SECURE CODE WARRIOR®

THREAT MODELLING OVERVIEW

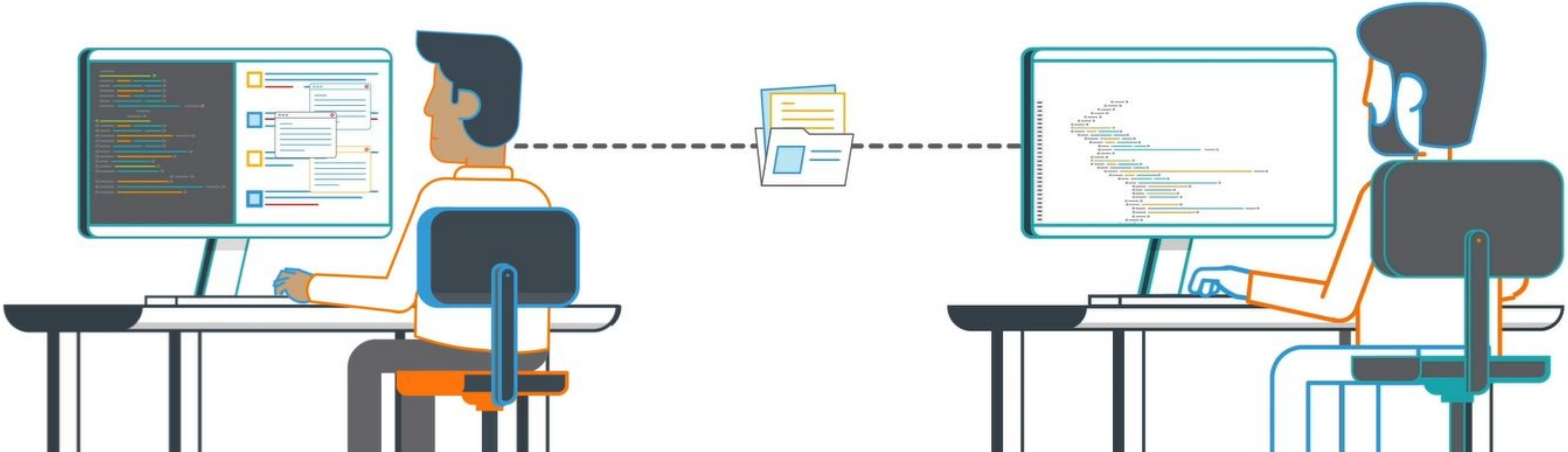
In this module

we'll be going through an overview of Threat Modeling.

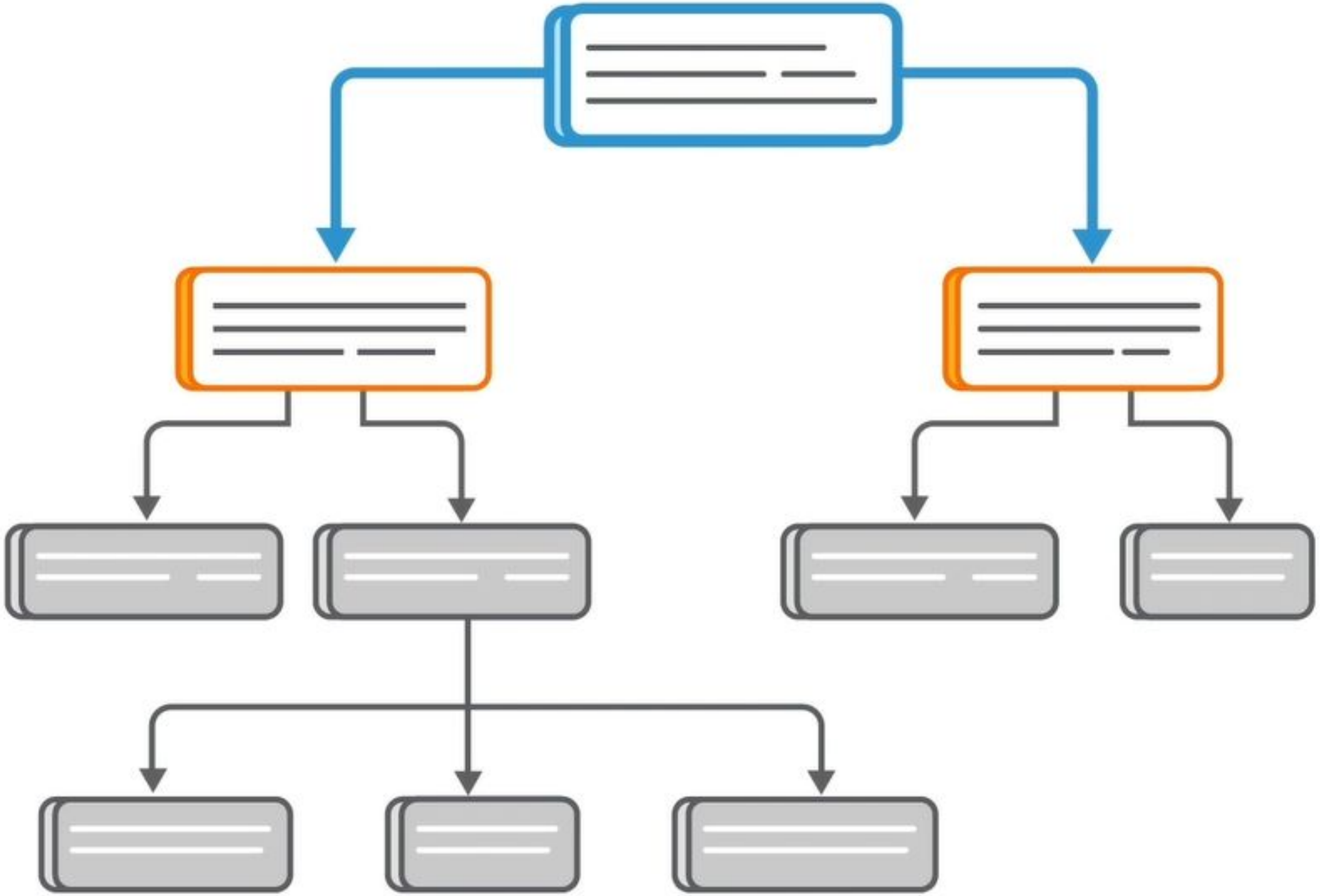
Threat Modeling is a way to identify, communicate, and understand security threats and mitigations.

IDENTIFY COMMUNICATE SECURITY THREATS MITIGATIONS

It helps teams evaluate and prioritize threats - and then allocate security resources accordingly.



A threat modeling process should be systematic and structured.



There are many Threat Modeling methodologies out there, such as STRIDE or Attack Trees,

STRIDE

S SPOOFING

T TAMPERING

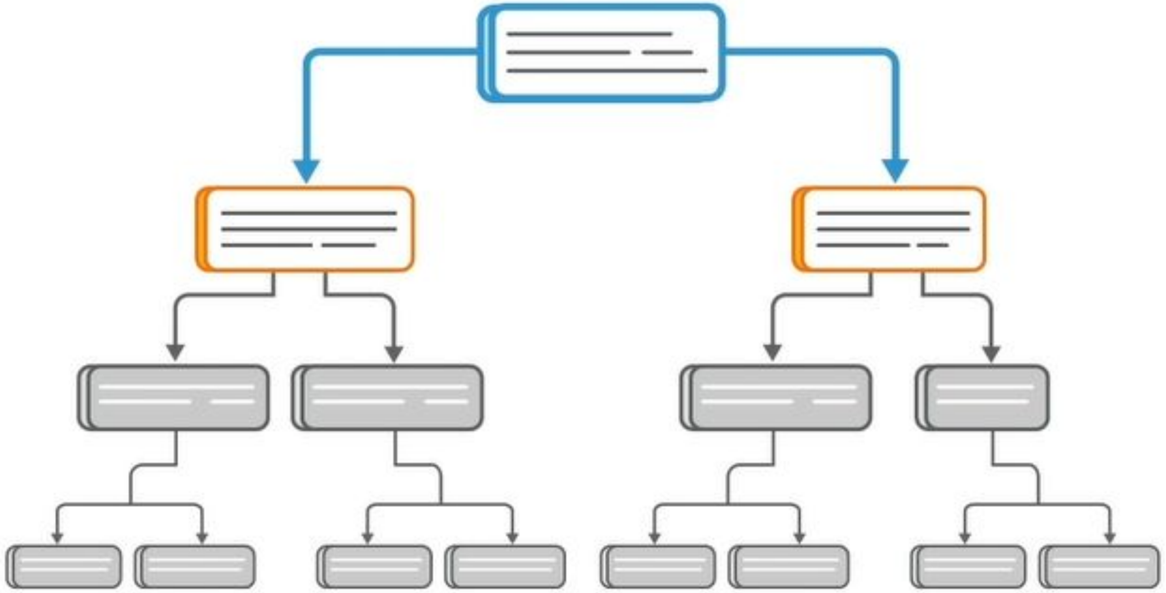
R REPUDIATION

I INFORMATION DISCLOSURE

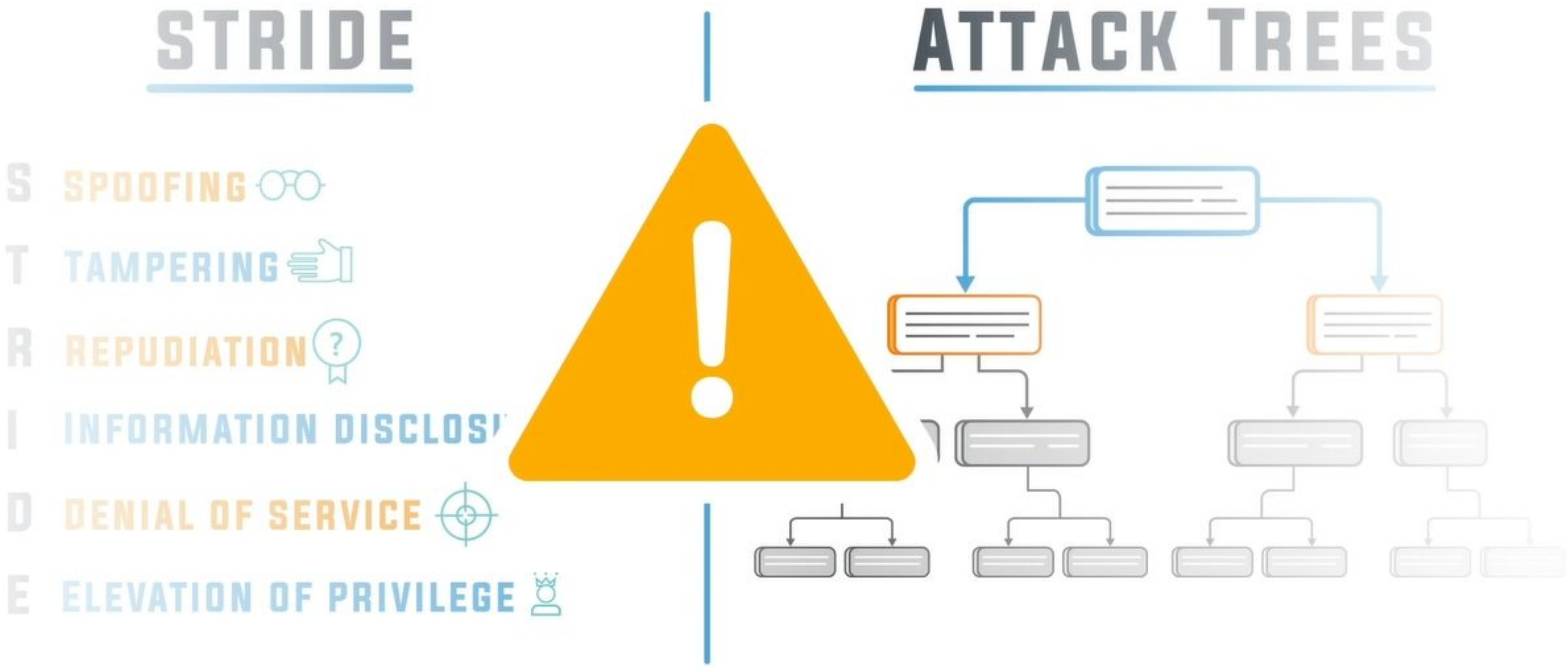
D DENIAL OF SERVICE

E ELEVATION OF PRIVILEGE

ATTACK TREES



but there is no single “correct” way to model

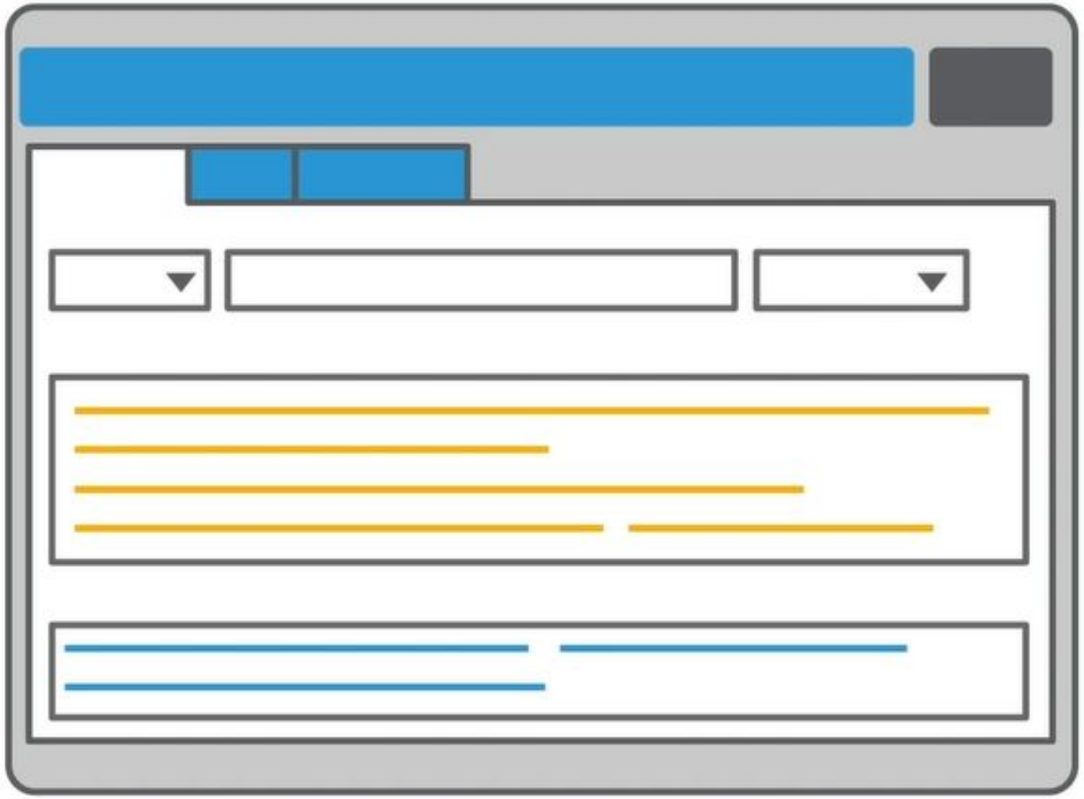


THERE ARE, HOWEVER, SOME COMMON ELEMENTS AMONG THREAT MODELING METHODOLOGIES.

A threat model should cover four main elements

1. ASSETS
2. VULNERABILITIES
3. THREATS
4. THREAT AGENTS

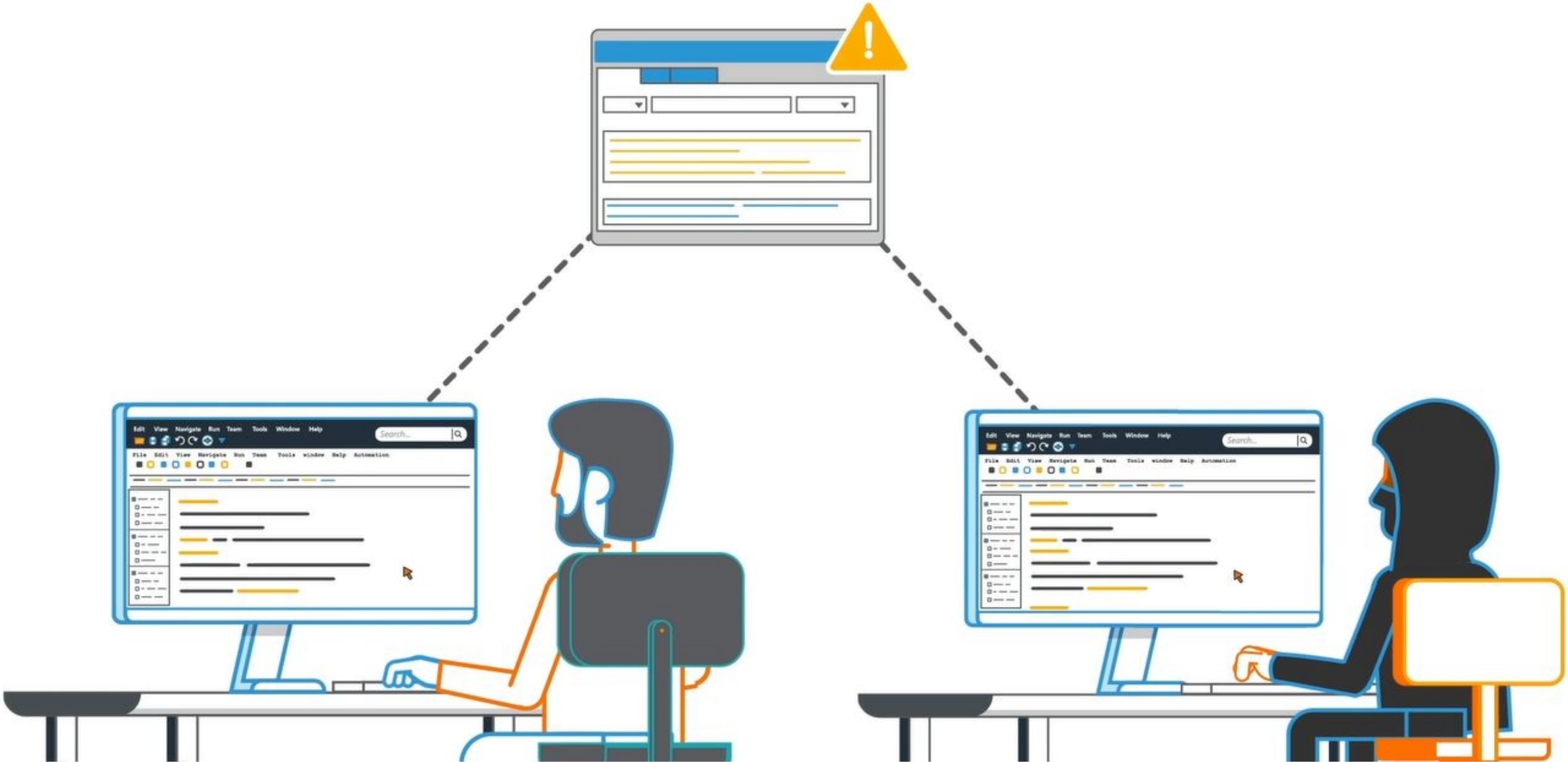
Assets - what needs to be protected (e.g. an app)



Vulnerabilities - weaknesses that, when exploited, could cause damage

Threats - potential damage that could occur as a result of exploiting a vulnerability

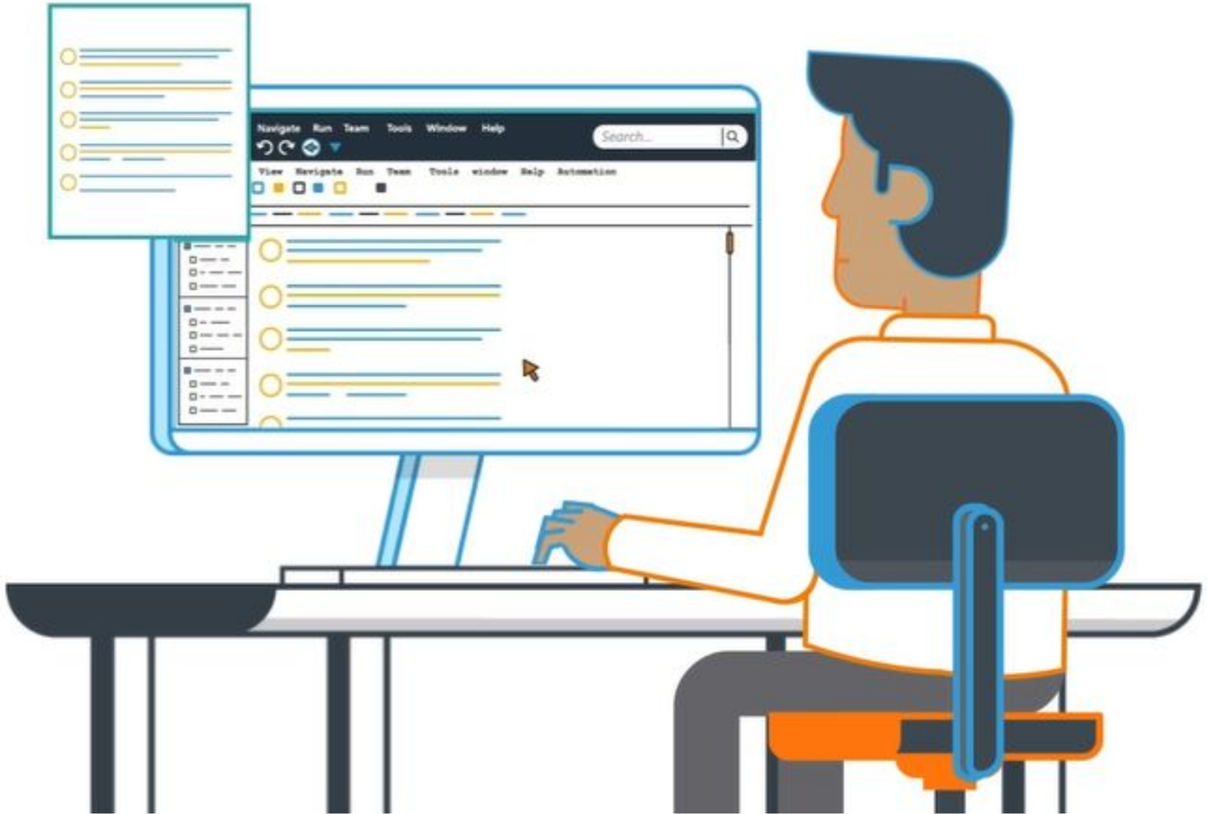
Threat Agents - one who exploits a weakness to cause a threat. Keep in mind, this could be an insider or an outsider.


Edit View Navigate Run Team Tools Window Help
Search...
File Edit View Navigate Run Team Tools window Help Automation
Edit View Navigate Run Team Tools Window Help
Search...
File Edit View Navigate Run Team Tools window Help Automation

A BASIC THREAT MODELING PROCESS SHOULD INCLUDE

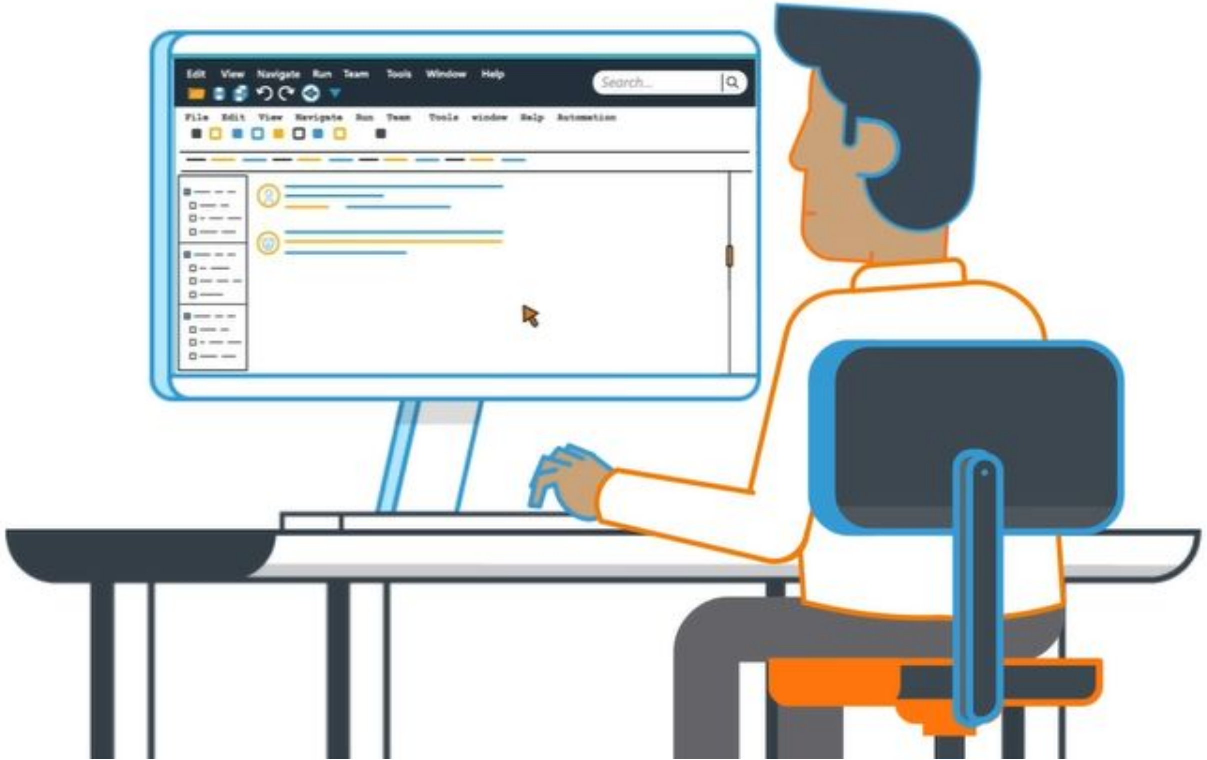
Assessment: a description or model of the asset being worked on and a list of assumptions about it

ASSESSMENT


Navigate Run Team Tools Window Help
Search...
View Navigate Run Team Tools window Help Automation

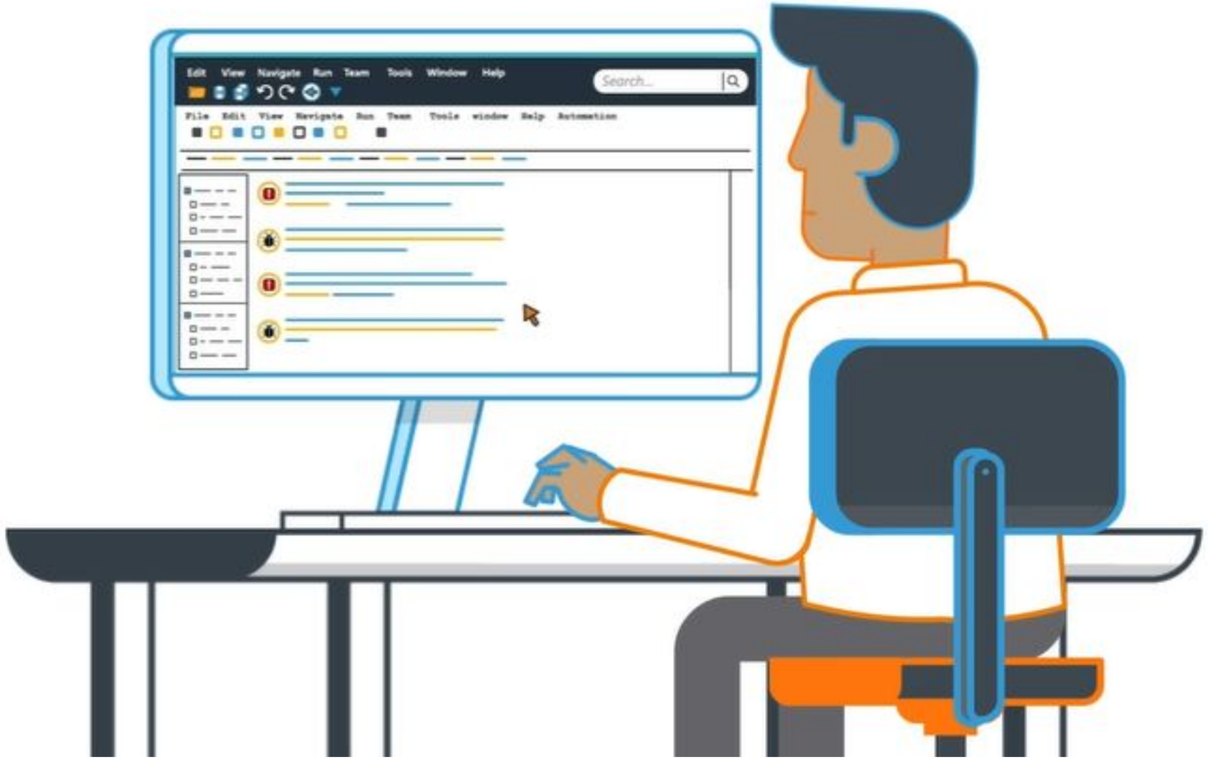
Threat Agent Identification: a list of agents who might be able to attack an application

THREAT AGENT IDENTIFICATION


Edit View Navigate Run Team Tools Window Help
Search...
File Edit View Navigate Run Team Tools window Help Automation

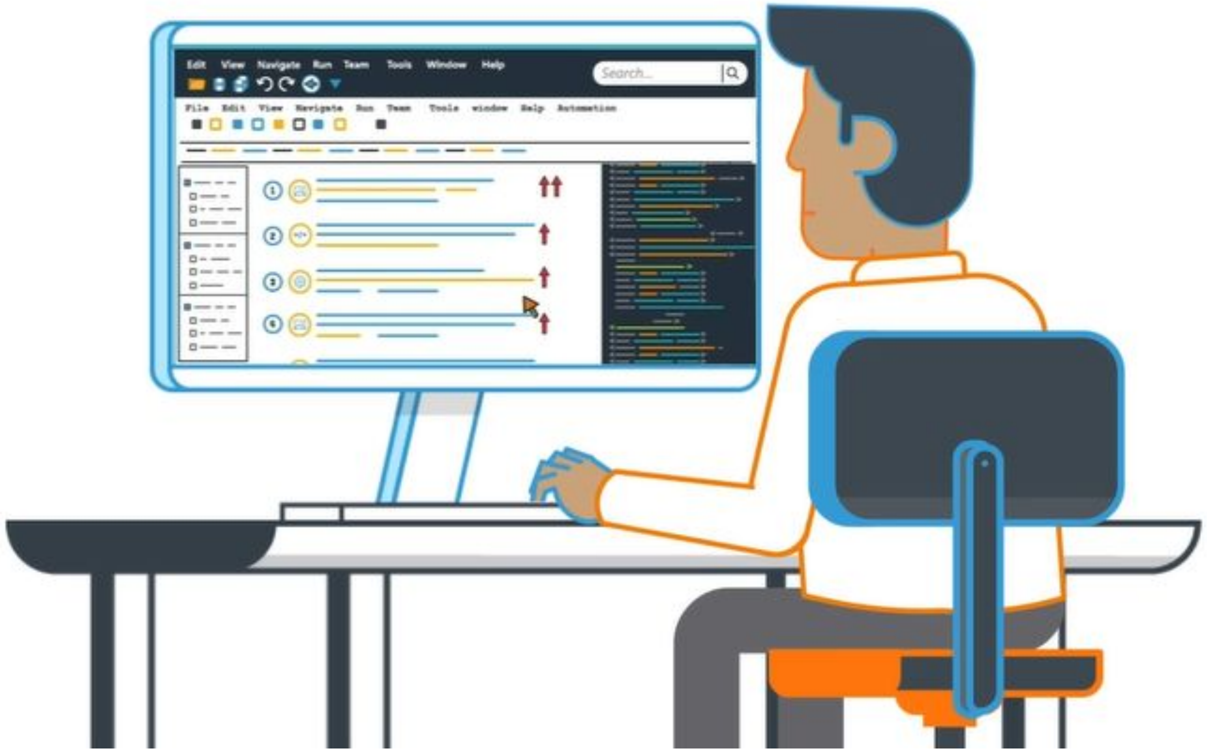
Threat Identification: a list of things that could go wrong

THREAT IDENTIFICATION


Edit View Navigate Run Team Tools Window Help
Search...
File Edit View Navigate Run Team Tools window Help Automation

Threat Prioritization: quantifying likelihood, impact factors etc.
- to determine the overall risk of each threat previously identified

THREAT PRIORITIZATION


Edit View Navigate Run Team Tools Window Help
Search...
File Edit View Navigate Run Team Tools window Help Automation

Remediation of threats: determining what countermeasures can be applied to reduce the risk level

REMEDIATION OF THREAT

Edit View Navigate Run Team Tools Window Help
Search...
File Edit View Navigate Run Team Tools window Help Automation

To start using Threat Modeling developers should keep in mind the following

- Threat modeling is most effective when done early on, so potential threats can inform app design
- Ensure business goals and requirements play a part in your model to ensure adequate protection
- Threat assessments should be revisited regularly as your project and landscape evolve

The Threat Modeling process should provide answers to the following questions

- What are we building?
- What could go wrong?
- Where am I most vulnerable to attack?
- Which threats are most relevant?

The Threat Modeling process should provide answers to the following questions

- What are we going to do about those threats?
- How can we safeguard against these threats?
- Did we do a good enough job?

Congratulations, you have now completed this module!

SECURE
CODE
WARRIOR
®