



# Stop doing software security wrong - do it right!

– Cloud Native Denmark, October 7th – 8th, 2025

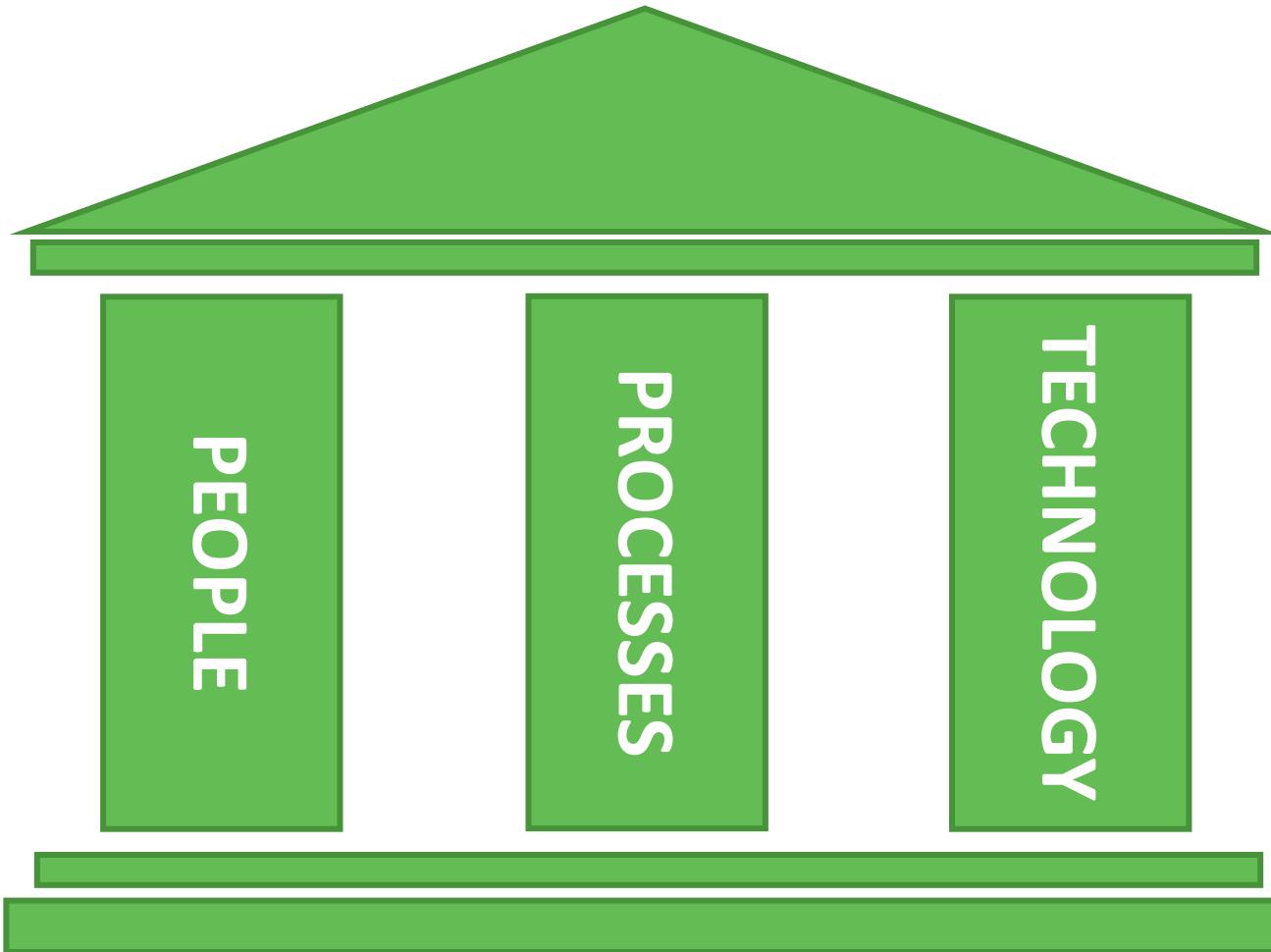
# Thomas Ljungberg Kristensen

1996	Aarhus University, Master of Computer Sciences Cryptographical Protocol Theory	
2003	Systematic, Systems Engineer	
2007	Danske Bank, Developer	
2012	Kamstrup, Systems Engineer	
2014	FortConsult (part of NCC group), Senior Security Consultant	

2015 –	<i>WelcomeSecurity, Security Advisor and Owner</i>	
2019 –	<i>OWASP Co-chapter Lead, Aarhus</i>	
2019	Deloitte, Senior Manager	
2020 – 2021	Norlys, IT Security Architect	
2021 – 2021	Amazon Web Services, Senior Security Consultant	



# The three pillars



The **technology** must support the **processes**  
supporting the **people** achieving their goals.

# High impact – low effort

## Demo time!

- Software Compositions checks (and Tracking)
- Statics application security testing (code and Infrastructure-as-Code)
- Dynamic application security testing (K8s)
- Cloud Management Interfaces
- Tying it all together!

```
tlk@development:~/Desktop/source_code/files-defect-dojo$ trivy image ubuntu:latest
2024-11-05T10:59:22.864+0100      INFO   Detected OS: ubuntu
2024-11-05T10:59:22.864+0100      INFO   Detecting Ubuntu vulnerabilities...
2024-11-05T10:59:22.881+0100      INFO   Number of language-specific files: 0

ubuntu:latest (ubuntu 22.04)

Total: 109 (UNKNOWN: 0, LOW: 53, MEDIUM: 54, HIGH: 2, CRITICAL: 0)
```

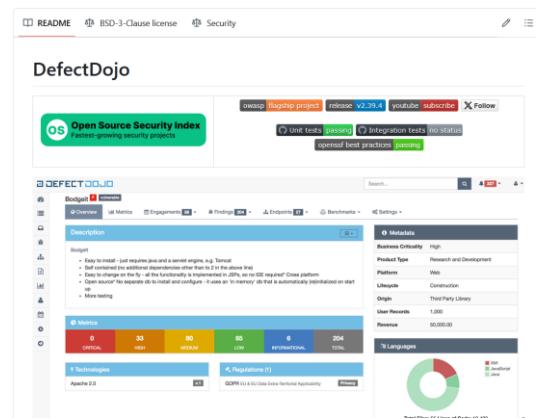


<https://github.com/prowler-cloud/prowler>

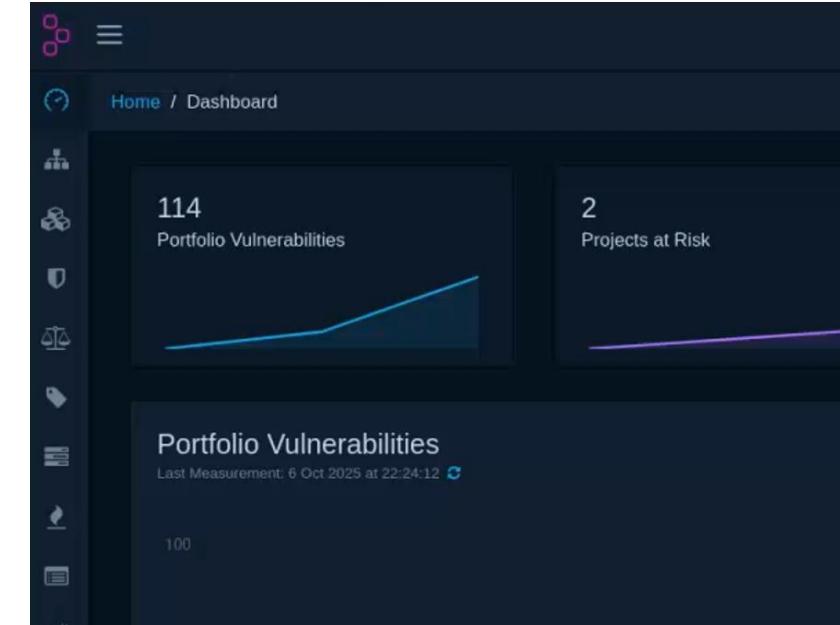
```
ubuntu:latest (ubuntu 24.04)

Total: 19 (UNKNOWN: 0, LOW: 7, MEDIUM: 12, HIGH: 0, CRITICAL: 0)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version
coreutils	CVE-2016-2781	LOW	9.4-3ubuntu6	
dpkg	CVE-2025-6297		1.22.6ubuntu6.1	1.22.6ubuntu6.5



<https://github.com/DefectDojo/django-DefectDojo>



<https://dependencytrack.org/>

Software  
Composition  
Analysis (SCA)

or

Software Bill of  
Material (SBOM)





tlk@development:~/demo\$

tlk@development:~/demo



# trivy image ubuntu:latest



tlk@development:~/demo\$

tlk@development:~/demo



trivy image alpine:latest



tlk@development:~/demo\$

tlk@development:~/demo



```
trivy image mcr.microsoft.com/dotnet/runtime:8.0
```

Activities

Terminal

6 Oct 22:00 •

✖ 🔍 🔍

tlk@development: ~/Desktop/source\_code/juice-shop

🔍 ⚙️

tlk@development: ~/Desktop/source\_code/juice-shop\$ █

cyclonedx-npm



Home / Dashboard

**114**  
Portfolio Vulnerabilities

A blue line chart showing the trend of portfolio vulnerabilities over time.

**2**  
Projects at Risk

A purple line chart showing the trend of projects at risk over time.

**80**  
Vulnerable Components

A blue line chart showing the trend of vulnerable components over time.

**596**  
Inherited Risk Score

A red line chart showing the trend of inherited risk score over time.

## Portfolio Vulnerabilities

Last Measurement: 6 Oct 2025 at 22:24:12

100

0

2 Apr 2025

12 Aug 2025

1 Sep 2025

6 Oct 2025



# Static Application Security Testing

Activities

Terminal

6 Oct 22:03 •

✖ 🔍 🔍

tlk@development: ~/Desktop/source\_code/juice-shop

tlk@development:~/Desktop/source\_code/juice-shop\$ █

semgrep . -- config auto

Activities

Terminal

6 Oct 22:07 •

✖ 🔍 🔍

tlk@development: ~/Desktop/source\_code/aws-cloudformation-templates/EKS



**tlk@development:~/Desktop/source\_code/aws-cloudformation-templates/EKS\$**

semgrep . -- config auto

# Dynamic “Application” Security Testing



Activities

Terminal

6 Oct 10:31 •

tlk@development: ~/demo

☰ 🔍 ⌂ ✕

tlk@development:~/demo\$ █

prowler aws

# Kube-Bench

The screenshot shows a AWS CloudShell interface with the region set to eu-central-1. The user has run the command `kubectl apply -f https://raw.githubusercontent.com/aquasecurity/kube-bench/main/job-eks.yaml`. The output of this command is displayed in a large central pane:

```
~ $ kubectl logs kube-bench-2wpd4
[INFO] 2 Control Plane Configuration
[INFO] 2.1 Logging
[WARN] 2.1.1 Enable audit Logs (Automated)

== Remediations controlplane ==
2.1.1 audit test did not run: No tests defined

== Summary controlplane ==
0 checks PASS
0 checks FAIL

== Summary total ==
12 checks PASS
1 checks FAIL
33 checks WARN
0 checks INFO
```

Below the main output pane, there is a smaller feedback pane with the text "Feedback".

# Tying all together



Platform ▾ Pricing ▾ Open-Source ▾ Resources ▾ Company ▾ Login 🗝 Book a Demo 📞

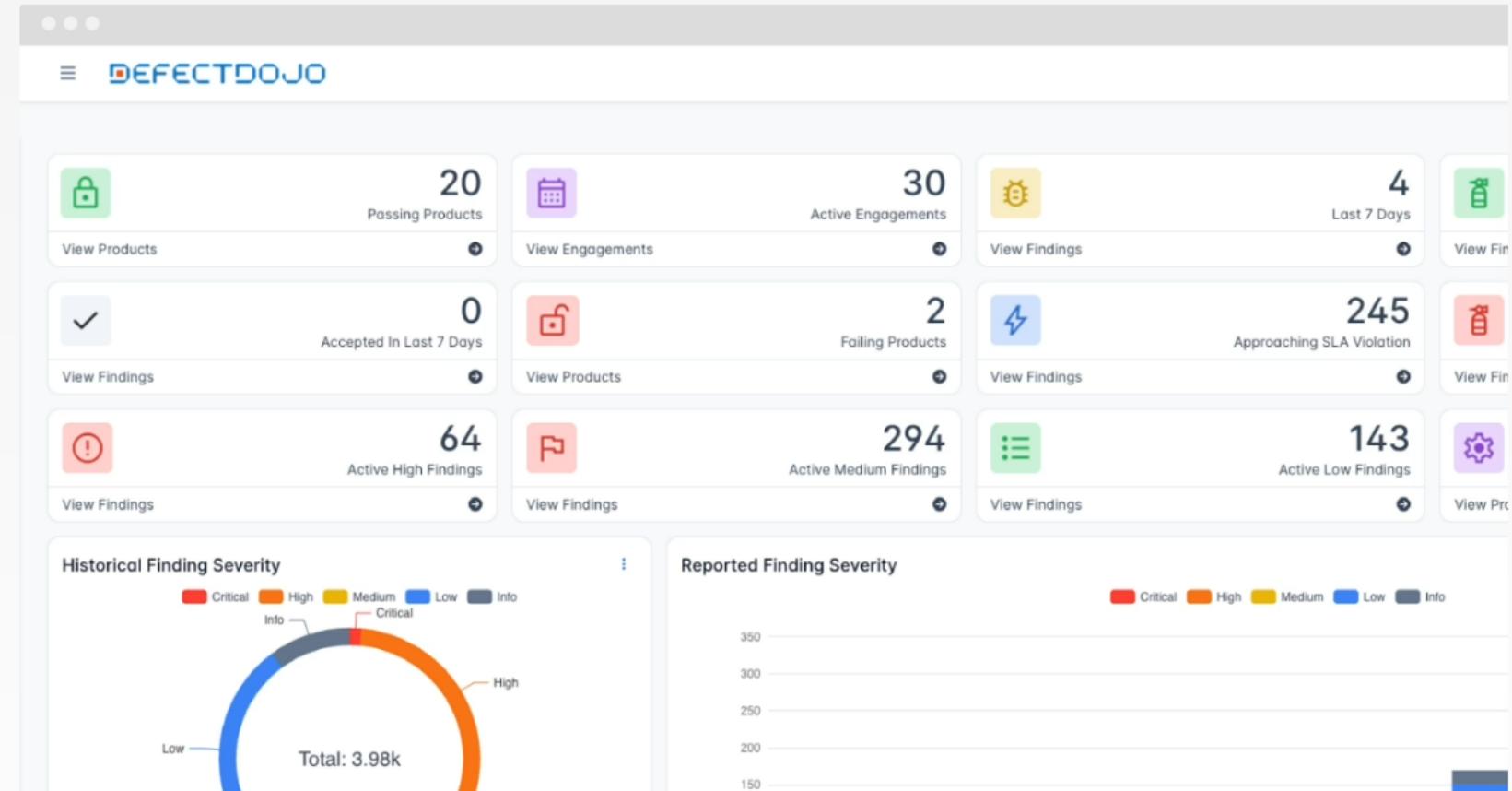
Platform

## Vulnerability Management that Works

Give your security team superpowers. Transform security into a business enabler, saving time and money while preventing potentially devastating breaches.

Get Started →

<https://defectdojo.com/>







**WelcomeSecurity**  
Security Sidekick to your Developers

# Thanks!

## Thomas Ljungberg Kristensen

[www.welcomesecurity.net](http://www.welcomesecurity.net)

+45 2158 1410

[thomas@welcomesecurity.net](mailto:thomas@welcomesecurity.net)

