Welcome!

GitLab

Hello

About me...

- 30 years in the industry
- 25 years in teaching
- Certified Cloud architect
- Passionate about learning
- Also, passionate about Reese's Cups!

Agenda

- Learning objectives
- What is GitLab?
- Building your application in GitLab
- Securing your application in GitLab
- Managing server vulnerabilities

How We’re Going to Work Together

- Slides and words to highlight key concepts
- Demos to bring those concepts “to life”
- Discussion groups and lab work (which will take place in sandboxes provided via AWS WorkSpaces) for hands-on reinforcement
- NOTE: I welcome being interrupted – if you need more info, or clarification, or anything else, just break in and ask. I am here to help you.

Learning Objectives

Learning Objectives

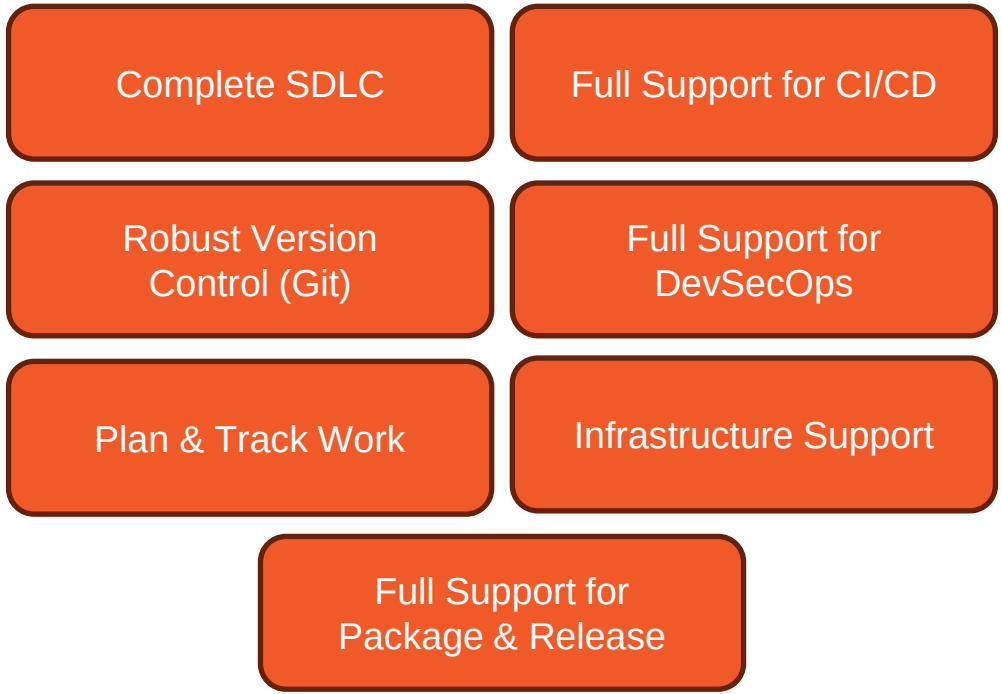
- Understand key concepts and considerations when leveraging DevSecOps in an Agile environment to help “shift security left” during software development
- Construct and prioritize a threat model for an application being developed and use that threat model as a planning tool to guide each phase of the SDLC in a security-minded manner
- Speak to the value of DevSecOps and its consistent application as a set of standards and best practices

Learning Objectives

- Monitor, patch and scan for vulnerabilities in the Operating System (Windows and Linx) and underlying Infrastructure configuration
- Effectively utilize GitLab for Source Code Management and CI/CD, including:
    - Understanding and navigating practical activities related to source code repositories in GitLab
    - Effectively use Software Composition Analysis (SCA), Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST)

What is GitLab?

GitLab Features



Terms

- Project – Where work is organized, managed, tracked, and delivered as part of software creation (like a repository)
- Group – Collection of projects or other groups (like a project)
- Issue – Unit of work in GitLab project (akin to a User Story)
- Epic – Collection of related issues
- Merge Request – Request for merge of one developer’s changes with the rest of the team (like a Pull Request)
- Milestone – Deliverable(s) out of a GitLab project for completion (like a release)

GitLab Flow

https://about.gitlab.com/topics/version-control/what-is-gitlab-flow/

Building Your Application in GitLab

LAB:

Complex Pipeline

https://docs.gitlab.com/ee/ci/quick_start/tutorial.html

LAB:

Publish Packages with CI/CD

https://docs.gitlab.com/ee/user/packages/pypi_repository/auto_publish_tutorial.html. For the Python app, you can use the app & tests at https://github.com/KernelGamut32/python-jenkins.

LAB:

Setup CI/CD Steps

https://docs.gitlab.com/ee/tutorials/setup_steps/index.html

LAB:

Project Runners

https://docs.gitlab.com/ee/tutorials/create_register_first_runner/index.html

Securing Your Application in GitLab

LAB:

Dependency Scanning

https://docs.gitlab.com/ee/tutorials/dependency_scanning.html

LAB:

Docker Container Scanning

https://docs.gitlab.com/ee/tutorials/container_scanning/index.html

LAB:

Security End-to-End

https://university.gitlab.com/learn/course/hands-on-lab-security-essentials/main/hands-on-challenge-gitlab-security-essentials

LAB:

IaC Scanning

https://docs.gitlab.com/ee/user/application_security/iac_scanning/

LAB:

Security End-to-End

Update your Docusaurus solution to include the various concepts we've been learning – add dependency scanning, SAST, DAST, additional stages, etc. to build out a more full-featured pipeline. Address any High or Critical vulnerabilities uncovered.

Managing Server Vulnerabilities

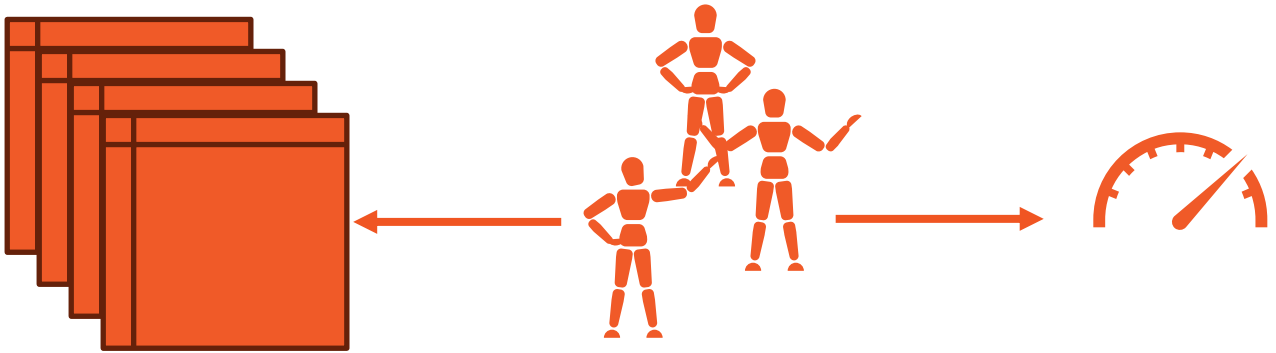
Open Source & Third-Party Products

- Several open source and third-party products are available to assist with scans on both Windows and Linux boxes
- Many of them are web server and website focused (understandably)
- These products include CLI’s or dockerized implementations for use in pipelines (like those leveraged with GitLab)

What Do They Scan?

Can search in several areas of focus, including:

- OWASP Top 10 exposure
- Misconfiguration – outdated software, default directories/files, and issues where configuration exposes the machine (or application) to attack
- As with all the other scans:



Code & Artifacts | Automated Scans | Findings/Results

Popular Options

Include:

- Nessus
- QualysGuard
- Lynis
- Nikto

Additional Protections

- Regular check of key log locations on the system
- Regular patching & security update application

Thank you!

If you have additional questions,
please reach out to me at:
asanders@gamuttechnologysvcs.com

PLURALSIGHT