This is session two for this evening and our topic area is host app and data security and let's go ahead and start with the first question.

Backup Keys - What is it called when an organization invests in a third party to archive their backup keys because they don't have the capability to store those keys securely on their \
own? Are we talking about: Issuing; Escrow; Revocation; or Stapling. What do you think?

So we've got someone else holding on to, in this case, or archiving backup keys because of a lack of ability to store them securely? What does this sound like?

So again is there some one of these answers that looks obviously incorrect?

Stapling?
Okay.

How about revocation? Is anything being revoked here, taken away? No not really.

In fact this this question is really kind of the definition of the word escrow.

For example if you have a mortgage payment right and you have mortgage on your home \
and your mortgage servicer takes in a certain amount of money and part of that is to pay for the mortgage and the money you've borrowed but also so they take money to put into escrow to pay your taxes every year so they are the third party, the party between you the owner and the local government to whom you pay the taxes so they are an escrow party and that's what we're looking at here. So there's our correct answer.

Email transmission port:

So right off the bat you can already see that this question is dealing with well-known ports
And you can see that's pretty much what's listed in the answer choices.

You need to set up your company's wireless routers to transport their log files via email to your central logging system but your email servers are behind a corporate firewall.

Which port would you need to unblock to enable the transmission of messages between these two hosts? okay what are you thinking is it: TCP 25; UDP 25; TCP 110; or UDP 23?

Anybody have an answer?

Okay so the question involving port numbers and, as I indicated earlier, well-known port numbers - so this is an expectation not just on Security+. If you were doing Network+ or even the A+ certification exams or Cisco CCNA, you would be expected to know what these port numbers are.

So what are we dealing with here? Is there there an answer that that is pretty much not right?

What could be eliminated pretty quickly?

Anybody want to take a guess at this?
Which one of these could be eliminated?

Or which two do you think may not be good choices?

So to answer that or to to think about that and be successful you have to know what the port numbers are and the one that sticks out as the easiest to eliminate is going to be choice number four because Port 23 is what does anybody know which protocol uses Port 23?

Okay so that's Telnet and that really doesn't have anything with to do with email transmission.

Okay so that's our one choice that gets eliminated pretty quickly; now to answer the question as I said you do have to understand.

What the port numbers are so Port 110 is used by POP3? Does anybody know what POP3 is?

Okay, so Post Office Protocol for unencrypted access to electronic mail. The
port is intended for end users to connect to a mail service to retrieve their messages and the question talks about transmission in this case wireless routers to transport
log files to a central logging system but the email servers are behind the corporate firewall
so 110 is not really what's being described.

In this question, so if you know those facts that leaves us with answer choices one and two and you know at this point you just have to know that TCP 25 is what we're looking for and basically when you're dealing with email transmission servers communicate using TCP port 25.

So the correct answer is TCP 25 and let's move on to the next question So we're dealing with
IoT security and IoT is what?

It's another acronym.

Internet of Things?
Yes, Internet of Things. So this is a multiple choice question.

Which of the following are examples of smart or IoT devices?

An air-gapped wearable device; UAVs/drones; System on a chip; a smart light bulb.

Okay, what do you think?

Is there something that can be easily eliminated?

A smart light bulb?

Okay why do you think that could be eliminated?

I already have a good justifiable reason it; just kind of stands out a little bit.
Okay, so when we talk about Internet of Things and sort of implied in the definition of the acronym Internet of Things, we're talking about devices that
have the ability to communicate over a network.

What does air-gapped mean? Have you heard this term before?

No.
So air-gapping is a technique to prevent network communications to a device

So if a system is air-gapped that means it is separated there is no connection
and so the ones answer Choice here that can bemost easily eliminated is an air-capped wearable device, okay, and that leaves us with three other choices: UAVs/drones; System on a chip; or a smart light bulb. Let's revisit a smart light bulb; because that is definitely one of the choices perhaps you seen or heard about
these things that you can purchase them.

These devices can be connected and such that you can be watching some type of movie and if you have several of these smart light bulbs they can change the brightness or their color based upon what you're seeing on the video so they qualify as an Internet of Things type of device.

Now that leaves us two other choices, UAVs/drones or System on a chip.

What do you think? Is it one or both?

It's definitely the drones because so they operate on a network as well.

Yes that is correct. How about a system on a chip?

I don't think so.
That's right. Well here again the implication is that you've got this isolated thing and you know there's nothing more in the description other than the word system so could it be like a microcomputer system sure could it be some type of subsystem, yes, but there's nothing really in the answer description itself that implies something that would have the ability to communicate with something bigger, that could have these type of communication abilities.

But by itself it's not a good answer so your best answers are UAVs/drones and a Smart light bulb when a software publisher is issued.

A/n _____ blank they guarantee the software application is both from the expected entity (Signed) and unchanged (signed digest).
So what are we talking about here? Root certificates; Code-signing certificates; Code signing
key; or offline CA.

Somebody want to take this one?

How about an answer that could be easily eliminated?

I think the answer has to be out of the second or the third one so I think the first and fourth can be eliminated. Okay, so of the second and third is there anything that looks like it might be
more correct than the others? The second one is what I'm leaning towards. And that’s a good choice because this is the correct answer.

So basically code-signing certificates are used by software developers to digitally sign applications and or drivers or other executable types of software and it allows end users to verify that the code came from someone and has not been altered by a third party.

The answering of this type of question also depends on knowing what some of the terms mean, so for example, offline CA and the offline CA provides separation between the root CA and the rest of the public key infrastructure which limits its exposure.

But that's not really dealing with software publishers issuing code-signed certificates.
Root certificates, again, nothing really to do with software publishers and code-signing keys or a key is typically something that is used to enable the transmission above and the sort-of
encryption or decryption of information. So code-signing certificate really is the
best answer for this type of question or for this question Specifically.
So okay let's go on to the next.

This question deals with Baseband. Which of the following is true regarding the term baseband?

And you're asked well it says choose all that apply but typically in the exams when you see the little radio buttons it's a single-choice answer and when you see the little square boxes it's multiple choices. Baseband is a digital signal after it is encoded; Baseband operating systems have been associated with several vulnerabilities over the years; Both NB-IoT and LTE-M are types of baseband technologies; or Baseband is a low-power wireless communications protocol used primarily for home automation.

So, here again, we're looking for something that can be easily eliminated. Do you see
any of those choices that can be easily eliminated?

So, when you look at the fourth choice and they talk about a low-power wireless communications protocol and they do say used primarily for home

automation maybe home use or personal use, does that sound like baseband or something else?

What do you think?

It sounds to me more like sort of a Bluetooth type of protocol, not something
that is going to be used over wider areas.

So I would probably look at that as a more easily eliminated type of answer. It helps if you understand something about baseband transmission which is the transmission of
an encoded signal using its own frequencies and it does not shift or modulate to higher frequencies.

Does that help?

Anybody have an idea? One, two, three?

Okay, so this is again one of those that has a knowledge-based component that you would have studied or come across in your coursework. So the correct answer is going to be “Baseband operating systems have been associated with several vulnerabilities.”

These vulnerabilities some of them have given attackers the ability to monitor phone communications, place calls or send premium SMS messages or even to cause large data transfers and without the phone owner's knowledge. Narrow band IoT is a wireless Internet of Things protocol using low power Wide Area Network technology and then LTM-M is LTE cat M1 or long-term evolution, which you might know is 4G category M1 and this technology is for IoT devices connecting to a 4G network. So here again this question definitely involves some knowledge-based type of questioning here.

You guys heard of this NB-IoT, LTE-M?
Is this familiar to you?
No, not me.
Okay, well, that’s why we’re here.

Let's move on to the next one.

This involves Host hardening. There have been some security issues on your legacy and modern IoT devices. Which of the following security issues could have been apparent to cause you to decide to put those devices on a firewall and isolated network?

This is definitely multi-select….questions.

Your choices are: The device doesn't allow the admin to reset their credentials;
Does that sound like a security issue or could it be?
[t could be.
Okay,
I agree it could be.

The device doesn’t provide support for transport layer. Security issue?
Yes or no?
Yes.
The device uses a low-cost firmware chip and the vendor never produces updates.
Security issue?
Yeah.
The device prevents the attachment of USB devices;
Security issue?
Doesn't sound like it.
No, not really.

Okay so for this question the first
three choices are the correct answers.

Let's move on.

In order to monitor your corporation's network for abnormal traffic patterns, you must start with setting up what? Network diagram; Baseline; Exploitation framework; or Access control list.

Network diagram?
Network diagram. Anybody got any other choices?

Access control list?
Control list. Okay, Morgan.

I think access control list.
Okay so it is not access control list and it is not a network diagram. So we're
looking for abnormal traffic patterns.

How would you know if a traffic pattern was unexpected or not?

You would need to compare it with something
The Baseline?
Absolutely okay you normally Baseline your traffic network traffic patterns and this can be done with respect to say, for example, days and times and let's just take an example of a business and let's say that well let's say it's maybe a law firm. And what do you think?

Traffic patterns would be like say between 9-5 Monday through Friday.

Busy?
Let's say it's a fairly large law firm and most of their business is going to occur \
during the normal work week and normal work hours.

Well, they say normal: Monday through Friday, say 9-5.

If you baseline the traffic patterns over
those days and times you'll get some result.

If on a Thursday afternoon, say around two o’clock, maybe people are just getting back \
from an hour lunch and starting to see clients again and instead of seeing what you have baselined or normally seen say every Thursday at two o’clock, let’s say you start seeing multiple spikes in network traffic so that would then qualify as something out of the norm or an abnormal traffic pattern and a baseline reference enables us to see this very clearly. In fact it is called baselines and so that's the answer to this question.

Let's go to the next.

Regedit.Exe. You are tasked with exporting a registry subkey. What command would you run
if you are using regedit.exe?

So clearly this is a another knowledge-based, pretty straight forward knowledge-based question.

First of all, are you familiar with regedit?

No. No.
Okay so Regedit is a utility to edit the registry on a Windows system and so you know
without knowing that and the specifics of using this utility you really wouldn't have too much
of a of a good chance of getting this because it would mainly be a guess so I'll just tell you that
the correct answer here is the third answer: regedit/Export key file.reg.

Regedit with the slash jetted with the slash e file dot reg key um and basically this allows the export of the sub key to the file name.

Okay, again, this is something that you just you have to know and also another one of those things that you need to have some experience with or use or have used a lot to be familiar with this.

Okay, let’s move on to the next question.

This involves customer data storage.

Which of the following best explains why some multinational corporations need to control
where in terms of geographical locations they can store their customer data?

Does the term geofencing cover this? or Asset allocation; Non-disclosure agreements: or Data sovereignty?

What do you think?

And again as always is there something that sticks out as easily eliminated from their four choices?

Is the answer geofencing?
No, it is not.

They kind of look like a lot of the answers look like they could be correct.

Geo-fencing, we are talking about storing customer data but there's a phrase in here that is pretty helpful for sort of narrowing down the answers that praises multinational corporations.

The geographical locations in parentheses could easily lead you to thinking geo-fencing and that answers definitely what I would call a misdirector.

That leaves us with Asset allocation; NSAs or non-disclosure agreements: or Data sovereignty.

So this question really is discussing data sovereignty. Have you heard GDPR?

Yes,
Okay, so General Data Protection Regulation and if you've heard of this this is a regulation brought into effect by the European Union in 2018.

So we are in fact talking about data sovereignty and GDPR is the perfect example of data sovereignty and what this question is referring to and so again this was sort of brought about by the European Union as a means of protecting customer data and information.

I would like to point out that I have seen several versions of this question and one of those involves questions on this type of certification exam and some other and it asks if United States companies are subject to GDPR.

Now as we said that as I've already said this is something has come about and basically started in the European Union GDPR specifically is what I'm talking about.

So do you think that it would be applicable to United States companies as well?

Yes.
Yes, that’s correct; it is. But you have to consider under what conditions if they're selling to other people who are part of the European Union like if you have a website that people from that region of the world access even over here you still have to respect those post guidelines.
That is absolutely correct, So services are offered to Europeans or their European
Organizations. Yes, U.S companies are absolutely subject to follow the regulation so it's another way that you might see this brought about.

Very good, let's move on to the next one.

Okay so this question um involves post security. Sam is a student who is failing his math class and he just learned that he cannot graduate if he does not pass this class he goes to his teacher's computer and inserts a small connector that captures everything the user types between the keyboard and the computer's USB port he hopes to discover the teacher's password to give himself a passing grade in the class manually. Which of the following is most likely being described?

Is this an adware attack; a backdoor attack; a key logger attack; or a brute force attack? What do you think?

A key logger?
Sure, that’s exactly what this is. The obviously incorrect answer here was is going to be adware attack and brute force really doesn't apply to this.

But this is absolutely a key logger attack and you know the the giveaway here is that the intent is to capture everything the user types between the keyboard and the computer’s USB port and the idea is to hope to capture some credentialing for grading system applications and so you could go in and manually change his grade which is highly unethical and not recommended.

Next question: PKI risk deduction.

Your network administrator should do which of the following if they want to reduce the security risk of their Public Key Infrastructure: Use a password to generate your certificate request key;
Do not choose a wild card domain request a shorter expiration date;
or all of the above.

Okay, so what are you thinking?

Do not use a wild card domain?

That could reduce security risks. Is there anything else or is that it? I guess wow.

Shorter expiration date?
So then would it be all of the above?
Yeah, because as soon as you can see in a single answer you know single answer choice question if one or more than one makes sense then the only real answer that's going to make sense is all of the above because you can't choose them separately and that's just a test-taking technique.

But Use any passwords to generate certificate requests, security reduction, security risk reduction, not choosing wild card and shorter expiration Date. So yes, we are left with all of the Above. Let’s go on to the next one.

You have created a registry entry to disable the Windows AutoRun feature and exported it

to a .reg file named disableautorun.reg. You plan on pushing it out to all company laptops in a security update later that month after you finish testing it and get approval to do so. What is the command line command that will need to bE executed on all client laptops? Here again, we're dealing with regedit and we understand that as we've already previously spoken about that it's the registry editor or utility so this does involve again some knowledge about regedit.

However is there something that is obviously not a good answer here?

So the question’s asking about exporting something called disableautorun. Which these choices is obviously not a good one?

Notepad?

Yes, Notepad is nothing; it’s just an application and we can probably look at the file

But that's not going to help us with the task here. How about Poledit? Does anybody know what that is?

It’s probably not too surprising; it is an old utility system policy editor.

Let's see if memory serves correctly: Windows 95/98 and it was not installed with the operating
system but it was kept on the distribution media so you could use it if you wanted it so that really doesn't help us. That leaves us with regedit and then the file or regimport and again
you know we are trying to export this. We are trying to push it out; we are not trying to import it. So that leaves us with regedit, Disableautorun. That’s the correct answer here.

We have some more so let's get on to the next one.

I'm sorry can I ask you a quick question about
that?
Sure.
Do all the command lines when using regedit like have regedit at the beginning?
It's the utility.
It’s how you actuate the utility and then there are parameters after that like /e or /s and then maybe some further parameters but and that's typical when
you use a command line utility to use the name of the utility first and then followed by whatever
the switches and parameters are that go with it.

So in Linux-based systems you can find this information using the man command - short for manuals - and you know there's always going to be some kind of documentation available for this.

But that's you know very typical.
Thank you.

IoT Security: A credit card and driver's license were mistakenly left on the sales department's printer scanner which was then remotely compromised by a malicious actor who scanned the cards and apparently used one for unauthorized online purchases.

And the driver's license used to open a bank account in the sales customer's name.

Further investigation reveals that the attacker identified vulnerabilities in the unpatched printer scanner's web application component which was revealed through web app error messages

Which terms best describe the nature of this attack? And we're told to choose two. Here again we're always
looking for something that sticks out as being easy to . Do you see anything like that?

Can you eliminate ransomware?
You can.

And I certainly would. What else do you think could easily be eliminated?
Brute force attack?
Absolutely brute force attack is going to try every combination say for example if you're trying to crack a password and what has happened here is that specific information was exfiltrated and used so that absolutely leaves out brute force attack.

There is no real indication of asking for ransom on the part of the attacker so that really only leaves us with identity theft which driver's license and data exfiltration which is exactly what
happened here. Let's move on.

Last question: What is the best description of a self-signed certificate?

A certificate that has been physically signed by themselves rather than by a certificate authority; A certificate that has been physically signed by a certificate authority; A certificate that has been digitally signed by themselves rather than by a certificate authority; or a certificate that has been digitally signed by certificate authority?

Number three?
Number three. That is the correct answer. Obviously we're talking about self-signed by some
organizations so that clearly lets out certificate authority or choices two and four and one can also be eliminated because certificates this we are not talking about physically signed entities; we are talking about digitally assigned so digitally signed by an organization or even a user who's using the certificate okay and that means or implies that it's being used for internal use and for an application used by the creator but not to be used externally.

So there it is. That concludes our review on data security.

I'd like to thank you all for joining us this evening and I hope you found this useful.