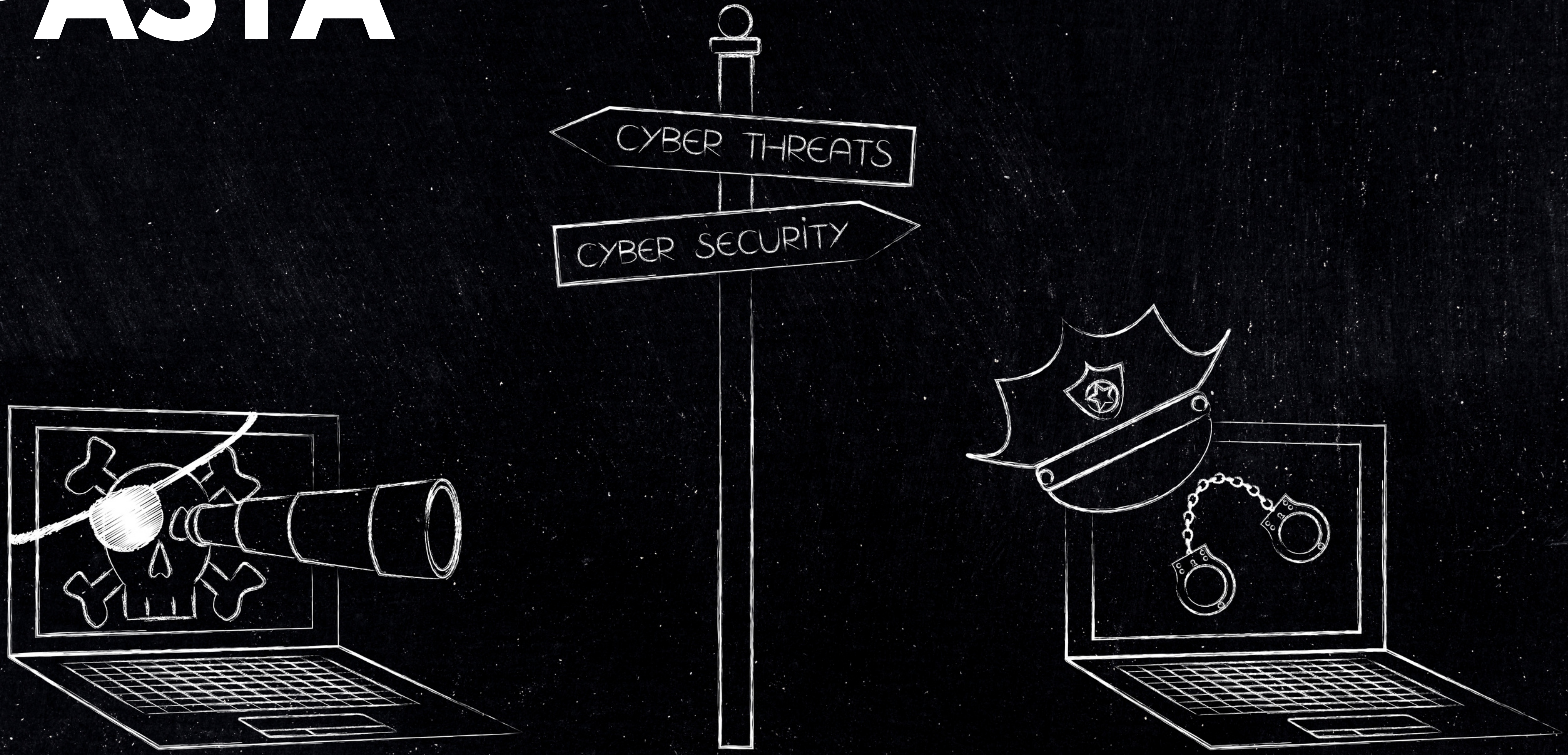
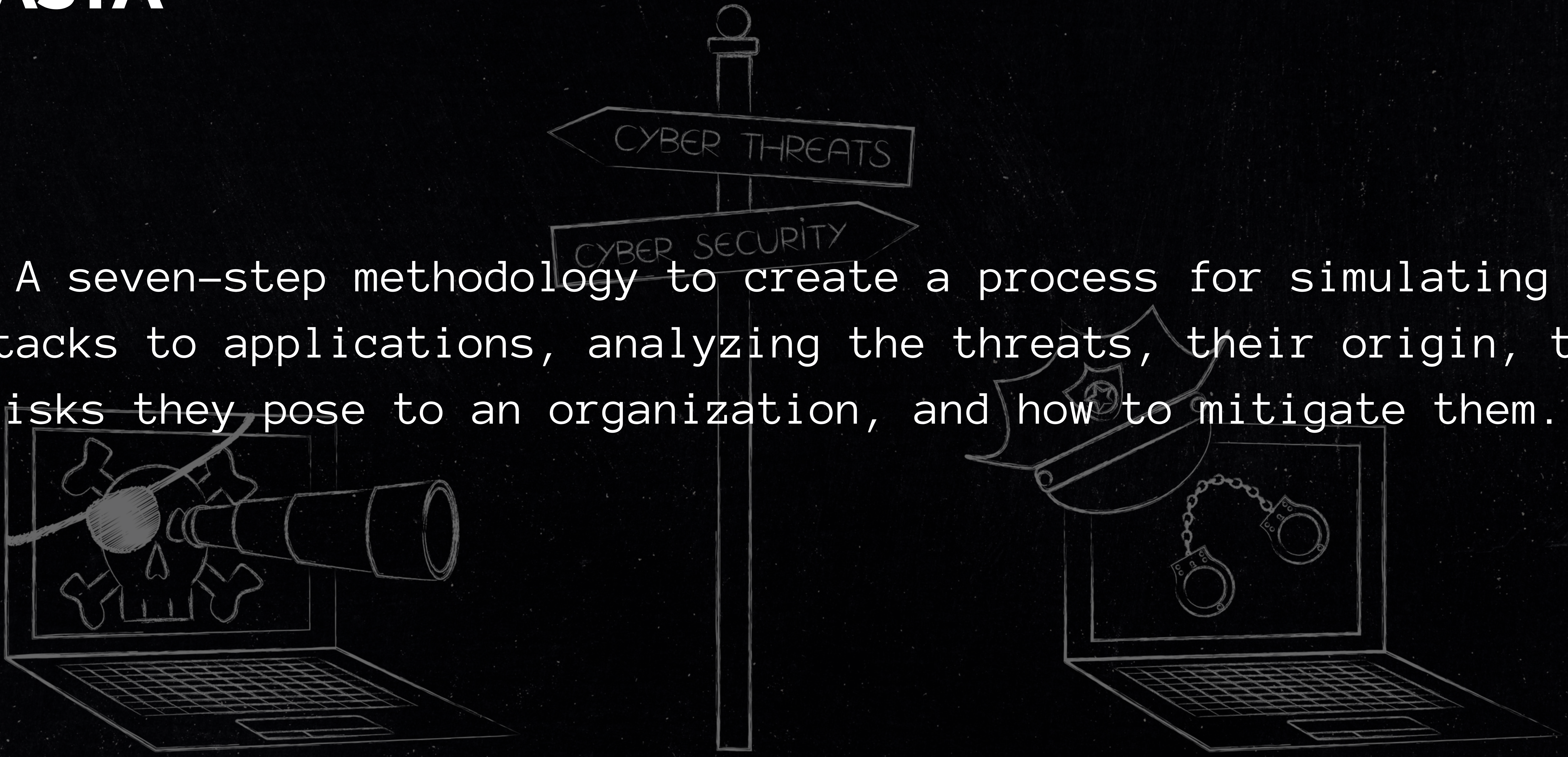
PASTA



PASTA

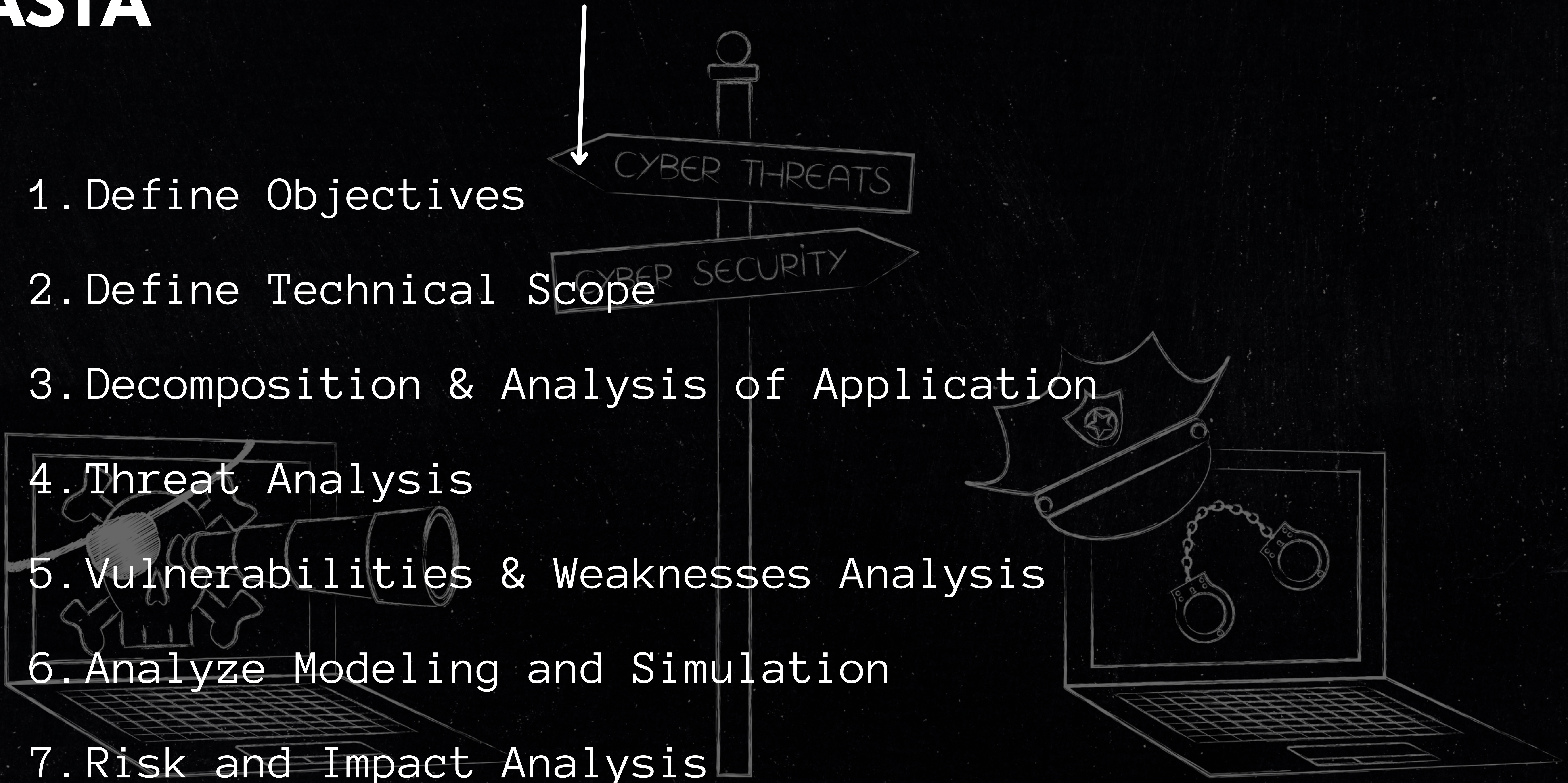
The Process for Attack Simulation and Threat Analysis

PASTA



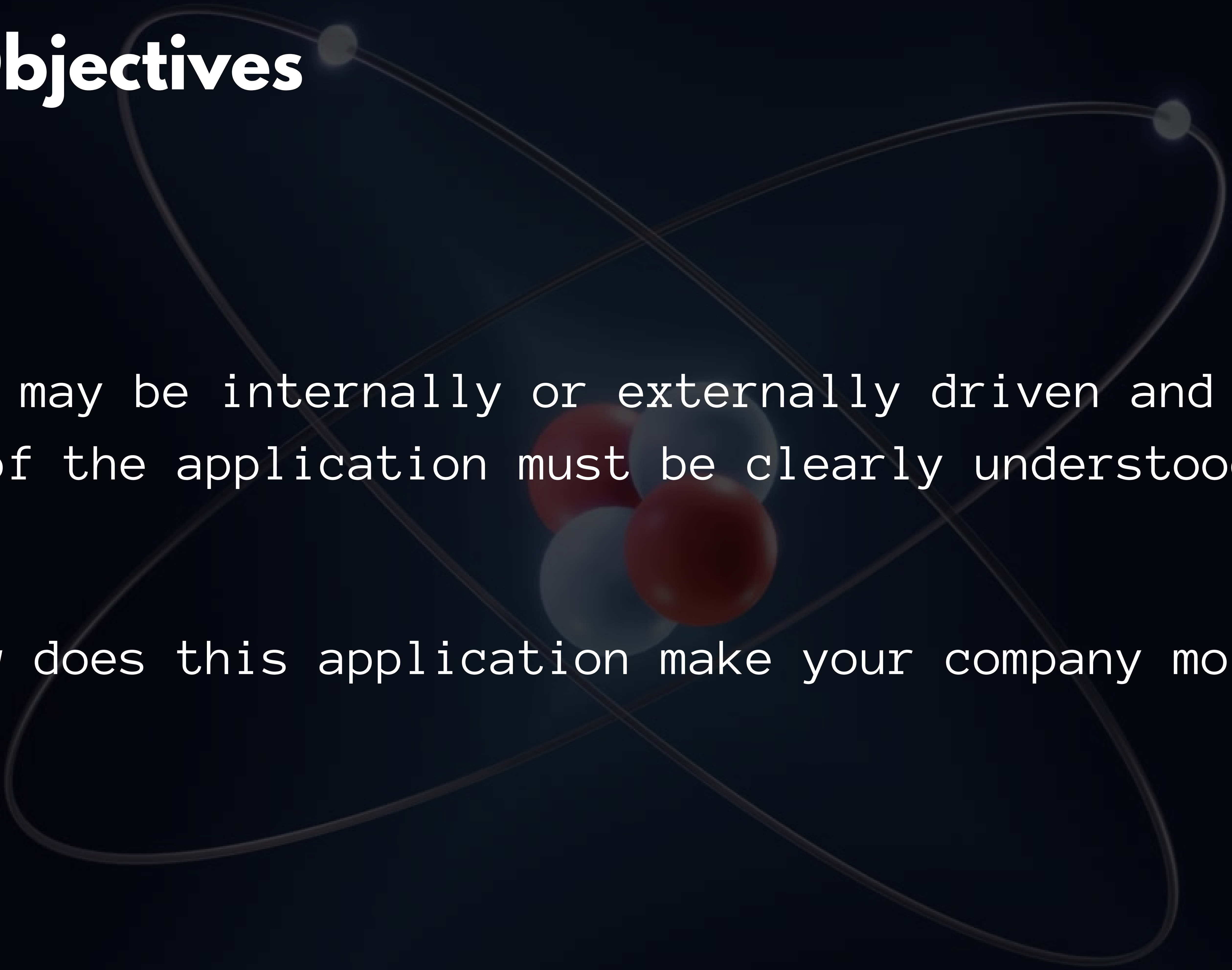
A seven-step methodology to create a process for simulating attacks to applications, analyzing the threats, their origin, the risks they pose to an organization, and how to mitigate them.

PASTA



1. Define Objectives
2. Define Technical Scope
3. Decomposition & Analysis of Application
4. Threat Analysis
5. Vulnerabilities & Weaknesses Analysis
6. Analyze Modeling and Simulation
7. Risk and Impact Analysis

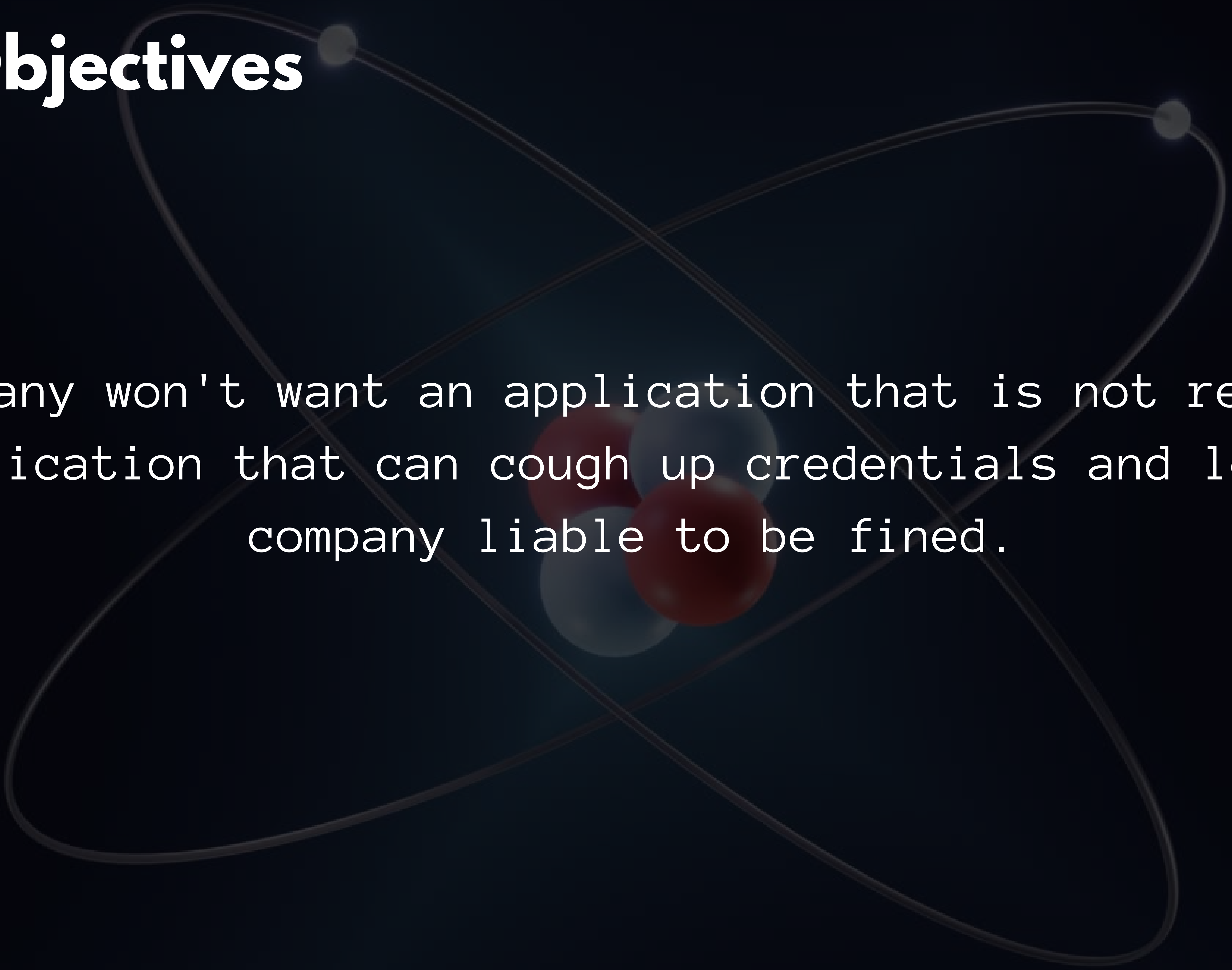
Define Objectives



Objectives may be internally or externally driven and the purpose of the application must be clearly understood.

How does this application make your company money?

Define Objectives



Your company won't want an application that is not resilient or an application that can cough up credentials and leave the company liable to be fined.

Define the Technical Scope

Time to understand the attack surface by defining exactly what you are protecting.

Dependencies on third party services should also be defined.

Define the Technical Scope

Attack Surface Component Examples:

- DNS Server
- Network Infrastructure
- Application Framework
- Web Application
- OS Settings
- Certificate Server

Decompose the Application

The key output of this stage is to understand if you have implicit trust models and where they are.

Analyze the Threats

Here potential threats against the application are analyzed. The data type and data consumption models are considered as well.

Vulnerability Analysis

Stage five correlates the application's vulnerabilities to the application's assets.

"What is wrong with the application?"

Attack Analysis

Here the vulnerabilities discovered in stage 5 are tested to see if they are actually viable.

Risk & Impact Analysis

Here the vulnerabilities discovered in stage 5 are tested to see if they are actually viable.