Our first question involves indicators of compromise
All of the following are examples of
indicators of compromise except for what?
Please take a moment look at the answers
and let's see what you're thinking.

So far,
it looks like everybody is saying that
A, an incorrect login attempt, is
not an indicator of compromise.
And another vote for a C and another vote for A. So the correct
answer here is an incorrect login attempt
and basically an indicator of compromise
is some kind of element or artifact
that indicates there's been a security breach so
excessive bandwidth usage could be one of those
certainly suspicious emails or Rogue Hardware but
an incorrect login attempt is not a breach so
that is the one that is not like the others and
A is the correct answer for this question.
An employee suspects that their work email
account has been compromised because they
keep getting suspicious email advertisements
from companies that they did not subscribe to.

What reconnaissance tool should the employee
use to further investigate this situation?
Take a moment look at your choices
and let's see what you're thinking.

Anybody have any suggestions as
to which is the correct answer?
We have one response, two.
So the two responses both are for Choice C.
Open source intelligence
Does anybody else have a suggestion?

And we have another response in the chat D. No.
C is the correct choice, open-source intelligence, so in the question
you're asked what reconnaissance tool
should the employees to further investigate
and I'm thinking and hoping that it's pretty
obvious that choices A and B are the ones that
can be the most easily eliminated um I've
really never heard of academic journals being
a reconnaissance tool or requests or comments RFCs
that does leave us with open source intelligence
and private internet information sharing
and analysis centers. Private information
sharing and Analysis centers - so
with open source intelligence
easily using open source roasts and
tools you can easily retrieve information
about a company that is available publicly

um so information sharing and analysis centers.

Basically we're talking about organizations
that provide a central resource for gathering
information on cyber threats and in many cases
that are the information that is critical to
infrastructure as well as allow two-way sharing of
information between the private and public sector
about root causes incidents threats as well as
sharing experience and knowledge and analysis.

So private ISAVCs were created to address
U.S. critical infrastructure vulnerabilities
and facilitated the sharing of actionable cyber
security intelligence among trusted organizations
within an industry and between sectors
private sector and public sector.

So open source intelligence is
the best answer for this question.

Let's go on to the next one.
I believe this is it:

Threat actor types: When someone is worried
about malicious users potentially compromising
their servers while remaining undetected for a
period of time, this is known as a blank threat.
Do you think is the correct answer here?

Let’s see what we have in chat - votes for ATT, which is Choice C
Vote for D, vote for C, vote for C [1]SEP Yeah advanced persistent threat is
correct.
We're worried about server compromise and
remaining undetected for a period of time.
The first choice may not be the most obvious
denial of service would probably be the most
easily eliminated and denial of services is
of course just that there is no really
attempt for basic denial of service to
remain undetected it happens service is denied.

So “man in the middle” or also
known as an on path attack,
and this occurs when the attacker sort of sits
in the middle between two stations and is able
to intercept information and sometimes they
cannot just over not only intercept and read
or just intercept and have it to work with
but they can change the information as well.
So this type of attack can occur without
anyone knowing uh that someone is sitting for
example in the middle of a conversation and

again that's that's why the classic name that I
think of uh for this type of attack is man in the
Middle. Cyber Espionage is the act of gathering
secret or sensitive information for personal gain
technological purposes or political reasons. It's
not military interaction by intent so really we
are left with advanced persistent threat or APTs
and here the goal is very clearly to remain
Undetected. there have been many such attacks
these some of these have gone undetected for months and months.

So the key in this question is remaining
undetected for a period of time and advanced persistent threat is the
correct answer. All right let's move on.

Which best describes the term Hacktivist?
Take a moment and let's
see what your responses are.
Good we have lots of responses coming in fairly
quickly; I think this one is fairly obvious.
So the correct answer is a malicious user
attempts to promote a political or ideological
stance; a hacker engaged in authorized
pen testing or other security consultancy
that is not a hacktivist; an inexperienced unskilled
attacker that typically uses tools or scripts
created by others. What kind of threat actor
is that?
A Script Kiddie.
Very good.

An unauthorized hacker
operating with malicious intent

What name might we give to
that type of threat actor?
Nobody has a suggestion for that?
An unauthorized hacker operating with malicious
Intent. We have a response: a cracker.

A black hat hacker that is the the typical
moniker given to this type of threat actor.
Hacker engagement authorized penetration
testing. I mean the the key there is
authorized so we're probably almost certainly
talking about a white hat.

So activists political or ideological stance

Next question.

One of your organization's employees
doesn't think they are getting paid enough.
when they notice that the salary database file

is available on the network they try to guess the password a couple of times which of the following choices best describes this type of threat.

Lots of responses good and it looks like they're B; this is The Insider Threat. It's not an external threat that's I would think pretty Obvious. An external threat would not be Primitives in organizations employees uh State actor this is not a state actor and it is not a hacktivist. This is again if we're thinking about you know How do you classify threat actors and you know we have a set of nomenclature for doing this of course examples again are useful. Insider threats of course are dangerous because they can be hard to detect especially if they are designed to go undetected for some time um the the common scenario here might be the disgruntled employee or or uh for for whatever reason so they're not getting paid as much as someone else or you know maybe they suspect that they're going to be released from employment for for some reason one common scenario with programmers or software engineers was that it they thought something like this would happen they might plant something like a logic bomb inside companies application product for sale to customers and um if we software wasn't contacted or given some type of code or validating access for a period of time then that would set off the logic bomb and cause whatever damage the disgruntled employee intended. So there's an example of an insider threat right.

Janice has just graduated from college and her first job has her conducting penetration tests; which type of hacker best describes Janice? This is what I expect lots of votes per D - white hat and that is the correct answer.

Obviously not a Script Kiddie let's see conducted penetration tests it does say her first job so we can barely safely assume it's not a black hat threat actor type nor is it a gray hat. That was pretty obvious on the subject of gray hats foreign there is a they are a type of in between sort of threat actor and what I mean by that is that a gray hat could be someone who violates ethical standards or principles but may not have the same malicious intent that a black hat hacker would have or that that we would ascribe to a black hat packet.

They can engage in practices that
are you know not exactly above board
but sometimes they do these things
and operate for the common good.
So if we try to classify great hat hackers
um there are those that great hats that hack
for personal gain and then those who hack for
personal gain but also to improve security which
you know it's it's hard to say
exactly what um those motivations are
so as far as classifying threat
actor types so sometimes we refer to
a white hat with a black heart - so wrong, very figurative speech -
but you know again you've kind of
got this this individual who is you know
part white hat and part black hat you know and
and um and that's really what it boils down to
it is a controversial practice that sort of
fits in between somewhere in between illegal and
legal activity  so a little unusual again.
You know I'm sure that there are many reasons
why somewhat would exploit a vulnerability and
then after receiving some type of gain for it.

All right let's go on to the next question.

A _____ is the type of malicious
actor that is most likely to have the
most resources and funding since they work with
their country's military and security services.
This one should be really easy.

I'm judging by the number of responses we are talking about the state
actor here and
I would like to point out that this even though
the question is talking about a malicious factor
the real threat here comes from the fact that
we aren't talking about just one but a multitude
of threat actors and then of course when you know
you have the funding and the backing of the state
of some countries military or security
services or other governmental service
you have typically a
formidable force to deal with.
Resources and funding typically not
a problem. Think about it in the
sense that you can have hundreds of people who you
know go to a job and their job is to sit there and
poke at us or some other country or organization
and to seek out vulnerabilities and exploit them
and that really is a danger here not
just that it's one malicious actor.

Let's go on to the next question

Which of the following is not
considered a potential insider threat?
Take a moment and let's see
what you think about this one.

So we have several responses for D and that is the correct choice.

As I I've pointed out before
and I will point this out again
when you are asked a question but it is not
which of the following is not this or that
these questions can sometimes be a little
confusing or not as obvious you just have to
think about it and as always good practice is to
read the question twice make sure you understand
what you're being asked for so which of the
following is not considered a potential Insider
Threat. Contractors, business partners all would
be involved with an organization at or by request.
Infected email file attachments
not an Insider threat. It comes
from an external source. So all of these are correct. Let’s go on.

Which of the following
is not true about a TTP?

Take a moment read the answer choices
carefully and let's see what you're thinking.
So we have a response in the chat or D Choice D
Any other suggestions? Which of the following
is not true about a TTP clearly one of the
things this question hinges on is understanding
the acronym TTP and what does it mean?

So a couple more choices - one for C and
one for…
I'm confused about this one — understandable
So again when faced with questions
that are asking you what something is not,
it helps to pinpoint what the question is talking
about and the question is talking about.
TTP - which does stand for tactics techniques and
procedures - so which of the following is not true:

TTP stands for tactics techniques and procedures; Well, that is a true
statement.
TTP encompasses the mapping out of specific malicious
user activity and that is a true statement.
TTP is evidence of an indicator of compromise.
That is not a true statement answer; Choice
C is the correct answer. TTP is a generalized
statement of adversary behavior and it can
be so the tactic is a high level description

of an action a threat actor takes a technique is
a more detailed description of a tactic and the
procedure provides step-by-step details on how
the threat actor would accomplish the behavior.
So again the question hinges on understanding what TTP means.
tactics techniques and procedures are what
it's an acronym for but then understanding
the meanings of the terms tactics techniques
and procedures and by what I've just told you.

Tactics being sort of the high level description
techniques being a more detailed explanation of a
tactic or description and then the procedures
finally are the step-by-step breakdown so you
can see that they sort of follow from one another
and so when you get this or you understand
that you can see why it is a generalized statement
of adversary behavior and compasses mapping out
of specific malicious activity and of course
stands for tactics techniques and procedures
leaving us with only evidence of an
indicator or compromise.

So again C is the correct answer - TTP is
evidence of an IOC that is not true and again uh and I just want
to add this as well that
when we talk about indicators
of compromise we are talking about
elements found on or in a system that
indicate that there has been a security breach
that's what an indicator of compromise is.

All right let's move on to the next question:

Which of the following is true regarding
gray hat hackers and white hat hackers? So
please take a moment read through the answer
choices and cast your vote for the correct one.

We've got responses in the chat.

And let's see so D votes, D vote, B vote, A and D.

A gray hat hacker and a white hat hacker both do
not have malicious intent so this question
sort of again shows us how you really
have to read the choices carefully and
if we start with say the first answer
a gray hat hacker has malicious intent.

As soon as we read that if you you understand how
gray hats work and perhaps what their motivation
is that is not necessarily true so we can
eliminate that choice a white hat hacker does

not have malicious intent that we know but the
gray hat has malicious intent not guaranteed.

A gray hat hacker and a white hat hacker both
have authorization. Well we can say that a
white hat does and be confident in that
a gray hat again may not have authorization.
A gray hat hacker and by the way
typically does not have authorization.

A gray hat hacker does not have malicious intent
while a white hat hacker has malicious intent in
that second phrase clearly rules out answer Choice
C so the correct answer a great hat hacker and a
white hat both do not have malicious intent is
the best answer for this question. The best answer.

Let's see what we have here…
That one is confusing
Because neither I feel like
neither a or D are definites because
s it not possible for gray hat
hackers to um have a malicious intent  is it
is that impossible to rule out is that an absolute
that a gray hat does not have malicious intent.
I'm asking could could it be that they
do have malicious intent it could be
I mean and again it kind of sort of depends on
your your interpretation of malicious intent
So if a gray hat compromises the
system and for some personal gain
and it stops right there so the the system the
network the resources compromised the gray hat
gets something out of it and that's the end
of it I mean do you think that's malicious
because I mean I would consider that
somewhat malicious.
I would too.

If a gray hat compromises some resource that
they clearly are not authorized to access

and they do it anyway but then they publicize the
vulnerability that they were to exploit or that
they did exploit and made it available here again
you have to ask  so they found a vulnerability, exploited but then they
made it available the
real sort of balance point here or the point
that's going to throw it out of balance
is who did they make it available to you.

For example if you compromise you know maybe
Acme bank for example right and then you know

you called up Acme headquarters and go hey
guess what I was able to get in your system
that's different than I compromised you
and then I made it publicly available.
If you make it publicly available who's to say
that another bad actor would not read about your
your information about a vulnerability found and
exploited and then go in and do the same thing.
Do you see what I'm saying.
Yes that's what makes it confusing it does make
it confusing because because the answers are
the are the answers are written as absolutes
sorry go ahead I was just saying trying to do
deductive reasoning just from even this this tonight's training because
you you spoke
about this just a little while ago and about
how sometimes gray hat hackers may have a
malicious intent mm-hmm yeah so so going
with that reasoning and then trying to answer
this question it's just confusing a little bit

So it's safe to assume when
we see a question like this that
we're not going to think that the
gray hat hacker has malicious intent
so I'm not sure I would say that or make
that statement um let's let's take the other
comment and then come come back around with us
so someone else was saying something yeah I was
going to say that this question seemed it's like
it's based off a probability and if that a gray
hat hacker goes one way A is the answer and the
other way D is the answer. So, here again this is
the problem with this so-called gray area right
I mean you know so a white hat hacker is one
extreme and a black hat hacker is another extreme
and then there's this gray area the problem can
easily be your definition or their definition the
test creators definition of malicious intent
the other sort of bit of information that I
want to throw out at you is that these questions
were developed based on the text that
I believe you will have access to
and so in order to avoid any
kind of problems with copyright
um for lack of a better way to put it these
questions are paraphrases of the information
so I'm not sure that it would be this
confusing  um based on what I've seen um
Certification testing not just you know SEC Plus
or CompTIA or whatever agency you want to choose. Cisco for example um
they do tend to have some
anchorable information that is some information
that when you discover it and if you understand

it that you know it would take some of the
either confusion out or give you a basis to reason
on to choose or to then choose a correct answer.
But the way this is worded it's it's a little
confusing and again it really does
hinge on this whole phrase about malicious intent
Let's see we have some more comments in the chat.

Gray hat is a computer hacker computer
security expert who may sometimes violate the law or typical ethical
standards but usually does not have malicious intent typical of black hat
black hat hackers sole focus is to sow chaos
gray hats may do it but as a byproduct of
their actions motivated by personal gain
and this is someone's interpretation.
Gray hat might not have had and the white
hat has no malicious intent again so
it's the use of the phrase malicious intent and
your interpretation because again and even if, well let's go back again
to the example of the
Acme Bank this this fictional bank that
we're making up and if you are doing whatever
maybe you're a student and a researcher or
or some some situation such as that and
you find the vulnerability and exploited
you do so without permission so right
away that takes you out of the realm
of the quote white hat hacker or pen tester
because you never do something like this without
full knowledge and disclosure and permission
and and that's that's just how it is
so again the question becomes is that malicious
intent and you cannot say necessarily that it is.
you know maybe uh someone does this
and who knows maybe it's their bank
right and they feel like they have a
stake in it because they have a mortgage
with this bank and checking accounts
and savings accounts and they're like
and I just found a vulnerability and when I
was trying to exploit it I was able to do so.

So now I'm going to contact this Bank and
make it known to them. is that malicious intent?

No I don't think it is but it's
certainly illegal yeah right
I mean so again interpretation of malicious intent but
that's like also what certain people do for
like work they go around and exploit vulnerability
not vulnerabilities and try to get paid from it.

They're not necessarily trying to do anything bad
to the companies but they're trying to show them

that they're vulnerable and then hopefully also
get paid in the process and and this is why though
We have codes and laws that we follow and and
procedures and and things such as you know full

disclosure and and not even trying to do something
like this um because you know it's it's not
your property it is not a system or a resource
that is under your authority or direct control
so therefore if you've found a vulnerability that
does not give you the right to exploit it and if
you found a vulnerability you must be poking at
this system or resource so having rules procedures
what we would call legal action versus
illegal action is how we stay out of this
mess, how we keep it from being what it
Is.
Could be depends on the individuals and default otherwise they would be a
black hat. So the argument here is that gray hat does not
have malicious intent by default otherwise
we would classify them as a black hat hacker
if they change their intent
after the fact that's different
that's a very interesting point of view yes sir
I guess I could unmute my mic for that that's how I
look at it like if you initially have malicious
intent you're a black cat hacker but if you go
into something without trying to have personal
gain but then change your mind in the process and
decide that you could get away with it it might be
worth it then you're the gray hat hacker.

So if we don't have um the intention of
let's say uh exfiltrating information
the question still has to be asked
why are you poking and looking for
vulnerabilities without permission?
I think by the very nature of
the action right that the default
sort of response is going to be you're
you're doing something that is illegal
and I guess then the question becomes do we
associate any legal action with malicious intent?
This is starting to sound
like a very circular conversation.
it's the way the question is worded it's asking
what is true of both of them in my opinion only
two options address that and only one is correct
I think they're also an organization not to like
drag this topic out but isn't there also an
organization that is like built and kind of
helps out people who do hack into systems and
get in trouble legally like they kind of help
ERS who might kind of get caught up in a mess

when their intentions initially weren't to
do something bad they were just curious
and wanted to see how far they could get.
I mean what do you mean by help like someone
who comes to their aid or provides legal yeah
there's like a group of I remember their name
but they provide like legal aid for people who
especially like majorities like younger people
who are like hacking might not know the legal
precautions of what they're doing but they're just
doing it or they can get there's like groups that
are there for that as well and and there may very
well be um I think if it gets to that point for
example if we're talking about the high school
student and they get caught you know poking at
Bank of America  for example um you know
where that ends up and who makes that decision
I think is going to determine what
happens after that point so if it goes to
some type of court or legal procedure.
As far as getting help for that
there may very well be organizations that do, I will say that I am not
aware of them
so I think the best advice is to follow
what we what we that means what we generally
think of as legal action is
to follow those procedures and
you know not poke at something that doesn't
belong you and that you have no business poking at
It's very interesting conversation and I'm
glad that we had this time to discuss it a bit

Let's go on to the next question -

What type of hacker has unauthorized
access and malicious intent?

This is a description of a black hat hacker.

The last question

When using a Tor web browser the user can
be confident of which of the following and
you're directed to choose to everybody
take a moment and look at the choices.
Selections in the
chat A and C; A and C; a C A; and C
Choice A and C are the correct choices I would point out something and
you know obvious or not when you
come across a question like this
and especially when the answer choices are
displayed in this fashion my eye goes right
to that first phrase because each answer Choice
starts with they remain anonymous  so to me

you know it's it might be a little
bit of noise I ignore it because
if you're just looking from the point of view of
I've got to determine which answer is correct and
maybe I have to do this through the process of
elimination this phrase they remain anonymous
does not figure into it. So is it because
there are multiple layers of encryption;
is it because their network is
using ip6; is it because they don't
authenticate to use Tor or because
there's one layer of encryption
so what it boils down to is looking at the second
phrase of all the answers and in this situation
the correct choices correctly describe what's
happening when using the Tor web browsing in other
words yes there are multiple layers of encryption
because their network is using ip6 not necessarily
because they don't authenticate no you don't
authenticate you are Anonymous and you don't
have to authenticate kind of you know would
sort of not work right for remaining anonymous
and then because there is one layer of encryption
well that's just not true there are multiple
layers  so again you're looking at the
second half and you're really looking at which
of these statements are true concerning to our
web browsing  and that's the last question
for this evening session. I'd like to thank
you all for joining us for this review session.