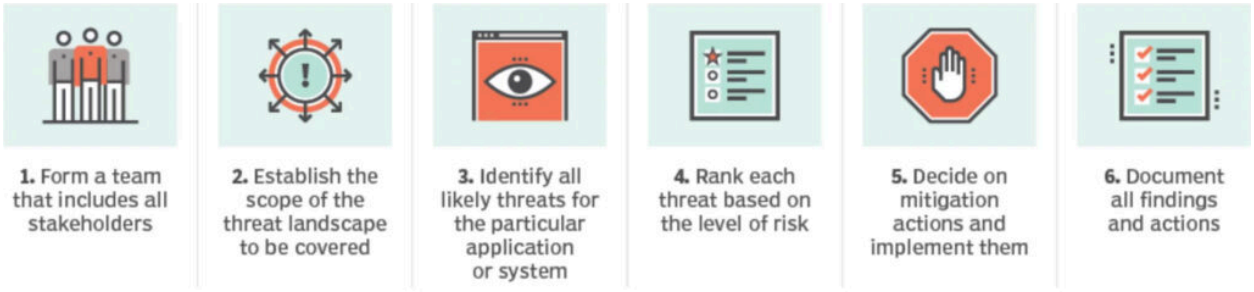
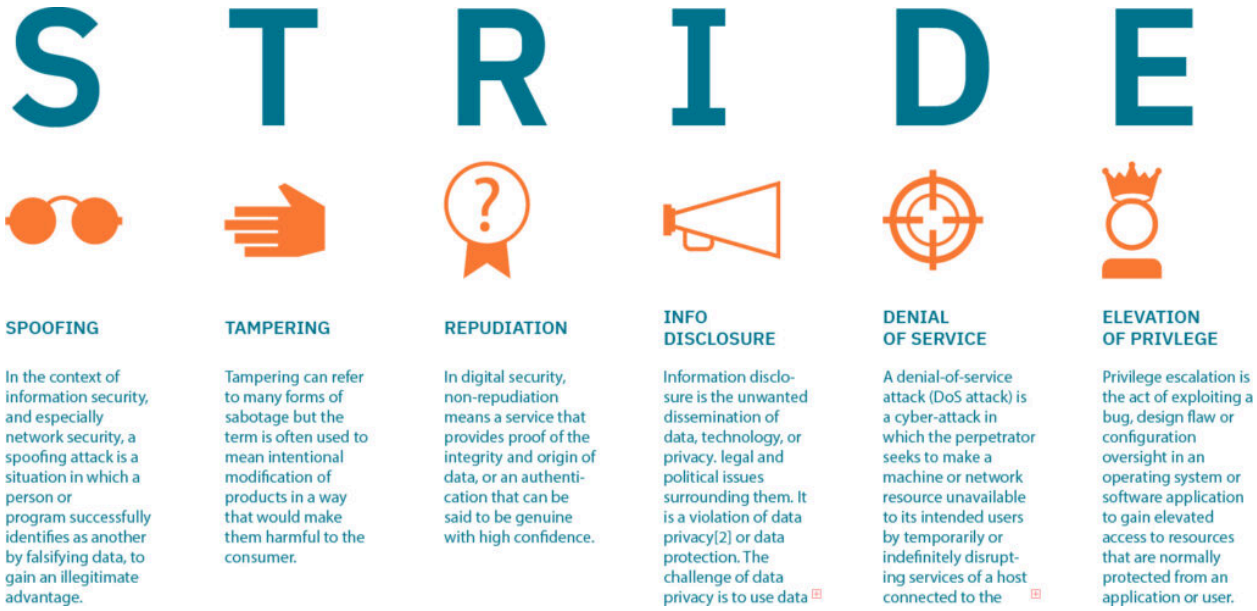
6 steps in the threat modeling process



Threat Modeling Frameworks and Methodologies

1. **STRIDE**



S - Spoofing is when a computer or person pretends to be something they are not
T - Tampering refers to violating the integrity of data
R - Repudiation interferes with the process of linking an action to the person who did it
I - Informative Disclosure involves giving away sensitive information
D - Denial of Service (DOS) makes it impossible for legitimate users to use a resource
E - Elevation of Privilege provides unauthorized access to a system or application to someone who already has a level of access

2. DREAD

D - Damage potential outlines how much damage can result from a negative event
R - Reproducibility determines how easy it is to replicate an attack
E - Exploitability refers to the ease with which an actor can launch an attack
A - Affected users involve detailing the percentage of users affected by the event
D - Discoverability examines how easy it is to locate the vulnerability

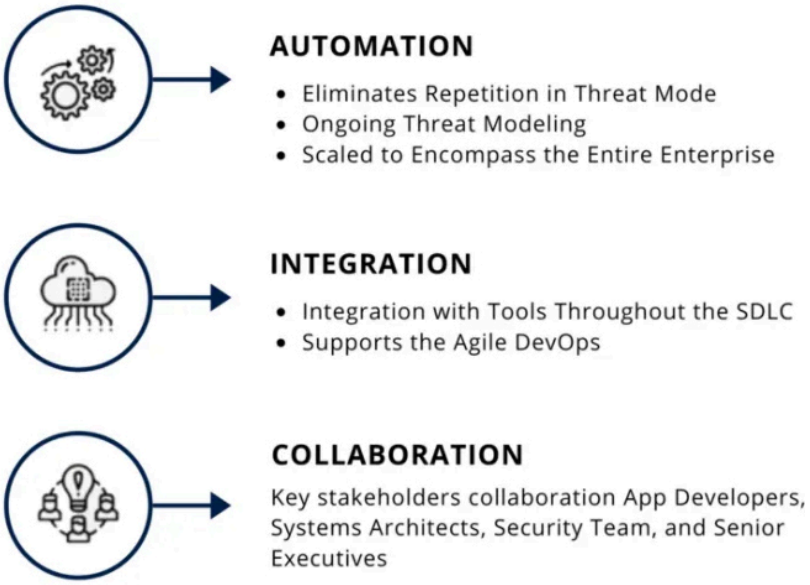
3. PASTA

The acronym PASTA stems from Process for Attack Simulation and Threat Analysis. This involves seven steps:

- Definition of your objectives
- Definition of the technical scope of the project
- Decomposition
- Analysis of threats
- Analysis of weaknesses and vulnerabilities
- Attacks modeling
- Analysis of the risk and impact on the business'

4. VAST

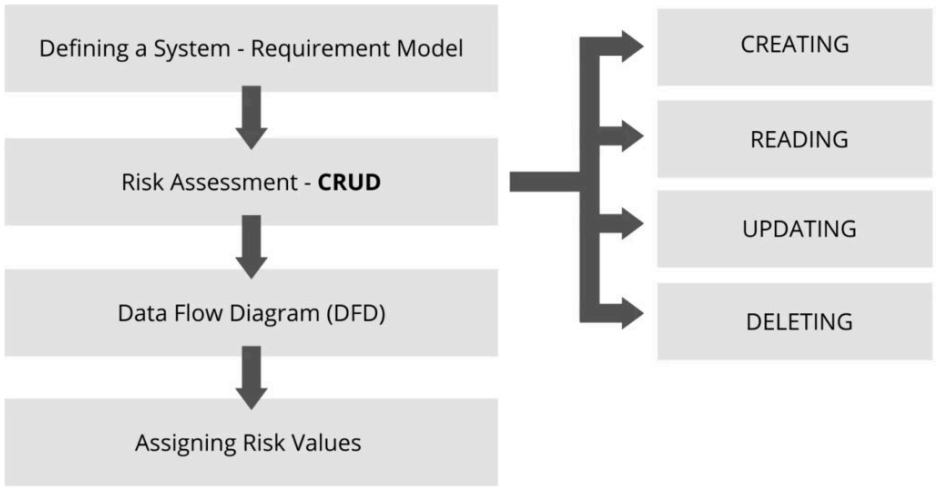
VAST refers to Visual, Agile, and Simple Threat modeling. VAST is a foundational element of a threat modeling platform called ThreatModeler. VAST integrates within workflows designed using the principles of DevOps.



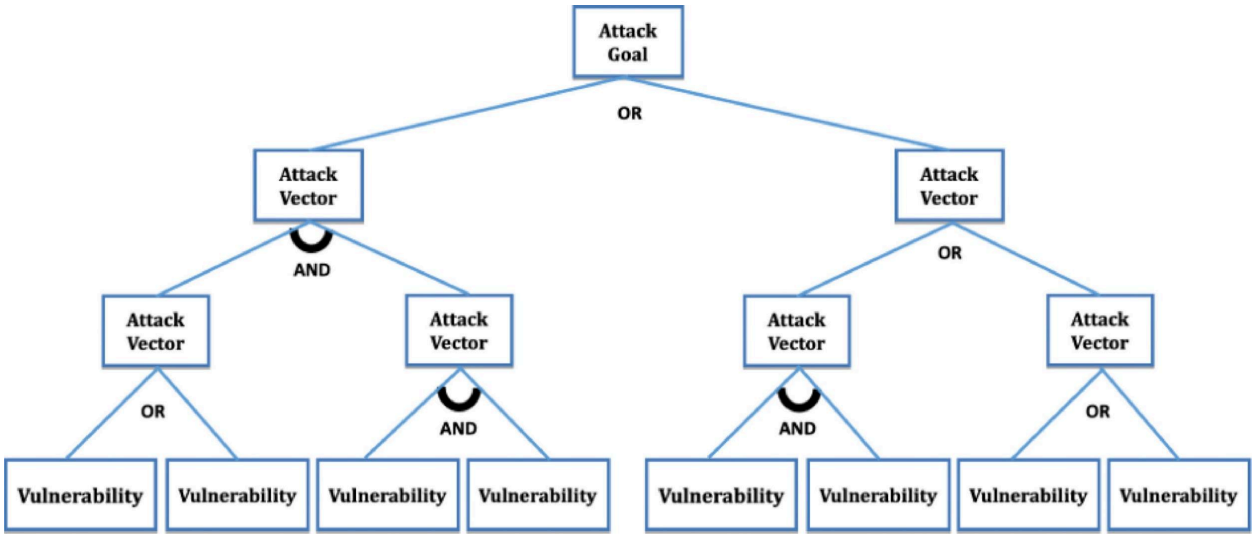
5. Trike

Trike is an open-source framework that seeks to defend a system instead of attempting to replicate how an actor may attack it. With the Trike framework, users make a model of the application or system they are defending. You then use the acronym CRUD to see who can:

1. Create data
2. Read data
3. Update data
4. Delete data



6. Attack trees



Attack trees are graphical and analytical conceptual diagrams. They are particularly useful for threat modeling in complex systems with multiple components and attack vectors, as it allows organizations to break down the system's attack surface into smaller, more manageable components to assess potential risks.

Attack trees are great support for an attacker-centric approach to threat modeling. They can be used to evaluate the effectiveness of existing security controls and identify gaps or weaknesses in the security posture, highlighting vectors where attacks are highly likely to happen.