SECURITY+ EXAM CRAM

THE COMPLETE COURSE

2024 EDITION

DOMAIN 4

Coverage of every topic in the official exam syllabus!

Series playlist in video description

with **Pete Zerger** vCISO, CISSP, MVP

4.0 SECURITY OPERATIONS

4.1 Given a scenario, apply common security techniques to computing resources

- **Secure baselines**
  - Establish
  - Deploy
  - Maintain
- **Hardening targets**
  - Mobile devices
  - Workstations
  - Switches
  - Routers
  - Cloud infrastructure
  - Servers
  - ICS/SCADA
  - Embedded systems
  - RTOS
  - IoT devices
- **Wireless devices**
  - Installation considerations
    - Site surveys
    - Heat maps
- **Mobile solutions**
  - Mobile device management (MDM)
  - Deployment models
    - Bring your own device (BYOD)
    - Corporate-owned, personally enabled (COPE)
    - Choose your own device (CYOD)
  - Connection methods
    - Cellular
    - Wi-Fi
    - Bluetooth
- **Wireless security settings**
  - Wi-Fi Protected Access 3 (WPA3)
  - AAA/Remote Authentication Dial-In User Service (RADIUS)
  - Cryptographic protocols
  - Authentication protocols
- **Application security**
  - Input validation
  - Secure cookies
  - Static code analysis
  - Code signing
- **Sandboxing**
- **Monitoring**

BASELINES, BENCHMARKS, AND CONTROLS

Control

a high-level description of a feature or activity that needs to be addressed and is not specific to a technology or implementation.

Is expressed in a

Benchmark

contains security recommendations for a specific technology, such as an IaaS VM.

and implemented through a

Baseline

is the implementation of the benchmark on the individual service.

BENCHMARKS/SECURE CONFIGURATION GUIDES

Benchmarks are recommended configuration baselines and best practices for securely configuring a system.

Platform-/Vendor-Specific Guides: released with new products so that they can be set up as securely as possible, making them less vulnerable to attack.

Web Servers: the two main web servers used by commercial companies are Microsoft's **Internet Information Server (IIS)**, and the Linux-based **Apache**.

Because they are public-facing, they are prime targets for hackers.

To help reduce the risk, both Microsoft and Apache provide security guides to help security teams reduce the attack surface, making them more secure.

These guides advise updates being in place, unneeded services are disabled, and the operating system is hardened to **minimize risk of security breach.**

BENCHMARKS/SECURE CONFIGURATION GUIDES

Benchmarks are recommended configuration baselines and best practices for securely configuring a system.

Operating Systems: Most vendors, such as Microsoft, have guides that detail the best practices for installing their operating systems.

OS benchmarks are also available from CIS and others

Application Server: Vendors produce guides on how to configure application, web, email or database servers, to make them less vulnerable to attack.

Network Infrastructure Devices: Companies like Cisco produce network devices and offer benchmarks for secure configuration.

benchmarks aim to ease process of securing a component, reduce attack footprint, and minimize risk of security breach.

Configuration, Change & Asset Management

Can prevent security related incidents and outages

Configuration Management

ensures that systems are configured similarly, configurations are known and documented.

Baselining ensures that systems are deployed with a common baseline or starting point, and imaging is a common baselining method.

Change Management

the policy outlining the procedures for processing changes

helps reduce risk associated with changes, including outages or weakened security from unauthorized changes.

requires changes to be requested, approved, tested, and documented.

SECURE BASELINES

Establish → Deploy → Maintain

Establish

- Identify Assets
- Threat Modeling
- Benchmarks (vendor and industry)
- Risk Assessment
- Tailoring

Deploy

- Configuration Management Tools
- AD Group Policy
- MDM Tools
- DevOps (CI/CD and Infrastructure as Code)
- Change Management

Maintain

- Vulnerability Scans
- Patch Management
- Configuration Monitoring
- Baseline Review and Update
- Auditing

Appropriate standards, tooling, automation, and maintenance are key

What is practice of hardening?

Hardening is the practice of reducing a system's attack surface, thereby enhancing its overall security posture.

Mobile devices

Strong passwords, app management, OS updates, remote wipe, and disable unused features.

Workstations

Strong login credentials, disable unneeded services, least privilege access, anti-malware, and host firewall.

Network devices

Strong passwords, disable unused features, firmware updates, access control lists (ACLs), and segment networks.

HARDENING TARGETS

Cloud infrastructure

DevOps, CI/CD, infrastructure-as-code

Identity and access management (IAM), encryption, logging and monitoring, and secure configuration.

ICS/SCADA

Segmentation (or isolation), physical security, change management, password management, and monitoring.

Embedded & RTOS

Secure coding practices, design with limited functionality, firmware updates, code reviews, limited network access, and secure boot.

Internet of Things

Strong passwords, firmware updates, network segmentation, limiting functionality, secure communication protocols.

Server Hardening

Hardening is the configuration of a machine into a secure state through application of a configuration baseline.

Baselines can be applied to a single VM image, or to a VM template created that is then used to deploy all VMs.

A hardened VM image may be customer-defined, CSP-defined, or from a third party, often available through a cloud marketplace.

The Center for Internet Security (CIS) offers hardened VM images in CSP marketplaces

HARDENING TARGETS

IaC

Infrastructure as Code

is the management of cloud infrastructure (networks, VMs, load balancers, and connection topology) described in code

just as the same source code generates the same binary, code in the IaC model results in the same environment every time it is applied.

IaC is a key DevOps practice and is used in conjunction with **C**ontinuous **I**ntegration and **C**ontinuous **D**elivery (CI/CD). "the CI/CD pipeline"

IaC, **CI/CD**, and **DevOps** are standard elements of deployment, change, and release in the cloud. **DevSecOps** is quickly growing in popularity.

HARDENING TARGETS

Open ports and services

listening ports should be restricted to those necessary, filtered to restrict traffic, and disabled entirely if unneeded.

Block through firewalls, disable by disabling underlying service.

Registry

access should be restricted, and updates controlled through policy where possible.

always take a backup of the registry before you start making changes.

Disk encryption

drive encryption can prevent unwanted access to data in a variety of circumstances. Using FDE - Bitlocker (Windows), dm-crypt (Linux)

OS (Operating System)

OS hardening can often be implemented through security baselines

Can be applied through group policies, IaC, or other management tools.

Baselines can implement all the above

HARDENING TARGETS

Patch Management

aka "update management"

ensures that systems are kept up-to-date with current patches.

will evaluate, test, approve, and deploy patches.

system audits verify the deployment of approved patches to system

Patch both native OS and 3rd party apps

Apply out-of-band updates promptly.

Orgs without patch management will experience outages from known issues that could have been prevented

SITE SURVEY

The process of investigating the presence, strength, and reach of wireless access points deployed in an environment.

WIRELESS DEVICES

SITE SURVEY

usually involves walking around with a portable wireless device, taking note of the wireless signal strength, and mapping this on a plot or schematic of the building.

HEAT MAPS

A **heat map** in wireless network coverage is a visual representation of signal strength across an area.

Strong signal areas: These are typically colored green or blue and indicate optimal signal strength for reliable connections and fast data transfer.

Weak signal areas: These are colored yellow, orange, or red and represent areas with poor signal quality that may experience slow speeds, dropped connections, or unreliable performance.

Planning access point placement: By identifying weak signal areas, network professionals can strategically position access points to improve overall coverage and eliminate dead zones.

HEAT MAPS

Troubleshooting network issues: Heat maps can help pinpoint areas with signal interference or connectivity problems

Allows for targeted troubleshooting efforts.

Optimizing network performance: Heat maps can be used to assess the effectiveness of existing access point configurations

Also reveals opportunities for optimizing network performance for better user experience

Capacity planning: As the number of devices on a network grows, heat maps can help assess current capacity and future needs.

Enables planning for controlled, secure growth through optimal device placement

MOBILE SOLUTIONS

Intune, AirWatch, MobileIron, etc.

Common features in secure **Mobile Device Management (MDM)**

Passwords and PINs: Some mobile devices, such as smartphones, are very easy to steal and you can conceal them by putting them in a pocket.

Strong passwords and PINs with six or more characters must be used.

Also allows device to be disabled on x failed attempts

Geofencing: Geofencing uses the Global Positioning System (GPS) or RFID to define geographical boundaries.

Once the device is taken past the defined boundaries, the security team will be alerted.

For the exam: remember Geofencing prevents mobile devices from being removed from the company's premises.

MOBILE DEVICE MANAGEMENT (MDM)

Application Management: Application management uses allow lists to control which applications are allowed to be installed onto the mobile device.

Content Management: Content management stores business data in a secure area of the device in an encrypted format to protect it against attacks.

Prevents confidential or business data from being shared with external users.

Remote Wipe: When a mobile device has been lost or stolen, it can be remotely wiped.

Device will revert to its factory settings and the data will no longer be available. wipe options allow removing business data only (BYOD)

Screen Locks: Screen locks are activated once the mobile device has not been accessed for a period of time.

After it is locked, the user gets a fixed number of attempts to correctly enter the PIN before the device is disabled.

MOBILE DEVICE MANAGEMENT (MDM)

Geolocation: Geolocation uses GPS to give the actual location of a mobile device.

used for location-aware authentication, geofencing, and other related security functions

can be very useful if you lose or drop a device.

Push Notification: messages that appear on your screen, even when your system is locked.

this information is usually pushed your device without intervention from the end user and may include sensitive information.

some MDM platforms provide policy-based control whether app notifications can appear with the notifications on lock screen.

MOBILE SOLUTIONS

Unified Endpoint Management (UEM)

Provides management of the hardware, such as desktops, tablets, smartphones, and IoT devices

Monitors and enforces configuration to ensure that they are secure and compliant.

Can manage the security and applications running on the devices.

Can identify and block devices have been jailbroken (iOS) or rooted (Android).

Multi-platform support is a key characteristic

Examples include **Microsoft Intune** and **AirWatch** which manage Windows, iOS, Android, and MacOS

MOBILE SOLUTIONS

Mobile Application Management (MAM)

Allows a security team to manage application and data security, even on unmanaged devices.

Controls access to company applications and data.

Can restrict exfiltration of data from the company applications.

Useful in BYOD scenarios, enabling business data access on personal mobile devices

ENFORCEMENT AND MONITORING (MOBILE)

Third-party application stores

There is a danger of downloading apps from third-party app stores as there is no guarantee of the security of the app being installed.

This could pose a security risk, as vetting process for mobile apps in third-party stores may be less rigorous than official app stores.

Sideloading

Enables directly installing an application package in .apk format on a mobile device.

Useful for developers to run trial of custom apps, but also allows unauthorized software to be run on a mobile device.

ENFORCEMENT AND MONITORING (MOBILE)

Rooting/jailbreaking

Custom firmware downloads are used to root an Android mobile device.

Gives user a higher level of permissions on that device and removes some elements of vendor security.

Jailbreaking is the Apple's iOS equivalent of rooting on Android: it allows you to run unauthorized software and remove device security restrictions.

You can still access the Apple App Store even though jailbreaking has been carried out.

For the exam: Rooting and jailbreaking remove the vendor restrictions on a mobile device to allow unsupported software to be installed.

ENFORCEMENT AND MONITORING (MOBILE)

Custom firmware

Custom firmware downloads are used so that you can root your mobile device.

Gives the user a higher level of permissions on that device and removes some elements of vendor security.

Carrier unlocking

When a mobile device is no longer tied to the original carrier. This will allow you to use your device with any provider, and also install third-party apps.

Firmware over-the-air (OTA) updates

Firmware is software that is installed on a small, read-only memory chip on a hardware device and is used to control the hardware running on device.

Firmware OTA updates are pushed out periodically by the vendor, ensuring that the mobile device is secure.

One example is when the mobile device vendor sends a notification that there is a software update.

ENFORCEMENT AND MONITORING (MOBILE)

Short Message Service (SMS)

Text messaging and has become a common method of communication.

Can be sent between two people in a room without other people in the room knowing about their communication.

Text messages can be used to launch an attack.

Multimedia Messaging Service (MMS)

A way to send pictures as attachments, similar to sending SMS messages.

Rich Communication Services (RCS)

An enhancement to SMS and is used in Facebook and WhatsApp to send messages so that you can see the read receipts.

You can also send pictures and videos.

Image capability makes MMS and RCS paths for data theft.

ENFORCEMENT AND MONITORING (MOBILE)

External media. SD card or other external storage media may enable unauthorized transfer of corporate data

USB On-The-Go (USB OTG). allows USB devices plugged into smartphones and tablets to act as a host for other USB devices.

Attaching USB devices can pose security problems as it makes it easy to steal information.

Apple does not allow USB OTG.

Recording microphone. smartphones and tablets can record conversations with their built-in microphones.

They could be used to take notes, but they could also be used to tape conversations or record the proceedings of a confidential meeting.

GPS tagging. When you take a photograph, GPS tagging adds the location where the photograph was taken.

Most modern smartphones do this by default.

ENFORCEMENT AND MONITORING (MOBILE)

Wi-Fi direct/ad hoc

Wi-Fi direct wireless network allows two Wi-Fi devices to connect to each other without requiring a WAP.

It is single-path and therefore cannot be used for internet sharing.

Ad-hoc wireless network is where two wireless devices can connect without a WAP, but it is multipath and can share an internet connection with someone else.

ENFORCEMENT AND MONITORING (MOBILE)

Wi-Fi direct/ad hoc

Wi-Fi direct wireless network allows two Wi-Fi devices to connect to each other without requiring a WAP.

It is single-path and therefore cannot be used for internet sharing.

Ad-hoc wireless network is where two wireless devices can connect without a WAP, but it is multipath and can share an internet connection with someone else.

Tethering

When a GPS-enabled smartphone can be attached to a laptop or mobile device to provide internet access.

If a user uses a laptop to connect to the company's network and then tethers to the internet, it may result in split tunneling.

This presents a security risk if device is compromised.

Mobile devices can often function as a wifi hotspot over USB or Bluetooth.

ENFORCEMENT AND MONITORING

Payment methods

Smartphones allow credit card details to be stored locally so that the phone can be used to make contactless payments using Near-Field Communications (NFC).

For BYOD, it needs to be carefully monitored as someone could leave the company with a company credit card and continue to use it.

MDM may prevent the payment function by disabling this tool in the mobile device management policies.

Camera use

MDM can also disable screen captures

Smartphone cameras pose a security risk to companies, as trade secrets could be stolen very easily.

Research and development departments ban the use of personal smartphones in the workplace. Prevents theft of intellectual property

MDM policies can disable cameras on company-owned smartphones

DEPLOYMENT MODELS

Bring Your Own Device (BYOD)

is where an employee is encouraged to bring in their own device so that they can use it for work.

cost effective for the company and more convenient for the user.

needs two policies to be effective, Acceptable Use Policy and On/Offboarding

Acceptable Use Policy (**AUP**): An AUP outlines what the employee can do with the device during the working day.

Onboarding Policy: Device configuration requirements to access corporate data (min OS system, not rooted/jailbroken, etc.)

Offboarding Policy: How corporate data will be wiped from the device (most MDM platforms support a selective wipe, removing only company data).

MDM solutions with MAM (mobile app management) functionality can manage corporate data on BYOD devices

DEPLOYMENT MODELS

Corporate-Owned

fully owned and managed by the company, enabling full IT control over MAM and MDM options.

Choose Your Own Device (CYOD)

new employee chooses from a list of approved devices.

employees can purchase devices on the list and bring them to work.

employee gets to choose device, but fewer types for IT to manage.

Corporate-Owned Personally-Enabled (COPE)

when the company purchases the device, such as a tablet, phone, or laptop, and allows the employee to use it for personal use.

often better solution for the company than BYOD from a management perspective, because IT can limit what applications run on the devices.

also frees the company to perform full device wipe if lost or stolen.

CONNECTION METHODS

5G

5th Generation Cellular

Faster speeds and lower latency than 3G/4G

Unlike 4G, 5G doesn't identify each user through their SIM card. Can assign identities to each device.

Some air interface threats, such as session hijacking, are dealt with in 5G.

Standalone (SA) version of 5G will be more secure than the non-standalone (NSA) version

NSA anchors the control signaling of 5G networks to the 4G Core

CONNECTION METHODS

5G

5th Generation Cellular

Diameter protocol, which provides authentication, authorization, and accounting (AAA), will be a target. (though 5G uses HTTP/2 for comm)

Because 5G has to work alongside older tech (3G/4G), old vulnerabilities may be targeted.

Because scale of IoT endpoint counts on 5G is exponentially greater, **DDoS** is a concern.

Some carriers originally launched an NSA version of 5G, which continues to rely on availability of the 4G core.

CONNECTION METHODS

SIM

Subscriber
Identity
Module cards

small computer chips that contain the information about mobile subscription

allows user to connect to telecommunication provider to make calls, send text messages, or use the Internet.

Used as a second factor in authentication...

And one of the auth factors most prone to attack

WIRELESS TECHNOLOGIES

Version	Speed	Frequency
★ 802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	200+ Mbps	2.4 GHz
802.11ac	1 Gbps	5 GHz

802.11 standard also defines WEP

CONNECTION METHODS

Bluetooth

(IEEE 802.15)

Bluetooth, or IEEE 802.15, personal area networks (PANs) are another area of wireless security concern.

Connects headsets for cell phones, mice, keyboards, GPS, and other devices

Connections are set up using pairing, where primary device scans the 2.4 GHz radio frequencies for available devices

Pairing uses a 4-digit code (often 0000) to reduce accidental pairings but is not actually secure.

MOBILE AND WIRELESS ATTACKS

To prevent, use long pin, 2FA, and disable discovery mode

Bluejacking
annoyance

pranksters push unsolicited messages to engage or annoy other nearby Bluetooth through a loophole in Bluetooth messaging options

Bluesnarfing
data theft

data theft using Bluetooth. Vulnerable devices are those using bluetooth in public places with device in discoverable mode.

Bluebugging
eavesdropping or hacking

developed a year after bluejacking, creates a backdoor attack before returning control of the phone to its owner.

MOBILE CONNECTION METHODS & RECEIVERS

RFID
RADIO FREQUENCY IDENTIFICATION

uses radio frequency to identify electromagnetic fields in a tag to track assets.

commonly used in shops as the tags are attached to high-value assets to prevent theft.

Common in access badge systems and retail anti-theft use cases

NFC
NEAR FIELD COMMUNICATION

Built on RFID, often used with payment systems.
Subject to many of the same vulnerabilities as RFID

The touch pay system at the grocery

GPS

uses satellites in the Earth's orbit to measure the distance between two points.

Used in map and find-my-phone use cases

MOBILE CONNECTION METHODS & RECEIVERS

USB
UNIVERSAL SERIAL BUS

Some mobile devices can be tethered to a USB dongle to gain access to the internet.

A flash USB device can be used to transfer data between devices

It is a data exfiltration concern, often blocked through policy

Infrared

device is purely line-of-sight and has a maximum range of about 1 meter. Can be used to print from your laptop to an infrared printer.

Not encrypted, but attack requires close physical proximity

MOBILE CONNECTION MODELS

Wireless technologies operate in one of **four major connection models**

Point-to-Point

one-to-one connection between the two devices communicating on a network, typically wireless

A directional antenna connecting two wireless networks or wireless repeater connecting WAPs

✓ **Point-to-Multipoint**

a central device (access point) communicates with multiple remote devices (clients)

802.11 networks are more commonly communicating from point-to-multipoint.

A WAP connecting to multiple wireless devices

MOBILE CONNECTION MODELS

Wireless technologies operate in one of **four major connection models**

Broadcast

data is sent from one source to all connected devices where everyone hears the same message

TV or radio, where a single station transmits signals to all receivers tuned to the same frequency

Mesh

multiple devices (nodes) communicate with each other directly, forming a self-healing network.

if one node fails, data can still find an alternative path.

City-wide Wi-Fi and some commercial solutions

MOBILE AND WIRELESS ATTACKS

Evil Twin

A malicious fake wireless access point set up to appear as a legitimate, trusted network.

Common in airports and coffee shops

Disassociation

A type of DoS attack in which the attacker breaks the wireless connection between the victim device and the access point.

Gives attacker a window to inject an evil twin

Jamming

A DoS attack that prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on.

Can be difficult to detect & often unintentional

WIRELESS SECURITY SETTINGS

CCMP

Counter-mode / CBC-MAC Protocol

Counter Mode with **C**ipher Block Chaining **M**essage Authentication Code **P**rotocol

created to replace WEP and TKIP/WPA

uses AES (Advanced Encryption Standard) with a 128-bit key

used with WPA2, which replaced WEP and WPA

WIRELESS SECURITY SETTINGS

WPA2

an **encryption scheme** that implemented the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP),

CCMP is based on the AES encryption scheme

WIRELESS SECURITY SETTINGS

SAE is a relatively new 802.11 authentication method.

SAE

Simultaneous
Authentication of
Equals

used with WPA3-Personal and replaces the WPA2-PSK Protects against brute-force attacks

uses a secure Diffie Hellman handshake, called dragonfly

uses perfect forward secrecy, so immune to offline attacks

WIRELESS SECURITY SETTINGS

WPA3

released in 2018 to address the weaknesses in WPA2.

uses a much stronger 256-bit Galois/Counter Mode Protocol (GCMP-256) for encryption

There are two versions: **WPA3-Personal** for home users, and **WPA3-Enterprise** for corporate users

WPA3 PERSONAL vs ENTERPRISE

WPA3
PERSONAL

uses Simultaneous Authentication of Equals (SAE).

SAE means users can use passwords that are easier to remember.

uses perfect forward secrecy (PFS)

WPA3
ENTERPRISE

supports 256-bit AES, whereas WPA2 only supported 128 bits 256-bit required by US gov't

uses Elliptic-Curve Diffie Hellman Ephemeral (ECDHE) for the initial handshake.

AAA PROTOCOLS

Several protocols provide centralized **authentication**, **authorization**, and **accounting** services.

Network Access Server
is a client to a RADIUS server, and the RADIUS server provides AAA services.

RADIUS
uses UDP and encrypts the password only.

TACACS+
uses TCP and encrypts the entire session.

Network access (or remote access) systems use AAA protocols.

WIRELESS AUTHENTICATION METHODS

Pre-Shared Key (WPA2-PSK)

was introduced for the home user who does not have an enterprise setup.

the home user enters the password of the wireless router to gain access to the home network.

PSK in WPA2 Replaced by SAE in WPA3

Wi-Fi Protected Setup (WPS)

Home use scenario

password is already stored and all you need to do is to press the button to get connected to the wireless network.

Password is stored locally, so could be brute-forced

Enterprise

a corporate version of WPA2 or WPA3, used in a centralized domain environment.

Often, where a RADIUS server combines with 802.1x, using certificates for authentication

WIRELESS AUTHENTICATION PROTOCOLS

IEEE 802.1x

is transparent to users because it uses certificate authentication

can be used in conjunction with a RADIUS server for enterprise networks.

RADIUS Federation

enables members of one organization to authenticate to another with their normal credentials.

trust is across multiple RADIUS servers across multiple organizations.

a federation service where network access is gained using wireless access points (WAPs).

WAP forwards the wireless device's credentials to the RADIUS server for authentication.

commonly uses 802.1X as the authentication method. which relies on EAP

WIRELESS AUTHENTICATION PROTOCOLS

LEAP
Lightweight...

a Cisco proprietary alternative to TKIP for WPA. developed to address deficiencies in TKIP before the 802.11i/WPA2 system was ratified as a standard.

PEAP
Protected...

encapsulates EAP methods within a TLS tunnel that provides authentication and potentially encryption.

EAP
extensible authentication protocol

an authentication framework. allows for new authentication technologies to be compatible with existing wireless or point-to-point connection technologies

Be familiar with EAP, PEAP, RADIUS, and 802.1x for the exam

Know the security features and improvements of WPA3 vs WPA2

CAPTIVE PORTALS

Common in airports and public spaces, wi-fi redirects users to a webpage when they connect to SSID.

User provides additional validation of identity, normally through an email address or social identity.

May include acceptable use policy and premium upgrade offer

APPLICATION SECURITY

Implement application security controls to prevent attacks.

Input Validation

ensures *buffer overflow*, *integer overflow*, and *SQL injection* attacks cannot be launched against applications and databases.

use where data is entered either using a web page or wizard.

only accept data in the correct format within a range of minimum and maximum values.

Incorrect format should be rejected, forcing user to re-enter

Secure Cookies

used by web browsers and contain information about your session.

can be stolen by attackers to carry out a session hijacking attack.

setting the secure flag in website code to ensure that cookies are only downloaded when there is a secure HTTPS session.

APPLICATION SECURITY

Implement application security controls to prevent attacks.

Hypertext Transfer Protocol (HTTP) Headers

HTTP headers are designed to transfer information between the host and the web server.

an attacker can carry out *cross-site scripting (XSS)* which is mainly delivered through injecting HTTP response headers.

can be prevented by entering the HTTP Strict Transport Security (HSTS) header:

HSTS ensures that the browser will ignore all HTTP connections

Code Signing

uses a certificate to digitally sign scripts and executables to verify their authenticity and to confirm that they are genuine.

Allow List

an allow list enable only explicitly allowed applications to run. This can be done by setting up an application whitelist.

Firewalls, IDS/IPS, and EDR systems can have an allow list

APPLICATION SECURITY

Implement application security controls to prevent attacks.

Block List/Deny List

prevents specified applications from being installed or run that are on the block list in the specified security solution.

Firewalls, IDS/IPS, and EDR systems can have a block list.

APPLICATION SECURITY

Implement application security controls to prevent attacks.

Secure Coding Practices: developer who creates software writes code in a manner that ensures that there are no bugs or flaws.

Intent is to prevent attacks such as *buffer overflow* or *integer injection*.

Static Code Analysis: analysis where the code is not executed locally but is analyzed by a static code analyzer tool.

source code is run inside the tool that reports any flaws or weaknesses.

Requires source code access

Dynamic Code Analysis: code is executed, and a technique called *fuzzing* is used to inject random input into the application.

output is reviewed to ensure appropriate handling of unexpected input.

exposes flaws in an application before it is rolled out to production.

Does not require source code access

Implement application security controls to prevent attacks.

Manual Code Review

code is reviewed line by line to ensure that the code is well-written and error free.
tends to be tedious and time-consuming.

Fuzzing

random information is input into an application to see if the application crashes or memory leaks result, or if error information is returned.

used to remedy any potential problems within application code before a new application is released. white box (open) testing scenario

can also be used to find any vulnerabilities with the application after release. This is called improper input validation. black box (closed) testing scenario

APPLICATION SECURITY

Firewalls
Web Application
aka "WAF"

protect web applications by filtering and monitoring HTTP/HTTPS traffic between a web application and the Internet.

typically protects web applications from common attacks like XSS, CSRF, and SQL injection.

Some come pre-configured with OWASP rulesets

Firewalls
Next Generation
aka "NGFW"

a deep-packet inspection firewall that moves beyond port/protocol inspection and blocking.

adds application-level inspection, intrusion prevention, and brings intelligence from outside the firewall.

Sandboxing

The application is installed in a virtual machine environment isolated from our network.

Enables patching, testing, and ensures that it is secure before putting it into a production environment.

Also facilitates investigating dangerous malware.

In Linux, this is called **chroot jail**.

It's a directory that contains a subset of the system files and libraries needed for a process to run in isolation from the rest of the system.

MONITORING

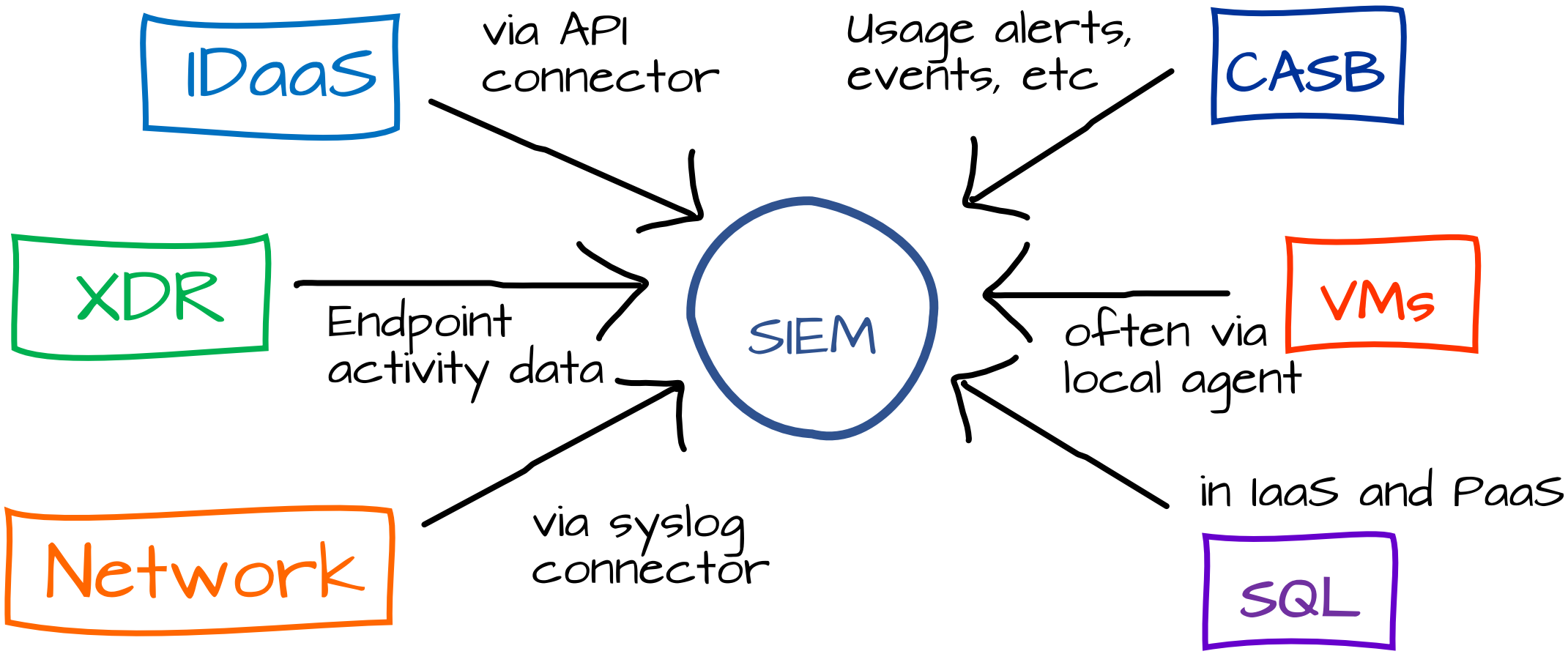
Logs are worthless if you do nothing with the log data. They are made valuable only by **review**.

That is, they are valuable only if the organization makes use of them to identify activity that is unauthorized or compromising.

SIEM (Security Information Event Monitoring) tools can help to solve some of these problems by offering these key features:

- Log centralization and aggregation
- Data integrity
- Normalization
- Automated or continuous monitoring
- Alerting
- Investigative monitoring

We will cover SIEM in depth later in Domain 4



Log Ingestion with a SIEM

EXAMPLE

4.0 SECURITY OPERATIONS

4.2 Explain the security implications of proper hardware, software, and data asset management

- **Acquisition/procurement process**
- **Assignment/accounting**
  - Ownership
  - Classification
- **Monitoring/asset tracking**
  - Inventory
  - Enumeration
- **Disposal/decommissioning**
  - Sanitization
  - Destruction
  - Certification
  - Data retention

WHAT you should be doing at each phase

WHY those activities are important to security

4.2: ASSET MANAGEMENT LIFECYCLE

What is the **asset management lifecycle**?

the process of tracking your valuable assets throughout their useful life, including hardware, software, and data.

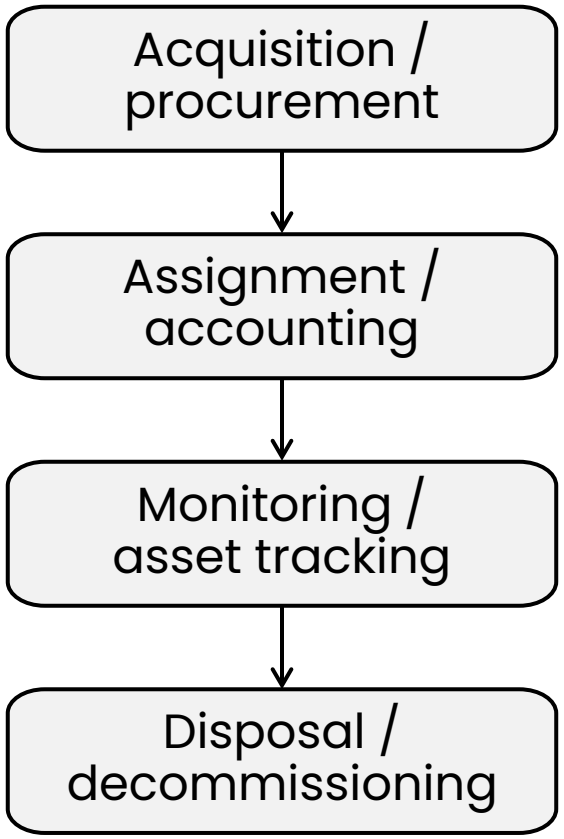
It outlines the key activities involved in:

- Acquisition/procurement
- Assignment/accounting
- Monitoring/asset tracking
- Disposal/decommissioning

GOAL

The overall security goal of asset management is to **minimize the risk of unauthorized access, disclosure, modification, or destruction** of an organization's assets.

4.2: ASSET MANAGEMENT LIFECYCLE



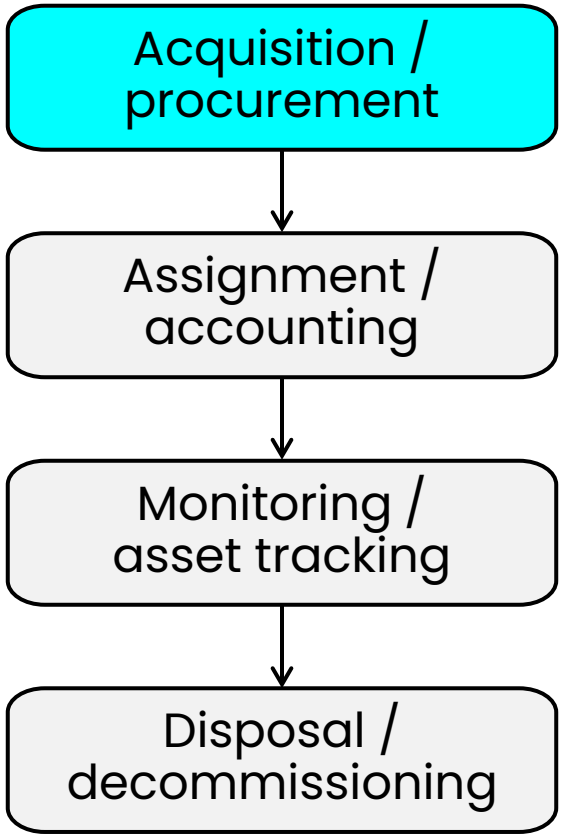
Stated simply, asset management is about:

- Keeping track of your stuff
- Making sure it's secure

By keeping tabs on everything you have, you can:

- Make sure it's all safe from getting stolen, changed, or lost.
- Only let the right people access what they need.
- Know when things are outdated and need fixing or replacing.
- Get rid of things you don't need anymore without leaving any sensitive information behind.

4.2: ACQUISITION/PROCUREMENT



Defines how assets enter the organization.

Key activities:

A secure process verifies vendors' reputations, ensures valid licensing for software

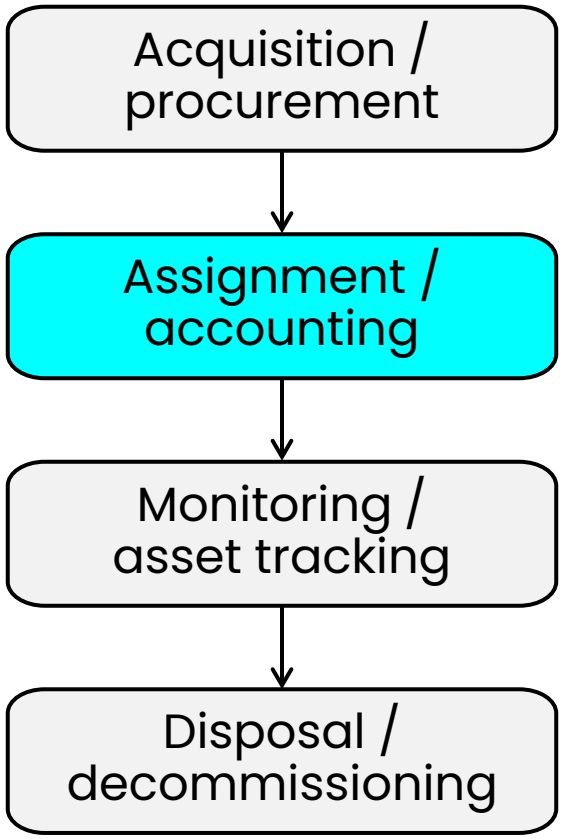
e.g., checking for valid licenses to avoid pirated software, no major vendor security incidents

Establishes baseline configurations for hardware

e.g., installing a secure operating system with the latest security patches

SECURITY CONCERNS: Malware-infected hardware (e.g., from an untrusted vendor) can introduce vulnerabilities. Unauthorized software or counterfeited licenses can lack security updates, leaving the system exposed.

4.2: ASSIGNMENT/ACCOUNTING



Ownership: Clearly defines who is responsible for the asset. e.g. person, department, or team

Classification: Categorizes assets based on sensitivity

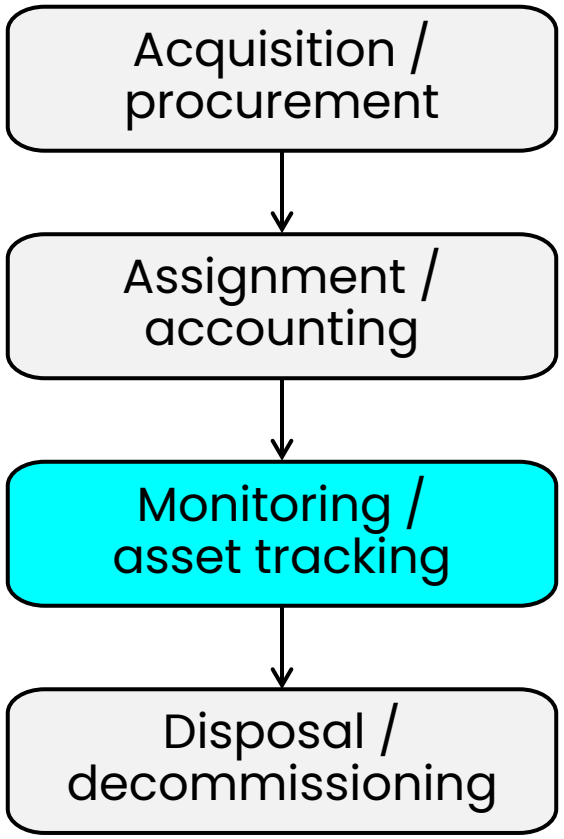
e.g., confidential financial data, public marketing materials

Importance:

Proper assignment and classification ensure appropriate access controls and security measures are implemented.

SECURITY CONCERNS: Unauthorized access to sensitive assets (e.g., an employee accessing customer data they don't have a legitimate need for) can lead to data breaches.

4.2: MONITORING/ASSET TRACKING



Inventory: Maintains an accurate record of all assets, including type, location, and owner.

Inventory tracked in a configuration management database (CMDB)

Enumeration: Regularly identifies and documents all assets on the network.

Importance:

Enables tracking asset location, status, and potential vulnerabilities.

Knowing where assets are located allows for faster response to security incidents.

SECURITY CONCERNS: Unknown or untracked assets create security blind spots, increasing the risk of breaches. An attacker might exploit an unmonitored device to gain access to the network.

How are physical assets tracked?

process where each asset belonging to the company has been tagged and recorded in an asset register.

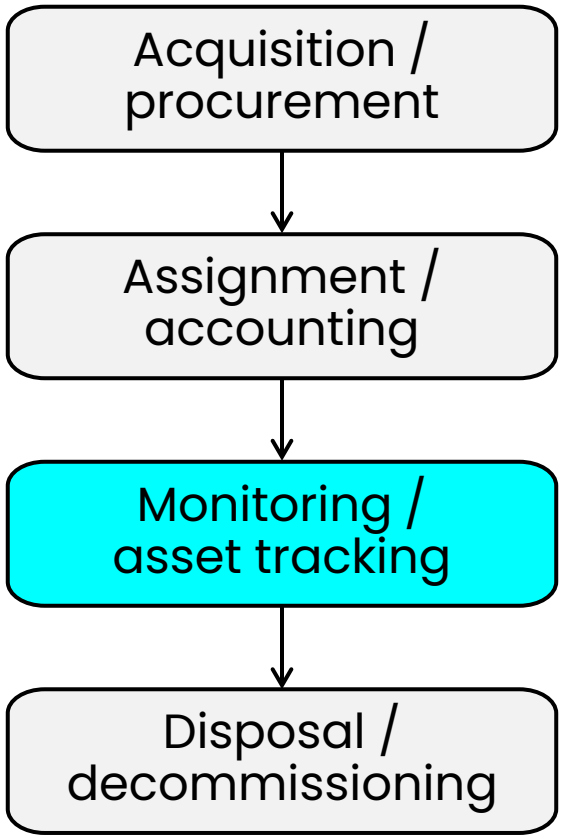
maintain an up-to-date asset register to ease the process of tracking and maintaining assets.

includes periodic audits (usually annual) need to be carried out to ensure that all assets are accounted for.

physical asset tags with **barcodes** or **QR codes** on each asset allows for quick scanning and ID during inventory.

These can help IT identify unauthorized devices on the network.

4.2: MONITORING/ASSET TRACKING



Inventory: Maintains an accurate record of all assets, including type, location, and owner.

Inventory tracked in a configuration management database (CMDB)

Enumeration: Regularly identifies and documents all assets on the network.

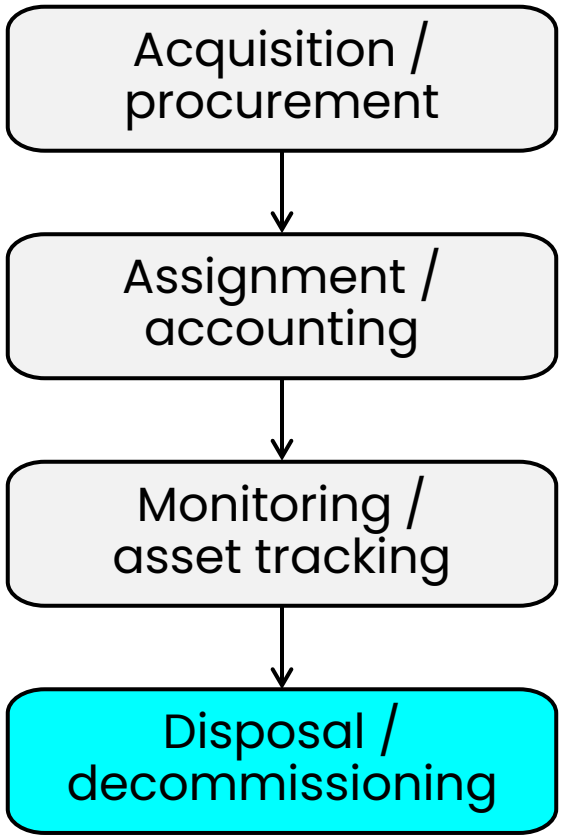
Importance:

Enables tracking asset location, status, and potential vulnerabilities.

Knowing where assets are located allows for faster response to security incidents.

SECURITY CONCERNS: Unknown or untracked assets create security blind spots, increasing the risk of breaches. An attacker might exploit an unmonitored device to gain access to the network.

4.2: DISPOSAL/DECOMMISSIONING



Sanitization: Ensures data removal from storage devices before disposal or recycling.

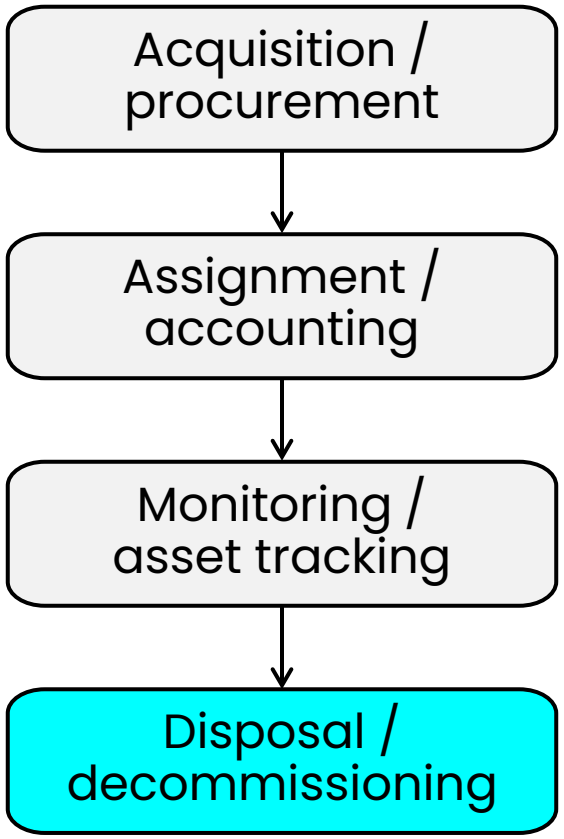
Destruction: Physically destroys assets beyond recovery when necessary.

Ensures data is securely destroyed when necessary

Certification: Provides documented proof of secure disposal for compliance purposes.

Data Retention: Defines how long data is kept based on legal or business needs.

4.2: DISPOSAL/DECOMMISSIONING



Importance:

Improper disposal can lead to data leaks and privacy violations

Deleted data should not be recoverable, even with forensic techniques

Data retention policies ensure compliance AND

Prevent unnecessary exposure of sensitive data being stored longer than required

Data that is kept longer than it is needed increases risk

SECURITY CONCERNS : Residual data on disposed assets *(e.g., incomplete data wiping)* or failure to adhere to data retention policies *(e.g., keeping customer data longer than necessary)* can lead to security incidents.

4.0 SECURITY OPERATIONS

4.3 Explain various activities associated with vulnerability management

- **Identification methods**
  - Vulnerability scan
  - Application security
    - Static analysis
    - Dynamic analysis
    - Package monitoring
  - Threat feed
    - Open-source intelligence (OSINT)
    - Proprietary/third-party
    - Information-sharing organization
    - Dark web
  - Penetration testing
  - Responsible disclosure program
    - Bug bounty program
  - System/process audit
- **Analysis**
  - Confirmation
    - False positive
    - False negative
  - Prioritize
  - Common Vulnerability Scoring System (CVSS)
  - Common Vulnerability Enumeration (CVE)
  - Vulnerability classification
  - Exposure factor
  - Environmental variables
  - Industry/organizational impact
  - Risk tolerance
- **Vulnerability response and remediation**
  - Patching
  - Insurance
  - Segmentation
  - Compensating controls
  - Exceptions and exemptions
- **Validation of remediation**
  - Rescanning
  - Audit
  - Verification
- **Reporting**

VULNERABILITY LIFECYCLE

The stages of the **vulnerability lifecycle**:

- Identification
- Analysis
- Response and remediation
- Validation of remediation
- Reporting

VULNERABILITY LIFECYCLE

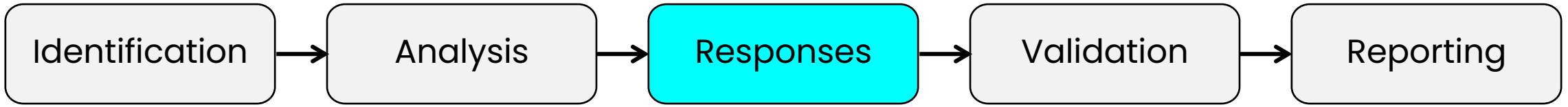
Vulnerability **identification** can come from scans, penetration tests, responsible disclosure, bug bounty programs, and audit results.

VULNERABILITY LIFECYCLE

Vulnerability **analysis** involves confirming the vulnerability, prioritizing it using CVSS and CVE, and considering organization-specific factors.

VULNERABILITY LIFECYCLE

Responses include applying patches, isolating affected systems, implementing compensating controls, transferring risk through insurance, or formally accepting the risk.



VULNERABILITY LIFECYCLE

Validation ensures the vulnerability is no longer present.

VULNERABILITY LIFECYCLE

Reporting informs stakeholders about the findings, actions, trends, and recommendations for improvement.

VULNERABILITY MANAGEMENT

Vulnerability Management — includes routine vulnerability scans and periodic vulnerability assessments.

Vulnerability Scanners — scan network and can detect known security vulnerabilities and weaknesses, absence of patches or weak passwords.

Are used to conduct:

Vulnerability Assessments — extend beyond just technical scans and can include reviews and audits to detect vulnerabilities.

VULNERABILITY SCAN OUTPUT

A **vulnerability scan** can identify and report various vulnerabilities before they are exploited, such as:

Examples include:
-software flaws
-missing patches
-open ports
-services that should not be running
-weak passwords

will help companies avoid known attacks such as SQL injection, buffer overflows, denial of service, and other type of malicious attacks.

Vulnerability reported in scan output will be **prioritized** based on severity and relative likelihood of vulnerability being exploited.

VULNERABILITY SCAN OUTPUT

A **vulnerability scan** can identify and report various vulnerabilities before they are exploited, such as:

Examples include:
-software flaws
-missing patches
-open ports
-services that should not be running
-weak passwords

will help companies avoid known attacks such as SQL injection, buffer overflows, denial of service, and other type of malicious attacks.

The **CVSS** (Common Vulnerability Scoring System) and **CVE** (Common Vulnerabilities and Exposures) info can help us prioritize

VULNERABILITY SCAN TYPES

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

Credentialed Scan: A credentialed scan is a much more powerful version of the vulnerability scanner. It has higher privileges than a non-credentialed scan.

Spot vulnerabilities that require privilege (login credentials)

Non-Credentialed Scan: A non-credentialed scan has lower privileges than a credentialed scan. It will identify vulnerabilities that an attacker would easily find.

Scans can find missing patches, some protocol vulnerabilities

VULNERABILITY SCAN TYPES

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

Non-Intrusive Scans: These are passive and merely report vulnerabilities. They do not cause damage to your system.

Intrusive Scans: Can cause damage as they try to exploit the vulnerability and should be used in a sandbox and not on your live production system.

Configuration Review: Configuration compliance scanners and desired state configuration in PowerShell ensure that no deviations are made to the security configuration of a system.

The combination of techniques can reveal which vulnerabilities are most easily exploitable in a live environment.

VULNERABILITY SCAN TYPES

Network Scans: These scans look at computers and devices on your network and help identify weaknesses in their security.

Application Scans: Before applications are released, coding experts perform regression testing that will check code for deficiencies.

Web Application Scans:
Crawl through a website as if they are a search engine looking for vulnerabilities.

Perform an automated check for site/app vulnerabilities, such as cross-site scripting and SQL injection.

There are many sophisticated web application scanners available, due in part due to mass adoption of cloud computing.

APPLICATION SECURITY

Static Analysis

Requires access to source code

Analysis that examines the code without executing it.

Dynamic Analysis

Does not require source code access

Code analysis checks the code as it is running.

Tests the applications ability to handle unexpected or malicious input gracefully

Package Monitoring

Tracking third-party and open-source libraries or packages used in your organization and monitoring for known vulnerabilities.

Ensures libraries are patched and versions up-to-date

THREAT INTELLIGENCE SOURCES

Open-source intelligence (OSINT)

Enables orgs to conduct cyber-threat intelligence gathering free of charge.

Examples include threatcrowd.org, openphish.com.

Closed/proprietary

You may see these vendor-specific threat intelligence feeds limited to paying customers, which are intended to keep customers informed and secure, while not tipping off threat actors (hackers).

e.g. Tenable, SecurityFocus, Rapid7 and many others

Vulnerability databases

MITRE CVE list, VulDB.com

such as www.shodan.io, allow you to search for vulnerabilities.

The National Institute of Standards and Technology (NIST) maintains a comprehensive database of vulnerabilities.

This is the **National Vulnerability Database** and it keeps within that database a list of CVEs (Common Vulnerabilities and Exposures).

THREAT INTELLIGENCE SOURCES

Public/private information sharing centers.

Programs, groups, and feeds to designed to share cyber intelligence in various forms to government and commercial organizations around the world.

The **Cybersecurity Infrastructure and Security Agency (CISA)**, an agency of the US federal government, maintains a list of information sharing centers at https://www.cisa.gov/information-sharing-and-awareness .

Dark web (Tor browser, .onion websites)

This is an overlay to the existing internet that requires specialized software to be able to access these private websites. There's extensive information to gather from the dark web, including the activities of hacker groups.

Indicators of Compromise (IoC)

sometimes called "threat indicators" are "pieces of forensic data", such as data found in system log entries or files, that identify potentially malicious activity on a system or network.

THREAT INTELLIGENCE SOURCES

What is a threat intelligence feed (threat feed)?

It is a continuous stream of data about potential cyber threats

This data is collected from various sources and formatted to provide security professionals with actionable intelligence.

Think of it like a real-time news feed, but instead of news articles, it delivers updates on the latest cyber threats

What's included in a threat feed?

It varies by provider, but can include indicators of compromise (IoCs), threat actor information, and emerging threats.

How are these feeds consumed?

Some are machine readable (STIX/TAXII format, consumable by a SIEM) others are human readable feeds, delivered via e-mail, dashboards, or reports.

Threat feeds can help organizations stay ahead of the latest cyber threats providing **early warning**, **improved detection**, and **informed decision-making**

THREAT INTELLIGENCE SOURCES

SIEM, NGFW, and IDPS solutions may ingest threat intelligence feeds

Automated Indicator Sharing (AIS)

A Cybersecurity and Infrastructure Security Agency (CISA) capability, enables the real-time exchange of machine-readable cyber threat indicators and defensive measures.

It's provided free to help protect participants of the AIS community and ultimately reduce the prevalence of cyberattacks.

Find it at https://www.cisa.gov/ais

Trusted Automated eXchange of Intelligence Information (TAXII)

Short for **T**rusted **A**utomated e**X**change of **I**ntelligence **I**nformation, defines how real-time cyber threat information can be shared via services and message exchanges.

Structured Threat Information eXpression (STIX)

Defines a common language for expressing cyber threat information.

TAXII is designed specifically to support transfer of STIX information.

STIX defines "what" is shared, and TAXII is the "how" STIX formatted messages are securely transferred between systems

THREAT INTELLIGENCE SOURCES

Predictive analysis

Leverages predictive intelligence, a mix of automation and human intelligence capabilities to optimize your cybersecurity program and gradually build capacity to predict and prevent attacks before they hit.

Threat maps

A cyber threat map, also known as a cyber attack map, is a real-time map of the computer security attacks that are going on at any given time.

Find cyber threat maps from Fortinet, FireEye and others in the Top 8 Cyber Threat Maps

File and code repositories

Google searching code repositories on sources like Github can show you what threat actors are using. For example, full source code of Mimikatz is available at https://github.com/ParrotSec/mimikatz.

If you're using open-source software for your business, know that hackers often review popular open-source apps looking for vulnerabilities.

RESEARCH SOURCES

Vendor websites

There's usually a page on a vendor's website where they keep track of all of the known vulnerabilities.

Often, there's some type of notification process so they can inform you immediately when a new vulnerability is discovered.

Conferences

These are great events to network with experts, hear talks often based on experiences of others, and even hear from members of product teams talking in-depth about security of their app or service.

Academic Journals

Offer information about attack types and how others have responded or recovered from them.

Available from a variety of government, education, and community sources, often peer-reviewed!

usually results in higher quality

EXAMPLES:

Oxford Academic Journal of Cybersecurity
https://academic.oup.com/cybersecurity

MDPI Switzerland
https://www.mdpi.com/journal/jcp

RESEARCH SOURCES

Request for comments (RFC)

A publication in a series, from the principal technical development and standards-setting bodies for the Internet, most prominently the **Internet Engineering Task Force (IETF)**.

An **RFC** is authored by individuals or groups of engineers and computer scientists in the form of a memorandum describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

RESEARCH SOURCES

Request for comments (RFC)

A publication in a series, from the principal technical development and standards-setting bodies for the Internet, most prominently the **Internet Engineering Task Force (IETF)**.

The IETF adopts some of the proposals published as Internet Standards.

However, many are informational or experimental in nature and are not standards.

RFCs have become official documents of Internet specifications, communications protocols, procedures, and events.

RESEARCH SOURCES

Learning from your peers and community experts

Local industry groups

You'll find local interest groups or user groups around cybersecurity (and many related topics) where you can learn from your peers and experts in your local community.

Social media

Hackers often publish recent vulnerabilities on **Twitter**

Security interest groups and certification study groups on **LinkedIn**.

Video learning content on **YouTube** on cybersecurity certification, concepts, and entertainment.

PENETRATION TESTS & TEST TYPES

What exactly is a **penetration test**?

A penetration test is an active test that attempts to exploit discovered vulnerabilities.

Often starts with reconnaissance, and a vulnerability scan.

The tester then attempts to bypass or actively tests security controls to exploit vulnerabilities.

Once they exploit a system, the tester will attempt privilege escalation techniques and lateral movement.

Pivoting is the process of using an exploited system to access other systems.

PENETRATION TESTING VS VULNERABILITY SCAN

These two sound similar, but what's the difference?

Vulnerability scan

A scan to identify weaknesses in your IT infrastructure.

Uses automated tools to scan systems for known vulnerabilities.

Reports the identified weaknesses and categorizes their severity (often a CVE).

May also suggest potential remediation steps.

Penetration test

A more in-depth exam, similar to a simulated cyber attack.

Uses a combination of automated tools and manual techniques.

Attempt exploit vulnerabilities and assess their potential impact.

Helps you understand how vulnerable you are to real-world attacks and how much damage could be done.

Like a fire alarm warns of a fire but doesn't say exactly where or how severe it is!

Like a firefighter testing the fire alarm and sprinkler system.

PENETRATION TESTING VS VULNERABILITY SCAN

Almost anyone can do

Vulnerability scan

A scan to identify weaknesses in your IT infrastructure.

Uses automated tools to scan systems for known vulnerabilities.

Reports the identified weaknesses and categorizes their severity (often a CVE).

May also suggest potential remediation steps.

Like a fire alarm warns of a fire but doesn't say exactly where or how severe it is!

Requires special skills

Penetration test

A more in-depth exam, similar to a simulated cyber attack.

Uses a combination of automated tools and manual techniques.

Attempt exploit vulnerabilities and assess their potential impact.

Helps you understand how vulnerable you are to real-world attacks and how much damage could be done.

Like a firefighter testing the fire alarm and sprinkler system.

PENETRATION TESTING VS VULNERABILITY SCAN

Generally, not intrusive

Vulnerability scan

A scan to identify weaknesses in your IT infrastructure.

Uses automated tools to scan systems for known vulnerabilities.

Reports the identified weaknesses and categorizes their severity (often a CVE).

May also suggest potential remediation steps.

Like a fire alarm warns of a fire but doesn't say exactly where or how severe it is!

Intrusive, may be disruptive

Penetration test

A more in-depth exam, similar to a simulated cyber attack.

Uses a combination of automated tools and manual techniques.

Attempt exploit vulnerabilities and assess their potential impact.

Helps you understand how vulnerable you are to real-world attacks and how much damage could be done.

Like a firefighter testing the fire alarm and sprinkler system.

PENETRATION TESTS & TEST TYPES

Known environment

white box test

penetration tester is given a map of target systems and networks. They go into the test with substantial/full information of the target systems and networks.

Unknown environment

black box test

penetration tester knows nothing about target systems and networks. They go into the test completely blind and build out the database of everything they find as they go.

Partially known environment

gray box test

limited information is shared with the tester, sometimes in the form of login credentials. Simulate the level of knowledge that a hacker with long-term access to a system would achieve through research and system footprinting.

Rules of engagement

Captured in a signed, legal contract

Rules of engagement define the purpose of the test, and what the scope will be for the people who are performing this test on the network.

They ensure everyone will be aware of what systems will be considered, date and time, and any constraints all should be aware of.

PASSIVE AND ACTIVE RECONNAISSANCE

Active reconnaissance interacts directly with the target in some way and as such, the target may discover, record, or log these activities.

Footprinting

Includes active and passive methods

An ethical hacking technique used to gather as much data as possible about a specific targeted computer system, infrastructure and networks to identify opportunities to penetrate them.

Active footprinting

Ping sweep
Tracert analysis
Nmap
Extracting DNS information

Passive footprinting

Browsing target website
Google search (Google hacking)
Performing WHOIS lookup
Visiting social media profiles

PASSIVE AND ACTIVE RECONNAISSANCE

Passive reconnaissance one is not interacting directly with the target and as such, the target has no way of knowing, recording, or logging activity.

OSINT

Much of the information gathered in this phase can be categorized as open-source intelligence or OSINT.

The data that you can gather through these open sources is extensive.

A site that gives you a base of information that you can gather and tools for doing so is available at https://osintframework.com

PENETRATION TESTING CONCEPTS

Lateral movement

Gaining access to an initial system, then moving to other devices on the inside of the network.

Privilege escalation

A security hole created when code is executed with higher privileges than those of the user running it.

Generally, a higher-level account, but in some cases, it is a horizontal privilege escalation where a user gains access to another users' resources.

Persistence

In the context of penetration testing refers to the testers ability to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access.

Enabling the ability to reconnect to the compromised host and use it as a remote access tool.

Exercise Types

Red Team offense

are internal or external entities dedicated to testing the effectiveness of a security program by emulating the tools and techniques of likely attackers in the most realistic way possible.

Blue Team defense

the internal security team that defends against both real attackers and Red Teams.

Purple Team process improvement

exist to ensure and maximize the effectiveness of the Red and Blue teams.

White Team judge / referee

responsible for overseeing an engagement/competition between a Red Team of mock attackers and a Blue Team of actual defenders.

RESPONSIBLE DISCLOSURE

Responsible disclosure programs

Enable individuals and organizations to report security vulnerabilities or weaknesses they have discovered to the affected software/app vendor.

When vulnerabilities are reported, the vendor receiving the report is expected to investigate and, if necessary, take appropriate steps to address the issue.

GOAL: to allow security issues to be addressed by the vendor before they are exploited by attackers, ultimately improving overall security for everyone

Bug bounty

A monetary reward given to ethical hackers for successfully discovering and reporting a vulnerability or bug to the application's developer.

Bug bounty programs allow companies to leverage the hacker community to improve security posture of their systems over time continuously.

SYSTEM/PROCESS AUDITS

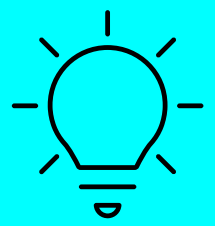
System and Process Audits

are used to assess organization's compliance with industry standards, best practices, and corporate security policies.

Typically review an org's systems, processes, and procedures to identify areas of non-compliance or potential risk.

During the audit process, auditors may use a variety of tools and techniques to collect information

e.g. system scans, interviews, document reviews, etc.



Audits can identify issues beyond identifying vulnerabilities, including deficiencies in policies and operations.

CONFIRMATION

A **vulnerability scan** assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

False Positive: where the scan believes that there is a vulnerability but when physically checked, it is not there.

False Negative: When there is a vulnerability, but the scanner does not detect it.

True Positive: This is where the results of the system scan agree with the manual inspection.

Log Reviews: Following a vulnerability scan, it is important to review the log files/reports that list any potential vulnerabilities.

Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS)

CVSS is the overall score assigned to a vulnerability. It indicates severity and is used by many vulnerability scanning tools.

CVE is simply a list of all publicly disclosed vulnerabilities that includes the CVE ID, a description, dates, and comments.

The CVSS score is not reported in the CVE listing – you must use the **National Vulnerability Database (NVD)** to find assigned CVSS scores.

The CVE list feeds into the NVD

The **National Vulnerability Database (NVD)** is a database, maintained by NIST, that is synchronized with the **MITRE CVE list**.

Vulnerability Classification

The process of categorizing vulnerabilities based on their severity and potential impact.

This helps prioritize remediation efforts and effective allocation of resources.

There are several vulnerability classification systems, but the most widely used the **CVSS**.

CVSS assigns a score from 0.0 (least severe) to 10.0 (most severe) based on three main metrics:

Exploitability: How easy is it to exploit the vulnerability?

Impact: What kind of damage can an attacker cause if they exploit the vulnerability?

Scope: To what assets or systems does the vulnerability apply?

Exposure Factor

The percentage of value an asset lost due to an incident.

It is the portion of an asset that the organization expects would be damaged if a risk materializes.

FOR EXAMPLE:
A building is worth $1,000,000 USD

It is estimated a tornado will result in 30% damage/loss

Exposure factor = 30%

A likely response is insurance (risk transference)

4.3 ENVIRONMENTAL VARIABLES

The specific circumstances and factors within an organization's environment **that can impact the severity, likelihood, or risk** associated with a particular vulnerability.

Asset criticality:
The importance of the affected system

Network topology:
The layout and configuration of the organization's network and access controls which can influence the potential impact of a vulnerability.

Data sensitivity:
The level of confidentiality, integrity, and availability required for the data stored or processed by the affected system.

User base:
The number and type of users accessing the vulnerable system, as well as their privileges and access rights.

4.3 ENVIRONMENTAL VARIABLES

The specific circumstances and factors within an organization's environment **that can impact the severity, likelihood, or risk** associated with a particular vulnerability.

External dependencies:

The reliance on third-party services, vendors, or partners that may be affected by the vulnerability.

Threat landscape:

The current state of threats, including the prevalence of attacks exploiting the specific vulnerability and the likelihood of the organization being targeted.

Operational constraints:

The organization's ability to implement remediation measures, considering factors such as maintenance windows, and potential disruption to business processes.

Regulatory requirements:

Industry-specific or general data protection and security regulations that the organization must comply with, such as GDPR, HIPAA, or PCI-DSS.

4.3 RISK TOLERANCE

Risk tolerance. Sometimes called *"risk appetite"*, is the amount of risk that a company is willing to accept.

These terms are often used interchangeably, though appetite is aggregate, and tolerance per individual risk.

Regulations that affect risk tolerance

regulations addressing data privacy and security that influence an organizations risk tolerance and posture include:

- General Data Protection Regulation (**GDPR**)
- Sarbanes-Oxley Act (**SOX**),
- Health Insurance Portability Accountability Act (**HIPAA**)
- Payment Card Industry & Data Security Standard regulations (**PCI-DSS**)

Responses to Risk

Risk Acceptance. Do nothing, and you must accept the risk and potential loss if threat occurs.

Risk Mitigation. You do this by implementing a countermeasure and accepting the residual risk.

The act of reducing risk

Risk Transference. Transfer (assign) risk to 3rd party, such as by purchasing insurance against damage.

Risk Avoidance. When costs of mitigating or accepting are higher than benefits of the service.

VULNERABILITY RESPONSE AND REMEDIATION

The process of eliminating vulnerabilities discovered in the vulnerability scan

Patching
Software patches are updates that correct OS and application vulnerabilities.

Firmware patches and driver updates address hardware vulnerabilities.

Insurance This is risk transference
Purchase of an insurance policy to provide payment for replacement in the event a risk is realized or vulnerability exploited.

Segmentation
Placing system on an isolated segment to reduce external exposure

VULNERABILITY RESPONSE AND REMEDIATION

The process of eliminating vulnerabilities discovered in the vulnerability scan

Compensating Controls

A secondary/supporting security control that prevents the vulnerability from being exploited.

A WAF is a backup for imperfect code-level input validation

Exceptions and Exemptions

Allowing a vulnerable system to continue to operate without doing anything to address the problem.

This is effectively risk acceptance

VALIDATION OF REMEDIATION

Ensures identified vulnerabilities have been effectively addressed, and that the chosen mitigation has actually eliminated the security weakness.

Rescanning The most common response

Security tools are used to re-scan the affected system after the remediation steps are completed.

Audit

An in-depth examination of the remediation process and documentation, that may involve review of the chosen mitigation strategy as well.

Verification

Actively testing the system to see if the vulnerability can still be exploited.

4.3 REPORTING

Communicating the findings, actions taken, and lessons learned to relevant stakeholders within the organization.

Ensures that decision-makers are informed about the actions taken and impact to current security posture.

Details any trends, patterns, or vulnerable areas requiring further attention.

Offers recommendations for improvements based on the findings and experiences throughout the lifecycle.

Closes the communication loop and completes the vulnerability lifecycle

4.0 SECURITY OPERATIONS

4.4 Explain security alerting and monitoring concepts and tools

- **Monitoring computing resources**
  - Systems
  - Applications
  - Infrastructure
- **Activities**
  - Log aggregation
  - Alerting
  - Scanning
  - Reporting
  - Archiving
  - Alert response and remediation/validation
    - o Quarantine
    - o Alert tuning
- **Tools**
  - Security Content Automation Protocol (SCAP)
  - Benchmarks
  - Agents/agentless
  - Security information and event management (SIEM)
  - Antivirus
  - Data loss prevention (DLP)
  - Simple Network Management Protocol (SNMP) traps
  - NetFlow
  - Vulnerability scanners

Concepts → benefits → examples

4.4 MONITORING

Systems

Tracks the health and activity of individual devices like servers, workstations, and network equipment

CPU, memory, disk usage, network activity, login attempts, running processes

Applications

Tracks the health and performance of specific software applications.

Application response times, resource usage, error logs, transaction failures

Infrastructure

Tracks the health and performance of the underlying IT infrastructure, including networks, firewalls, and storage systems.

Network traffic volume, bandwidth utilization, latency, packet loss, storage capacity

Significant fluctuation in baseline monitoring metrics can indicate potentially malicious activity or even attack in progress!

4.4 ACTIVITIES

The activities in this list would apply to standard system, infrastructure, and application monitoring, but security will be the focus on the exam.

Log Aggregation

Often with SIEM

Security tools collect logs from various systems, applications, and network devices.

Log aggregation centralizes these logs for easier analysis and threat detection

Alerting

Security tools trigger alerts based on predefined rules or anomalies detected in logs.

These alerts notify security teams of potential threats requiring investigation

Example: An alert might be generated if a user logs in from an unusual location, potentially indicating unauthorized access.

4.4 MONITORING

Scanning

involves proactively searching systems and networks for vulnerabilities, malware, or misconfigurations.

Example: Regularly scanning for vulnerabilities helps identify and patch security weaknesses before attackers exploit them.

Reporting

Security tools generate reports summarizing security events, identified threats, and overall security posture.

Provide insights for security teams and management to assess security risks and make informed decisions

Archiving

Logs and security events are archived for future reference and forensic analysis in case of a security incident.

Benefit: Archived data helps investigate the root cause of security breaches and identify trends in attacker behavior over time

ACTIVITIES

Apply to SIEM, XDR, IDS/IPS, CASB, and other tools

Alert response, remediation, and validation

Alert Response:
When an alert is triggered, security teams need to investigate it to determine if it's a real threat or a false positive.

Remediation/Validation:
If the threat is real, steps need to be taken to contain the damage and remediate the issue.

Validation Similar options to those described in 4.3
Involves confirming the threat and the effectiveness of remediation efforts.

Quarantine: In some cases, quarantining infected systems or data might be necessary to prevent further spread of the threat.

Alert Tuning: Security teams fine-tune alert rules to reduce false positives and ensure alerts are triggered only for significant security events.

TOOLS

SCAP is used by SIEM, vulnerability scanners, and other security configuration management tools

Security Content Automation Protocol (SCAP) is a set of open standards that facilitates the automated management of vulnerabilities and security policy compliance.

Benefits of SCAP

Automation:
SCAP automates vulnerability management tasks, saving time and resources for security teams.

Standardization:
SCAP promotes a standardized approach to vulnerability management, enabling interoperability between different security tools.

Improved Accuracy:
Automation reduces the risk of human error in vulnerability scanning and assessment.

Compliance:
SCAP helps organizations comply with security regulations that require vulnerability management and configuration control.

BENCHMARKS

Quick refresher from section 4.1

Control

a high-level description of a feature or activity that needs to be addressed and is not specific to a technology or implementation.

Is expressed in a

Benchmark

contains security recommendations for a specific technology, such as an IaaS VM.

and implemented through a

Baseline

is the implementation of the benchmark on the individual service.

Benchmarks provide guidance on secure configuration and when implemented as **baselines**, enforce desired configuration.

AGENTS/AGENTLESS

for logging and monitoring

Agents

Agents are used to send logs for systems that don't have a specific logging/forwarding capability.

Often used on server and desktop endpoints

Agentless

Agentless options are used to send data without a separate program or agent deployed to allow that.

Network appliances send syslog data without the need for a local agent

An agent-based solution may be more vulnerable to tampering, requires updates, and may consume excessive resources.

SIEM AND SOAR

uses AI, ML, and threat intelligence

SIEM
Security Information Event Management

system that collects data from many other sources within the network.

provides real-time monitoring, analysis, correlation & notification of potential attacks.

Log aggregation happens here!

SOAR
Security Orchestration Automation, & Response

centralized alert and response automation with threat-specific runbooks.

response may be fully automated or single-click.

Many providers deliver these capabilities together

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

Playbook

paperwork

a document or checklist that defines how to verify an incident

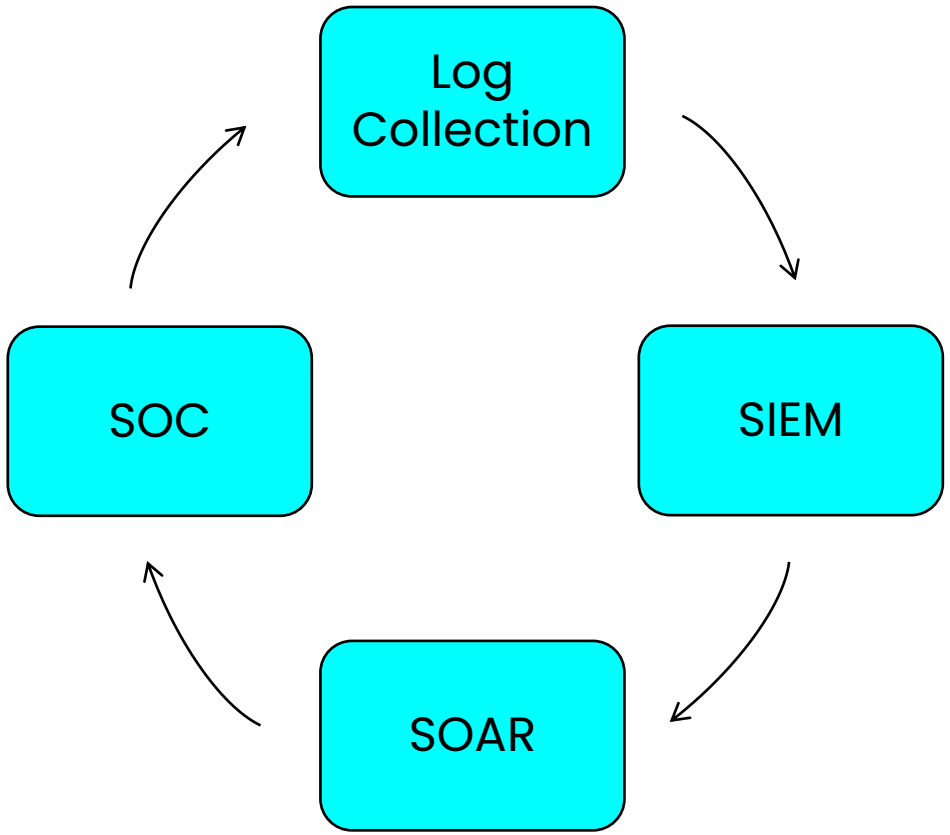
Runbook

technology

implements the playbook data into an automated tool

LOG AGGREGATION IN THE SOC WORKFLOW

The role of log aggregation to incident analysis and response procedures in the security operations center (SOC).



Integrates your security processes and tooling in a central location.

Response automation, using machine learning and artificial intelligence, make it faster than humans in identifying and responding to true incidents.

Reduces MTTD and accelerates response

Uses **playbooks** and **runbooks** that define an incident and response (on paper and in practice).

Capabilities vary by situation & vendor

SOC analysts interpret SIEM and SOAR information and response accordingly.

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Log centralization and aggregation

Rather than leaving log data scattered around the environment on various hosts, the SIEM platform can gather logs from a variety of sources, including:

- operating systems
- applications
- network appliances
- cloud infrastructure
- cloud services
- user devices

ARTIFICIAL INTELLIGENCE vs MACHINE LEARNING

Knowing the difference may help on the exam!

Artificial Intelligence

Focuses on accomplishing "smart" tasks combining machine learning and deep learning to emulate human intelligence

Machine Learning

A subset of AI, computer algorithms that improve automatically through experience and the use of data.

Deep Learning

a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called **artificial neural networks**.

LOG ANALYSIS

User Entity Behavior Analysis (UEBA)

This is based on the interaction of a user that focuses on their identity and the data that they would normally access on a normal day.

It tracks the devices that the user normally uses and the servers that they normally visit. It creates a baseline of "normal"

Sentiment Analysis

Artificial intelligence and machine learning to identify attacks.

Cybersecurity sentiment analysis can monitor articles on social media, look at the text and analyze the sentiment behind the articles.

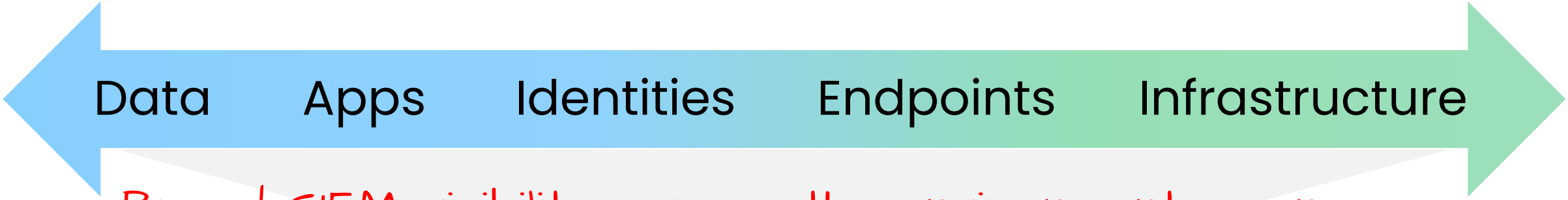
Over time, can identify a users' attitudes to different aspects of cybersecurity.

SECURITY INFORMATION EVENT MANAGEMENT (SIEM)

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Investigative monitoring

When manual investigation is required, the SIEM should provide support capabilities such as querying log files, generating reports.



Broad SIEM visibility across the environment means better context in log searches, & security investigations

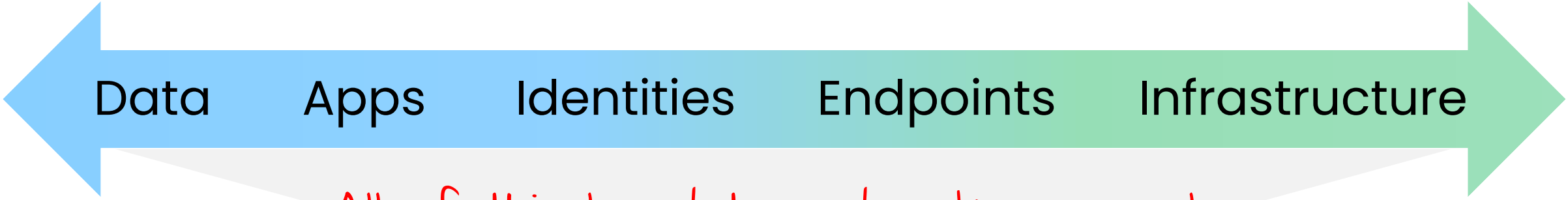
SIEM

SECURITY INFORMATION EVENT MANAGEMENT (SIEM)

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Investigative monitoring

When manual investigation is required, the SIEM should provide support capabilities such as querying log files, generating reports.



All of this log data and makes complex response automation via SOAR possible

SIEM + SOAR

SIEM REPORTING AND & DASHBOARDS

Dashboards are very useful to the security operations centers as they provide centralized visibility and information on threats in real time.

Sensor: Sensors are deployed across your network to monitor and collect changes in network patterns or monitor changes in log file entries as events occur.

Varies by solution and device. May be a sensor, syslog, text log, API or other format.

Sensitivity: can monitor PII, PHI, and other sensitive information to ensure regulatory compliance (HIPAA, PCI DSS, GDPR)

Trends: can identify trends in network traffic, event volume, or changes in activities/ activity levels across identities, endpoints, network and infrastructure.

Alerts: provide information about events on hosts and network devices.

Email notification and response automation (runbooks via SOAR) are options.

Correlation: correlates, aggregates, and analyzes the log files from multiple sources can generate a broad, centralized view.

Because sequence of events crosses multiple sources, time sync matters (NTP).

ANTIVIRUS

Modern **antivirus solutions** have evolved to combat increasingly sophisticated cyber threats. Features include:

Real-time Protection: Continuously monitor system activity for suspicious behavior, blocking malware before it can infect the device.

Multi-layered Defense: Combine various techniques like signature-based detection, behavior analysis, and machine learning to identify and block a wider range of threats.

Heuristic Analysis: Analyze files for suspicious characteristics even if they haven't been encountered before (zero-day attacks).

Sandboxing: Isolate suspicious files in a virtual environment to test their behavior before allowing them to run on the system.

Cloud-based Threat Intelligence: Access to real-time updates on new threats and vulnerabilities from centralized databases.

Some even have direct cloud connection for real-time sample submission and evaluation

DATA LOSS PREVENTION (DLP)

DLP

Data Loss Prevention

a system designed to identify, inventory, and control the use of data that an organization deems sensitive.

spans several categories of controls including detective, preventative, and corrective.

Policies can be typically applied to email, SharePoint, cloud storage, removeable devices, and databases

DATA LOSS PREVENTION (DLP)

DLP

Data Loss Prevention

is a way to protect sensitive information and prevent its inadvertent disclosure.

can identify, monitor, and automatically protect sensitive information in documents

monitors for and alerts on for potential breaches, policy violations like oversharing

Protection travels with the document, file, or other data, preventing local override of DLP protections

4.4 SNMP

SNMP

SIMPLE **N**ETWORK
MANAGEMENT
PROTOCOL

Monitors and manages network devices, such as routers or switches

Can modify device configuration or report status to a management system

Agents installed on devices send info to an SNMP manager through notifications known as SNMP traps

Remember this for the exam!

SNMPv1 and v2 both have vulnerabilities, including sending passwords across the network in cleartext, but **SNMPv3 encrypts credentials** before sending them over the wire.

4.4 NETFLOW

A feature available on many routers and switches that can collect IP traffic statistics and send them to a NetFlow collector.

The **NetFlow collector** receives and stores the data.

Protocol analyzers like Wireshark enable capture and view of data, including headers and payloads of individual packets.

By comparison, NetFlow only records counts or stats related to data a device receives.

Uses templates to identify what data to include in a NetFlow packet, but generally includes:

Timestamps identifying the start and finish time of the flow

Input interface identifier (on router or switch)

Output interface identifier (will be zero if a packet is dropped)

Source information (source IP address and port number, if used)

VULNERABILITY SCANS

Role of vulnerability scans in monitoring and maintenance

Vulnerability scan

A scan to identify weaknesses in your IT infrastructure.

Uses automated tools to scan systems for known vulnerabilities.

Reports the identified weaknesses and categorizes their severity (often a CVE).

May also suggest potential remediation steps.

A monthly vulnerability scan establishes a pattern in which the team can quickly spot negative changes month-to-month

Regular vulnerability scans can verify the efficacy of your configuration management, identifying new issues and regressions

4.0 SECURITY OPERATIONS

How are these used in the enterprise and to what benefit?

4.5 Given a scenario, modify enterprise capabilities to enhance security

- **Firewall**
  - Rules
  - Access lists
  - Ports/protocols
  - Screened subnets
- **IDS/IPS**
  - Trends
  - Signatures
- **Web filter**
  - Agent-based
  - Centralized proxy
  - Universal Resource Locator (URL) scanning
  - Content categorization
  - Block rules
  - Reputation
- **Operating system security**
  - Group Policy
  - SELinux
- **Implementation of secure protocols**
  - Protocol selection
  - Port selection
  - Transport method
- **DNS filtering**
- **Email security**
  - Domain-based Message Authentication Reporting and Conformance (DMARC)
  - DomainKeys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Gateway
- **File integrity monitoring**
- **DLP**
- **Network access control (NAC)**
- **Endpoint detection and response (EDR)/extended detection and response (XDR)**
- **User behavior analytics**

4.5 FIREWALL

A **firewall** is a security system that controls incoming and outgoing network traffic according to predefined rules.

Rules

Define the firewall's security policies, which include:

Source: The IP address or network segment allowed to initiate communication.

Destination: The IP address or network segment allowed to receive communication.

Port/Protocol: The specific port number and communication protocol (e.g., TCP, UDP) used for the traffic.

Action: Whether to allow or deny the traffic.

4.5 FIREWALL

A **firewall** is a security system that controls incoming and outgoing network traffic according to predefined rules.

Access Lists (ACLs)

Collections of firewall rules that define what traffic is allowed or denied.

There are two main types:

Standard ACLs: Simple rules based on source IP address and destination IP address.

Extended ACLs: More complex rules that consider additional factors like port numbers, protocols, and direction of traffic.

If no allow rule is encountered in the list, the last rule is generally a **deny all** rule.

4.5 FIREWALL

A **firewall** is a security system that controls incoming and outgoing network traffic according to predefined rules.

Ports/Protocols:

Every network communication happens over a specific port (think of it as a channel) using a particular protocol (language).

Common protocols include:

TCP (Transmission Control Protocol): Reliable, connection-oriented protocol used for web browsing, file transfer, etc.

UDP (User Datagram Protocol): Connectionless protocol used for streaming services, online gaming, etc.

ICMP (Internet Control Message Protocol): Used for network diagnostics (e.g., ping).

4.5 SCREENED SUBNET

A boundary layer between the Internet and trusted network that hosts resources.

Front-end web and email servers may reside in a screened subnet.

Systems with sensitive data or hosting identity and access management would not. e.g. Active Directory

The firewall acts as a screen, only allowing authorized traffic to flow between internal and external

Traffic allowed into the screened subnet is based on the defined rules and access lists

Other names for a screened subnet are **Demilitarized Zone (DMZ)** or **perimeter network**.

IDS/IPS

Trends

trends refer to patterns and anomalies observed in network traffic or system activity over time.

can help identify potential threats that might not be immediately obvious from a single event

Signatures

pre-defined patterns of malicious activity used by IDS/IPS systems to detect known threats

based on indicators of compromise (IOCs) associated with specific attacks or malware

Both host-based and network-based IDS/IPS can use trends, signatures, or a combination of both.

IDS/IPS

Behavior based

aka "anomaly-based" or "heuristic-based"

creates a baseline of activity to identify normal behavior and then measures system performance against the baseline to detect abnormal behavior.

can detect previously unknown attack methods

Signature based

aka "knowledge-based"

pre-defined patterns of malicious activity used by IDS/IPS systems to detect known threats.

only effective against known attack methods

Both host-based and network-based IDS/IPS can be knowledge based, behavior based, or a combination of both.

4.5 WEB FILTER

A centralized proxy device or agent-based tool that allows or blocks traffic based on content rules.

Deployment Methods

Two primary solution/deployment models:

Agent-based. Software agents are installed on individual devices (computers, laptops) and monitor web browsing activity directly on those devices.

Supports filtering in a '***work from anywhere***' scenario

Centralized proxy. All web traffic from the network is routed through a central server (proxy) that performs the filtering.

This offers ***centralized management*** but can introduce performance overhead and potential bottlenecks.

4.5 WEB FILTER

A centralized proxy device or agent-based tool that allows or blocks traffic based on content rules.

Filtering Techniques

URL scanning. Web filters can check URLs against blacklists of known malicious or inappropriate websites.

Content categorization. Web filters can analyze the content of web pages and categorize them

May be based on pre-defined categories (e.g., social media, gambling, news), augmented by custom admin configuration.

Access can be allowed or blocked based on these categories.

Block rules. Administrators can define custom rules to block access to specific websites or types of content

4.5 WEB FILTER

A centralized proxy device or agent-based tool that allows or blocks traffic based on content rules.

Filtering Techniques

Reputation. Web filters can leverage reputation databases that assign trust scores to websites based on various factors.

This can help identify potentially risky websites based on their historical behavior.

Benefits

Benefits can include improved security, enhanced productivity, and better compliance.

An effective approach will balance security with user needs, **minimize false positives** and consider **user privacy**.

OPERATING SYSTEM SECURITY

Group Policy

In Active Directory Domain Services

Provides policy-based control of Windows systems and domain settings through Group Policy Objects (GPOs).

Enables policy-based control of operating system, application, and user settings

SELinux

Security-Enhanced Linux is a Linux kernel-based security module that provides additional security capabilities and options

Implemented for multiple Linux distributions and Android, and used with embedded device apps

4.5 SECURE PROTOCOLS

PROTOCOL	TCP/UDP	PORT	USE CASES
Secure Shell (SSH)		22	Secure remote access (Linux and network)
Secure copy protocol (SCP)		22	Secure copy to Linux/Unix
SSH File Transfer Protocol (SFTP)		22	Secure FTP download
DNSSEC	TCP/UDP	53	Secure DNS traffic
Kerberos		88	Secure authentication
Simple Network Management Protocol version 3 (SNMP v3)	UDP	162	remote monitoring and configuration of SNMP entities (such as network devices)
Lightweight Directory Access Protocol over SSL (LDAPS)		636	Secure directory services information (e.g. - Active Directory Domain Services)
Hypertext Transport Protocol over TLS/SSL (HTTPS)		443	Secure web browsing
Transport Layer Security (TLS) / Secure Sockets Layer (SSL)		443	Secure data in transit
Internet Protocol Security (IPSec)	UDP	500	Secure VPN session between two hosts

Know the protocols and modes for IPSec

4.5 SECURE PROTOCOLS

PROTOCOL	TCP/UDP	PORT	USE CASES
Secure Simple Mail Transfer Protocol (SMTPS)		587	Secure SMTP (email)
Secure Internet Message Access Protocol (IMAP4)		993	Secure IMAP (email)
Secure Post Office Protocol 3 (POP3)		995	Secure POP3 (email)
Secure/Multipurpose Internet Mail Extensions (S/MIME)		993	Encrypt or digitally sign email
File Transfer Protocol, Secure (FTPS)		989/990	Download large files securely
Remote Desktop Protocol (RDP)		3389	Secure remote access
Session Initiated Protocol (SIP)		5060/5061	Signaling and controlling in Internet telephony for voice and video
Secure Real Time Protocol (SRTP)		5061	Encryption, message auth, and integrity for audio and video over IP networks

For the exam, grouping by use case may be helpful in memorization

IPSec Protocols

Authentication Header (AH) and **Encapsulating Security Payload (ESP) protocols**

AH protocol provides a mechanism for authentication only.

Because AH does not perform encryption, it is faster than ESP.

ESP protocol provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection).

ESP can be used with confidentiality only, authentication only, or both confidentiality and authentication.

IPSec Modes

In **transport mode**, the IP addresses in the outer header are used to determine the IPsec policy that will be applied to the packet.

It is good for ESP host-to-host traffic

In **tunnel mode**, two IP headers are sent. The inner IP packet determines the IPsec policy that protects its contents.

It is good for VPNs, and gateway-to-gateway security.

Characteristics of a secure protocol

Confidentiality. Ensures only authorized parties can access the information being transmitted.

This is often achieved through encryption.

Integrity. Guarantees that data is not tampered with during transmission.

May use digital signatures to detect any unauthorized modifications

Authentication. Verifies the identity of the parties involved in the communication.

Can involve user or machine authentication

Non-repudiation. Prevents any party from denying their involvement in a transaction.

Digital signatures can be used to achieve non-repudiation, where the sender cannot deny sending the message.

Availability. Ensures the system or resource is accessible to authorized users when needed.

Involves measures like redundancy (having backup systems) and access control mechanisms to prevent unauthorized access

4.5 DNS FILTER

Intercepts DNS requests before they reach malicious websites, protecting users from online threats

How it works

Blocks malicious domains using a list of prohibited domains, subdomains, and hosts.

Replaces correct response with an alternate DNS response. May block and redirect to an internal site or allow access with a warning to user.

Benefits

Multiple benefits, including improved security posture, phishing protection, enhances content filtering.

Offers centralized management, and many solutions are cloud-based deployments. but monitor false positivies and response latency

EMAIL SECURITY - DKIM

What are the functions and benefits of **DomainKeys Identified Mail (DKIM):**

Function:

Acts like a digital signature for your emails.

DKIM attaches a cryptographic signature to outgoing emails.

This allows receiving servers to verify the email originated from your authorized mail server.

BENEFIT

Helps prevent email spoofing, where attackers forge email addresses to impersonate legitimate senders.

EMAIL SECURITY - SPF

Defines and verifies authorized senders

What are the functions and benefits of **Sender Policy Framework (SPF):**

Function:

Acts like a whitelist.

It publishes a list of authorized mail servers allowed to send emails on behalf of your domain.

Receiving servers can check the SPF record (in DNS) to see if the sender's IP address is authorized.

BENEFIT

Helps prevent email spoofing by verifying if the email originated from an authorized mail server.

EMAIL SECURITY - DMARC

What are the functions and benefits of Domain-based **Message Authentication Reporting and Conformance (DMARC):**

Function:

Tells receiving mail servers what to do with emails claiming to be from your domain (e.g., yourcompany.com).

DMARC HAS THREE ENFORCEMENT POLICIES

None (monitor): Tracks email activity but doesn't take action (for initial setup).

Quarantine: Quarantines emails failing SPF or DKIM checks for review.

Reject: Rejects emails failing SPF or DKIM checks entirely.

DKIM, SPF, and DMARC Together

These technologies work **TOGETHER** in a complementary fashion:

SPF and DKIM

Work together to verify the legitimacy of the sender's email address and message.

SPF verifies sender, **DKIM** verifies the message

DMARC

Leverages the information from SPF and DKIM to determine how to handle emails that fail authentication checks.

This multi-layered approach helps **ensure only authorized visitors (emails) reach your inbox.**

4.5 EMAIL GATEWAY

Acts acts as a security checkpoint for all incoming and outgoing emails within an organization's network

How it works

Uses filters and advanced detection techniques to identify and block emails containing malware (viruses, ransomware, etc.) and spam

This helps prevent these emails from reaching employees and potentially compromising systems or leading to phishing attacks.

Benefits

Acts as a critical first line of defense, significantly reducing the risk of these threats reaching your employees.

There are two actions we can take to reduce the risk of ransomware;
1) reduce malicious emails delivered 2) reduce employee clicks on them

4.5 FILE INTEGRITY MONITORING

FIM safeguards critical files and system configurations from unauthorized modification.

How it works

During initial setup, FIM creates a baseline (fingerprint) for each monitored file, often using a cryptographic hash function (MD5, SHA-256)

It then monitors to see if that fingerprint changes outside of our normal processes that update files, capture changes, and update fingerprints.

Benefits

Multiple benefits, including improved security posture, faster incident response, reduced downtime, and improved audit trails.

Great for monitoring the integrity of system files and sensitive data.
It serves as a measure of configuration management/enforcement

DATA LOSS PREVENTION (DLP)

DLP

Data Loss Prevention

is a way to protect sensitive information and prevent its inadvertent disclosure

can identify, monitor, and automatically protect sensitive information in documents

monitors for and alerts on for potential breaches & policy violations like oversharing

Policy actions include **applying sensitivity labels**, **blocking access**, or **user notifications (policy tips)** to offer guidance on sensitive data handling.

DATA LOSS PREVENTION (DLP)

DLP

Data Loss Prevention

is a way to protect sensitive information and prevent its inadvertent disclosure

can identify, monitor, and automatically protect sensitive information in documents

monitors for and alerts on for potential breaches & policy violations like oversharing

Policies can be typically applied to email, SharePoint, cloud storage, removeable devices, and databases

DATA LOSS PREVENTION (DLP)

DLP

Data Loss Prevention

is a way to protect sensitive information and prevent its inadvertent disclosure.

can identify, monitor, and automatically protect sensitive information in documents

monitors for and alerts on for potential breaches & policy violations like oversharing

Protection travels with the document, file, or other data, preventing local override of DLP protections

NETWORK ACCESS CONTROL

SCENARIO: A desktop or laptop off the network for an extended period may need multiple updates upon return.

After a remote client has authenticated, **Network Access Control** (**NAC**) checks that the device being used is patched and compliant with corporate security policies.

A compliant device is allowed access to the LAN.

A non-compliant device may be redirected to a boundary network where a remediation service address issues

Boundary network is sometimes called a "quarantine network"

NETWORK ACCESS CONTROL

Agent-based or agentless

Some operating systems include network access control as part of the operating system itself. And no additional agent is required.

These generally perform checks when the system logs into the network and logs out of the network, making them less configurable.

If you need additional functionality, you may require a persistent or dissolvable agent.

Persistent: A permanent agent is installed on the host.

Dissolvable: A dissolvable agent is known as temporary and is installed for a single use.

EXTENDED DETECTION AND RESPONSE

Leverages AI, ML, and threat intelligence

XDR

e**X**tended **D**etection and **R**esponse

Integrates security visibility across an organization's entire infrastructure

Provides visibility into endpoints, cloud infrastructure, mobile devices, apps. etc.

Supports proactive threat hunting and can respond automatically to identified threats.

EDR is focused on protecting the endpoint, providing in-depth visibility and threat prevention for a particular device.

XDR takes a wider view, integrating security across endpoints, cloud computing, email, and other solutions.

USER BEHAVIOR ANALYTICS (UBA)

UBA is roughly equivalent to User Entity Behavior Analytics (UEBA)

A cybersecurity technique that analyzes user activity within a network or system to identify potentially malicious or risky behavior.

It focuses on understanding what constitutes "normal" user activity and then flagging deviations from that baseline as potential threats.

How it Works:

UBA systems collect data on user activities from various sources, including:

- Login and logout times
- File access and changes
- Network traffic patterns
- Application and device usage
- Data downloads and uploads

Notice "apps and devices" in the list?

Those are "entities"

USER BEHAVIOR ANALYTICS (UBA)

Data is then analyzed **using statistical methods**, **machine learning algorithms**, and **historical baselines**

UBA looks for anomalies or suspicious patterns that might indicate:

Compromised accounts

If a user logs in from an unusual location or time, or accesses unauthorized files, it could indicate a compromised account.

Insider threats

e.g. mass upload, download, or deletion

UBA can identify unusual activity patterns for employees, identifying anomalies that indicate potentially malicious insider behavior.

Malware infections

Malware can exhibit specific behaviors like unusual network traffic or file access patterns. UBA can help detect these anomalies.

USER BEHAVIOR ANALYTICS (UBA)

Goals and Benefits:

Early detection of security threats

By identifying suspicious activity early, security teams can investigate and respond before any damage occurs.

Reduced false positives

UBA focuses on user behavior patterns, leading to fewer alerts compared to traditional security tools that rely solely on signatures.

Improved investigation efficiency

UBA provides valuable context about user activity, helping security teams investigate potential threats more efficiently.

UBA can make security investigation and detection **more proactive**, **more accurate**, and **more efficient** (lower effort).

4.0 SECURITY OPERATIONS

4.6 Given a scenario, implement and maintain identity and access management

- **Provisioning/de-provisioning user accounts**
- **Permission assignments and implications**
- **Identity proofing**
- **Federation**
- **Single sign-on (SSO)**
  - Lightweight Directory Access Protocol (LDAP)
  - Open authorization (OAuth)
  - Security Assertions Markup Language (SAML)
- **Interoperability**
- **Attestation**
- **Access controls**
  - Mandatory
  - Discretionary
  - Role-based
  - Rule-based
  - Attribute-based
  - Time-of-day restrictions
  - Least privilege
- **Multifactor authentication**
  - Implementations
    - Biometrics
    - Hard/soft authentication tokens
    - Security keys
  - Factors
    - Something you know
    - Something you have
    - Something you are
    - Somewhere you are
- **Password concepts**
  - Password best practices
    - Length
    - Complexity
    - Reuse
    - Expiration
    - Age
  - Password managers
  - Passwordless
- **Privileged access management tools**
  - Just-in-time permissions
  - Password vaulting
  - Ephemeral credentials

Provisioning and Deprovisioning

Provisioning

Least privilege, identity proofing

Creating new user accounts with appropriate access levels based on their job function at onboarding.

This can be automated/templated for efficiency/accuracy.

Deprovisioning

Immediately at separation (timing is key)

Disabling or deleting user accounts when employment ends or roles change.

Prevents unauthorized access after someone leaves the company.

PERMISSION ASSIGNMENT AND IMPLICATIONS

User

Direct assignment of permissions to a user can ensure least privilege assignment.

Increases risk of permissions creep and management effort when users change roles

Group

More efficient than direct assignment to users

Offers a way to simplify permission management for sets of users with similar needs.

Role

A more dynamic and flexible approach vs groups

Defined by the tasks or responsibilities a user has within the organization.

Offers a more functional approach to permission management.

IDENTITY PROOFING

Knowledge-Based Authentication (KBA)

This is normally used by banks, financial institutions, or email providers to identify someone when they want a password reset.

There are two different types of KBA, dynamic and static, and they have their strengths and weaknesses:

Static KBA: These are questions that are common to the user.

For example, *"What is the name of your first school?"*

Dynamic KBA: These are deemed to be more secure because they do not consist of questions provided beforehand.

Example: confirm identity, a bank may ask the customer to name three direct debit mandates, the date, and the amount paid.

IDENTITY PROOFING

KBA may also be used to help confirm a new user's identity when they are creating an account for the first time.

This process is known as **identity proofing**.

Sometimes referred to as identity verification, confirms a person claiming a particular identity is actually who they say they are.

Common methods include:

- document verification
- knowledge-based verification
- biometric verification
- out-of-band verification (SMS, phone, or email)

Key aspects of identity proofing **verifying claimed identity**, **validating documentation**, and **matching identity**

4.6 FEDERATION

Federation is a collection of domains that have **established trust**

The level of trust may vary, but typically includes authentication and almost always includes authorization.

Often includes a number of organizations that have established trust for shared access to a set of resources.

Example

You can federate your on-premises environment with cloud identity providers and use this federation for authentication and authorization.

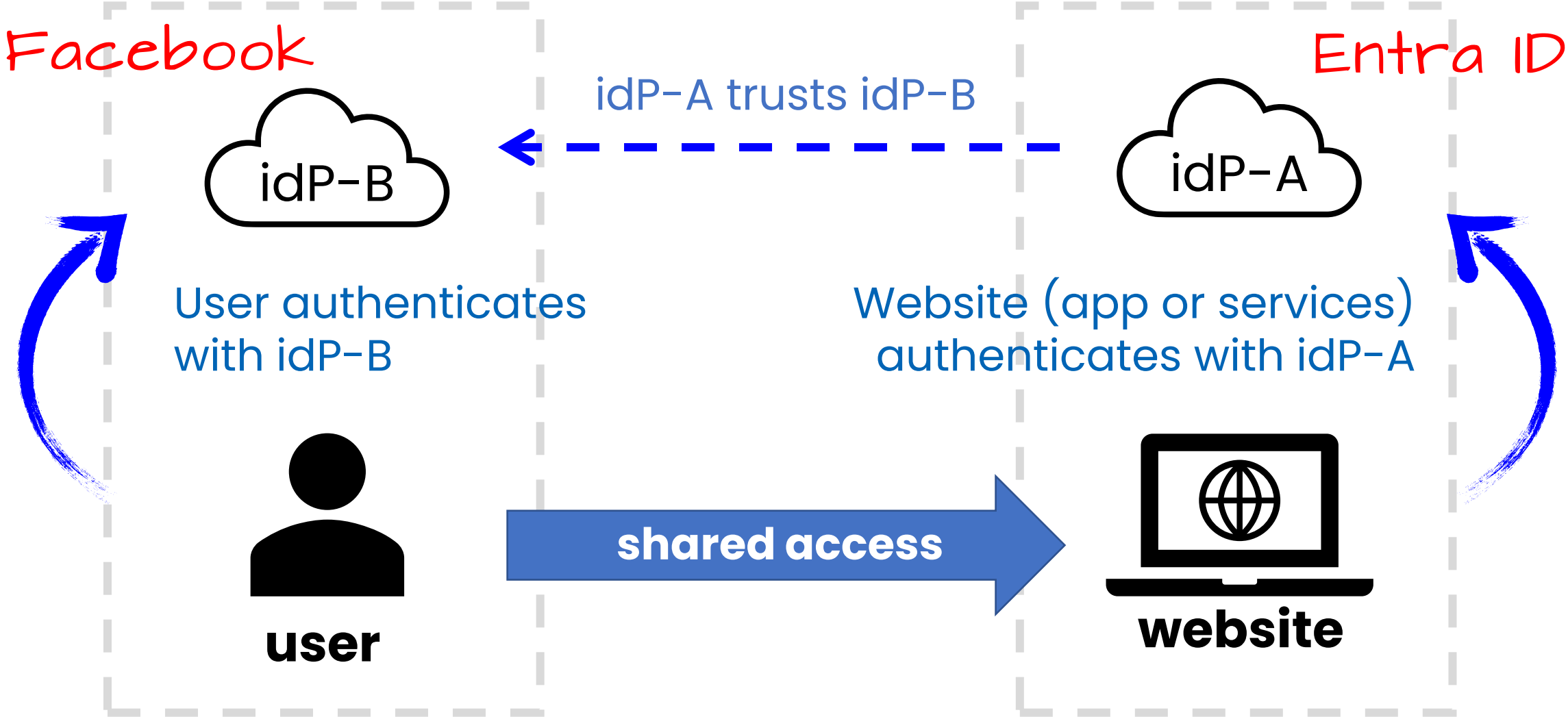
This sign-in method then ensures that all user authentication occurs on-premises.

Allows administrators to implement more rigorous levels of access control.

Certificate authentication, key fob, card token

IDENTITY FEDERATION (EXAMPLE)

may be cloud or on-premises



trust is not always bi-directional

SINGLE SIGN-ON

Single Sign-on (SSO)

Single sign-on means a user doesn't have to sign into every application they use.

SINGLE SIGN-ON

Single Sign-on (SSO)

Single sign-on means a user doesn't have to sign into every application they use.

The user logs in once and that credential is used for multiple apps.

SINGLE SIGN-ON

Single Sign-on (SSO)

Single sign-on means a user doesn't have to sign into every application they use.

The user logs in once and that credential is used for multiple apps.

Single sign-on based authentication systems are often called "**modern authentication**".

SINGLE SIGN-ON

Security Assertion Markup Language (SAML)

an XML-based, open-standard data format for exchanging authentication and authorization data between parties,

in particular, between an **identity provider** (Active Directory, Entra ID) and a **service provider** (the app or service).

Common in on-premises federation scenarios

OAuth 2.0 Open Authorization

is an open standard for **authorization**, commonly used as a way for Internet users to log into third party websites using their social identities without exposing their password.

Microsoft, Google, Facebook, Twitter, etc

Directory Services

used to store, retrieve, and manage information about objects, such as user accounts, computer accounts, mail accounts, and information on resources

LDAP is a common protocol for a directory service (used by Microsoft's Active Directory)

Directory Services

used to store, retrieve, and manage information about objects, such as user accounts, computer accounts, mail accounts, and information on resources

LDAP = Lightweight Directory Access Protocol

Directory Services

is coupled with an authentication service to authenticate entities (users, computers, etc.) attempting to access resources

Kerberos is an example of protocol for authentication (used by Microsoft's Active Directory)

DIRECTORY SERVICES

Active
Directory

a set of directory services developed by Microsoft as part of Windows 2000 for **on-premises domain-based networks**.

gives organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.

does ***not*** natively support mobile devices, SaaS or LOB apps that require **modern authentication**.

AD domains can scale from a single server (called a domain controller) into the hundreds of servers as the organization grows and needs to scale.

DIRECTORY SERVICES

Kerberos

The authentication protocol for an Active Directory domain

To access a service, the client requests an authentication ticket

An authentication server checks the client's credentials and responds with a ticket

When the client wants to use a service, it uses this ticket to request resource access

Prevents replay attacks by using **timestamps** ensuring that authentication messages are fresh and haven't been intercepted and reused by an attacker

Interoperability

In the context of identity management, interoperability is about ensuring identity providers and applications can work together seamlessly

Especially important in federation and single-sign on scenarios

Attestation

One of the conditions to access corporate resources may require the access request to originate from an approved, managed device.

Attestation is the process of confirming the device (laptop, mobile device, etc) is an approved device compliant with company policies.

Remote attestation involves checks that occur on a local device and are reported to a verification server. as with an MDM solution

Generally, includes validation of a unique identifier for the hardware that confirms the device is known.

Device attestation is common in zero trust architecture

Hardware Root of Trust

A line of defense against executing unauthorized firmware on a system

And when certificates are used in FDE, they use a hardware root of trust for key storage.

It verifies that the keys match before the secure boot process takes place

A **Trusted platform module (TPM)** is an implementation of hardware root of trust.

Trusted Platform Module

A chip that resides on the motherboard of the device.

Multi-purpose, like storage and management of keys used for full disk encryption (FDE) solutions.

Examples: Bitlocker (Windows) dm-crypt (Linux)

Provides the operating system with access to keys, but prevents drive removal and data access

For the exam, know that the TPM provides secure storage of cryptographic keys to support ***secure boot*** and ***full disk encryption***.

4.6 ACCESS CONTROL

Object = resource
Subject = user

Non-discretionary Access Control

Enables the enforcement of system-wide restrictions that override object-specific access control. RBAC is considered non-discretionary

Discretionary Access Control (DAC)

Use-based, user-centric

A key characteristic of the Discretionary Access Control (DAC) model is that every object has an owner, and the owner can grant or deny access to any other subject.

Example: New Technology File System (NTFS) on Windows

Role Based Access Control (RBAC)

Typically mapped to job roles.

User accounts are placed in roles or groups.

Admins assign access through the roles and groups rather than to users directly.

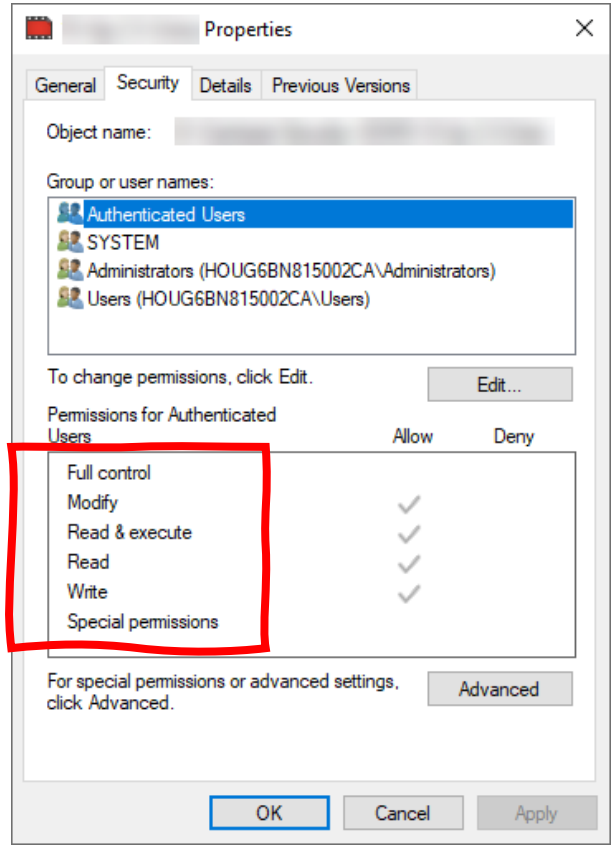
Rule-based access control

A key characteristic is that it applies global rules that apply to all subjects. Rules within this model are sometimes referred to as **restrictions** or **filters**.

Example: a firewall uses rules that allow or block traffic to all users equally.

NTFS permissions (Windows)

Are applied to every file and folder stored on a volume with NTFS file system



An example of a **discretionary access control (DAC)** system

Every object (file, folder) includes a **discretionary access control list (DACL)**

The DACL is a list of **Access Control Entries (ACEs)**

DAC specifies every object have an owner who has full control

MANDATORY ACCESS CONTROL

a model in which every object and every subject has one or more labels.

These labels are predefined, and the system determines access based on assigned labels

ATTRIBUTE-BASED ACCESS CONTROL

access is restricted based on an attribute on the account, such as department, location, or functional designation.

For example, admin my require user accounts have the 'Legal' department attribute to view contracts

ACCESS CONTROLS

Time-based logins

May be established for users based on role as a company may have many different shift patterns.

Employers may not wish their employees to access their network outside of their working hours.

For example, employees may be restricted to accessing the network between 7 am and 6 pm.

This prevents data theft by preventing users from coming in at 3 a.m. when nobody is watching and stealing corporate data.

Can be effective in preventing individual fraud, as well as collusion, by enforcing restrictions of schedule rotations.

Common in some industries, such as financial services, with shift workers in sensitive roles

ACCESS CONTROLS

Least Privilege

a subject should be given only those privileges necessary to complete their job-related tasks.

Can prevent or limit scope of security incidents and data theft

Need to know

data access is restricted unless one has a specific need to know.

meaning access to the information must be necessary for one to conduct one's official duties.

May result in a user being denied access even if the user has security clearance

ACCESS CONTROLS

Need-to-know and the principle of **least privilege** are two standard IT security principles implemented in secure networks.

They limit access to data and systems so that users and other subjects have access only to what they require.

They help prevent security incidents

They help limit the scope of incidents when they occur.

When these principles are not followed, security incidents **result in far greater damage** to an organization.

MULTIFACTOR AUTHENTICATION (MFA)

MFA

MFA works by requiring two or more of the following authentication methods:

MFA FACTORS AND ATTRIBUTES

MFA

Something you **know** (pin or password)

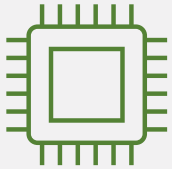
Something you **have** (trusted device)

Something you **are** (biometric)

Authenticator app

Voice call

SMS (text msg)



HW auth token

MFA ATTRIBUTES

Somewhere you are

Your expected location, such as the company office, your home or home city.

Something you can do

such as writing your signature.

Something you exhibit

The personalized manner you perform an action, such as your gait (the way you walk).

Someone you know

Responding to challenge with knowledge of a characteristic of a specific individual you know.

BIOMETRICS

a method of authentication using an **individual's physical characteristics**, which are unique to the individual.

Fingerprint Scanner

Fingerprint scanners are now very common, and used not only in MFA, but various travel, financial, and legal situations.

Retina Scanner

With appropriate lighting, the retina can be accurately identified as the blood vessels of the retina absorb light more readily than the surrounding tissue.

BIOMETRICS

a method of authentication using an **individual's physical characteristics**, which are unique to the individual.

Iris Scanner
Confirms the identity of the user by scanning of their iris.

Both retina and iris scanners are physical devices.

Voice Recognition
The voice patterns can be stored in a database and used for authentication.

BIOMETRICS

a method of authentication using an **individual's physical characteristics**, which are unique to the individual.

Vein

Using blood vessels in the palm can be used as a biometric factor of authentication.

Gait Analysis

gait is the way an individual walks. Identification and/or authentication using gait is possible even with lower resolution video

Biometric authentication is common today, but still may raise privacy concerns that should be addressed

BIOMETRICS

a method of authentication using an **individual's physical characteristics**, which are unique to the individual.

Facial Recognition

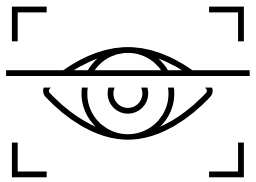
Looks at the shape of the face and characteristics such as mouth, jaw, cheekbone, and nose.

Light and angle/direction can be a factor, especially in software.

Microsoft facial recognition, called **Windows Hello**, was released with Windows 10.

It uses a special USB infrared camera and, as such, is better than other facial recognition programs that can have problems with light.

BIOMETRICS



Crossover Error Rate

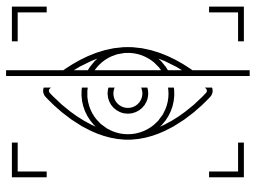
Biometric methods identify users based on characteristics such as fingerprints.

The **crossover error rate (CER)** identifies the accuracy of a biometric method.

It shows where the false rejection rate is equal to the false acceptance rate.

To move the CER higher or lower, you can increase or decrease the sensitivity of the biometric device.

BIOMETRICS



Crossover Error Rate

A **false acceptance** occurs when an invalid subject is authenticated. Type 2 error

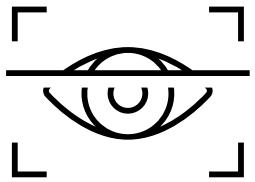
Sometimes called a false positive authentication.

A **false rejection** occurs when a valid subject is rejected. Type 1 error

Sometimes called a false negative authentication.

False rejection is undesirable, but false acceptance is worse

BIOMETRICS



Crossover Error Rate

A **false acceptance** occurs when an invalid subject is authenticated. Type 2 error

Sometimes called a false positive authentication.

A **false rejection** occurs when a valid subject is rejected. Type 1 error

Sometimes called a false negative authentication.

For the exam, remember **FAR=false acceptance rate** and **FRR=false rejection rate**.

HARD/SOFT TOKENS

TOTP

Time-based **O**ne-**T**ime **P**assword

is based on HOTP but where the moving factor is time instead of the counter.

uses time in increments called the timestep, which is usually 30 or 60 seconds.

each OTP is valid for duration of the timestep

HMAC

HMAC-based **O**ne-**T**ime **P**assword

aka "HOTP"

uses a keyed-hash message authentication code, or an HMAC

relies on two pieces of info: the seed, a secret known only by the token and validating server

the second is a moving factor – a counter.

HARD/SOFT TOKENS

What is an OATH token and how does it work?

OATH (Open Authentication) is an open standard that specifies how time-based, one-time password (TOTP) codes are generated.

Soft Authentication Tokens

Are typically applications. Identify provider generates the secret key, or seed, that's input into the app and used to generate each OTP.

Hard Authentication Tokens

Small hardware devices that look like a key fob that displays a code that refreshes every 30 or 60 seconds, with secret key/seed pre-programmed.

HARD/SOFT TOKENS

Authentication applications

"Authenticator apps"

is a software-based authenticator that implements two-step verification services using the Time-based One-time Password Algorithm and HMAC-based One-time Password algorithm, for authenticating users of software applications.

Examples include Microsoft Authenticator and Google Authenticator.

Authenticator apps from companies like Microsoft and Google generate one-time passcodes using open standards developed by the **Initiative for Open Authentication (OATH)**.

You'll hear HMAC and TOTP tokens called OATH tokens with some of these providers.

Push notifications

Where the server is pushing down the authentication information to your mobile device.

Uses the mobile device app to be able to receive the pushed message and display the authentication information.

These apps are available on iOS and Android

AUTHENTICATION MANAGEMENT

Security Key | looks like a USB device and works in conjunction with your password to provide multi-factor authentication

One example is YubiKey is a FIPS 140-2 validation that provides code storage within a tamper-proof container

4.6 PASSWORD BEST PRACTICES

Complexity

Complex passwords (sometimes known as strong passwords) are formatted by choosing at least three of the following four groups:

lowercase (a, b, and c), **uppercase** (A, B, and C), **numbers** (1, 2, and 3), **special characters** ($, @)

Length

Longer passwords are more secure (ideally 12+ characters).

Reuse = History

Prevents someone from reusing the same password. For example, if number remembered is 12 passwords, only on 13th change could it be reused.

Age

Passwords should have a minimum age, so they cannot work around the reuse restriction.

With history of 12, minimum age of 1 day means 13 days to return to original password

PASSWORD MANAGER

Password Manager

designed to help users create, store, and manage secure passwords.

stored locally, uses strong encryption (e.g. AES-256) to protect secrets in the vault.

support storing additional info, like expiration, notes, and URLs.

Examples include LastPass, KeePass, and 1Password

Windows, macOS, and web browsers (Chrome, Edge) also provide password managers.

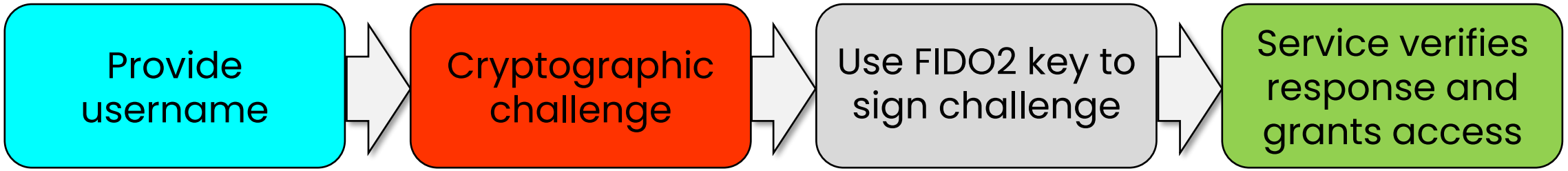
FIDO2/PASSWORDLESS

What is FIDO2 and how does it work?

Uses public-key (asymmetric) cryptography for user authentication

User has a physical device (USB or NFC)

Authentication sequence



Windows Hello for Business

An authentication feature built into Windows 10+, replaces passwords with strong two-factor authentication on PCs and mobile devices.

Passwordless

Allows users authenticate to:

- A Microsoft account
- An Active Directory account
- An Entra ID account
- Identity Provider Services OR
- Relying party services that support Fast ID Online (FIDO) v2.0 authentication

Windows Hello is for personal devices and uses a pin or biometric gesture

WH4B Uses asymmetric keys (on TPM) that require a user gesture (PIN or biometrics) to authenticate.

PASSWORDLESS

Solves the following problems

- Strong passwords can be difficult to remember, and users often reuse passwords on multiple sites.
- Server breaches can expose symmetric network credentials (passwords).
- Passwords are subject to replay attacks.
- Users can inadvertently expose their passwords due to phishing attacks.

Reduces phishing exposure

PRIVILEGED ACCESS MANAGEMENT TOOLS

Privileged Access Management

allows an organization to apply more stringent security controls over accounts with elevated privileges

e.g. admin or root-level accounts

Just-in-time PERMISSIONS

a concept in which administrators request activation of administrative privilege when they are needed

The activation expires and privileges are revoked after a set period of time.

PRIVILEGED ACCESS MANAGEMENT TOOLS

Password Vaulting

allows users to access privileged accounts without needing to know a password.

often allows privileged credentials to be checked out as needed.

ensures that passwords are available for emergencies and outages

Password vaulting is sometimes used with **Privilege Access Management (PAM)** solutions.

PRIVILEGED ACCESS MANAGEMENT TOOLS

Ephemeral Credentials

Ephemeral credentials automatically expire after a brief period—usually just a few minutes.

They are commonly used in scenarios where temporary, time-bound access is required.

Often used in PAM scenarios where short-lived credentials are needed.

FOR THE EXAM: ephemeral credentials enhance security by minimizing the exposure window for unauthorized access

4.0 SECURITY OPERATIONS

4.7 Explain the importance of automation and orchestration related to secure operations

- **Use cases of automation and scripting**
  - User provisioning
  - Resource provisioning
  - Guard rails
  - Security groups
  - Ticket creation
  - Escalation
  - Enabling/disabling services and access
  - Continuous integration and testing
  - Integrations and Application programming interfaces (APIs)
- **Benefits**
  - Efficiency/time saving
  - Enforcing baselines
  - Standard infrastructure configurations
  - Scaling in a secure manner
  - Employee retention
  - Reaction time
  - Workforce multiplier
- **Other considerations**
  - Complexity
  - Cost
  - Single point of failure
  - Technical debt
  - Ongoing supportability

ORCHESTRATION & AUTOMATION

Orchestration

Manages automated tasks to form complete workflows

Focuses on enhancing overall security posture.

EXAMPLES:

- Incident response
- Orchestrating actions across tools in incident response
- Automating end-to-end security workflow

Automation

Involves mechanizing a single process or a few related tasks

Reducing manual effort and improving efficiency.

EXAMPLES:

- Patch management
- Scanning for malware and creating reports
- Resetting user passwords or changing group memberships

ORCHESTRATION & AUTOMATION

Orchestration

Process-level, coordination and integration across tools

SOAR - Security Orchestration, Automation, and Response

Automation

Task-level, usually single tool, often simple scripts

4.7 USE CASES

There are common use cases for automation and scripting in security operations that benefits most orgs.

- ☑ User provisioning
- ☑ Resource provisioning
- ☑ Guard rails
- ☑ Security groups
- ☑ Ticket creation
- ☑ Escalation
- ☑ Enabling/disabling services and access
- ☑ Continuous integration and testing
- ☑ Integrations and APIs

USE CASES

User provisioning

Automating user provisioning (and potentially deprovisioning) ensures that access control is maintained efficiently and securely.

Can help prevent unauthorized access and maintain the principle of least privilege.

Resource provisioning

Automation can be used to create, configure, and decommission resources like virtual machines, storage, and networks.

Helps maintain a standardized, secure environment while reducing the potential for human error and configuration drift.

Guardrails

Sets acceptable boundaries without human review

Automated guardrails can enforce security policies and ensure that security best practices are consistently followed

USE CASES

Escalation

Automation can be used to escalate security incidents or events.

Automation can route to appropriate personnel or teams based on predetermined criteria, improving response times.

Faster response reduces the potential impact of security threats

Ticket creation

Automated ticket creation can be used to streamline incident response processes.

Ensures that issues are quickly reported and assigned to the appropriate teams for resolution.

Security groups

Can prevent "permissions creep"

Automation can be used to manage security groups.

Ensures that access controls are consistently applied and updated.

USE CASES

Enabling/disabling services and access

Automation can be employed to enable or disable services or access.

Can help maintain a secure environment by limiting unnecessary access and reducing potential attack surfaces

Continuous integration and testing

Automation is crucial for continuous integration and testing processes.

Ensures that code is consistently reviewed, tested, and deployed in a secure manner. Can help prevent the introduction of vulnerabilities

Integrations and APIs

Automation can be used to integrate various security tools and platforms, enabling real-time communication and orchestration.

Tools with standards-based APIs (REST, etc.) ensure interoperability, but is a feature you should verify before adoption

4.7 BENEFITS

Automation and orchestration can deliver several benefits to security operations and the organization.

- ☑ Efficiency/time saving
- ☑ Enforcing baselines
- ☑ Standard infrastructure Configurations
- ☑ Scaling in a secure manner
- ☑ Employee retention
- ☑ Reaction time
- ☑ Workforce multiplier

Benefits to our costs, our people, and our security posture

BENEFITS

Efficiency/time saving

Know automation ROI before you build

Can significantly reduce the time required for various tasks.

Automating high-frequency, high-effort tasks allows IT and security teams to focus on more strategic and high-value activities

Enforcing baselines

Remember "configuration enforcement"?

Automation enables the consistent enforcement of security baselines and policies across an organization's infrastructure.

Ensures all systems and applications are configured in a secure manner and that any deviations are quickly addressed.

Standard infrastructure configurations

Automation enables organizations to maintain standard configurations that adhere to security best practices.

BENEFITS

Scaling in a secure manner

Automation allows organizations to scale their operations securely and efficiently.

Can ensure that security measures are consistently applied and maintained without the need to grow staff.

Employee retention

Automating repetitive and time-consuming tasks can increase job satisfaction by enabling employees to focus on more engaging and strategic work.

Can contribute to higher employee retention rates and a more motivated workforce.

BENEFITS

Reaction time

Automation can help improve an organization's reaction time to security incidents and vulnerabilities.

Can more quickly detect, report, and address issues, minimizing the potential impact and reduce response time.

Workforce multiplier

Can act as a workforce multiplier, allowing IT/security teams to manage more systems and processes without the need for additional personnel.

Can result in cost savings and a more efficient allocation of resources.

4.7 OTHER CONSIDERATIONS

Automation and orchestration can bring negative consequences if the org doesn't avoid these pitfalls

- ☑ Complexity
- ☑ Cost
- ☑ Single point of failure
- ☑ Technical debt
- ☑ Ongoing supportability

These are all potential impacts to consider in the envisioning/design phase

Avoiding these pitfalls is key to automation that is **supportable**, **maintainable,** and **cost effective** for the long-term.

OTHER CONSIDERATIONS

Complexity

Make sure you have the skills on staff or on contract

Implementing automation and scripting can add complexity to an organization's infrastructure and processes.

Ensure that the added complexity is manageable and that it does not introduce new vulnerabilities or challenges

Cost

Subscription automation platforms can eat into your savings

Can lead to cost savings in the long run, but the initial investment in tools, infrastructure, and training may be significant.

Organization should carefully weigh the costs and benefits before embarking on an automation project.

Single point of failure

Establish redundancies so you can fall back

Over-reliance on a single automation tool/platform or scripting can create a single point of failure in some cases.

OTHER CONSIDERATIONS

Technical debt

Plan for regular updates/reviews to mitigate risk

As tools evolve, there may be a need to update or replace existing scripts and integrations.

Can result in technical debt, where outdated or poorly maintained scripts or runbooks cause issues or vulnerabilities

Ongoing supportability

Ensure solutions are maintainable and supportable to deliver long-term success.

This includes training, documentation, monitoring, and updating.

Consider the resources required to maintain before you start

4.0 SECURITY OPERATIONS

4.8 Explain appropriate incident response activities

- **Process**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- **Training**
- **Testing**
  - Tabletop exercise
  - Simulation
- **Root cause analysis**
- **Threat hunting**

Digital forensics
- Legal hold
- Chain of custody
- Acquisition
- Reporting
- Preservation
- E-discovery

The 7 phases of incident response

4.8 PROCESS

Represents the phases of incident response

1	**Preparation**	Where incident response plans are written, and configurations documented, team is formed.
2	**Detection**	Monitoring events, using tools like SIEM, SOAR, XDR, IDS/IPS, and UEBA to identify potential incidents.
3	**Analysis**	Analyzing detected events to verify if the events identify an actual incident. Is it really an incident?
4	**Containment**	Limiting damage (scope) of the incident declared in the Analysis phase.
5	**Eradication**	Once affected systems are identified, coordinated isolation or shutdown, rebuild, and notifications.
6	**Recovery**	Root cause is addressed and time to return to normal operations is estimated and executed.
7	**Lessons Learned**	Helps prevent any recurrence, improve IR process. Includes **root cause analysis** to identify source of failure.

Important terminology

1. Preparation
2. Detection
3. **Analysis**
4. Containment
5. Eradication
6. Recovery
7. Lessons Learned

Analyzing detected events to verify if the events identify an actual incident. Is it really an incident?

Important terminology

1. Preparation
2. Detection
3. **Analysis**
4. Containment
5. Eradication
6. Recovery
7. Lessons Learned

Triage

The initial assessment and prioritization of an incident.

Determining the severity and scope of the incident.

Important terminology

1. Preparation
2. Detection
3. Analysis
4. **Containment**
5. Eradication
6. Recovery
7. Lessons Learned

Limiting damage (scope) of the incident declared in the Analysis phase.

Important terminology

1. Preparation
2. Detection
3. Analysis
4. **Containment**
5. Eradication
6. Recovery
7. Lessons Learned

Containment

Attempts to limit and control the incident from spreading.

Example: disconnecting infected hosts from the network.

Mitigation

Steps taken to reduce the severity of the incident.

Where the org begins to take actions necessary to fix the incident

Important terminology

1.
2. Detection
3. Analysis
4. Containment
5. **Eradication**
6. Recovery
7. Lessons Learned

Once affected systems are identified, coordinated isolation or shutdown, rebuild, and notifications.

Important terminology

Eradication

Removing artifacts of the incident like malware and backdoors.

Example: completely wiping and reinstalling compromised systems.

Important terminology

Root cause is addressed and time to return to normal operations is estimated and executed.

Important terminology

Recovery

Restoring affected systems and services back to normal operations.

Addresses the root cause(s) of the incident.

Example: restoring data from backups and bringing production systems back online.

Returning the environment back to its previous normal state

4.8 TRAINING

An **incident response team** is composed of employees with expertise in different areas.

Together, they have the knowledge and skills to respond to an incident, which often come through extensive training.

Training includes concepts such as how to:

- identify and validate an incident
- triage, communicate, and contain incidents
- to collect and protect evidence
- recover from an incident

Investigators also learn how to become better prepared by **retrospectively analyzing the incident**, and reporting on findings.

Types of **incident response exercises**

Tabletop

Paper-based, hypothetical

You distribute copies of incident response plans to the members of the incident response team for review.

The team walks through the plan for a specific incident.

Team members then provide feedback about any updates needed to keep the plan current.

Simulation

Similar to tabletop exercise, except some of the response measures are then tested (on non-critical functions).

This one involves some form of 'doing'

ROOT CAUSE ANALYSIS

Process that focuses on identifying the underlying cause for an issue or compromise.

Aims to identify how to fix the underlying problems that allowed the event or incident to occur.

Ensures that any systemic issues that led to the problem are also addressed.

Findings will be captured in a report for stakeholders, and should include actionable recommendations

GOAL: to learn from the incident and prevent future recurrence of a similar incident.

THREAT HUNTING

A process of proactively and regularly seeking out cybersecurity threats inside your network from attackers and malware threats.

Intelligence Fusion

involves industry and government

Fusion centers in the US and abroad play an important role in countering cyber threats, attacks, and crime through gathering, analyzing, aggregating, and sharing threat information.

Threat Feeds

Threat intelligence feeds

Enable organizations to stay informed about indicators of compromise (IoCs) related to various threats that could adversely affect the network.

Threat hunters operate under the "presumption of compromise"

THREAT HUNTING

A process of proactively and regularly seeking out cybersecurity threats inside your network from attackers and malware threats.

Intelligence Fusion

involves industry and government

Fusion centers in the US and abroad play an important role in countering cyber threats, attacks, and crime through gathering, analyzing, aggregating, and sharing threat information.

Threat Feeds

Threat intelligence feeds

Enable organizations to stay informed about indicators of compromise (IoCs) related to various threats that could adversely affect the network.

Threat intelligence feeds often integrate with security tools

THREAT HUNTING

A process of proactively and regularly seeking out cybersecurity threats inside your network from attackers and malware threats.

Advisories and Bulletins

Advisories and security bulletins provide good advice on how to keep your company safe.

The advisories tend to be released by government-funded agencies.

Bulletins tend to be released by vendors or private companies.

4.8 DIGITAL FORENSICS

Legal Hold

protecting any documents that can be used in evidence from being altered or destroyed.

sometimes called litigation hold

Chain of Custody

tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle

documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Confirms appropriate collection, storage, and handling

Requirements for evidence to be **admissible in a court of law**:

TO BE ADMISSIBLE:

Evidence must be relevant to a fact at issue in the case. makes a fact more or less probable than without the evidence

The fact must be material to the case. Is important in proving a case

The evidence must be competent or legally collected. competent means "reliable" here

Must be obtained by legal means.

To prevail in court, evidence must be **sufficient**, which means “convincing without question, leaving no doubt”

Importance of collecting

EVIDENCE

As soon you discover an incident...

You must begin to collect evidence and as much information about the incident as possible.

Evidence can be used in a subsequent legal action or in finding attacker identity.

Evidence can also assist you in determining the extent of damage.

Areas and considerations in **evidence acquisition**.

Disk aka hard drive. Was the storage media itself damaged?

Random-access memory (RAM). Volatile memory used to run applications.

Swap/Pagefile. used for running applications when RAM is exhausted.

OS (operating system). Was there corruption of data associated with the OS or the applications?

Device. When the police are taking evidence from laptops, desktops, and mobile devices they take a complete system image.

The original image is kept intact, installed on another computer, hashed, then analyzed to find evidence of any criminal activity.

4.8 DIGITAL FORENSICS

Firmware. embedded code, could be reversed engineered by an attacker, so original source code must be compared to code in use.

a coding expert to compare both lots of source code in a technique called regression testing. rootkits and backdoors are concerns

Snapshot. If the evidence is from a virtual machine, a snapshot of the virtual machine can be exported for investigation.

Cache. special high-speed storage that can be either a reserved section of main memory or an independent high-speed storage device.

memory cache AND disk cache, both are volatile

Network. OS includes command-line tools (like netstat) that provide information that could disappear if you reboot the computer.

Like RAM, connections are volatile and lost on reboot.

Artifacts. any piece of evidence, including log files, registry hives, DNA, fingerprints, or fibers of clothing normally invisible to the naked eye.

4.8 DIGITAL FORENSICS

Video

CCTV can be a good source of evidence for helping to identify attackers and the time the attack was launched.

Can be vital in apprehending suspects and reconstructing timeline of events.

Timelines / sequence of events

Time stamps. Each file has timestamps showing when files were created, last modified, and last accessed

Time offset. where evidence is collected across multiple time zones, you must record offset based on time zone.

For example, recording the time offset, it looks as if it started in Chicago, but if we apply time normalization, when it is 4 a.m. in London, the time in Chicago is 10 p.m.

Tags

eDiscovery tags virtual are virtual 'sticky notes' or labels attached to documents, making them easier to search/find.

Helps legal team stay organized and build a defensible case.

ORDER OF VOLATILITY

To determine what happened on a system, you need a copy of the data. **What evidence should you collect first?**

If it disappears in system reboot, power loss, passage of time, it is volatile

Volatility, in approximate order:

1. CPU, cache, and register contents
2. Routing tables, ARP cache, process tables, kernel statistics
3. Live network connections and data flows
4. Memory (RAM)
5. Temporary file system and swap/pagefile
6. Data on hard disk
7. Remotely logged data
8. Data stored on archival media and backups

FOR THE EXAM: Remember that volatile (perishable) information should be collected ***first***.

4.8 PRESERVATION

Evidence needs to be **preserved** in its original state so that it can be produced as evidence in court.

Original data must remain unaltered and pristine.

What is a "forensic copy" of evidence?

an image or exact, sector by sector, copy of a hard disk or other storage device, taken using specialized software, preserving an exact copy of the original disk.

Deleted files, slack space, system files and executables (and documents renamed to mimic system files and executables) are all part of a **forensic image**.

Putting a copy of the most vital evidence in a **WORM drive** will prevent any tampering with the evidence (you cannot delete data from a WORM drive.)

You could also write-protect/put a legal hold on some types of cloud storage.

To preserve original evidence, investigators will work with a **forensic copy**

EVIDENCE STORAGE

Understand the concerns for **evidence storage**

How to retain logs, drive images, VM snapshots, and other datasets for recovery, internal and forensic investigations?

Protections for evidence storage include:

- locked cabinets or safes
- dedicated/isolated storage facilities
- offline storage or immutable storage
- access restrictions and activity tracking
- hash management and encryption

E-DISCOVERY (ELECTRONIC DISCOVERY)

eDiscovery e-discovery is about gathering the data.

the process of **identifying, preserving, collecting, processing, reviewing,** and **producing** electronically stored information (ESI) in litigation.

The **digital forensics** process involves identifying, preserving, collecting, recovering, analyzing, and reporting on digital information.

During e-discovery, Cloud Service Providers (CSP) may be subpoenaed to allow collection, review, and interpretation of electronic documents and data.

Digital forensics vs eDiscovery: what's the difference?

computer forensics involves the use of a forensic expert to protect data integrity and to copy/capture/recover the data stored on a device.

eDiscovery firms typically do not analyze the data they collect.

Forensic investigators have specialized training enabling them to analyze data, protect data integrity, and recover missing or deleted data.

DATA RECOVERY

requires specialized training and knowledge

Forensic data recovery

A process used to retrieve data which will be used for legal purposes.

Investigators must work with information in a way that will not change or compromise the original source.

They can use a variety of techniques to fill in missing pieces or make information meaningful.

EXAMPLE: restoring a damaged or deleted partition, looking for traces of information which could reveal how and when the partition was used.

Critical when working with computers seeded with safety measures to prevent legal investigations, requiring special procedures.

E-discovery works in conjunction with digital forensics; Their functions are complementary.

4.8 REPORTING

After analyzing all the relevant evidence, digital forensic experts create a report documenting their findings.

What is typically in this report?

No set format, but often document the tactics, techniques, and procedures (TTP) used in an attack.

Common report elements:

- Executive summary of findings and recommendations
- List of the forensic tools used in the investigation
- List of evidence collected and analyzed
- Findings derived from evidence analysis
- Recommendations based on the findings

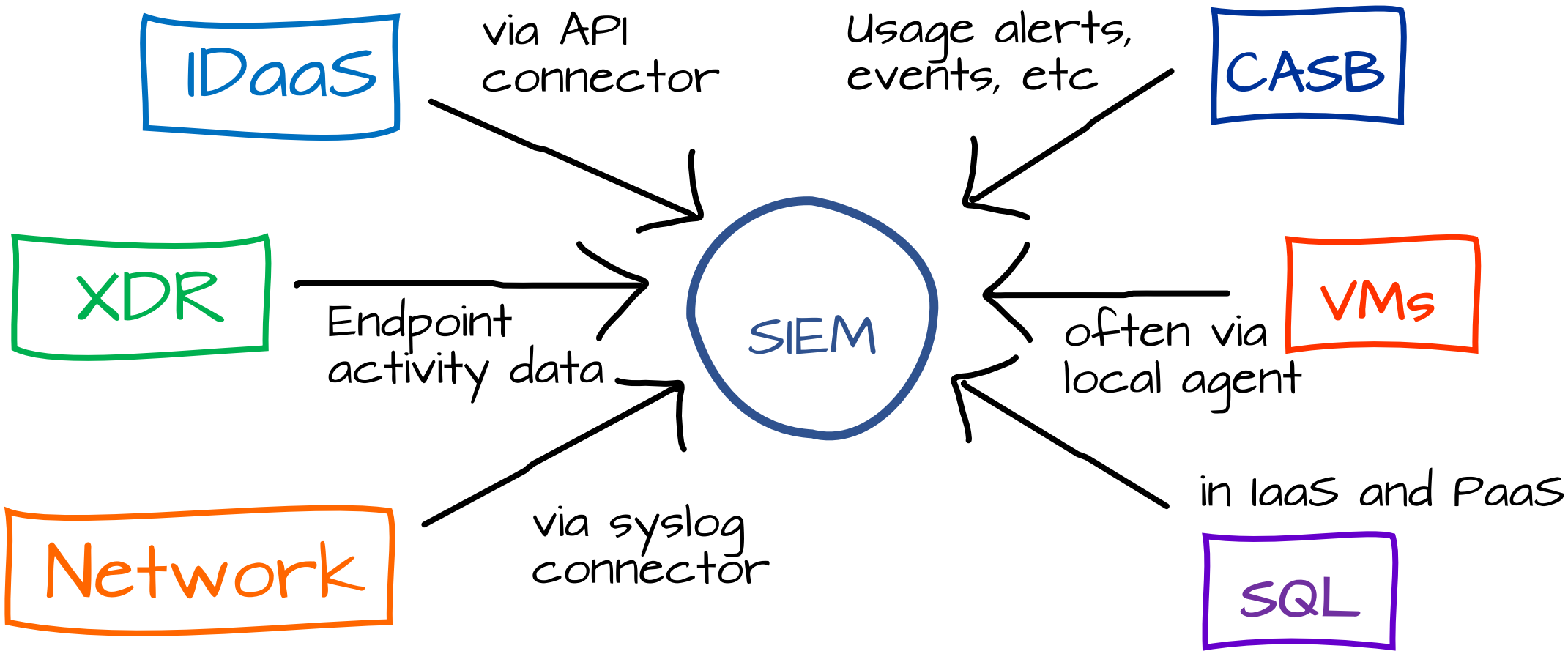
4.0 SECURITY OPERATIONS

4.9 Given a scenario, use data sources to support an investigation

- **Log data**
  - Firewall logs
  - Application logs
  - Endpoint logs
  - OS-specific security logs
  - IPS/IDS logs
  - Network logs
  - Metadata
- **Data sources**
  - Vulnerability scans
  - Automated reports
  - Dashboards
  - Packet captures

These are many of the logs that will be collected and aggregated by a SIEM

Accelerates investigation thru aggregation and automation (SOAR)



Log Ingestion with a SIEM

EXAMPLE

4.9 LOG DATA

By examining specific types of logs, you can pinpoint when and where malicious activities took place

Firewall Logs

Track network traffic entering and leaving your network.

They record the traffic allowed or blocked by the firewall based on predefined rules.

Application Logs

Capture the events and activities within specific applications.

Can provide insights into user actions, errors, and anomalies within the application.

4.9 LOG DATA

By examining specific types of logs, you can pinpoint when and where malicious activities took place

Endpoint Logs

Generated by individual devices or endpoints, such as clients (desktops and laptops) or servers (physical or VM).

They record system events, user activities, and security-related information specific to each endpoint.

OS-specific security Logs

Generated by the operating system and focus on security-related events. Event logs (Windows), Syslog (Linux)

Can include information about user logins, privileged account activities, and system configurations.

4.9 LOG DATA

By examining specific types of logs, you can pinpoint when and where malicious activities took place

IPS/IDS Logs

Record detected security threats, suspicious activities, and potential attacks on the network.

IPS logs will include entries of threats blocked.

Network Logs

routers, switches

Capture the traffic and activities occurring on the network.

Typically, via syslog

Can include information about network connections, data transfers, and communication between devices.

4.9 LOG DATA

Metadata is data about other data, created as part of files, documents, database transactions and more.

File. includes file info like created date, who created it, when it was modified, and when it was last accessed.

Email. includes items such as the header, who sent it, who they sent it to, and when they sent it.

Web. includes items in the header of a webpage, like title, character set, and other info developers add in meta tag.

Mobile. is often a rich data source of evidence for investigators.

It includes users' location, call history, message history, website history, and more.

4.9 LOG DATA

There is metadata related to endpoints, devices, and management platforms that can enrich SIEM data

Metdata Logs

Provides additional data about the data in log entries:

- Timestamps
- Source and destination IP addresses
- User and device identifiers

When aggregating logs, timestamps are critical

Helps security solutions (SIEM, XDR) in **correlating events** and understanding the **sequence of logged activities**

4.9 DATA SOURCES

These data sources offer additional insights to complement logs in the investigation of security incidents.

Vulnerability scans

Provide insight into potential vulnerabilities in systems, networks, or applications.

Scan reports can reveal if unpatched weaknesses might be exploited in the current incident.

Automated reports

Visibility into recent suspicious activity

Generated by security tools and systems that automatically collect and analyze data.

Can provide a high-level overview of suspicious activity and prioritize investigation efforts.

4.9 DATA SOURCES

These data sources offer additional insights to complement logs in the investigation of security incidents.

Dashboards

Often show trends (and changes in trends)

Offer a centralized view of security metrics and alerts.

Analyzing trends and spikes in these dashboards can help identify ongoing attacks or emerging threats.

Packet Captures

Reveals protocol-level details

Provide detailed information about the data being transmitted, including the content of the packets.

Can reveal malicious content within packets, identify source of attack, or reveal how vulnerabilities are exploited.

THANKS

FOR WATCHING!