Pre assessment 21

Monday, July 24, 2023 9:18 PM

21. Org wants to combine security controls to control incoming and outgoing traffic. Should include stateless inspection, malware inspection, and a content filter

A. VLAN
B. NAT
C. UTM
D. DNSSEC
C. WAF

Unified threat management

UTM - advance firewall that combines multiple controls together like stateless inspection, malware analysis, and content filter

no other answers provide these

VLAN is for network segmentation on switch

Network Address Translation

NAT - converts public to private IP addresses and vice versa

DNSSEC provides validation for DNS responses

Web app Firewall WAF – pro.
web server from internet based attacks

22. Deploying Linux server in screened subnet. Want to manage from pc in private network

A. Forward proxy server
B. Reverse proxy server
C. Web app firewall
D. Jump server

Jump server – placed between security zones and is used to manage devices in the other zone

could connect to jump server using SSH, then linux server using SSH forwarding

forward proxy for outgoing internet traffic

reverse proxy for incoming internet traffic

23. Several attacks against servers in DMZ. Which will prevent?

A. Anomaly based IPS
(B.) inline IPS
C. Passive IDS
D. Signature-based IPS

inline IPS only one that will prevent

24. Coffee Shop stopped broadcasting SSID for wireless network. Turn on laptop and see the SSID, what is the attack?

A. Rogue AP
(B.) Evil twin
C. Jamming
D. Bluejacking

evil twin - a rogue Access point (AP) with the same or similar service set identifier SSID

jamming - not allowing anybody to connect to wireless network

bluejacking - related to bluetooth

25. Must put smartphone in conductive metal box before entering area. Which is greatest risk to IP this mitigate?

(A.) Bluesnarfing
B. Theft of phone
C. Data exfiltration from mobile hotspot
D. Enable geofencing

Bluesnarfing - unauthorized access to info on wireless device through bluetooth

conductive metal boxes are a faraday cage that blocks bluetooth signals

lockboxes prevent theft but not main concern if conductive

Wireless hotspots are in public locations

virtual

geofencing - creates a virtual fence using GPS, but devices in cage won't access GPS

26. Designing site to site VPN between offices in different cities. Use of certificates for mutual authentication. Want to ensure internal IP addresses are hidden.

A. IPsec VPN using tunnel mode

B. IPsec VPN using transport mode

C. L2TP VPN

D. VLAN VPN

IPsec VPN provides mutual authentication

tunnel mode - encrypts payload and IP headers

transport mode - only encrypts payload

Layer 2 tunneling protocol

does not encrypt

VLAN VPN - provides network segmentation but does not act as VPN

27. Want to use HSM on server in network. What does this add to server?

A. Provide full drive encryption

B. Reduce risk of confidential info outside org

C. Provide webmail to clients

(D.) Generate and store keys for servers

hardware security module - generate and store RSA keys

can be used to encrypt data sent to and from server

trusted platform module TPM provides full drive encryption

Data loss prevention DLP - reduce risk of sending confidential

info outside org

SaaS provides webmail

28. Need to send email with sensitive info. Which best maintains confidentiality?

A. Digital signature

(B.) Encryption

C. Data masking

D. Hashing

encryption provides confidentiality of any type of info

digital signature provides integrity, non-repudiation, and authentication

data masking modifies original data producing data that looks valid but not authentic

hashing provides integrity

24. Stores some data in cloud with its own resources. Another company also stores data in cloud at own

resources. Both decide to share data in both clouds for educational purposes.

A. Community
B. Private
C. Public
D. XaaS

created a community cloud
both clouds separate were private, but shared resources were not

in this scenario, they are sharing only with each other, meaning it is not public - visible by everyone

Anything as a Service XaaS
Cloud services beyond IaaS, PaaS, and SaaS

30. Planning to implement a CYOD deployment model. Which are appropriate for policy?

A. SCADA access
(B.) Storage segmentation
C. Database security
D. Embedded RTOS

Storage segmentation - create separate storage areas in mobile devices

can be used with choose your own device (CYOD) - users own their own devices

no other answer related to mobile

Supervisory control and data acquisition SCADA - controls industrial control system ICS's such as nuclear plants or water treatment

SCADA should be isolated

Database security - use of permissions and encryption to protect data in database

Embedded systems use real-time OS RTOS when system

must react within [illegible]
time

31. Plan to implement desktops via cloud. Each will include OS and core group of apps. Cloud will manage desktops. Employees can access from anywhere and any device

A. IaaS
B. CASB
C. SaaS
(D.) XaaS

anything as a service XaaS would include desktops as a service

IaaS - vendor provides access to pc, but customer must install OS and apps

Cloud access security broker

CASB - software tool used to provide additional security for cloud resources but provides underlying

cloud services

SaaS provides apps but not entire desktops

32. Want to improve security posture. Doesn't have any security staff.

A. SOAR
B. MSSP
C. SaaS
D. XaaS

Managed security service provider MSSP - 3rd party vendor that provides security services for org

security orchestration, automation, and response SOAR - automates incident response for some events

requires security staff

SaaS and XaaS still need security staff

33. Allow employees to connect to internal network using personal device. Having problems: devices updated

- do not keep
- no standardization of devices
- no adequate control over devices

Want to allow to keep using personal devices, which is best?

A. BYOD
B. COPE
C. CYOD
D. IaaS

CYOD - includes a list of acceptable devices that employees can purchase and connect to network

IT can can then use mobile device management MDM system for standardized management

Bring your own device BYOD does not have standasdization

corporate owned personally enabled

COPE policy - orgs own

devices, not employees

34. Discover new systems on network during vulnerability scan. Systems weren't authorized because someone installed w/out going through standard process.

A. Hacktivist
B. Script kiddie
C. Shadow IT
D. Authorized hacker

Shadow IT - any systems or apps installed on network without auth or approval

employees often add to bypass security controls

Hacktivist - launches attacks as part of activist movement

Script kiddie - uses existing software or scripts to attack and often has little technical ability

authorized hacker who

White hat - security professional working with law to protect org

35. Received phishing email with malicious attachment. Opened and installed malware that quickly spread to other systems on network. Exploited vulnerability that wasn't previously known by any trusted sources.

A. Backdoor

(B.) Zero-day

C. Hoax

D. DDoS

Zero-day - not known by trusted sources like antivirus

Hoax - not a specific attack, message spread about impending doom of virus security threat that

or
doesnt exist

DNS comes from multiple sources

36. Completed antivirus scan and detected trojan. Removed trojan but worried attackers may still be able to access.

(A.) Backdoor
B. Logic bomb
C. Rootkit
D. Botnet

trojans often create backdoors

Logic bombs and rootkits can create backdoors but trojans dont create logic bombs and rarely install rootkit

37. Some network appliances monitoring incoming data sending alerts about malicious files. These are PE32 files with tar.gz extension and being downloaded

exfiltration to several systems. User opened email with infected MHT file.

A. systems joined botnet
B. installed ransomware
C. installed RAT
D. Shadow IT running in network

users installed RAT when they opened MHT file - MHTML is a webpage archive that stores HTML, JS, CSS, images, etc.

after installing RAT, installed portable executable PE32 files

systems may have joined botnet but scenario doesn't indicate

ransomware would encrypt data

Shadow IT are unauth systems in network

38. Unable to access [illegible] see message that data has been encrypted until pay ransom.

A. Criminal syndicate
B. Ransomware
C. Fileless virus
D. Rootkit

Criminal syndicate - launches criminal organized attack motivated by money

fileless virus - injects code into existing scripts and may install ransomware but not ransomware itself

rootkit - program or group of programs that provide root-level access to system but hides itself

34. SIEM sending alerts saying malware has infected several pcs. Examine border firewall and NIDS logs, but can't [illegible] traffic entering

find malicious traffic from internet. All employees affected attended trade show in past 2 days

(A.) fileless virus via vCard

B. Malware on USB

C. Trojan from botnet

D. Worms from presentation media

vCard virtual contact file

VCF - people usually share contact info w/ vCards but can contain malicious code

USBs not mentioned

malicious traffic from botnet comes from internet but IT didnt find any

speakers at trade shows use presentation media but viewing presentation wont infect systems

40. Receive email saying won lottery. Need to confirm identity w/ name, phone, address, bday. Will receive prize after.

A. Spear phishing
(B.) Phishing
C. Smishing
D. Whaling

general phishing, not targeted (spear/whaling) smishing from text, not email

41. Some protocols include sequence #'s and timestamps. Which does these thwart?

A. MAC flooding
(B.) Replay
C. SYN flooding
D. Salting

and sequence

timestamps

#s act as counter measures against replay attacks

Media access control MAC flood attack - floods switch with different MAC addresses

SYN flood disrupt TCP handshake

Salting is not an attack

42. Reviewing logs for web server and see sus entries. Suspect an attacker trying to write more data into web app memory than it can handle

A. Pointer/object dereference

B. Race condition exploit

C. DLL injection attack

(D.) Buffer overflow attack

buffer overflow attack - write more data into app memory than it

can handle

pointer/object dereference - programming error that can corrupt memory

programmers, not attackers cause this

race condition exploit - programming conflict where 2 or more apps or app models try to access or modify same resource at the same time

dynamic link library DLL injection attack injects DLL into memory and causes it to run

DLL - Microsoft windows module of functions or data other programs or DLLs can use

43. Org hosts web app selling digital products. Customers can post comments. Attackers looking for ways

Attacker ... to exploit. What is best way to test resilience of app?

A. Fuzzing
B. Input validation
C. Error handling
D. Anti-malware

fuzzing - type of dynamic code analysis that tests site resilience

sends random data to app to see if it crashes site or expose data

input validation and error handling protect, but not test

Same with anti-malware

44. Attacker launched successful xss attacks on web app. Which are best to protect and prevent?

analysis

A. Dynamic code ana—

(B.) Input validation

C. Code obfuscation

(D.) WAF

E. Normalization

input validation and WAF are best

input validation - validate input before using

WAF - additional firewall that monitors, filters, and blocks HTTP traffic to web server

Dynamic code analysis is testing method

Code obfuscation - makes code harder to read

Normalization - organize tables and columns in database to reduce redundant data and improve overall database

performance

45. User has account to post comments. Enters username and pword to login and Site displays username. Changed username to JS code. other users experienced unexpected results when hovering over name.

(A.) Cross site scripting
B. Input validation
C. Privilege escalation
D. Directory traversal

this is XSS

input validation is how you protect against it

privilege escalation - attempt to give attacker more rights or permissions

directory traversal attack - attacker navigates system's directory structure and

reads files

46. Which best describes purpose of risk register?

A. Shows risk on plot or graph

(B.) Listing of risks, risk owner, and mitigation measures

C. Shows risks in color coded graph

D. Evaluates supply chain

risk register - lists risks and often includes risk, risk owner, mitigation measures, and risk score

risk matrix - plots risks in graph

heat map - plot risks onto color-coded graph or chart

risk register does evaluate supply chain risks, but does a lot more.

47. Performing risk assessment. Identifies loss for previous year due to specific risk as $5000.

A. SLE
B. ARO
C. MTBF
(D.) ALE

Annual loss expectancy
ALE - identifies expected loss for a given year based on specific risk and existing security controls

Single loss expectancy SLE
identifies cost of single loss

Annual rate of occurrence
ARO - how many times

a specific risk
occor in a year

SLE x ARO = ALE

Scenario refers to specific risk but doesn't mention how many times it occurred over the year

Mean time between failures
MTBF - measure of system's reliability and usually measured in hours

48. Developing new tech, worried about stealing company secrets. Which will help identify potential dangers related to loss of tech?

(A.) Threat hunting
B. Vulnerability
C. SOAR
D. SIEM

threat hunting - looking network

for threats in ...
before automated tool
detects

Vulnerability scan - evaluates vulnerabilities with network but doesn't look for threats

SOAR and SIEM can assist in detecting/resolving threats but need more

49. Org hired expert to perform security assessment. After running vulnerability scan found:

Host IP ... OS Apache httpd 2.4.53 vulnerable to mod_auth exploit

However, mod_auth not installed or enabled.

A. false negative
(B.) false positive
C. result of credentialed scan
... non-credentialed

D. result of
scan

scanner saying vulnerability
with mod_auth, but
hasn't been enabled
so can't represent vuln

false negative would be
vuln exists but not
found

Scenario doesn't give info
about credentialed vs.
non

Credentialed scan - allow
vulnerability scanner to
have more visibility over
the systems it scans,
compared to non-credentialed
scan

50. Reviewing report created
after vulnerability scan.
Not sure if it was
credentialed or not.
Which is best indication
that it was?

versions

(A) Shows software ... of installed apps

B. Large # of false positives

C. Listing of IP addresses discovered

D. List of open ports

Credentialed scan - show software versions of installed apps

will also show fewer false positives

any scan will show discovered IPs and open ports

51. IT has dedicated group for cybersecurity testing. Each member has knowledge of TTPs and how to use. Each has knowledge of security controls that would be implemented to protect resources.

A. Red team

B. Blue team

(C) Purple team
D. White team

Purple team = Red + Blue

Red team - attacks and use tactics, techniques, and procedures TTP that attackers have used in actual attacks

Blue team - defends and has knowledge of security controls used to protect resources

White team - dont do testing but set roles and oversee testing

52. Servers in screened subnet are being attacked by internet based attacker. Want to view IPv4 packet data.

(A) Protocol analyzer
B. IP scanner
C. Vulnerability scanner
D. Proxy server
E. Heuristic-based IDS

... captures and

protocol analyzer - displays packets

IP scanner or network scanner identifies hosts within network by identifying active IP addresses and other info about host

Vulnerability scanners look for vuln

Proxy servers forward requests from client

Heuristic-based IDS or behavior-based - detect intrusions by identifying anomalies

53. Org wants to move data to cloud. 3 possible choices. Wants to ensure they have strong security controls in place. Which reports do they want CSP to provide?

A. SOC 2 Type I
(B) SOC 2 Type II
C. SOC 3
D. SOC I

System and organization controls

SOC 2 - report of org controls that cover cybersecurity

SOC 2 Type II - identifies controls in place during a date range of at least 6 months

SOC 2 Type I - identifies controls in place during certain date

SOC 3 report - generalized report sometimes available to public

SOC 1 report - detailed report covering financial and auditable controls for orgs that is sometimes provided by orgs that handle financial data

54. Want to identify and mitigate potential single points of failure in org's security operations.

A. Disaster recovery plan

B. Business impact analysis

[illegible] loss expectancy

C. Annualized

(D.) Separation of duties

if only one person can perform security tasks, then that person becomes a single point of failure

Separation of duties solves this

Disaster recovery plan - identifies how to recover systems after disaster

business impact analysis BIA
helps org identify critical systems and components

ALE is expected annual loss of specific risk

55. Want to increase cybersecurity resiliance of key servers by adding fault tolerance. But budget is limited.

A. Alternate processing site

(B.) RAID-10

C. Backups

D. Faraday cage

V. Farm / [illegible]

redundant array of inexpensive disks 10

RAID-10 - subsystem that provides fault tolerance for disks and increases cybersecurity

resiliance = ability to continue to operate after adverse event

alternate processing site - does provide resiliance but expensive and provides more than fault tolerance

backups - good for resiliance but not fault tolerance

faraday cage - room or enclosure that blocks all signals

56. Orgs backup policy for file server says amount of time needed to restore backups should be minimal.

A. Full backups Sunday incremental on other 6

B. Full on Sunday [illegible] other 6

(15.) full
differential on other

C. Incremental on Sunday
differential other 6

D. Differential on Sunday
Incremental on other 6

Full backup - entire data backup

differential backup - only files changed since most recent full backup

incremental backup - only files changed since last backup

full/differential is best since a restore would only require 2 backups

full/incremental would require to restore multiple backups
ex: data loss on friday
would require restore
full backup and 4
incremental backups

backups must start with a full backup

so inc/diff or diff/inc not possible

differential would be one backup growing each day

incremental is individual backups per day

57. Completed BIA and defined maximum acceptable outage time for a critical system.

(A.) RTO
B. RPO
C. MTTR
D. MTBF

recovery time objective RTO is max amount of time it can take to restore a system after outage

directly related to maximum acceptable outage time defined by BIA

RPO

recovery point objective
identifies a point in time where data loss is acceptable - referring to databases

mean time between failures
MTBF - measures system's reliability and is represented in hours

mean time to repair MTTR
average time it takes to restore failed system

58. Want to ensure critical business systems are protected from isolated outages. Which tells how often these systems will experience outages?

A. MTTR
(B.) MTBF
C. RTO
D. RPO

MTBF gives you idea of how often failures occur

alternate location

59. Considering ... as part of continuity of operations plan. Which site resiliance solution has shortest recovery time?

A. Cold site
B. Warm site
(C.) Hot site
D. Snapshot

hot site - shortest recovery time; most expensive

cold site - longest recovery, least expensive

Warm sites - in between

snapshot - backup of a disk at a moment in time used for forensics

60. Creating detailed plan how to recover critical systems after complete loss.

A. Backup plan
B. Incident response plan
C. Communications plan
D. Recovery plan

(D.) Disaster recovery

disaster recovery plan DRP
how to recover critical systems after disaster

backup plans – how to backup and restore data not systems

incident response plan
implemented after incident but not all incidents are disasters

communications plan – part of incident response plan
how to comm issues related to incident

61. Expanding cloud services to public. Expand data center. Has 1 row of racks for servers, want to add 1 more. Calculated power and HVAC reqs and last way to reduce costs is to make sure [illegible] are facing opposite

direction.

A. provide fire suppression
B. Reduce power consumption
(C.) Create cold and hot aisles
D. Create an air gap

hot and cold aisles - have servers facing opposite ways for more efficient cooling

reduces cost for heating, ventilation, and air conditioning HVAC

this reduces power consumption but does not reduce power consumption of servers

hot and cold aisles do not provide fire suppression

air gap - ensures systems are not connected to same network

scenario where
are connected for cloud
servers

62. Receive antivirus alert indicating file hash of known malware. File was pushed from org's patch management system and scheduled to be applied next morning. File and hash were:

gcga-upgrade.exe

518...-

Logs of patch management system you see:

Status	Update name	Hash
pushed	gcga-upgrade.exe	518...

A. File was infected after pushed out

B. File embedded with crypto-malware before it was pushed

C. File was listed in patch management systems blacklist

D. File was infected when
management system

patch management downloaded it

most likely infected when downloaded because name and hash are same on server and patch management server

if it were infected after it was pushed out, it would have different hash

not possible to tell if crypto malware

blacklist blocks files so it wouldnt have been pushed out if it was on patch management blacklist

63. Org requests bids for contract via email. After winning bid, couldnt meet reqs of contract and tried to [illegible] it never bid. which

Say ... would be proof?

A. Digital signature
B. Integrity
C. Repudiation
D. Encryption

digital signatures - provide verification of who sent message, non-repudiation preventing them from denying, and integrity verifying message wasn't modified

integrity verifies message wasn't modified

repudiation isn't a security concept

encryption protects confidentiality but doesn't verify who sent or non-repudiation

64. App requires to login with pwords. Want to store and protect from rainbow

tables.

(A.) Salting
B. Hashing
C. Homomorphic encryption
D. Perfect forward secrecy

Salting will prevent
hashing won't

homomorphic encryption
used to protect data in
cloud and allows it to
remain encrypted while
being processed

perfect forward secrecy
related to encryption and
indicates system generates
random keys per session

65. SIEM alert for failed logins. Login failures for 100 accounts. Then show same accounts have login failures 3 hours later.

A. brute force attack
B. dictionary attack
(C.) spraying attack
[illegible] attack

D. account lockout

Spraying attack
SIEM shows attack loops through list of accounts guessing on pword for one account at a time

brute force and dictionary don't loop through accounts
account lockout attack not relevant

66. Org has data center to store data. Want to move lots of financial data into cloud. Data is regularly accessed and manipulated by employees, customers, and vendors. Data always needs to be encrypted in cloud.

A. Symmetric encryption
B. Asymmetric encryption
C. Homomorphic encryption
D. Steganography encryption

this allows data to

homomorphic ... be accessed and manipulated while it is encrypted

Symmetric and asymmetric require data to be decrypted before manipulated

Steganography - not real encryption, only hides data within data

67. Need to exchange emails over internet using unsecured channel. Emails need to provide non-repudiation. Decide to use certificates on each of their pcs. What would they use to sign their certificates?

A. CRL
B. OCSP
C. CSR
(D.) CA
E. DSA

Certificate authority CA manages certificates and would sign certificates issued to users

non-repudiation comes from digital signatures and each user would need a certificate assigned to them to create digital signature

Certificate revocation list
CRL - list of revoked certificates

Online certificate status protocol
OCSP - alternative to CRL provides real-time response indicating validity of cert

Certificate signing request
CSR - used to request a certificate

Digital signature algorithm
DSA - used to create digital signature

they would use digital signatures to sign emails, certificates are needed to create digital signature, but you can't certificate w/

Sign a
digital signature - this
is for CA

68. Admin installing certificate with private key on server which cert type?

A. DER
B. P12
C. CER
D. P7B

P12 (PKCS #12) certificates commonly include a private key and are used to install private key on server

distinguished encoding rules
DER-based certificate
binary encoded file

canonical encoding rules
CER-based certificate
ASCII encoded file

DER and CER define format not content (private key)

P12 does use DER but not all DER certificates include private keys

P7B (PKCS #7) certificate used to share public key and never includes private key

PKCS - public key cryptography standards

69. Org negotiating with outside vendor to host cloud-based resources. Want to ensure they commit to returning systems to full operation after an outage within a certain time. Which negotiating?

A. MTTR
B. NDA
C. SLA
D. DLP

service level agr...

SLA – agreement between company and vendor for performance expectations including recover system within timeframe

MTTR is the mean time but is not the guarantee

NDA – do not disclose proprietary data

DLP data loss prevention device that monitors outgoing traffic for sensitive info

70. Org hired consultants to evaluate forensic processes. Evaluating processes and tools used for digital forensics to identify any variation that may exist.

A. AUP
B. NDA
C. SLA
(D.) MSA

...ecurity analysis

measurement system

MSA - evaluates processes and tools used to make measurements

Acceptable use policy AUP

informs users of company expectations when they use pcs and networks

defines acceptable rules of behavior

71. Org developed incident response policy and starting on plan. What is first step of incident response process?

(A.) Preparation
B. Identification
C. Containment
D. Eradication

Preparation
Identification
Containment
Eradication
Recovery
Lessons learned

to increasing

72. Been responding to [illegible] amount of alerts. Want to automate responses without realtime involvement of team.

A. SOAR
B. DLP
C. STIX
D. TAXII

Security orchestration, automation, and response

SOAR

Structured threat information eXpression

STIX - standard language used to share cyber threat info

Trusted automated exchange of indicator information

TAXII - set of services and message exchanges to share info

STIX = what to share

TAXII = how to share

73. Admins isolated linux server after successful attack. Forensic analysis needs to create image of hard drive.

A. tcpreplay
B. chmod
C. dd
D. Cuckoo

dd - copy files and disks for analysis

tcpreplay - suite of utils used to edit packet captures and resend them

Cuckoo - open source malware analysis system
analyzes in sandbox

74. Forensic expert preparing to analyze drive. What to do first?

A. Capture image with dd
Identify order of

D. [illegible]
volatility

C. Copy contents of memory with memdump

D. Create chain of custody document

before analyzing, capture image then analyze image

first real step is to Create hash of original drive

order of volatility - which data is most volatile (cache) and least volatile (hard drive)

memdump - copy contents of memory, not disk

Chain of custody document is created when evidence is first created

Host ecommerce site

15.

selling renewable subs.
Monthly, annually auto.
Dont want to store credit card info. What use instead?

A. Pseudo-anonymization
(B.) tokenization
C. Data minimization
D. Anonymization

tokenization - stores token created by card processor instead of card #

pseudo-anonymization - replaces data with artificial identifies, but process can be reversed

data anonymization - modifies data to protect privacy of people by either removing PII or encrypting it

data minimization - require orgs to limit the data they collect and use