Scenario

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a hash function is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint.

Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Remember, an **IoC (Indicators of compromise)** is 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 the IoCs are blocked by security teams.

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 take advantage of 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 make sure you do not upload personal information.*