**What you'll learn**

* How to identify, evaluate, and prioritise potential security threats and vulnerabilities to determine the levels of risk and develop plans to mitigate those risks

**What you'll do**

* Complete a risk assessment for a client and help them define the context, assess their risk matrix, and identify potential risk scenarios

**SCENARIO 2**

Your initial research on the APT group is a crucial step because it helps to identify the potential attackers and their methods, motives and targets. Understanding the TTPs of APT34 helps identify specific vulnerabilities and attack vectors that could be exploited.

This has laid a solid foundation for the next task, which is to conduct a comprehensive risk assessment for the client. The client has a fence around the perimeter of its property and a padlock on its entrance gate to prevent unauthorised access. However, the leadership team is concerned about potential risks and vulnerabilities that could compromise the security of its information and systems. They require a comprehensive risk assessment to identify potential security threats and vulnerabilities in their system or network.

As a cybersecurity consultant, you understand that conducting a risk assessment is an essential component of any effective cybersecurity strategy. This involves identifying, evaluating and prioritising potential security threats and vulnerabilities to determine the level of risk and develop a plan to mitigate those risks. During the risk assessment, you will need to identify the assets that need to be protected, define the risk matrix and identify potential risk scenarios. You will assess the risk ratings for each scenario, both with and without existing measures in place. Finally, you will provide a risk assessment report to the client summarising your findings and recommendations for mitigating risks and improving the institution's security posture.

The goal of the risk assessment is to help the client prioritise and implement appropriate security measures to mitigate and minimise risks. This will ensure the confidentiality, integrity and availability of their information and systems, as well as protect their reputation and financial resources. Ultimately, your work will help the client comply with regulatory and legal requirements and standards and provide peace of mind knowing that their security is being handled by a knowledgeable and experienced cybersecurity expert.