DevSecOps pipeline contains these 5 continuous phases:

- **Threat Modeling**: This phase involves modeling the risks facing a software deployment. Threat modeling details attack vectors and scenarios, risk analysis, and potential mitigations related to the software DevSecOps teams create. It's important to note that threats are constantly evolving, and threat modeling is a continuous process

- **Security scanning and testing**: This phase is where DevSecOps pipeline tools like SAST and DAST become prevalent. Code is continuously scanned, reviewed, and tested as developers write, compile, and deploy to different environments.

- **Security analysis**: The scanning and testing phase often leads to discovering previously unknown security vulnerabilities. This phase of the DevSecOps pipeline deals with analyzing and prioritizing those issues for remediation.
- **Remediation**: This phase of DevSecOps pipelines deals with actually addressing vulnerabilities discovered in other phases. By analyzing threats and remediating the highest priority issues first, enterprises can strike a balance between delivery speed and threat mitigation that matches their risk appetite.
- **Monitoring**: The monitoring phase of a DevSecOps CI\CD pipeline deals with security monitoring of deployed workloads. This phase can uncover real-time threats, misconfigurations, and other security issues.