Welcome to week 1

Welcome. In my role as Principal Security Strategist,
I've seen how the incident response operations that you'll learn about in this course are implemented in an organization.
One of the things I find so exciting about detecting and responding to incidents is the challenge of using data to understand what an adversary has done in my organization's environment.
No two investigations are ever the same, but there are patterns of behavior that you can learn to spot as you hone your analytic skills.
Previously, you established a solid understanding of asset security, threats, and vulnerabilities.
You explored the NIST Cyber Security Framework, or CSF, as a methodology for risk management.
You learned about mitigating organizational risk through classifying and securing assets.
And you also explored security and privacy controls to safeguard data.
You used tools like MITRE and CVE to investigate common vulnerabilities and used techniques like threat modeling to develop an attacker's mindset.
Next, we'll revisit the NIST CSF with a focus on the incident response lifecycle.
You'll be given your own incident handler's journal, which you'll use throughout the rest of the course.
You'll also be introduced to incident response teams, including the different team roles and how they organize to respond to incidents.
And finally, you'll learn about the different types of documentation, detection, and management tools you'll use as a security professional working in incident response.
Later on, you'll have an opportunity to use these tools.
Are you ready to begin your journey in detection and response?
Let's begin!

Revision #1
Created 5 September 2023 05:25:35 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai