

# DevSecOps with OWASP DevSlop

Tanya Janca

CEO and Co-Founder – **Security Sidekick**

# What are we going to talk about today?



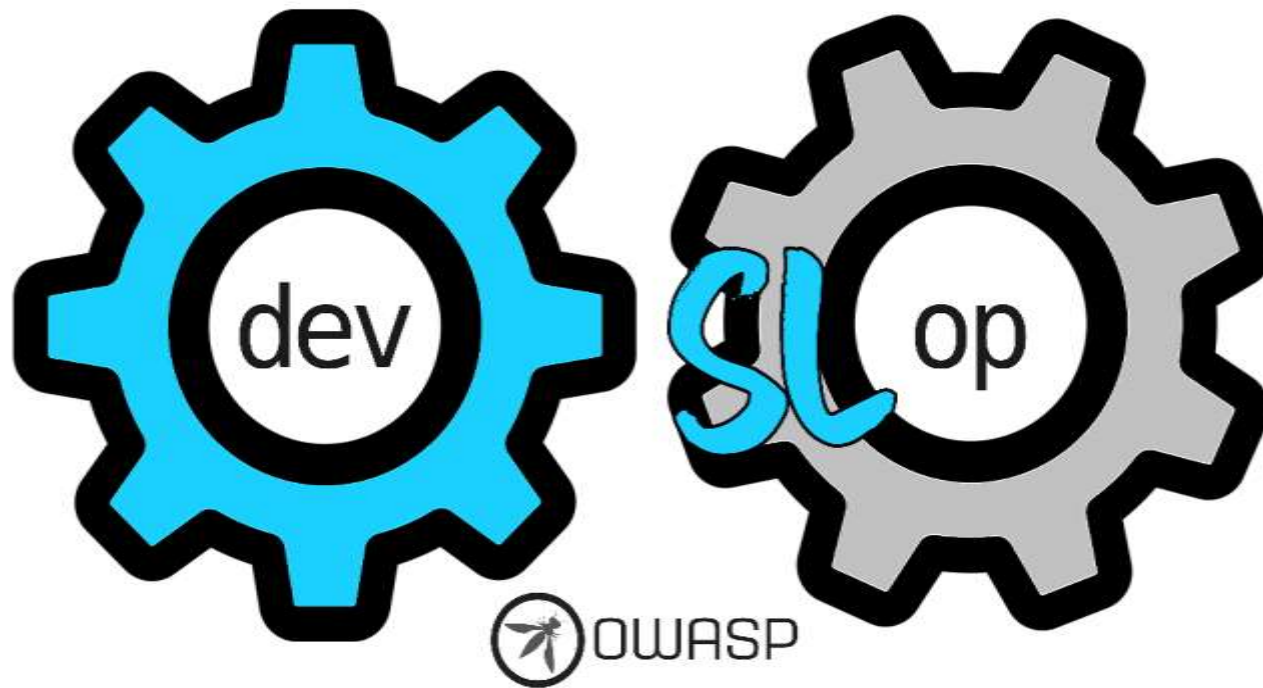
# DevOps

What are we going to talk about today?



DevSecOps

# What are we going to talk about today?



What are we going to talk about today?



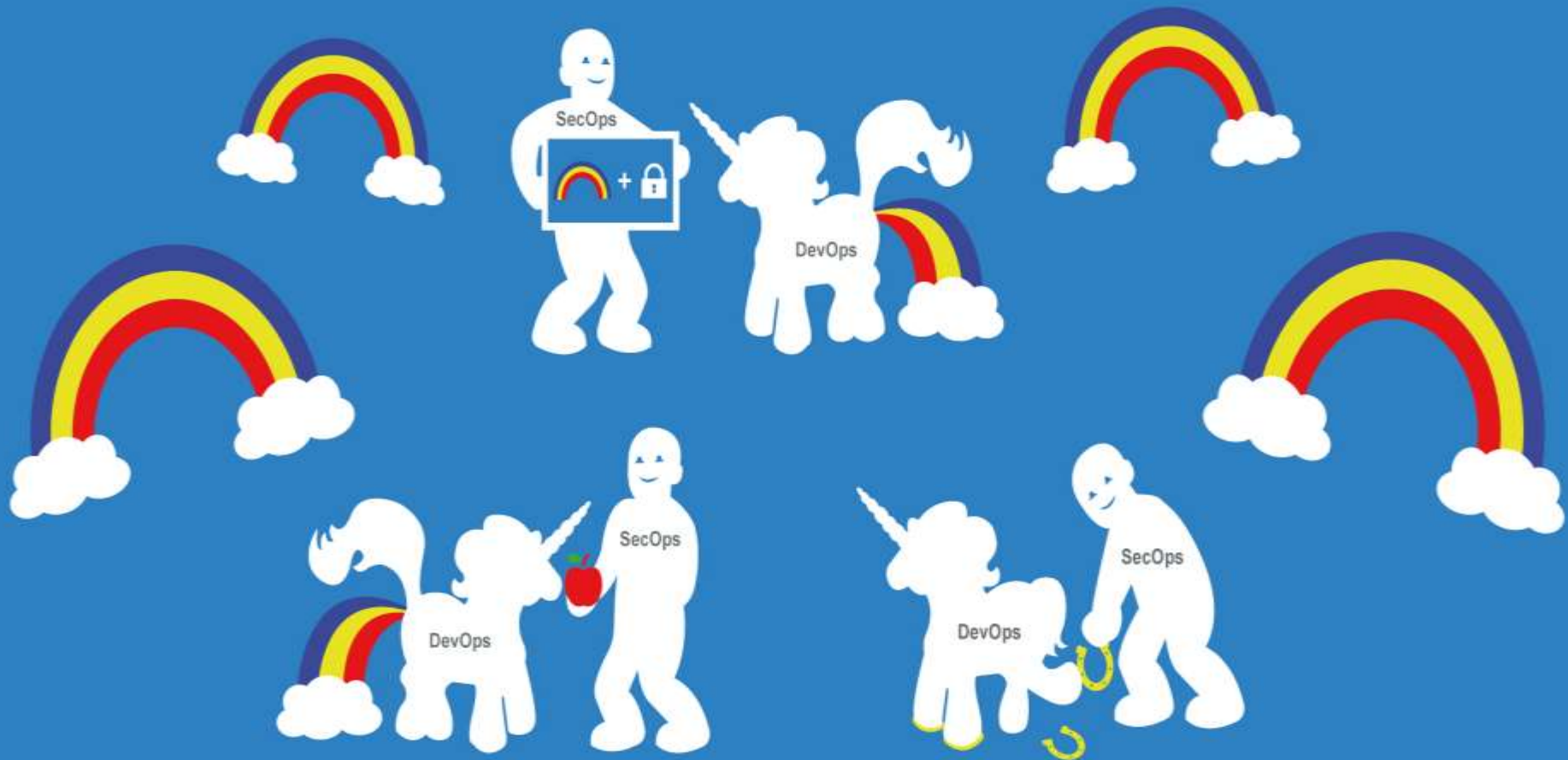
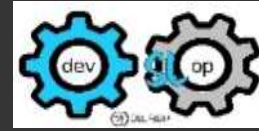
# Patty the (DevSecOps) Pipeline

# How *some* security people see DevOps



Slide Credit: Pete Cheslock

# This is how WE see DevOps: DevSecOps

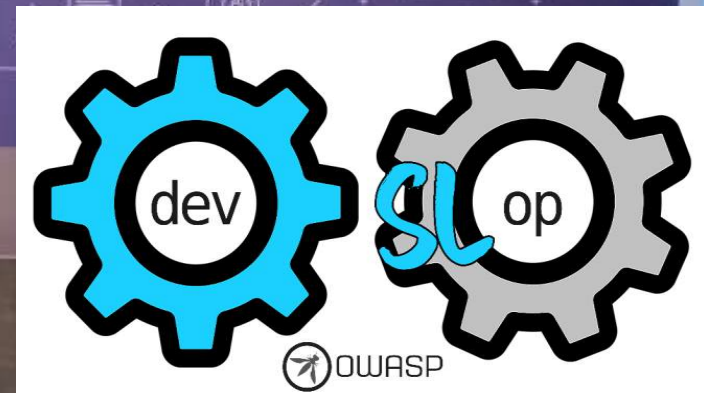




This is me. **Je suis bilangue.**

AKA: @SheHacksPurple

I'm Tanya Janca.





# 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

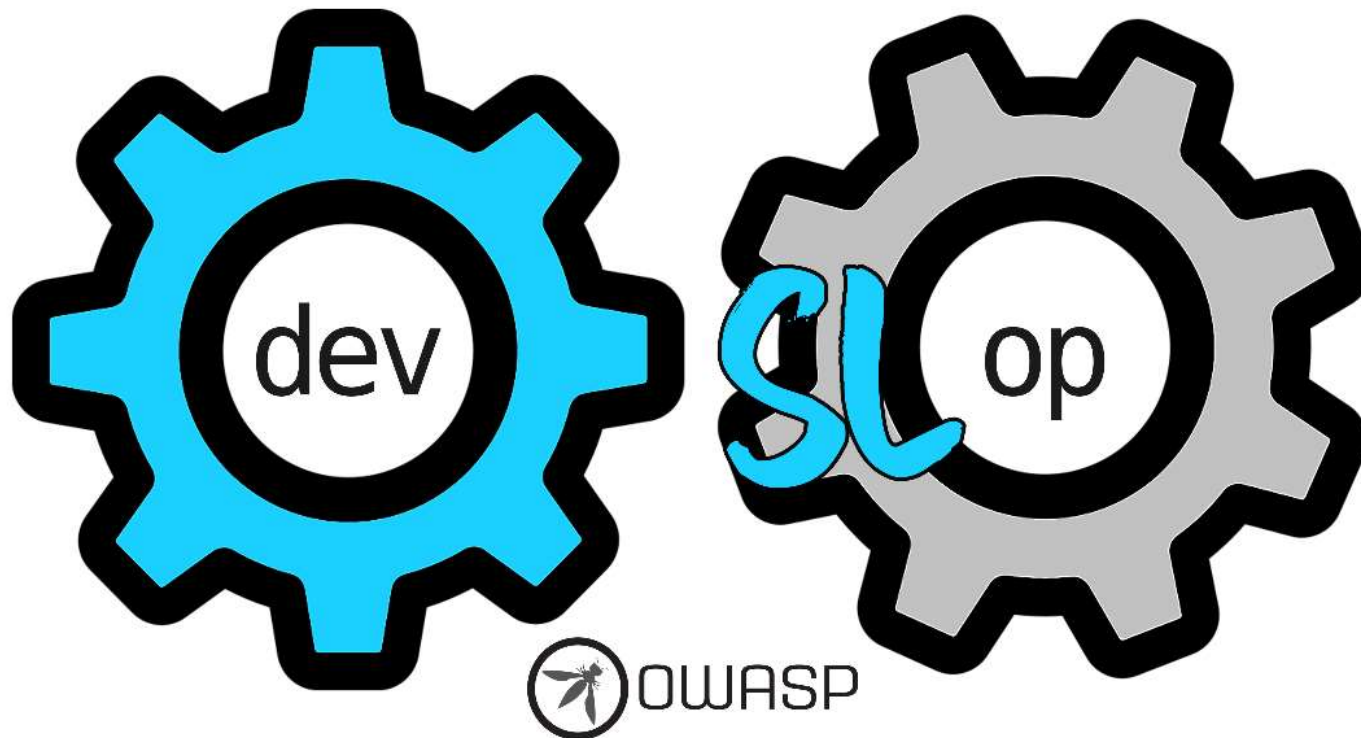
# What is DevSecOps?



"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



YouTube CA

Search

Home

Trending

Subscriptions

LIBRARY

History

Watch later

Liked videos

OWASP DevSlop ...

Tanya Talks Tech

Subscriptions

Popular on YouTube...

Music

Sports

Gaming

MORE FROM YOUTUBE

YouTube Premium

Movies & Shows

dev slop

OWASP DevSlop

403 subscribers

CUSTOMIZE CHANNEL

YOUTUBE STUDIO (BETA)

HOME VIDEOS PLAYLISTS CHANNELS DISCUSSION ABOUT

Uploads PLAY ALL

FEATURED CHANNELS

POPULAR CHANNELS

BuzzFeedVideo

SUBSCRIBE

The ACE Family

SUBSCRIBE

Tasty

SUBSCRIBE

OWASP DevSlop E13 - Juice Shop with Björn Kimminich!

15 views • 2 days ago

OWASP DevSlop E12.1 - Adding Zap to the Azure...

20 views • 4 days ago

OWASP DevSlop E11 - ZSC Tool Project with Johanna...

11 views • 4 days ago

OWASP DevSlop E10 Patty the Pipeline Publishes for th...

14 views • 4 days ago

@Owasp\_DevSlop

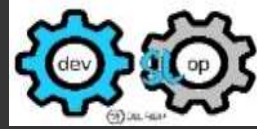
<https://aka.ms/DevSlopShow>



@SheHacksPurple



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

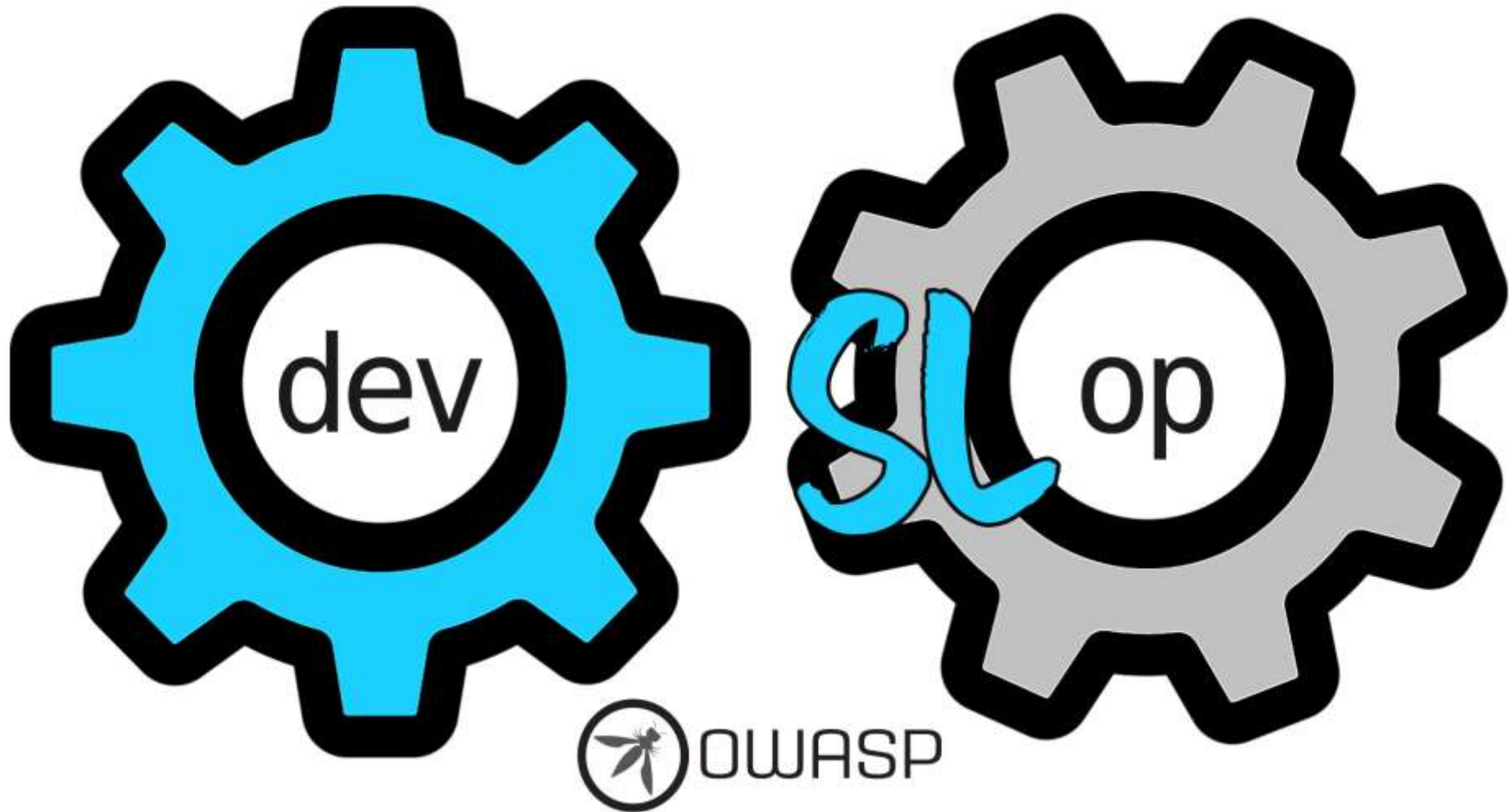


Abel Wang

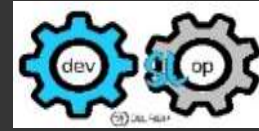


Nancy Gariché

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



Azure DevOps

tajanca / DevSlop-Patty / Pipelines

Search

Save + Release View releases

All pipelines > DevSlop-Patty - CD

Pipeline Tasks Variables Retention Options History

Artifacts | + Add

Stages | + Add

Drop

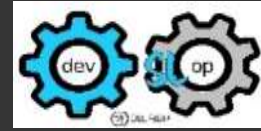
Dev  
2 jobs, 3 tasks

QA  
1 job

Schedule not set

Similar Tools:  
Jenkins  
CircleCI  
GitLab

# Patty: an Azure DevOps Pipeline



**Let's look at each part.**



# Step 1: Verifying 3<sup>rd</sup> party components



#9 on the OWASP Top Ten

Photo: #WOCTechChat

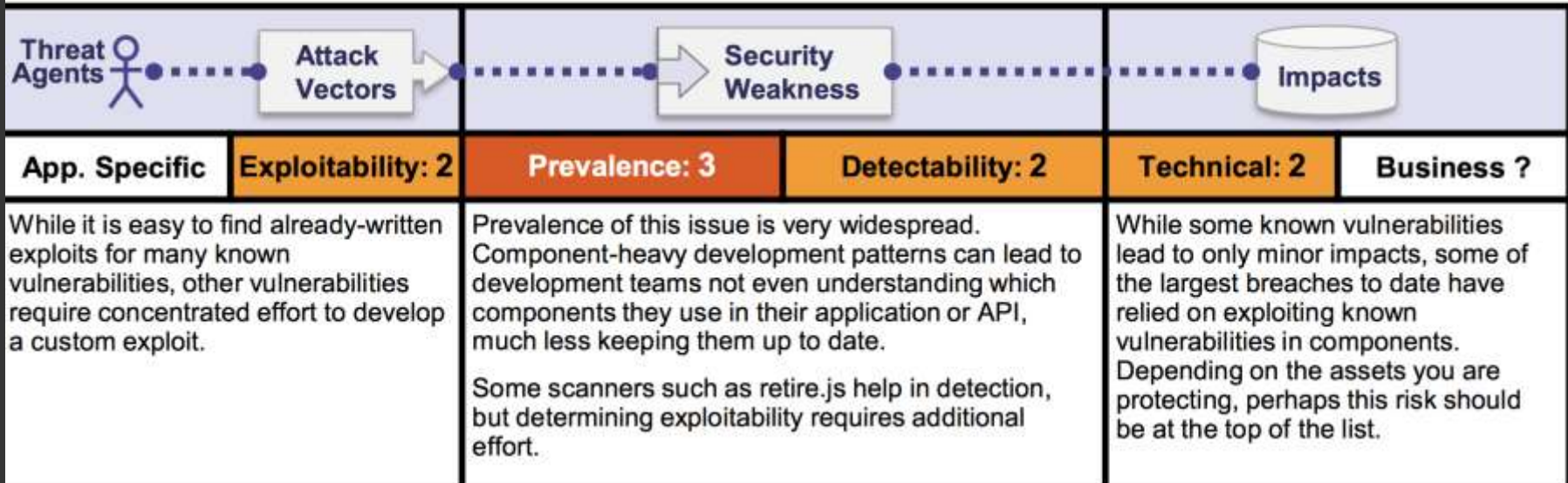
# Step 1: Verifying 3<sup>rd</sup> party components



**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 3<sup>rd</sup> party components



Azure DevOps > Azure Pipelines > WhiteSource Bolt



## WhiteSource Bolt

WhiteSource | 1,601 installs | (9) | Free

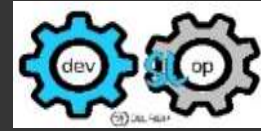
Detect & fix security vulnerabilities, problematic open source licenses.

Get it free

**Similar Tools:**  
**Owasp Dependency Check**  
**Sonatype Nexus**  
**Retire.js**  
**Hakiri**  
**Audit-bundler**  
**SRC:CLR**  
**Black Duck**  
**Veracode**

<https://aka.ms/whitesourcebolt>

# Demo 1: White Source Bolt



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



# Step 2: Static Code Analysis (SAST)



Photo: #WOCTechChat



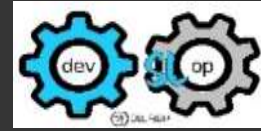


**sonarqube** 

**sonarcloud** 

**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

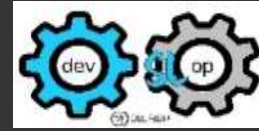
Vega

Arachni

SkipFish

## OWASP Zed Attack Proxy Project

# Demo 3: Zed Attack Proxy (Zap!)



<https://aka.ms/OWASP-Zap>

# Step 4: Infrastructure



Photo: #WOCTechChat

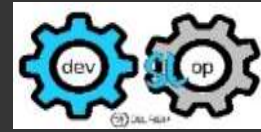
# Demo 4: Infrastructure



**Similar Tools**  
**Nessus**  
**Nexpose**  
**NMap**

<https://aka.ms/DevSlop-AzSK>

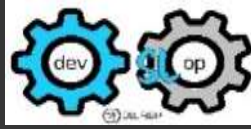
## Demo 4: AZsK (Secure DevOps Kit for Azure)



<https://aka.ms/DevSlop-AzSK>

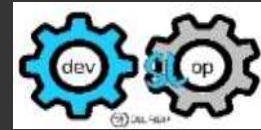


# Step 5: Security Hygiene (HTTPS & Encryption)





# Demo 5: Security Hygiene (HTTPS & Encryption)



Azure DevOps > Azure Pipelines > SSL Labs Test



## SSL Labs Test

Kasun Kodagoda | 46 installs | ★★★★★ (2) | Preview

Analyse the SSL configuration of any public web server using the Qualys SSL Labs SSL Server test.

Get it free

Overview Q & A Rating & Review

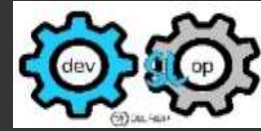
### SSL Labs Test Task

Visual Studio Team Services build/release task for running a SSL Labs Assessment on a give hostname powered by Qualys SSL Labs.

Similar Tools  
Hardenize.io  
Qualys  
SecurityHeaders.com

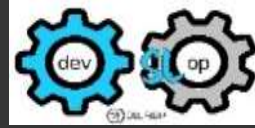
<https://aka.ms/ssllabs>

# Demo 5: SSL Labs



<https://aka.ms/ssllabs>

# Step 6: Using a Secret Store



# Demo 6: Using a Secret Store



## DevSlopKeyVault

Key vault

**Similar Tools:**

**Truffle Hog**

**Torus**

**Vault by Hashicorp**

**GitSecrets**

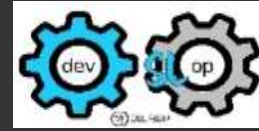
**DockerSecrets**

**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



Run CredScan

CredScan (Preview)



Run Roslyn Analyzers

Roslyn Analyzers



Create Security Analysis Report

Security Analysis Report (Preview)



Create Security Analysis Report

Security Analysis Report

## Similar Tools:

[Yelp/detect-secrets](https://yelp.com/detect-secrets)

GittyLeaks

Git Secrets

Repo Supervisor

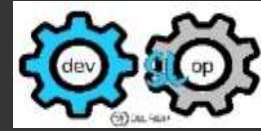
Git Hound

Ava

<https://aka.ms/credscan-globalappsec>

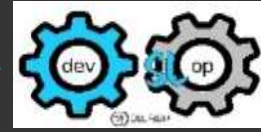


## Step 7: Scanning for secrets



<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

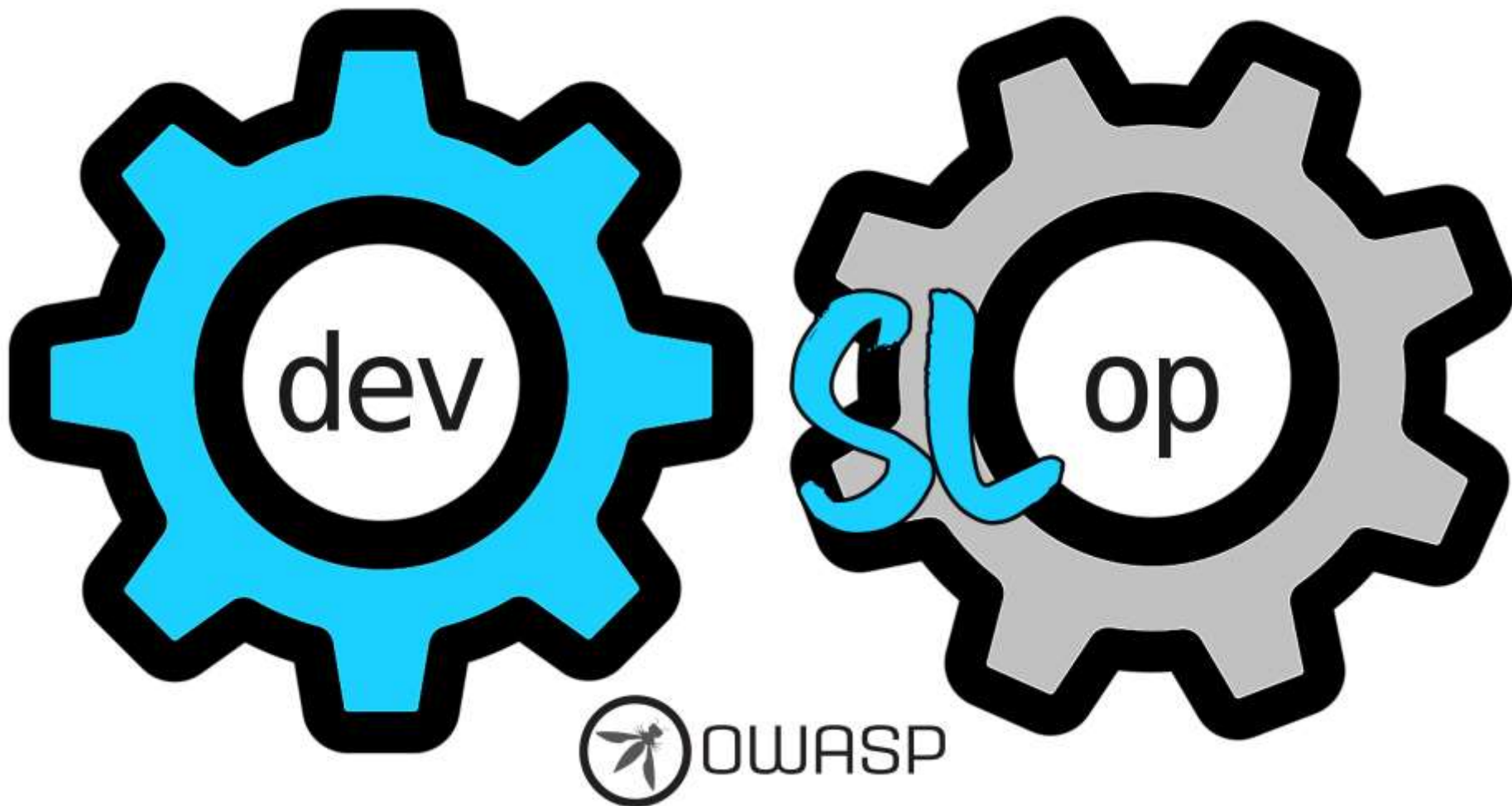
Linting (Grammar Police, strict parsing)

# Resources

*A long-term (DevSecOps)  
relationship*



# OWASP DevSlop Has Your Back!

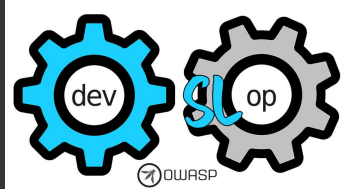


DevSlop.co

<https://aka.ms/DevSlopShow>



@SheHacksPurple



## Follow DevSlop?

Twitter: @OWASP\_DevSlop

[https://dev.to/owasp\\_devslop](https://dev.to/owasp_devslop)

<https://aka.ms/DevSlopShow>

<https://DevSlop.co>

owasp\_devslop

# Resources: ME!

## Follow me?

Twitter: @SheHacksPurple

<https://medium.com/@SheHacksPurple>

<https://dev.to/SheHacksPurple>

<https://YouTube.com/SheHacksPurple>

<https://mailchi.mp/e2ab45528831/shehackspurple>



# Resources: Mentoring Monday

A laptop screen with a dark background. The text '#MentoringMonday' is written in a large, yellow, sans-serif font. Below it, the words 'EVERY MONDAY' are written in a smaller, white, sans-serif font.

#MentoringMonday

EVERY MONDAY

# Resources: Open Web Application Security Project



#OWASPllove

<https://owasp.org>



# 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