Welcome to week 3

Wow! We've covered a lot together!
It's hard to believe we've reached the midpoint of this course.
I hope you're getting a clearer picture of this exciting field and all the opportunities it has to offer.
And most importantly, I hope you're having fun doing it.

We've come a long ways from where we started.
When we began our journey together, we were introduced to the three building blocks of every security program: assets, threats, and vulnerabilities.
We focused a lot on assets early on and the wide range of things security professionals work to protect.

We then turned our attention to a core component of asset security, protecting assets.
You learned about the importance of guarding sensitive information.
You also learned about some security controls that protect information from being lost or stolen.

On the next part of our journey,
we're going to turn our focus to vulnerabilities.
Every asset we protect has a series of vulnerabilities, or flaws, that we need to be aware of.
Staying informed of these things is a critical part of protecting people and organizations from harm.

In this next part of the course, you'll gain an understanding of the vulnerability management process.
First, you'll explore a common approach to vulnerability management: the defense and depth model.
Then, you will learn about how vulnerabilities are documented in online libraries like the CVE list.
We'll discuss the attack surfaces security teams protect.
And lastly, you'll expand your attacker mindset by exploring the common attack vectors cybercriminals try to exploit.

Security analysts play an important role in identifying and correcting vulnerabilities in systems.
I know I'm excited to keep exploring,
are you?
Then let's go!

Revision #1
Created 2023-07-27 17:02:44 UTC by naruzkurai
Updated 2023-08-15 18:44:12 UTC by naruzkurai