



Microsoft Security
USER GROUP

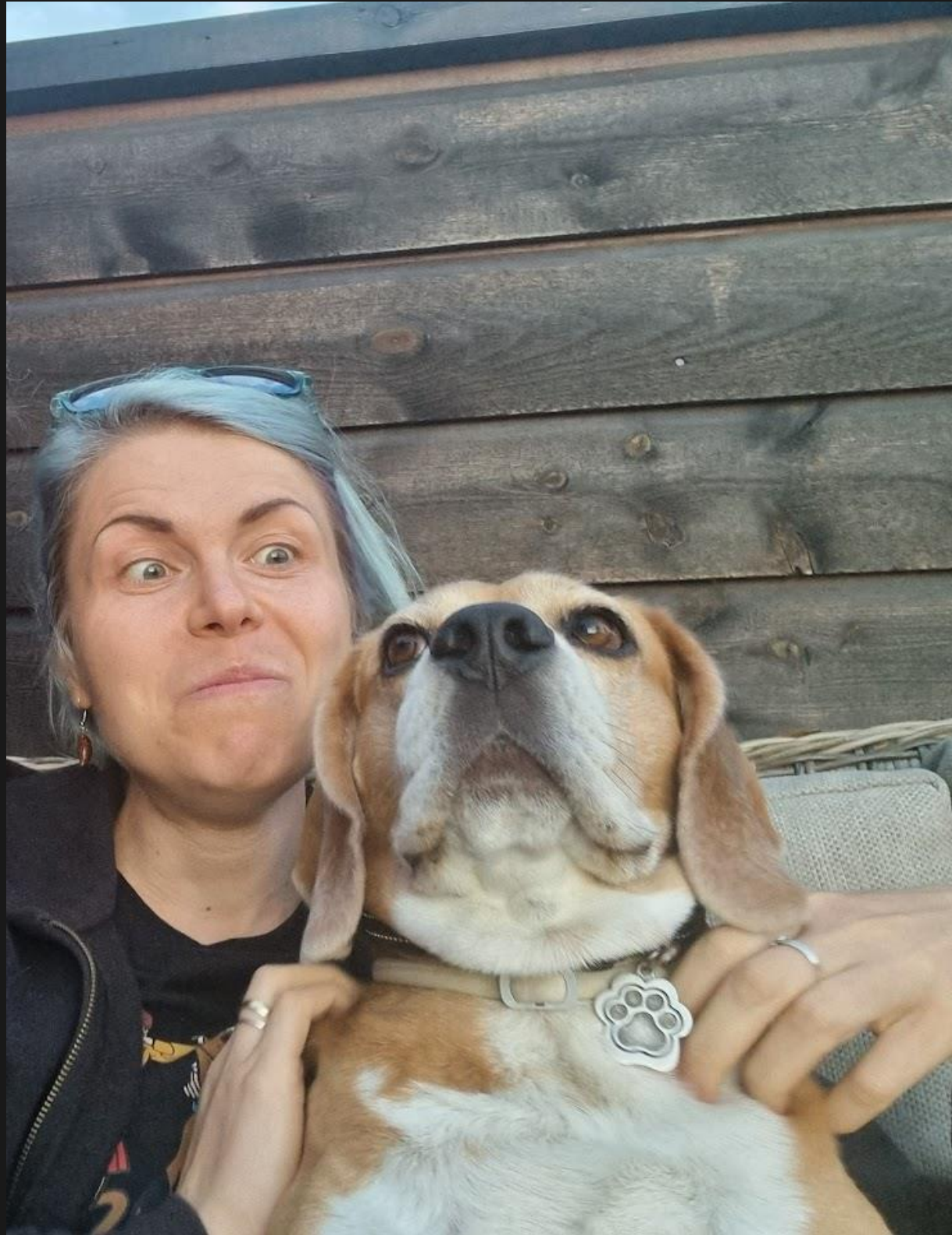
EXPLORING DEVSECOPS CONTROLS FOR AKS THROUGHOUT THE VALUE CHAIN

<https://kristhecodingunicorn.com>

Kristina Devochko
Software Architect



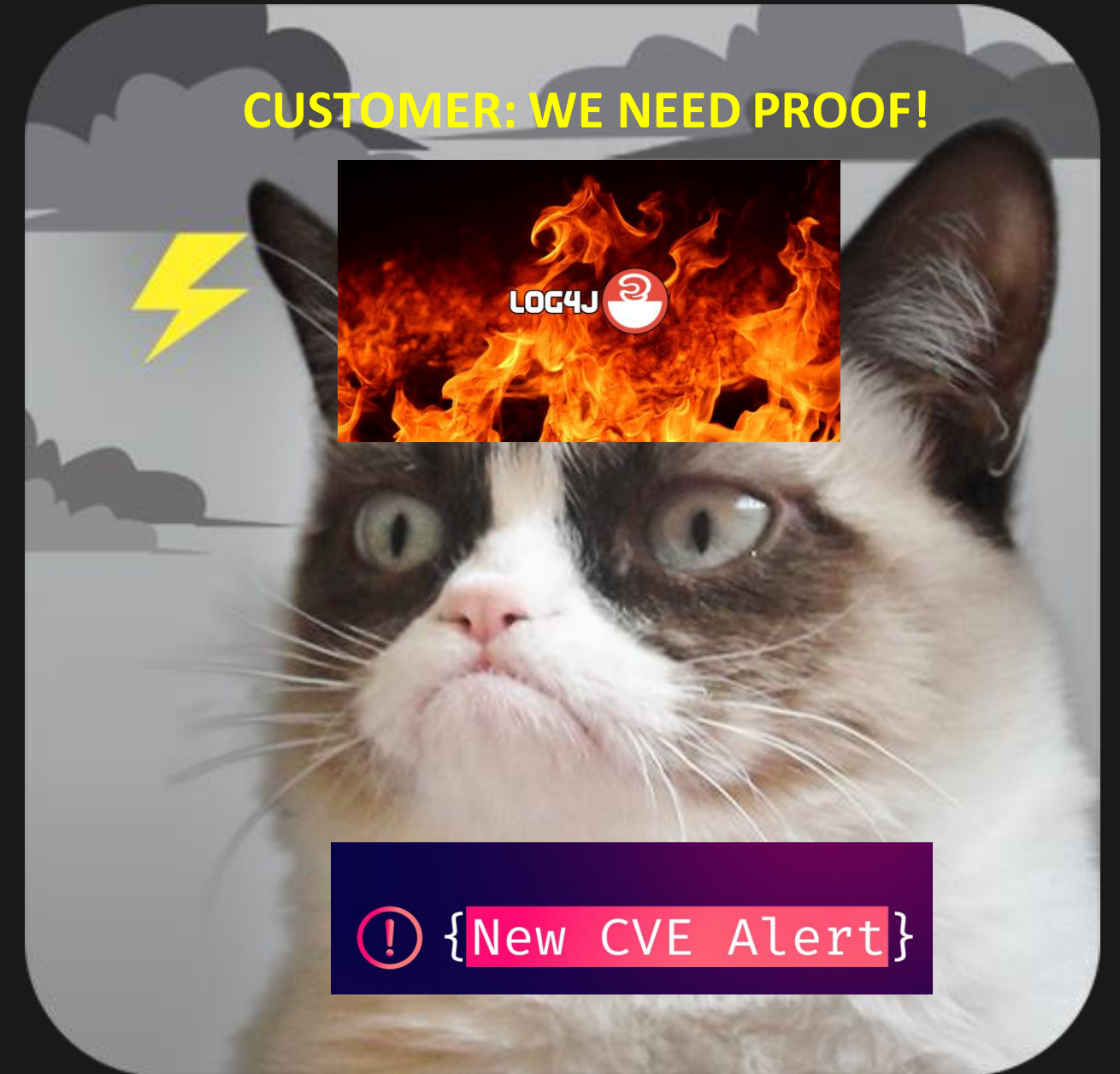
WHOAMI



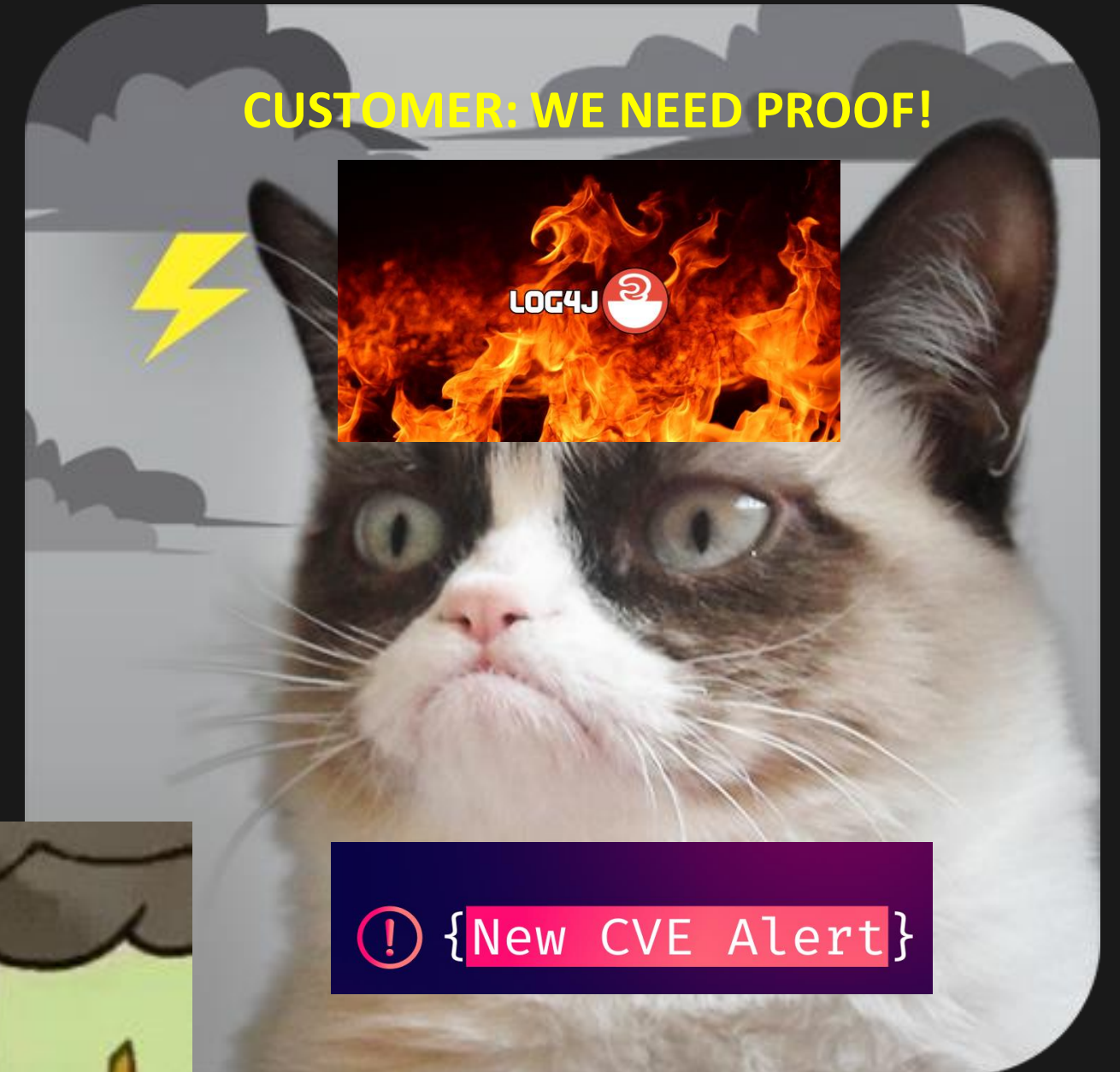
- Microsoft Azure MVP 🌩️
- Working as a Software Architect 🏗️
- Contributing back to the tech community as a tech blogger, community volunteer, speaker and open sourceress 🧑💻
- Focusing on Cloud Native application development, Secure and Sustainable Software Engineering and spreading love for cats 🐱
- Potterhead, Cat Mom of 3, Hiker, Puzzler, Retro Games Fan 🧩



A TALE OF NOT SECURING KUBERNETES...

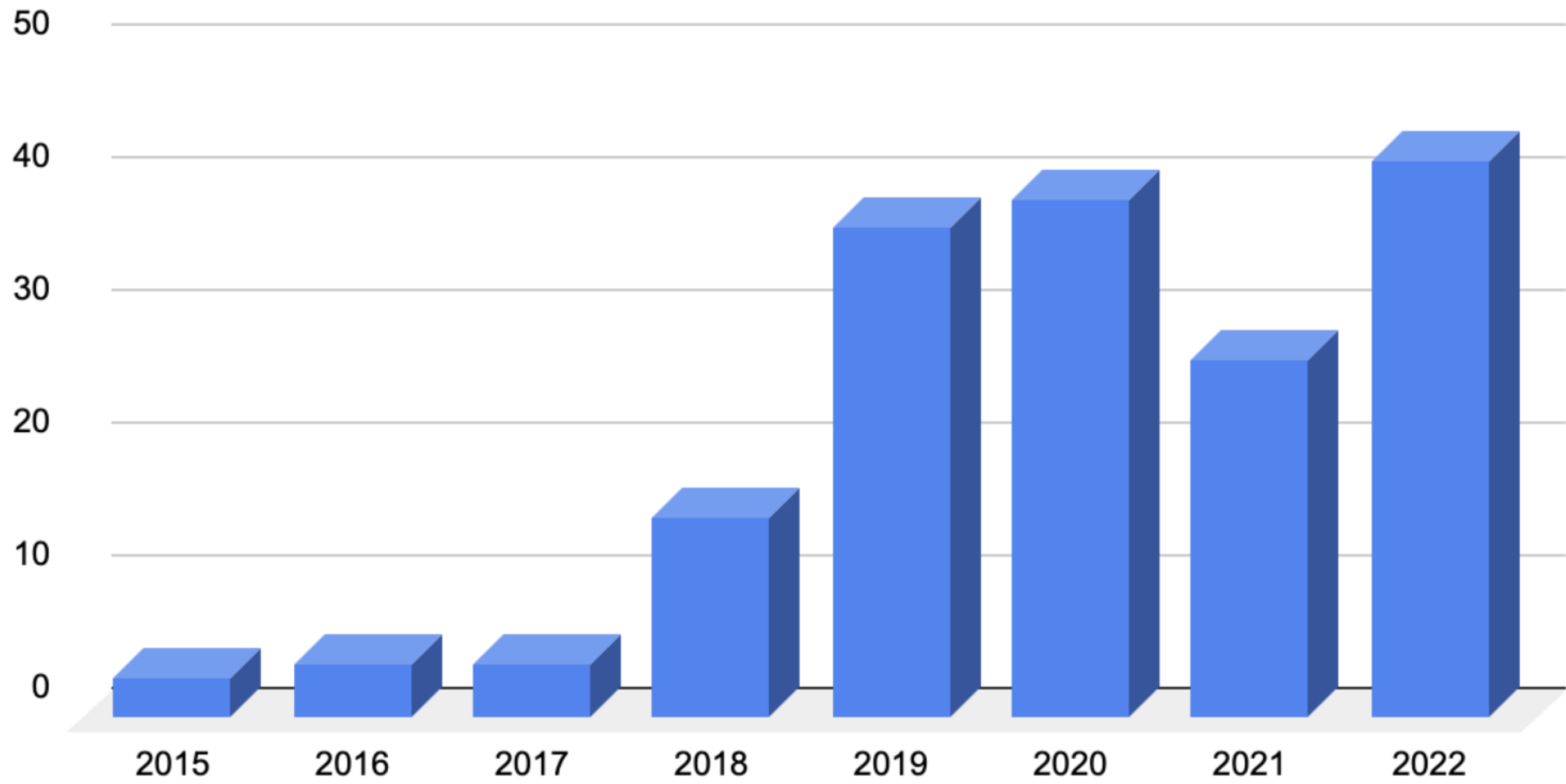


A TALE OF NOT SECURING KUBERNETES...



KUBERNETES IS SECURE BY DEFAULT

IT'S A TRAP!



Kubernetes' first major security hole discovered

There's now an invisible way to hack into the popular cloud container orchestration system Kubernetes.



Written by **Steven Vaughan-Nichols**, Senior Contributing Editor
on Dec. 3, 2018

CVE-2018-1002105 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

In all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade requests in the kube-apiserver allowed specially crafted requests to establish a connection through the Kubernetes API server to backend servers, then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection.

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



CNA: Kubernetes

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:

CVE-2018-1002105

NVD Published Date:

12/05/2018

NVD Last Modified:


06/28/2019

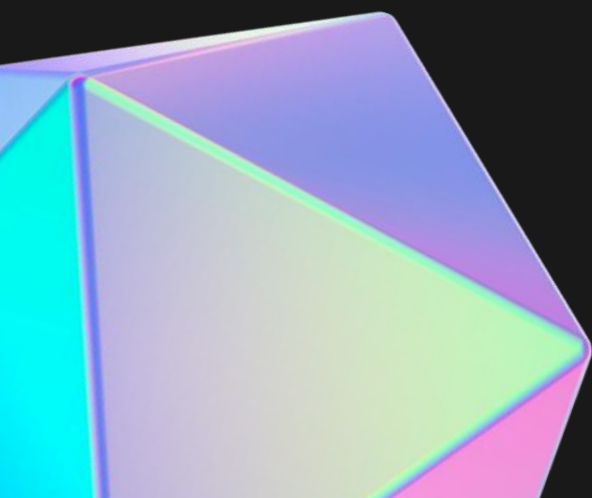
Source:

Kubernetes

Argo CD will trust invalid JWT claims if anonymous access is enabled

Critical jannfis published GHSA-r642-gv9p-2wjj on May 18


Package	Affected versions	Patched versions	Severity
 github.com/argoproj/argo-cd (Go)	1.4.0 through 2.1.14, 2.2.8, 2.3.3	2.3.4, 2.2.9, 2.1.15	Critical 10.0 / 10



CVE-2022-37968 Detail

Current Description

Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability.

 [Hide Analysis Description](#)

Analysis Description

Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



CNA: Microsoft Corporation

Base Score:

10.0 CRITICAL

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:

[CVE-2022-37968](#)

NVD Published Date:

10/11/2022

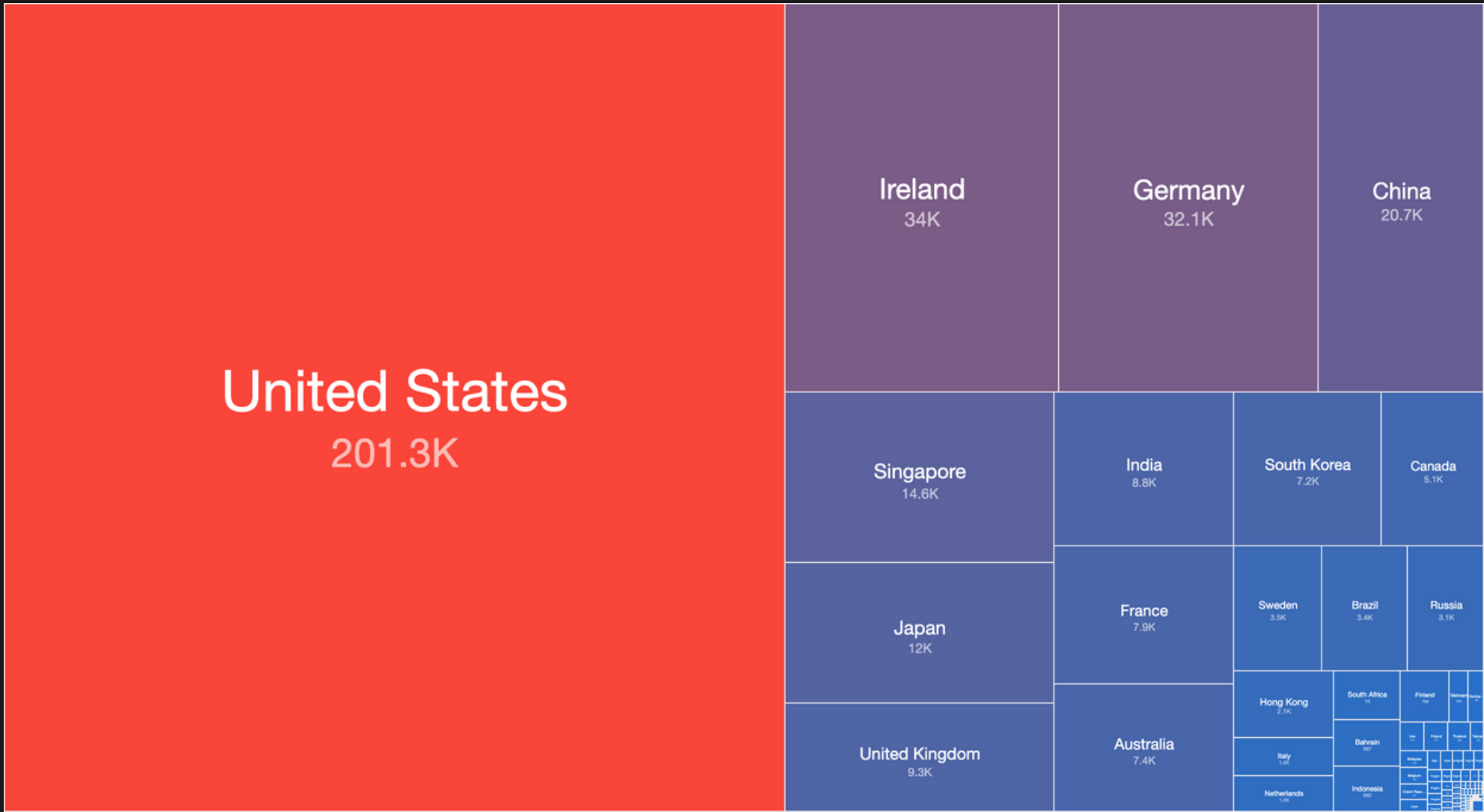
NVD Last Modified:

10/12/2022

Source:

Microsoft Corporation

- **May 2022:** SHADOWSERVER DISCOVERED OVER 380 000 OPEN KUBERNETES API SERVERS.
- **JUNE 2022:** CYBLE RESEARCH LABS OBSERVED OVER 900,000 KUBERNETES EXPOSURES.
- **OCTOBER 2022:** REDHUNT LABS UNCOVERED 574,913 MISCONFIGURED INTERNET-FACING K8S CORE COMPONENTS.



- CONTAINER IMAGES ARE RUNNING WITH ROOT USER BY DEFAULT.
- EXAMPLE: ASP.NET CORE, NGINX BASE IMAGES REQUIRE A ROOT USER TO RUN
- NOT ALL BASE IMAGES LET YOU SWITCH TO NON-ROOT USER THAT EASILY...

Pull requests92

Actions

Projects7

Wiki

Security8

Insights

Unable to start Kestrel. System.Net.Sockets.SocketException (13): Permission denied while running alpine as non root user #4699

Closedmuratg opened this issue on Oct 24, 2018 · 27 comments

muratg commented on Oct 24, 2018

Contributor

From @endejoli on Monday, 22 October 2018 19:03:34

Steps to reproduce the issue

1.Use the below Dockerfile to build image

```
FROM microsoft/dotnet:2.1-aspnetcore-runtime-alpine3.7
EXPOSE 5000
WORKDIR /app
COPY ./app/* /app/
RUN adduser -D buildadmin
RUN chown buildadmin:buildadmin /app /app/*
USER buildadmin
ENTRYPOINT ["dotnet", "Template.Sample.dll"]
```

2. Building and running the image gives below error

```
18:10:59 INF] Starting web host
[18:10:59 INF] User profile is available. Using '/home/buildadmin/.aspnet/DataProtection-Keys' as key repository
[18:10:59 INF] Creating key {c07b8334-0237-48ed-817e-9dc73382d0e} with creation date 2018-10-22 18:10:59Z, act
[18:10:59 WRN] No XML encryptor configured. Key {c07b8334-0237-48ed-817e-9dc73382d0e} may be persisted to stor
[18:10:59 INF] Writing data to file '/home/buildadmin/.aspnet/DataProtection-Keys/key-c07b8334-0237-48ed-817e-9
[18:10:59 FTL] Unable to start Kestrel.
System.Net.Sockets.SocketException (13): Permission denied
   at System.Net.Sockets.Socket.UpdateStatusAfterSocketErrorAndThrowException(SocketError error, String caller)
   at System.Net.Sockets.Socket.DoBind(EndPoint endPointSnapshot, SocketAddress socketAddress)
   at System.Net.Sockets.Socket.Bind(EndPoint localEP)
```

Assignees

No one assigned

Labels

area-runtimeinvestigateservers-kestrel

Projects

No one yet

Milestone

Discussions

Development

No branches or pull requests

Notifications

Subscribe

You're not receiving notifications from this thread.

15 participants

- MULTI-LA
- AUTOMA
- POLICY C



Code

Scan via



COLLABORATION CULTURE

It's a better way to stay on top of what's happening.

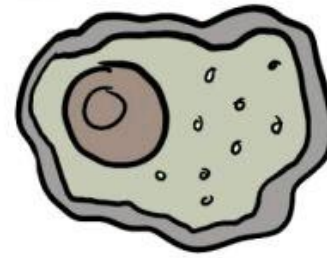
ule checking



me
rity

EVOLUTION OF OPERATIONS

OPS



- PRIMORDIAL, PROTOZOIC
- BORN IN THE SWAMPS OF PERL
- OPERATES IN A SINGLE-CELL SILO
- SURPRISINGLY RESILIENT

DEVOPS



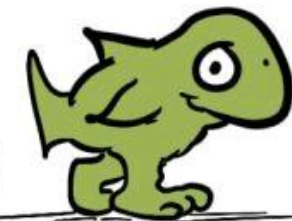
- A CROSS-FUNCTIONAL MARVEL
- VASTLY INCREASED AGILITY
- SECRETLY JUST A BUNCH OF SINGLE CELLS THAT HAVE LEARNED NOT TO KILL EACH OTHER

DEVSECOPS



- MORE ADVANCED, MORE PARANOID
- SECURITY IS AUTOMATED RIGHT INTO ITS DNA
- KNOWS THAT SHARED RESPONSIBILITY IS THE ONLY ESCAPE FROM FOSSILIZATION

DEVSECMLOPS



- WHAT EVEN IS THIS?
- IS IT A FISH WITH FEET?
- WE SHOULD PROBABLY LEAVE IT ALONE FOR A FEW MILLION YEARS AND SEE WHAT HAPPENS

TRICERATOPS



- DOES NOT CARE ABOUT YOUR ORG STRUCTURE
- VULNERABLE ONLY TO DIRECT METEOR STRIKES
- WHAT WERE WE TALKING ABOUT, AGAIN?

@acloudguru



Plan and Develop

- ☐ Threat modelling
- ☐ IDE Security plugins
- ☐ Pre-commit hooks
- ☐ Secure coding standards
- ☐ Peer review

Commit the code

- ☐ Static application security testing
- ☐ Security unit and functional tests
- ☐ Dependency management
- ☐ Secure pipelines

Build and test

- ☐ Dynamic application security testing
- ☐ Cloud configuration validation
- ☐ Infrastructure scanning
- ☐ Security acceptance testing

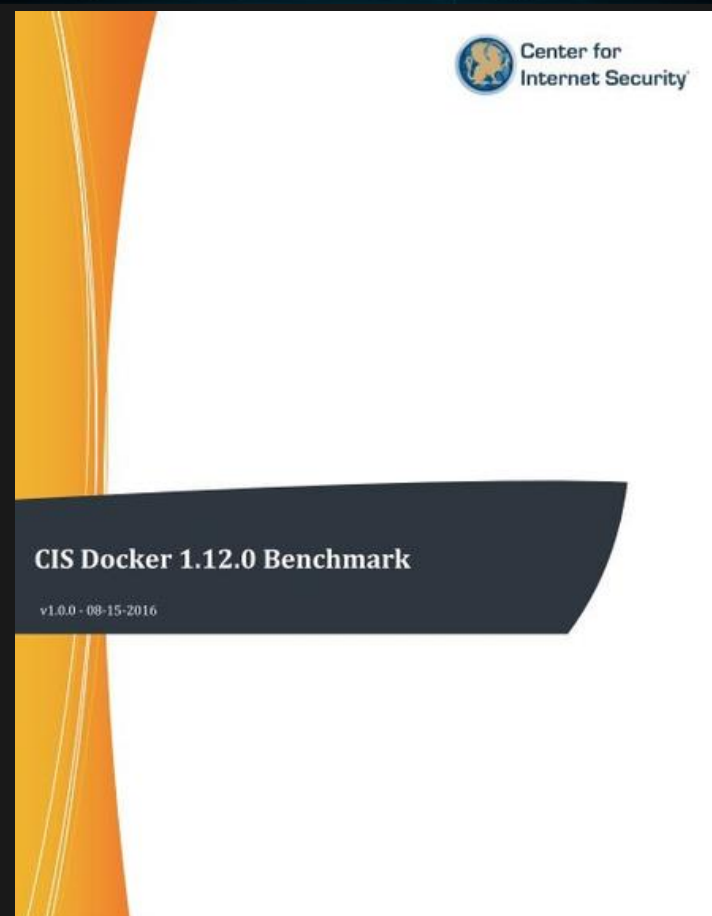
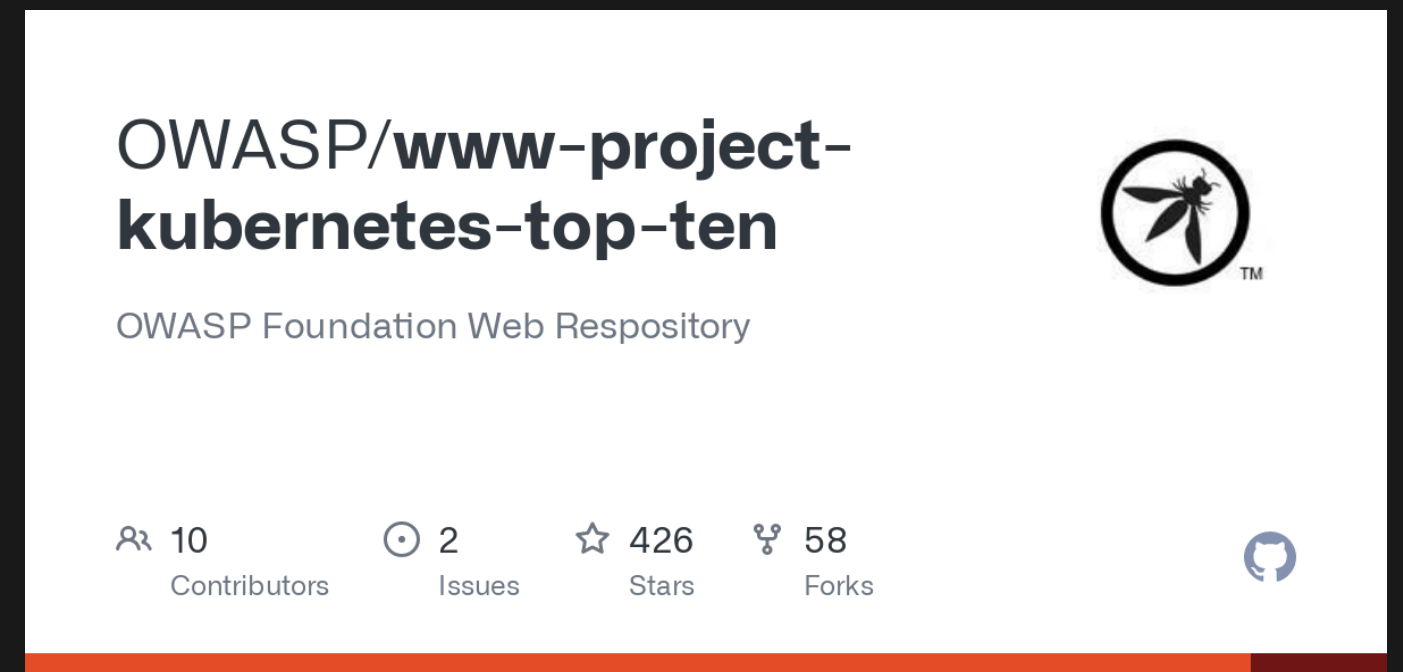
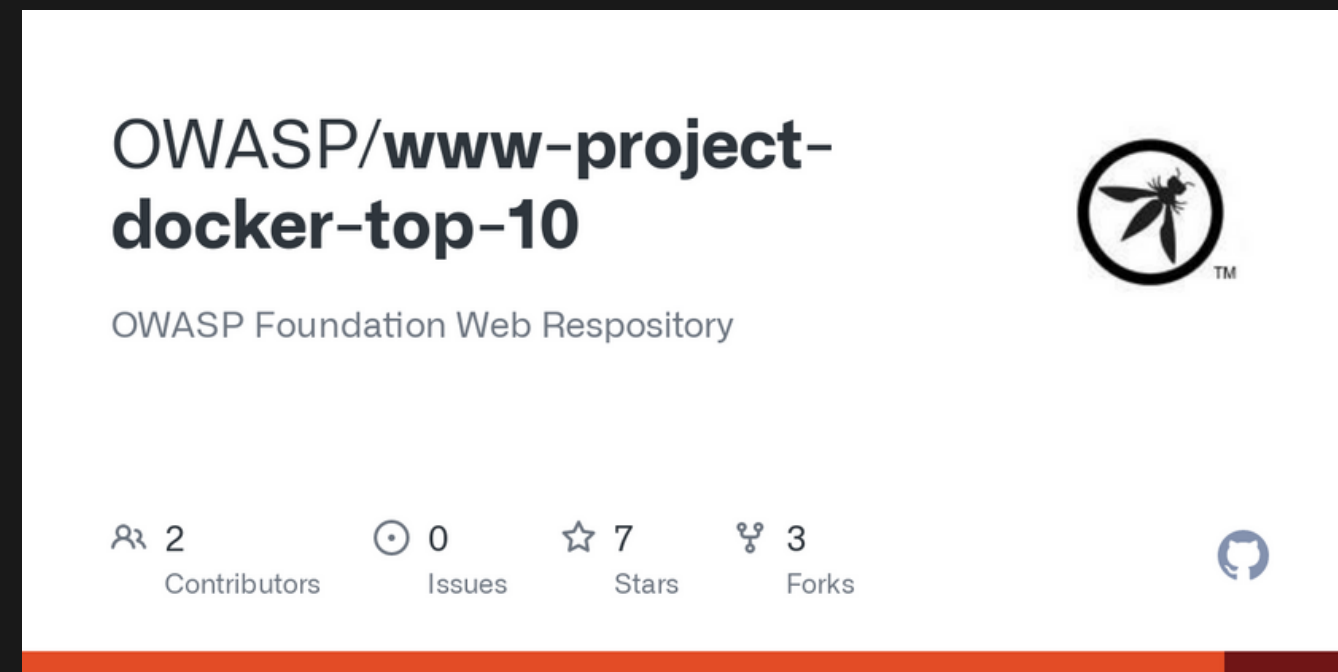
Go to production

- ☐ Security smoke tests
- ☐ Configuration checks
- ☐ Live Site Penetration testing

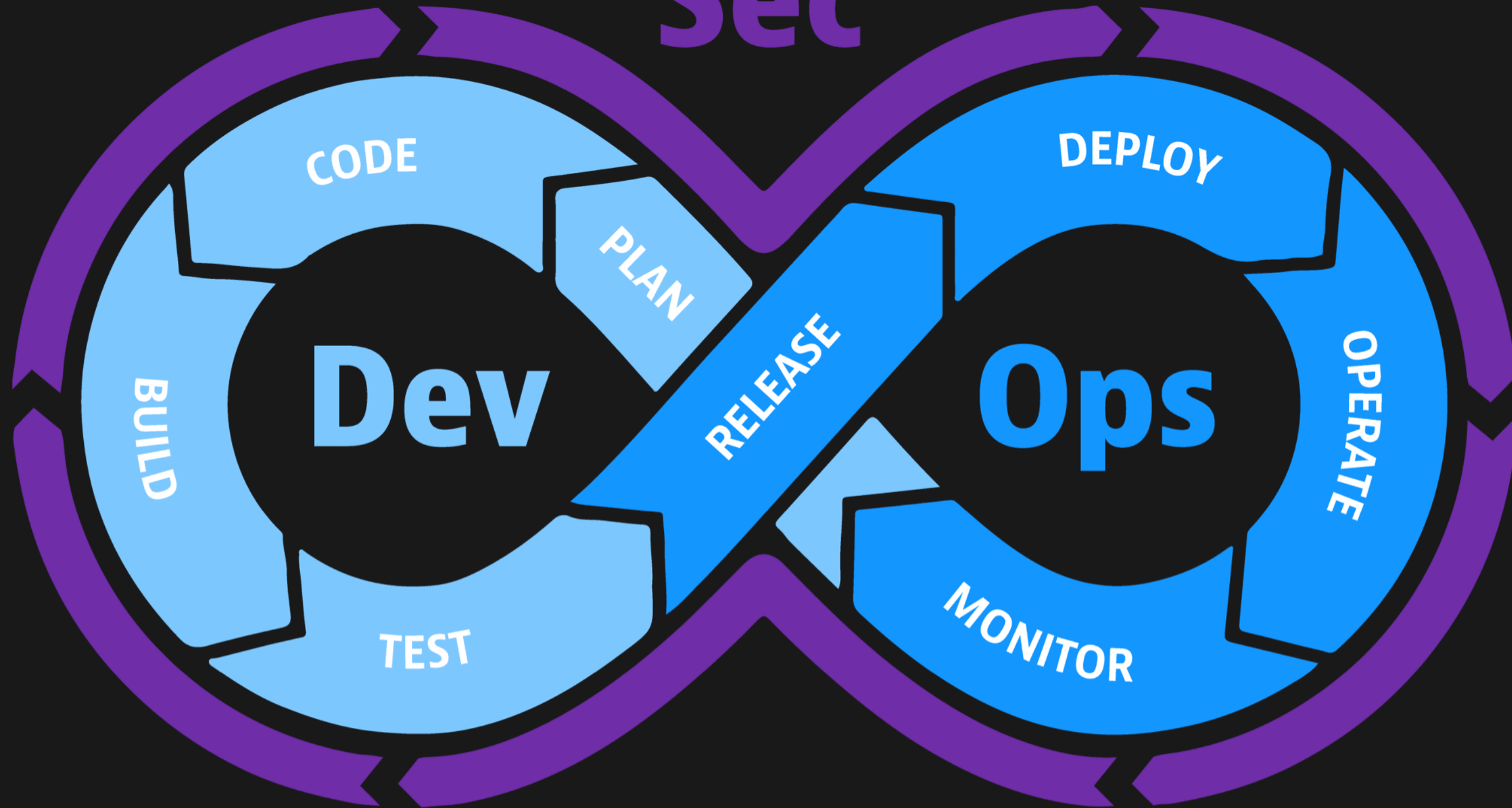
Operate

- ☐ Continuous monitoring
- ☐ Threat intelligence
- ☐ Penetration testing
- ☐ Blameless postmortems

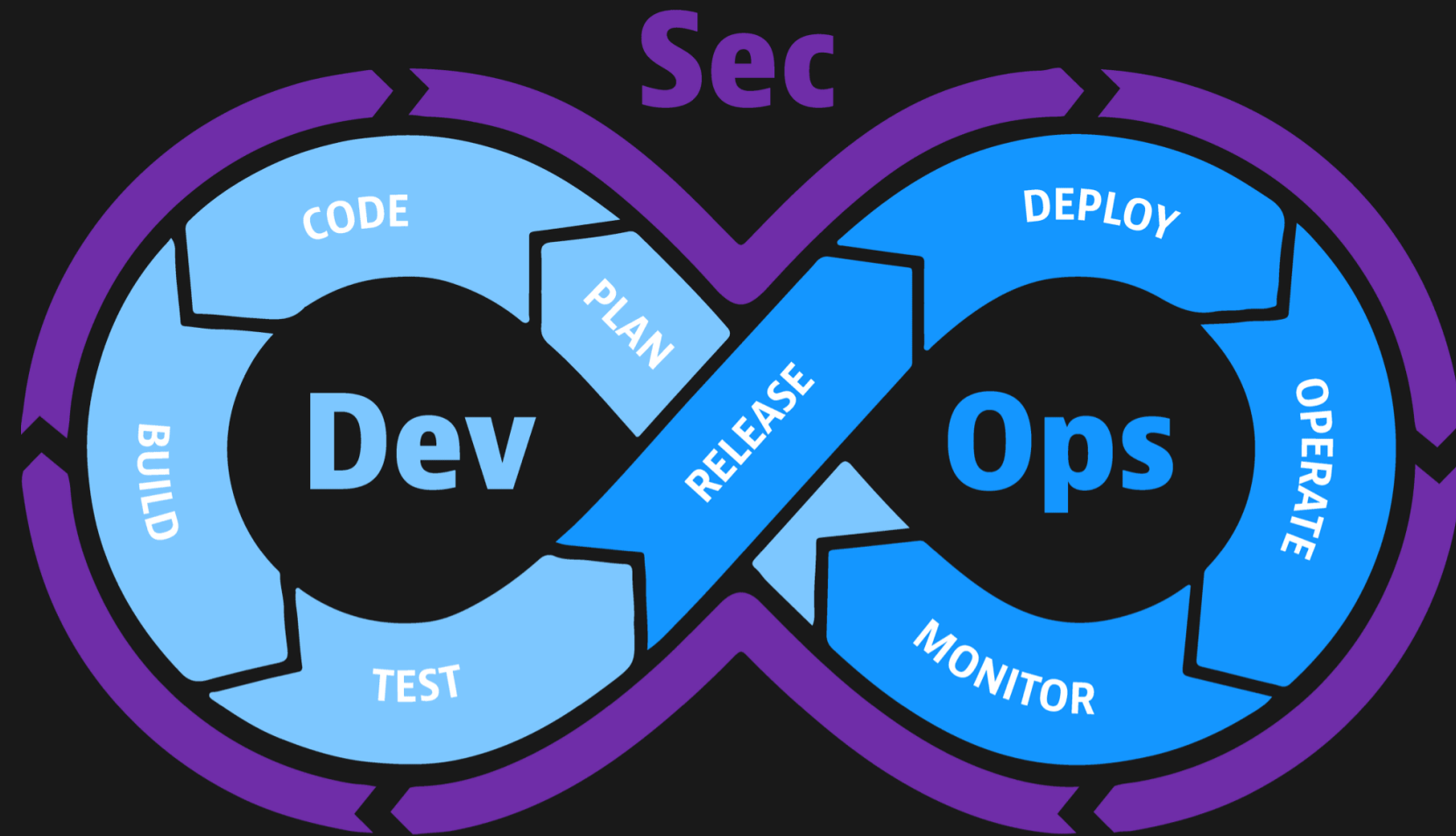
- **DAILY ROUTINE:** A CUP OF COFFEE AND MORNING READ ON SECURITY FRAMEWORKS AND STANDARDS 😊
- CUSTOMERS WILL REQUIRE PROOF SOONER OR LATER.



Sec

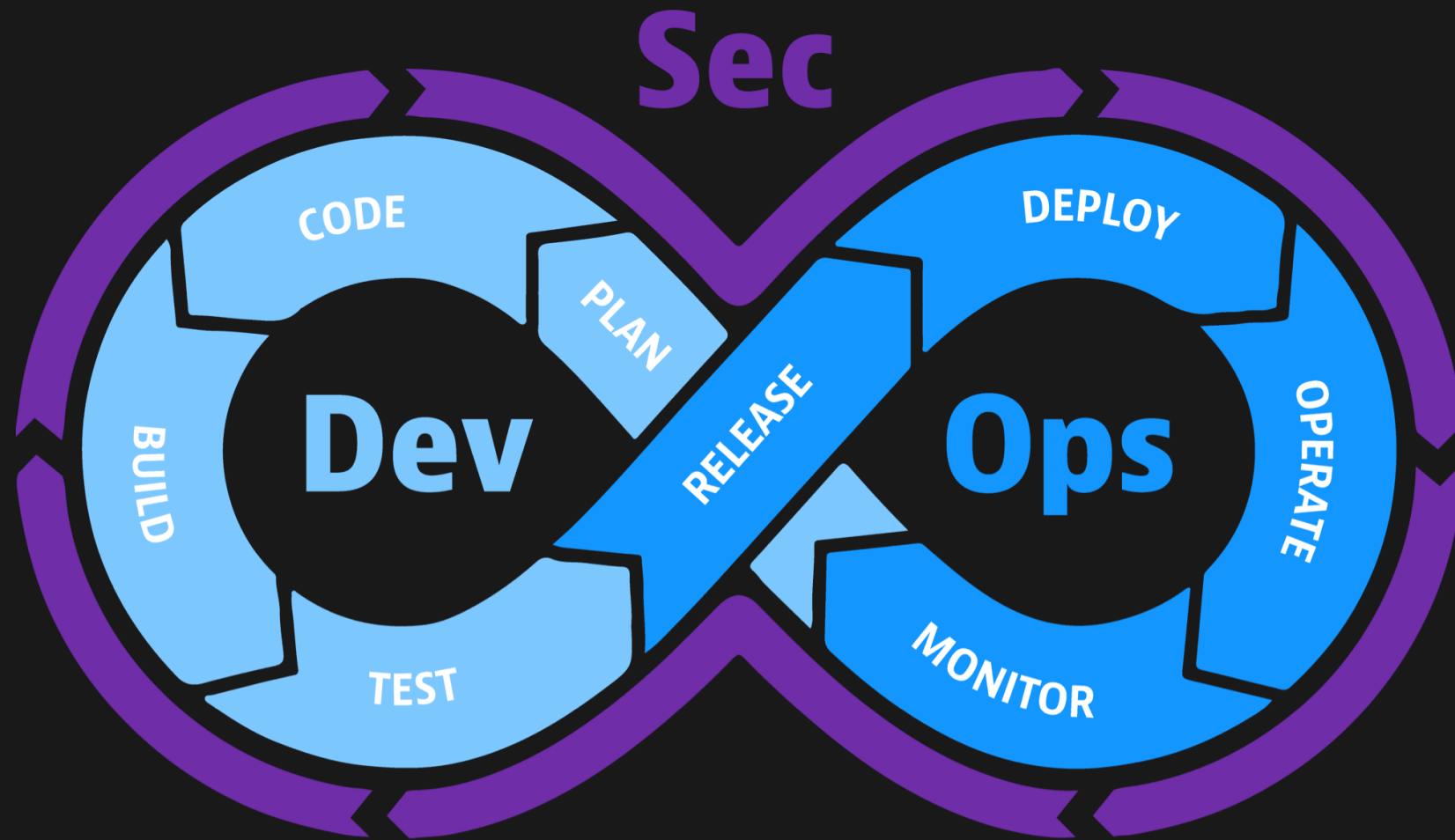


Plan && Code



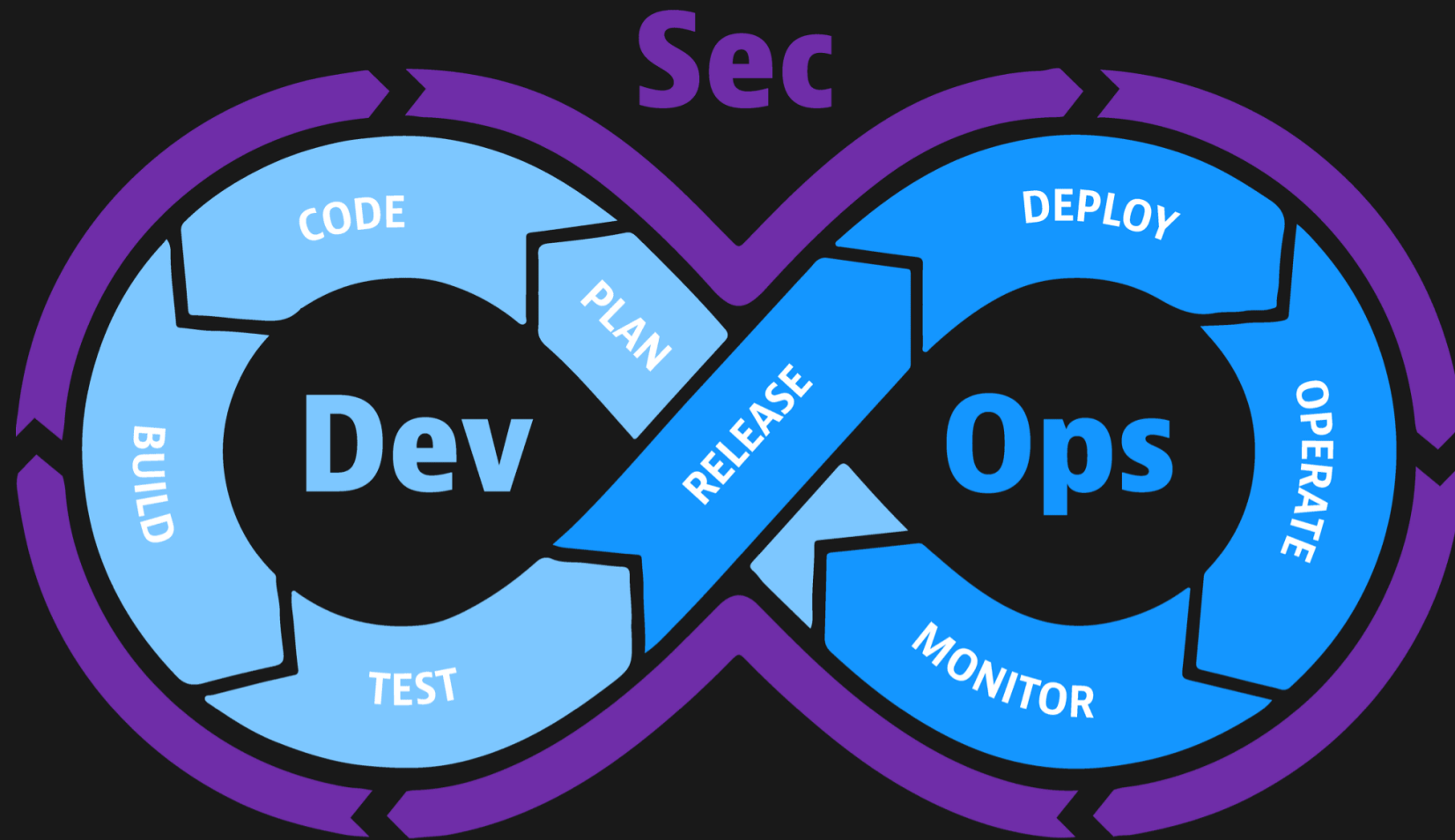
- Day Zero adoption stage
- Risk Assessment
- Threat Modeling (MTMT, OWASP Threat Dragon)
- Application and IaC scan/lint IDE plugins (Pluto, Hadolint, KubeLinter, tfscan, Trivy, Snyk, Checkov++)
- Blueprints, review checklists, abstraction

Build && Test



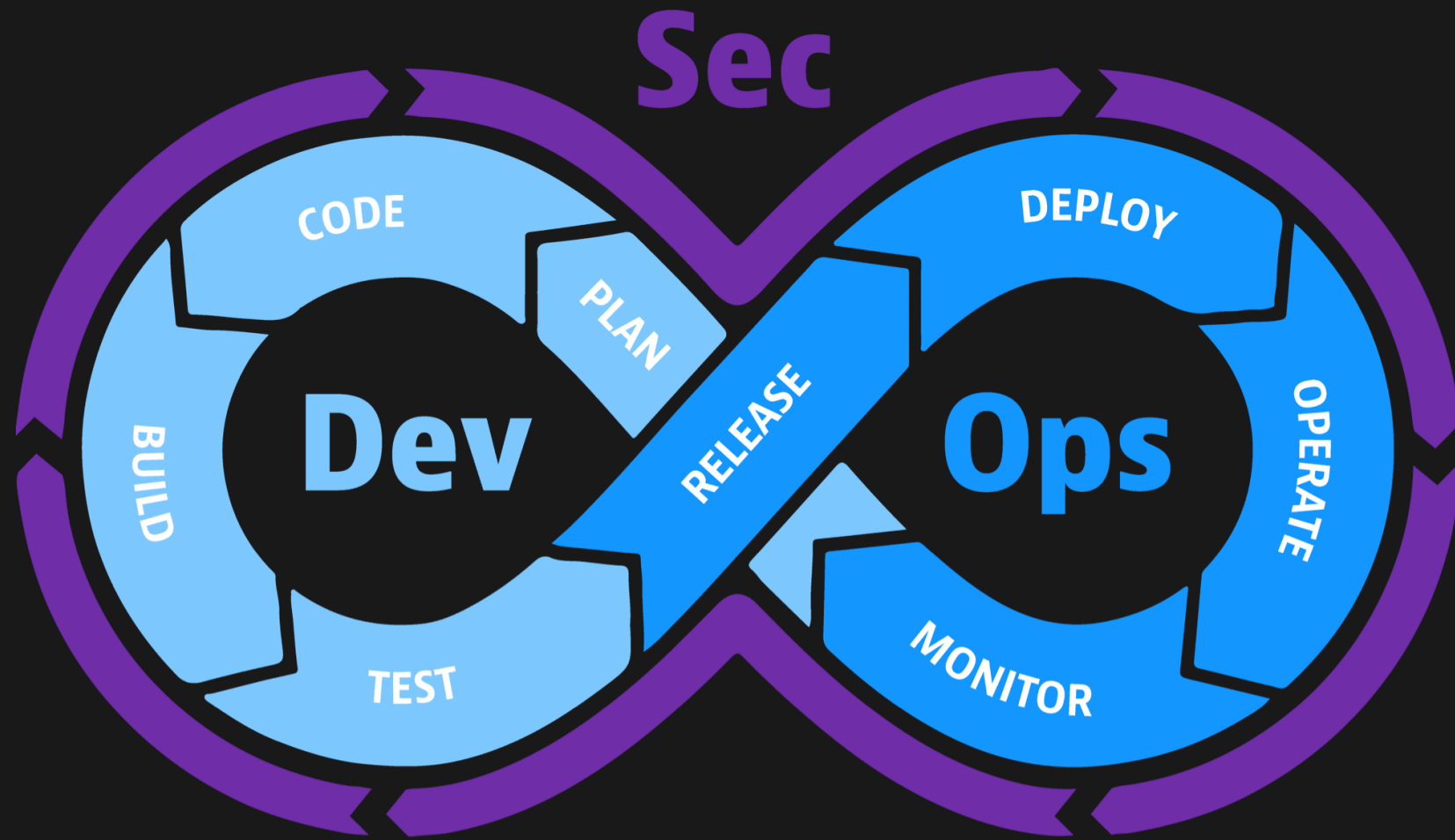
- Automated app and IaC scans
- Supply chain security controls (dependency scanning, SBOM)
- Private container registry (ACR)

Release && Deploy



- Governance (Azure Policy)
- Private cluster/IP ranges
- Network policies
- mTLS
- Kubernetes Security Context
- Secrets management
- IAM && Least privilege principle (AAD Auth + RBAC)

Operate && Monitor



- Cluster, node, container image upgrade
- Azure Monitor
- Microsoft Defender and Azure Advisor
- Microsoft Sentinel
- Backup
- Penetration testing

Sec

Communication and Awareness



DID I HEAR DEMO?



OHMAGIF.COM



SUMMING IT UP...




Kubernetes is NOT secure by default!

Utilize existing frameworks and baselines – not only for compliance but as a cheat sheet.

Communication and education of the teams is crucial.

Automate, Automate, Automate. Also for security.





Scheduling & Orchestration

Coordination & Service Discovery

Remote Proc



Cloud Native Storage



Automation & Configuration

Container Registr



CLOUD NATIVE Landscape

CLOUD NATIVE COMPUTING FOUNDATION



l.cncf.io

This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

Special



BOO!



BOO!



CNCF Landscape!



BOO!



AHHHH!!!



Observability and Analysis

Monitoring



Logging



Tracing



Chaos Engineering



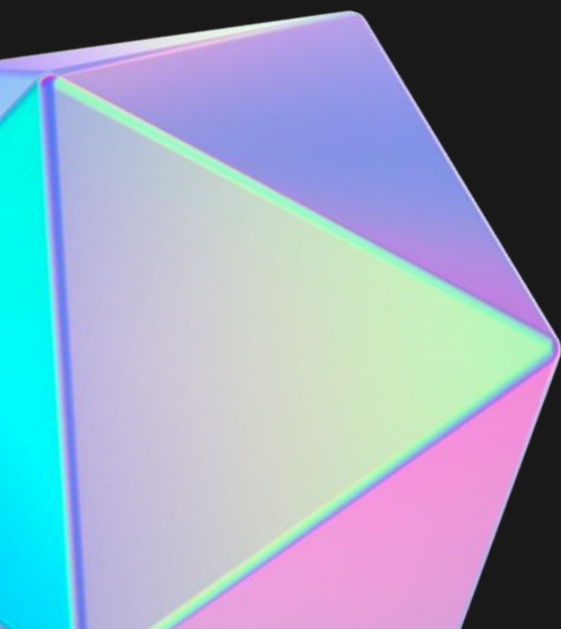
**NOW WITNESS THE POWER OF THIS
FULLY OPERATIONAL**



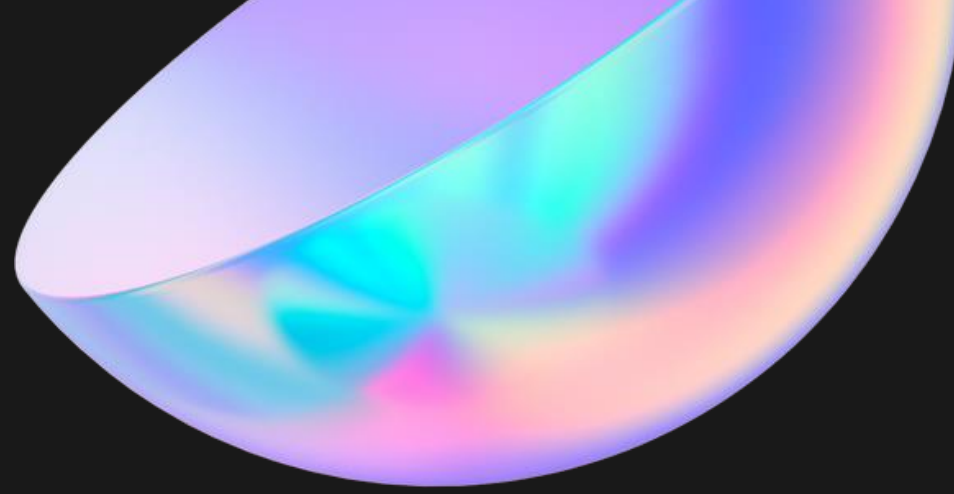
SECURED

KUBERNETES CLUSTER

memegenerator.net



THANK YOU!



SCAN ME

Questions? Let's connect! 🐾

- Tech Blog: <https://kristhecodingunicorn.com>
- LinkedIn: <https://www.linkedin.com/in/krisde>
- Twitter: [@kristhecodingu1](https://twitter.com/kristhecodingu1)
- GitHub: [@guidemetothemoon](https://github.com/guidemetothemoon)

