



On Demand Webinar

Introducing a Security Feedback Loop to your CI Pipelines

Matthew Barker | Twistlock

Dustin Van Buskirk | Codefresh

Varun Tagore Korrapati | Steelcase



Matthew Barker
Senior Solutions Architect





Dustin Van Buskirk
Senior Solutions Architect





Varun Tagore Korrapati
DevOps Engineer

Steelcase

How to Implement Security Scanning with Codefresh and Twistlock

- How Twistlock Improves Security
- Why Steelcase uses Security Scanning in their CI Pipelines
- How Codefresh Automation Works
- DEMO!
Twistlock CLI / Docker image scanning as part of your Codefresh pipelines.

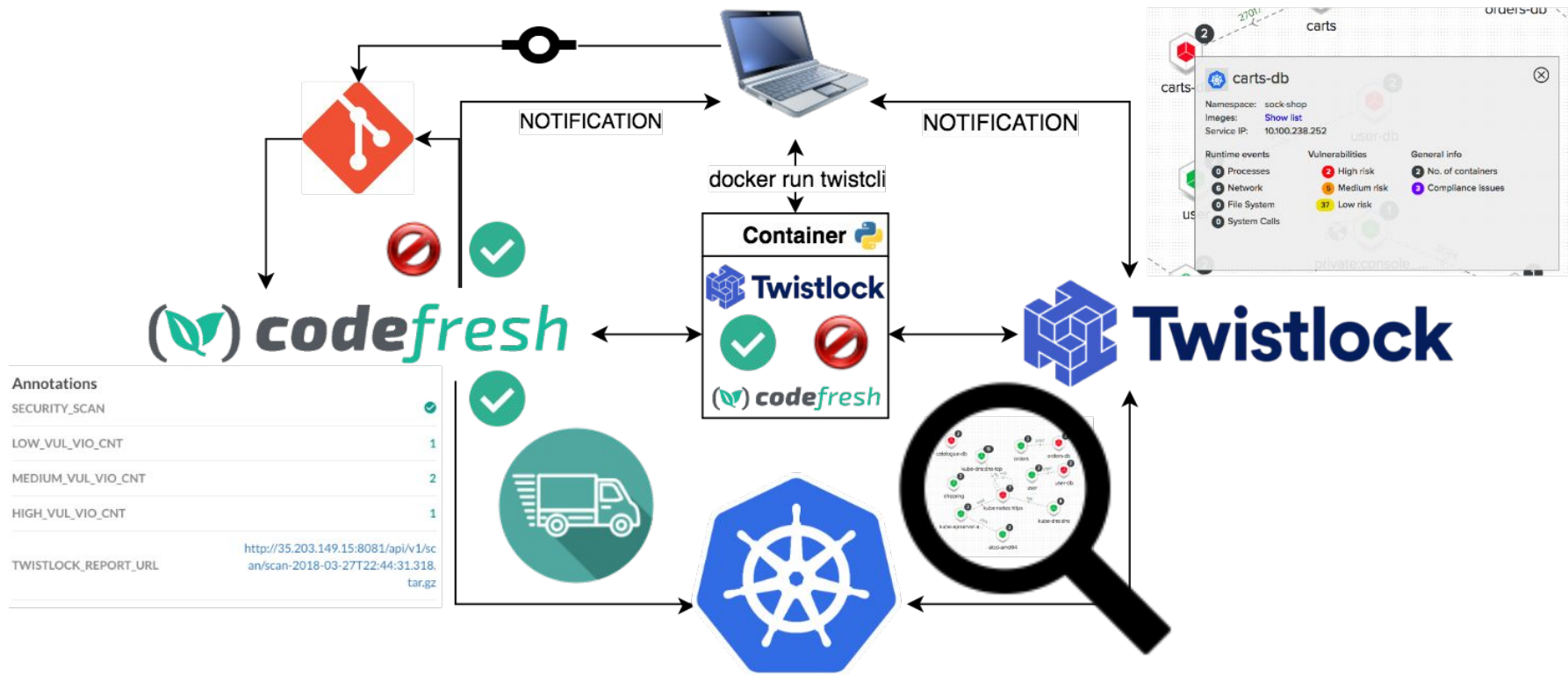
Steelcase



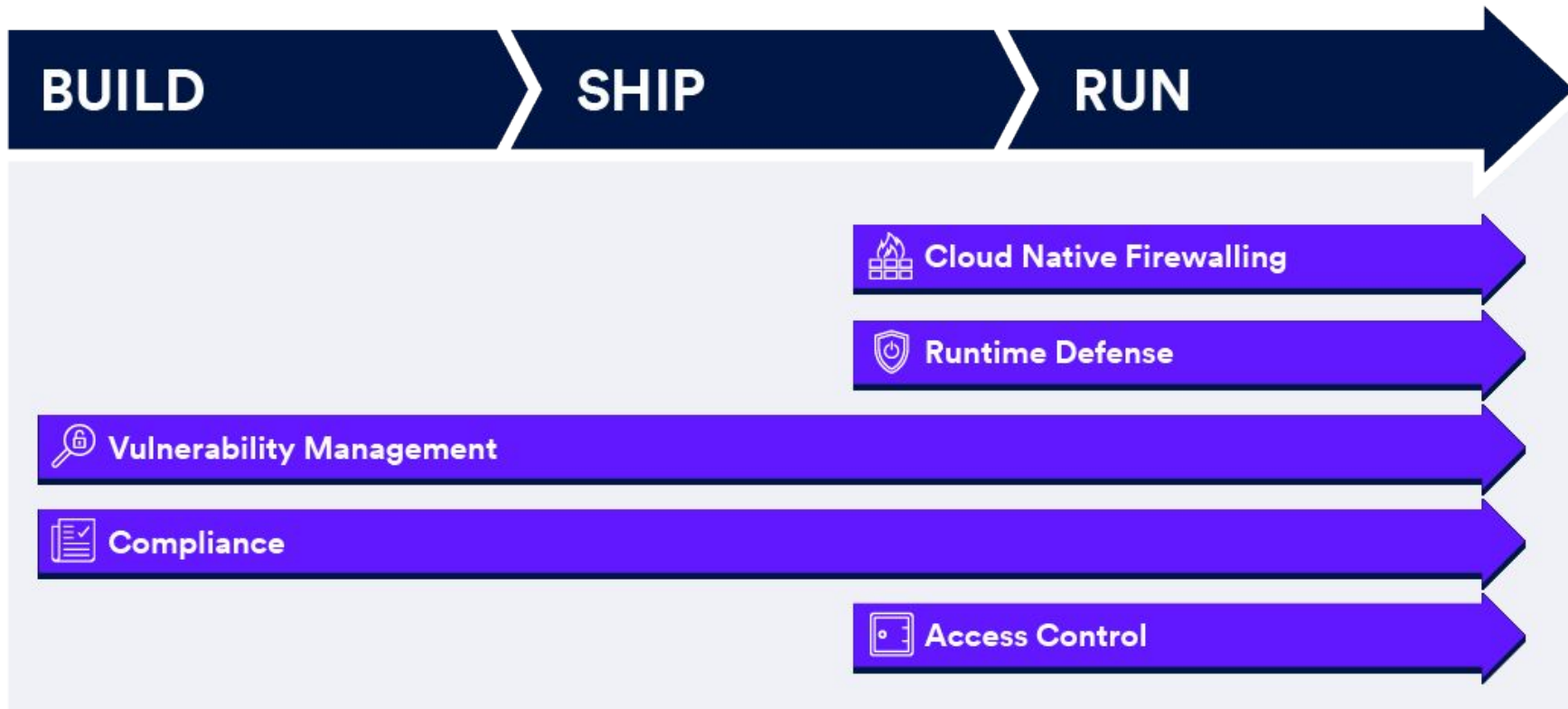
- Steelcase is a 106 year old furniture company.
- Steelcase also offers a various services like Workplace Advisor.
- Thousands of IOT devices deployed.
- Fortune 500 Customers.

Privacy is critical!

Steelcase



Introducing the Twistlock Platform



Security scanning is a critical part of vulnerability management:

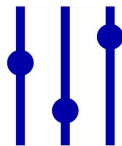
- 1 Reduce cost compared to fixing flaws in production
- 2 Eliminate high or critical vulnerabilities as soon as possible
- 3 Improved code quality helps avoid costly breaches

Advantage of scanning with Twistlock



Accuracy:

Fewer false positives and negatives



Control:

Set thresholds based on vulnerability or compliance status



Fix status:

Put remediation information in developers' fingertips

What thresholds can I set with Twistlock?

Alert or block specific package based on specific vulnerability level

Example 1: Block all High vulnerabilities in XXXX library

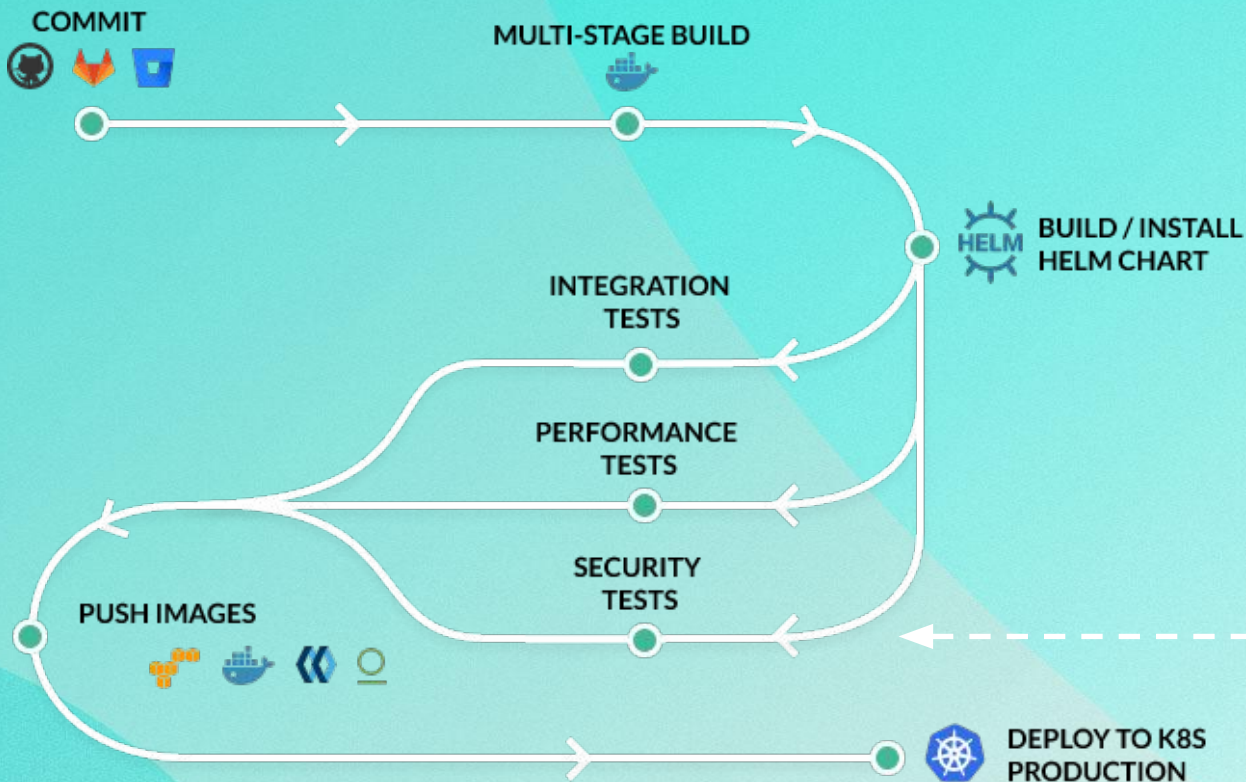
Alert or block specific builds based on compliance issues

Example 2: Alert on builds that have Medium or higher compliance issues

Incorporate status of fixes for added control

Example 3: Block all builds Medium or higher that have a known fix

Where does Twistlock integrate with Codefresh?



Why Codefresh?



Adopting Kubernetes by cobbling together lots of tools and scripts is costly and time consuming

- Build servers
- Staging servers
- Build automation
- Webhooks
- Docker registry
- Kubectl
- Helm
- CI Tests
- Integration Tests
- UI Tests
- Performance Tests
- Security Scans
- Deployment tools
- Secrets management
- Configuration testing
- Traceability
- Dashboards

Codefresh is a DevOps Platform Built for Kubernetes



**Kubernetes
CI/CD Pipelines**



**Self-Service Test
Environments**



**Release
Management**



**Docker & Helm
Registry**

Steelcase Use Cases

Before/Why?

- how much security is enough security?
- No security implementation in code and docker container configuration?
- Hard to control what security standards and practices are followed when there are multiple developer teams working on different applications.
- Get unified security standards for all the microservices.
- ?Secure application from within.

Why Automate:

- Catch up with Security ask!
- Doesn't satisfy the laws of DevOps speed.
- Scan the images before they go to production or even master.
- Fast and Secure development with continued feedback.
- In microservice model, faster onboarding of a secure microservice with no compromise in security standards.
- Less security patch releases to production.

Now

- Automated security scan in protected branches.
- Logical conditions to run it in other specific branches.
- All new microservices have to have security steps configured in CI build.

Next

- Fail the CI build if the results cross threshold.
- Block the merge or PR to protected branch when results crosses thresholds for security and compliance.

DEMO



Twistlock / Codefresh Integration

- Docker image containing Twistlock CLI, Codefresh CLI and Python scripting to tie the two together.
- Runs locally and on Codefresh (Docker Swarm or K8S)
- Adds Docker image metadata (Annotations)
 - Compliance and Vulnerability counts for each level [critical, high, medium, low]
 - Security Scan results Pass/Fail
 - Twistlock Report URL
- Determine Build Success or Failure based on exit code of the Twistlock scan and pass that back to Version Control System

<https://github.com/SC-TechDev/docker-twistcli>

CHECK OUT OUR BLOG POST:
codefresh.io/blog



Twistlock™

Talk to Twistlock

[Sign up for a Free Trial!](#)

[@ Twistlock.com](#)



Get a Codefresh Demo

[Schedule 1:1](#)

[@ Codefresh.io](#)

Thank You For Joining Us