Attack tree:

1.Asset

2.Actor

3.Usecase

4.Abuse case

5.Vulnerability

6.Exploit

7.Countermeasure

Attack surface

Threat/Attack vector (comes from DFD) 

3.Trust boundaries

1.System components

2.Data flow diagram

4.Identifying threats using Attack tree

-Cyber kill chain

5.List threat events

6.Attack modelling

Attack tree sample:

Asset/Component

Vuln

Vuln

Vuln

Vuln

Vuln

Threat 3

Threat 2

Threat 1

Threat tree:

Component

Threat Vector

Threat Vector

Threat Vector

Threat event

Threat event

Threat event

Threat event

Threat event

Threat Modelling

Threat Modelling

Threat Modelling

Threat Modelling

Threat Modelling

8.Attack modelling

-MITRE ATT&CK

-Lockheed Martin Cyber Kill Chain

7.List possible threat events

-TTP

-Categorize the events using methods such as STRIDE-LM, NIST SP 800-154,Security cards or OCTAVE

-Identify various threat types->STRIDE-LM

-Incorporate the threat events into DFD

1.Gather information

6.Identify threat vectors

5.Trust boundaries

4.Data flow diagram (DFD)

3.Identify system components

2.Demarcate Perimeter Boundary

|  |  |  |
| --- | --- | --- |
| Table 15 | STRIDE | PASTA |
| -Threat events are drawn from NIST SP 800-30R1.  - A few additional events based on other frameworks, particularly the ODNI CTF and ATT&CK, are included. | -Users identify threat vectors for individual components/assets enumerated previously. From the system’s DFD generated in the previous step.  - categorise threat events using methods such as STRIDE-LM, NIST SP 800-154, Security Cards or OCTAVE.  -Attack modelling using MITRE ATT&CK and Cyber kill chain | -Attack analysis/modelling using Attack trees |

Threat Surface

Achieving threat modelling with the help of threat tree

Threat Modelling

Threat Event

Threat Vector

Threat Tree

Root node/goals:

1. Initial Access (TA0001)

2. Privilege escalation (TA0004)

3. Credential access (TA0006)

4. Data Theft

5. Theft

6. Tampering (Modification/Alteration)

2. Privilege escalation Threat Vectors:

* [1. Credential Exploitation](https://www.cynet.com/network-attacks/privilege-escalation/#heading-5)
* [2. Vulnerabilities and Exploits](https://www.cynet.com/network-attacks/privilege-escalation/#heading-6)
* [3. Misconfigurations](https://www.cynet.com/network-attacks/privilege-escalation/#heading-7)
* [4. Malware](https://www.cynet.com/network-attacks/privilege-escalation/#heading-8)
* [5. Social Engineering](https://www.cynet.com/network-attacks/privilege-escalation/#heading-9)