SANS CLOUD SECURITY

Container Security 101

Jon Zeolla

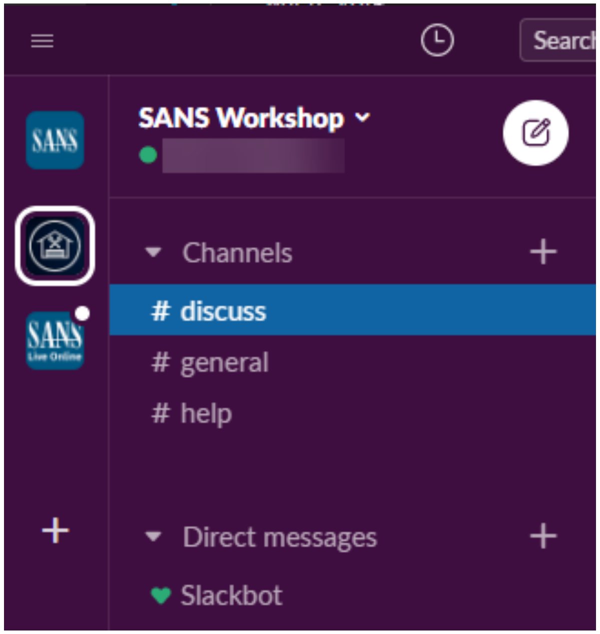
2023-04-27 WORKSHOP

Jon Zeolla

- Co-Founder and CTO at SEISO
- SANS SEC540 – Cloud Security and DevSecOps Automation Instructor
- Helping Software companies with Cloud Native Security & Compliance
- Based in Pittsburgh, PA
- BSides Pittsburgh, Steel City InfoSec, PittSec
- Recipient of the 2021 Start-Up Innovator of the Year

Using Slack for SANS Workshops

- **Join our Workshop Slack workspace from the following link:**
  - https://sansurl.com/sans-workshop
- **Register with any email address you can access**
  - It does not need to be a "work" or SANS portal address
- **Once you click on the confirmation email, you'll be prompted to provide a name & password**
- **Once in Slack, keep an eye out in the #general channel for announcements. We are using #discuss & #help for our main collaboration channels. See you there!**



SANS | CLOUD SECURITY

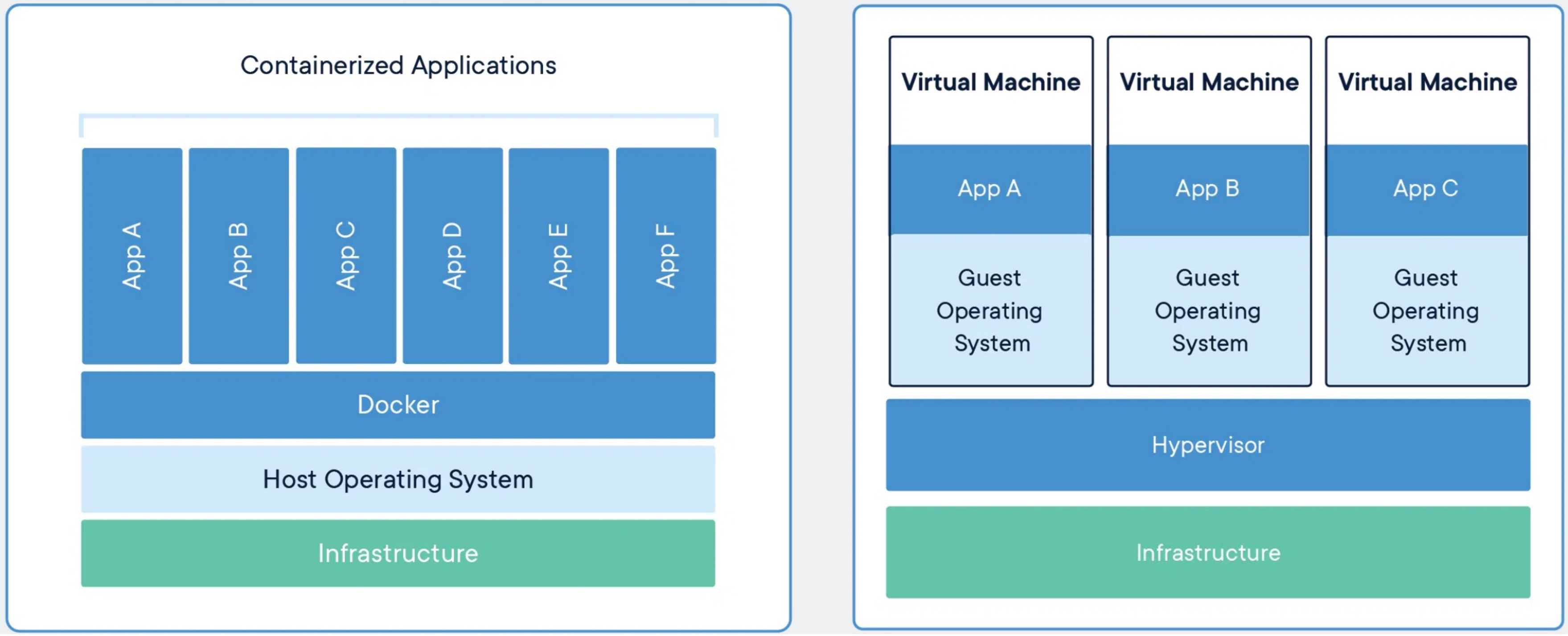
Why use Containers?

Why Containers?

- **Horizontal scaling** – application components scale independently (microservices)
- **Containers are Portable** – deployment and rollback simplified, dependencies are self-contained
- **Resource Isolation** – processes share the same resource pool, but with limits
- **Very Efficient** – less overhead than Virtual Machines
- **Supported by Automation tools and Cloud Providers**
- **Enables use of modern toolsets**
- **Improved consistency** between developer laptops, test, and production

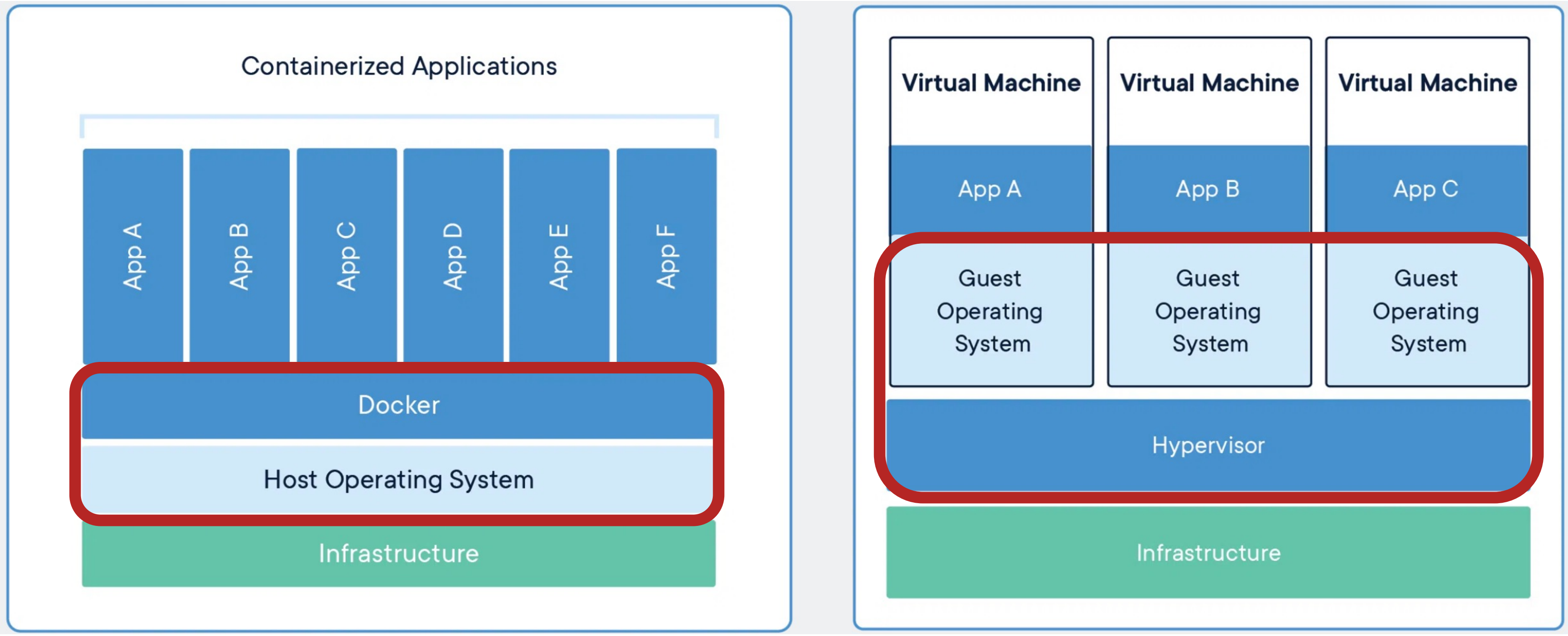
What are Containers?

Containers vs Virtual Machines



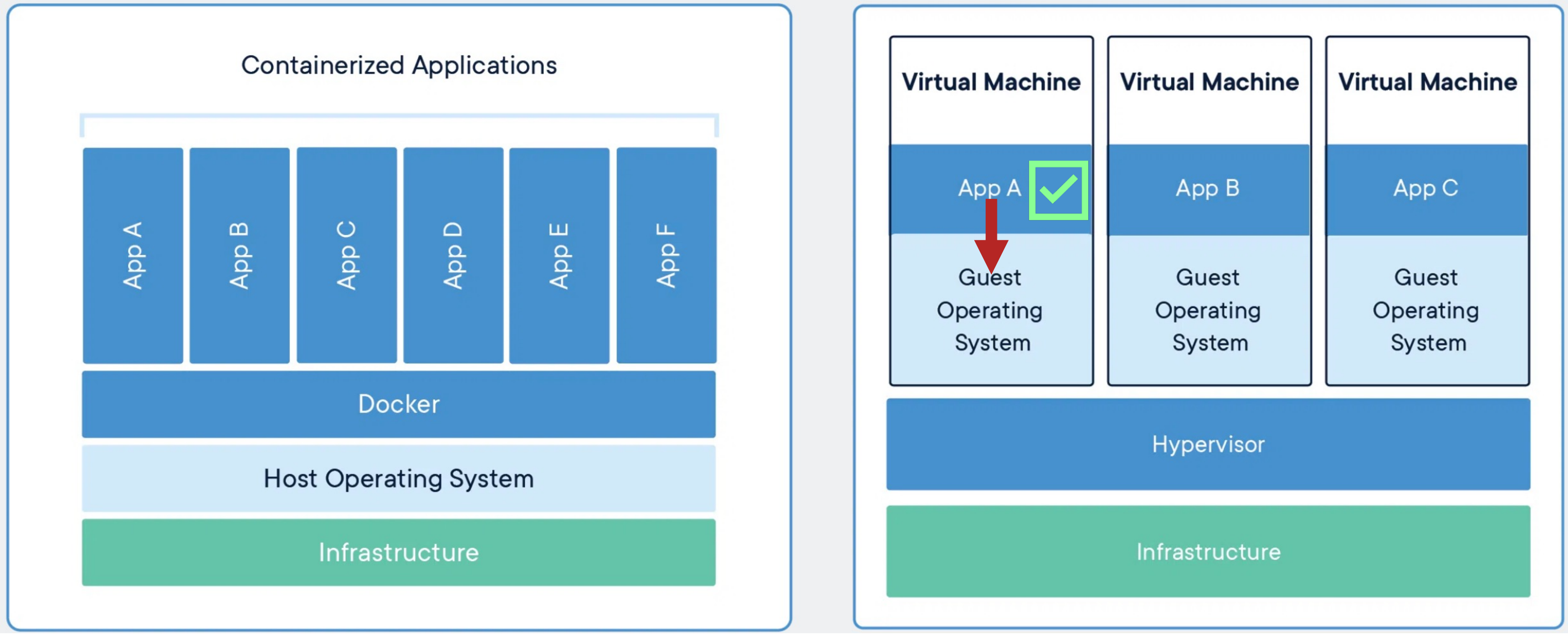
https://www.docker.com/resources/what-container

Containers vs Virtual Machines



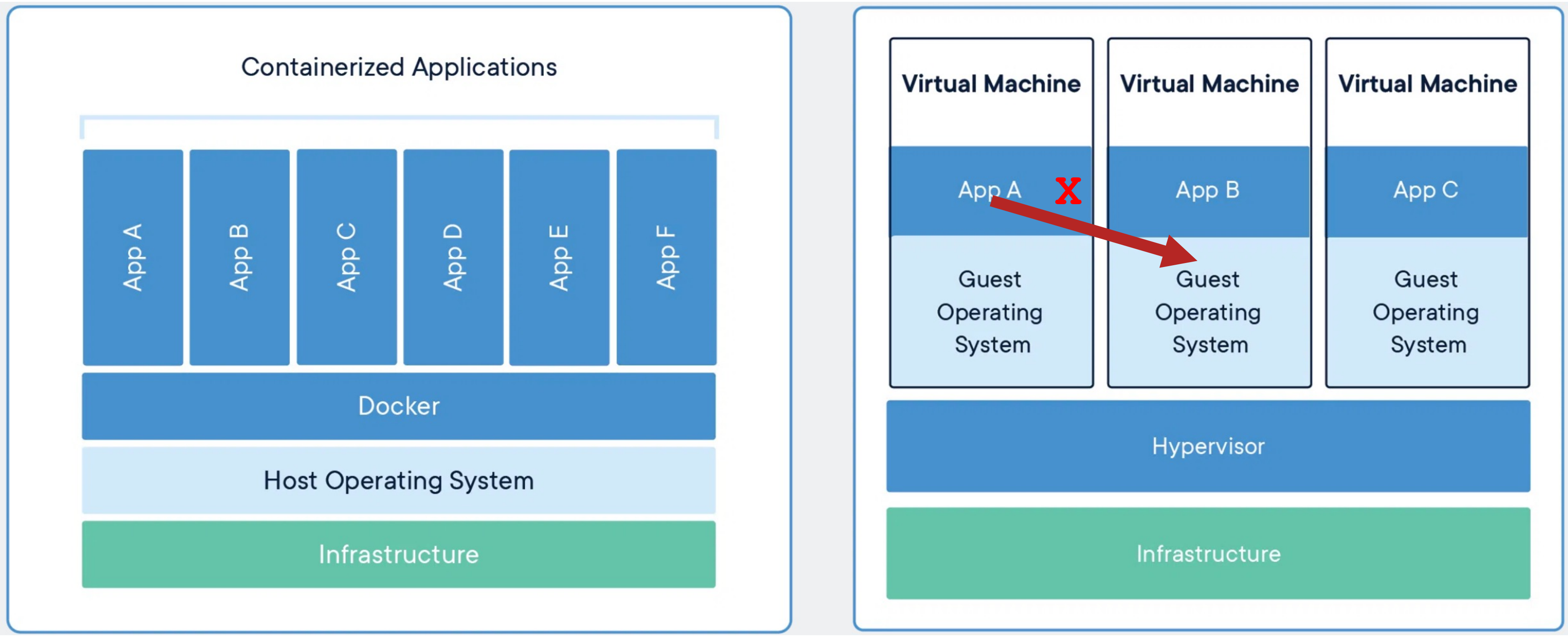
https://www.docker.com/resources/what-container

Containers vs Virtual Machines



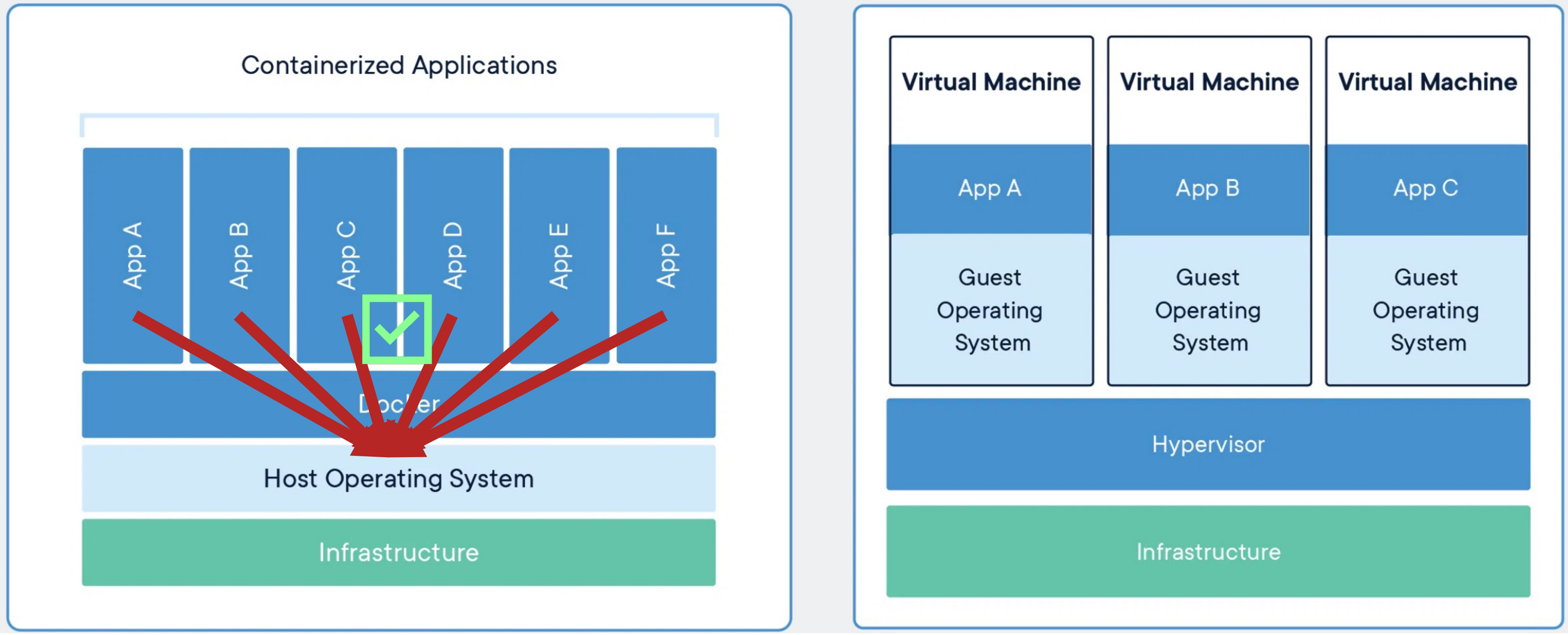
https://www.docker.com/resources/what-container

Containers vs Virtual Machines



https://www.docker.com/resources/what-container

Containers vs Virtual Machines



https://www.docker.com/resources/what-container

Containers (a little deeper)

- Containers are processes, which have been constrained
  - → Cgroups
  - → Capabilities
  - → Namespaces
  - → Chroot jails (or more specifically, `pivot_root`) to restrict file access
  - → Seccomp profiles
  - → LSMs (Linux Security Modules) – AppArmor, SELinux, etc.

Containers (a little deeper)

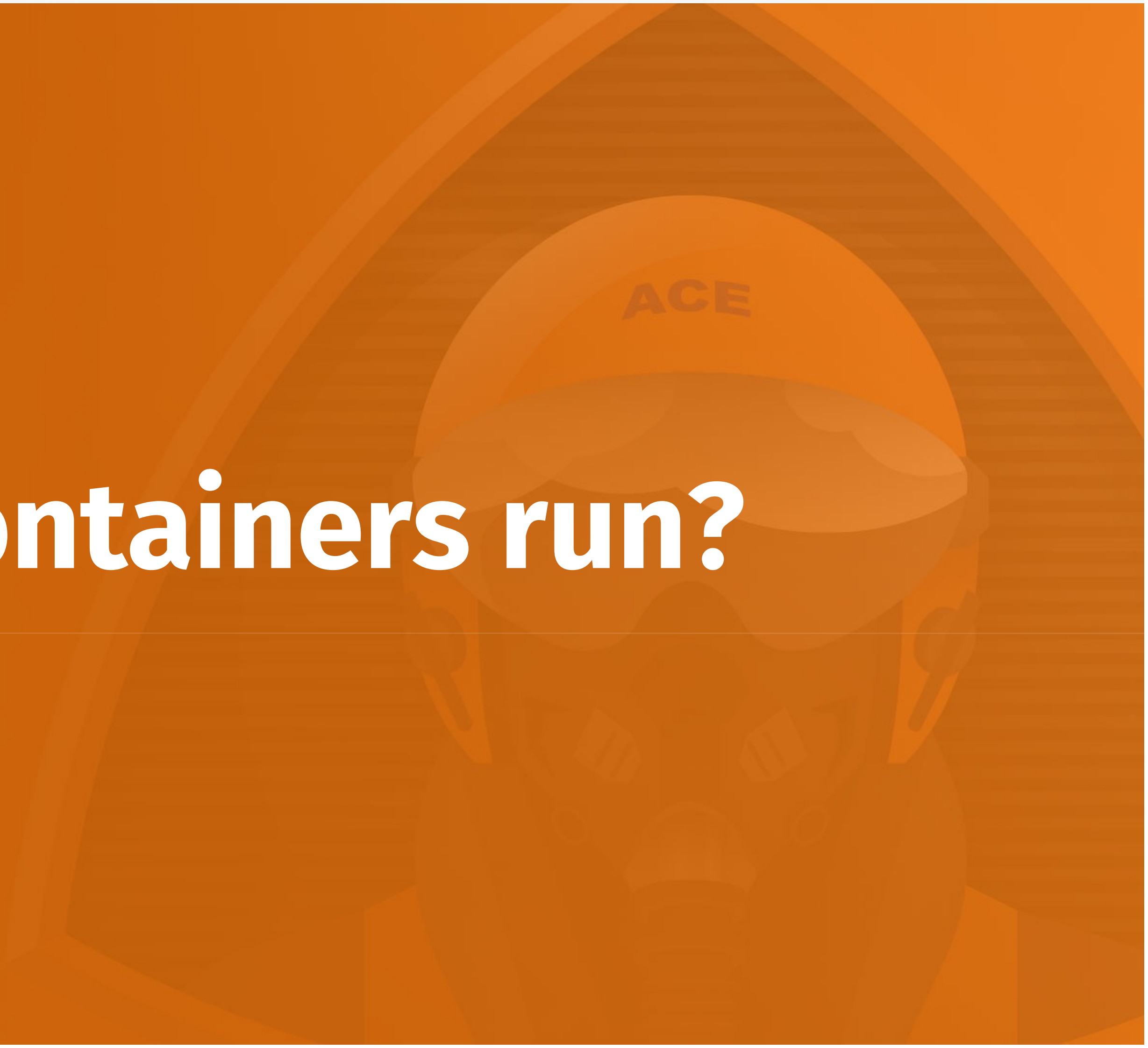
```
$ mkdir alpine
$ curl -o alpine/alpine.tar.gz \
https://dl-cdn.alpinelinux.org/alpine/v3.17/releases/x86_64/alpine-minirootfs-3.17.3-x86_64.tar.gz
$ pushd alpine
$ tar xvf alpine.tar.gz
./
./root/
./var/
...
$ popd
$ sudo unshare --pid --fork chroot alpine /bin/ash
/ # mount -t proc proc proc
/ # This is a (very simple) container! 🎉
```

Containers (a little deeper)

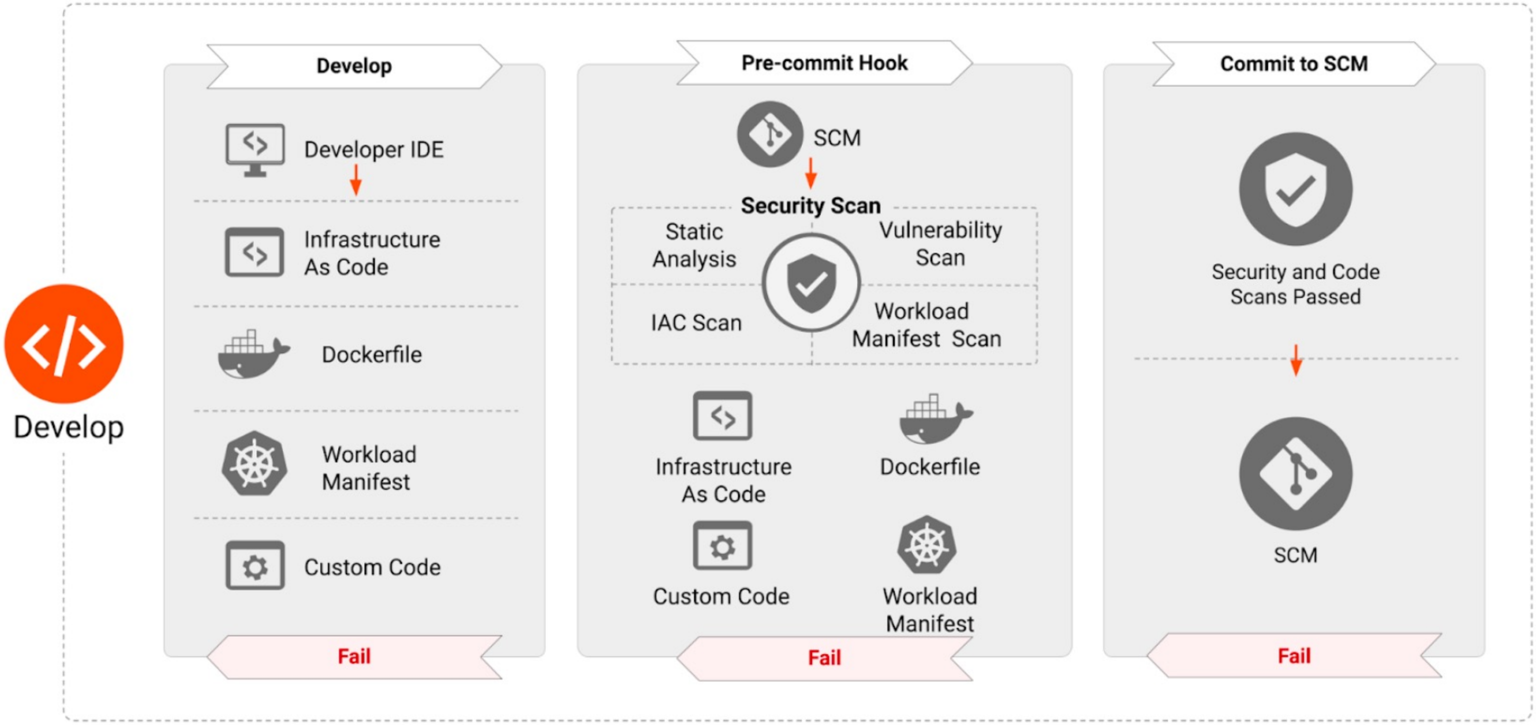
```
UID          PID    PPID  C    SZ   RSS PSR STIME TTY          TIME CMD
root        4079    4046  0  2792  4608   0 16:32 pts/0    00:00:00 sudo unshare --pid --fork chroot alpine /bin/ash
root        4080    4079  0  1810   580   0 16:32 pts/0    00:00:00 unshare --pid --fork chroot alpine /bin/ash
root        4081    4080  0   430  1060   0 16:32 pts/0    00:00:00 /bin/ash
```

Here is the “container”

Where do Containers run?

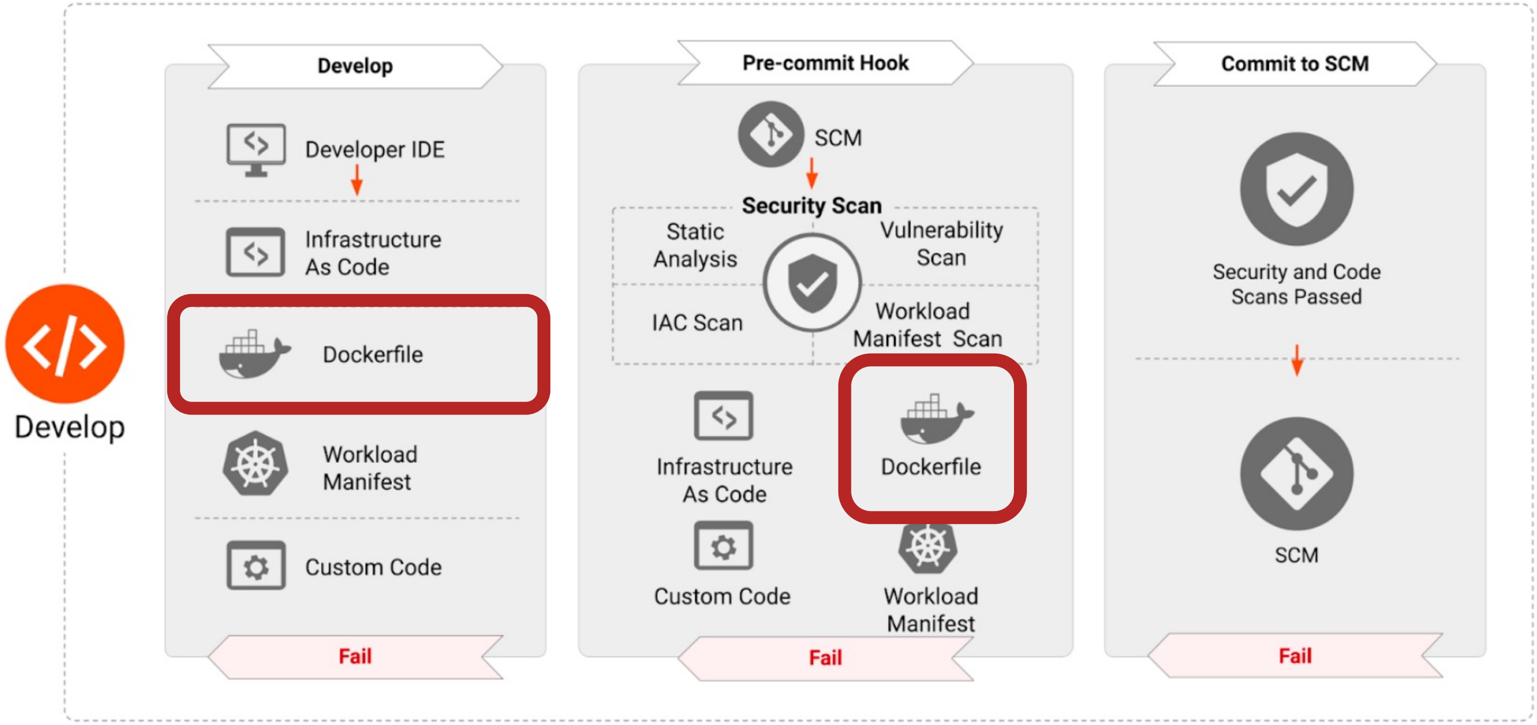


Container Usage



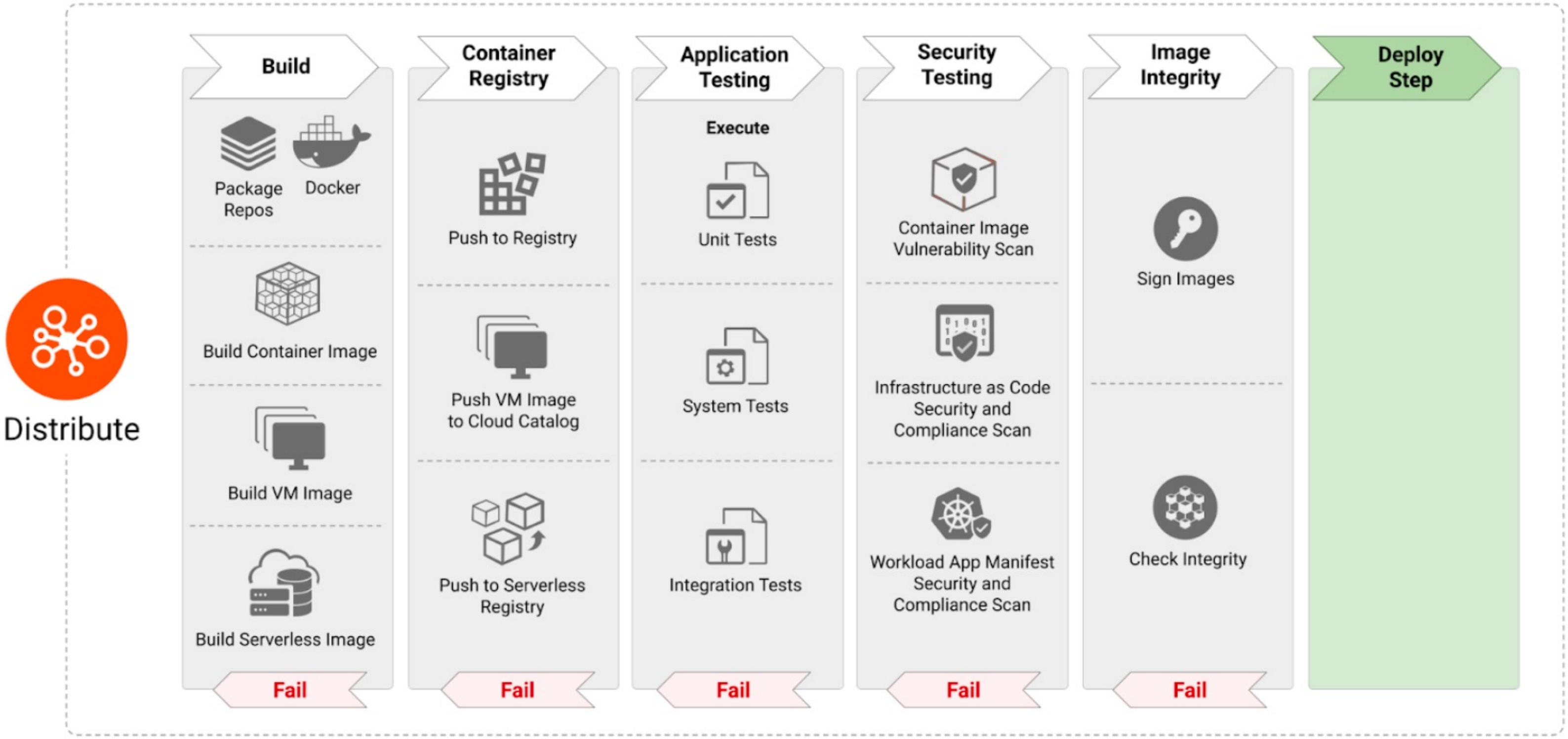
https://github.com/cncf/tag-security/blob/21fe04ad14845069d7c7d8db5c8f98c0547b4a66/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

Container Usage



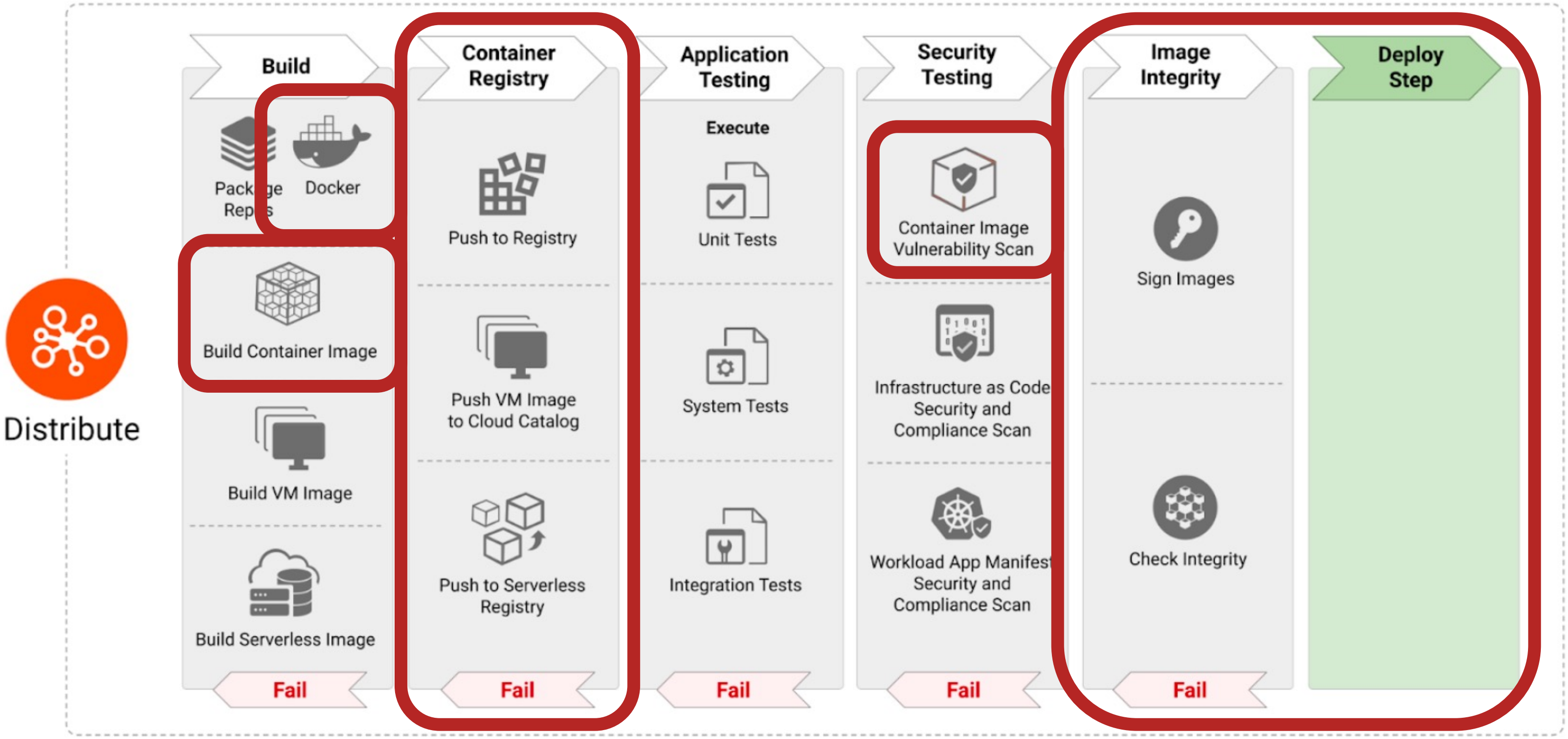
https://github.com/cncf/tag-security/blob/21fe04ad14845069d7c7d8db5c8f98c0547b4a66/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

Container Usage



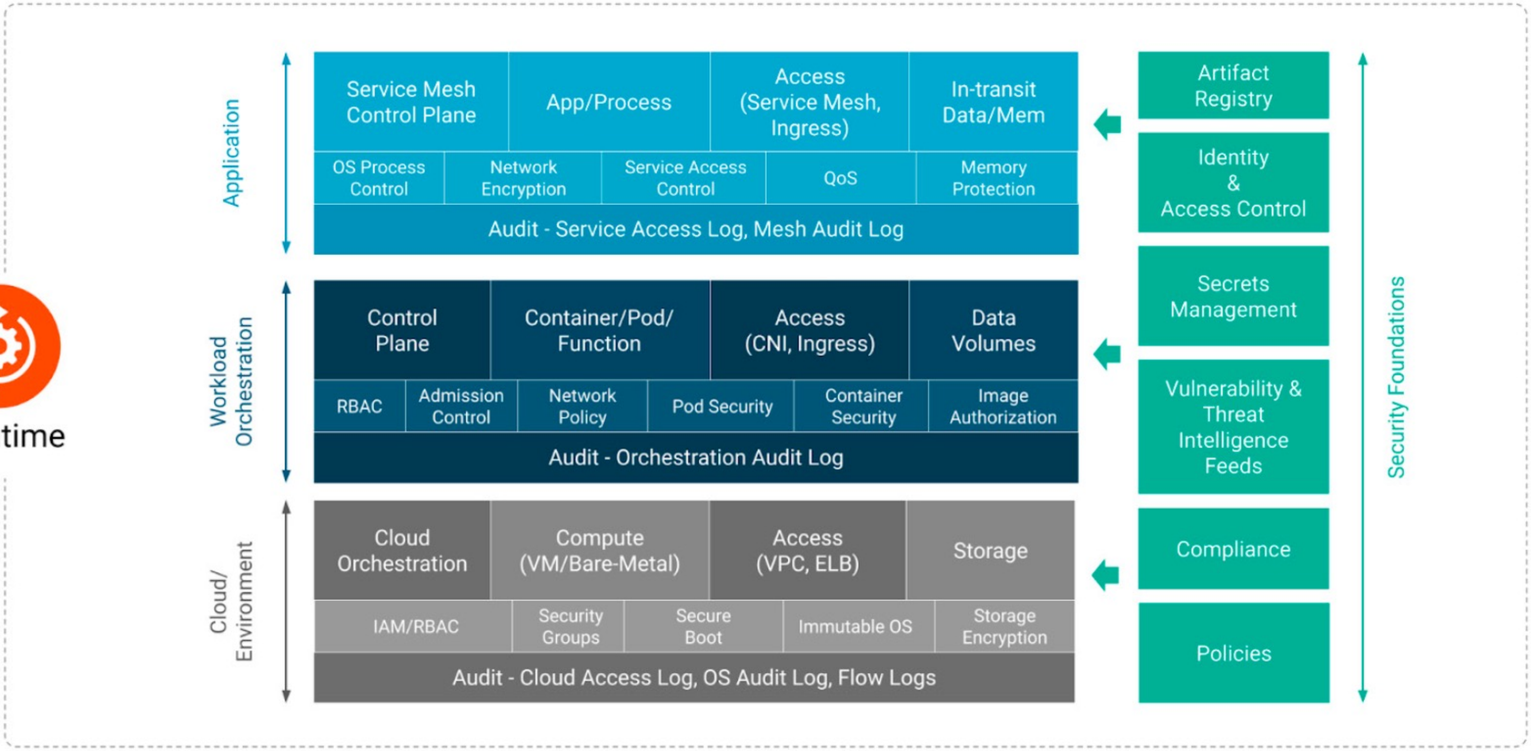
https://github.com/cncf/tag-security/blob/21fe04ad14845069d7c7d8db5c8f98c0547b4a66/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

Container Usage



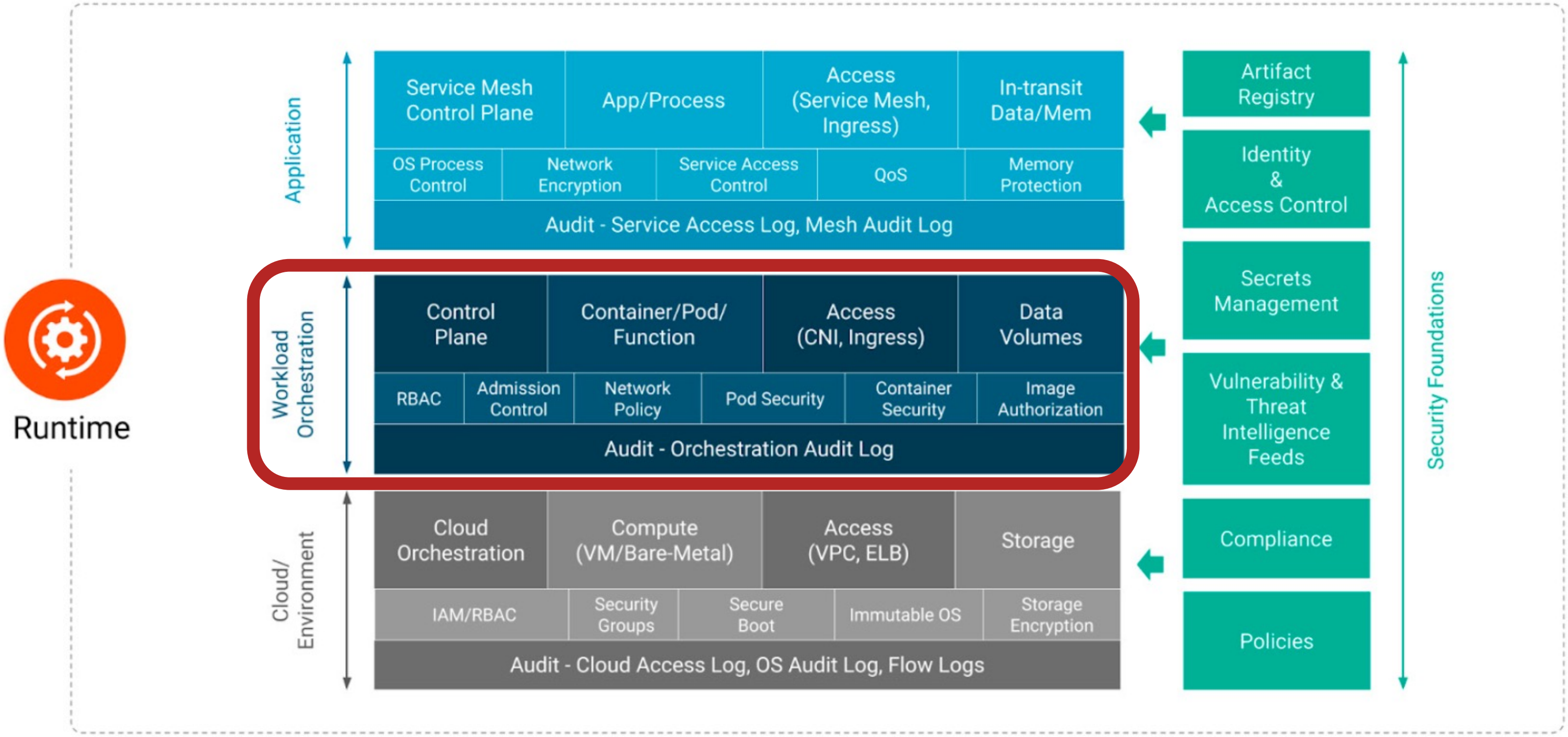
https://github.com/cncf/tag-security/blob/21fe04ad14845069d7c7d8db5c8f98c0547b4a66/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

Container Usage



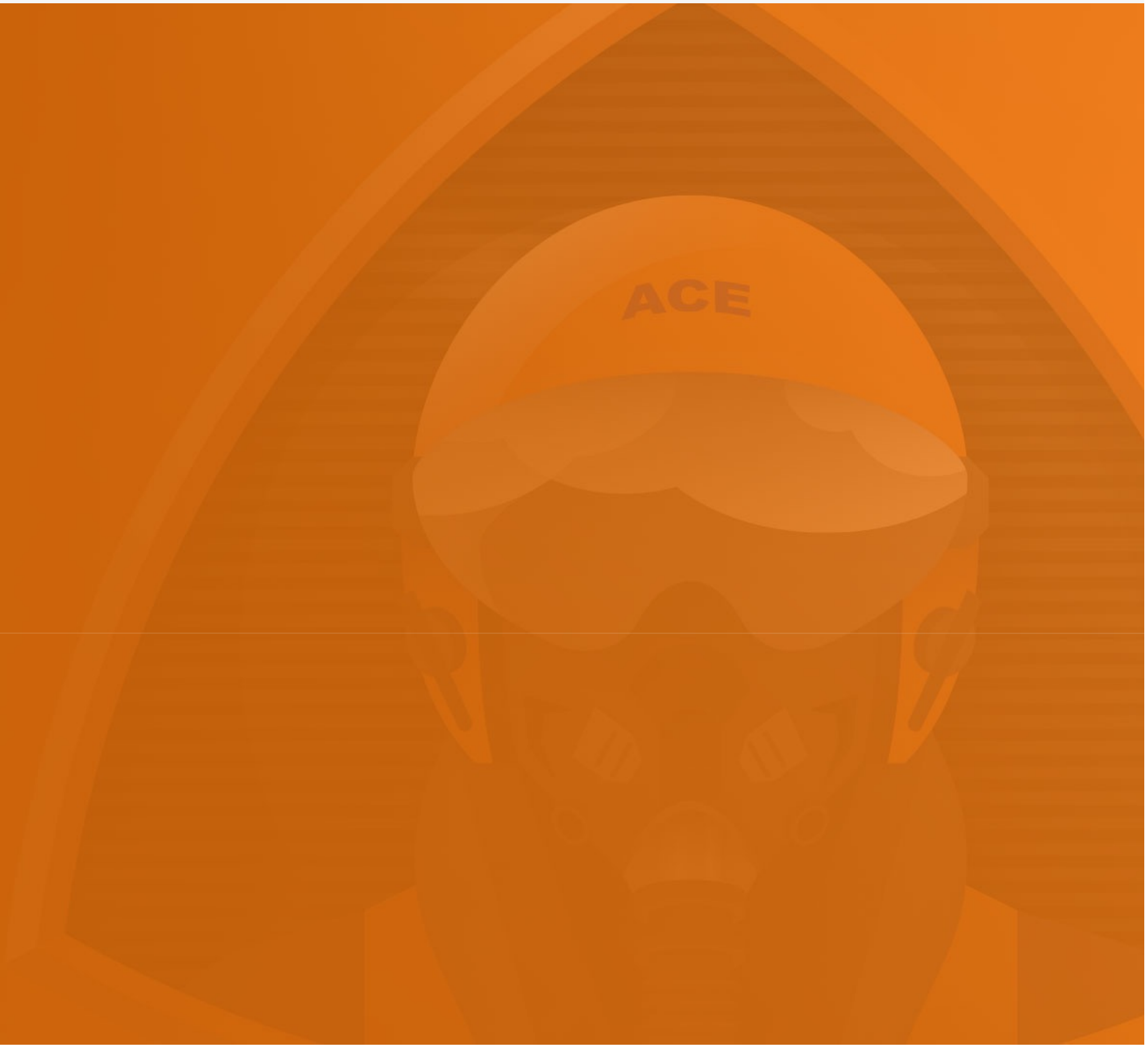
https://github.com/cncf/tag-security/blob/21fe04ad14845069d7c7d8db5c8f98c0547b4a66/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

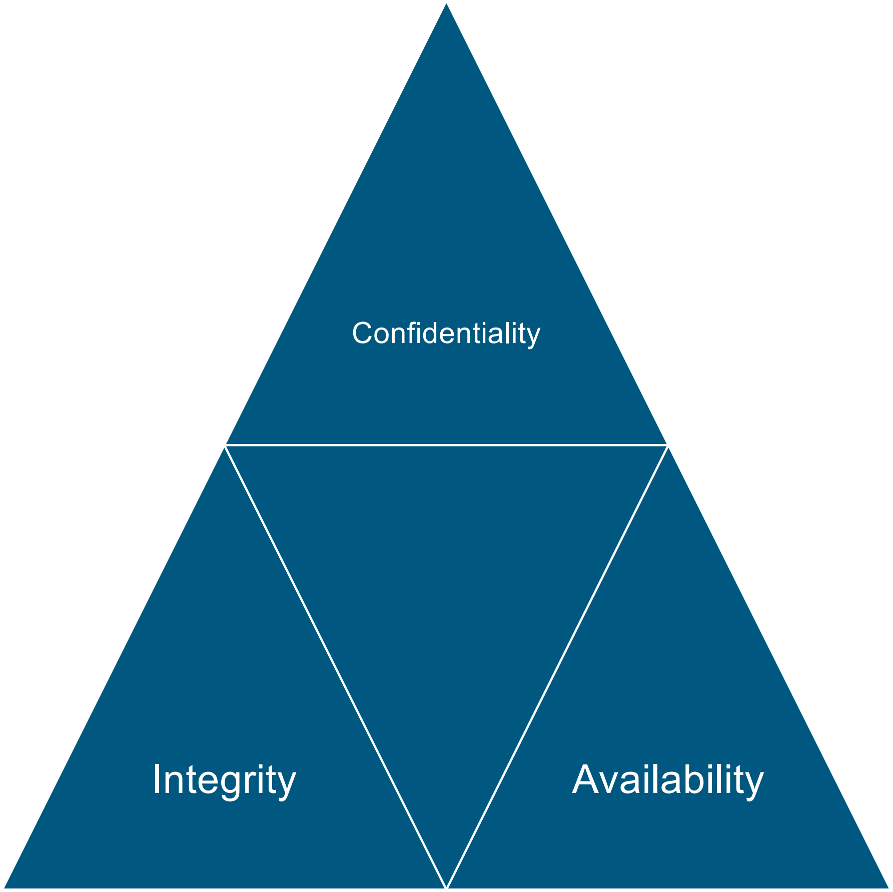
Container Usage

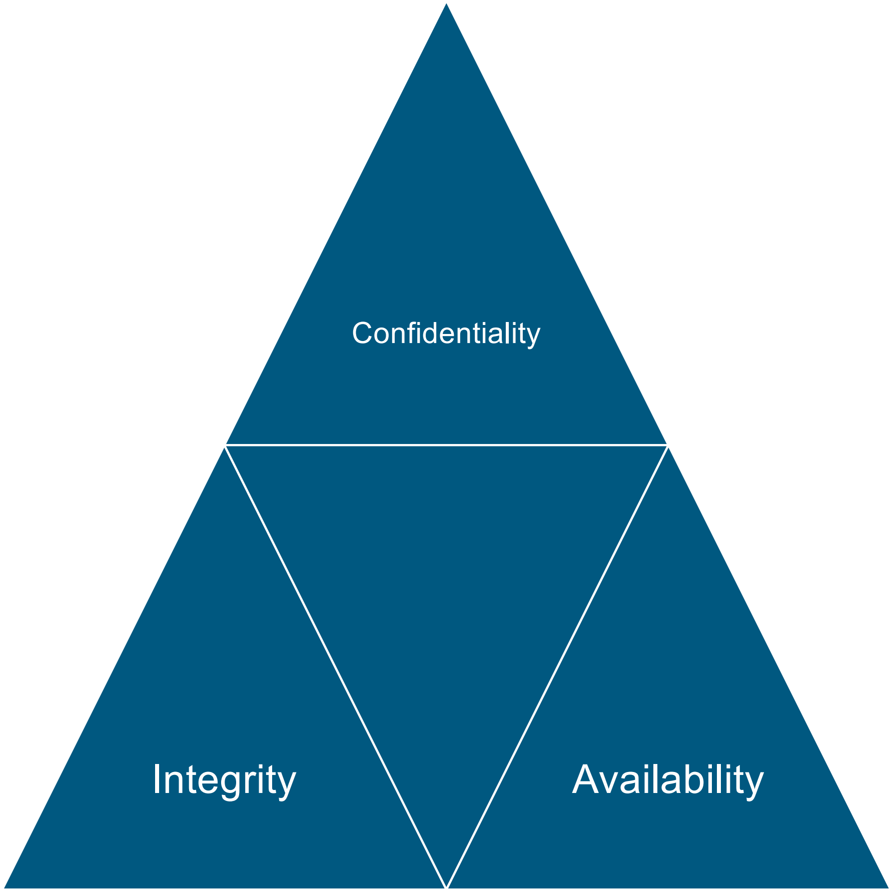


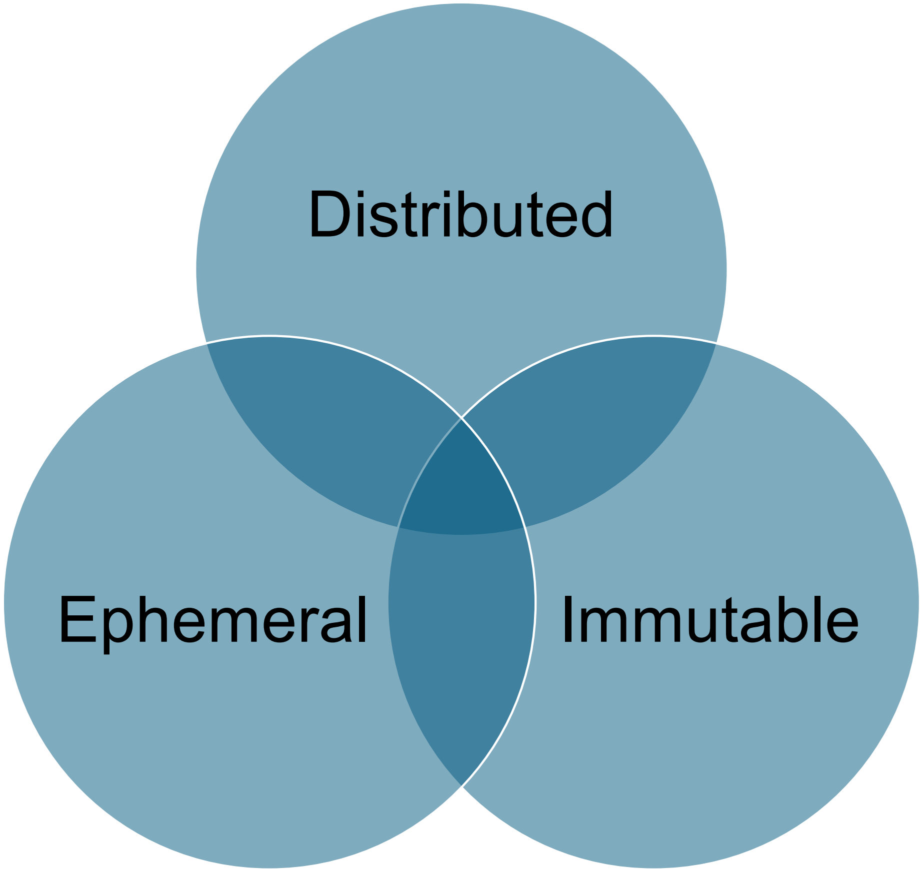
https://github.com/cncf/tag-security/blob/21fe04ad14845069d7c7d8db5c8f98c0547b4a66/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

Security!

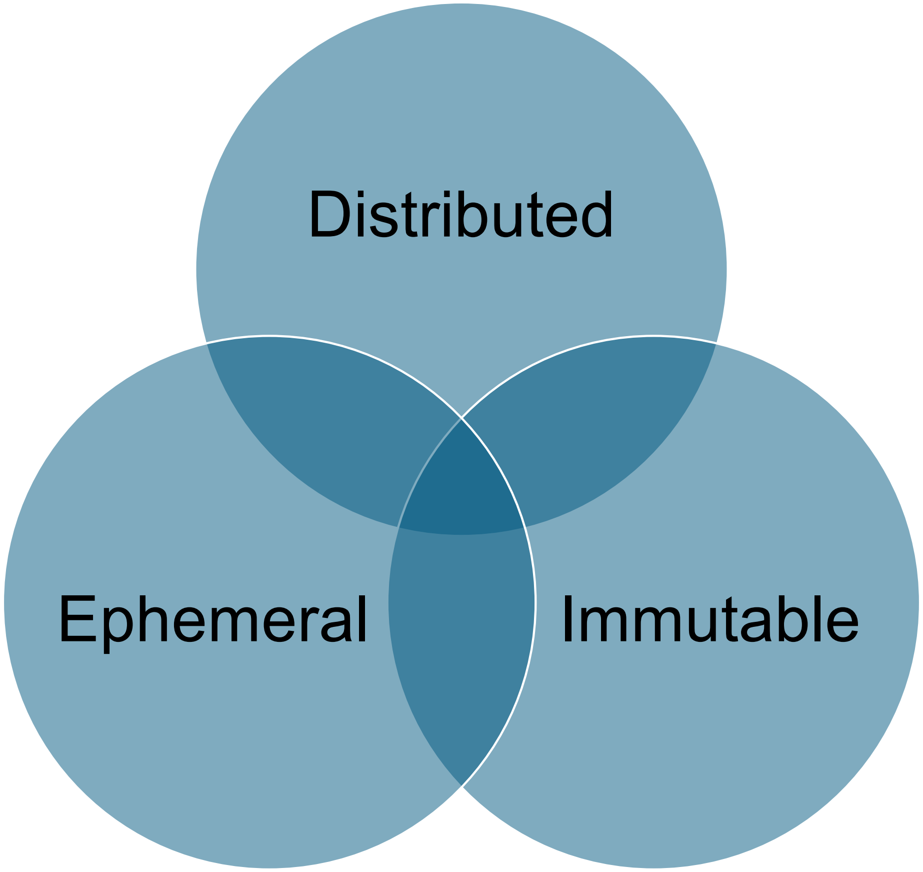



Confidentiality
Integrity
Availability



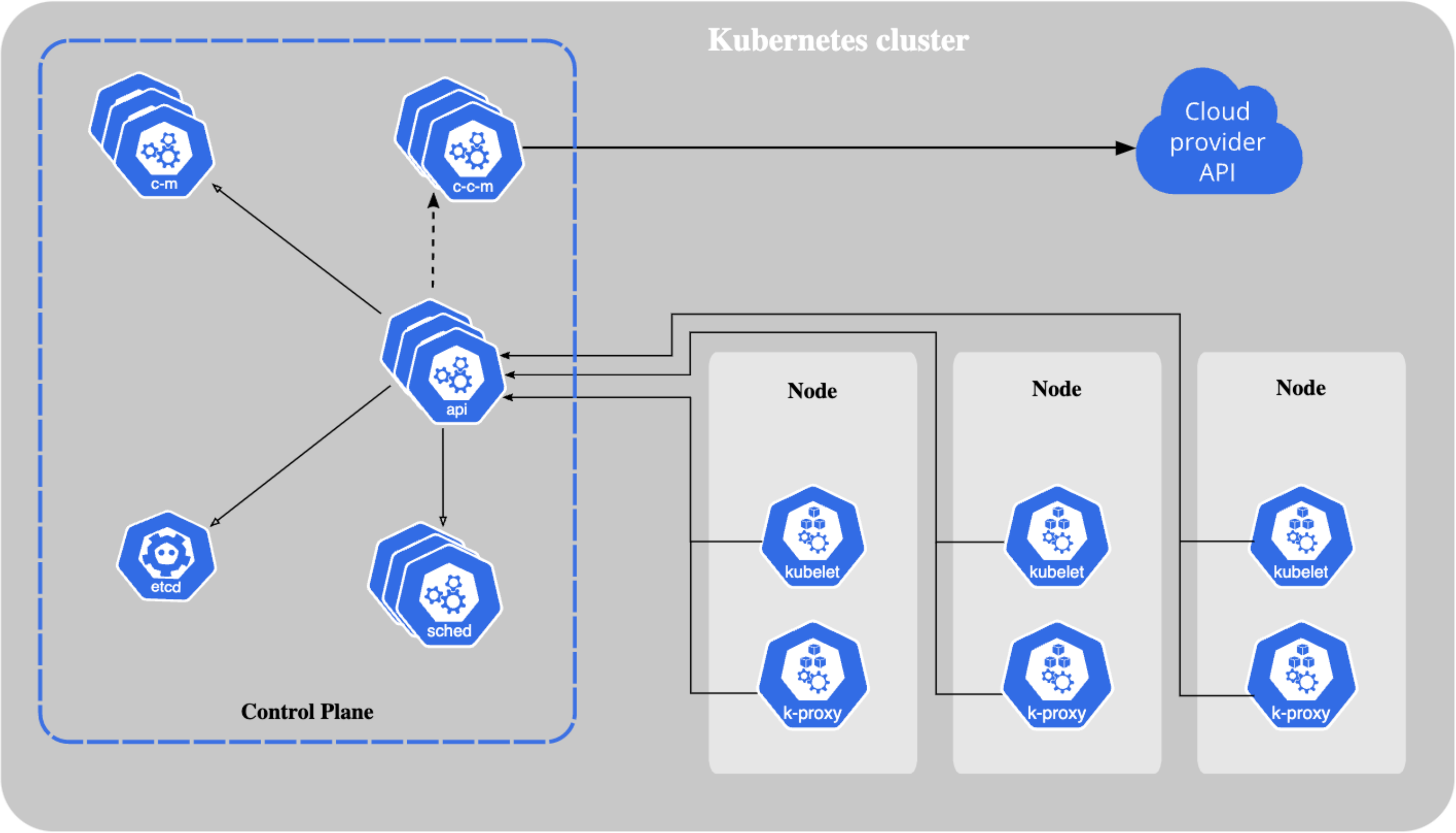


Credit to Sounil Yu and the Cyber Defense Matrix



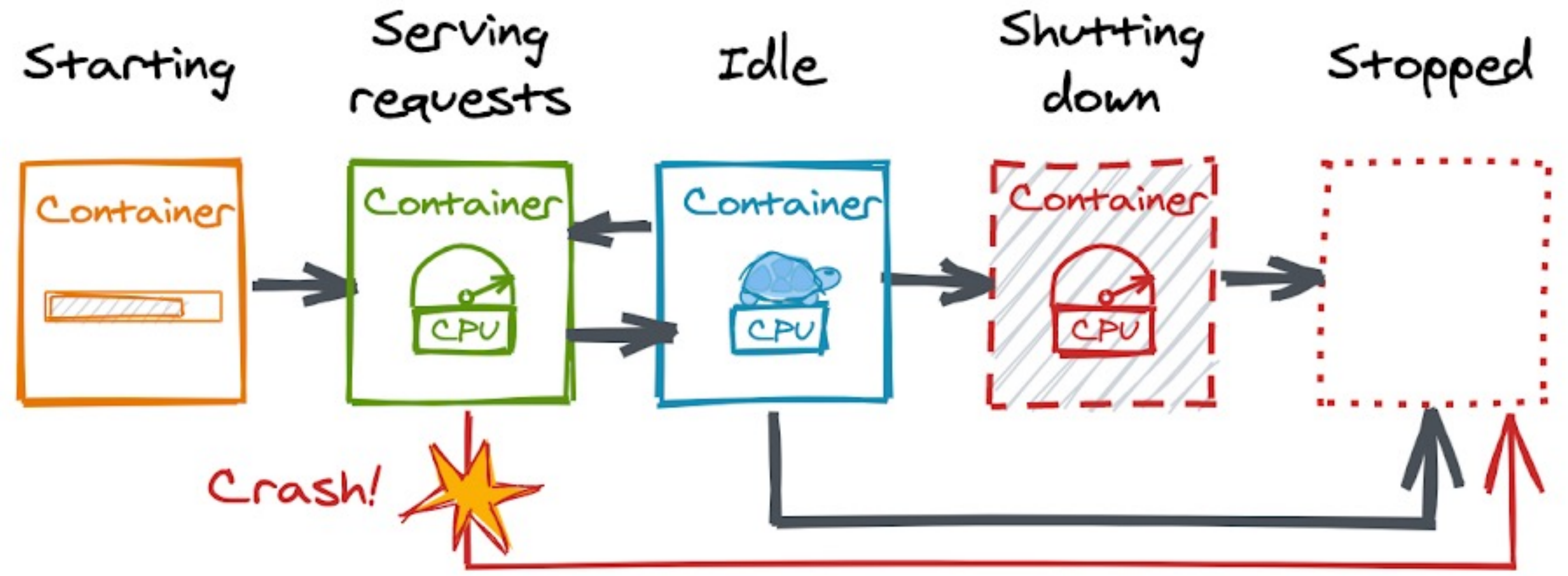
Credit to Sounil Yu and the Cyber Defense Matrix

Distributed



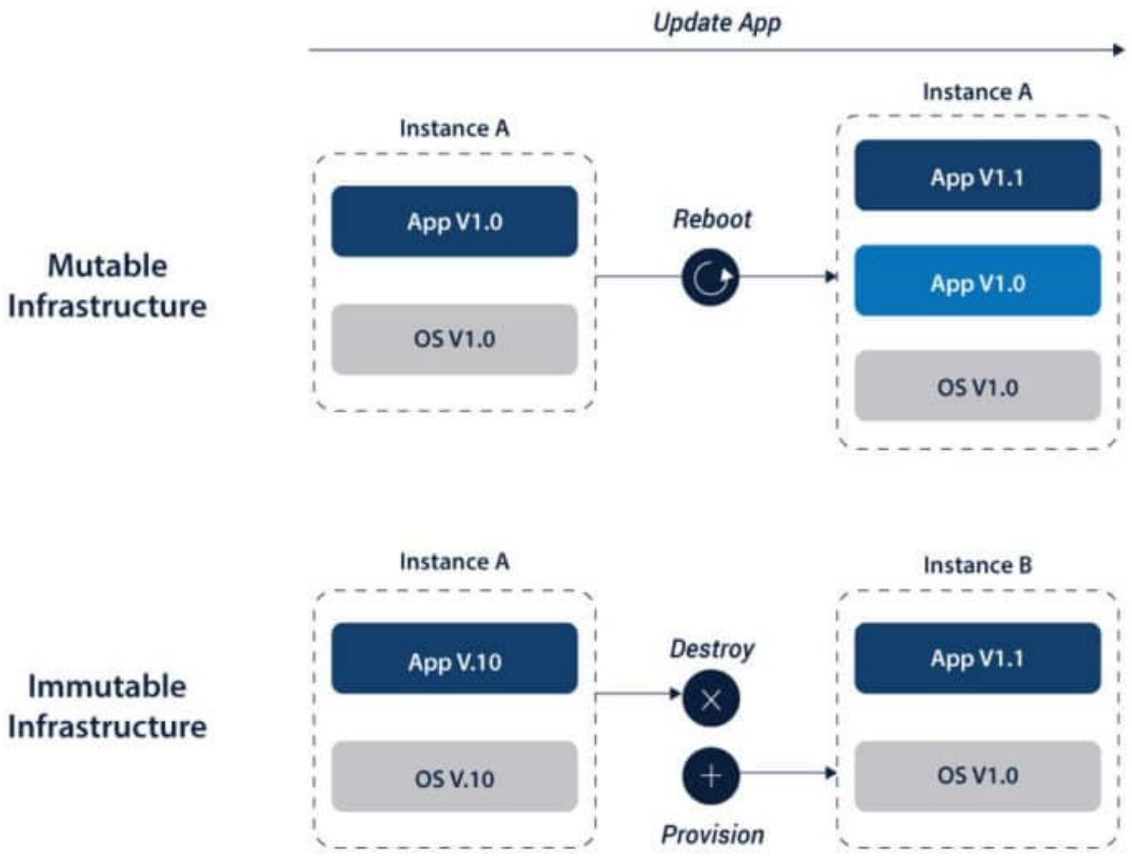
https://kubernetes.io/docs/concepts/overview/components/

Ephemeral



https://cloud.google.com/blog/topics/developers-practitioners/lifecycle-container-cloud-run

Immutable



https://blog.isweluiz.com.br/2022/10/mutable-vs-immutable-infrastructure.html

DIE and CIA

- **Distributed** systems are resilient
  - → High **Availability**
- **Ephemeral** workloads are fast-moving
  - → Breach of **Confidentiality** is less likely because persistence / abuse is difficult
- **Immutable** environments cannot be changed
  - → Strong **Integrity**

Modern Attacks

- **Supply Chain Security**
  - → What is in your containers and software (SBOM)
  - → How was it created (Provenance)
  - → Who created it (Signing)
- **Policy as Code**
  - → Least Privilege
  - → Vulnerability Management
  - → Runtime Protections
- **…**

Workshop

- Ensure you have an Ubuntu 20.04 x86 system running
- Run the Getting Started steps at https://jonzeolla.com/workshop.html

SANS

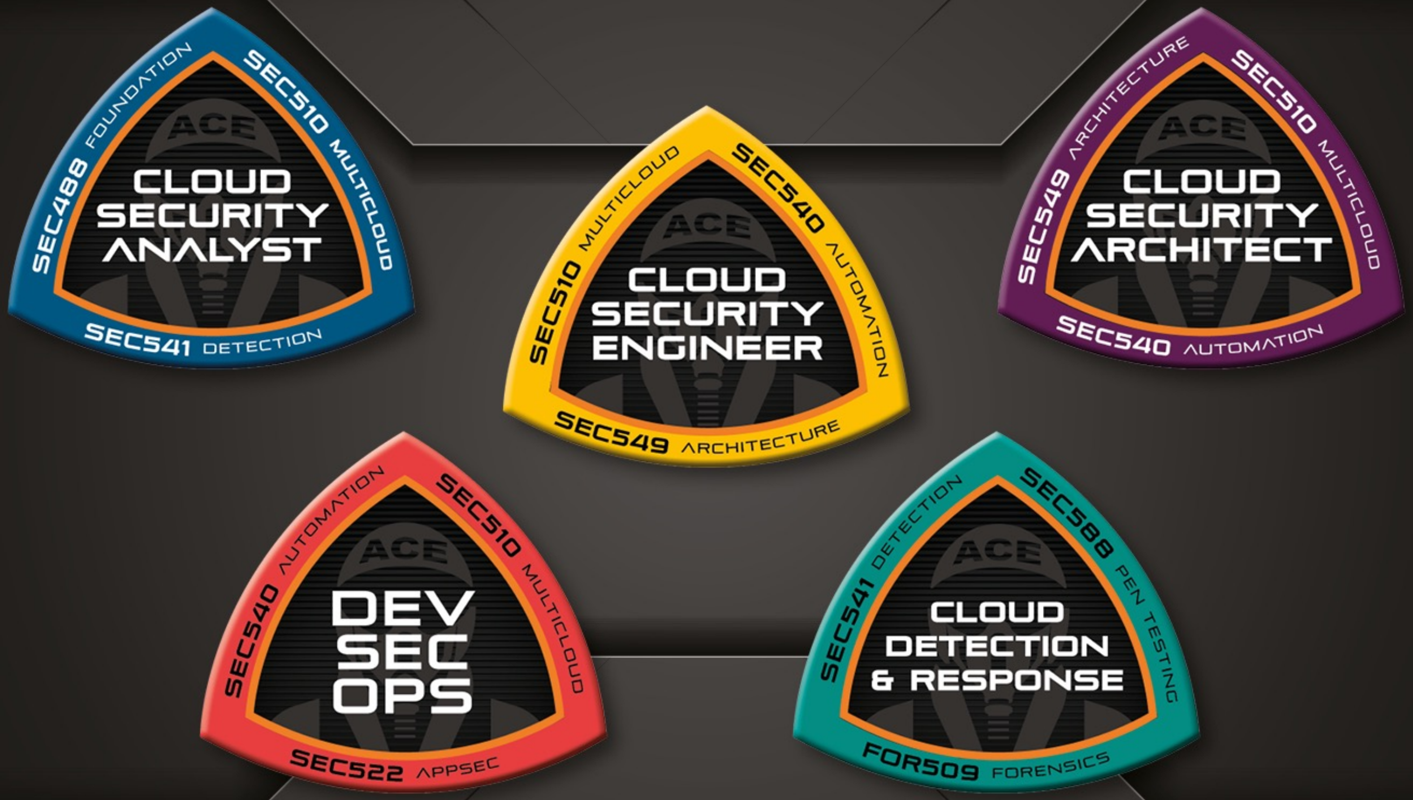
CLOUD SECURITY

Flight Plan – Career Progression

CURRICULUM

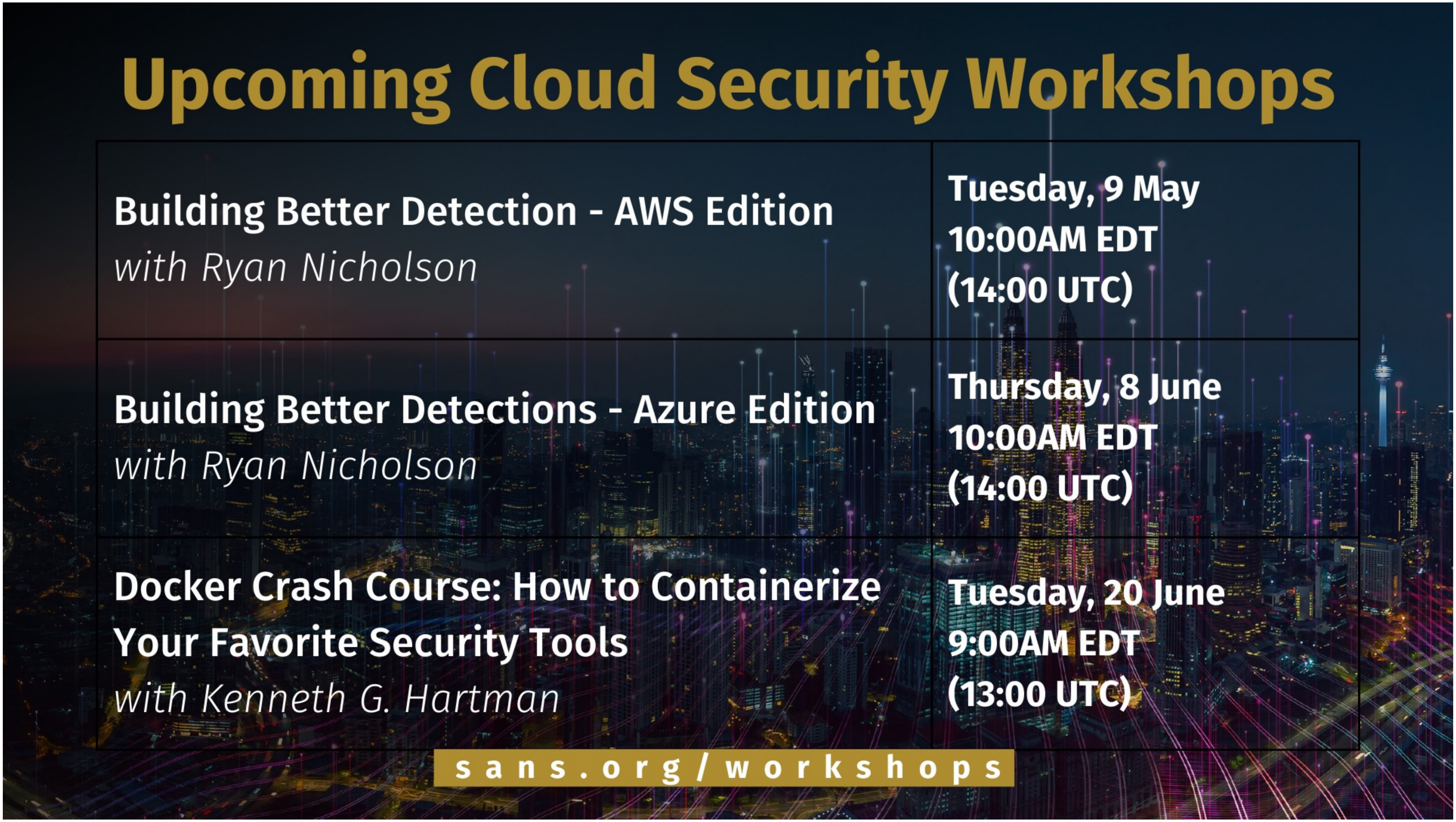
				Cloud Security Analyst	Cloud Security Engineer	Cloud Security Architect	Cloud Security Manager	DevOps Professionals
				Use cloud security solutions to respond to incidents and enable defenses	Build security solutions for cloud workflows	Design how security functions will adopt cloud services, define knowledge, tooling, and approach for cloud solutions	Develop cloud security roadmap, plan, procurement models, ensure policy and procedure is defined to support cloud	Develop, deploy, and manage secure applications and systems
BASELINE	SEC 388	**Introduction to Cloud Computing and Security** *Ground school for cloud security*		●			●	
FOUNDATIONAL	SEC 488	**Cloud Security Essentials** *License to learn cloud security*	GIAC CLOUD SECURITY GCLD ESSENTIALS	●	●	●	●	
CORE	SEC 510	**Public Cloud Security: AWS, Azure, and GCP** *Multiple clouds require multiple solutions.*	GIAC PUBLIC GPCS CLOUD SECURITY	●	●	●		●
	SEC 540	**Cloud Security and DevSecOps Automation** *The cloud moves fast. Automate to keep up.*	GIAC CLOUD SECURITY GCSA AUTOMATION		●	●		●
	SEC 541	**Cloud Security Attacker Techniques, Monitoring, and Threat Detection** *Attackers can run but not hide. Our radar sees all threats.*	GIAC CLOUD GCTD THREAT DETECTION	●	●			
	SEC 549	**Enterprise Cloud Security Architecture** *Design it right from the start.*			●	●	●	
SPECIALIZATION	SEC 522	**Application Security: Securing Web Apps, APIs, and Microservices** *Not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how.*	GIAC CERTIFIED WEB GWEB APPLICATION DEFENDER					●
	SEC 588	**Cloud Penetration Testing** *Aim your arrows to the sky and penetrate the cloud.*	GIAC CLOUD GCPN PENETRATION TESTER	●	●			
	FOR 509	**Enterprise Cloud Forensics and Incident Response** *Find the storm in the cloud.*	GIAC CLOUD FORENSICS GCFR RESPONDER	●				
MANAGEMENT	MGT 520	**Leading Cloud Security Design and Implementation** *Chart your course to cloud security.*				●	●	

CLOUD ACE JOURNEYS



CLOUD SECURITY

SANS



Upcoming Cloud Security Workshops

Building Better Detection - AWS Edition *with Ryan Nicholson*	**Tuesday, 9 May** **10:00AM EDT** **(14:00 UTC)**
Building Better Detections - Azure Edition *with Ryan Nicholson*	**Thursday, 8 June** **10:00AM EDT** **(14:00 UTC)**
Docker Crash Course: How to Containerize Your Favorite Security Tools *with Kenneth G. Hartman*	**Tuesday, 20 June** **9:00AM EDT** **(13:00 UTC)**

sans.org/workshops

SANS | CLOUD SECURITY

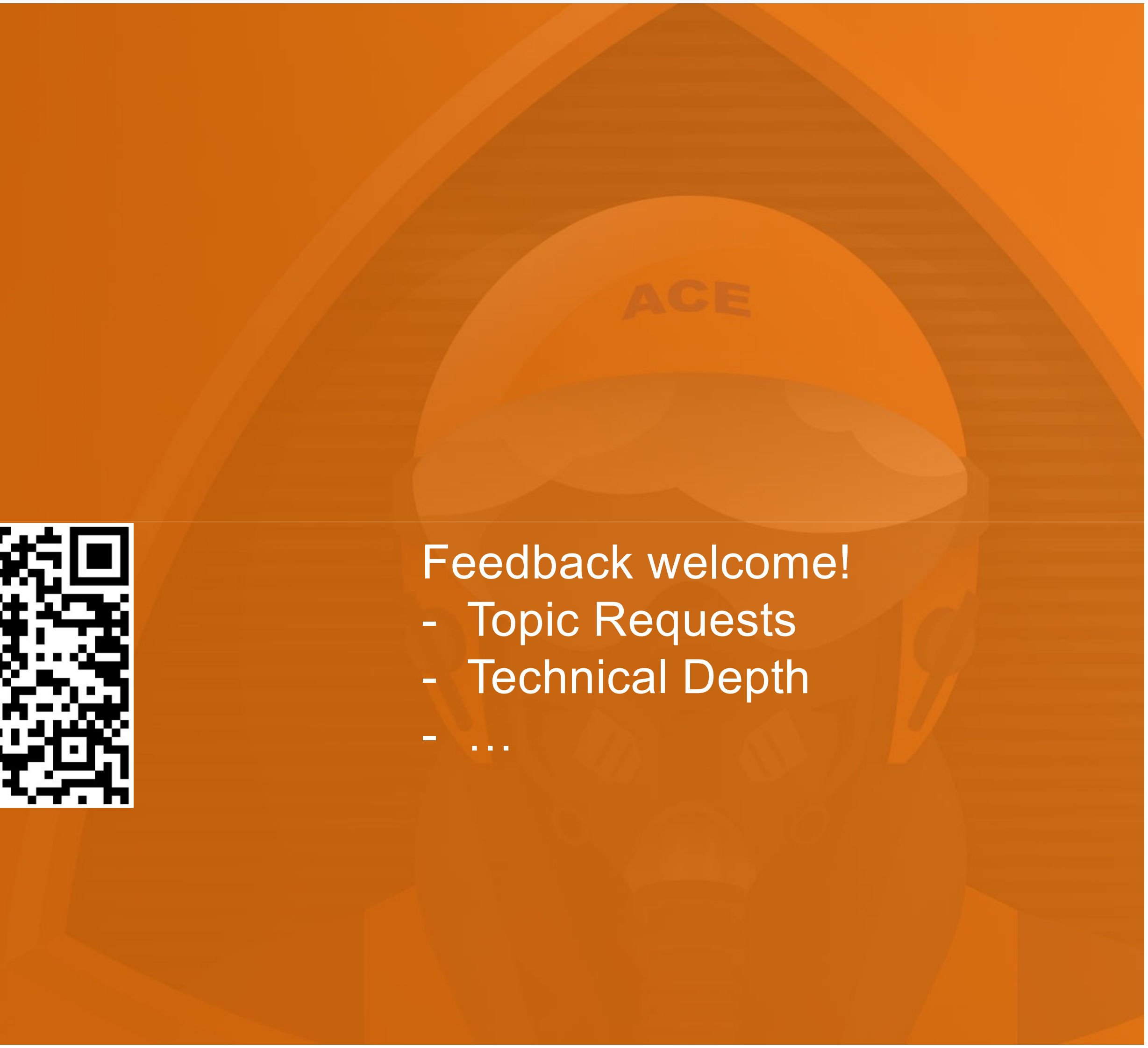
Thank You

Jon Zeolla

LinkedIn.com/in/jonzeolla

jzeolla@sans.org

Jon.Zeolla@SeisoLLC.com



Feedback welcome!

- Topic Requests
- Technical Depth
- …