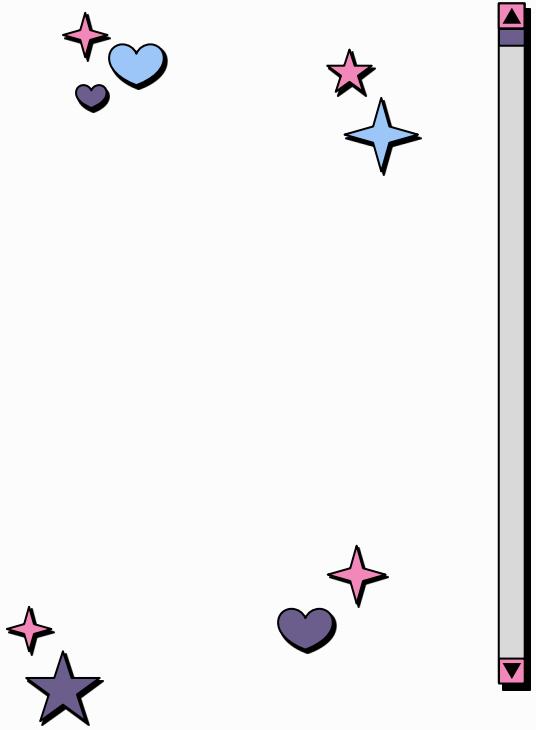
Minimalism:

Key to Cloud Security



Back

Next

$ whoami

Barun Acharya (@daemon1024)

- Software Engineer @ Accuknox
- Maintainer and Tech Lead @ KubeArmor (CNCF Sandbox)
- CNCF Ambassador
- Google Summer of Code
- LFX Mentorship

Back

Next

Container

Back

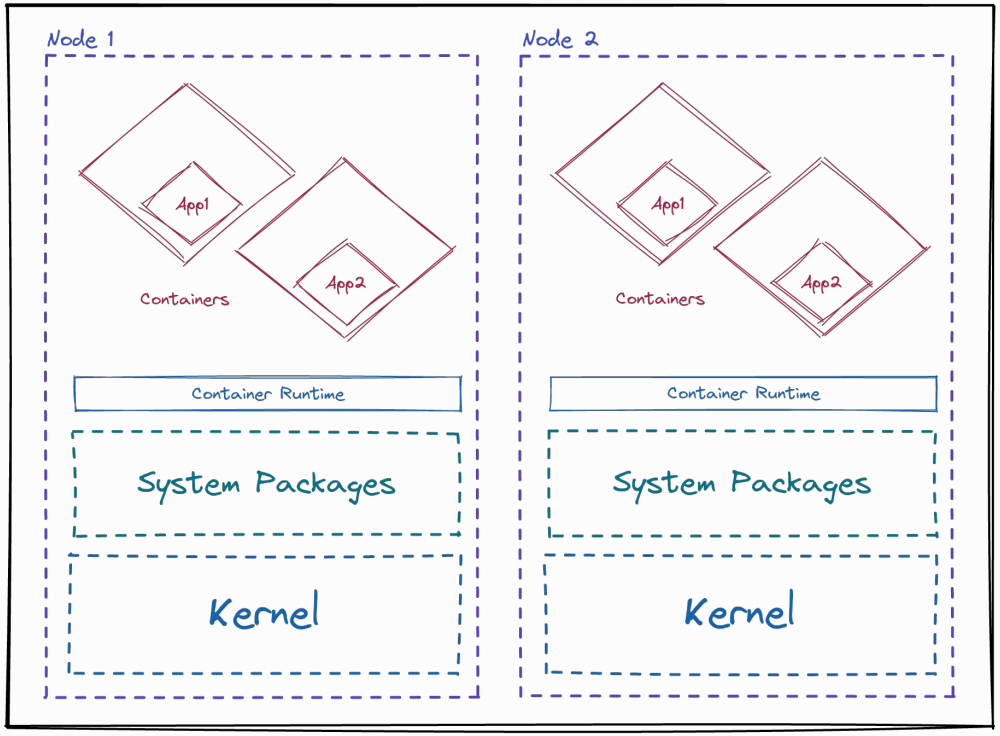
Next

Container Security

Back

Next

Kubernetes Cluster



Back

Next

Malicious Actors

Kubernetes Cluster

Node 1

App1

App2

Containers

Container Runtime

System Packages

Kernel

Node 2

App1

App2

Containers

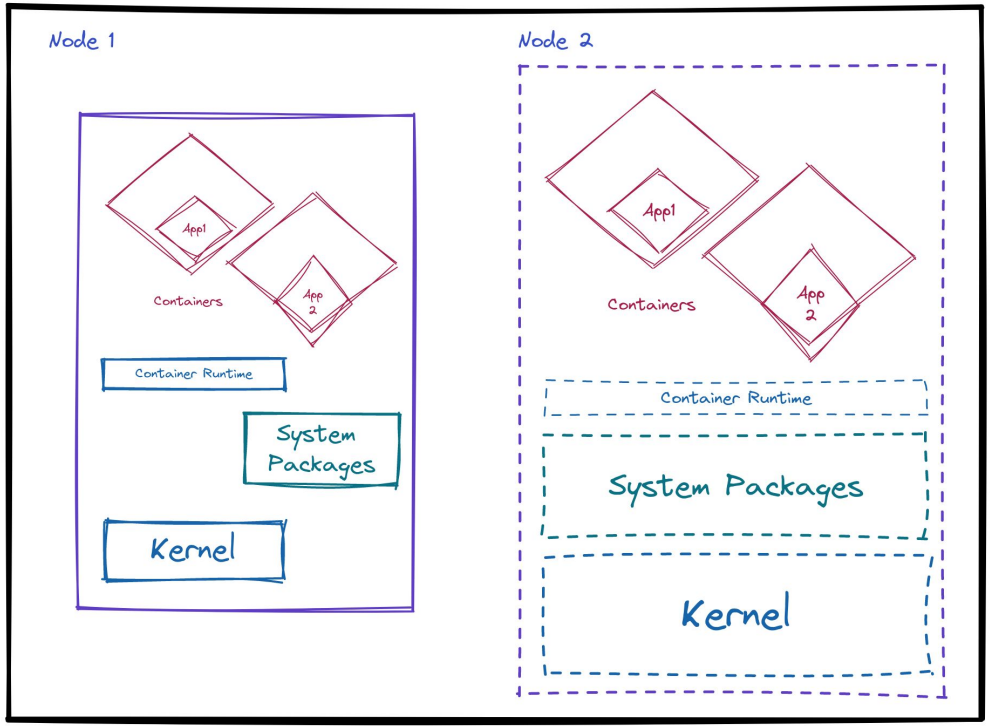
Container Runtime

System Packages

Kernel

Back

Next

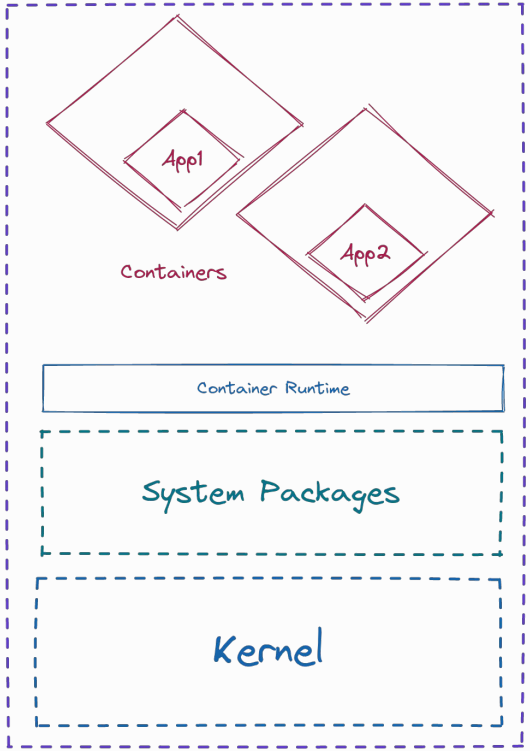

Node 1
App1
App 2
Containers
Container Runtime
System Packages
Kernel
Node 2
App1
App 2
Containers
Container Runtime
System Packages
Kernel

Back

Next

Minimal Node Images

- Container Optimized OS by Google Cloud
- BottleRocket by AWS
- Azure Linux (CBL Mariner) by AKS
- RancherOS
- .....

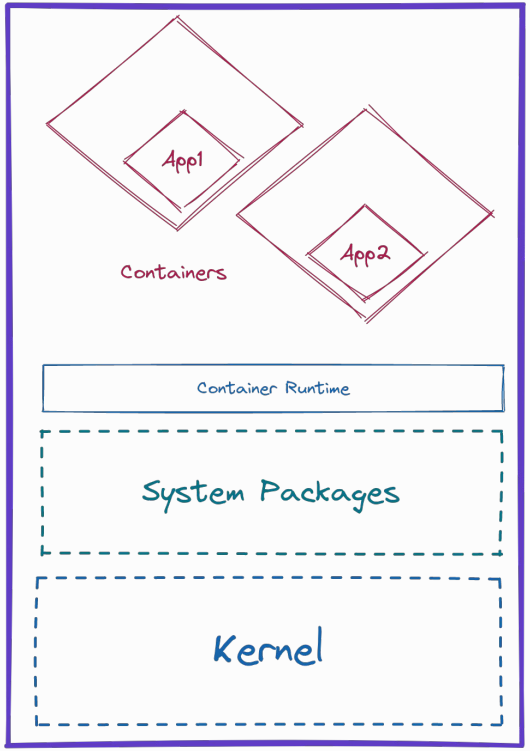


Back

Next

Minimal Node Images

- Immutable Root File System

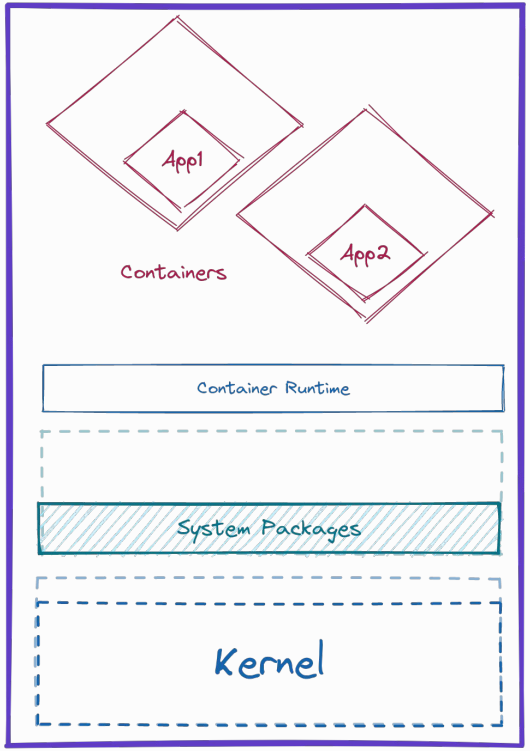


Back

Next

Minimal Node Images

- Immutable Root File System
- Reduced System Bloat

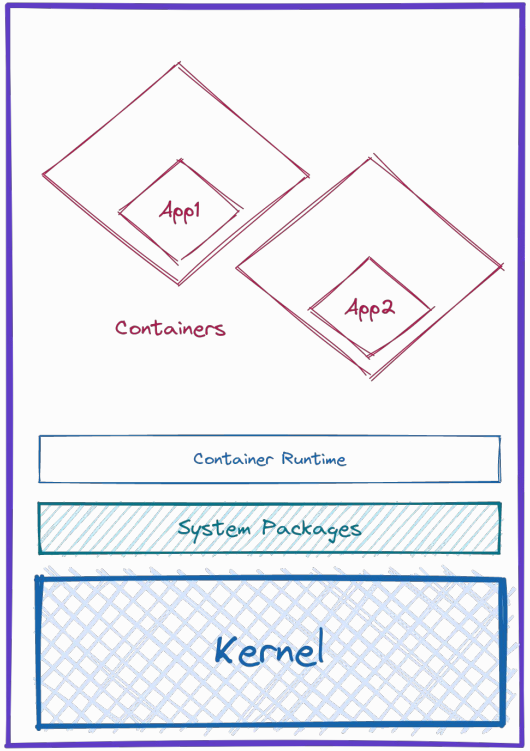


Back

Next

Minimal Node Images

- Immutable Root File System
- Reduced System Bloat
- Hardened Kernel

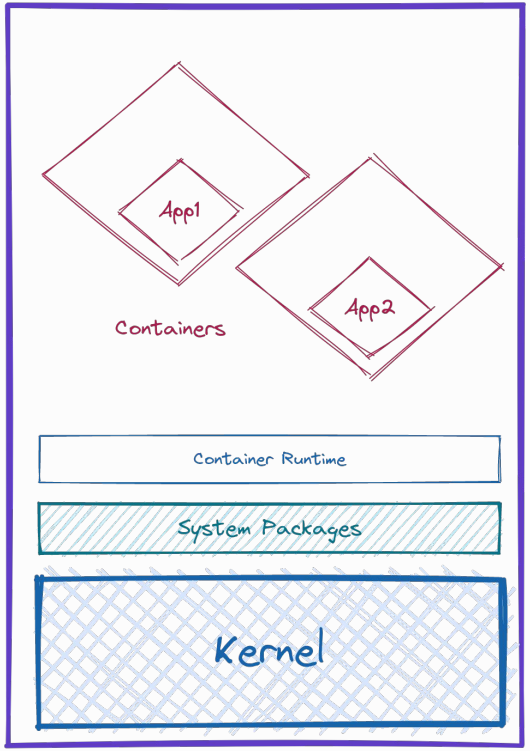


Back

Next

Minimal Node Images

- Immutable Root File System
- Reduced System Bloat
- Hardened Kernel
  - Integrity Measurement Architecture (IMA)

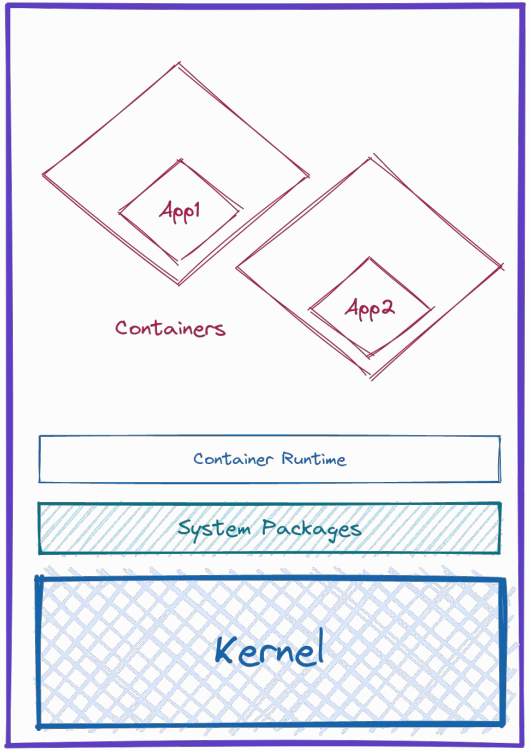


Back

Next

Minimal Node Images

- Immutable Root File System
- Reduced System Bloat
- Hardened Kernel
  - Integrity Measurement Architecture (IMA)
  - Secure Boot



Back

Next

Rocke Malware

Back

Next

https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang

Rocke Malware

- Self-Replication:
  - The malware copies itself from "/tmp/kthrotlds" to "/usr/sbin/kthrotlds."
  - It alters the modified time stamp of the copied file, setting it back 416 days.
- Shared Object Injection:
  - The malware writes code to "/usr/local/lib/libcset.c" and compiles it using GCC into a shared object at "/usr/local/lib/libcset.so."
  - If GCC is not installed, the malware attempts to install it and recompile.
- Startup Scripts:
  - The malware installs an "init.d" startup script at "/etc/init.d/netdns" and a systemd service script at "/usr/lib/systemd/system/netdns.service."
  - It changes the modified time of these files in a similar manner.

Back

Next

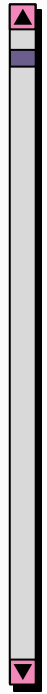
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang

- ~~Self-Replication:~~
  - ~~The malware copies itself from "/tmp/kthrotlds" to "/usr/sbin/kthrotlds."~~
  - ~~It alters the modified time stamp of the copied file, setting it back 416 days.~~

    Immutable Root File System
- ~~Shared Object Injection:~~
  - ~~The malware writes code to "/usr/local/lib/libcset.c" and compiles it using GCC into a shared object at "/usr/local/lib/libcset.so."~~
  - ~~If GCC is not installed, the malware attempts to install it and recompile~~.

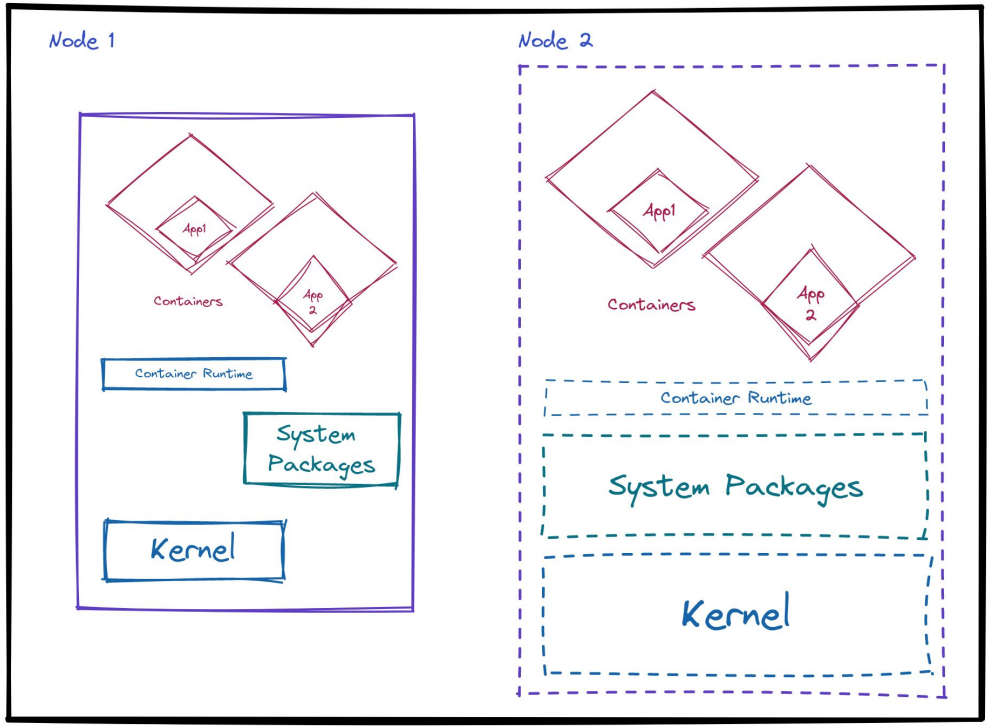
    No system packages/package managers and File Integrity
- ~~Startup Scripts:~~
  - ~~The malware installs an "init.d" startup script at "/etc/init.d/netdns" and a systemd service script at "/usr/lib/systemd/system/netdns.service."~~
  - ~~It changes the modified time of these files in a similar manner.~~

    Secure Boot



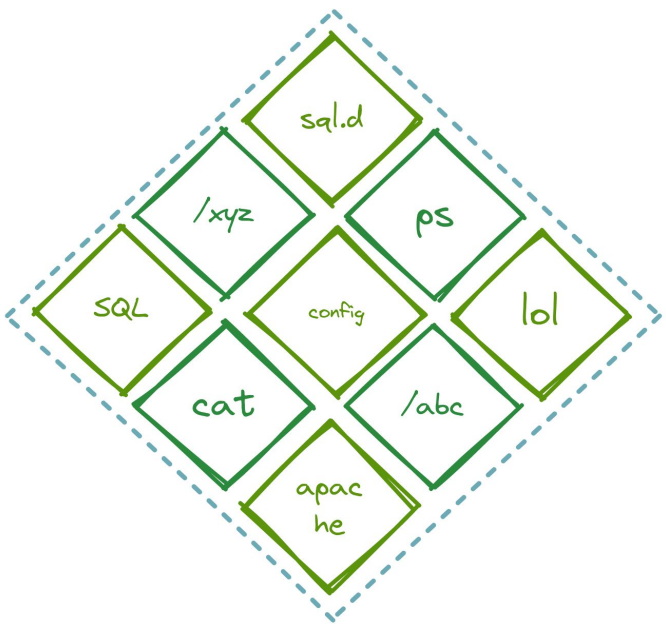
Back

Next


Node 1
App1
App 2
Containers
Container Runtime
System Packages
Kernel
Node 2
App1
App 2
Containers
Container Runtime
System Packages
Kernel

Back
Next

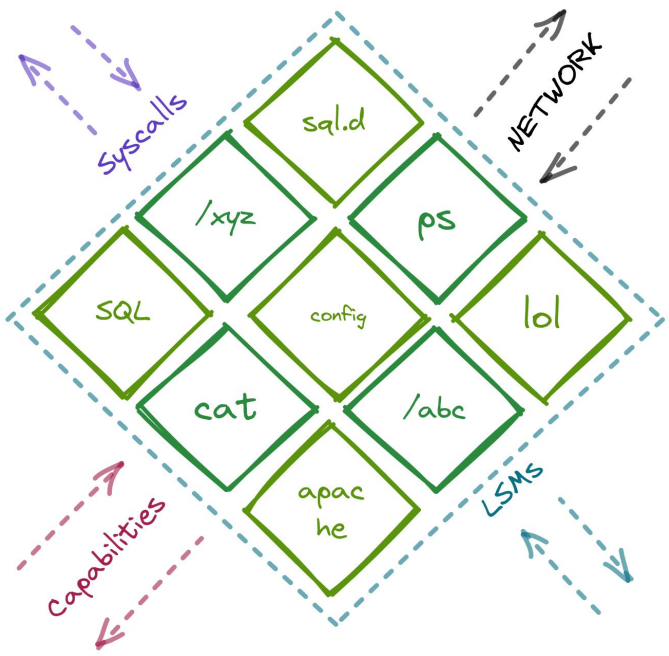
Containers



Back

Next

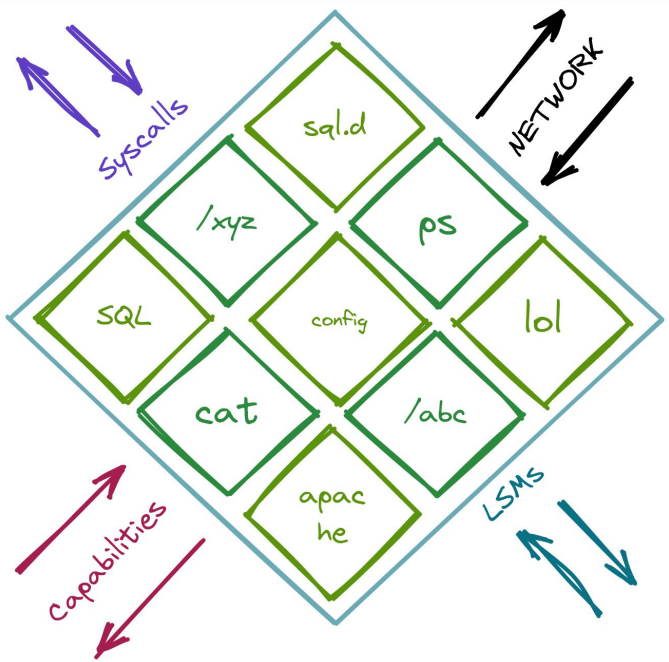
Containers



Back

Next

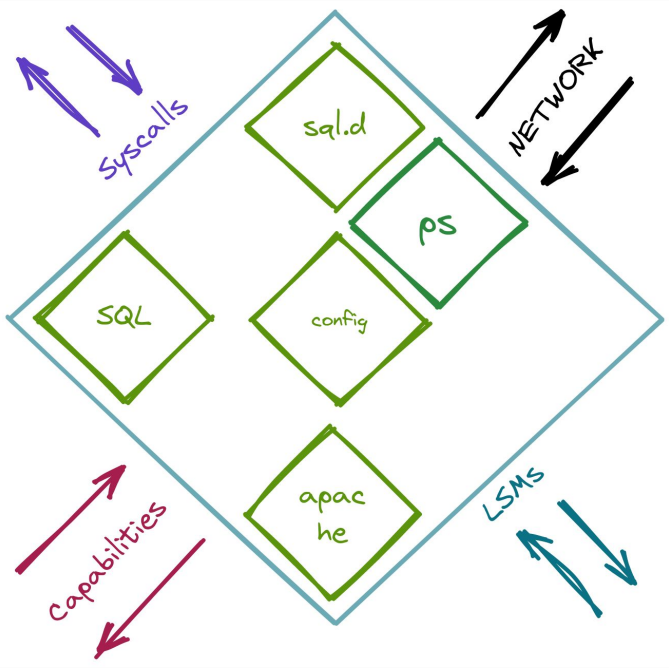
Containers



Back

Next

Lightweight Images

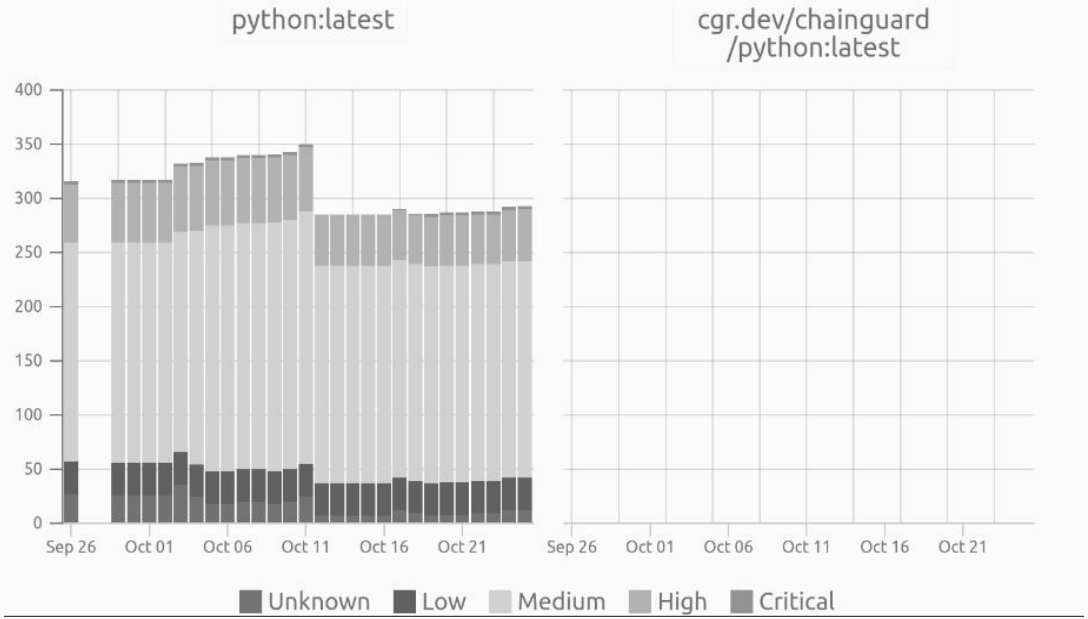


Back

Next

Lightweight Images

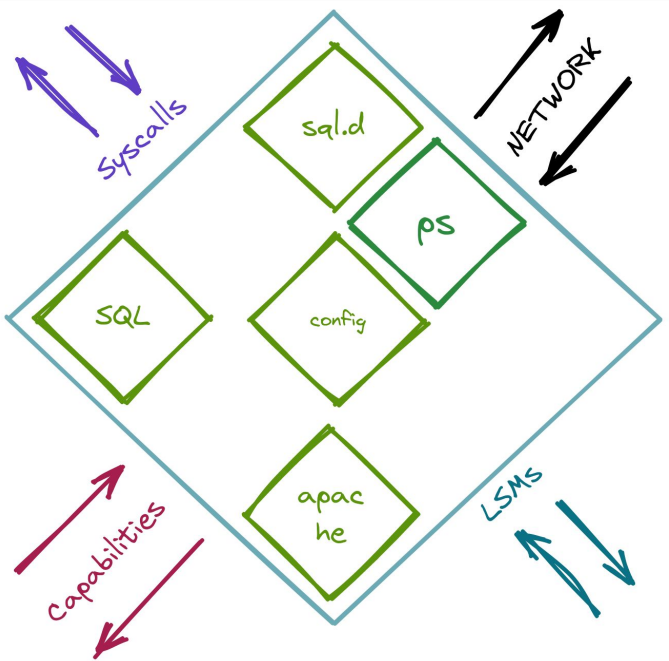
Comparing the latest official Python image with cgr.dev/chainguard/python



Back

Next

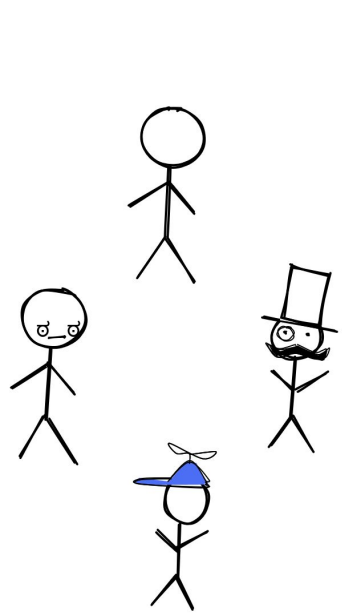
- Kubernetes Security Context
  - LSM Profiles/Labels
  - Seccomp
  - Capabilities
- Docker Security Opts
  - Other Container Runtimes Support this as well
- Proxy Filters/Service Mesh/Container Networking Interface Rules
- Docker Slim to trim down unnecessary filesystem
- Like Node Images use lighted base images for container like alpine, wolfi



Back

Next

Role Based Access Control



Kubernetes API

Docker API

Production

Staging

Development

Back

Next

Uber Social Engineering Attack

- Perimeter Security around Sensitive Files using VPN
- VPN Access protected through Multi Factor Authentication

Back

Next

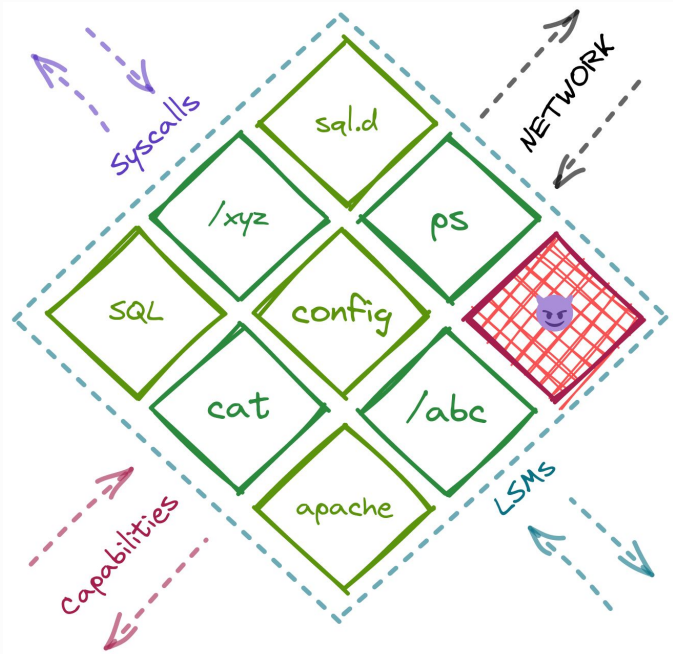
Uber Social Engineering Attack

- MFA breached through Social Engineering
- Attacker Scans Intranet for Sensitive Assets
  - Finds Shell Script with Admin Password to PAM
  - Finds secrets to all services through PAM

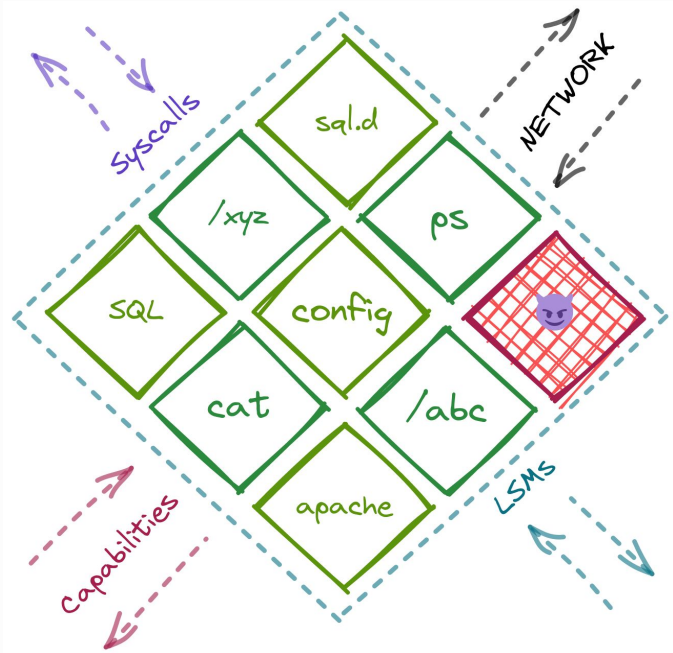
Back

Next

What if
we are already
compromised?



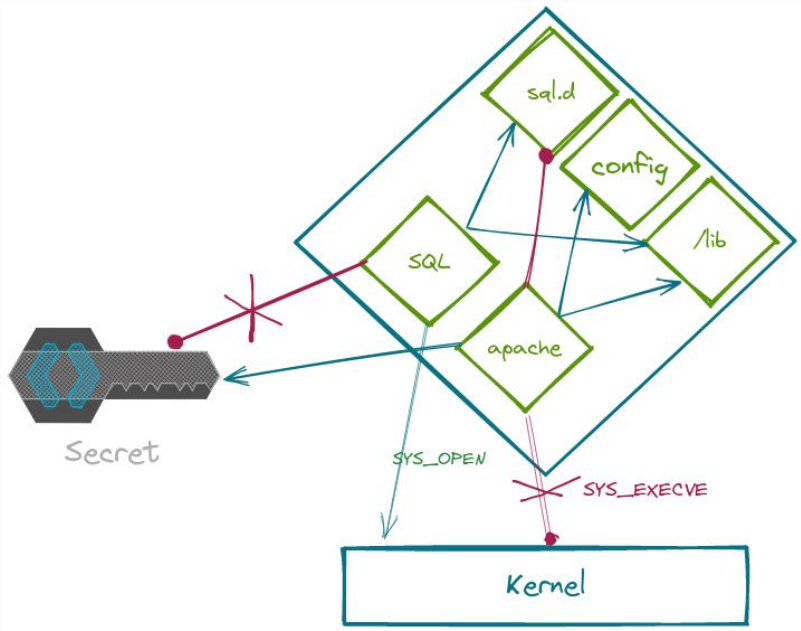
~~What if~~
we are already
compromised



Back

Next

Access Control Inside Containers

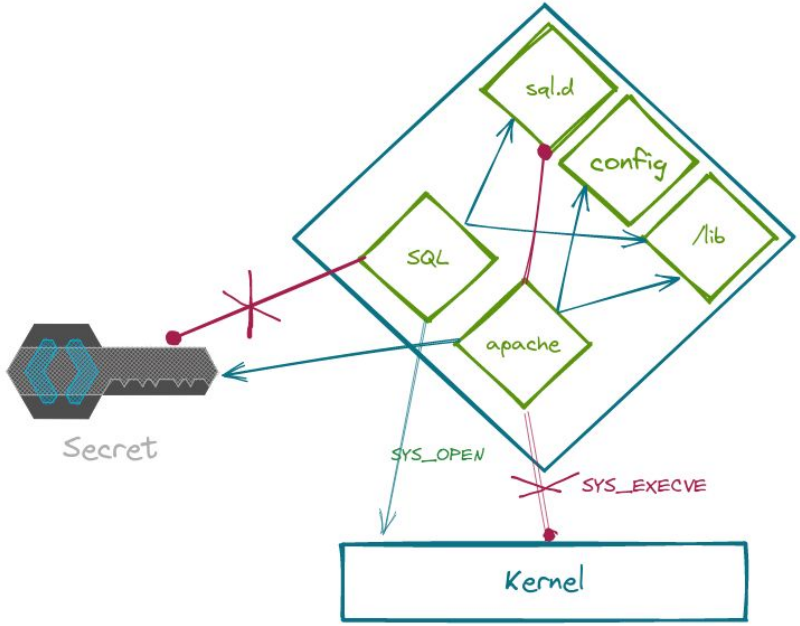


Back

Next

Access Control Inside Containers

- Setup Observability to gain visibility
- Linux Security Modules
- Userspace Interception
  - LD_PRELOAD
  - Ptrace

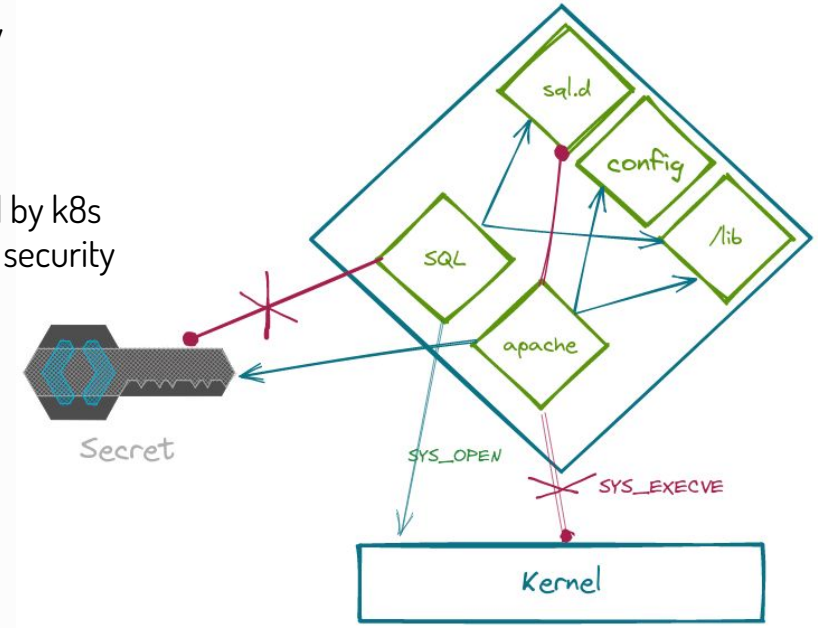


Back

Next

Access Control Inside Containers

- Setup Observability to gain visibility
  - Falco
  - Tracee
- Linux Security Modules
  - AppArmor Rules (supported by k8s security context and docker security opts)
- KubeArmor



Back

Next

Conclusion

Minimalism : Key to Cloud Security

Back

Next

Conclusion

Minimalism : Key to Cloud Security

- Need for Multi Layered Minimalistic Approach
- Minimal Node Images / Runtime Infrastructure
- Setup Perimeter Around Containers to minimize outside access
- Minimize Attack Surface Outside and Inside Containers by removing unnecessary dependencies
- Setup Perimeter Inside Containers to minimize unnecessary accesses
- Minimum Permissions to all users to prevent social engineering attacks

Back

Next

ThankYou

(づ｡◕‿‿◕｡)づ

Back

Next

ThankYou

Questions (づ｡◕‿‿◕｡)づ

Back

Next

kubearmor.io

ThankYou

barun.cc

Questions (づ｡◕‿‿◕｡)づ

Back

Next