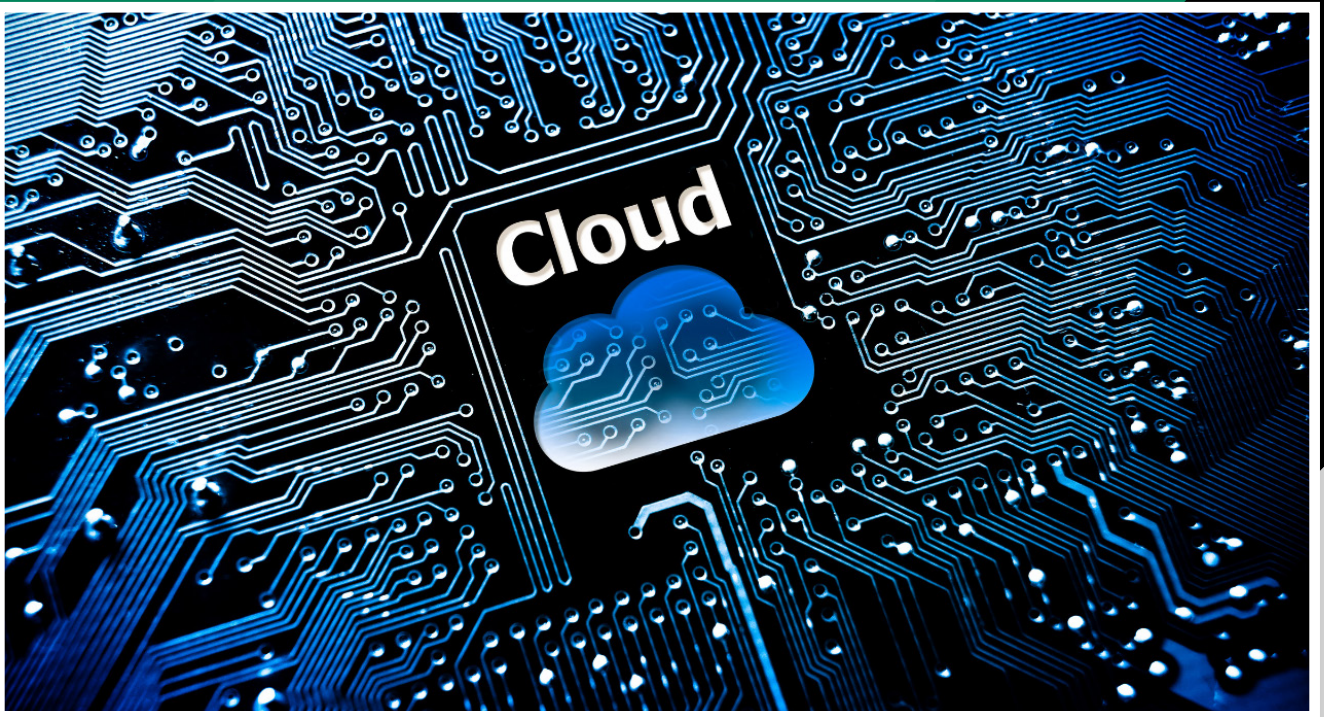
Micro-services - micro service-based development shares many similarities with agile software project management and the processes of continuous delivery and deployment.

The main difference from SOA is that while SOA allows a service to be built from other services, each micro-service 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, micro-services integration and cloud services/virtualization, integration generally is very often implemented using orchestration tools.

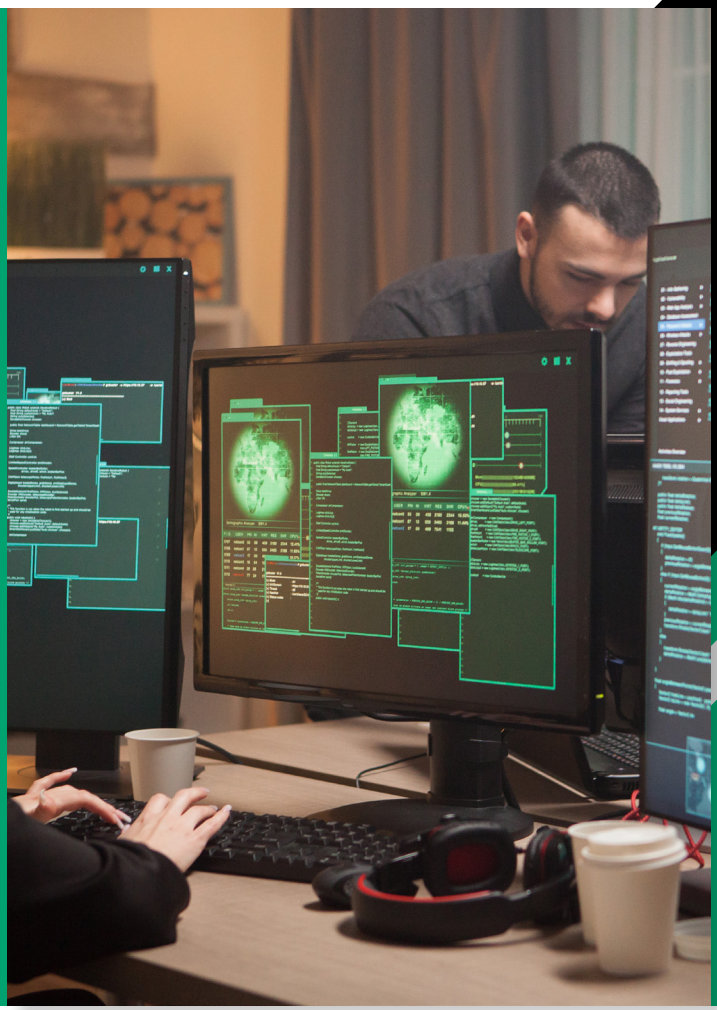
Automation focuses on making a single discrete task easily repeatable while orchestration performs a sequence of automated tasks.

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

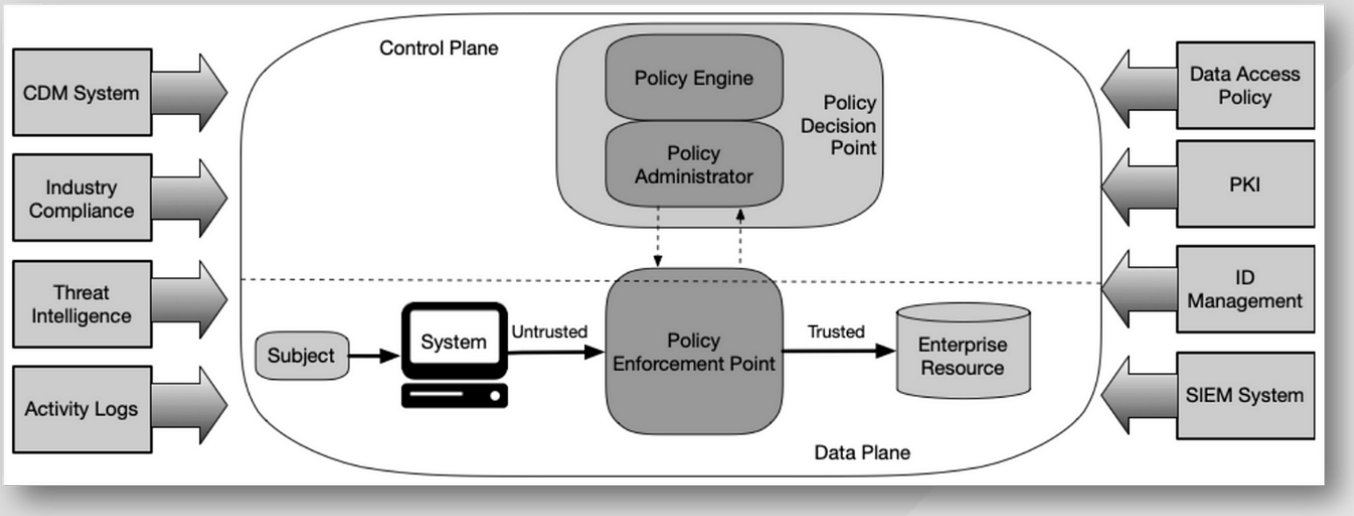
- **No Implicit Zone Trust -** Assets should always act as though an attacker was present in the enterprise network
- Devices on the network cannot be owned or configured by users
- Assume all network connections are insecure

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 micro-controller 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

System On Chip - this is a system where all processors, controllers and devices are provided on a single processor die or chip. this is often very power efficient and is commonly used with embedded systems.

RaspberryPI 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.

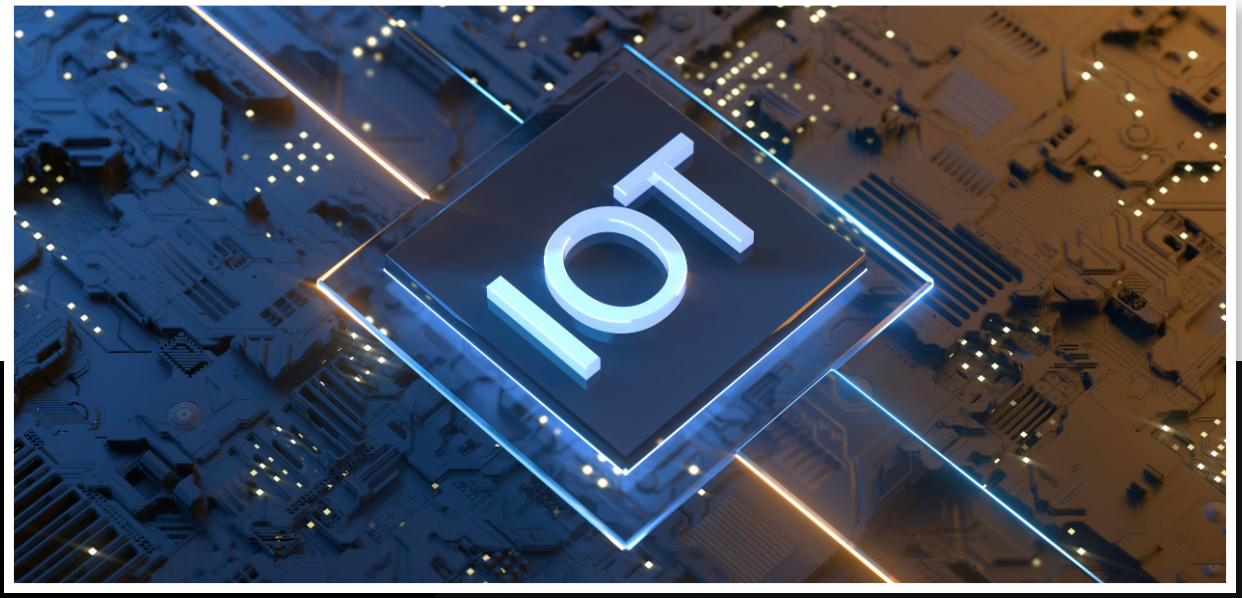
Operational Technology (OT) Networks - these are cabled networks for industrial applications and typically use either serial data protocols or industrial Ethernet. Industrial ethernet is optimized for real-time and deterministic transfers.

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 (ICs) 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:

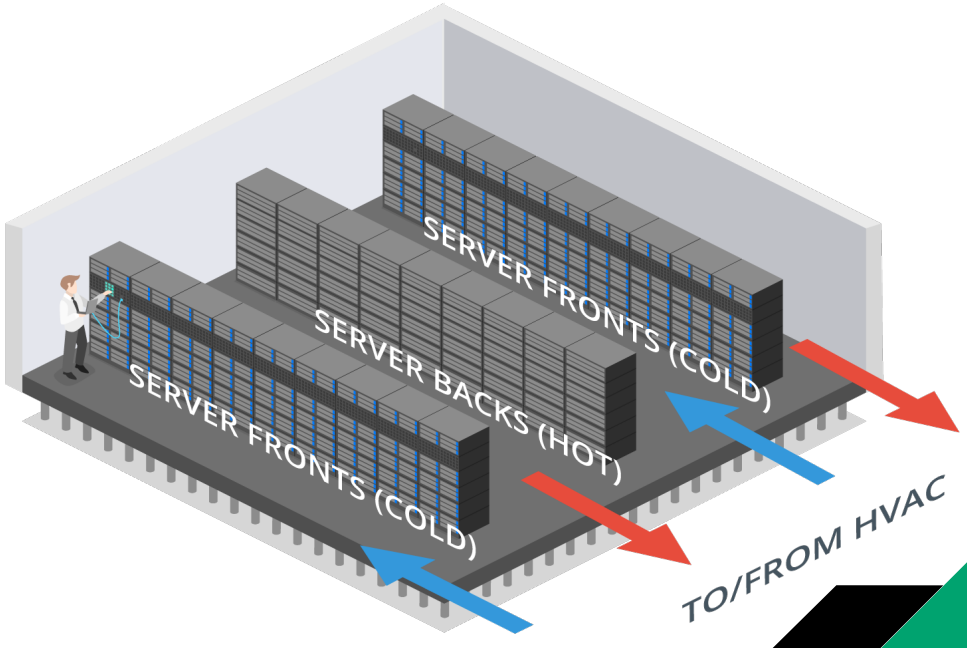
- An attacker could eavesdrop using a tap
- An attacker could cut the cable (dos)

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.

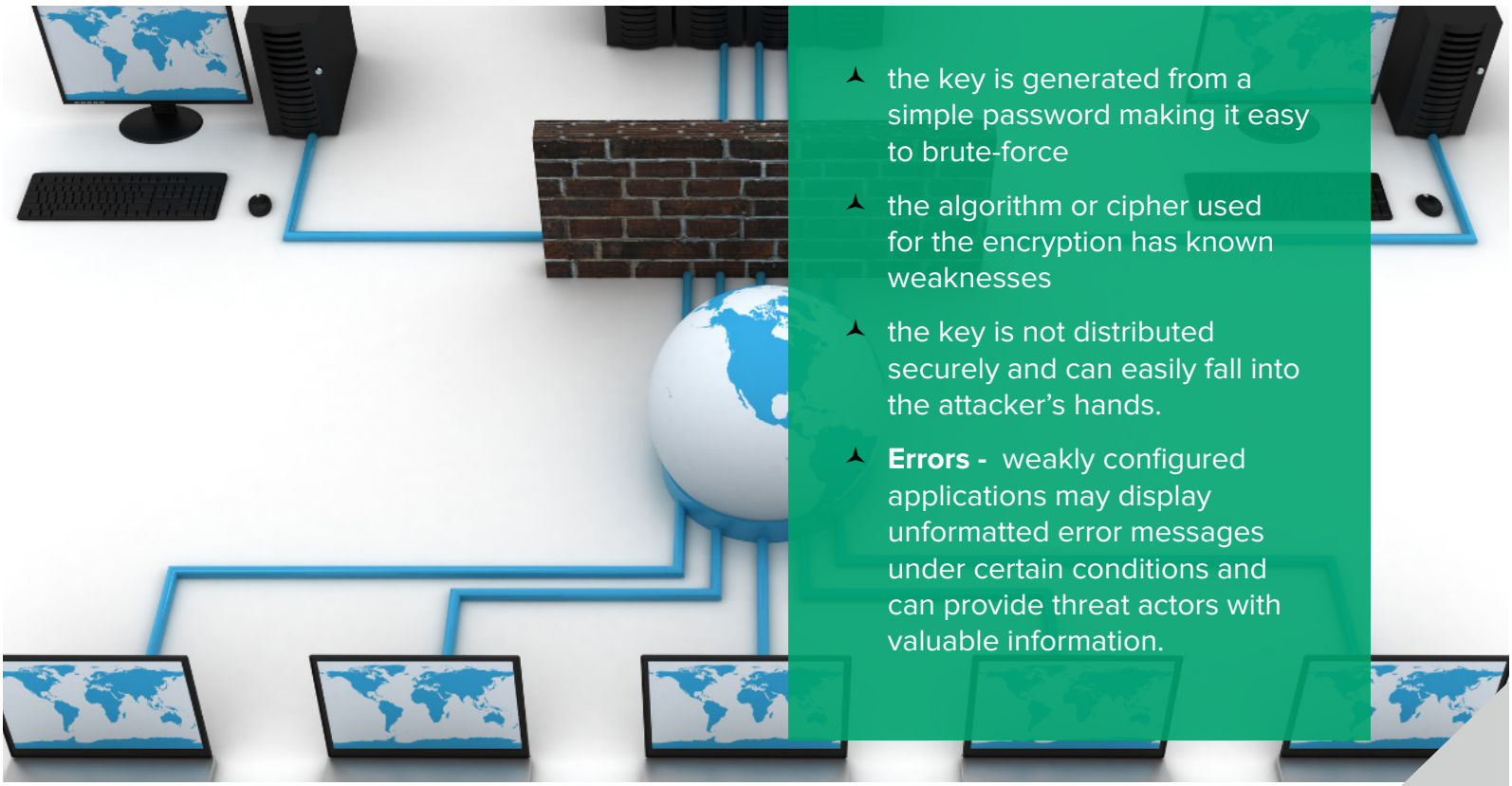
The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

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.

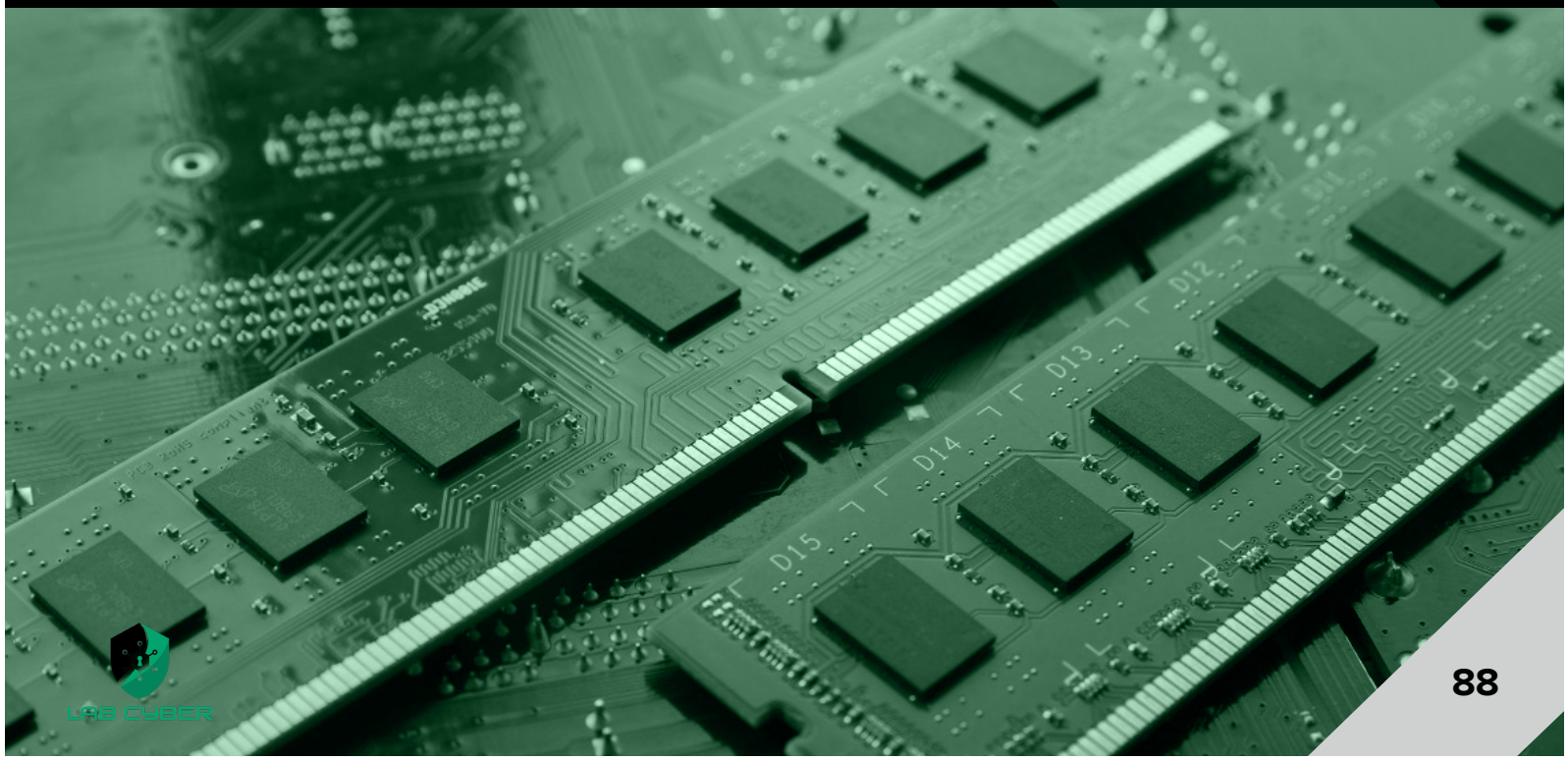
A **race condition** is a way of engineering a null pointer dereference exception.

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