chainguard

Cloud Native, AI Native 환경을 위한,

Zero CVE 솔루션

OSC

sales@osckorea.com

기존 오픈소스 취약점 관리의 한계

chainguard

빠르게 누적되는 CVEs

의존성에 대한 패치가 배포판 업데이트에 반영되는데 수개월 소요됨

공개된 이미지의 한계

전반적인 보안 표준화를 위해서는 직접 빌드와 하드닝을 수행할 수밖에 없음

Zero-day 리스크 노출

불필요한 OSS 아티팩트로 인해 Zero Day 위협에 노출되어 있음

공급망을 통한 악성 공격 증가

연간 수십만건의 악성 패키지가 다양한 공급망을 통해 유포됨

OSC

CVE 관리 비용 및 리스크

chainguard

반복되는 CVE 점검 및 패치

새로운 버전이 나올 때 마다 끊임없는 패치작업과 테스트/검증 과정이 요구됨

제한된 인력을 통한 골든 이미지 관리

엔지니어 및 자동화 한계로 인해 이미지 관리에 한계가 있음

패치 작업의 한계

의존성에 대한 주체가 없는 경우가 많고 알려지지 않은 Zero-Day에 대한 패치가 존재하지 않음

사이버 공격에 노출

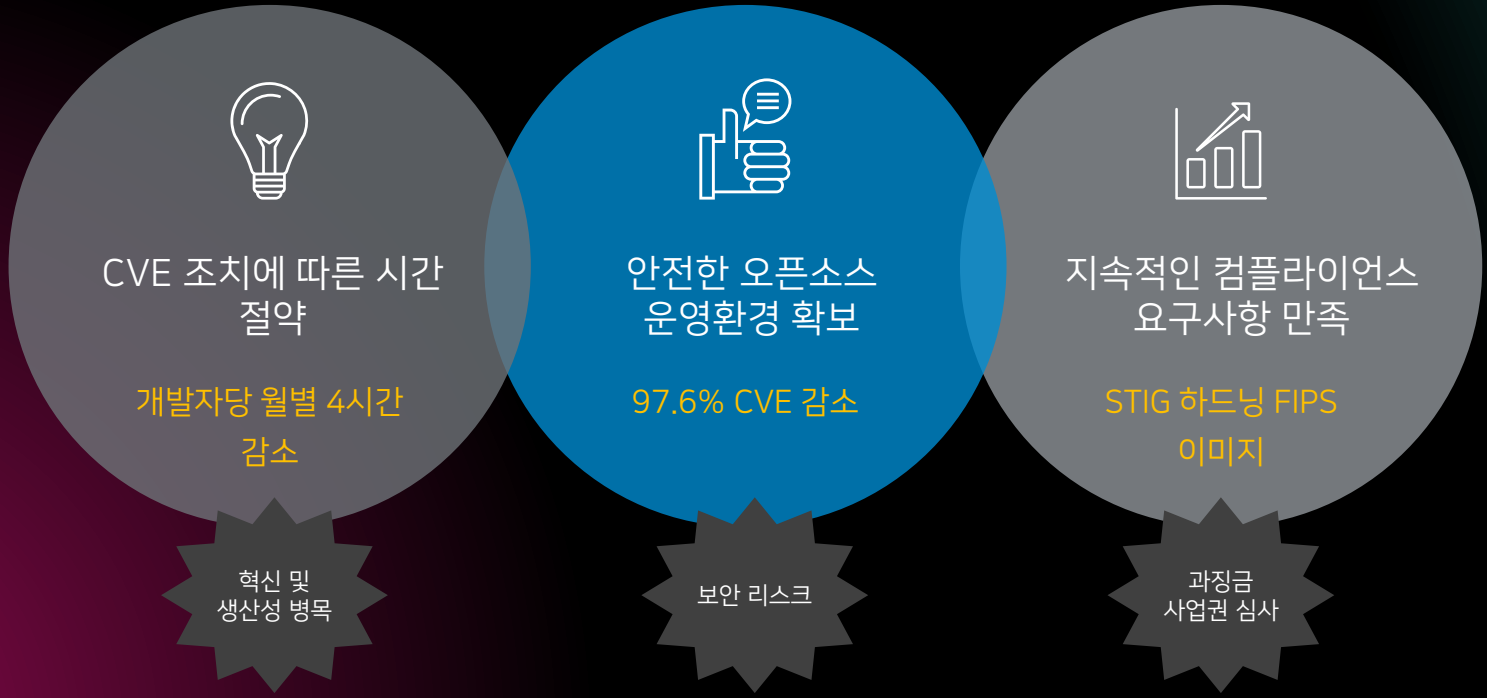
불필요한 취약점 노출로 인해 효율적인 예방이 어려움

OSC

Chainguard 컨테이너 이미지 서비스

chainguard

"Upstream 프로젝트 소스에서 직접 빌드한 안전한 Zero CVE 컨테이너 이미지를 지속적으로 제공합니다"



OSC

Chainguard 투자 유치 이력 (누적 투자 : $612M)

chainguard

Chainguard raises $50M in Series A to make software supply chain secure by default, introduces secure container base images

Chainguard, Inc.
June 2, 2022

시리즈 A (675억)
안전한 소프트웨어 공급망을 위한 보안 컨테이너 베이스 이미지

Chainguard raises $61 million series B round as enterprises move to fortify open source software

Chainguard
November 1, 2023

시리즈 B (823억)
기업의 오픈소스 소프트웨어 보안 강화

Chainguard Raises $140 Million in Series C Funding to Secure the Next Frontier of AI Workloads

Chainguard
July 25, 2024

시리즈 C (1,890억)
AI 워크로드의 보안 강화

Announcing Chainguard's Series D: Building the Safe Source for All Open Source

Dan Lorenc, CEO
April 23, 2025

시리즈 D (4,800억)
안전한 오픈소스 제공
기업가치 : 약4.75조원 ($3.5B)

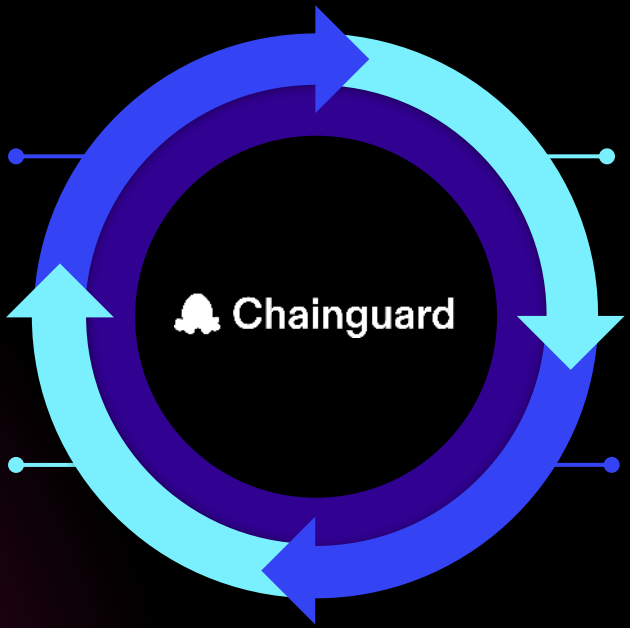
OSC

Chainguard OS & Chainguard Factory

chainguard

소스로부터 Daily 빌드

- 모든 이미지 새로 빌드
- 모든 패키지는 소스로부터 컴파일
- 완전한 통제 및 출처 (Control & Provenance)



의존성 통제

- 의존성 트리내 모든 버전 업그레이드 (OS, toolchain, libraries, application)
- 최소 의존성 최적화

엄격한 테스트

- 단위테스트 및 인수테스트
- 오픈소스 프로젝트에 대해 혁신적인 테스트 프레임워크 보유
- 호환성 보장

첨단 자동화

- 자동화된 AI 기반의 소스코드 변경 탐지, CVE 조치, 의존성 버전 업그레이드
- 10,000+ 오픈소스 프로젝트, 1,400+ 이미지에 대해 자동 리빌드

OSC

Chainguard Factory

chainguard

Continuous Integration

- Analyze (actions)
- Wolfictl Lint
- Lint
- Analyze (java-kotlin)
- Analyze (javascript-typescript)
- Analyze (python)
- **CodeQL** No new alerts in code changed by this pull request
- **Enforce - Commit Signing** Successfully verified commit signature.
- **Package Update Config Check** Package Update Config Check
- **Trust Policy Validation** Valid trust policy.
- **Wiz Data Scanner** Wiz Data Scanner
- **Wiz IaC Scanner** Wiz IaC Scanner
- **Wiz Secret Scanner** Wiz Secret Scanner
- **Wiz Vulnerability Scanner** Wiz Vulnerability Scanner
- **ci-apk-add** ci-apk-add
- **ci-cve-scan** CVE scan report
- **ci-diff-report** Package diff
- **ci-mal-report** malcontent scan complete
- **ci-so-check** ABI compatibility check
- **elastic-build** APKs built successfully

OSC

Chainguard 의 가치 (Value)

chainguard

- 1,400+ 개의 Zero (최소) CVE 이미지 제공
- 5,000+개의 버전 태그
- Daily 업데이트 – 소스로부터 직접 패치

Safe Source For Open Source

Upstream 소스 직접 빌드
초경량 이미지로 CVE 발생가능성 최소화

Infrastructure App Coverage

클라우드 네이티브 환경에서 필요한 각종
어플리케이션 지원

Supply Chain Provenance & Verification

모든 빌드에 대해 SBOM, 증명(Attestation),
서명, SLSA 보안 프레임워크 지원

Vulnerability SLA

Critical CVE에 대한 7일 SLA
(High/Medium/Low : 14일)

Seamless Integration

기존 보안 스캐너, SCA 도구와 이음새
없는 정합

Enterprise Customization

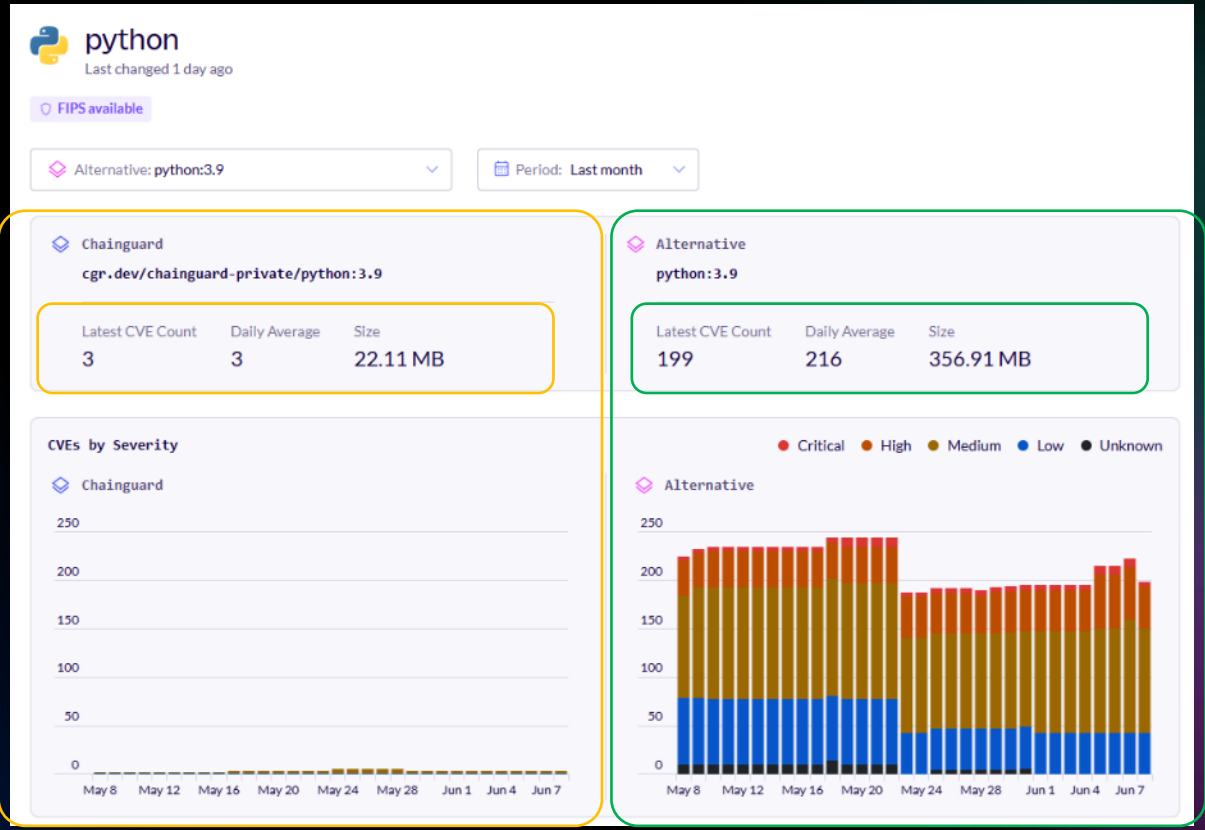
맞춤형 이미지 제작을 위한 다양한
베이스 이미지 제공

OSC

Chainguard 이미지 vs. 표준 이미지

chainguard

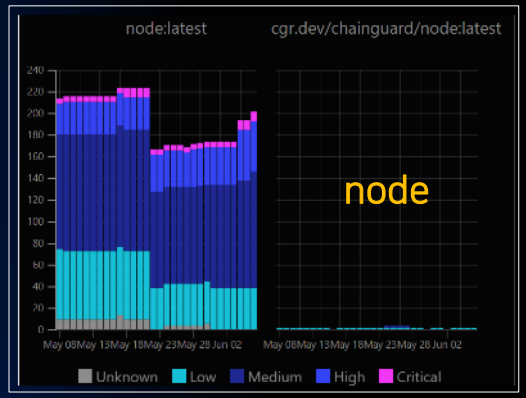
Chainguard 이미지



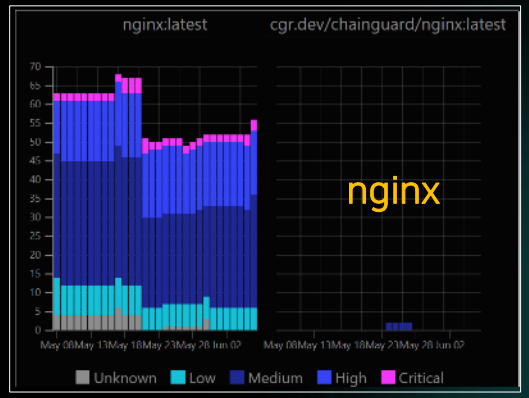
표준 이미지

표준 이미지 vs. Chainguard 이미지

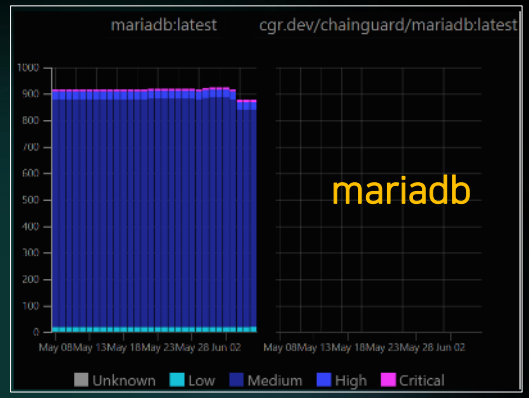
chainguard



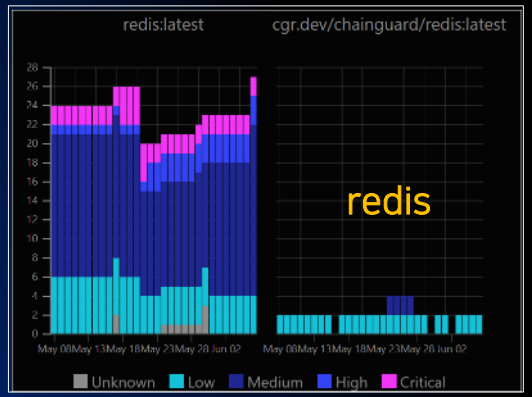
표준 이미지 Chainguard 이미지



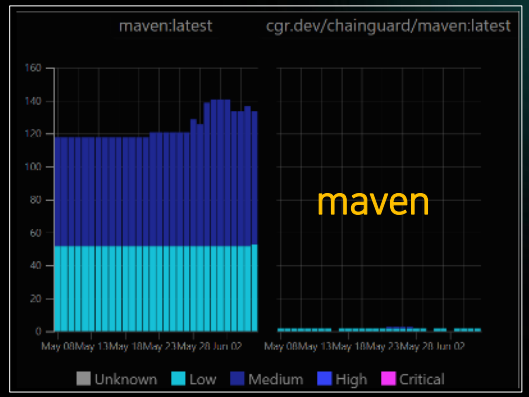
표준 이미지 Chainguard 이미지



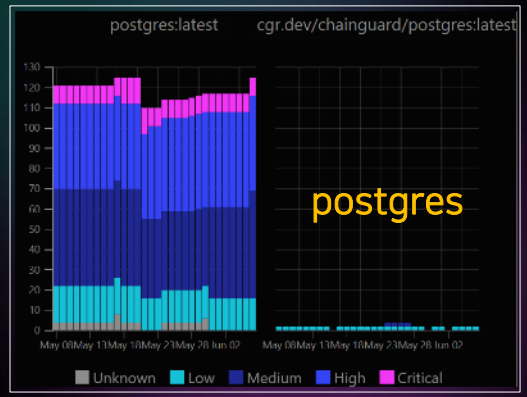
표준 이미지 Chainguard 이미지



표준 이미지 Chainguard 이미지



표준 이미지 Chainguard 이미지

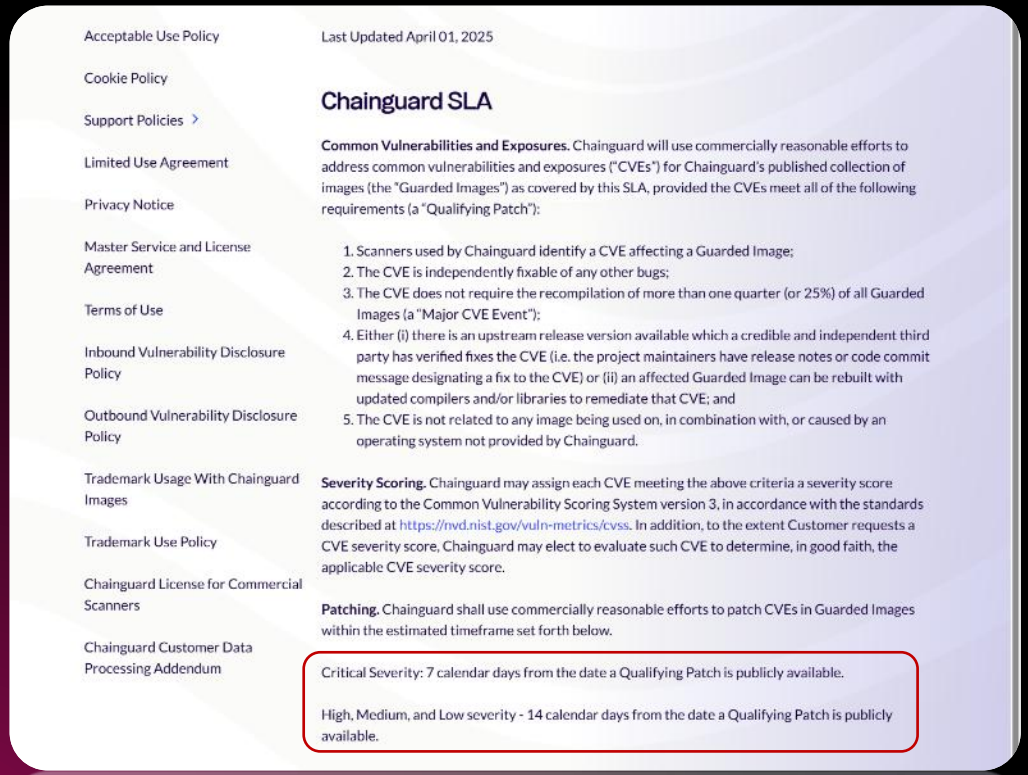


표준 이미지 Chainguard 이미지

OSC

CVE SLA

https://www.chainguard.dev/legal/cve-sla



Acceptable Use Policy
Cookie Policy
Support Policies
Limited Use Agreement
Privacy Notice
Master Service and License Agreement
Terms of Use
Inbound Vulnerability Disclosure Policy
Outbound Vulnerability Disclosure Policy
Trademark Usage With Chainguard Images
Trademark Use Policy
Chainguard License for Commercial Scanners
Chainguard Customer Data Processing Addendum

Last Updated April 01, 2025

Chainguard SLA

Common Vulnerabilities and Exposures. Chainguard will use commercially reasonable efforts to address common vulnerabilities and exposures ("CVEs") for Chainguard's published collection of images (the "Guarded Images") as covered by this SLA, provided the CVEs meet all of the following requirements (a "Qualifying Patch"):

1. Scanners used by Chainguard identify a CVE affecting a Guarded Image;
2. The CVE is independently fixable of any other bugs;
3. The CVE does not require the recompilation of more than one quarter (or 25%) of all Guarded Images (a "Major CVE Event");
4. Either (i) there is an upstream release version available which a credible and independent third party has verified fixes the CVE (i.e. the project maintainers have release notes or code commit message designating a fix to the CVE) or (ii) an affected Guarded Image can be rebuilt with updated compilers and/or libraries to remediate that CVE; and
5. The CVE is not related to any image being used on, in combination with, or caused by an operating system not provided by Chainguard.

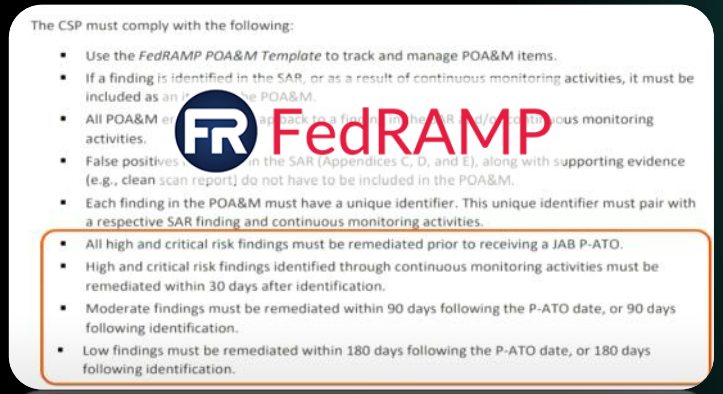
Severity Scoring. Chainguard may assign each CVE meeting the above criteria a severity score according to the Common Vulnerability Scoring System version 3, in accordance with the standards described at https://nvd.nist.gov/vuln-metrics/cvss. In addition, to the extent Customer requests a CVE severity score, Chainguard may elect to evaluate such CVE to determine, in good faith, the applicable CVE severity score.

Patching. Chainguard shall use commercially reasonable efforts to patch CVEs in Guarded Images within the estimated timeframe set forth below.

Critical Severity: 7 calendar days from the date a Qualifying Patch is publicly available.

High, Medium, and Low severity - 14 calendar days from the date a Qualifying Patch is publicly available.

	Chainguard	FedRAMP
Critical	7일	30일
High	14일	30일
Medium	14일	90일
Low	14일	180일

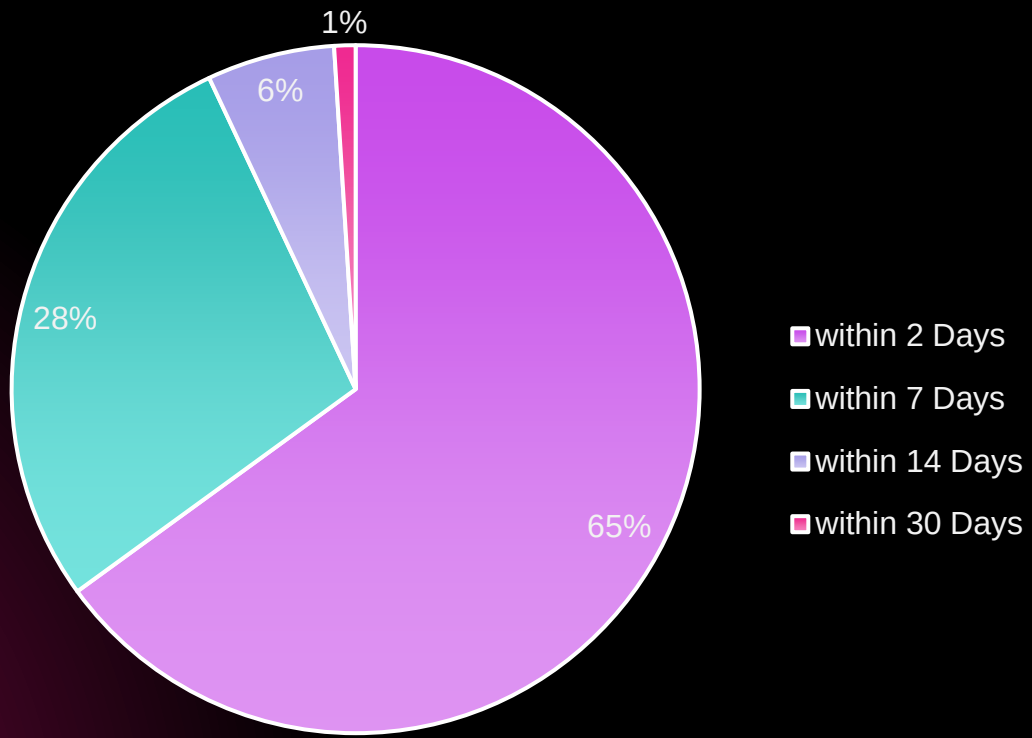


The CSP must comply with the following:

- Use the *FedRAMP POA&M Template* to track and manage POA&M items.
- If a finding is identified in the SAR, or as a result of continuous monitoring activities, it must be included as an
- All POA&M
- False positives
- Each finding in the POA&M must have a unique identifier. This unique identifier must pair with a respective SAR finding and continuous monitoring activities.
- All high and critical risk findings must be remediated prior to receiving a JAB P-ATO.
- High and critical risk findings identified through continuous monitoring activities must be remediated within 30 days after identification.
- Moderate findings must be remediated within 90 days following the P-ATO date, or 90 days following identification.
- Low findings must be remediated within 180 days following the P-ATO date, or 180 days following identification.

FedRAMP

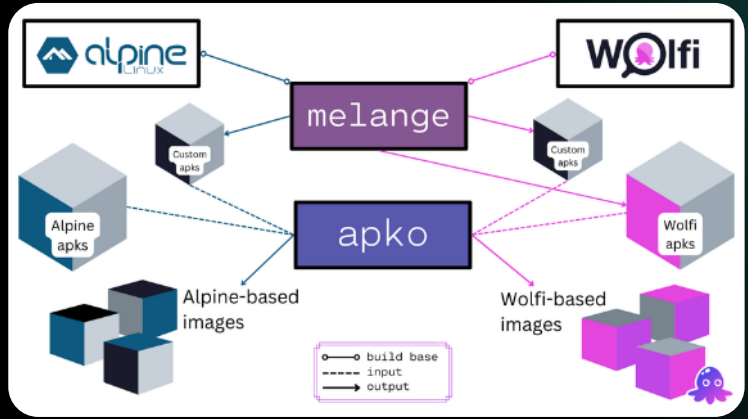
CVE Fix에 소요된 시간 통계



Zero CVE Secret #1 - Wolfi

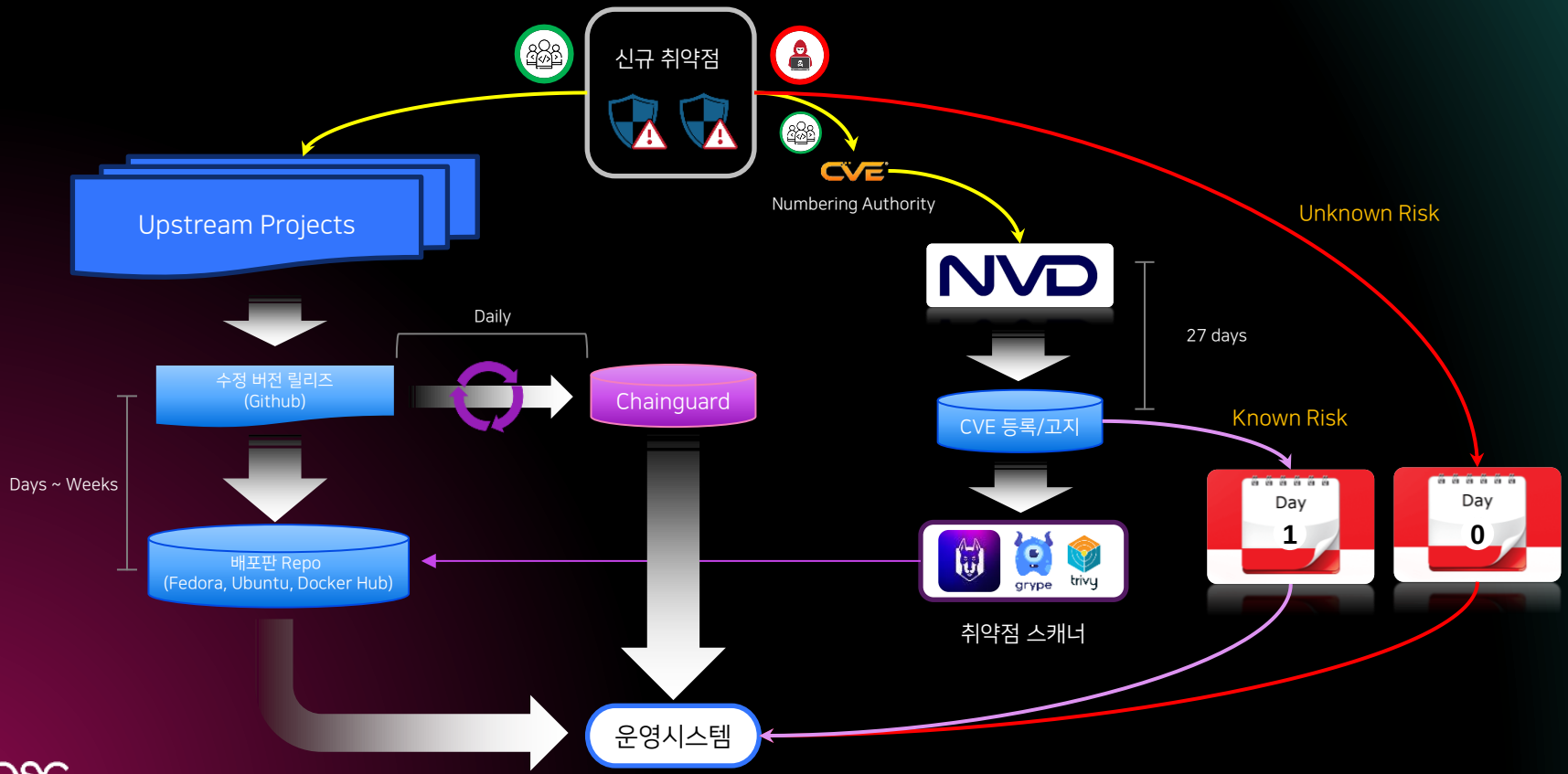
chainguard

- Wolfi
  - ✓ 컨테이너 동작에 필요한 최소한의 패키지만 포함된 리눅스 배포판 (Undistro)
  - ✓ apk (Alpine Package Manager) 기반
  - ✓ glib-c 기반 (Alpine의 경우 MUSL 사용으로 호환성 부족)
- Melange
  - ✓ 패키지는 YAML로 정의되고 Melange (apk 빌드 툴)로 빌드됨
- Apko
  - ✓ OCI 이미지 빌더
  - ✓ SBOM 자동생성



Zero CVE Secret #2 – 소스 모니터링 및 빌드

chainguard



2%

Your team's code

98%

Not your code (open source)

python

Java

GO

node

cilium

MariaDB

Grafana

kubernetes

2%

Your team's code

98%

Not your code (open source)

chainguard

Guarded from CVEs

python

Java

GO

node

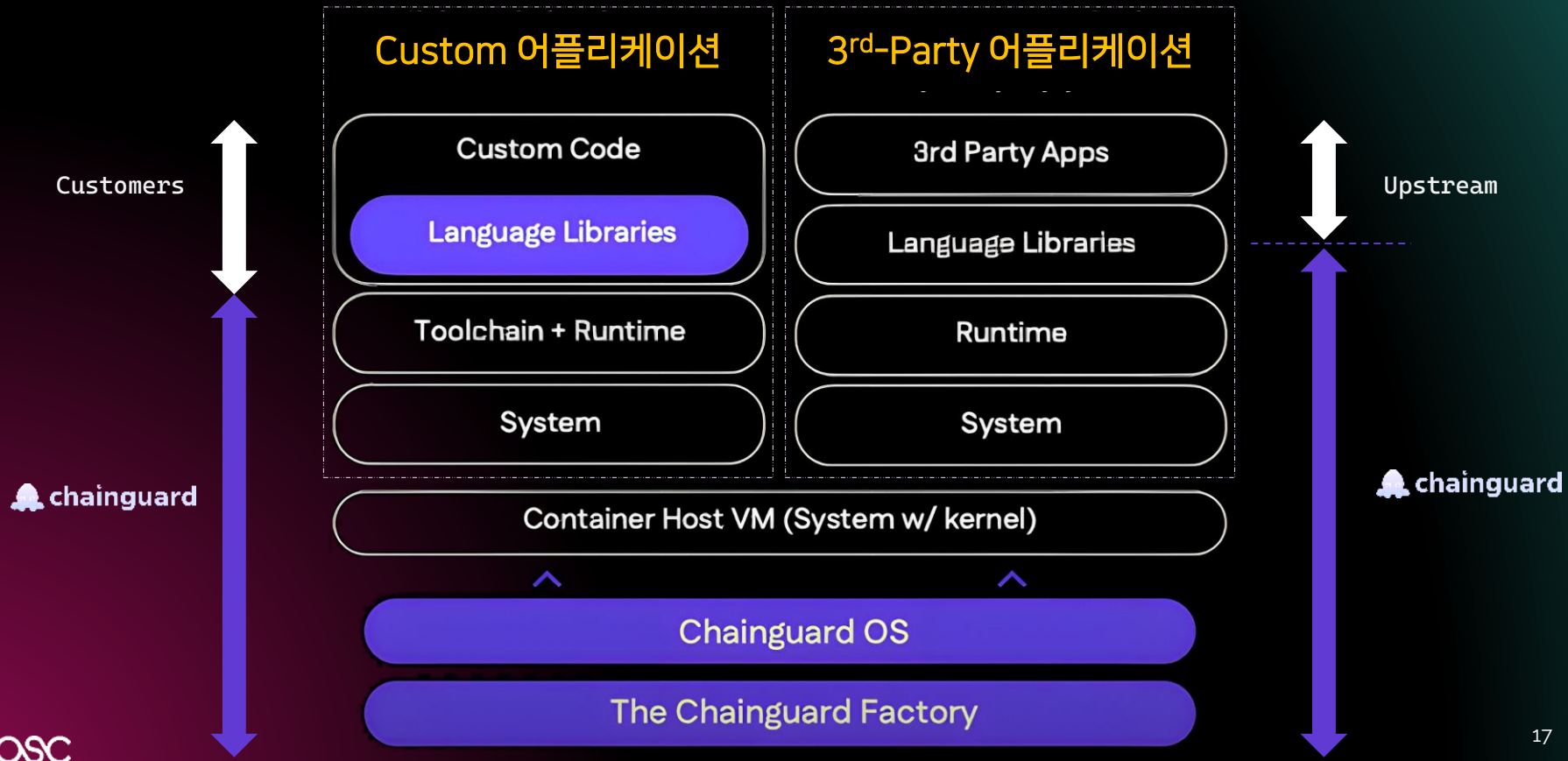
cilium

MariaDB

Grafana

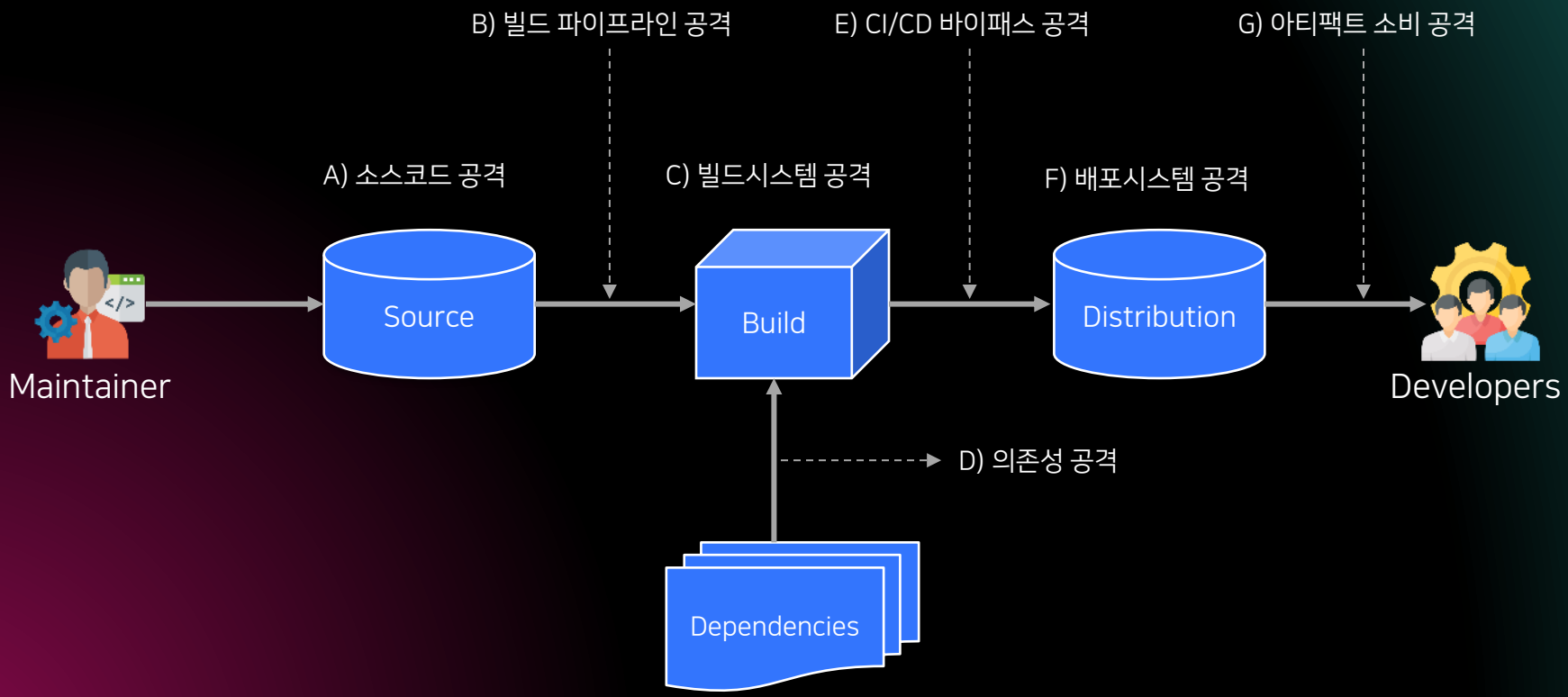
kubernetes

Chainguard 지원범위



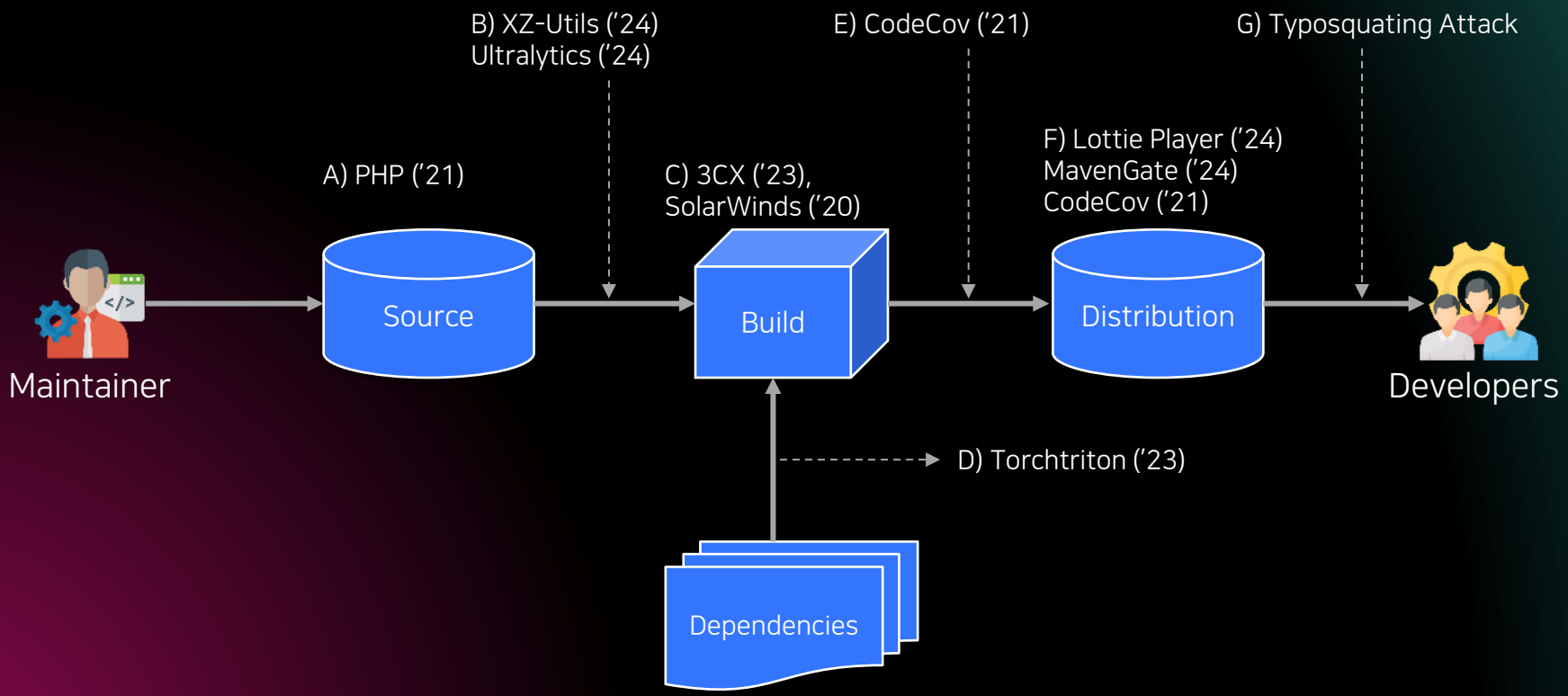
패키지 Lifecycle 및 공급망 공격 유형

chainguard



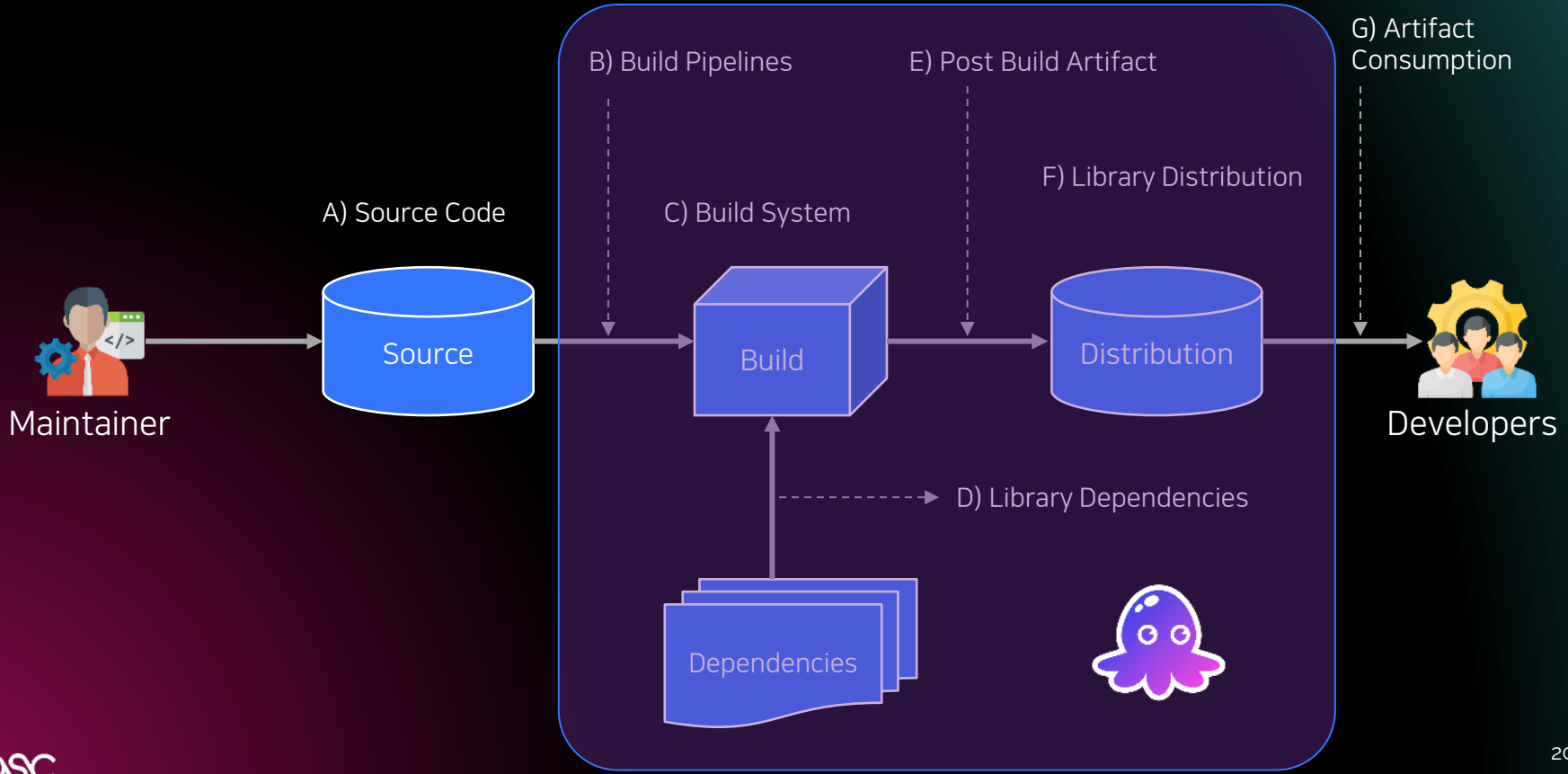
패키지 Lifecycle 및 공급망 공격 사례

chainguard



Chainguard 지원 영역

chainguard



Chainguard Products

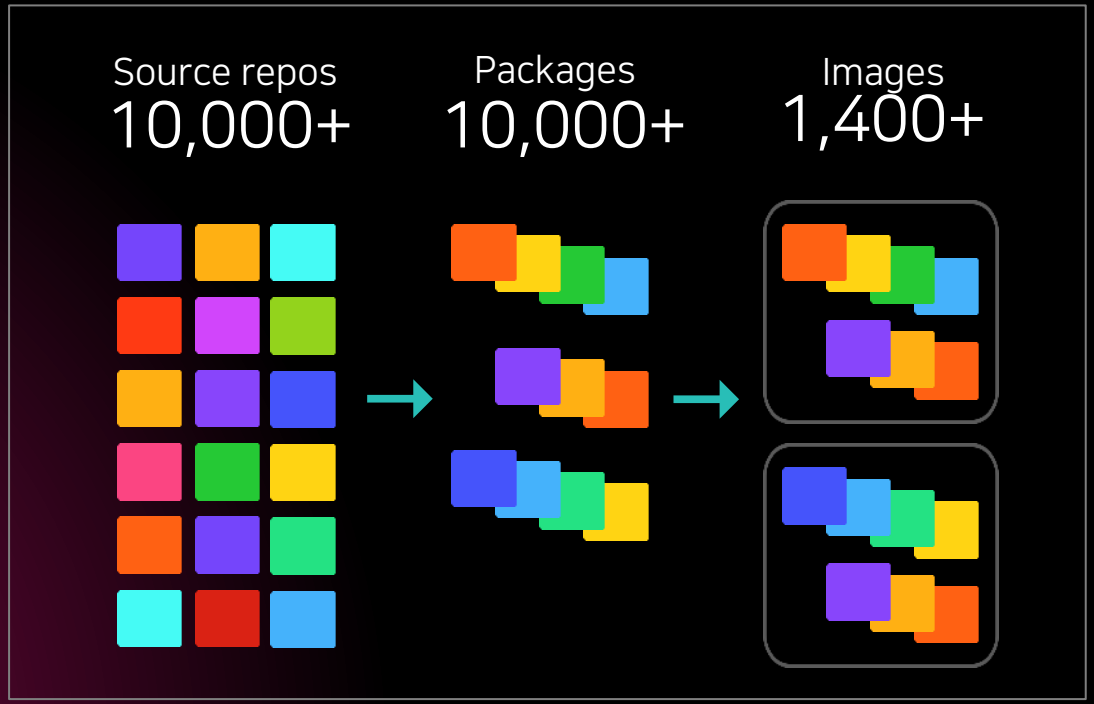
chainguard

OSC

Chainguard를 통한 소프트웨어 공급망 지원

chainguard

- 소스로부터 직접 빌드
- Delta 최소화
- Nano-updates 및 Rebuilds
- Minimal, hardened, immutable artifacts



Purpose-built Zero-CVE 이미지

chainguard

Base Images

런타임 언어 및 프레임웍

Application Images

서버, Dev Tools, DB

FIPS Images

FIPS Cryptography and
OS-Level STIGs

OpenSSL
Cryptography and SSL/TLS Toolkit

Bouncy Castle
with Keyfactor

AI Images

GPU-Based ML
Workloads

Application Images - Migration

chainguard

Helm Charts Update를 통해
Chainguard 이미지로 업데이트

단순 대체 (Drop-in replacement)

without:

```
helm install \
  cert-manager jetstack/cert-manager \
  --namespace cert-manager \
  --create-namespace \
  --version v1.16.1 \
  --set crds.enabled=true
```

with:

```
helm install cert-manager jetstack/cert-manager \
  --namespace cert-manager \
  --create-namespace \
  --version v1.16.1 --set image.repository=cgr.dev/chainguard/cert-manager-controller \
  --set image.tag=latest \
  --set cainjector.image.repository=cgr.dev/chainguard/cert-manager-cainjector \
  --set cainjector.image.tag=latest \
  --set acmesolver.image.repository=cgr.dev/chainguard/cert-manager-acmesolver \
  --set acmesolver.image.tag=latest \
  --set webhook.image.repository=cgr.dev/chainguard/cert-manager-webhook \
  --set webhook.image.tag=latest \
  --set crds.enabled=true
```

OSC

Base Images - Migration

chainguard

Chainguard Base 이미지 사용을 위한 변경내역

- dockerfile 및 multi-stage builds 업데이트
- Non-Root 실행 변경
- No package manager 또는 package manager 변경
- 기타 코드 변경 (Chainguard는 범용 OSS 라이브러리 사용으로 코드변경 최소화)

```
FROM cgr.dev/chainguard/node:dev AS builder
WORKDIR /app
COPY package*.json ./
COPY tsconfig*.json ./
COPY src src
RUN  npm ci && npm run build

FROM cgr.dev/chainguard/node:runtime
WORKDIR /app
COPY package*.json ./
RUN npm install --production
COPY --from=builder /app/dist/ dist/
ENTRYPOINT ["npm", "run", "start:prod"]
```

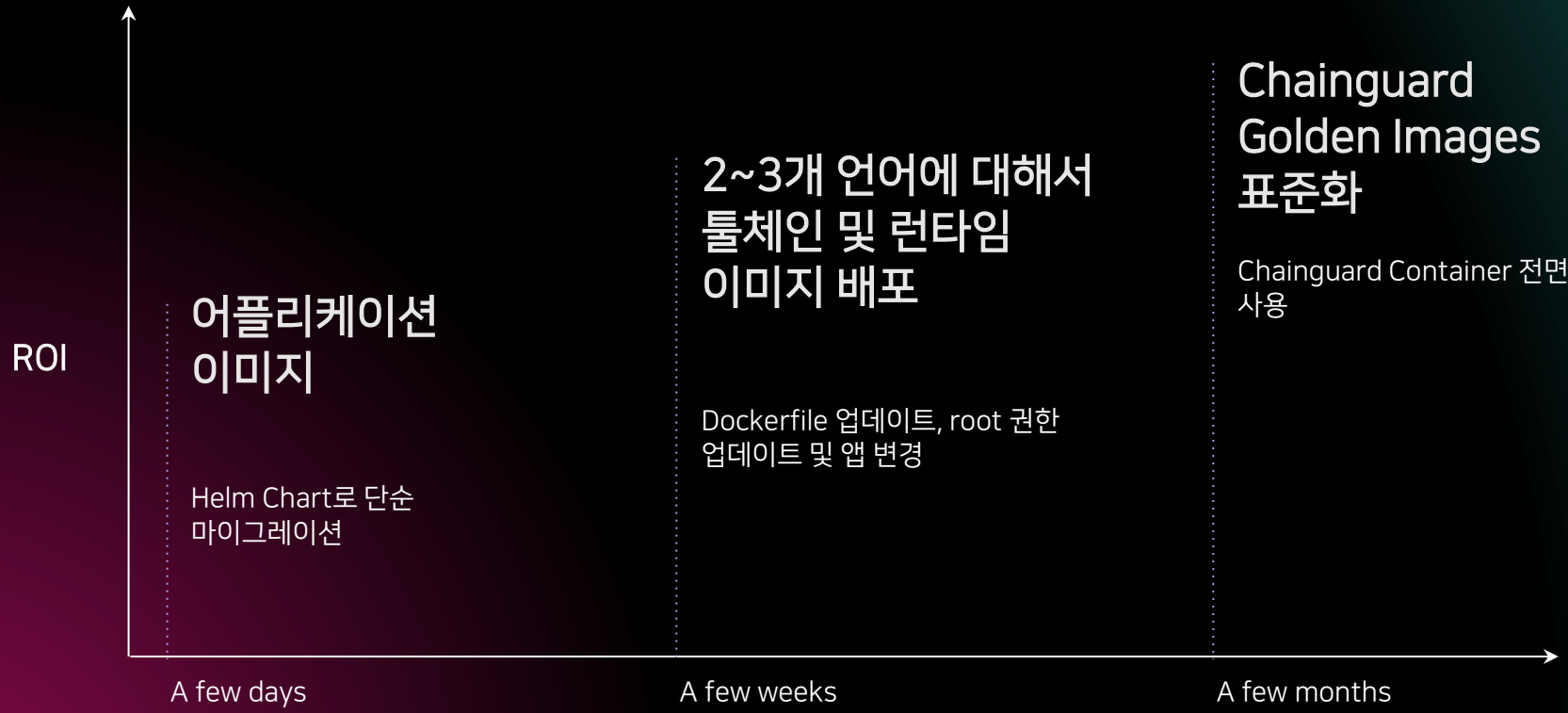
```
FROM cgr.dev/chainguard/jdk:openjdk-17 AS builder

COPY HelloWolfi.java /home/build/
RUN /usr/lib/jvm/openjdk/bin/javac HelloWolfi.java

FROM cgr.dev/chainguard/jre:openjdk-17
COPY --from=0 /home/build/HelloWolfi.class /app/
CMD ["HelloWolfi"]
```

OSC

Chainguard 도입 여정



Q&A

chainguard.dev