comptia-7

Mobile device enforcement and monotitoring. mdm tools often manage devices deifferently depending on who owns them if the orfanization owns the device the mdm otol typically will downlaod and install all required apps and ensure they are uptodate. if device is employee owned mdm tools will monitor them for compliance and block access to the network.

unauthorized software

obtain appsonly through approved sources..
Jail breaking refers to removing all software restrictions from an apple device after jailbreaking devices users can install software from any source. rooting is the process of modifying an android device to give the user root level access sto the device.. updateds to the os overwirete firmware using over the air update techniques.. firmware ota updates the device.

sideloading is the process of copying an application package in the application packet kit. format to the device and then activating it

Jailbreaking removes all software restrictions from a apple device rooting modifies an android device. giving users root level access.. overwriting the firmware onan android with custom firmware is another way to root an android device sideloading is the process of installing software onan android device from a source that is not authorized

**RIch Communitcation services is a newer communication porotocol designed to replace sms for text messaging similar to mms, rcs can transmi multimedia but it has additional features.. **
**usbotg.... universal serial bus on the go. cables
unauthorized connections..
tethering can be used within a organiation they can bypass security sch as firewalls and proxy srvers.

****tethering and mobiel hotspots allow devices to access the net and bypass network controls wifi direct is a standard that allow devices to connect without a wireless access point or wireless router. mdm tools can block access to devices using tethering mobile hotspot or wifi direct access to the internet.
**

SEANDROID..SECURITY ENHANCED ANDROID SECURITY MODEL USES SECURITY ENHANCED LINUX SELINUX ENFORCE ACCESS SECURITY. WHEN ENABLED SELINUX SUPPORTS TWO MODES..

ENFORCING MODE. ENFORCES THE SELINUX POLICY

PERMISSIVE MODE. DOES NOT ENFORCE POLICY .

SEANDROID ONLY USES ANDROID DEVICES.

**EXPLORING EMBEDDED SYSTEMS. AND EMBEDDED SYSTEM IS ANY DEVICE THAT HAS A DEDICATED FUNCTION AND USES A COPUTER SYSTEM TO PERFORM THAT FUNCTION. DESKTOP PCS LAPTOPS AND SERVERS ALL USE CENTRAL PROCESSIG UNITS, OPERATING SYSTEMS APPLICATIONS TO PERFORM

A FIELD PROGRAMMABLE GATE ARRAY.. FPGA .. A PROGRAMMABLE INTEGRATED CIRCUIT INSTALLED ON A CIRCUT BOARD.

ARDUINO... IS A MICROCONTROLLER BOARD AND THE CIRCUT BOARD CONTAINS THE CPU. AND RANDOM ACCESS MEMORY.
UNDERSTANDING INTERNET OF THINGS. IOT

*.....REFERS TO THE WIDE ASSORTMENT OF TECHNOLOGIES THAT INTERACT WITH THE PHYSICAL WORLD THEY COMMONLY HAVE EMBEDDED SYSTEMS AND TYPICALLY CONNECT TO A DEVICE OR APP AND COMMUJNICATE VIA INTERNET.

***iNDUSTRIAL CONTOL SYSTEMS. IS A BROAD TERM ENCOMPASSING SUPERVISORY CONTROL AND DATA ACQUISITION SCADA SYSTEMS DISTRUBUTED CONTROL SYSTEMS AND PROGRAMMABLE LOGIC CONRTROL(IPL)
SYSTEMS.THESE SYSTEMS ARE WIDELY USED IN POWER GENERATION CHEMICAL PROCESSING AND TELECOMMUNICATIONS INDUSTRIES.. STUXNET A ALICIOUS COMPUTER WORM THAT INFECTED SCADA AND PLC SYSTEMS USED TO CONROL IRANIAN NUCLEAR CENTRIFUGES.

ICS AND SCADA SYSTEMS.

**Ics typically refers to systems with large facilities such as power plants and water treatment facilities a serpervisory control and data acquisition system, typically controls an ics by monitoring and sending it commands.

Manufacturing and industrial.. uses include any plants used to manufacture products.

facilities uses include monitoring the temp and humidity and keeping environment relatively stable.

enery uses include oill and gas power processing.
logistics uses include monitoring process within shipping facilities.

**A supervisory control and data acquisition system has embedded systems that control industrial control systems ics such as one used at a power plantor water treatment faciltiy .. embedded systems are also used for special purposes like medical devices automotive vehicles aircraf=t and unmanned aeriel vehicles

wearables..... refers to any device you cna wear or have implaned these devices can then be used to interact with other devices. +++microchips for pets.
Camera systems home automation. wireless thrmostats lighting coffee makers

---

System On a CHip SOC. an intefrated circuit that includes all the functionality of a comuting system within the hardware it typically includes an application contained within onboard memory.
a real time operating system. .reacts toinput within a specific time. it cant respond within a specidfied time. it doesnt process data and typically reports error.

**An embedded system is any device that has a dedicated function and uses a computer system to perform that function. it includes any devices in the internet of thins iot category such as wearables and home automation systems.

security implication os embedded systems. ;;;;when vendors discover vulnerabilites in computers and apps they write and release patches. when you apply the patch the system is no longer vulnerable to the exploit.
Embedded system constraints

**commpute.....limited
**crypto
**power.. ost use batters.
**range connect to other devices using wireless protocol
** network. interface to configre devices..
**cost the cost of the device can be minimized by sacrificing features..
**inability to patch
**implied trus a lot of devices are vulnerable
**weak defaults..

**Understanding threat actors. **

**APT advanced Persistent Threat is a group of organized threat actors that engage in targeted attacks against organizations.f

while apts can be any group.. APT can be state actors these state actors typically have specific target such as a certain company orgqanization and government aagency..

apt sponsored by many governments..

++*chin
*iran
*Northi Korea
*Russia
**An advanced persistent threat refers to an organized and sophisticated group of threat actors nation

states govt sponsor them and give them specific targets and goals criminal syndicates are groups of individuals involved A CRIME.

** **criminal syndicates are composed of a group of individuals working together in criminal activities. usually the goal is money.

crowdstike..

**hacker WAS KNOWN AS SOMEONE PROFICIENT WITH COMPUTERS WHO WANT TO SHARE KNOWLEDGE WITH OTHERS HOWEVER THE DEFINITION HAS MORPHED

A **SCRIPT KIDDIE IS AN ATTAKER WHO USES EXISTING COMPUTER SCRIPTS OR CODE TO LAUNCH ATTACKS. MO AGE LIMIT.
A **HACKTIVIST LAUNCHES ATTACKS AS PART OF AN ACTIVIST MOVEMENT OR TO FURTHER A CAUSE.. HACKTIVISTS TYPICALLYARENT LAUNCHING THESE ATTAKCS FOR THEIR BENEFIT.

WHIT,BLACK, GREY HATS.. (WHITE= PENTESTERS) BLACK(CRIMINAL) GREY.. BOTH.

**insider threat is anoyone who has legit access to an organizations internal resources.

(revenge,money)

**Attack vectors. are the paths that attackers used to gain access.
**email.. attackers frequently send out spam with malicious links or attachments. its estimated that 91 % of all attakcs start with an email.

**social media attackers often use social media to gather info on targets via soceal media this includes social media sites such as facebook and twitter.

**Shadow IT. refers to any unauthorized systems or applications within an organization most orfanizations have specific processes in place ot approve new systems an dpps.

**malware.. includes a wide range of software that has malicious intent

**virus is a malicious code that attaches itself to a host application.

***shadow It refers to unauthorized systems or apps installed on a network without authorization or approval

***worms self replicating malware that travels throught a network without the assistance of a host application or user interaction. a worm resides in memory and can use different transport protocos to travel over the network .

***a logic bomb is a string of code embedded into ana pp or script that willececute in response to an event. the event migt be a spcific date or tiem.

**a logic bomb executes in response to an event such as when a specific application is executed.
**A backdoor provides another way of accessing a system similar to how a backdoor in a house provides another mode of entry

**trojan also called a horse typically looks like something beneficial

*****A backdoor provdes another way to access a system many types of malware create backdoors allowng attackers toaccess systems from remote locations. exmployees have also creted backdoors in apps and systems.
a**

malware includes a wide variety of malicious code including viruses worms trojans and ransomware and more. a virus is malicous code that attaches instelf to an application and runs when the applicatiion is started. a worm is self replicatin and doewnt need user interaction to run

***A trojan appears to be something useful but includes a malicious ocmponent such as installing a backdoor on a users system many trojans are delivered via driveby downloads. they can also infect systems rom fake antiviurs software piated software games...

**RAT remote access trojon type of malware that allows attackers to control systemsfrom remote locationns it is often delivered via drive by downloads or malicious attachments in email. once installed on system attakcers can access the infected computer..

KEYLOGGERS attemt to capture keystrokes. the keystrokes are store d in a file either to send immdiately or store.

***spyware is software instlled on users; system without their awareness or consent its purpose is often to monitor the users' computer and the user's activity spyware takes some level of control of computer.

** Key loggers capture keystrokes. spware monitors user computr often uses keyloggers.

**ROOTKIT>
a group of programs or in rare instances 1 program.. that hides the fact that a system has been infected or compromised. by malicous code. a user might suspect something is wrong but antivirus scans and other checks indicate....
Rootkits have system level or kernel access and can modify system files and system access. rootkits hide their running process to avoid detection

**BOTS are software robots. for example google uses bots in search engine spiders to travel through the internet looking for pages.

**comand and control. resources to control infected computers. after a computer is infected with malware .. the attempts to conncet to a command and control resource for instructions.
***some criminals have migrated to peer to peer botnets(P2P)

**Botnets are groups of compters controlled by attackers and compters in a botnet check in command and control server periodically for instructions.. attackers frequentlyuse botnets to launch DDOS attacks.

RANSOMWare and cryptomalware. (trojans) attakcers take control of computers or networks. locking out users. with cryptomalware attackers encrypt the data computers within the network to prevent access.

VCPI(VIRTUAL CARE PROVIDER INCO.. SUFFERED A MASIVE RANSOMWARE ATTCK IN 2009)

***RANSOMWARE IS A TYPE OF MALWARE THAT USERS A SYSTEMS DAT. CRYPTOMALWARE ENCRYPTS USERS DATA. CRIMINALS THEN ATTEMPT TO EXTOR PAYMENT FROM THE VICTIM. RANSOMWARE OFTEN INCLUDES THREATS OF DAMAGING A USERS SYSTEM OF DATA IF THE VICTIM DOES NOT PAY THE RANSOM. AND ATTACKERS INCREASINGLY TARGET HOSPITALS CITIES AND OTHER LARGER ORGANIZATIONS.

(pup)**POTENTIALLY UNWANTED PROGRAMS. ...

**A FILELESS VIRUS ALSO CALED FILELESS MALWARE. IS A TYPE OF MALICOUS SOFTWARE THAT RUNS INMEMORY IN CONTRAST MOST MALWARE IS WRITTEN TO DISK.

***FILELESS VIRUSS RUN MEMORY INSTEAD OF FROM A FILE ON A DISK. THEY ARE OFTEN SCRIPTS THAT ARE INJECTED INTO LEGITIMATE PROGRAMS. THEY CAN ALSO BE HIDDEN IN VCARDS

**MEMORY CODE INJECTION.. THE MALWARE INJECTS CODE INTO LEGITIMATE APS USING KNOWN UNPATCHED GLNERABILITIES IN THES APPS

***SCRIPT BASED TECHNIQUES TWO COMMON EXAMPLES ARE SAMSAM RANSOMWARE AND OPERATION COBALT KITTY .. SAMSAM USED ENCRYPTED CODE THAT IS ONLY DECRYPTED WHEN RUN. MAKING IT DIFFICULT TO DETECT.

**WINDOWS REGISTRY MANIPULATION. THE MALWARE USES A WINDOWS PROCESS TO WRITE AND EXEVUTE CODE INTO THE REGISTRY..

POTENTIAL INDICATORS OF MALWARE ATTACK.

**EXXTRA TRAFFIC

**DATA EEXFILLTRATION (UNAUTHORIZED TRANSFER OF DATA)

EXCRYPTED TRAFFIC

TRAFFIC TO SPECIFC IPS
OUTGOING SPAM.**SOcial engineering. is the practive of using tactics to gain information. its often low

tech encourages. individuals to do something they wouldnt normall do.

**SOcial engineering uses social tactivs to trick users into giving up information and performing actions they wouldnt normally take. social engineering attacks can occur in person over the phone or while surfing the internet.

**tricking and hoaxss. a hoax is a mess
***encouraging someone to perform risky action
***encouraging someone to reveal sensitive information
***impersonating someone such a an authorized tech.
***using flattery and conning
***assuming a position of authority

**A social engineer can gain unauthorized information just by looking over someones shouldor this might be a person, such as when a user is at a computer of remotely using a camera screen filters help prevent shoulder surfing by obuscuring people view unles sthey are directly in front of the monitor.

**impersonation..
shoulder surfing... simply looking over someones shoulder.
age often scirculated through email. which tells of impending doom from a virus or security threat.

**Tailgaiting is the practive of one following too closely behind another without showing credentials

**Dumpser diving s the practice ofyet .. searching through trash or recycling cotainers to gain fnformation from discarded documents.

**Zero Day vulnerablilities.
... a vulnerability bug that is unkown to trusted sources suh as os system and antiviurs vendors.

***Tailgating is a social engineering tacic that occurs when one user follows closely behind another user without credentials access control vestibules also called mantraps, allow a single person to pass a time. sophisticated mantraps can identify and authenticate individuals before allowing dumpster divers search through trhas lookinfor info, shredding or burning papers instead of thrrowing them away mitigates the threat.

***zero day exploits the advantage of vulnerabilities that dont have available patches it could be bc vendors dont know about the vulnerability or havent written patches to fix it zero day exploits can evade up to date antifuris software.

***watering hole attacks attempts to discover which websites a group of people are likely to visit then infects those websites with malware that can infect the visitors

***typeo squatting also caled url hijacking occurs when someone buys a domain name that is close to a legitimate domain name.

**hosting a malicious site
**earning ad revenue
**reselling the domain.

**eliciting information. is the act of getting information without asking for it directly social engineers often sue casual conversation to gather info without giving the tagets any idea the attakcer is trying to gather info.

**active listening
reflective questioning.pretecting and prepending. are similar and some user the termms interchangible however there is a subtle difference..

**false statements.

**bracketing.
a pretext is a fictitous scenario added to a conversation to make a request more believable.
prepending simply means to add something to the beginning of something else.

Identity theft and fraud. when someone steals personal information about you.

GASLIGHTING AND INFLUENCE CAMPAIGNS.

***GASLIGHTING IS A FORM PSYCHOLOGICAL MANIPULATION TO GET INDIVIDUALS TO QUESTION THEIR SANITY.. THE TERM COMES FROM THE 1938 PLAY GAS LIGHT WHERE A HUSBAND ATTEMPTS TO CONVINCE HIS WIFE SHEIS INSANE BY CHANGING THINGS IN THE ENVIRONMENT THEN INSISTING THEY HAVENT BEEN CHANGED

**INVOICE SCAMS. SOME CRIMINALS USE INVOCE SCAMS TRYING TO TRICK PEOPLE OR ORGANIZATINS INTO PAYING FOR GOODS OR SERVICES THEY DIDNT REQUEST.

***PHISHING. IS THE PARACTICE OF SENDING EMAIL TO USERS WITH THE PURPOSE OF TRICKING THE INTO REVEALING PERSONAL INFOMATION BU CLICKING ON A LINK .

***SPAM IS UNWANTED EMAIL PHISHING IS MALICOUS SPAM ATTAKERS ATTEMPT TO TRICK USERS INTO REVEALING SENSITIVE PERSOANL INFORMATION BY CLICKING ON A LINK.

***BEWARE OF EMAILS FROM FRIENDS.
PHISHING TO INSTLAL MALWARE.
PHISINIG TO VALIDATE EMAILS.
PHISHING TO GET MONEY
SPEAR PHISHING .... IS A TARGETED FORM OF PHISHING. INSTAD OF SENDING THE EM AIL OUT TO EVERYONE, IT ATTEMPTS TO TARGET SPECIFIC GROUPS AND PEOPLE.

**whaling is a form of spear phishing that attempts to target high level executives las vegas casinos refer to big spenders as whales.

***a spear phising attack targets spcific groups of users it could targe employtees withtin a company of custoers of a company digital signatures provide assurances to recipients about who sent anemail and can reduce the success of spear phising

++vishing. attakcs use phone systems to trick users into giving up personal and financial information vishing often uses voie over IP voip technology. allowing the attaker to spoof caller ID

**smishing a mashup of sms and phising is a form of phishing that uses text instead of email..

**vishing is aform of phishing that uses the phone system or voip some vishingattempts are fuflly automated. others start as automatted calls but an attacker takes over at some point during the call smishing is a form of phishing that using text messages.

one click lets them in.. **

blocking malware and other attacks. spam filter o mail gateways phishig attacks are delivered with malicous spam.

**smishing. is a form of phishing that uses text instead of email. some smishing texts include malicous attachents and some try to trick the user into giving up personal information.

**vishing is a form of phishing that uses the phone system or VOIP soem vishing attempts are fully automated. others start as automated calls but an attacker takes over at some point during the call. smishing is a form of phishing using text messages.

**one click lets them in. the attacker use sopen source intelligence to identify a target.
**next the attacker crafts a spear phishing email. with a malicous link.

**the attakcer sends the spear phishing email to the target from an internet based system.
**ththe user clicks on the link it takes the user to a website that looks legitimate but.
**if the nalicious link tricked the user into entering credentials.

**attakcer uses credentials to access malicous syste
the original target may ae limited access within the network. a
**alware searches for data within the network such as emails files computers and servers.

***blocking malware and other attacks.
*spam filter on mail gatewarys
**antimalware software on mail gateways
**all systems.
**boundaries or firewalls.
spam filters

((the challenge with an SPAM FILTER is to filter out spam only and never filter out legitinmate email.)

)***Anditivurs software detects and removes malware, such as viruses trojans and wors SIgnature-based antiviurs software dtects known malware based on signature fefinitions. Heuristic based software detects previously unknow malware based on behaviour.