The value of documentation

Hi there.
Previously, you learned how an incident handler's journal is used for documenting the 5 W's of an incident:
who, what, where, when, and why an incident occurred.
In this section, we'll continue our discussion on documentation by exploring the different types of documentation, the importance of effective documentation, and we'll finish off with the discussion on documentation tools.

Documentation is any form of recorded content that is used for a specific purpose.
This can be audio, digital, or handwritten instructions, and even videos.
There is no set industry standard for documentation, so many organizations set their own documentation practices.
Regardless, documentation is meant to provide instruction and guidance on a specific topic.

There are also many types of documentation, and you may already be familiar with some of them from the previous lessons.
These include playbooks, incident handler's journals, policies, plans, and final reports.
Remember, there isn't an industry standard for documentation, which means that one organization's documentation practices may look completely different than another's.
Often, organizations will tailor their documentation practices according to their needs and legal requirements. They may add, remove, or even merge documentation types.

Have you ever purchased a product, and didn't know how to use it, and consulted the product manual for instructions on how to do something like turn it on?
Congrats, you've used documentation to solve an issue.

Previously, you've learned about how playbooks keep business operations safe, and in incident response, playbooks work similar to a product manual.
As a refresher,
a playbook is a manual that provides details about any operational action. You'll learn more about playbooks later.

Let's revisit that product manual example.
Have you ever consulted a product manual for help and found yourself confused with the instructions and unable to get the help you needed?
Whether it's had to do with unclear visuals and instructions or a confusing layout, you weren't able to use the documentation to solve your issue.
This is an example of ineffective documentation.

Effective documentation reduces uncertainty and confusion.
This is critical during a security incident when tensions are high and urgent response is required.
As a security professional, you'll be using and creating documentation regularly.

It's essential that the documentation you use and produce is clear, consistent, and accurate, so that you and your team can respond swiftly and decisively.

Word processors are a common way to document.
Some popular tools to use are Google Docs, OneNote, Evernote, and Notepad++.

Ticketing systems like Jira can also be used to document and track incidents.

Lastly, Google Sheets, audio recorders, cameras, and handwritten notes are also tools you can use to document.

Our discussion on documentation has only just begun.
Soon, you'll use your incident handler's journal to put your documentation skills to work.

Revision #1
Created 2023-09-06 10:57:28 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai