Good evening everyone I'm Dr. Mann and I'd like
to welcome you to tonight's review session
for the Security+ exam. Tonight's topic is
threat actors and intelligence parts one and two.
Our first question tonight involves
attack vectors: While adding a new employee
to the configured network you realize that there
is an additional Wi-Fi network configured that
you were not aware of as the system owner. What term describes what has
taken place?

Please take a few moments, look over the answer
choices and then let's see what you're thinking.
It looks like we've got a few votes for D, Shadow IT
and Shadow IT is in fact the correct
answer. Shadow IT refers to information
technology systems deployed by departments
other than the central IT Department to perhaps work around perceived
shortcomings
or maybe actual shortcomings of the network.

This often introduces security and compliance
issues, the kind that we really don't need
the obviously incorrect answers here
are going to be penetration testing
and pen testing or ethical hacking, authorized simulated cyber attack on
systems
It is not also industrial camouflage.
Industrial camouflage is really the act of
designing buildings possibly even campuses so
as to hide their true size and nature or purpose.
And then automated indicators sharing is
basically a mechanism that allows the sharing
of real-time threat information among communities
such as CISA - cyber security infrastructure agency.
So it really leaves us with the best answer being
Shadow IT. Let's move to the next question.
And it will be attack vectors too
Okay a company's IT specialist is
currently configuring the firewall settings.
He is configuring it so that the web server
which resides in the company server room only
allows HTTP connections. Additionally there are
important customer data on the back end database
that is stored on the same post. Which of the
following security problems best fit the scenario?

Again take a few moments look over the
answers and let's see what you're thinking.
We have several votes for Choice A
and Choice A - indirect physical access Insider
threat - is not the correct answer. Now as we
look at these choices and let's say we have
another vote in the okay we have vote for D

in the chat, okay, and so direct physical
access Insider threat is the correct answer.

I think it's pretty clear
that phishing doesn't really
have anything to do with the scenario so we
can pretty readily eliminate choices B and C.

So the IT specialist working for
the company is directly interacting with
firewall to only allow HTTP connections to
the server and this action by job constitutes
an Insider threat because first of all by
only allowing HTTP connections to the server.
You know we're we're allowing unencrypted data
to be transmitted between server and client
and so if there is anybody monitoring then you
know they can intercept data and read it but
this this insider thread comes from the fact that
the IT specialist working for the company has
made what you might consider a grievous error but
really it's it's a little more than that certainly
an IT specialist is going to understand the
ramifications of allowing HTTP connections through
the firewall. So the best answer the security
problem that best fits this scenario is direct
physical access inside or threat.
Let’s go to the next question.

Attack vectors III:

One infamous example of this type of
security issue regarding attack vectors

is the Target data breach which
was made via Target’s HVAC supplier.

Okay take a moment and see what you think.
Okay that's good this did not take long;
let's see what you what you're thinking.
so the majority of votes are for Choice
D we supply chain and that is correct
The Target data breach was an
example of a supply chain attack
This was way back in 2013 Target was hit by
one of the largest data breaches in the history
of retail industry and the attackers were able to
exploit third-party access to export trade payment
information which ended up impacting more than
41 million customers so in supply chain attack.
It's in the attack strategy that targets an
organization through vulnerabilities in its
supply chain; these vulnerable areas are usually
linked to vendors with poor security practices

a data breach through a third party vendors
possible because vendors require access to

sensitive data to integrate with internal systems
the choices the rest of the choices are not best
bits or even good fits so with social media the
attack vector of a big one a major one is phishing.

Email so an example of an attack using email
as the attack vector would be spear phishing
and cloud-based attacks attacked or attacks that
are focused on the cloud services provided to the
company so the choice that best describes this
and is the most accurate is supply chain attack.

Okay

Attack Vectors IV:

An employee named Janice is on her way to work
when she is walking into the office she stumbles
upon a mysterious thumb drive; the next day
Janice's computer is filled with malware
even though her company's network is not
connected in any way to any external networks.

What most most likely caused
the malware on her computer?

C
Was that B or D. Did you say D?
Yeah.
Let's see what's in the chat; yes lots of votes

Janice connected the removable device
to her computer and it was infected okay so that
is the clearly correct answer and what is this
type of attack known as? What would you call this?
Anybody?
I read the help once I got that so
so what what kind of attack…
I did not hear you clearly.

Okay that might have been ambient noise. So this type of attack is known
as baiting
and um it really does play on human
nature and our curiosity about things.
I've heard of it being done
with you know optical disks but the
probably the most expedient way to you know
commit this attack is to use something like
the flash drive. This is not
clicking on email filled with malware
um it's not downloading a malicious

file on a web browser or credentials.
If you are talking about malicious
files on web browsers we're talking by

Drive talking about drive by download tag um or
if we are talking about weak credentials the
implication here is that um we're talking
about some type of brute forcing attack.
This obviously happens when you have
weak credentials such as a password
That might be spelled uppercase P@ssw0rd. I know you've all seen this one over and over.
This is a baiting attack
description okay I don't know

Okay attack vectors V: A _____ will
verify that a vulnerability exists then we'll
actively test and bypass security controls and
will finally exploit vulnerabilities on the system.
Take a look at the choices which
term describes the situation.
We have answers coming into the chat
and it looks like the majority of them
are for A; we have some choices for D.
00:13:12.660 --> 00:13:18.240
And one for C.
So the correct answer here is a penetration test, colloquially known as pen test or ethical
Hacking. This is an authorized simulated cyberattack on a computer system or network performed
to evaluate the security of the system and should
not be confused with the vulnerability assessment
a cyber threat hunt or cyber threat hunting
is a proactive cyber defense activity.
it is the process of proactively and iteratively
searching through networks to detect and isolate
Advanced threats that evade existing security
solutions now vulnerability assessment is the
process of identifying quantifying and ranking
the vulnerabilities in a system. It's a common
security procedure as it provides a detailed view
of the security risks an organization may face
enabling them to better protect their information
technology and sensitive data from cyber threats
and finally finally the vulnerability scanner
is an automated vulnerability testing tool that
monitors or misconfigurations or coding
flows cause pose cybersecurity threats.
Vulnerability scanners either rely on a database
of known vulnerabilities or probe or common law
types to discover other types of vulnerabilities
the best answer here is penetration test.

All right. Moving onto the next question: Dark Net.

Which of the following is an example of a dark net?
Okay
Let's see what you're thinking?
Okay so we have some votes for Choice B and D
Okay one for all D okay so in this situation the
correct answer is D all choices all answer choices
are correct okay so freenet, peer-to-peer platform
for censorship resistant anonymous communication

It uses a decentralized distributed data
store to keep and deliver information and

has a suite of free software for publishing and
communicating on the web without clear censorship
pre-net is considered a part of the
dark web it is a decentralized network
that allows for the chain exchange and encrypted
data giving users more anonymity okay it's
important to note that not all content on freenet
is illegal or harmful and it may be used by people
who want to communicate Anonymous anonymously
and securely for legitimate reasons tour is what?

Anybody?

I think most people know what tour
is okay we have some responses is

it like a browser? oh yeah it's
a browser
Okay what else is it?
Or what does it use?
Okay.
So first of all it's short for or an acronym for the onion router free
open
source web browser um and allows you of course
to use the internet anonymously it is open source
and um the technique used is called onion routing
which involves encrypting your data multiple times
then passing it through a network of volunteer run
servers so TOR is a critical part of the dark web
um it is often used to create and access
the dark web however it is important to
note that not all content on TOR is
illegal or harmful and again people
could be using it for perfectly legitimate
reasons and then I2P - who knows what that is?
so I2P - the invisible internet project - is
an anonymous network layer that allows for
censorship resistance peer-to-peer communications
it is a peer-to-peer distributed communication
layer designed to run any traditional
internet service like Usenet IRC file sharing

Etc as well as more traditional distributed applications okay so this also can provide an encrypted entrance to the dark web and therefore it makes up a part of the dark web ecosystem

okay um I guess also to note the I2P has stayed somewhat clear of criminal and malicious activity it is still an important data source for Security Professionals and you should be aware of it.
Let's move on.
So which role is primarily responsible for data quality?
Okay I have one response.
Two responses for Choice B
Okay anybody else have some input into this?
May be an A.
okay so the correct answer here is data steward now a data steward is an oversight or data governance role within an organization and is responsible for ensuring the quality and fitness for purpose of the organization's data assets including the metadata for those.
they create processes that allow members of the company to interact with data.
For example they may create processes for how to collect data how to enter it in databases and how to share it between databases data stewards use their problem solving skills to detect the causes of errors in the data and to determine solutions that protect the Integrity of the data they may also solve problems by creating policies and processes that help prevent issues that may occur during data collection and maintenance okay.

All right so we have several questions involving data roles and responsibilities

Let's go to the next one

So what is the data owner primarily responsible for
A?
Maintaining the confidentiality integrity and availability of an information asset
so if you do some research including in your textbook or other places like INFOSEC, the data owner has basically several responsibilities including establishing the rules for data usage and protection, cooperating with information system owners on the security requirements and security controls for the systems on which the data exists, the data owner also determines how data is classified, managed

and secured which plays an important role in
the company's cyber security controls, a data owner
holds accountability for a specific data set.

Let’s move on to the next question:
Customer email data is sold to a third party
that then gets inadvertently used by spammers.
Which data role is responsible for this data leak>
Votes for B D and B in the chat. Anybody else want to weigh in on this?
Okay, the correct answer here is data
controller and the data controller is an
individual organization that manages how the data
is processed and is responsible for complying
with data protection regulations. They manage
data processors dictating how the organization
analyzes and uses personal data such as contact
information, addresses and identification numbers.

Let's move on to the next one.

Your data controller picks a vendor to handle their marketing campaign
but sensitive user information is leaked; what role is the third party
plane?
B.
Okay so you think data privacy officer?
Or did you say deed data controller?
I said B.
Okay, All right. Anyone else?
I was thinking D because assembly to the last one okay
So the correct answer here is a data processor.
I think you're seeing that or maybe it's feeling like there's some
overlap
in the roles and again especially
when preparing for as part of the
exam you want to be clear on the roles that are
related to each other but interact differently
so the role that data processor is
to be responsible for carrying out
the actual processing of the data under the
specific instructions of the data controller.
The duties of the data processor may include
design create and implement it processes and
systems that would enable the data controller to
gather personal data use tools and strategies to
gather personal data and Implement security
measures that would Safeguard personal data
the processor must ensure that the people
processing the data are subject to the duty
of confidentiality appropriate measures need to
be taken to ensure the security of the processing
under a written contract the processor
must only engage a sub-processor
with the controller's prior approval
so there's a relationship there

but they are different and they do have
different responsibilities.
Okay so we have here
00:27:55.260 --> 00:28:01.260
I see your point they are all similar
and vague is there a way to distinguish them
and my suggestion is to use more than one
source of information and of course you want

to use trusted sources and read through and make
notes um because you're right there there is some,
there can be confusion here and again it's because
when two roles like processor and controller
can easily be confused you really need
to sort of delineate what each role does
and you'll see that one sort of either feeds
into the other or manages the other and it
really boils down to again careful research
and making some notes and the other thing.
The other advice that I can give you that I
know works is to try to come up with examples
or finding samples if you find these confusing
I have a few more notes here that I want to
give you on some of these roles and since we're on
data processor right now I would also like to say
that data processors is responsible for creating
and implementing process implementing processes
that enable the data controller to gather data
store it and transfer it if it's necessary
a processor may be more or less involved in
the processing but the main differentiator
is the fact that the controller determines the
overall purpose of the processing.
Data custodians - the data
custodian - is responsible for the implementation
and maintenance of security controls in a
way that meets the requirements for security
has determined by the data owner the data
custodian manages the technical environment where
data resides and ensures safe custody transport
and storage of the data okay so are they like when
someone is leaving a company and they have or
someone has certain rules in the company do they
manage who has access to that like say you go on
vacation and you're in control of certain parts
um you do like a specific job and someone's
coming to take over that room light are they
in control over like they divvy out who has
access while you're gone kind of yeah it kind
of flows from the owner to the controller and the
processor so you know it's not exactly to correct
to say that you know one entity manages it all I
really prefer to think of it as sort of the chain
of actions and again typically starting with the

owner flowing through the controller the processor
um the custodian has some say for example is um
that it was going to be stored on the cloud for
example so so that's like a technical environment
where the data would reside and that falls in the
purview of the data custodium so again you know
looking at the hierarchical flow could be very
helpful or understanding this um and then there's
a question is there any flow chart of these roles.

I've looked through the
text that these questions are are developed
from I don't exactly see or have not seen
a flowchart but I think it'd be a great idea
if you made something akin to that it could be
a flow chart of roles and responsibilities and
or or some other hierarchical flow diagram that
would you know sort of help you to delineate the
functions associated with each role and again
examples usually help to clarify this as well.
It can be kind of confusing
so again careful notes and
again a type of a flow chart or a
hierarchical layout and organization

Okay all right let's move on

A detective believes that a terrorist
has embedded top secret military information
in an image as a way to create a confidential
message channel with an anonymous user which
of the following techniques describes what the
detective believes that terrorists had perpetrated
So okay so you got lots of responses right
away and I'm betting they're all going to
be a that's really good so everybody's on this
and the correct answer is steganography.
If we look at the other options that are incorrect
we should talk about those the key stretching it's
also known as key strengthening and it's a
technique used to ensure that a weak key such
as a password is not or does not fall victim
to a brute force attack in key stretching a
special algorithm it's used to convert a weak
credential or password into a stronger key
and there are two common algorithms used to
strengthen the key uh pbk dm2 and decrypt so pbk
df2 I just have to love these acronyms stands
for password-based key derivation function two

It's a key derivation function with a
sliding computational cost used to reduce
vulnerability to brute force attacks. pvkdf2
applies a pseudo-random function such as a hash

based message authentication code to the input password or passphrase along with the salt value and we've talked about that in the past and repeats the process many times to produce a derived clean which can then be used as a cryptographic key in subsequent operations. Clustering is a type of unsupervised machine learning that enables

companies to uncover hidden patterns and structures in large sets of data. Okay so not what steganography is; it's it's looking for these but steganography is actually doing this to embed something within something else um let's see clustering means grouping together similar or related data points that are found throughout the network making it possible to reveal unusual patterns of activity and detect attacks that would not be detectable by analyzing a single point clustering techniques can help to uncover the hidden patterns and structures from data sets. I think everybody got this very very quickly.

Next question:

Honey pots - Your organization's IT specialist has intentionally configured a honey pot on your network to make sure that your vulnerability scans are accurate unfortunately the vulnerability scans are not accurate because they did not report the honey pots as being vulnerable. Which of the following is most likely a reason for this malfunction? Take a moment and look at the choices. We have five responses in the chat. They are for Choice D. Choice D is correct all answer choices are correct. So the scan was not as administered as root so if performing a vulnerability scan you should ensure that you're performing it um uh well first of all as an unauthenticated user. It's non-credentialed to find out what information is being exposed to unknown persons on the network and then you should perform the scam as or logged in as an administrative account as root for example and this way you're unable to collect as much system information as possible information you couldn't get if you weren't using an administrative account or logged in as root Okay um let's see the vulnerability database needs to be updated that's a possibility if you're using that and finally nothing's perfect. Vulnerability scanners do not

always catch everything and that's a fact
on another note a vulnerability scanner
is different from a port scanner the
vulnerability scanner will scan the system for
known vulnerabilities and then report the problems
that have been found the vulnerability scanner
bases the decisions on a vulnerability database that is hopefully
constantly updated when the
vulnerability scanner compares the patch level

and configurations of the systems against
the information contained in the database
then it enables you to know if you have been
following for example best practices or if
in fact there are vulnerabilities so that covers those responses.