Section Introduction, Tactical Intelligence

This section of the Threat Intelligence domain will focus on tactical intelligence roles and responsibilities. A typical day in the life as a Cyber Threat Intelligence Analyst focusing on tactical intelligence typically involves performing threat exposure checks to see if malicious indicators have been identified within the environment, conducting public exposure assessments to see how what information about the company and it's employees is freely available online, and if that could be exploited in any way, and collecting and using actionable intelligence to improve defenses by implementing threat feeds to power automated defenses and provide context to security investigations.

LEARNING OBJECTIVES

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

- Understand how threat exposure checks are conducted to identify the presence of indicators of compromise.
- Understand how organizations can monitor for IOCs using SIEM, EDR, and IDS systems to alert for positive matches.
- Understand what public exposure assessments are and why they can be valuable to defenders and attackers.
- Understand how information can be collected from open and dark-web sources and the legal constraints of this activity.
- Understand what MISP is, why it's used, and how to deploy it.