DevSecOps with OWASP DevSlop

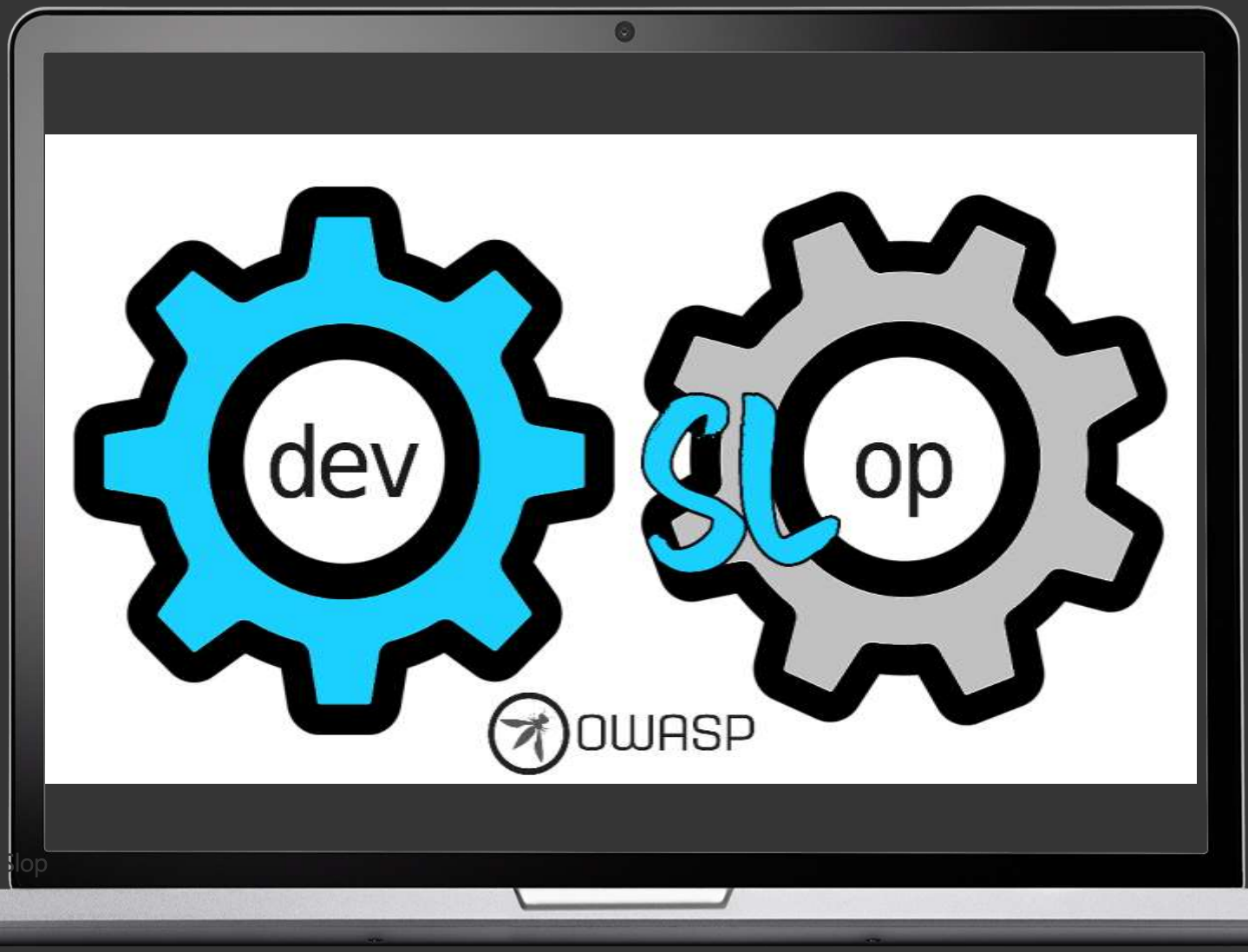
Tanya Janca
CEO and Co-Founder – Security Sidekick

@SheHacksPurple

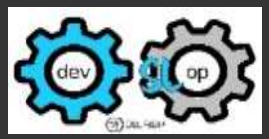
What are we going to talk about today?

What are we going to talk about today?

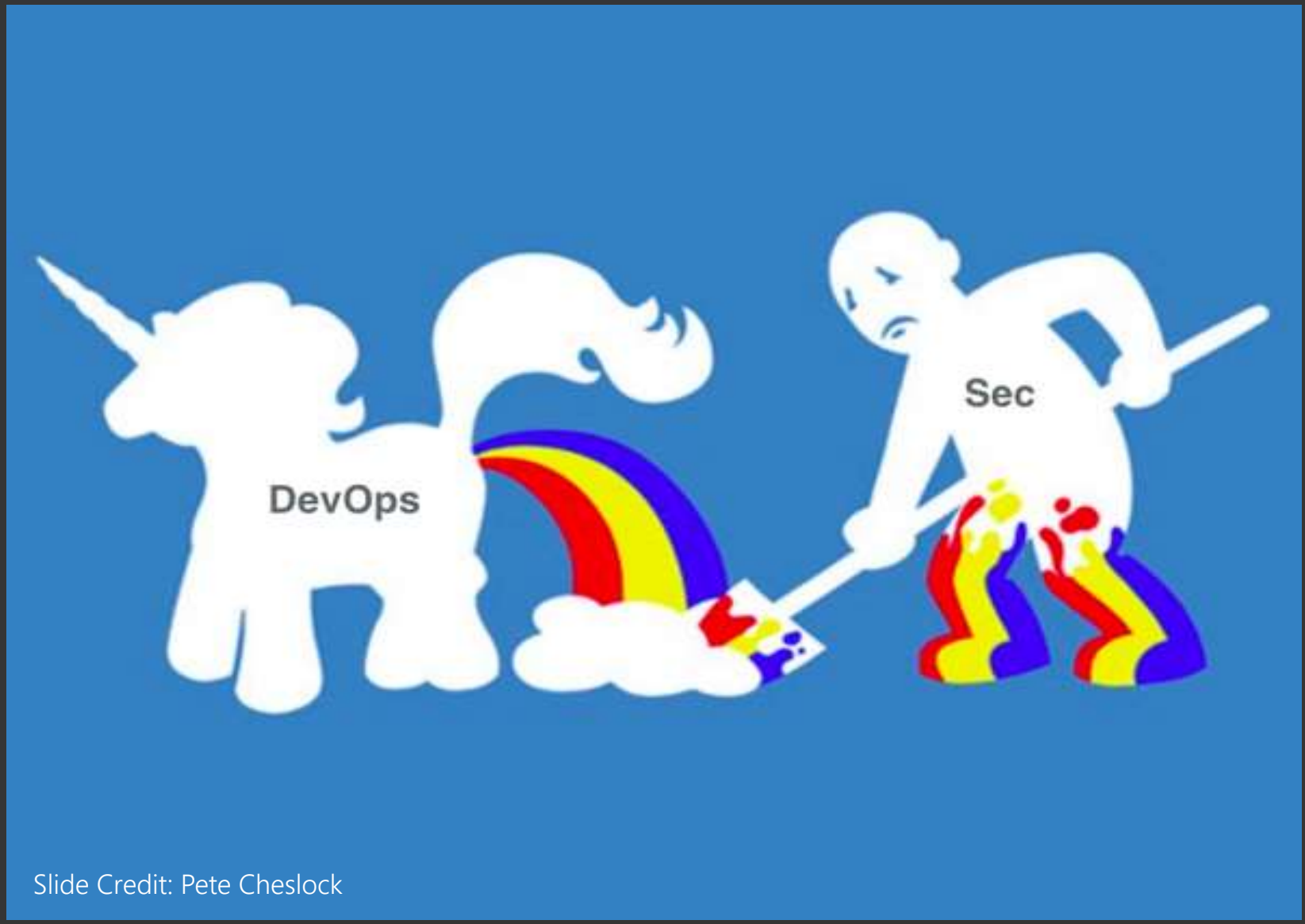
What are we going to talk about today?



What are we going to talk about today?

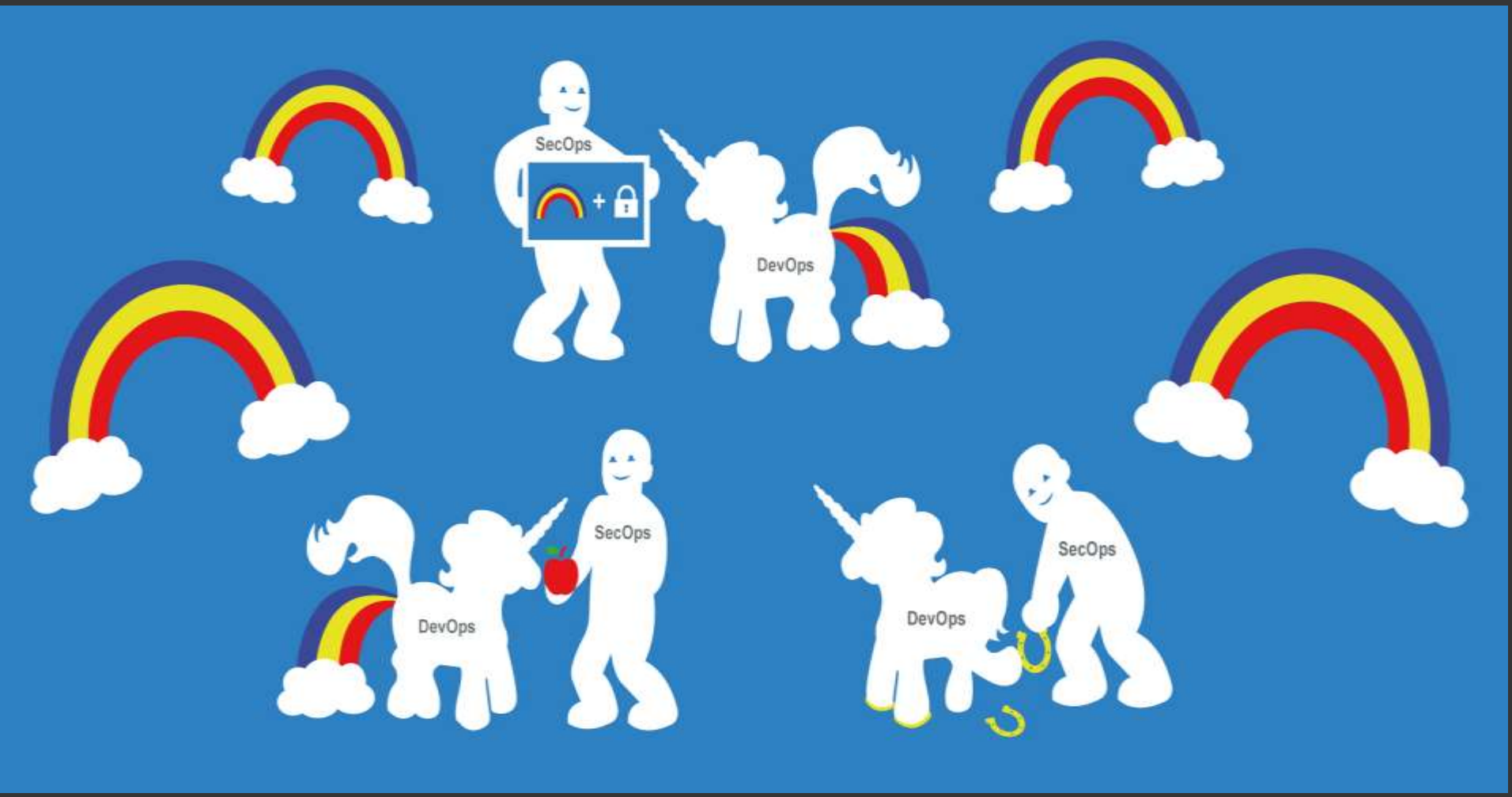


How *some* security people see DevOps



Slide Credit: Pete Cheslock

This is how WE see DevOps: DevSecOps



Slide Credit: DevSecCon

This is me.

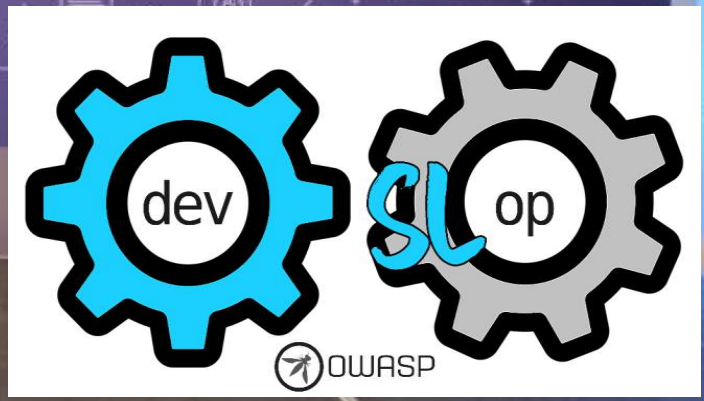
Je suis bilangue.

I'm Tanya Janca.

AKA: @SheHacksPurple

Security Sidekick

CEO & Co-Founder!



WHAT is OWASP?

Open Web Application Security Project

What is AppSec?

"It's any and every activity that you perform to ensure that your software is secure."

-Me

What is DevSecOps?

"It's AppSec in a DevOps environment."

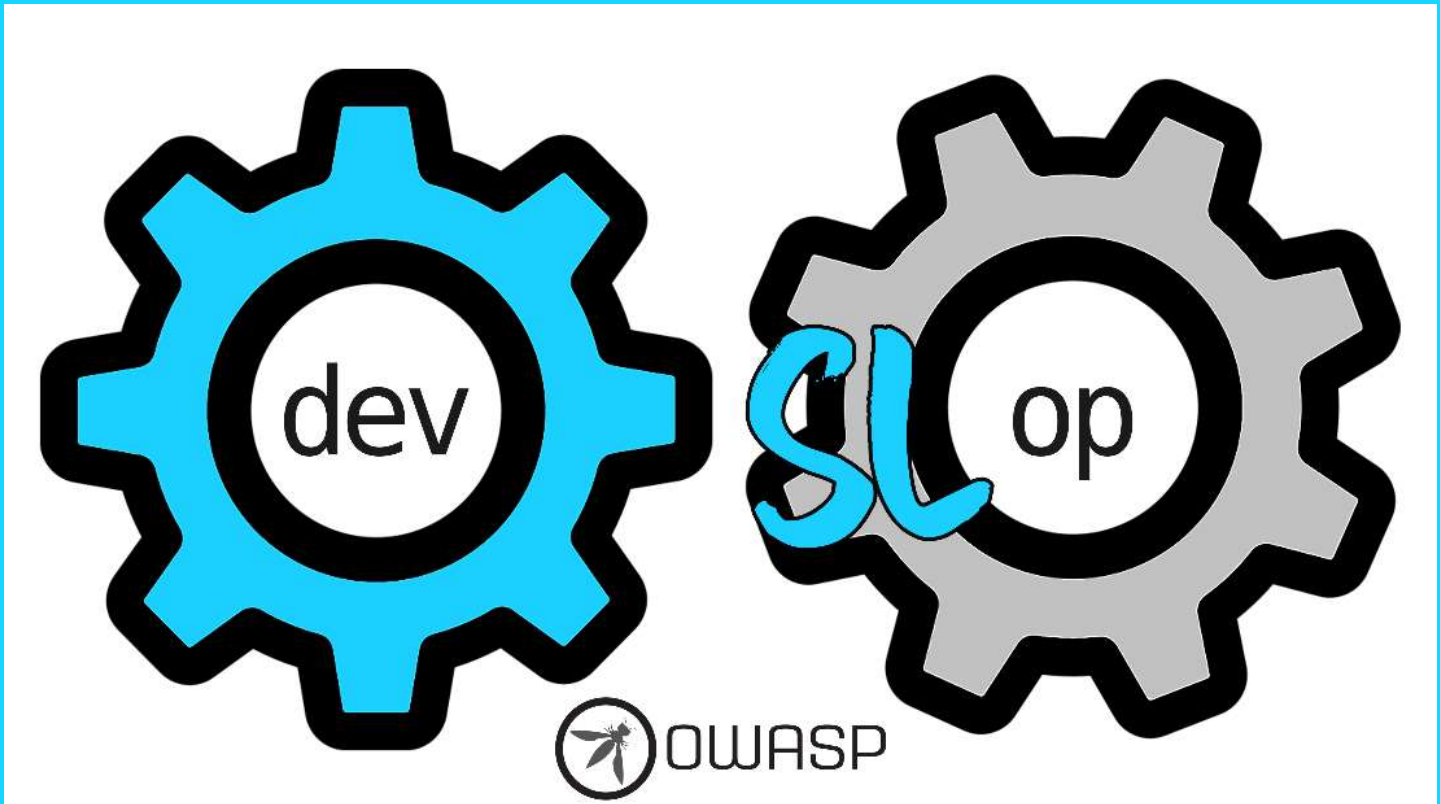
-Imran Mohammed

What is DevSecOps?

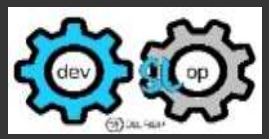
"It's DevOps, done properly."

-Everyone Ever

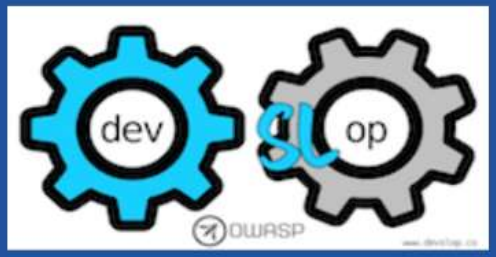
What is DevSlop?



The OWASP DevSlop PROJECT



OWASP DevSlop Home About Modules Team Schedule Contact



Welcome to OWASP DevSlop

Learn DevSecOps by using these tools!

DevSlop Project Modules

We have many different parts to our project, called Modules, figure out which one works for you.

Watch the DevSlop Show!

We stream LIVE every Sunday from 1-2 pm, Eastern Standard Time on Mixer and Twitch!
You can catch the shows you've missed on **YouTube**.

Learn *With* Us

Find out more about what DevSlop can teach you. Check out our teaching schedule.

The OWASP DevSlop Show

@Owasp_DevSlop

https://aka.ms/DevSlopShow

First, it was just Nicole and Tanya.

Nicole Becher

Franziska Bühler

Tanya Janca

Mordecai Kraushar

Marco Tietz

Patxi Gortázar

Manuel Lopez Arredondo

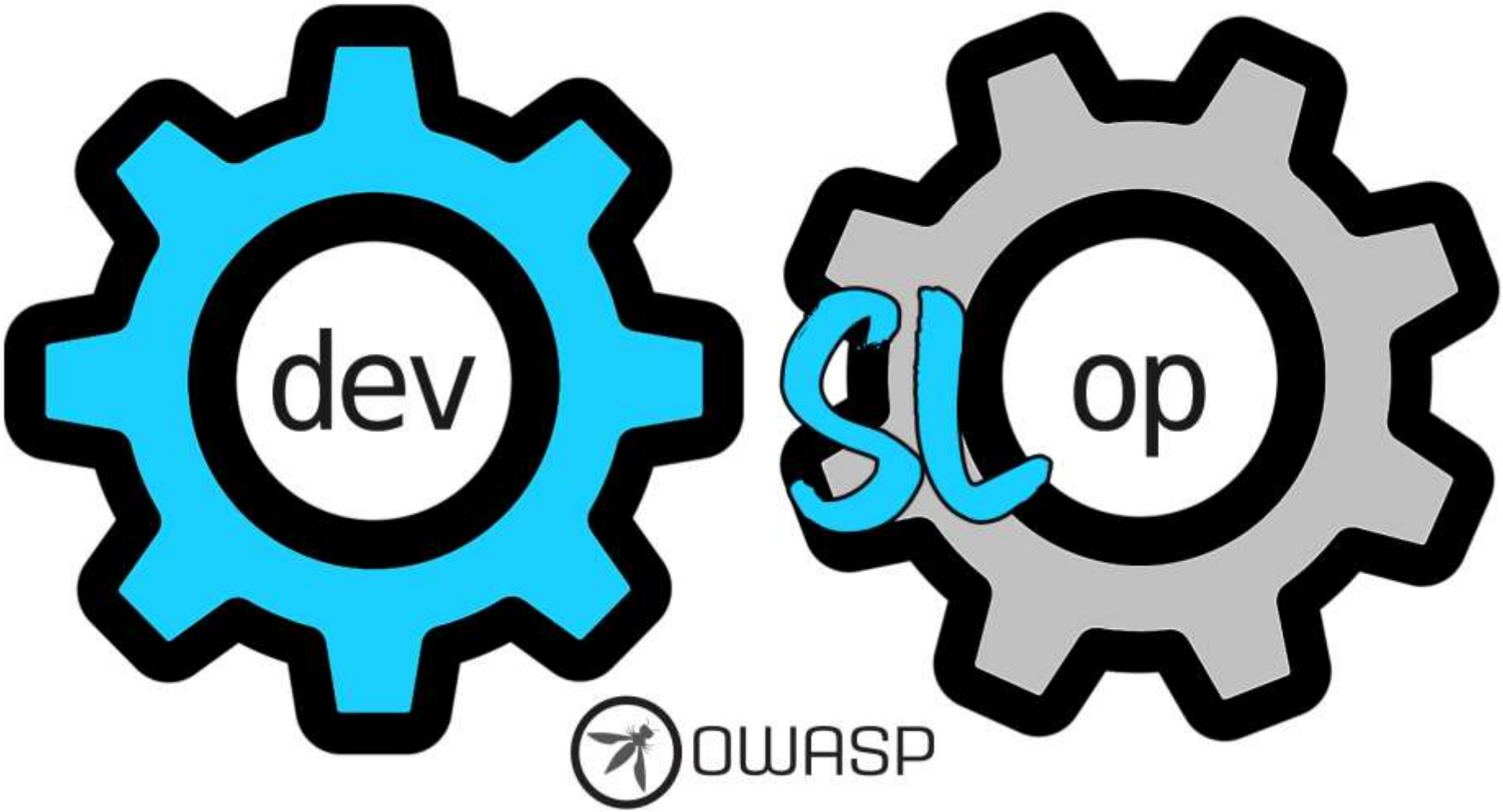
Dominique Righetto

Carl-Hugo Marcotte

Abel Wang

Nancy Gariché

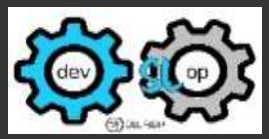
Our beautiful logo: made by Nikki Becher!



How do you learn DevSecOps?

You do it.

The 7 Steps of 'Patty the Pipeline'



01 Verify 3rd Party Components

02 SAST

03 DAST

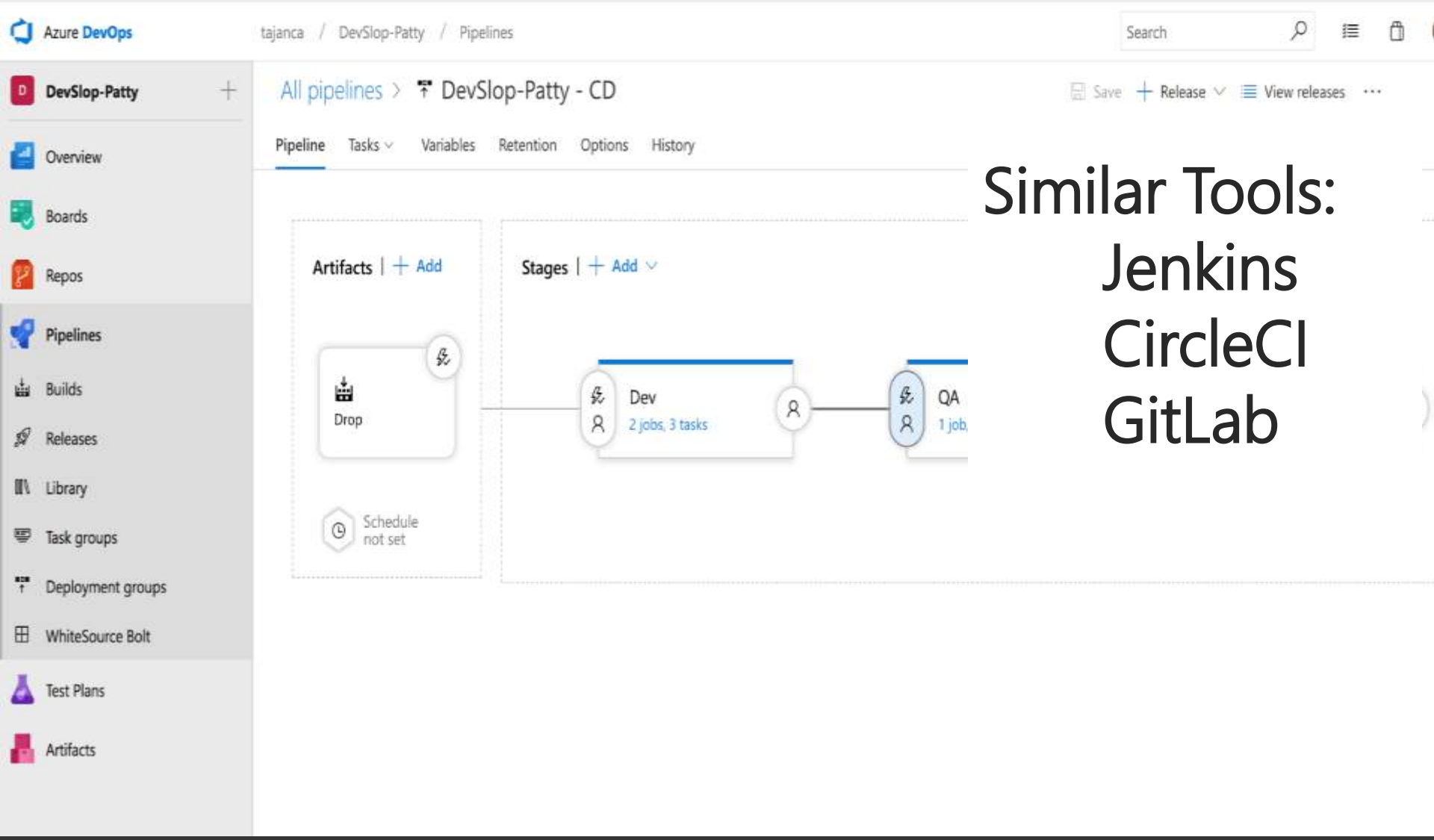
04 Infrastructure

05 Security Hygiene (HTTPS and Encryption)

06 Secret Store

07 Scanning for credentials and secrets

Patty: an Azure DevOps Pipeline



Similar Tools:
Jenkins
CircleCI
GitLab

Patty: an Azure DevOps Pipeline

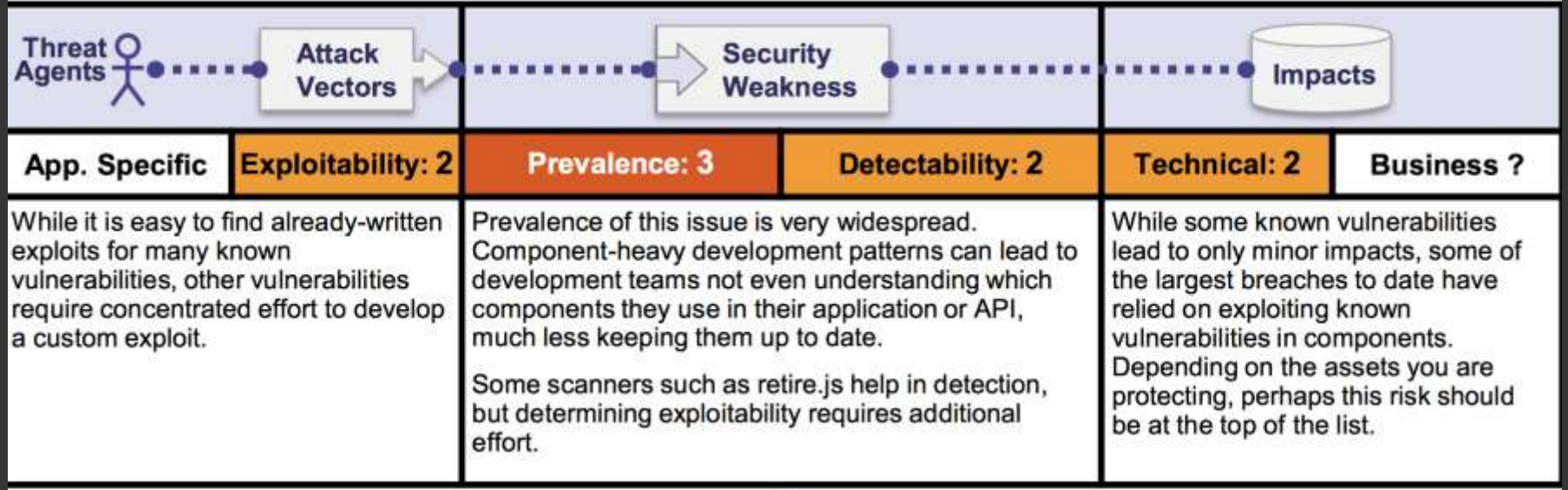
Let’s look at each part.

Step 1: Verifying 3rd party components

Step 1: Verifying 3rd party components

A9 :2017 Using Components with Known Vulnerabilities

15



Is the Application Vulnerable?

You are likely vulnerable:

- If you do not know the versions of all components you use (both client-side and server-side). This includes components you directly use as well as nested dependencies.
- If software is vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all

How to Prevent

There should be a patch management process in place to:

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Continuously inventory the versions of both client-side and server-side components (e.g. frameworks, libraries) and their dependencies using tools like versions, DependencyCheck, retire.js, etc. Continuously monitor sources like CVE and NVD

Demo 1: Verifying 3rd party components

https://aka.ms/whitesourcebolt

Similar Tools:

Owasp Dependency Check

Sonatype Nexus

Retire.js

Hakiri

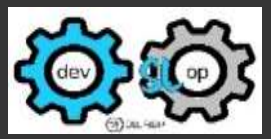
Audit-bundler

SRC:CLR

Black Duck

Veracode

Demo 1: White Source Bolt



Video Here: https://aka.ms/whitesourcebolt

Step 2: Static Code Analysis (SAST)

Demo 2: Static Application Security Testing (SAST)

Similar Tools:

Checkmarx

Fortify

Veracode

Find Bugs

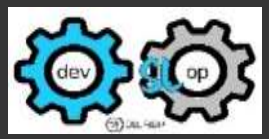
AppScan Source

Synopsys

Roslyn

Puma Scan

Demo 2: SonarQube



Video Unavailable

Step 3: Dynamic Testing (DAST)

Photo:
Franziska Buehler
DevOpsDays Zurich, 2018

Demo 3: Dynamic Application Security Testing (DAST)

Similar Tools

SonaType
Burp Suite
AppScan
App Spider
VeraCode
NetSparker
Acunetix
Vega
Arachni
SkipFish

Demo 3: Zed Attack Proxy (Zap!)

https://aka.ms/OWASP-Zap

Step 4: Infrastructure

Photo: #WOCTechChat

Demo 4: Infrastructure

Similar Tools
Nessus
Nexpose
NMap

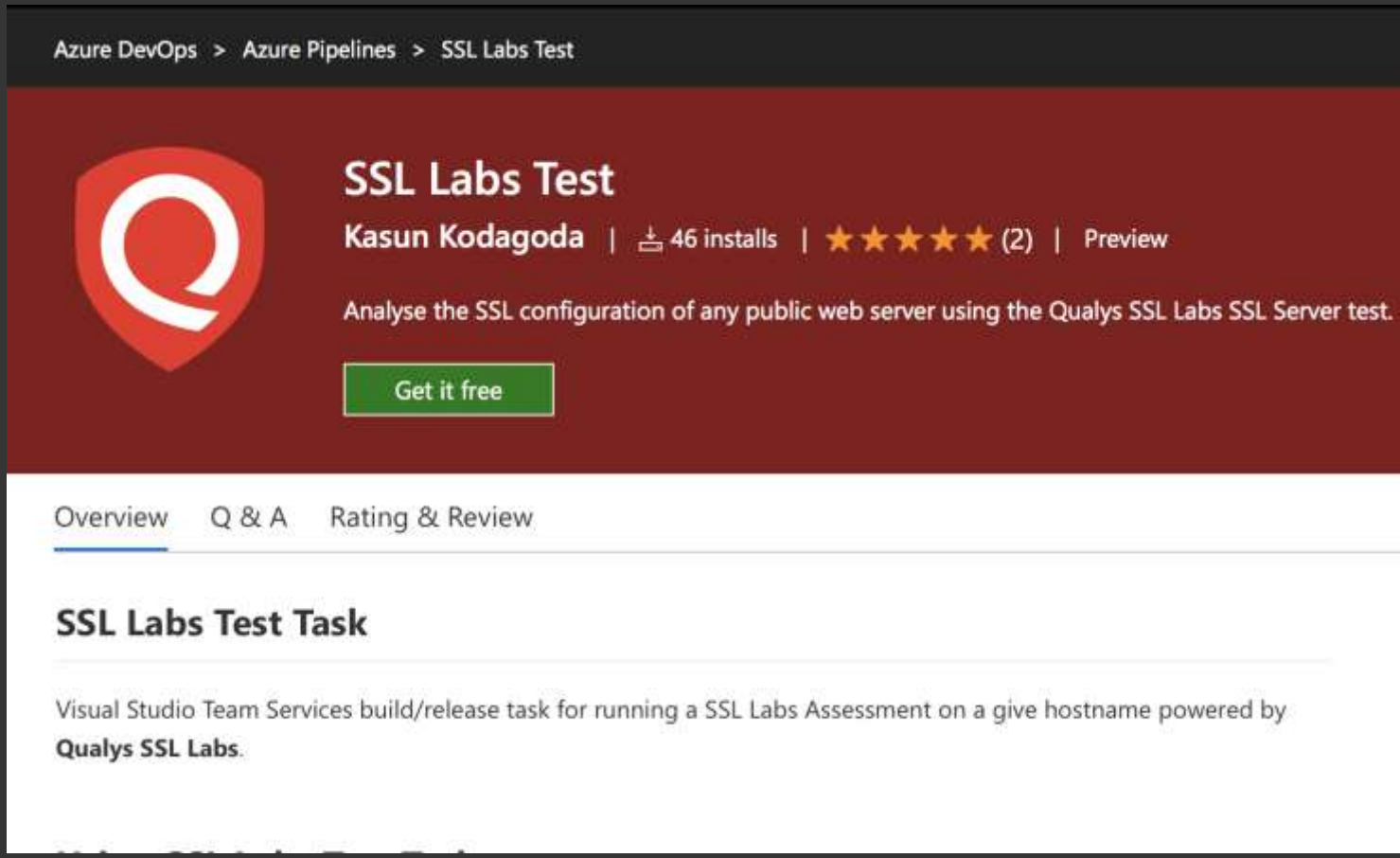
https://aka.ms/DevSlop-AzSK

Demo 4: AZsK (Secure DevOps Kit for Azure)

https://aka.ms/DevSlop-AzSK

Step 5: Security Hygiene (HTTPS & Encryption)

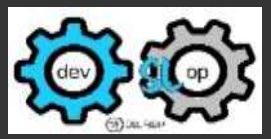
Demo 5: Security Hygiene (HTTPS & Encryption)



Similar Tools
Hardenize.io
Qualys
SecurityHeaders.com

https://aka.ms/ssllabs

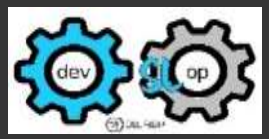
Demo 5: SSL Labs

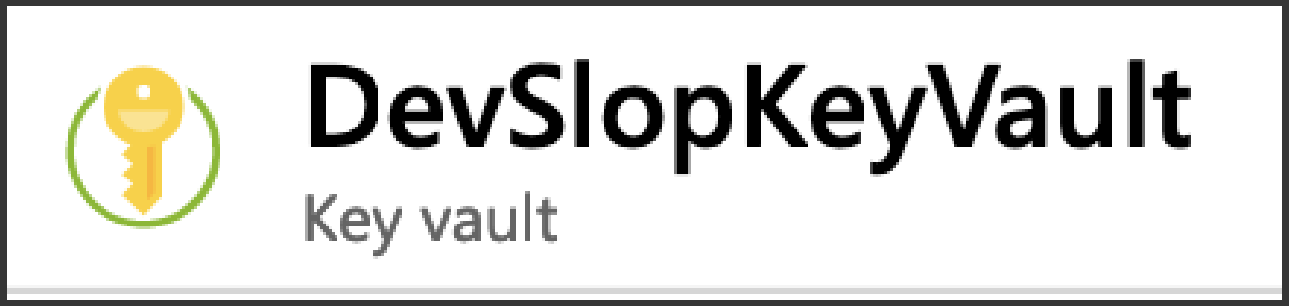


https://aka.ms/ssllabs

Step 6: Using a Secret Store

Demo 6: Using a Secret Store





Similar Tools:
Truffle Hog
Torus
Vault by Hashicorp
GitSecrets
DockerSecrets
Google KMS
Amazon KMS

https://aka.ms/Key-Vault

Demo 6: Azure Key Vault

https://aka.ms/Key-Vault

Step 7: Scanning for secrets

Step 7: Scanning for secrets

Similar Tools:

Yelp/detect-secrets

GittyLeaks

Git Secrets

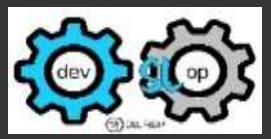
Repo Supervisor

Git Hound

Ava

https://aka.ms/credscan-globalappsec

Step 7: Scanning for secrets



https://aka.ms/credscan-globalappsec

REVIEW: The 7 Steps of 'Patty the Pipeline'

01 Verify 3rd Party Components

02 SAST

03 DAST

04 Infrastructure

05 Security Hygiene (HTTPS and Encryption)

06 Secret Store

07 Scanning for credentials and secrets

Even More DevSecOps Options!

01 Negative Unit Tests

02 IaST (Interactive App Security Testing)

03 WAF (Web App Firewall)

04 RASP (Real-time App Security Protection)

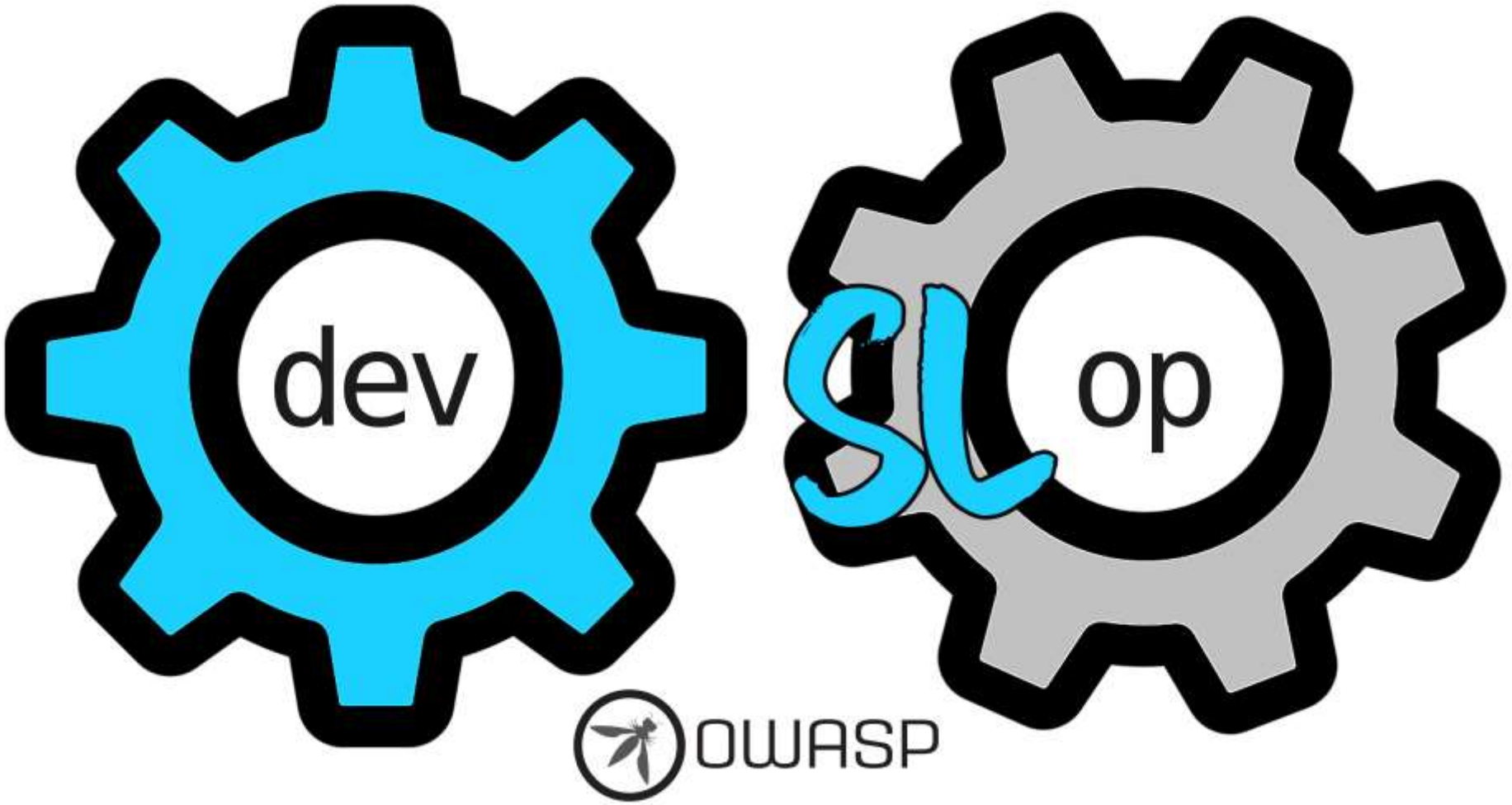
05 Linting (Grammar Police, strict parsing)

Resources

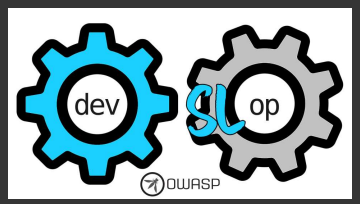
A long-term (DevSecOps) relationship

@OWASP_DevSlop

OWASP DevSlop Has Your Back!



Resources



Follow DevSlop?

Twitter: @OWASP_DevSlop

https://dev.to/owasp_devslop

https://aka.ms/DevSlopShow

https://DevSlop.co

Resources: ME!

Resources: Mentoring Monday

Resources: Open Web Application Security Project

Women of Security welcomes you!

WoSEC

Paris, Ottawa, San Francisco, Singapore, Dallas, Houston, Austin, Vancouver, Portland, Ottawa, Chicago, Bangalore, Boise, Montréal, Zurich, Nairobi, Johannesburg, Stockholm , Victoria, Milwaukee, Detroit, Denver, Barcelona, Madrid

Canada, France, USA, India, Switzerland, Kenya, South Africa, Sweden, Spain

@WoSECtweets

Thank You

Tanya Janca

CEO and Co-Founder Security Sidekick
WoSEC Co-Founder & Victoria Chapter Leader
OWASP DevSlop Project Leader

@Owasp_DevSlop

@SheHacksPurple