Welcome to module 4

History books. Receipts. Diaries.
What do all these things have in common?
They record events.
Whether it's historical events, financial transactions, or private diary entries, records preserve event details.
And having access to these details can help us in many ways.
Previously, we explored the different types of processes and procedures involved during each phase of the incident response lifecycle.
In this section, we'll direct our focus on one of the key components of incident investigation, logs and alerts.
In security, logs record event details and these details are used to support investigations.
First, you'll learn all about logs, what they are, and how they're created.
You'll also learn how to read and analyze logs.
Then, we'll revisit intrusion detection systems.
You'll explore how to interpret signatures.
You'll have an opportunity to apply what you've learned through hands-on activities using a tool called Suricata.
Finally, you'll search in SIEM tools like Splunk and Chronicle to locate events of interest and access log data.
Events are a valuable data source.
They help create context around an alert, so you can interpret the actions that took place on a system.
Knowing how to read, analyze, and connect different events will help you identify malicious behavior and protect systems from attack.
Ready?
Let's begin.

Revision #1
Created 2023-11-01 01:23:47 UTC by naruzkurai
Updated 2023-11-01 01:24:15 UTC by naruzkurai