Section Introduction, Operational Intelligence

This section of the Threat Intelligence domain will cover what operational intelligence is, and the activities and work that is involved. This includes a deep understanding of indicators of compromise and precursors, as well as attack frameworks such as MITRE's ATT&CK framework and the Lockheed Martin Cyber Kill Chain.

This section of the Threat Intelligence domain will focus on operational intelligence roles and responsibilities. A typical day in the life as a Cyber Threat Intelligence Analyst focusing on operational intelligence typically involves collecting indicators, indicators of compromise, and precursors in order to share actionable intelligence with other entities, and work to make malicious actor's lives harder by hitting them at different levels of the Pyramid of Pain, a concept that covers how difficult it is for threat actors to change certain aspects of their operations.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand what indicators of compromise and precursors are, and how they can be used to share intelligence.
- Understand and apply cyberattack frameworks from Lockheed Martin and MITRE.
- Understand what attribution is, and the issues there are with trying to link activity to a threat group.
- Understand what the pyramid of pain is, and why it's used.