AWS Builders Online Series

ビルダーのビルダーによる ビルダーのためのセキュリティ

桐山 隼人
アマゾン ウェブ サービス ジャパン合同会社
技術統括本部
シニアセキュリティソリューションアーキテクト

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ビルダーのセキュリティ
Security of Builder

© 2021, Amazon Web Services, Inc. or its affiliates.

ビルダーとは

実現したい事を迅速に行う人

- ✓ イノベーションを実現
- ✓ 自由を獲得
- ✓ サイクルを迅速に回す

© 2021, Amazon Web Services, Inc. or its affiliates.

経験・体験を繰り返す事により成長できる

そして小さな成功を積み上げていく

それが自信につながる

© 2021, Amazon Web Ser

AWSクラウドはビルダーを支えるプラットフォーム

© 2021, Amazon Web Services, Inc. or its affiliates.

Securityの由来

sē + cūra

(離れて) (心配)

© 2021, Amazon Web Services, Inc. or its affiliates.

At Amazon, we hire Builders and let them build.

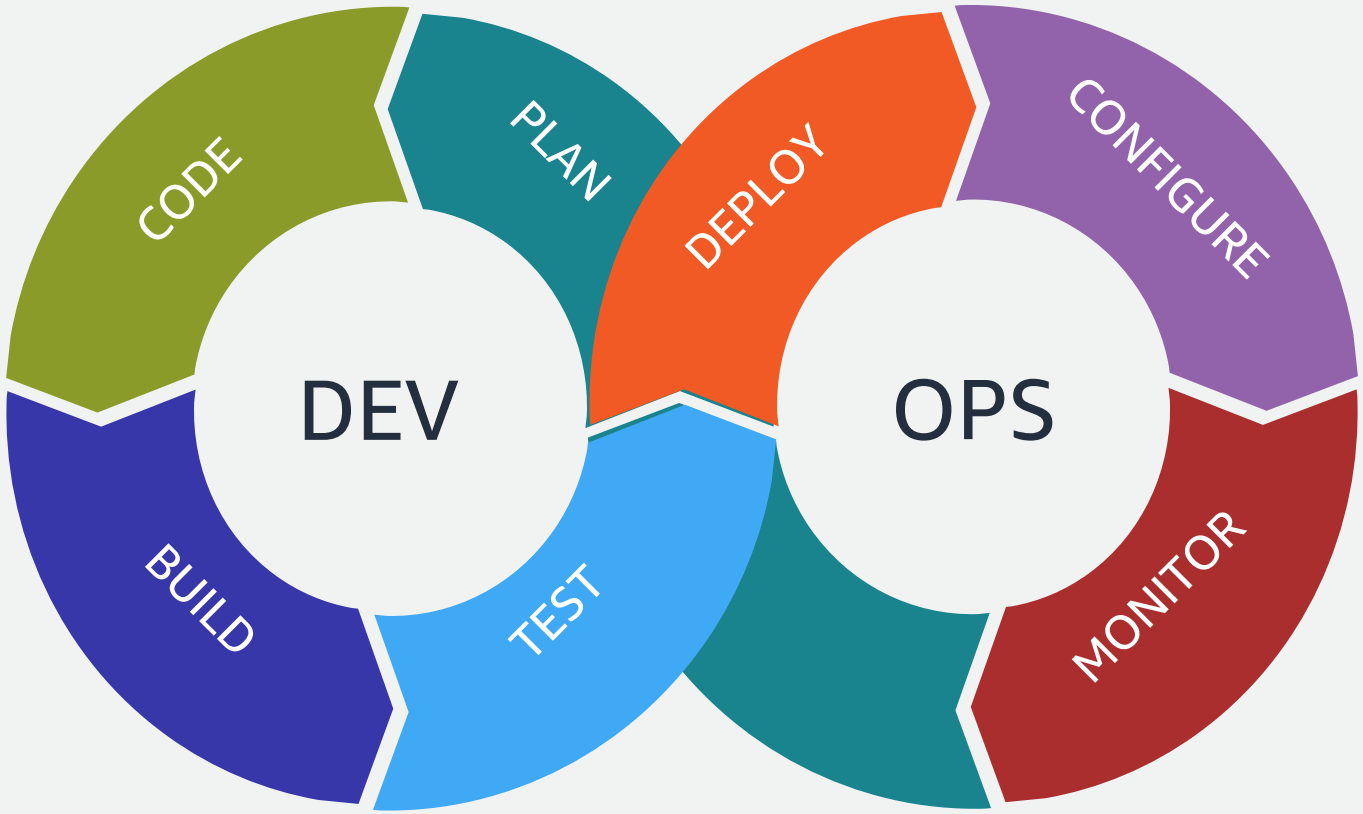
aws

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ビルダーによるセキュリティ
Security by Builder

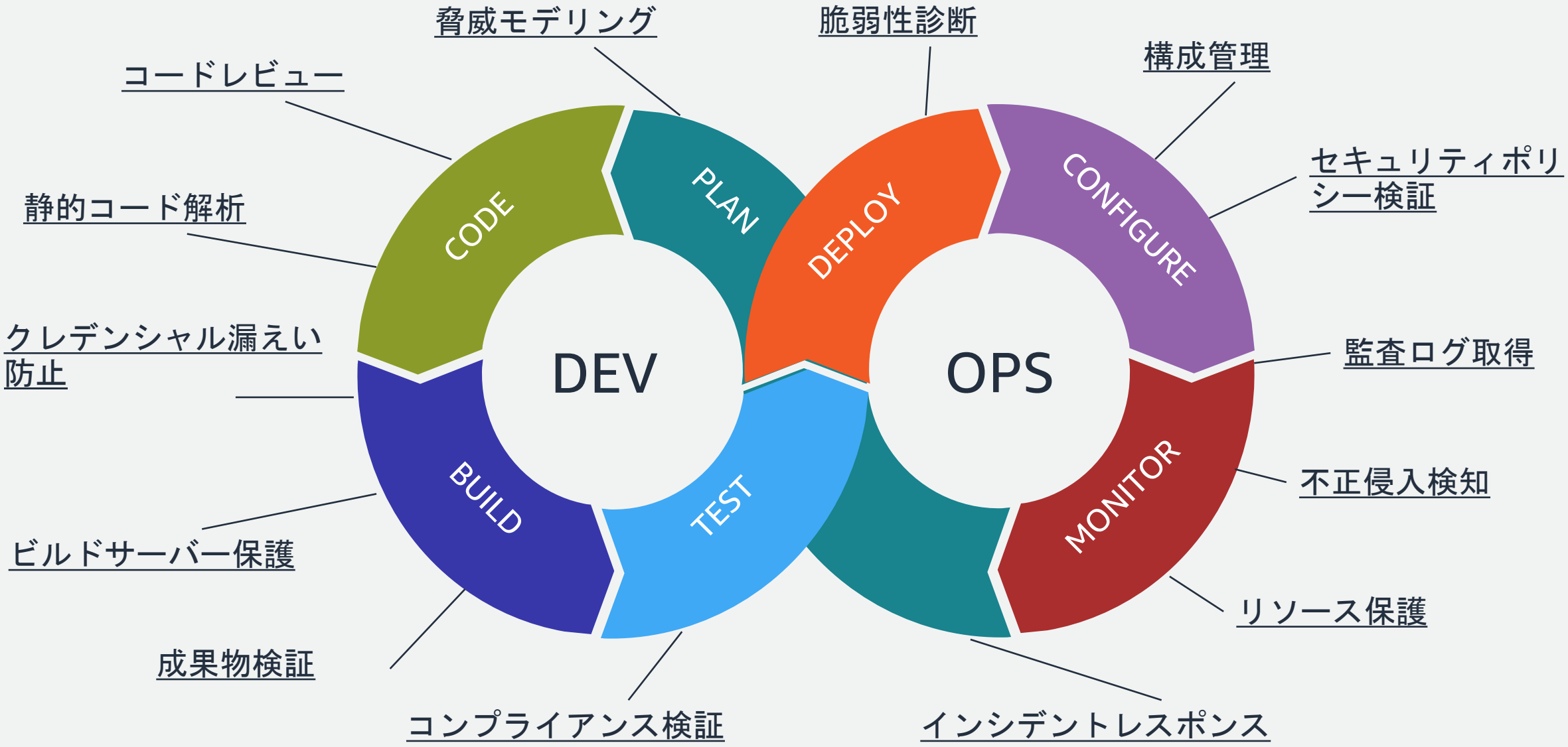
© 2021, Amazon Web Services, Inc. or its affiliates.

継続的にビジネス目標を達成するための**DevOps**サイクル



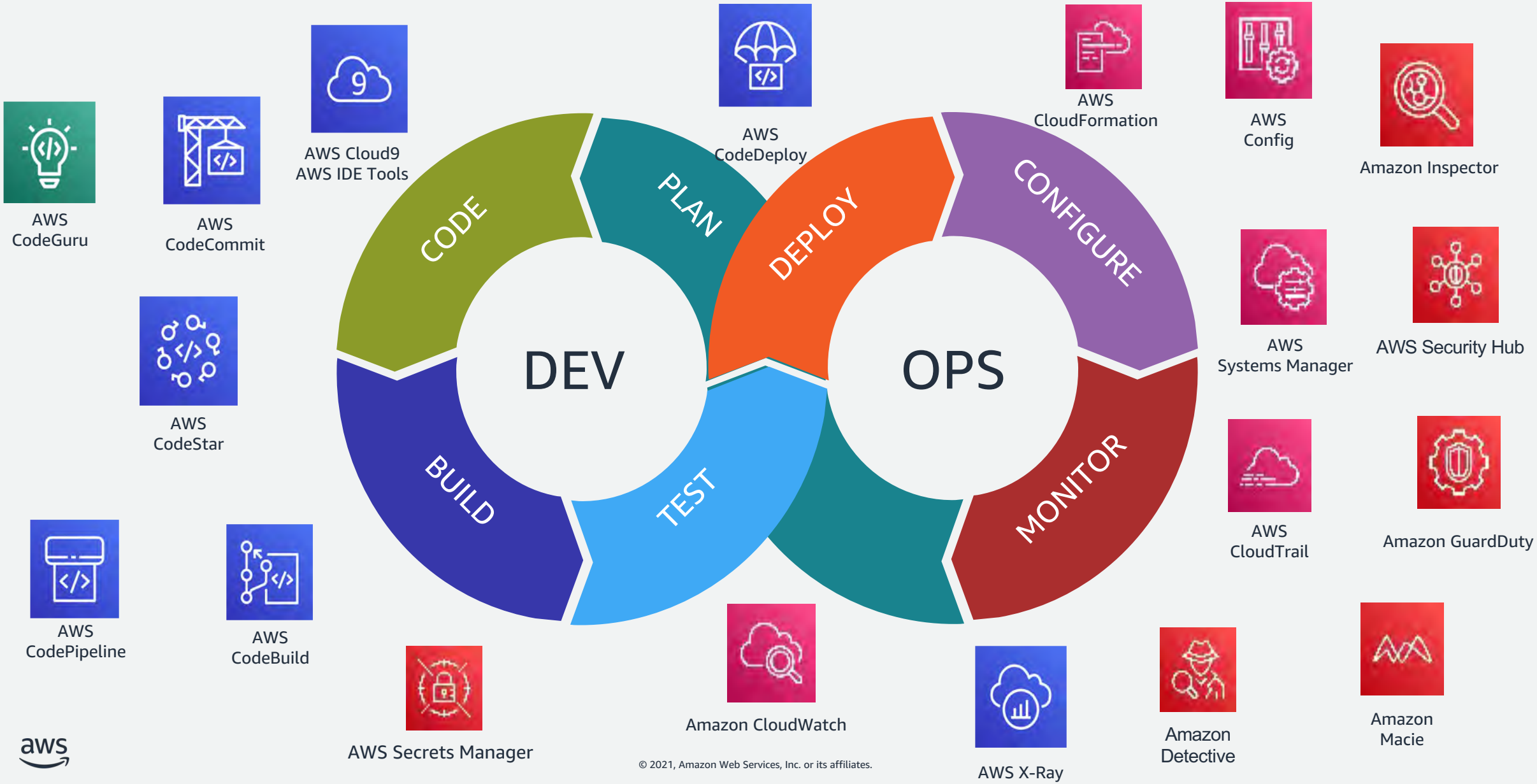
© 2021, Amazon Web Services, Inc. or its affiliates.

DevOpsサイクルにセキュリティを組み込む



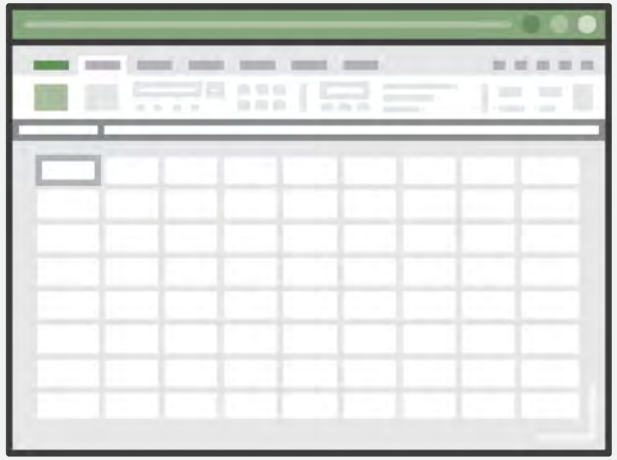
© 2021, Amazon Web Services, Inc. or its affiliates.

DevSecOpsサイクル全体を実現するAWSサービス



© 2021, Amazon Web Services, Inc. or its affiliates.

従来のセキュリティ業務



スプレッドシート

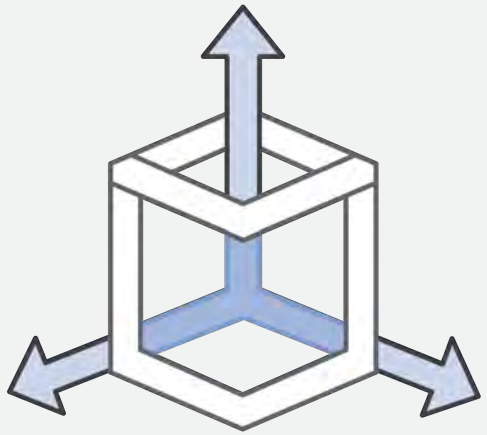
ポリシー文書

チェックリスト

大きな労力が必要(Heavy Lifting)な作業が
オートメーション(自動化)によって削減できる

© 2021, Amazon Web Services, Inc. or its affiliates.

クラウド時代ではセキュリティ自動化が不可欠に



拡張性

▼

セキュリティの
自動追従

コスト

▼

労力・時間
の削減

信頼性

▼

品質の担保
人為的ミス排除

© 2021, Amazon Web Services, Inc. or its affiliates.

“私達はドキュメント化された堅牢なAPIが必要でした。

それぞれのチームが話すことなしに協業するためにです。

それには何年もかかりました・・・

しかし、一度できてしまうと、私たちはさらに速く前進することができるようになったのです”

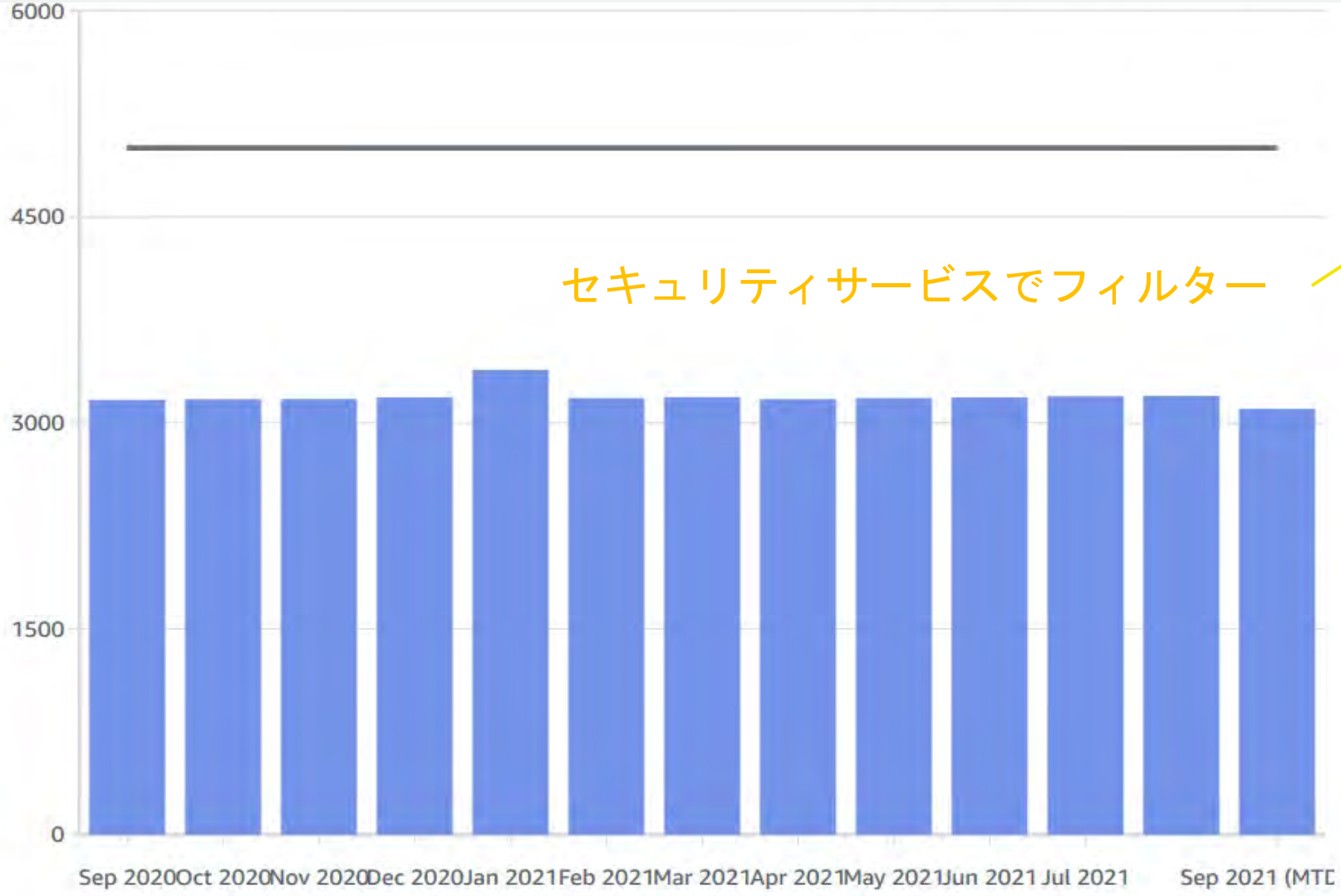
ANDY JASSY
CEO, AMAZON

ビルダーのためのセキュリティ
Security for Builder

© 2021, Amazon Web Services, Inc. or its affiliates.

Security Guardrail

コストガードレール (AWS Budgets)



セキュリティサービスでフィルター

Filters Info

Remove all

Services included (16) Remove

CloudTrail, CloudWatch, Cognito, Config, Detective, Firewall Manager, GuardDuty, Inspector, Key Management Service, Macie, Secrets Manager, Security Hub, Service Catalog, Shield, Systems Manager, WAF

Edit filter

Add filter

▼ Advanced options

Aggregate costs by

Unblended costs

Supported charge types

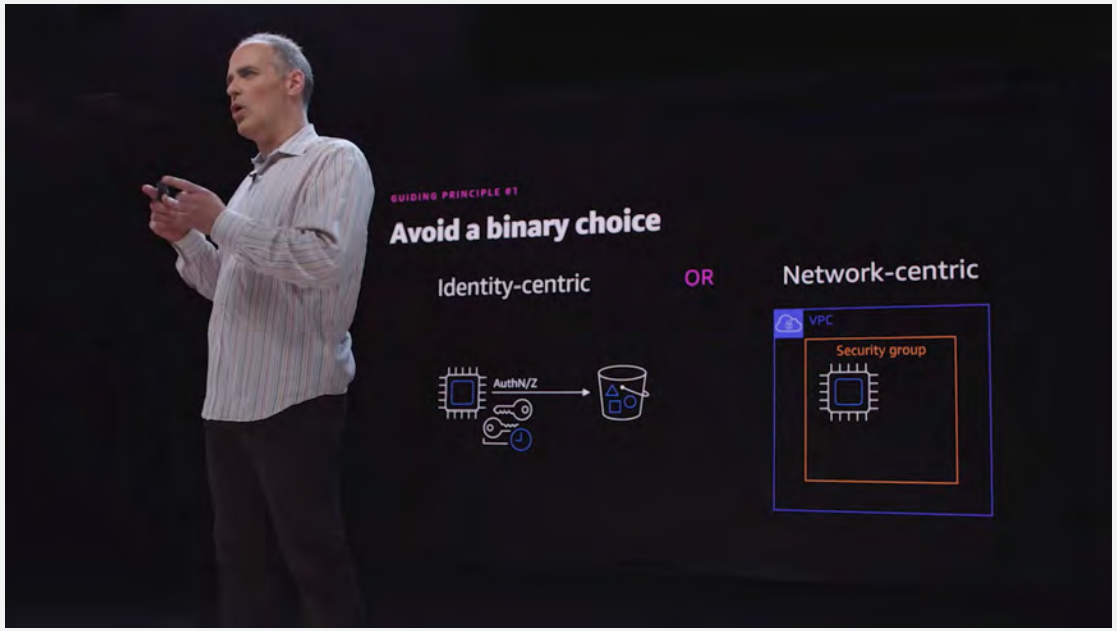
Upfront reservation fees ✕

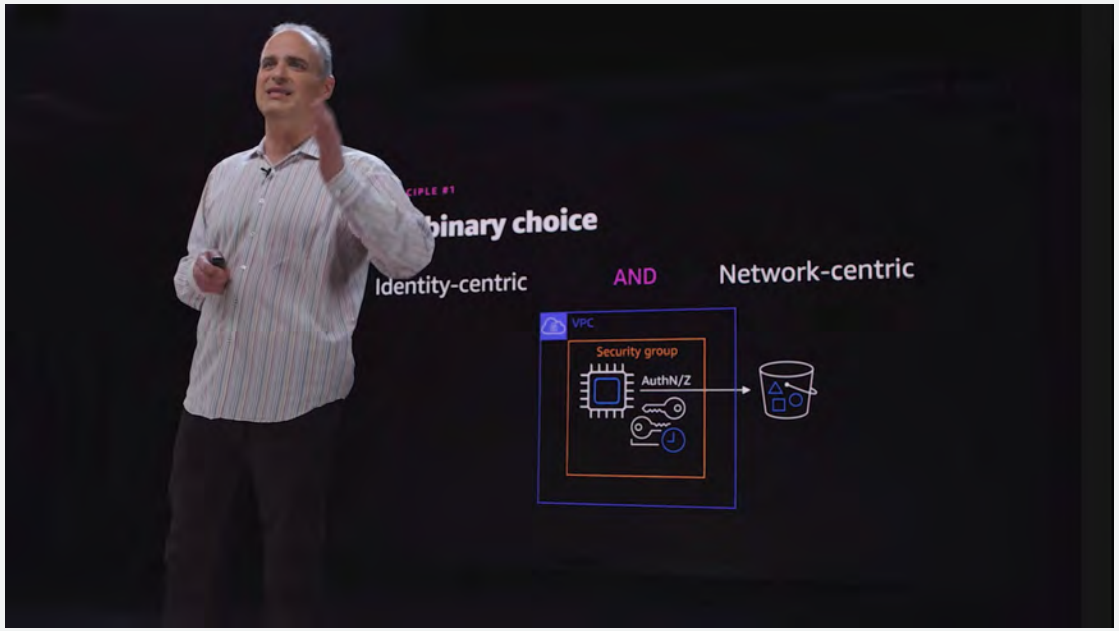
Recurring reservation charges ✕

© 2021, Amazon Web Services, Inc. or its affiliates.

Zero Trust

アイデンティティ中心のセキュリティとネットワーク中心のセキュリティを共存させるだけでなく、お互いを拡張させるもの





[AWS re:Invent 2020] AWS security: Where we've been, where we're going (Stephen Schmidt, AWS CISO)
https://www.youtube.com/watch?v=ScybA4Zb4kA

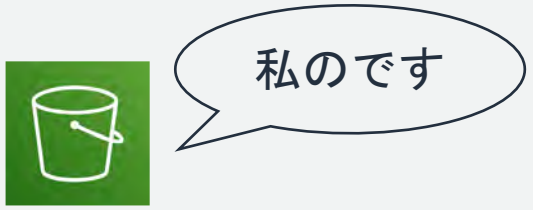
© 2021, Amazon Web Services, Inc. or its affiliates.

Data Perimeter (データ境界)

信頼されたアイデンティティが

想定されたネットワーク場所から

信頼されたリソースにアクセス



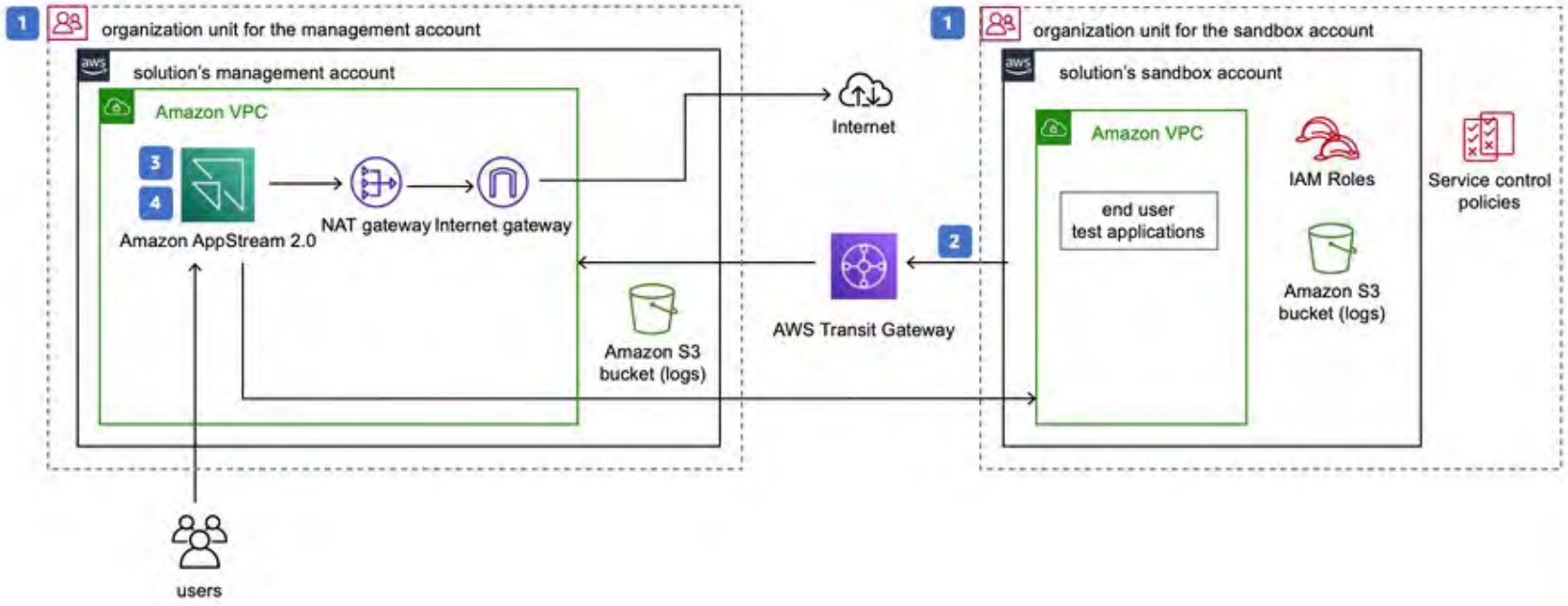
するためのガードレール

© 2021, Amazon Web Services, Inc. or its affiliates.

AWS Innovation Sandbox ソリューション

AWS ソリューション実装の概要

下の図は、このソリューションの実装ガイドと付属の AWS CloudFormation テンプレートを使用して、自動的にデプロイできるアーキテクチャフローを表しています。



拡大イメージを見る

AWS Innovation Sandbox

バージョン 1.0.0
リリース: 2021 年 8 月
作成者: AWS

見積りデプロイ時間: 30 分

予想費用
ソースコード
CloudFormation テンプレート

実装ガイドを表示

AWS コンソールで起動する

https://aws.amazon.com/jp/solutions/implementations/aws-innovation-sandbox/

© 2021, Amazon Web Services, Inc. or its affiliates.

Security Guardians

culture *(n)*

- 教養、洗練、(ある国・ある時代の)文化、精神文明
- (伝承される信仰・伝統・習俗などの総体としての)文化、カルチャー、訓練、修養、養殖、栽培

tenet *(n)*

- (個人または集団が信奉する)主義、教義
- 公理、自明の理、原理

© 2021, Amazon Web Services, Inc. or its affiliates.

AWSセキュリティチームのTenets

1. 私達はお客様と私たちのAWSリソースへの不正アクセスを率先して防ぎます。継続的にシステムを評価し、露出を特定し、リスクを定量化し緩和することを妥協しません

2. 私達は、データに基づき、注意深く優先順位付けされた最も大きい潜在的リスクを可視化し、常に企業幹部に提供します

3. 私達は適切に、積極的にエスカレーション(上位層へ報告)し、セキュリティ課題を迅速に、高い判断力で解決します。まだ疑わしい状況であってもエスカレーションします

4. 私達はお客様のプライバシーと信頼の守護者(ガーディアン)です。セキュリティに関連する全てでお客様を支持します

5. 私達は、サードパーティーやオープンソースのソフトウェア含め、全てのAWSのセキュリティに責任を持ちます。たとえ、同じ企業で作られたものでも、当然とは思わず、全てのコンポーネントを広くテストします。もし何かが機能しなければ、使用を取りやめます

6. 私達はAWSにおいて全てのセキュリティに関する質問に対応します。私達が答えを知らない場合でも、回答が得られるまで責任を持ちます

7. 私達はビジネスにとって最も重要なセキュリティリスクに業務を集中させます。ビジネスが最優先であり、サービス開発チームの優先度はその次です。私達はそれぞれの思いを良く理解し、行動可能にし、適切なツールで支援します

(unless you know better ones…)

© 2021, Amazon Web Services, Inc. or its affiliates.

まとめ

1. Builderの存在がセキュリティを進化させる
2. セキュリティは自分達Builderの手で作り上げる
3. ガードレールでBuilderに自由を提供する

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates.

まとめ

1. Builderの存在がセキュリティを進化させる
2. セキュリティは自分達Builderの手で作り上げる
3. ガードレールでBuilderに自由を提供する

© 2021, Amazon Web Services, Inc. or its affiliates.