Section Introduction, Strategic Intelligence

This section of the Threat Intelligence domain will focus on strategic roles and responsibilities. A typical day in the life as a Cyber Threat Intelligence Analyst focusing on strategic intelligence typically involves collecting and sharing actionable intelligence with partners and the internal security team to provide threat intelligence context, giving defenders more useful information about malicious actor activity on a global scale. Strategic Analysts tend to focus on the geopolitical activity of hostile nations, working to monitor if there is or will be an increased threat from that nation and their associated Advanced Persistent Threats (APTs) in the future. This role is all about collecting intelligence from a wide range of sources, analyzing it, passing it to appropriate team members, and sharing it with other organizations through intelligence partnerships.

LEARNING OBJECTIVES

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

- Understand how indicators of compromise and tactics, techniques, and procedures can be shared between organizations and the value it generates.
- Develop your understanding of how threat intelligence teams work to track malicious campaigns and report this information to the security team so they can prepare for attacks.
- Compare the strengths and weaknesses of both OSINT-acquired intelligence and intelligence purchased from vendors.