Unit 1

I learned the detailed landscape of cyber security. Also about the CIA triad.

There are more factors than I thought in order to stay protected, but standards were great to learn.

At my work there’s many ways social engineering and ransomware can be a big threat. At a personal level I really want to stay aware of the risks and help friends and family to be more aware too.

I will extend the information to colleagues and teams, friends and family, making sure we're all educated, trained, and ready. I will keep myself up to date with [ENISA](https://enisa.europa.eu) reports, and other news media. The CIA triad can be used to better protect data at work and in my personal life.

Unit 2

I learned how encryption/decryption works in practice and when to apply a specific method.

Asymmetric encryption was interesting since I use SSH a lot, how symmetric encryption compares, and also how they are combined (hybrid encryption). Hashing and why it's used reminded me how we use it at work, and it made more sense to why this was the best method in some areas.

It makes sense that these techniques are not only used in dev environments, but in all communications.

I want to learn more about the math behind these different techniques to better understand them. I also want to learn more about the threats. And I want to review what encryption/decryption techniques are used at work and home.

Unit 3

I learned about the process of identifying and giving access to a user, what methods are used, and what threats there are.

Confirmed what I knew about weak passwords, but gave me insights into the importance of policies and guidelines. I enjoyed learning that passwordless was utilizing a key-pair to authenticate, and how combined hashing techniques can be used to store passwords.

Everybody needs to be able to prove who you are, what you've done, and having access to what is yours.

I will go over the process of identifying, authenticate, and authorize users at my work. I will also review the policies and guidelines, update them and make sure teams are informed. I also want to apply what I learned at home, helping my wife set up a password manager.

Unit 4

I learned that the internet and the World Wide Web are different, and how different devices can communicate based on shared protocols.

I really liked the overview that I got thanks to the OSI model and how the different protocols were designed to handle data between transmission layers.

The internet and World Wide Web is massive and used by almost everyone daily, and I think it's good for anyone to know how it all can work so well while expanding continuously.

At my work I'm most affected by the top layer (7. Application) of the OSI model, and I want to get more familiar with it and the neighboring layers in order to stay protected.

Unit 5

I learned more in detail what cyber threats there are and how to prepare and mitigate them.

I was chocked about the impact a successful attack can have, especially how common and impactful social engineering and ransomware attacks are, and it made me directly think it's super important to be prepared.

Being aware of the risks on the internet and the mentality of planning for WHEN, not IF is something everyone should adapt, not only cybersecurity professionals.

I will thoroughly go through the systems and routines at my work to make sure we follow vital security defenses, maybe even ask my boss if we can implement some type of pen testing. I also want to apply the learning in my personal life, educating my wife and elderly parents.

Unit 6

I learned a lot about how standards and directives help managing security in different technologies like networking, applications, cloud computing, smart devices and even operational technologies and IoT.

I personally discovered multiple areas I've not considered enough to be a security threat, by the help of the directives and standards made by the different organizations.

Standards and directives are a major help to guide and enforce a high standard of security, to plug the holes that you otherwise easily miss, and it's beneficial for not only organization but also for the individual and the society.

I want the applicable standards and directives to be implemented at my work, and I'll also do a personal journey to implement them in my personal life when applicable.

Unit 7

I learned how to properly analyze risk and provide a plan to mitigate or handle incidents.

The scale of possible incidents dawned on me, and made me question if we have a proper plan for all different risks at my work.

It's made clear it's important with critical thinking and planning for incidents and catastrophes, and I think everyone can benefit from having this skill and way of thinking.

We do have a great system in place at my work for monitoring, mitigating, responding, and resolving attack/bugs, but I will look if we can improve anything from what I learned in this unit, and also start thinking more at risks as inevitable and plan ahead.

Unit 8

I've been interested in ethical hacking for a while, and this unit gave me more insights into the details of a pen tester.

I felt a fire of passion in me that this is what I want to do.

Pen testers not only hack, they report and provide valuable information as well, which is a good skill to have.

I will continue to do more rooms at Try Hack Me, and other similar platforms I've started before, and try to get more roles at my work similar to pen testing. I will try and ask my boss if we can conduct more pen testing scenarios, even if they are made from us and not as professional.

Unit 9

It was made more clear to me that cybersecurity merges with crime and police work.

As a first responder to attacks at my work, I was reminded that I could do better PROVING an attack through indisputable evidence.

In a more general sense, it made me think that I should stop and think before I do stuff, to prevent myself or anyone else to tamper anything important.

I will try to be more methodical when I do investigations at my work, maybe even practicing thinking like I'm working at a crime scene when I collect evidence and report my findings. More thorough reports is something I would like to practice as well, which would prepare me in a potential future role of a pen tester.

Unit 10

Mostly I learned about the different OSINT tools that are publicly available for free.

It made me curios, and a bit more aware of the risks of publicly available information. I was actually a bit worried about my own information (which I already was before this).

Everybody can and should to some extend be more aware how information about them is being publicly available, and be more cautious.

I will go over my online present, and I will also be even more careful to trust organizations, sites, or emails. I would also like to practice in gathering publicly available information like this and also practicing any skills in social engineering, to learn a pen testers role.

Unit 11

I didn't learn anything new in this unit, but was more reminded of policies, controls, frameworks from previous units, and to think about what I want to do next with my cybersecurity career.

I felt the urge to continue my learnings about cybersecurity and ethical hacking.

This meant for me that it's good to practice the learning from this course in real life.

I will implement the things I learned in this course at my work, by promoting us to create a dedicated security team, in which we should try to go over what governance we have implemented and what is missing. And I want to continue solving challenges on different platforms to further improve my skills and knowledge.

Unit 12

I learned a bit about AI and other emerging tech, from which blockchain was one thing I read more about.

It made me aware that guidelines and controls are needed for AI at businesses, even more important now when we are using AI more and more at my work.

Emerging tech are always coming, so it's good to learn about them and what security threats there are. It’s fun with opportunities, but we must be aware of the risks as well.

I will check with my work what controls and guidelines we have for AI, and make sure we implement some if we don’t. My parents use AI a lot as well, and it would be great to help them stay protected while gaining the benefits of AI.