HashiCorp

GitHub Universe Recap

HashiCorp Vault と GitHub Actions 連携

Solutions Engineer
Tadashi Ito (伊藤 忠司)
LinkedIn: tadashii-itochu

December 2023

HashiCorp

Leading Cloud Infrastructure Automation

インフラ *Infrastructure*

Terraform
インフラ構築の自動化
Infrastructure as Code

Packer
イメージビルドの自動化
Images as Code

Nomad
ワークロードオーケストレーション
Workload orchestration

Waypoint
アプリデリバリの標準化
App deployment workflow

セキュリティ *Security*

Vault
シークレット中央管理 & データ保護
Secret management & Data protection

Boundary
セキュアリモートアクセス
Secure Remote Access

Consul
サービスメッシュとサービスディスカバリ
Mult-cloud service networking

Vault | Vault の主なユースケース

アイデンティティベースのアクセス制御

シークレット管理	証明書	鍵管理	データ保護(暗号化)
Static Dynamic Database Kubernetes	PKI	KMS KMIP HSM	Encryption Signatures Tokenization

Vault | Vault の主なユースケース

アイデンティティベースのアクセス制御

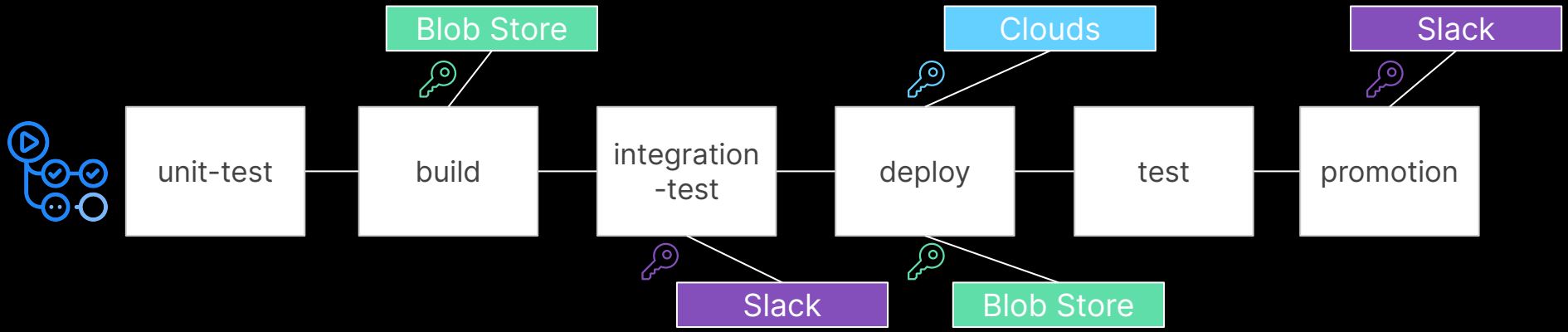
シークレット管理	証明書	鍵管理	データ保護(暗号化)
Static Dynamic Database Kubernetes	PKI	KMS KMIP HSM	Encryption Signatures Tokenization

パイプラインでのシークレットに関するチャレンジ

シークレットをどの様にセキュアに扱うか

CI/CD パイプラインで扱うシークレット

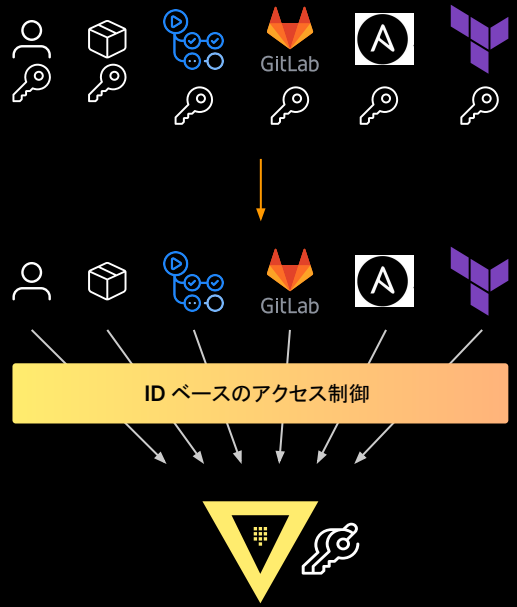
- クラウドのアイデンティティ
- 証明書 / SSH パスワード
- レポジトリや Slack のトークン等



Vault のシークレット管理の特徴

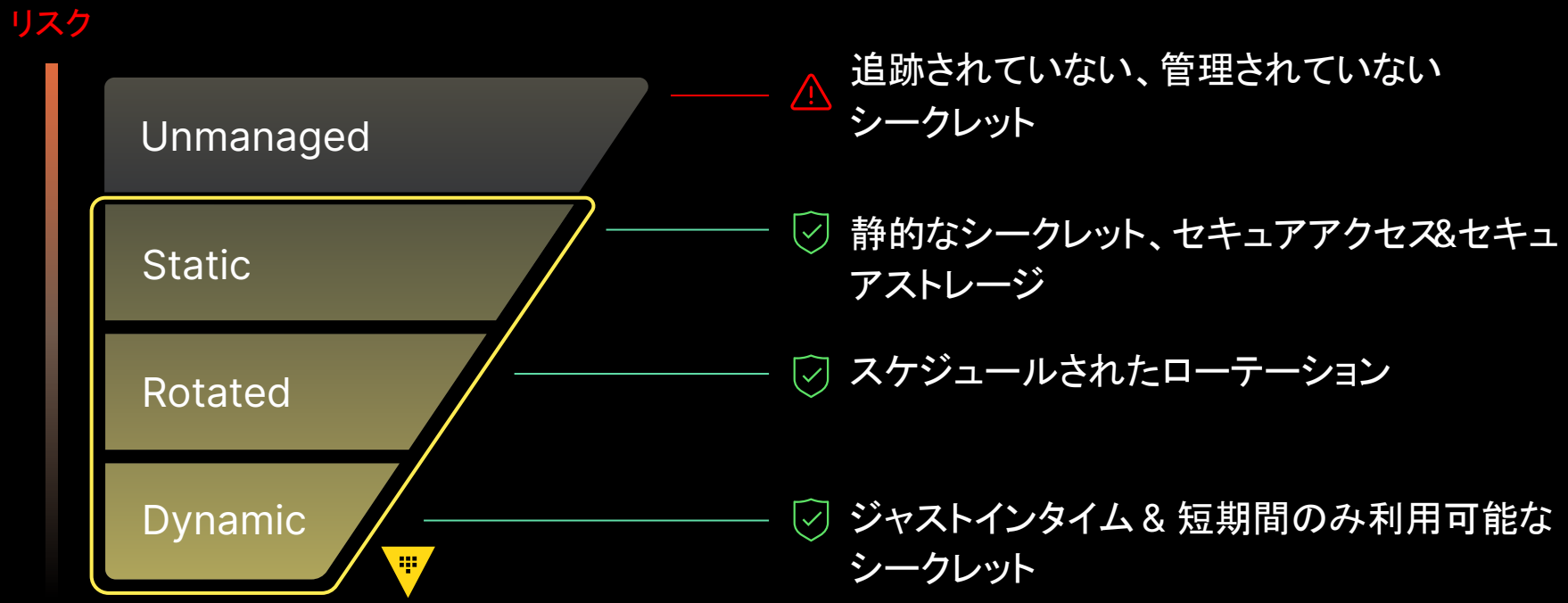
悪意ある攻撃者に空間的な制約・時間的な制約をかける

空間的な制約：攻撃対象面積の削減



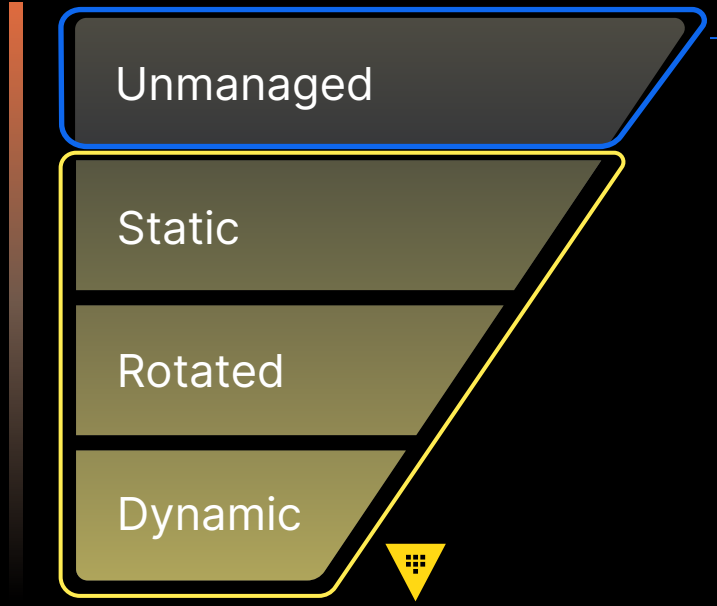
時間的な制約：攻撃可能時間の削減

シークレットライフサイクル管理

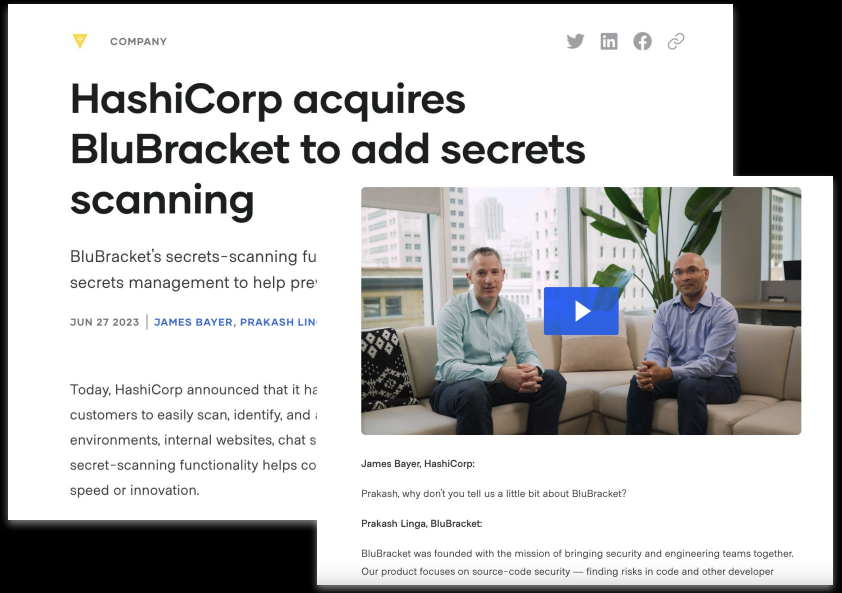


シークレットライフサイクル管理

リスク



[6月に買収した BluBracket](#) の
フォーカスエリア


COMPANY

HashiCorp acquires BluBracket to add secrets scanning

BluBracket's secrets-scanning fu
secrets management to help pre

JUN 27 2023 | JAMES BAYER, PRAKASH LIN

Today, HashiCorp announced that it ha
customers to easily scan, identify, and
environments, internal websites, chat s
secret-scanning functionality helps co
speed or innovation.

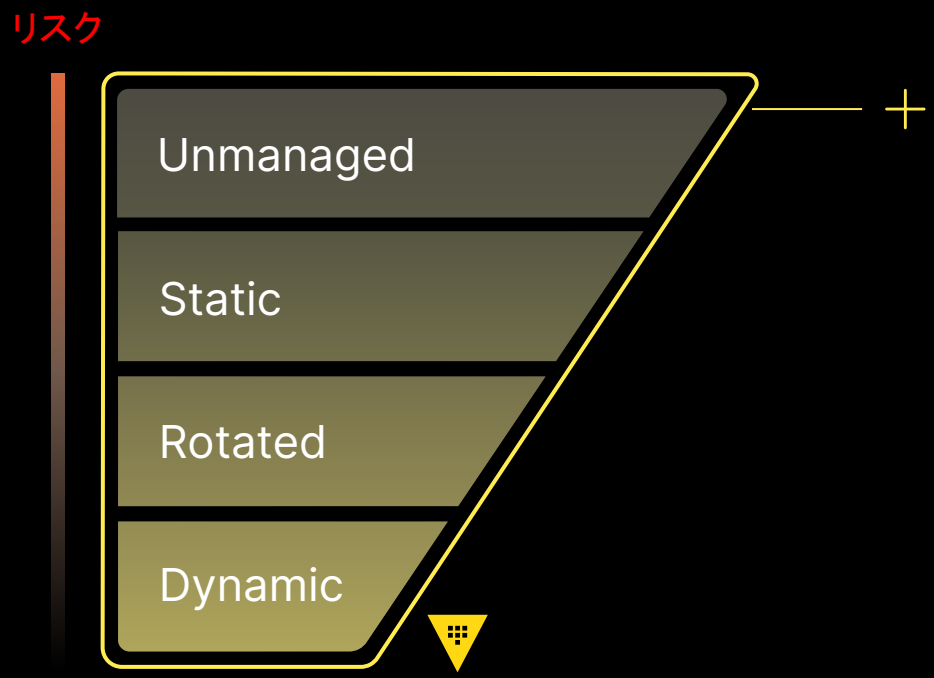
James Bayer, HashiCorp:

Prakash, why don't you tell us a little bit about BluBracket?

Prakash Linga, BluBracket:

BluBracket was founded with the mission of bringing security and engineering teams together. Our product focuses on source-code security — finding risks in code and other developer

シークレットライフサイクル管理



HCP Vault Radar

New!!

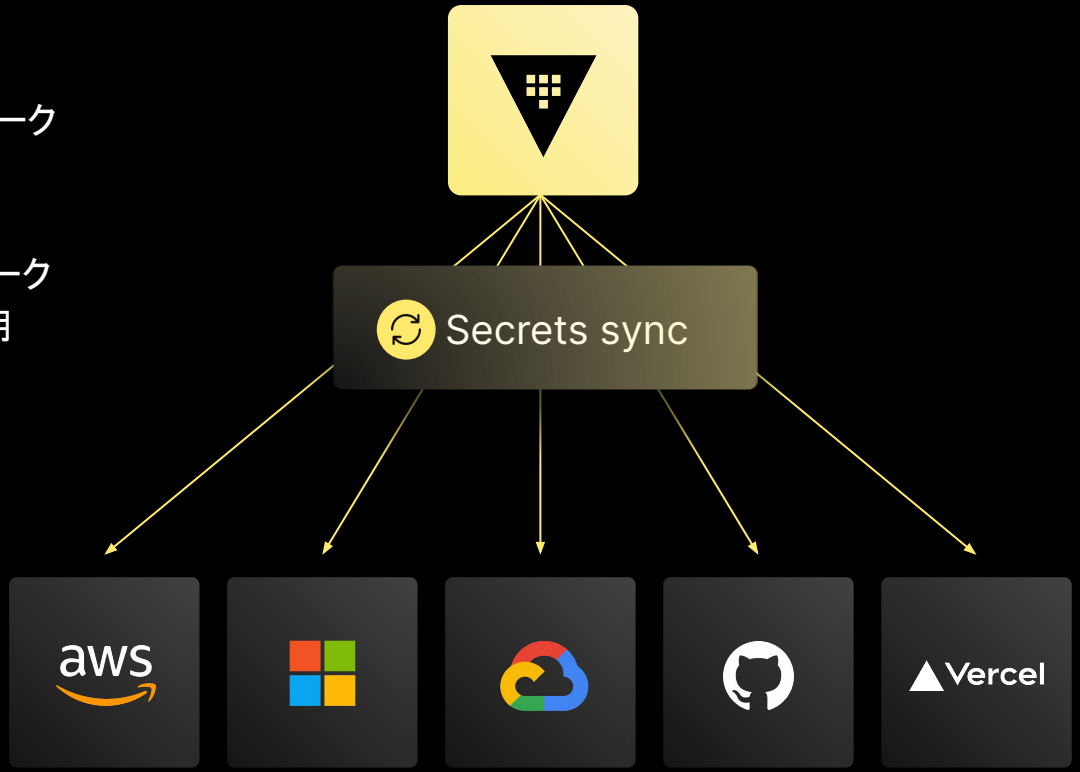
シークレットの散在を解消

- 複数のデータソースから300以上のシークレットパターンを検出
  - Git ベースのバージョン管理システム
  - Confluence
  - ファイルシステムのディレクトリ
  - S3 etc

Secrets Sync

New!!

- Vault からのクラウドのネイティブなシークレットマネージャへのシークレット同期 (One-way sync)
- アプリなどはクラウドのネイティブなシークレットマネージャからシークレットを利用

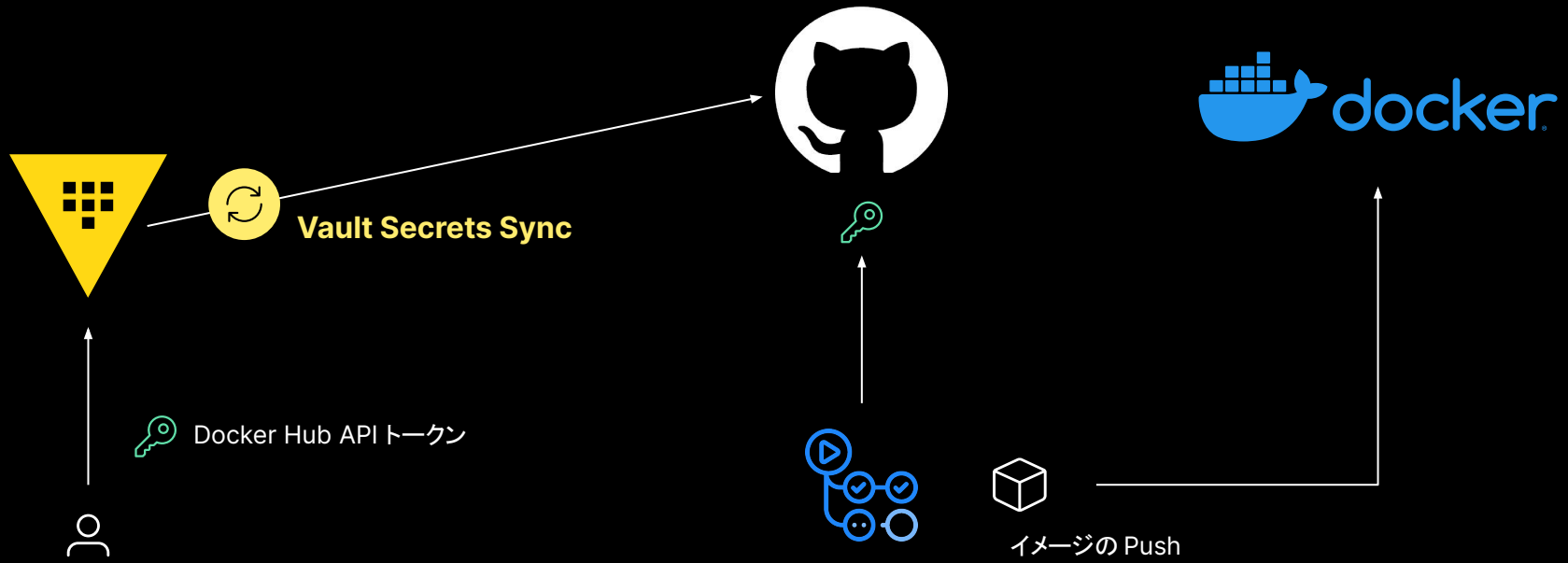


メリット

- 運用者は Vault を使ってセキュリティ態勢を改善
- 開発者はアプリケーションの改修をせず利用

デモ

Vault Secrets Sync + GitHub Actions



まとめ

シークレットライフサイクル管理を全て包括出来るのが Vault です

- HCP Vault Radar で管理されていないシークレット情報の可視化も可能になります

GitHub Actions で利用するシークレットを Vault で一元管理しつつ、GitHub Actions の Secrets に同期出来ます

- アプリ側は、GitHub Actions のシークレットから必要なシークレットを利用できます

Thank you

jp-marketing@hashicorp.com

ご質問やお問い合わせはこちらから