**Threat Modelling: DREAD, PASTA, and Their Differences**

**Threats vs. Vulnerabilities**

* **Threats**: Potential dangers that could exploit a weakness in a system.
* **Vulnerabilities**: Weaknesses in a system, process, or technology that threats can exploit.
* **Risk**: Combination of the likelihood of a threat exploiting a vulnerability and its impact. Two real dimensions- likelihood and impact.

**DREAD**

A risk assessment model that scores threats based on five factors:

1. **Damage Potential** – Severity of impact if exploited.
2. **Reproducibility** – Ease of replicating the attack.
3. **Exploitability** – Ease of exploitation.
4. **Affected Users** – Number of impacted users.
5. **Discoverability** – Ease of finding the vulnerability.

* **Pros**: Structured, repeatable, useful for prioritisation.
* **Cons**: Subjectivity in scoring, deprecated by Microsoft due to inconsistent application, lacks business context.

**PASTA**

A seven-step risk-based threat modelling methodology:

1. **Define Objectives** – Business and security goals.
2. **Define Technical Scope** – System components and dependencies.
3. **Application Decomposition** – Data flows and trust boundaries.
4. **Threat Analysis** – Identifying potential threats.
5. **Vulnerability & Weakness Analysis** – Identifying system flaws.
6. **Attack Simulation** – Simulating adversarial behaviour.
7. **Risk & Impact Analysis** – Prioritisation based on business risk.

* **Pros**: Business-aligned, structured, integrates attack simulation, supports both qualitative and quantitative risk assessment.
* **Cons**: Time-intensive, requires detailed system knowledge, complex implementation.

**Key Differences Between DREAD and PASTA**

| **Feature** | **DREAD** | **PASTA** |
| --- | --- | --- |
| **Type** | Quantitative risk scoring | Process-driven threat modelling |
| **Focus** | Impact and likelihood | Business-aligned risk evaluation |
| **Methodology** | Numerical scoring system | Seven-step structured process |
| **Threat Simulation** | No | Yes |
| **Business Context** | Minimal | Strong focus on business objectives |
| **Ease of Use** | Simple but subjective | More complex but comprehensive |

**When to Apply Different Techniques**

| **Scenario** | **Recommended Approach** |
| --- | --- |
| Business-driven security assessment | PASTA, OCTAVE |
| Regulatory compliance | PASTA, NIST 800-30 |
| Secure architecture design | STRIDE, Attack Trees |
| Adversary-based threat simulation | PASTA, ATT&CK Framework |

**When to Combine Techniques**

* **DREAD + STRIDE** – STRIDE categorises threats, DREAD prioritises them.
* **PASTA + Attack Trees** – PASTA aligns threats with business risk, Attack Trees model potential attack paths.
* **STRIDE + PASTA** – STRIDE identifies threat categories, PASTA assesses impact and mitigation.
* **DREAD + CVSS** – CVSS quantifies vulnerabilities, DREAD prioritises threats.

Combining methods helps balance **qualitative and quantitative** risk assessments, improves **threat coverage**, and integrates **business considerations** with technical risks.

**Summary**

* **DREAD**: Quick risk scoring, lacks business alignment.
* **PASTA**: Process-driven, integrates business risk and attack simulation.
* **Different techniques suit different scenarios** – combining them can enhance analysis.
* **Hybrid models** (e.g., PASTA + Attack Trees, DREAD + STRIDE) improve threat modelling by covering **technical risks** and **business impact**.