

snyk



Develop fast. **Stay secure**



金 承顕

shoken.kim@snyk.io

- カリフォルニア大学バークレー校卒業(応用数学)
- リクルートで情報通信事業に従事
- 2009年～2016年 ブラックダックソフトウェアアジア代表
- 2017年よりFOSSID(OSS管理ツール)
- 2021年5月Snyk社によるFOSSID買収により、Snykのジャパンカントリーマネジャーに

Snykによる

「develop fast & stay secure」 の実現

Founded in

2015

Employees

900+

Raised

\$770M

Developers

2.5M

PROTECTED BY SNYK

Google

reddit

mongoDB®

salesforce

skyscanner

intuit®

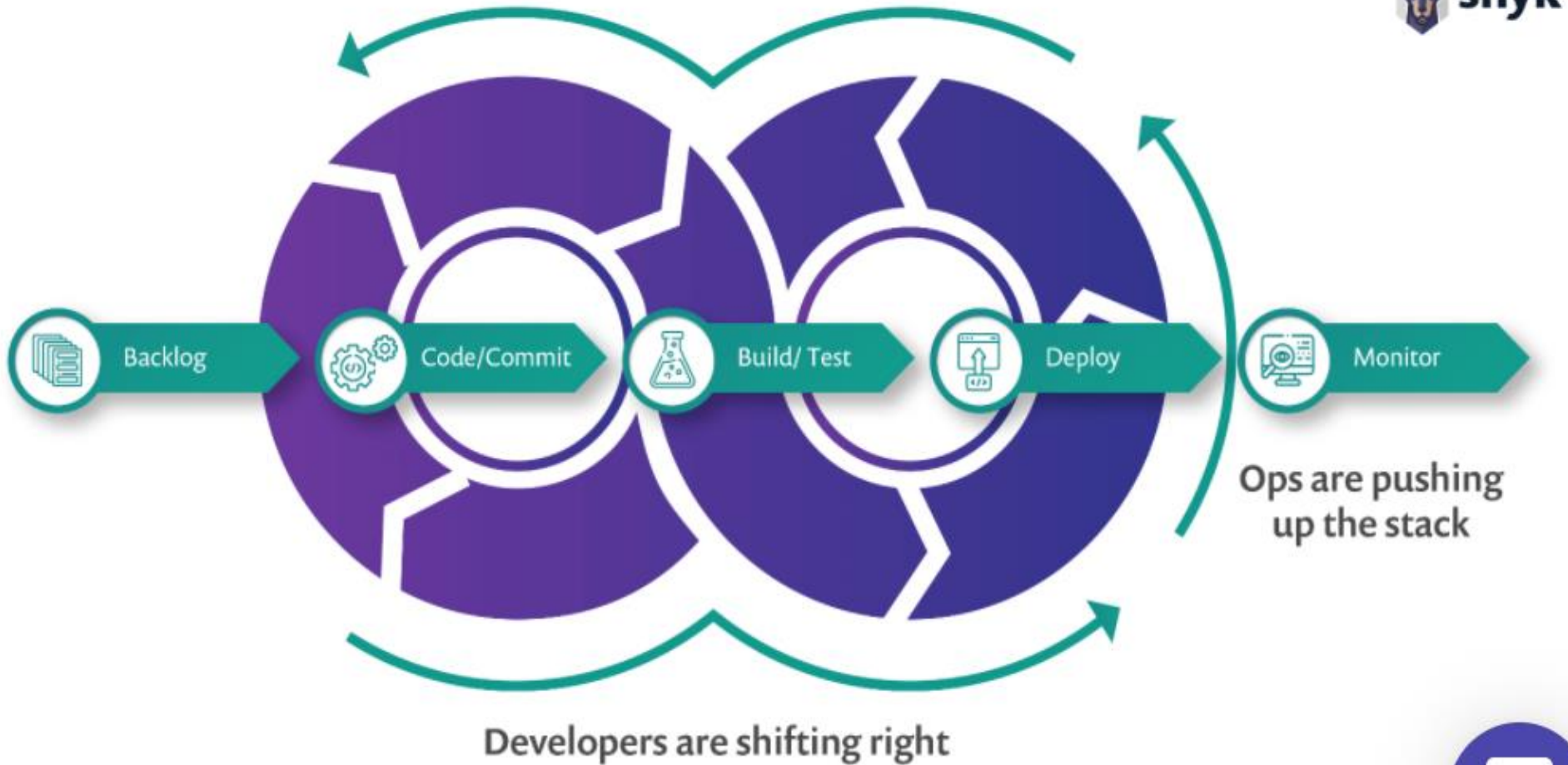
New Relic®

asurion

Telstra

ASOS
discover fashion online

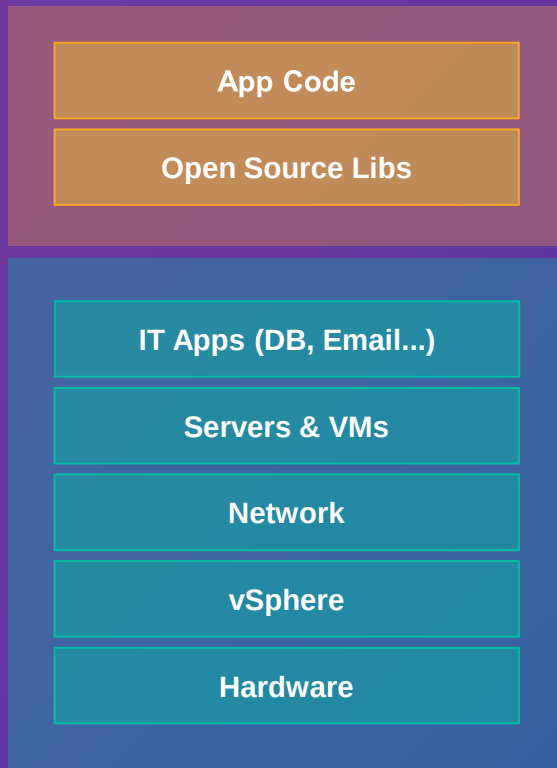
DevSecOps



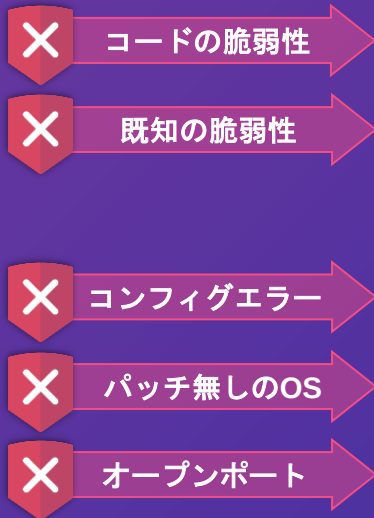
Cloud : IT => App Services



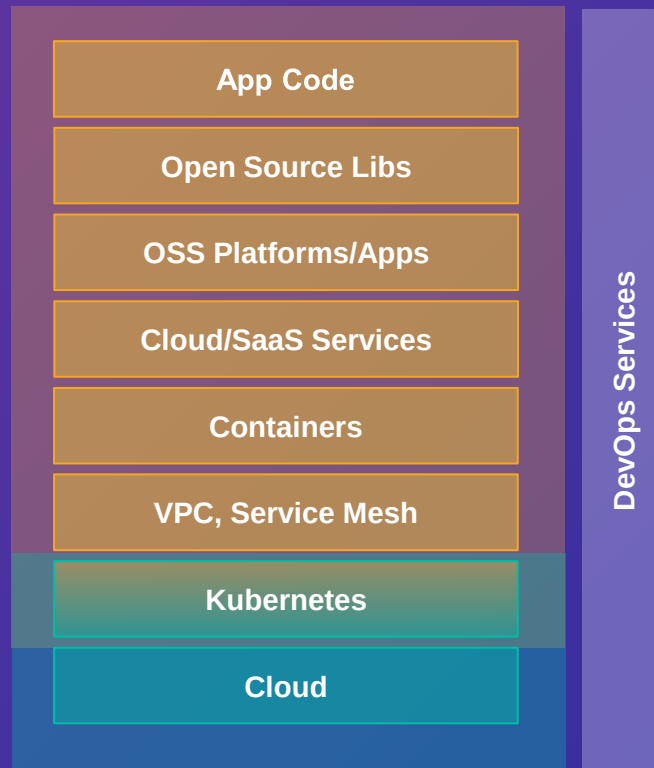
クラウド時代の以前



Digital Transformation



クラウド時代の アプリケーションセキュリティ要件



Software Supply Chain:

Code



- 10-20% => カスタムコード
- 頻繁なソフトウェアリリース => ウォーターフォール型では間に合わない

Open Source Code



- 80-90% => OSS
- 80% => 間接的な依存関係にあるOSSの脆弱性

Containers



- 100以上 => パブリックソースにあるLinuxパッケージ
- ビルド、デプロイ、スケールを 瞬時に

Infrastructure
as Code



- クラウドの脆弱性の最大原因 => コンフィグエラー [NSA]
- ネットワークアクセス、ストレージサーバ => コードと同スピードでデプロイ

Cloud Native App Security Platform

Container
Open Source

Code

IaC

 garethr ...	✓ 26 days ago	
 .github/workflows	26 days ago	
 assets	7 months ago	
 dist	26 days ago	
 spec	6 months ago	
 Dockerfile	6 months ago	
 Gemfile	6 months ago	
 Gemfile.lock	6 months ago	
 LICENSE	7 months ago	
 Makefile	7 months ago	
 README.md	7 months ago	
 Rakefile	7 months ago	
 app.rb	6 months ago	
 config.ru	7 months ago	
 puma.rb	6 months ago	
 snykit.yaml	6 months ago	
 values.yaml	6 months ago	

開発側

デベロッパーが使えるGUI

SDLCとの自動連携

Code

Open
Source

Containers

Infrastructure
as Code

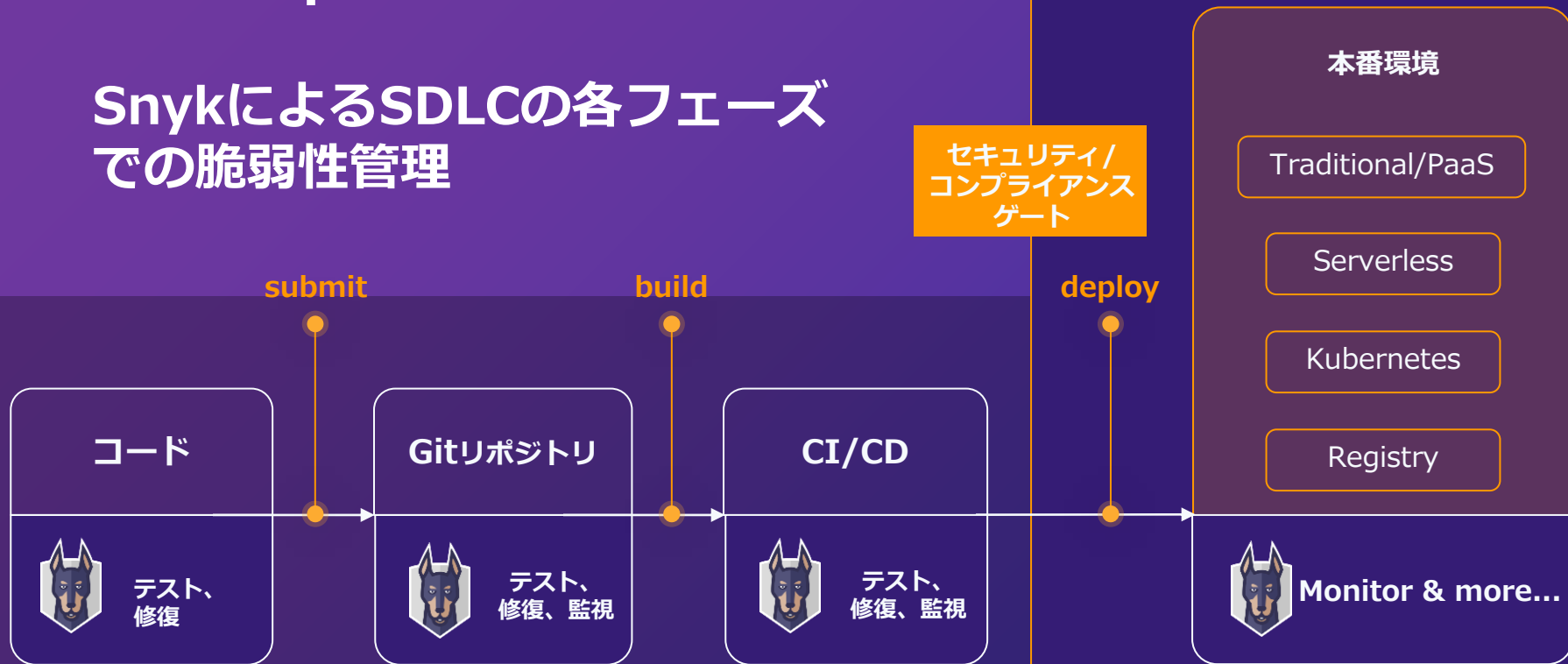
セキュリティインテリジェンス

エンタープライズガバナンス

Snykプラットフォーム

DevSecOps:

SnykによるSDLCの各フェーズでの脆弱性管理



自動修復

複雑な修復ロジックから解放されます

ワンクリックにて修復プルリクエストを発行



Open a fix PR

github.com/snyk

Vulnerabilities with a fix

An upgrade or patch is available to fix the vulnerable dependencies.

- H** Regular Expression Denial of Service (ReDoS) in debug
- H** Content & Code Injection (XSS) in marked
- H** Regular Expression Denial of Service (ReDoS) in fresh

OPEN A FIX PR

when there is one)
Set to ignore for 30 days (updates policy)

最高品質の **Snyk Intel 脆弱性データ** Snyk製品の中核

+441%

包括的で豊富なデータ

公開されている中で、最大の商用データベースよりも441%も多く脆弱性データをカバーしています

92%

どこよりも早く

NVDのJavaScriptの脆弱性の内、92%がSnyk Intel データベースに最初に追加されました

抜群の正確性

誤検知が極端に少ない：すべてのアイテムは、専門チームによって分析され、その正確性がテストされています

Contributing to the Community



CVE
numbering
authority
(CNA)



OWASP
contributing
member



Linux
Foundation
security
partner



OpenJS
Foundation
Security
Group

Trusted by the Industry



Red Hat
Dependency
Analytics



Application
Security



Google
Chrome
Lighthouse



Datadog
Continuous
Profiler



Rapid7
tCell &
InsightVM



IBM Code
Risk Analyzer



Trend Micro
Deep Security



Docker

Snyk の先進的アプローチ



開発者がセキュリティ対策

Snykの開発者向けの使いやすいツールは、開発者が使用する開発ツールと統合されているため、開発者がセキュリティを簡単に実装できます。



自動修復

開発工程の一部として、修復の自動化プロセスを備えています。修復の推奨事項を実装するためのアルゴリズムベースの修復テクノロジーを持っています。



深いレベルでのセキュリティ確保

Snykのセキュリティ調査チームが補足する
Snyk独自の情報データベースを搭載



SCALE



ACTIONABILITY



COVERAGE