COALFIRE RAMPCON

06.09 — 06.10.2025 • WASHINGTON D.C.

Container Hardening:

Hardening containers in a FedRAMP environment

Jason Macallister | Senior Manager / Coalfire
Thomas Kennedy | Senior Consultant / Coalfire
Aaditya Jain | Product Marketing Manager / Chainguard

Agenda

- FedRAMP and Container Hardening Requirements
- Container Hardening Guidelines
- Vulnerability Considerations
- Solutions

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

FEDRAMP IS HARD

Container Hardening:

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

COALFIRE RAMPCON
06.09 — 06.10.2025 • WASHINGTON D.C.

Why?



Compliance is Difficult



Encryption



Continuous Monitoring



Vulnerability Management

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

FedRAMP Container Hardening Requirements

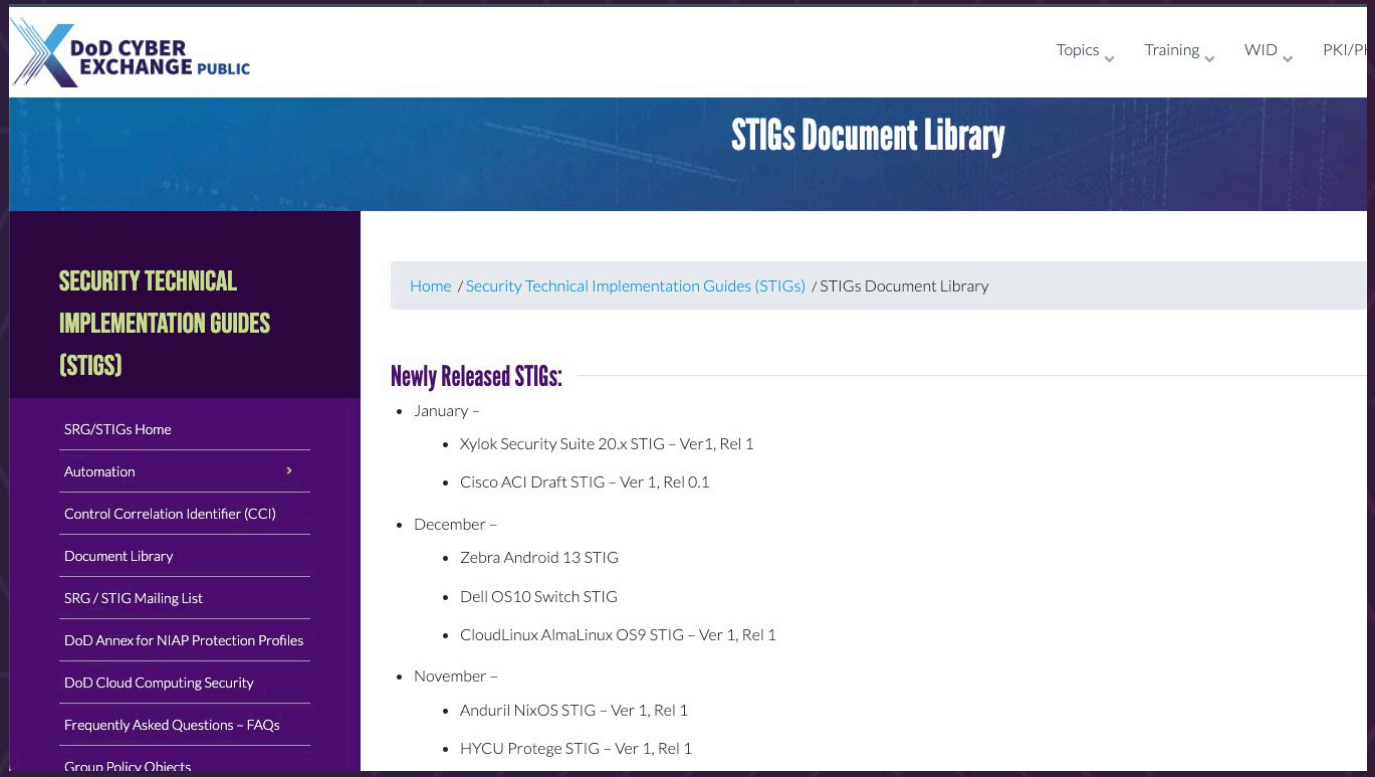


- CSPs must utilize hardened containers for containerized workloads
  - CM-6 (a): "Requirement 1: The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available."
- Benchmarks should align with baseline controls: CM-6, RA-5, SC-2, SC-3, SC-4, SC-28 and SC-39
  - End container hardened image can vary from baseline
  - 3PAO's must validate the CSP's container hardening practice
- Hardened images should not contain known exploited vulnerabilities in production
  - CISA's Known Exploited Vulnerabilities Catalog (KEV Catalog)

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

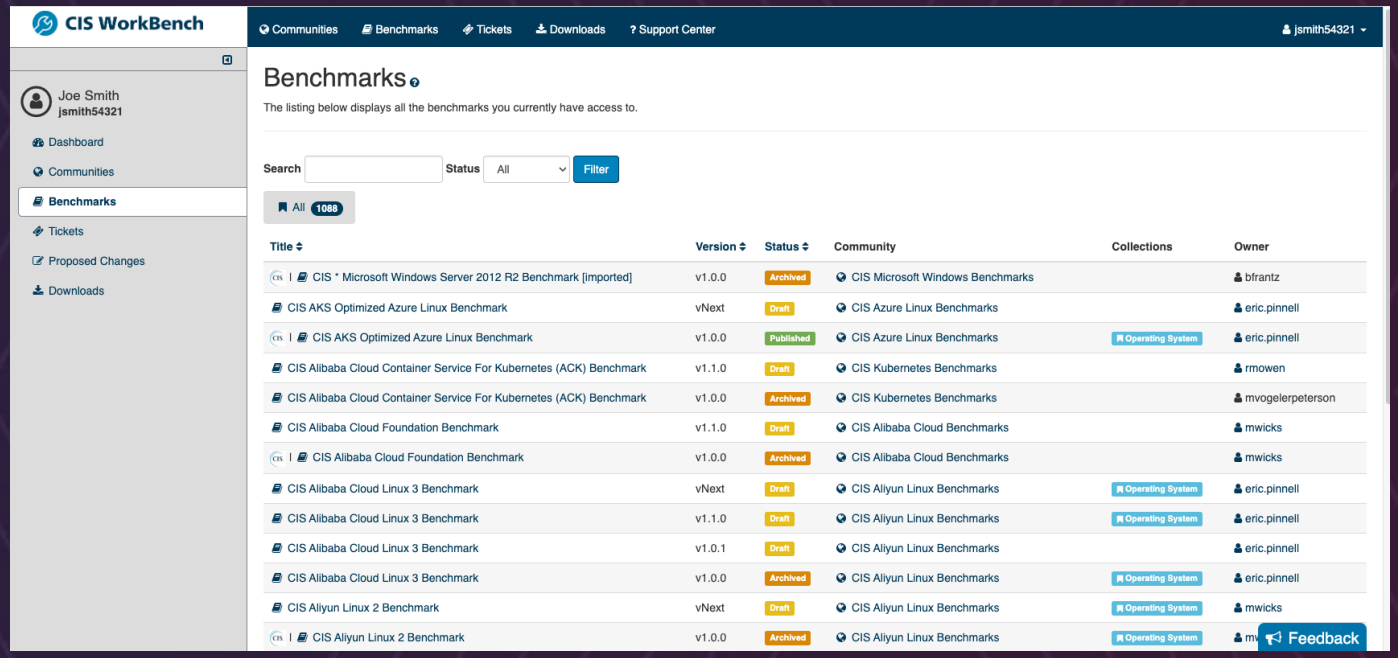
Container Hardening Guidelines - STIGs

- Sourcing STIGs from an approved source
- https://public.cyber.mil/stigs/downloads/
  - DISA provides: Kubernetes STIGs, and OS-level STIGs
  - Compliance baseline in DoD and FedRAMP High/Moderate systems.
- Always check if a STIG exists for your container
- Currently, containerized STIGs are limited



Container Hardening Guidelines – CIS Level 1 and CIS Level 2

- Getting CIS Level 1 and CIS Level 2 from an approved source
- https://workbench.cisecurity.org/
  - Level 1: foundational security controls
  - Level 2: advanced hardening & tighter security
- More CIS benchmarks than DoD STIGs



Vulnerability Considerations

- **Hardened images still need to be scanned for vulnerabilities**
- **Two ways to conduct vulnerability scanning:**
  1. Build pipeline scanning
  2. Runtime scanning
- **Results Show up on the monthly Plan of Action and Milestones (POA&M)**
- **Timeframe to remediate:**
  - High/Critical: 30 days
  - Moderates: 90 days
  - Lows: 180 Days

Solutions - Overview



SOURCE IRON BANK IMAGES



CUSTOM HARDENED IMAGES

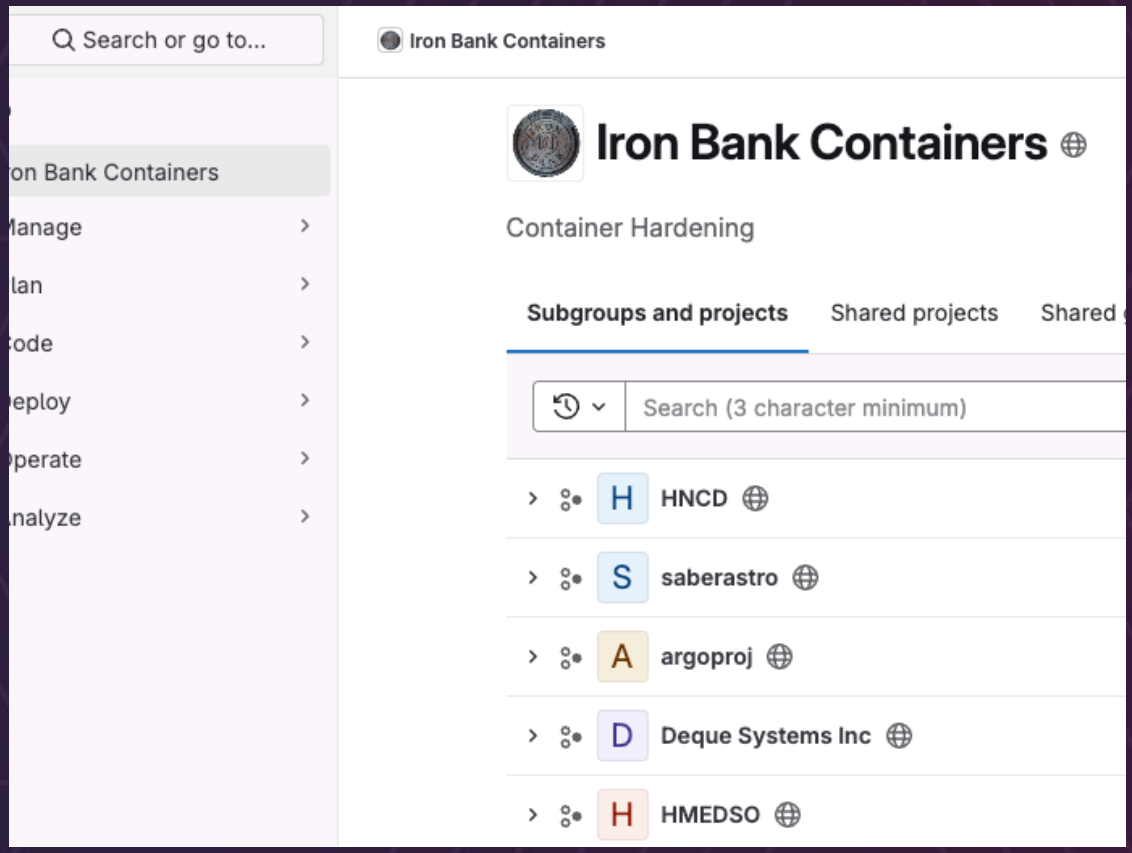


UTILIZE CHAINGUARD IMAGES

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

Solution – Iron Bank Containers

- Iron Bank is a public repo of hardened containers
- https://repo1.dso.mil/dsop
- Over 200 images
- Challenges:
  - Potentially stale repositories
  - Images contain vulnerabilities
  - Vulnerabilities need to be patched according to FedRAMP guidelines

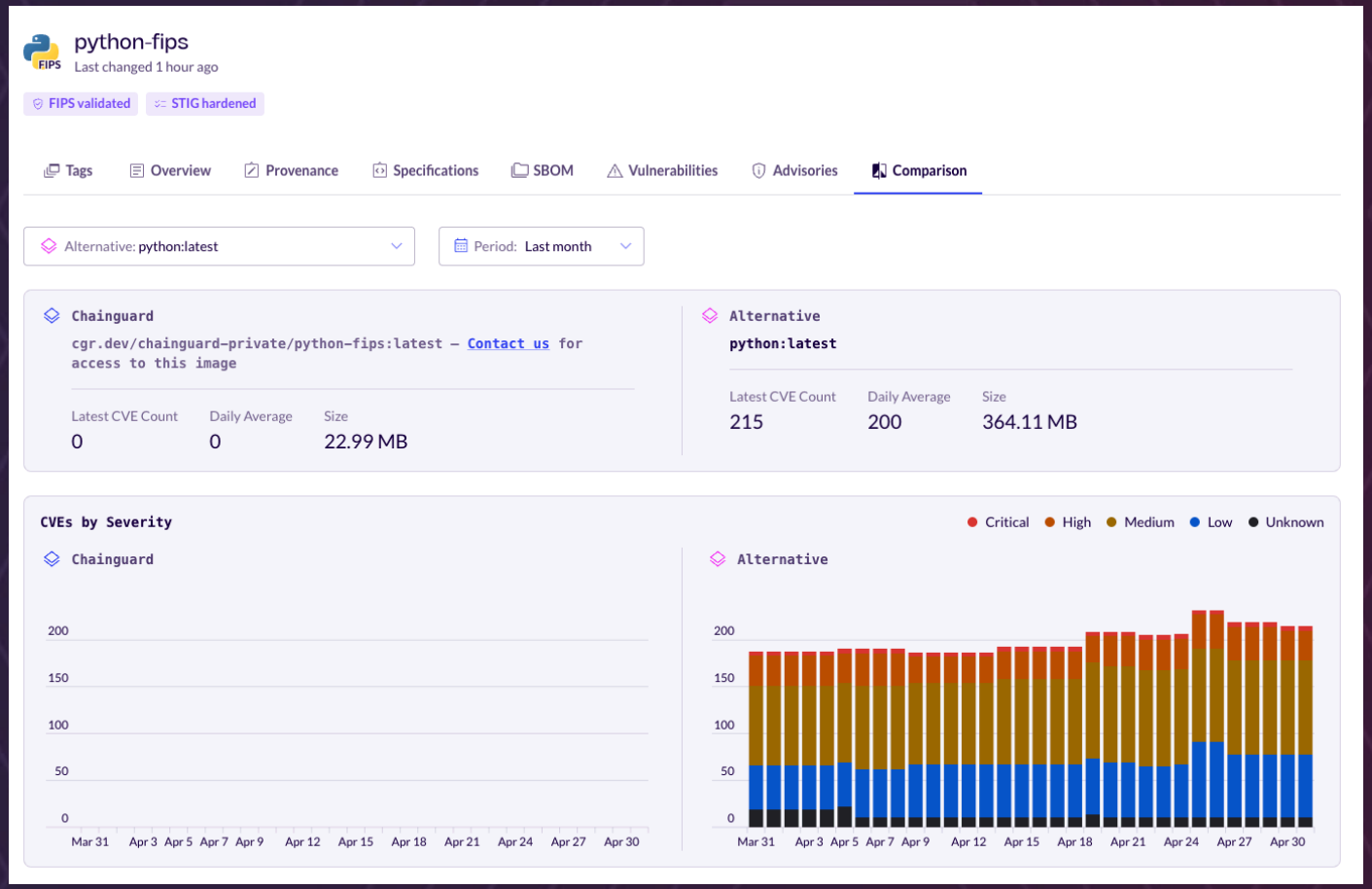


Solution - Custom Container Hardening

- **Must align with FedRAMP Controls CM-6, RA-5, SC-2, SC-3, SC-4, SC-28, and SC-39**
  - Secure Configuration (CM-6)
  - Vulnerability Monitoring and Scanning (RA-5)
  - Separation of duties (SC-2, SC-3)
  - Prevent unauthorized transfer of data (SC-04)
  - Protect information at rest (SC-28)
  - Process isolation (SC-39)
- **STIG or CIS Benchmark Baseline can be altered**
- **Some vendors may provide hardened images**

Solution – Chainguard

- 1,300+ hardened, minimal images that start at zero CVEs and stay there
- SLA for CVE remediation (7 days for critical, 14 for high/med/low)
- 400+ FIPS-validated images
- Paired with OS-Level STIGs
- Build-time SBOMs
- Sigstore Signed

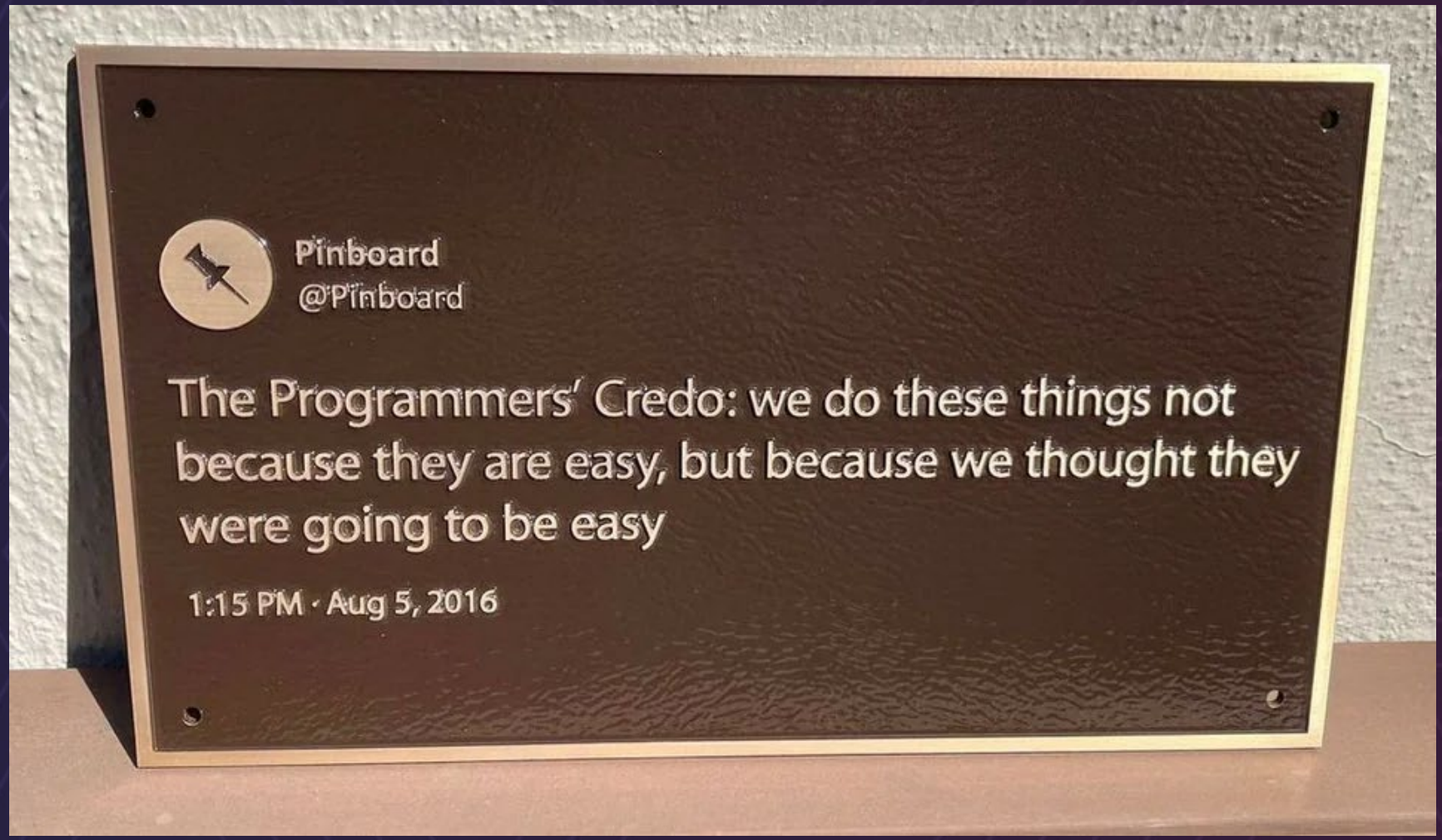


How Chainguard Hardens our Containers – Basics

Some things are simple and regular best practices

- Don’t run containers as root
- Enhanced compiler flags
- Verifiable cryptographic signatures
- Full build-time SBOMs

Others are much harder… so why did we do them?



Container Hardening:

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

But also because Customers and FedRAMP demand it

FedRAMP Control	Overview	Chainguard Coverage
Asset Management	Catalog and track all the assets within the boundary	✅
FIPS Validation	Build and maintain FIPS-validated cryptography	✅
STIG Hardening	Harden and test secure configuration + controls	✅
CVE Elimination	Hardened containers should not have vulnerabilities	✅
CVE Management (POA&M Reporting)	CVE remediation under strict SLAs and reporting all CVEs if they persist	✅

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

Advanced Hardening: Minimal, Purpose-Specific Containers

Minimalism and Purpose-Specific – our containers contain only the components your application needs to run

Building images from source without excess components allows us to start at zero CVEs

But we want to be flexible and extensible too… so we meet customers where and how they build

- Debugging "-dev" variants of containers with a shell and a package manager
- Standard distroless variants that exclude the shell and package manager

Ultimately, we strive to avoid the "kitchen sink" approach taken by other distros

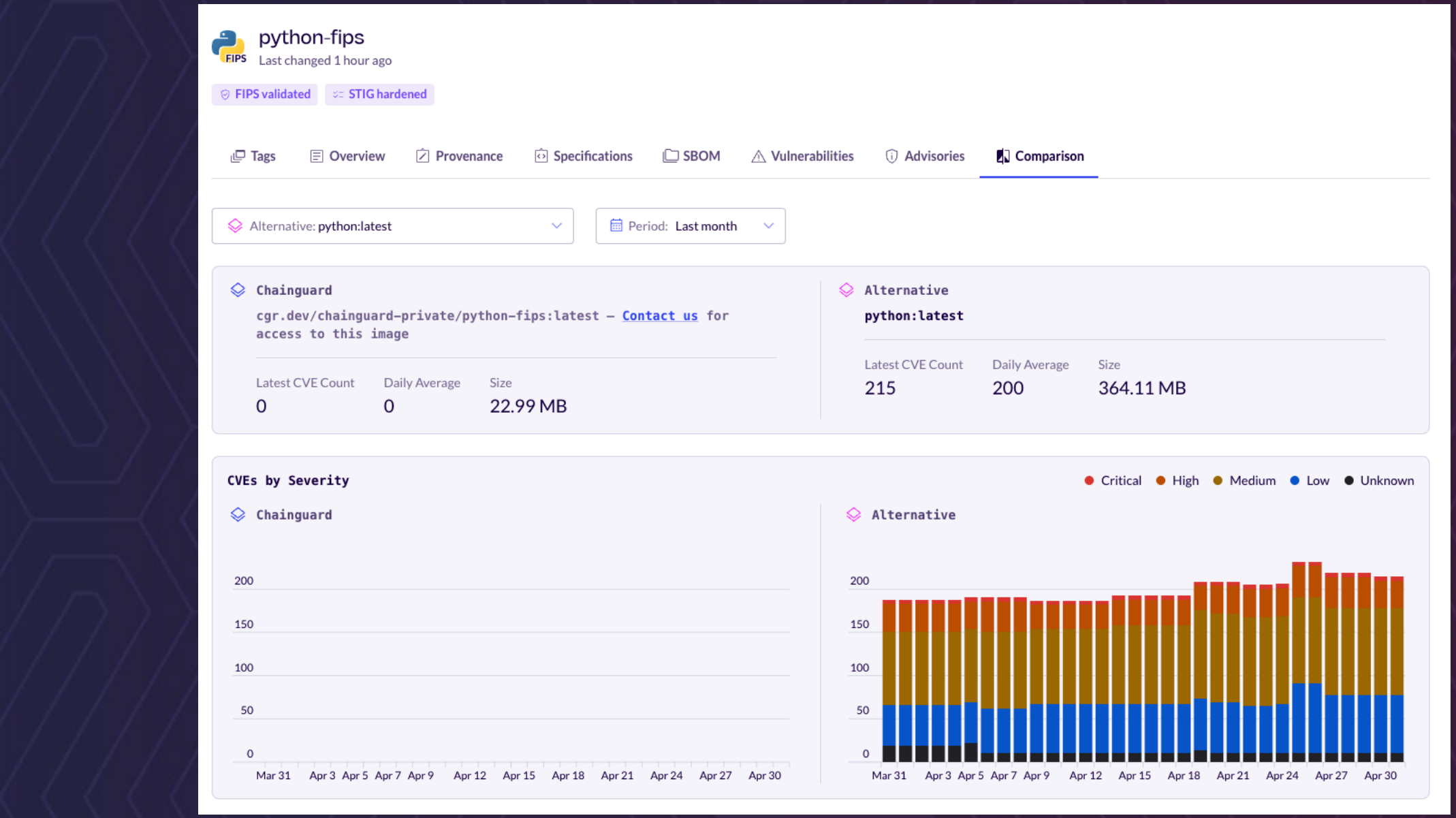
Advanced Hardening: CVE Remediation

CVE Remediation – FedRAMP has an SLA of 30/90/180 days

Chainguard goes even further with our SLA – 7 days for critical, 14 days for high, medium, and low

So not only do our images start at zero CVEs… they accumulate CVEs more slowly, and when they do pop, Chainguard remediates them for you

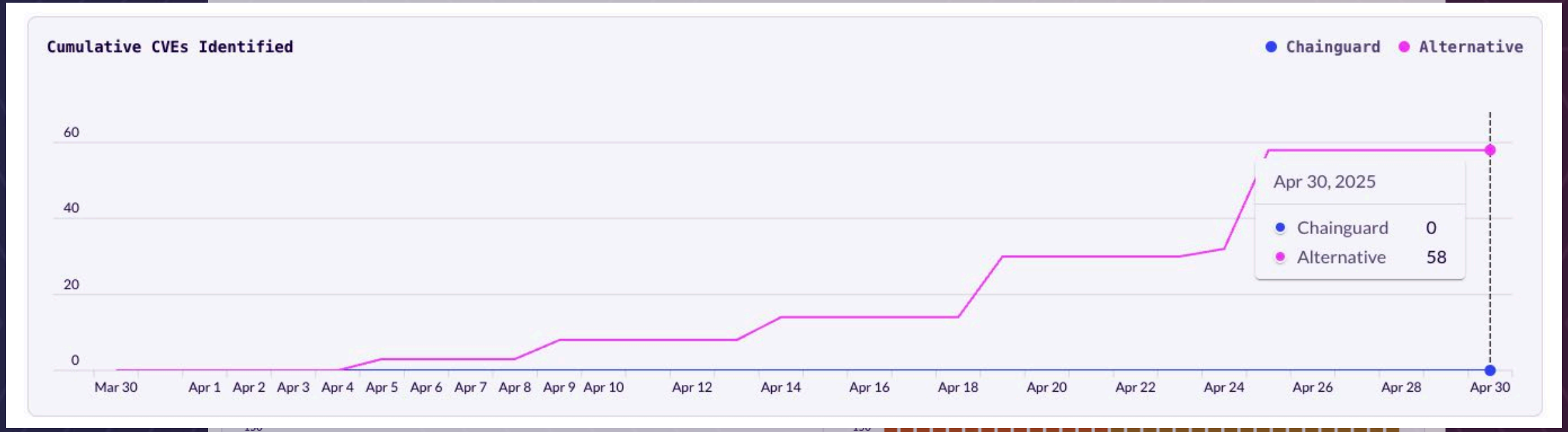
Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard



Container Hardening:

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

COALFIRE RAMPCON
06.09 — 06.10.2025 • WASHINGTON D.C.



Container Hardening:

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

COALFIRE RAMPCON
06.09 — 06.10.2025 • WASHINGTON D.C.

Advanced Hardening: STIGs

General purpose operating system (GPOS) security requirement guide SRG – security requirements for OS running in a network

Presented in XCCDF format and ingestible into a SCAP-validated tool (like OpenSCAP and SCAP Viewer) to ensure compliance and transparency of hardening metrics

Integrations with your existing GRC solutions to make validation and auditing easy

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

Advanced Hardening: FIPS is a Four-Letter Word

Chainguard supports OpenSSL (CMVP #4856), Bouncy Castle (CMVP #4943), and BoringCrypto (CMVP #4407) across almost 400+ FIPS-validated images

Kernel independent FIPS compliance – the entropy source (CPU Time Jitter RNG #E191 Entropy Certificate) resides at the image level instead of the host

That means you can use Chainguard's FIPS-validated container images with any underlying host

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

And now we're even FIPS-ing the Un-FIPS-able





Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

Chainguard aims to be the trusted partner for FedRAMP

FedRAMP Control	Overview	Chainguard Coverage
Asset Management	Catalog and track all the assets within the boundary	Full build-time SBOMs
FIPS Validation	Build and Maintain FIPS-Validated Cryptography	400+ FIPS-validated images
STIG Hardening	Harden and Test Security Controls	General Purpose OS-level STIG
CVE Elimination	Hardened containers should not have vulnerabilities	Containers start at zero CVEs and have slower CVE accumulation rate
CVE Management (POA&M Reporting)	CVE remediation under strict SLAs and reporting all CVEs if they persist	7 days for critical, 14 days for high/med/low

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

Q&A

Jason Macallister & Thomas Kennedy | Coalfire Cloud Services
Aaditya Jain | Chainguard

REFERENCE SLIDES

References

- CSP_Vulnerability_Scanning_Requirements - Includes content on container hardening FedRAMP Security Controls Baseline
- KEV Catalog