Activity Overview

In this activity, you'll analyze an artifact using VirusTotal and capture details about its related indicators of compromise using the Pyramid of Pain.

Previously, you were introduced to the concept of the Pyramid of Pain, which is used to understand the different types of indicators of compromise (IoCs). Remember, an IoC is an observable evidence that suggests signs of a potential security incident. The Pyramid of Pain describes the relationship between IoCs and the level of difficulty that malicious actors experience when security teams block the IoCs.

VirusTotal is one of many tools that security analysts use to identify and respond to security incidents. VirusTotal is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. Through crowdsourcing, VirusTotal gathers and reports on threat intelligence from the global cybersecurity community. This helps security analysts determine which IoCs have been reported as malicious. As a security analyst, you can use shared threat intelligence to learn more about threats and help improve detection capabilities.

Important Note: Data uploaded to VirusTotal will be publicly shared with the entire VirusTotal community. Be careful of what you submit, and do not upload personal information.