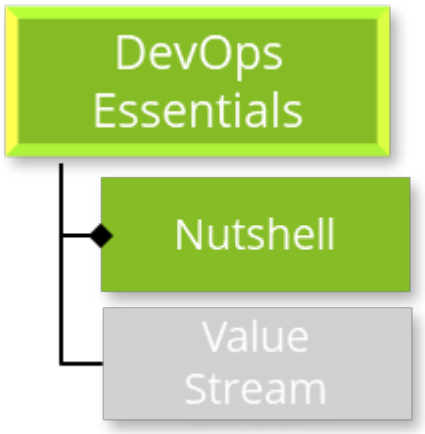
03. DevOps

DevOps는 애플리케이션과 서비스를 빠른 속도로 제공할 수 있도록 조직의 역량을 향상시키는 문화 철학, 방식 및 도구의 조합입니다. 기존의 소프트웨어 개발 및 인프라 관리 프로세스를 사용하는 조직보다 제품을 더 빠르게 혁신하고 개선할 수 있습니다. 이러한 빠른 속도를 통해 조직은 고객을 더 잘 지원하고 시장에서 좀 더 효과적으로 경쟁할 수 있습니다. (AWS)

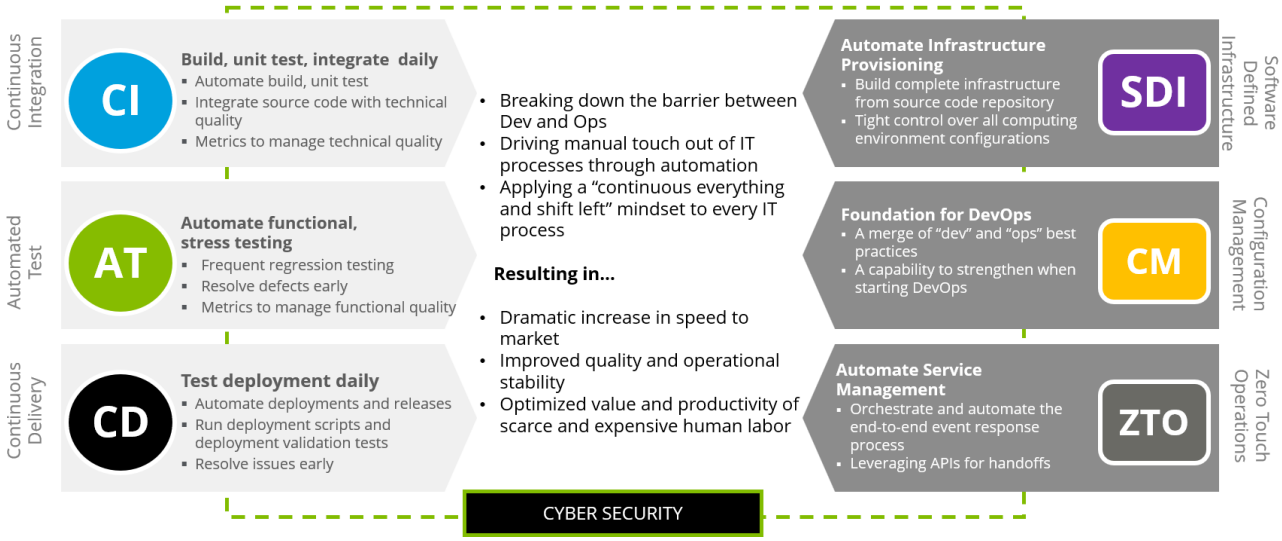
- DevOps Essentials: Nutshell
- DevOps Essentials: Value Stream

DevOps Essentials: Nutshell

DevOps in a Nutshell

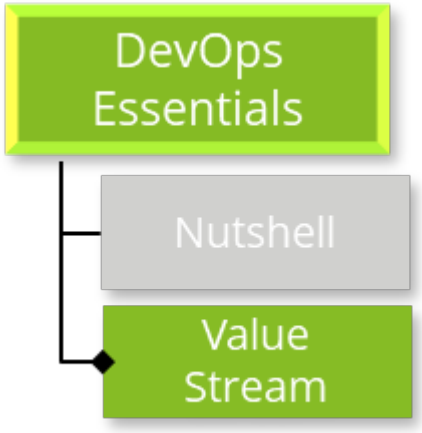


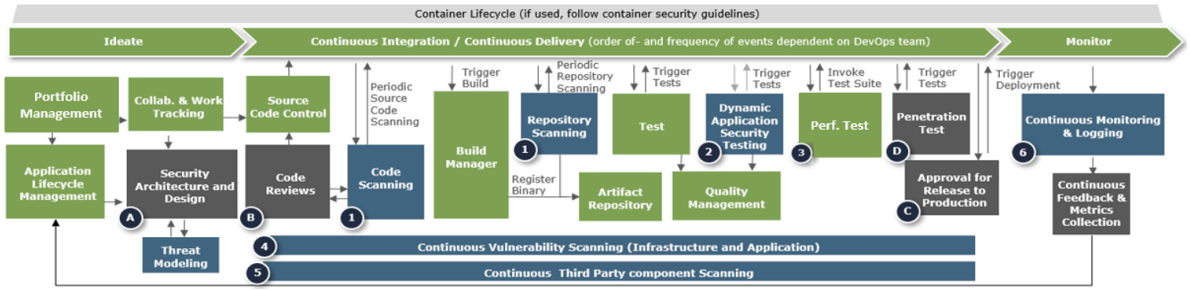
"Agile 및 Lean Thinking을 기반으로하여 기술을 더 빠르게 제공하면서 더 큰 안정성, 품질 및 보안을 제공하는 방식과 행동"



DevOps Essentials: Value Stream

DevOps Value Stream with inbuilt security practices





Built-in Security Automation

The following are commonly identified security gaps in a DevOps Pipeline:

1. Static code scanning to support code quality and secure coding standards (e.g., Fortify, SonarQube, Veracode, Checkmarx)
2. Dynamic application security testing for applications is performed (e.g., WebInspect)
3. Automates performance / load testing for all web applications are completed (e.g., VSTS)
4. Continuous vulnerability scanning of all infrastructure and applications (e.g., Nexus, Qualys)
5. Continuous third party component scanning for vulnerabilities (e.g., Sonatype)
6. Continuous logging and monitoring of production environment (e.g., Splunk)

Manual Security Processes

Checkpoints and gates must be implemented so security controls are in place:

- A. Security and architecture designs are reviewed and documented in a central repository (e.g., Confluence, etc.)
- B. Code reviews are enabled in the workflow and secure coding standards are upheld (e.g., VSTS Pull Requests)
- C. Gates/checkpoints are in place to ensure that release to production goes through the appropriate approval process and exceptions are managed
- D. Periodic penetration tests are performed (e.g., OWASP Zap)

Color Legend

Green	DevOps Processes
Blue	Security Automation
Gray	Security Processes