Wrap-up; terms and definitions from course 5, week 1

Well done! You made it to the end of this section!
Being a security practitioner takes commitment and a desire to learn.
A big part of the job involves keeping current with best practices and emerging trends.
Thinking back on my own journey into the world of security, I'm so proud of you for your continued commitment.
We've covered a lot of material this week, and this is a good time to reflect and look back on the key concepts we explored together.

We covered the building blocks of organizational risk management: assets, threats, and vulnerabilities.

We also spent some time demonstrating the importance of asset inventories.
It's much easier to protect company assets if you know where they are and who's responsible for them.

After that, we moved on to explore the challenges in a rapidly changing digital world.
Part of protecting data in this world is understanding if it's in use, in transit, or at rest.

Finally, in our high-level exploration of policies, standards, and procedures, we talked about how each of them factor into achieving security goals.
There's no one-size-fits-all approach to achieving security.
While exploring the NIST Cybersecurity Framework, you gained an appreciation of how it supports good security practices.

Attackers are also constantly building their skills and finding new ways to break through the defenses we put up.
Remember, the landscape is always changing.
There's always more to learn if you want to be a good security practitioner.

Next up, we're going to expand our security mindset by learning more about the different systems security teams use
to protect organizational assets.
I'm looking forward to it!

Glossary terms from week 1

Asset: An item perceived as having value to an organization

Asset classification: The practice of labeling assets based on sensitivity and importance to an organization

Asset inventory: A catalog of assets that need to be protected

Asset management: The process of tracking assets and the risks that affect them

Compliance: The process of adhering to internal standards and external regulations

Data: Information that is translated, processed, or stored by a computer

Data at rest: Data not currently being accessed

Data in transit: Data traveling from one point to another

Data in use: Data being accessed by one or more users

Information security (InfoSec): The practice of keeping data in all states away from unauthorized users

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

Policy: A set of rules that reduce risk and protect information

Procedures: Step-by-step instructions to perform a specific security task

Regulations: Rules set by a government or other authority to control the way something is done

Risk: Anything that can impact confidentiality, integrity, or availability of an asset

Standards: References that inform how to set policies

Threat: Any circumstance or event that can negatively impact assets

Vulnerability: A weakness that can be exploited by a threat

Revision #5
Created 2023-07-18 05:00:18 UTC by naruzkurai
Updated 2023-08-28 18:43:38 UTC by naruzkurai