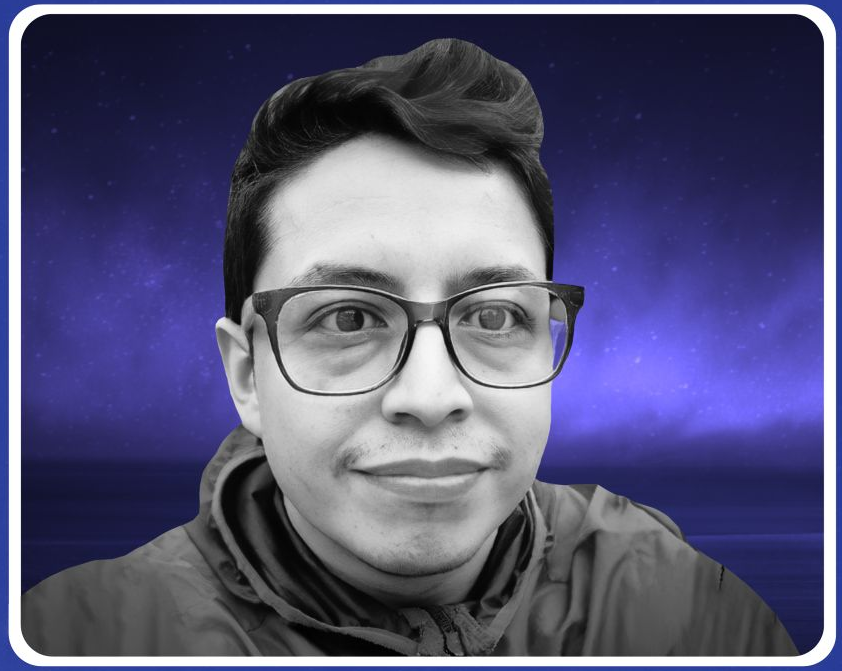
Jhonnatan Gil Chaves

DevOps Engineer at Globant



DevSecOps: Adding security to development for reliable continuous delivery

Conf42 DevSecOps 2023

Thursday • November 30th • 5PM GMT

CONF42

DevSecOps: Adding security to development for reliable continuous delivery

Discover how to merge DevOps and security in your development process to achieve reliable continuous delivery and protect your applications from the latest threats. Define the best practices for secure development in this talk.

Who is JhonnyPong (Jhonnatan Gil)

Just a human who loves Linux, share knowledge and very passionate about tech in general especially with make more easy every life that needs deploy in local mode on prem or bare metal and any other environment

@jthan24

“Life is really simple, but we insist on making it complicated..”
Confucius

In this talk, we will explore container analysis tools and how they can help cybersecurity engineers enhance application security in a containerized environment. Processes within organizations can be complex and tedious, especially when it comes to ensuring application security.

We will address the benefits and challenges of using container image analysis tools to detect potential security vulnerabilities before deployment. We will discuss how these tools can help ensure that container images used in the continuous delivery process meet security and compliance requirements, and how they can be used to implement proactive security measures.

Furthermore, we will delve into how container analysis tools can improve visibility and control of security throughout the application lifecycle. We will discuss how these tools can be used to detect and remediate security vulnerabilities in real-time and how they can help address the challenges of identity and access management in a multi-container environment.

Agenda

- Containerized applications?
- How help on SDLC
- General Challenges
- Address on SDLC
- DEMO
- Conclusion

Containerized applications?

Containers

Application Fundamental

What it is

A container is a running process with reso
managed by a computer's operating syste
container process are packaged as a cont
adjacent to each other on the same machi
system prevents the separate container pr
each other. https

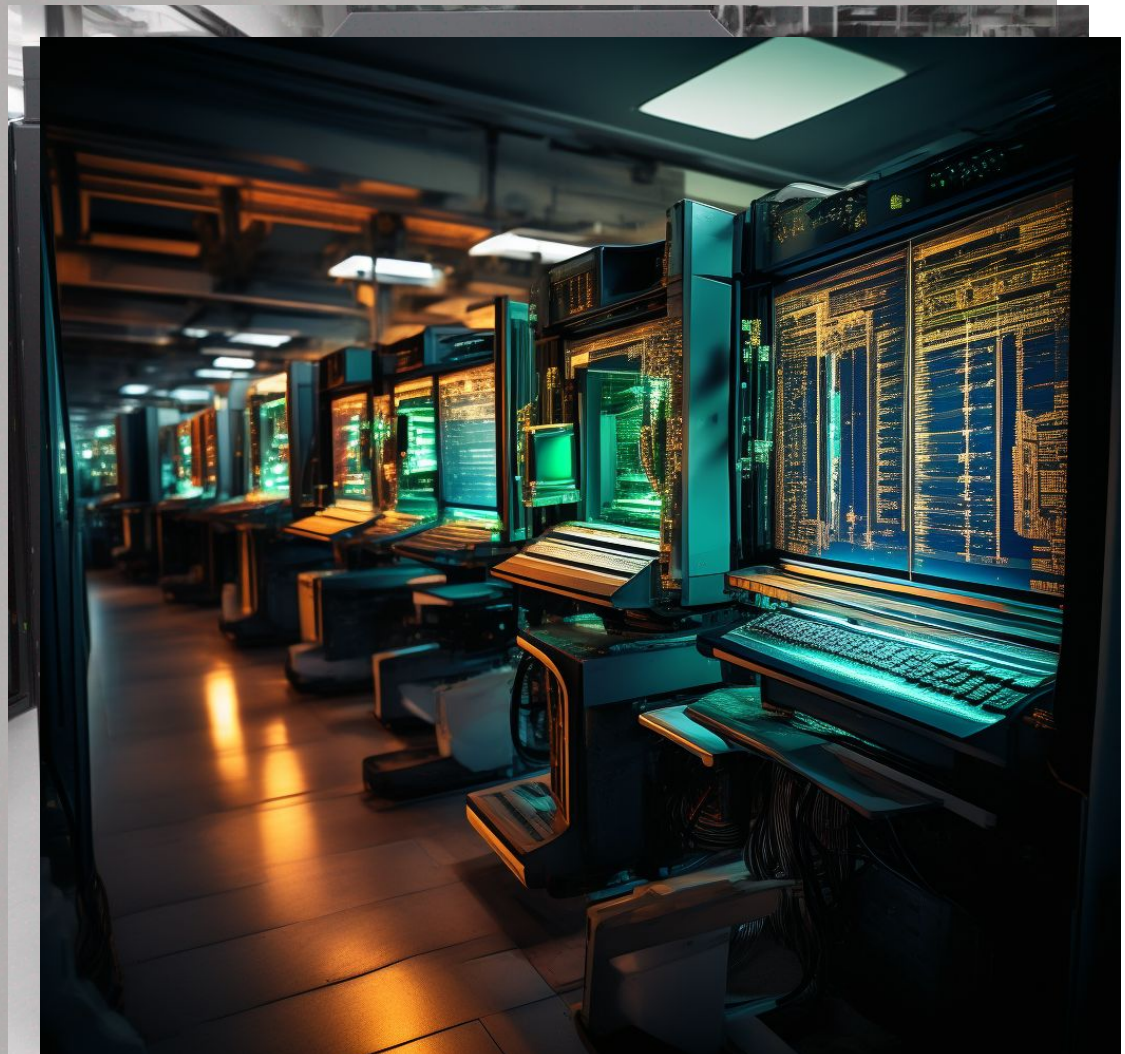
Containerization

Application

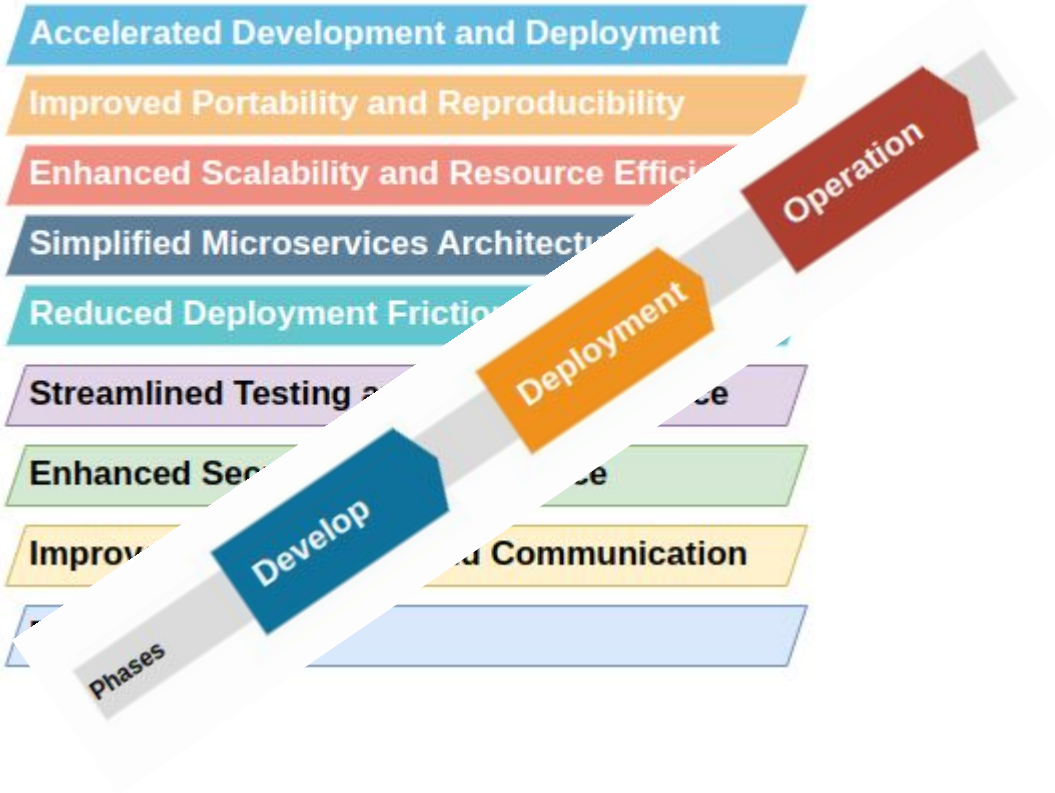
What it is

Containerization is the process of bundling an application and its dependencies into a container image. The container build process requires adherence to the **Open Container Initiative** (OCI) standard. As long as the output is a container image that adheres to this standard, which containerization tool is used doesn't matter.

https://glossary.cncf.io/containerization/



How help on SDLC



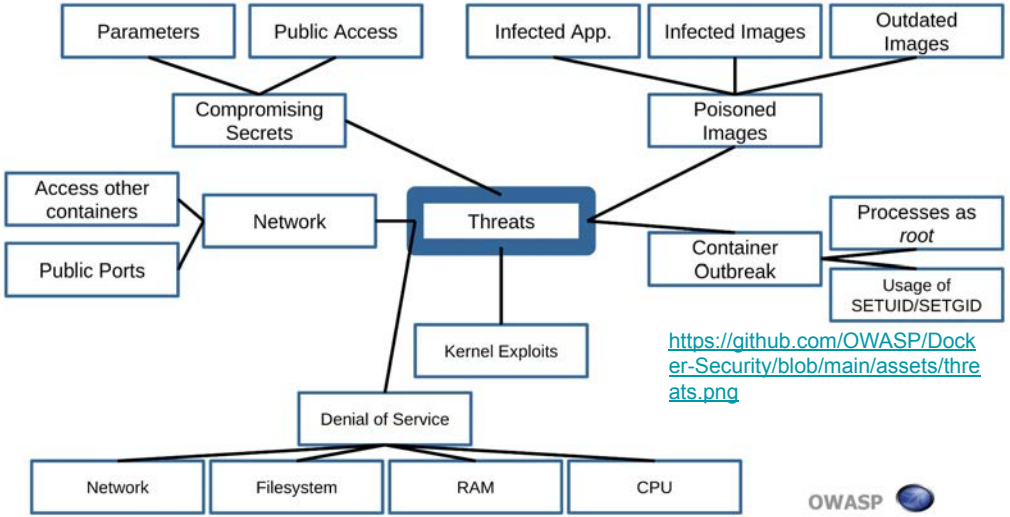
General challenges

Image Vulnerabilities

Misconfigurations

Supply Chain Attacks

Identity and Access Management



https://github.com/OWASP/Docker-Security/blob/main/assets/threats.png

Vulnerabilities

Misconfiguration

Chain Attacks

Identity and Access Mar

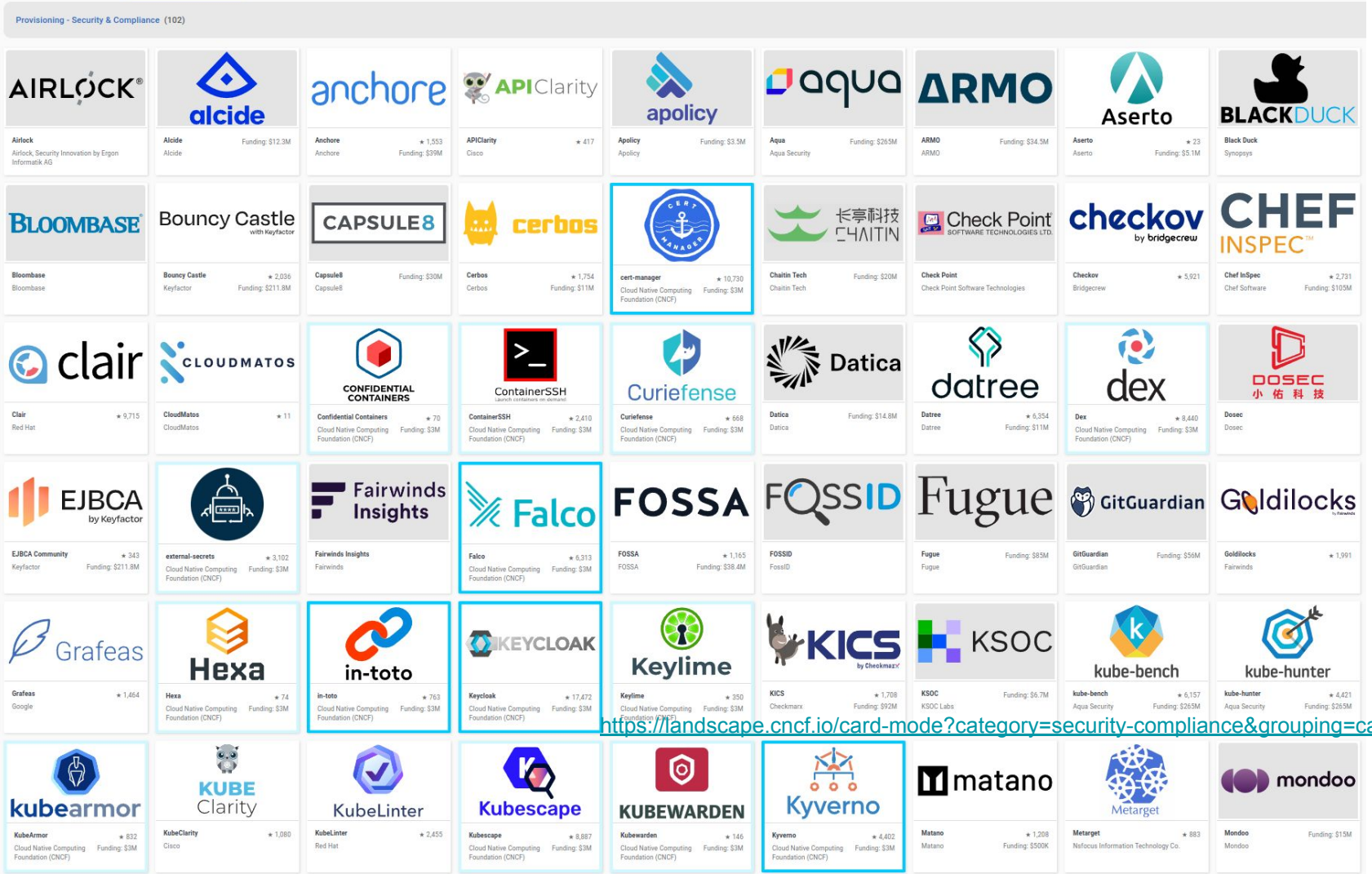
Address on SDLC

Vulnerability Detection

Misconfiguration Detection

Supply Chain Security

IAM Enforcement


Provisioning - Security & Compliance (102)
AIRLOCK
Airlock
Airlock, Security Innovation by Ergon Informatik AG
alcide
Alcide
Alcide
Funding: $12.3M
anchore
Anchore
Anchore
★ 1,553
Funding: $39M
APIClarity
APIClarity
Cisco
★ 417
apolicy
Apolicy
Apolicy
Funding: $3.5M
aqua
Aqua
Aqua Security
Funding: $265M
ARMO
ARMO
ARMO
Funding: $34.5M
Aserto
Aserto
Aserto
★ 23
Funding: $5.1M
BLACKDUCK
Black Duck
Synopsys
BLOOMBASE
Bloombase
Bloombase
Bouncy Castle
with Keyfactor
Bouncy Castle
Keyfactor
★ 2,036
Funding: $211.8M
CAPSULE8
Capsule8
Capsule8
Funding: $30M
cerbos
Cerbos
Cerbos
★ 1,754
Funding: $11M
CERT MANAGER
cert-manager
Cloud Native Computing Foundation (CNCF)
★ 10,730
Funding: $3M
卡亭科技
CHAITIN
Chaitin Tech
Chaitin Tech
Funding: $20M
Check Point
SOFTWARE TECHNOLOGIES LTD.
Check Point
Check Point Software Technologies
checkov
by bridgecrew
Checkov
Bridgecrew
★ 5,921
CHEF
INSPEC
Chef InSpec
Chef Software
★ 2,731
Funding: $105M
clair
Clair
Red Hat
★ 9,715
CLOUDMATOS
CloudMatos
CloudMatos
★ 11
CONFIDENTIAL CONTAINERS
Confidential Containers
Cloud Native Computing Foundation (CNCF)
★ 70
Funding: $3M
>_
ContainerSSH
Launch containers on demand
ContainerSSH
Cloud Native Computing Foundation (CNCF)
★ 2,410
Funding: $3M
Curiefense
Curiefense
Cloud Native Computing Foundation (CNCF)
★ 668
Funding: $3M
Datica
Datica
Datica
Funding: $14.8M
datree
Datree
Datree
★ 6,354
Funding: $11M
dex
Dex
Cloud Native Computing Foundation (CNCF)
★ 8,440
Funding: $3M
DOSEC
小佑科技
Dosec
Dosec
EJBCA
by Keyfactor
EJBCA Community
Keyfactor
★ 343
Funding: $211.8M
external-secrets
Cloud Native Computing Foundation (CNCF)
★ 3,102
Funding: $3M
Fairwinds
Insights
Fairwinds Insights
Fairwinds
Falco
Falco
Cloud Native Computing Foundation (CNCF)
★ 6,313
Funding: $3M
FOSSA
FOSSA
FOSSA
★ 1,165
Funding: $38.4M
FOSSID
FOSSID
FossID
Fugue
Fugue
Fugue
Funding: $85M
GitGuardian
GitGuardian
GitGuardian
Funding: $56M
Goldilocks
Goldilocks
Fairwinds
★ 1,991
Grafeas
Grafeas
Google
★ 1,464
Hexa
Hexa
Cloud Native Computing Foundation (CNCF)
★ 74
Funding: $3M
in-toto
in-toto
Cloud Native Computing Foundation (CNCF)
★ 763
Funding: $3M
KEYCLOAK
Keycloak
Cloud Native Computing Foundation (CNCF)
★ 17,472
Funding: $3M
Keylime
Keylime
Cloud Native Computing Foundation (CNCF)
★ 350
Funding: $3M
KICS
by Checkmarx
KICS
Checkmarx
★ 1,708
Funding: $92M
KSOC
KSOC
KSOC Labs
Funding: $6.7M
kube-bench
kube-bench
Aqua Security
★ 6,157
Funding: $265M
kube-hunter
kube-hunter
Aqua Security
★ 4,421
Funding: $265M
https://landscape.cncf.io/card-mode?category=security-compliance&grouping=category
kubearmor
KubeArmor
Cloud Native Computing Foundation (CNCF)
★ 832
Funding: $3M
KUBE
Clarity
KubeClarity
Cisco
★ 1,080
KubeLinter
KubeLinter
Red Hat
★ 2,455
Kubescape
Kubescape
Cloud Native Computing Foundation (CNCF)
★ 8,887
Funding: $3M
KUBEWARDEN
Kubewarden
Cloud Native Computing Foundation (CNCF)
★ 146
Funding: $3M
Kyverno
Kyverno
Cloud Native Computing Foundation (CNCF)
★ 4,402
Funding: $3M
matano
Matano
Matano
★ 1,208
Funding: $500K
Metarget
Metarget
Nsfocus Information Technology Co.
★ 883
mondoo
Mondoo
Mondoo
Funding: $15M

DEMO time

https://github.com/jthan24/conf42-2023devsecops

Don’t run this on production

Conclusion

- Continuous deployment reliable
- Our first steps for DevSecOps
- Generate commitment on our teams
- Start a security culture on our teams

Brief resume

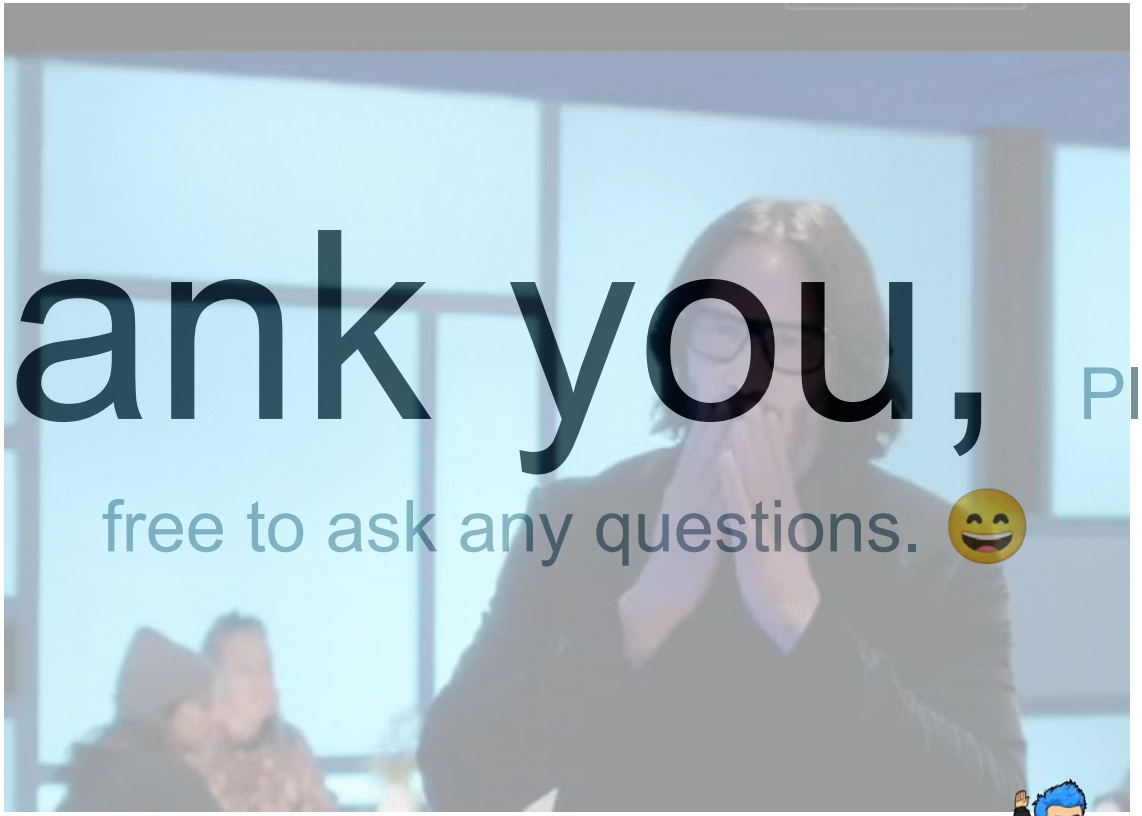
Containers, SDLC

- Containerized applications
- SDLC
- General Challenges
- Address on SDLC
- CNCF
- Open Source Tools

Survey time

Thank you,

Please feel free to ask any questions. 😄



@jthan24

http://thehive-project.org/

https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html

https://github.com/OWASP/Docker-Security/blob/main/001%20-%20Threats.md

https://owasp.org/www-chapter-dorset/assets/presentations/2020-07/Security-Of-Containers-Shruti-Kulkarni.pdf

https://owasp.org/www-project-docker-top-10/

https://aws.plainenglish.io/project-deploy-a-sample-app-on-aws-eks-devsecops-practices-961dd871c473

https://thehackernews.com/2023/11/cicd-risks-protecting-your-software.html?m=1

https://landscape.cncf.io/card-mode?category=security-compliance&grouping=category