**DevSecOps**

* This is the practice that involves security earlier in SDLC.
* To implement DevSecOps, Organizations consider variety of applications security tools (AST) to integrated with various stages of CI/CD Process. Commonly used AST tools include
* SCA (Software Composition Analysis)
* SAST (Static Application Security Testing)
* DAST (Dynamic application security Testing)

**Software Compostion Analysis (SCA)**

* SCA tools scan source code and binaries to identify known vulnerabilities in open source and third-party components.
* They also provide insight into security and license risks.

**Static application Security Testing (SAST)**

* These tools scan propietary code or custom code for coding errors and design flaws that could lead to exploitable weakness.

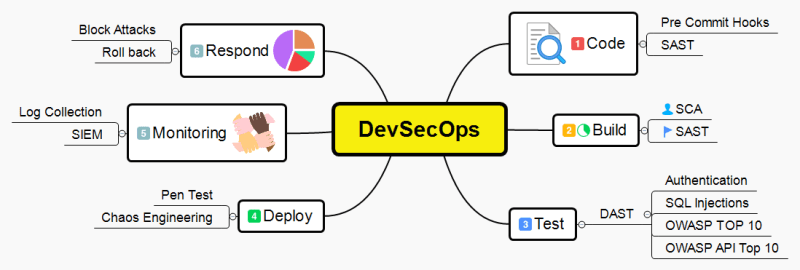
**Dynamic Application Security Testing (DAST)**

* DAST is automated opaque black box testing technology that mimics how a hacker could interact with your web application or API.
* This tests application over a network connection & by examining the client side rendering of application.

**DevSecOps Tools**

* Aqua Security:
  + Used with cloud-native applications i.e cloud native application protection platform (CNAPP).
  + This is very popular for kubernetes, serverless, container security etc
  + <https://www.aquasec.com/> for the offical web page for aqua security
* Checkmarx:
  + This is very popular is application security testing (AST).
  + We can perform
    - SCA
    - SAST
    - Interactive Application Secirity testing
  + <https://checkmarx.com/> for the official web page for CheckMarx
* Micro Focus Cyber Res Fortify:
  + This is very popular in IDE scanning of the code and they offer different products around
    - SAST
    - DAST
    - SCA
  + <https://www.microfocus.com/en-us/cyberres/application-security> for the official web page for Fortity
* Synopsys:
  + AST tools include SCA, interactive,DAST and SAST
  + <https://www.synopsys.com/software-integrity/solutions/devsecops.html> for the official web page
* Veracode:
  + This is cloud solution provider for SAST
  + <https://www.veracode.com/> for veracode
* WhiteSource:
  + This offers SAST, dependecy scanning and risk exposure
  + <https://www.mend.io/> for official web page
* OWASP ZAP:
  + This is from OWASP community which is opensource.
  + Automated active and passive scanning of web applications for vulnerabilities
  + This is DAST testing
  + https://owasp.org/www-project-zap/ for the official pages for OWASP ZAP

**Integrating Security To CI/CD Pipelines**

* Overview of Integration  
  

**Terms To Be Understood**

* OWASP
* OWASP TOP 10
* SIEM - Security information and event management
* NVD - National Vulnerability Database
* CVE- Common Vulnerabilities and Exposures