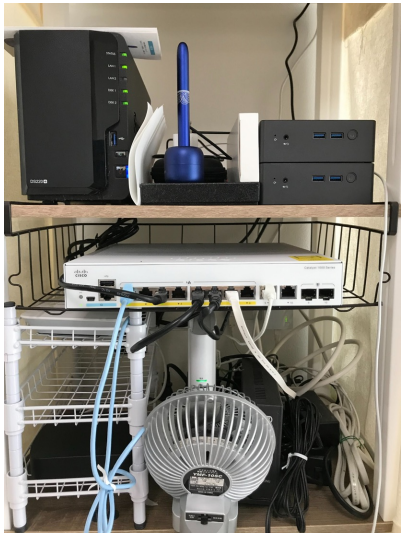
AWS 初心者が取り組んだ セキュリティ強化の 2 年間とこれから

弥生株式会社
開発本部　情報システム部　CCoE / インフラ
峯岸純也

弥生

自己紹介

- 弥生株式会社 開発本部 情報システム部 CCoE/インフラ TechL（Technical Leader）
- ねぎ（峯岸 純也：みねぎしじゅんや）
- 2020年1月に弥生に入社
  - インフラ経歴**ゼロ**でインフラチームへ
  - AWS経験もゼロ（※ここ大事）
- 弥生インフラ領域の何でも屋さんです
  - 前職はJava / C#メインで開発 etc
  - プログラミングが苦手
  - 自宅にCisco Catalyst 1000あります
- 最近のお仕事内容
  - AWSセキュリティ/ガバナンス
  - オンプレ→AWS移行
- 趣味
  - **お酒ミニボトル集め**



弥生

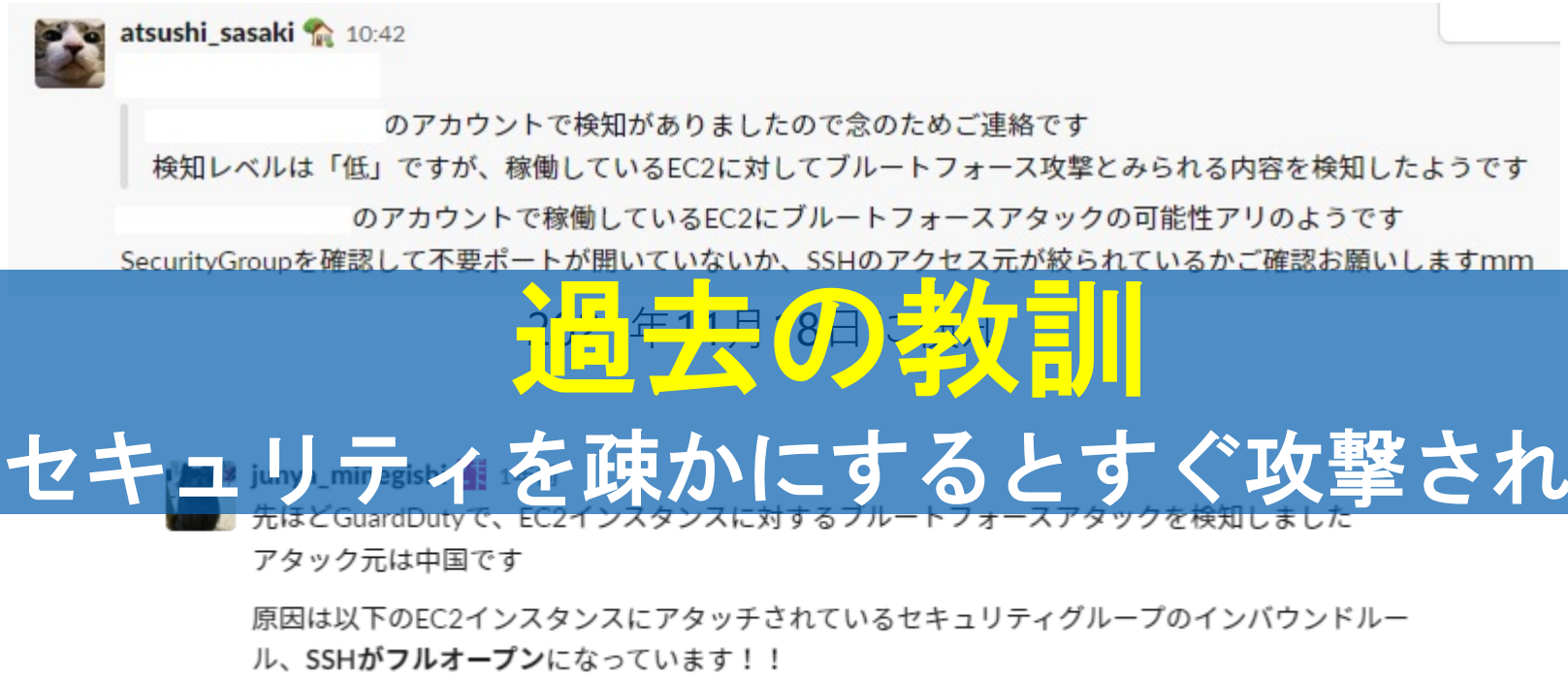
弥生のAWSに関連した数字

弥生のAWSにまつわる数字①

2021年10月～2022年9月：2件
2022年10月～2023年8月：0件

答え

- AWS環境でブルートフォースアタックを検知した件数です



過去の教訓

セキュリティを疎かにするとすぐ攻撃される

2022年03月10日に検知

弥生

弥生のAWSにまつわる数字②

2021年8月：23

2022年8月：66

2023年8月：132

答え

- AWS環境のアカウント数です

300〜500アカウント

規模を見据えた運用

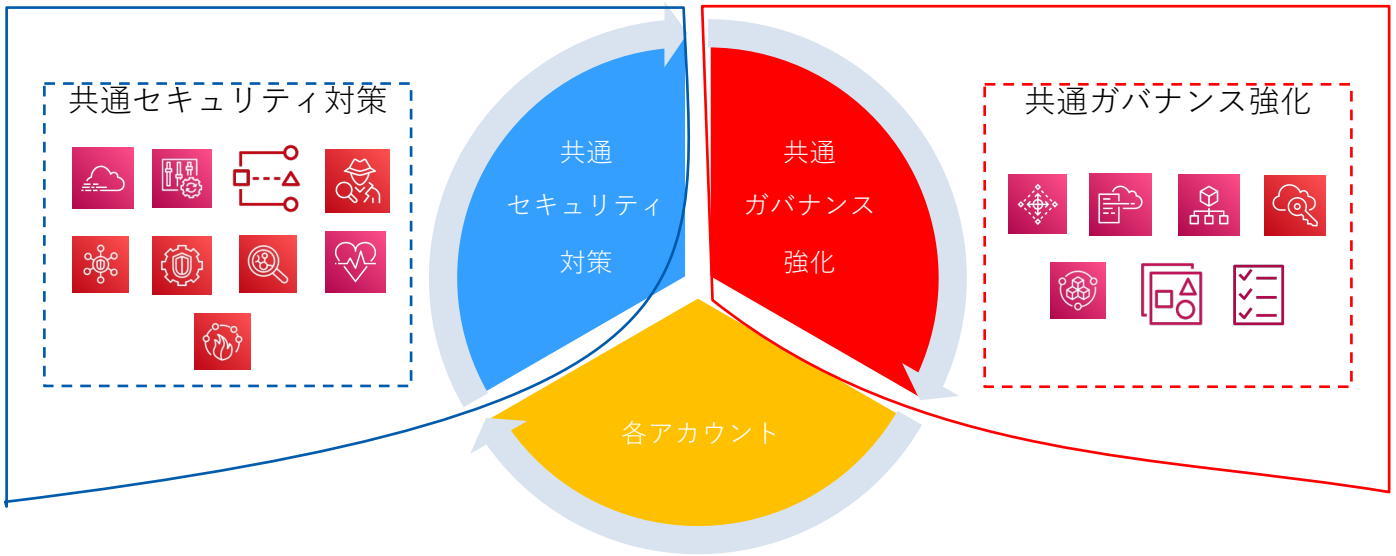
本日のお話

- 弥生で取り組んでいるセキュリティ施策
  - AWS SecurityHubの検知・自動修復対応
    - AWSでの自動化されたセキュリティ対応
      - https://aws.amazon.com/jp/solutions/implementations/automated-security-response-on-aws/
  - SIEM環境の構築
    - SIEM on Amazon OpenSearch Service
      - https://github.com/aws-samples/siem-on-amazon-opensearch-service/blob/main/README_ja.md

弥生のAWS環境の役割分担

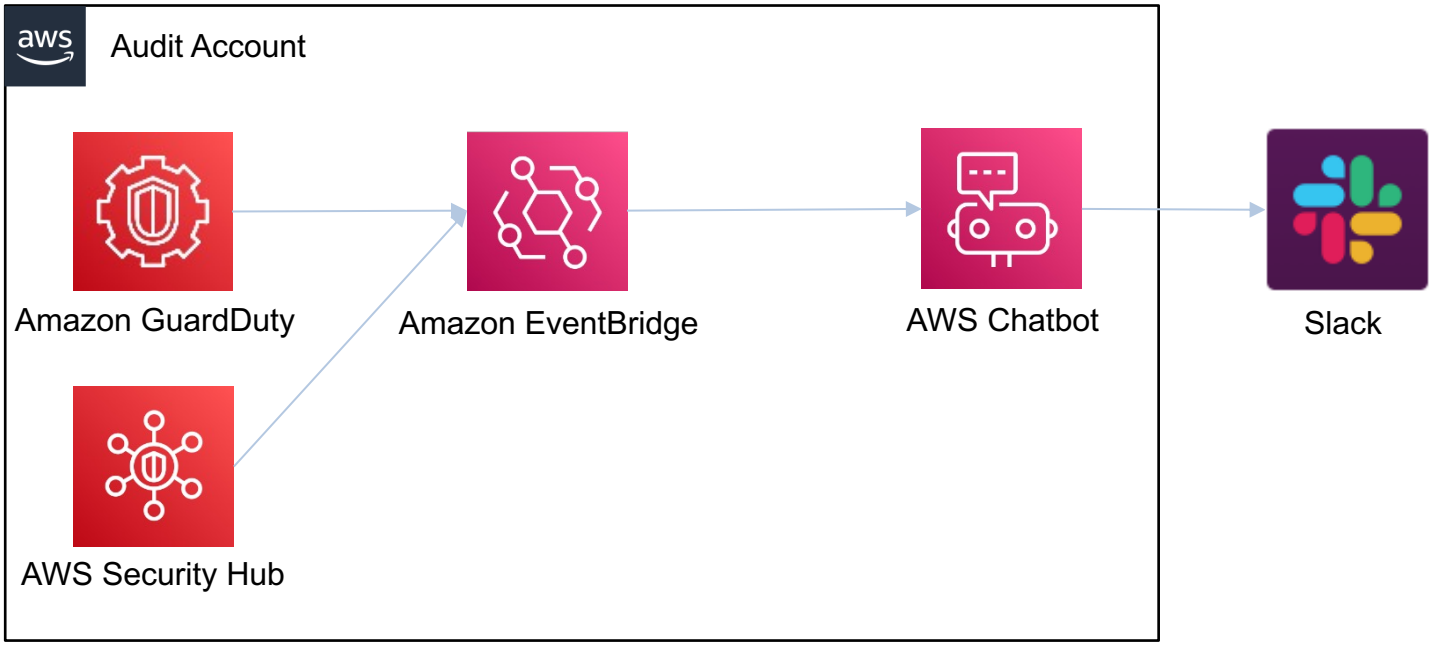
AWS環境の役割分担

- 共通セキュリティ対策：担当インフラチーム
  - AWS Security Hub + αのサービスを活用した自動修復+検知
    - 例：SSH/RDPフルオープンのセキュリティグループを自動修復
- 共通ガバナンス強化：担当インフラチーム
  - AWS Control Tower + AWS IAM Identity Centerによる防御、認証認可
    - 例：ルートユーザーとしてのアクションを許可しない
- 各アカウント：各サービス担当者
  - 各AWSアカウント内のセキュリティ
    - 例：セキュリティグループ設定の見直し、AWS WAFによる防御



弥生のAWSセキュリティ

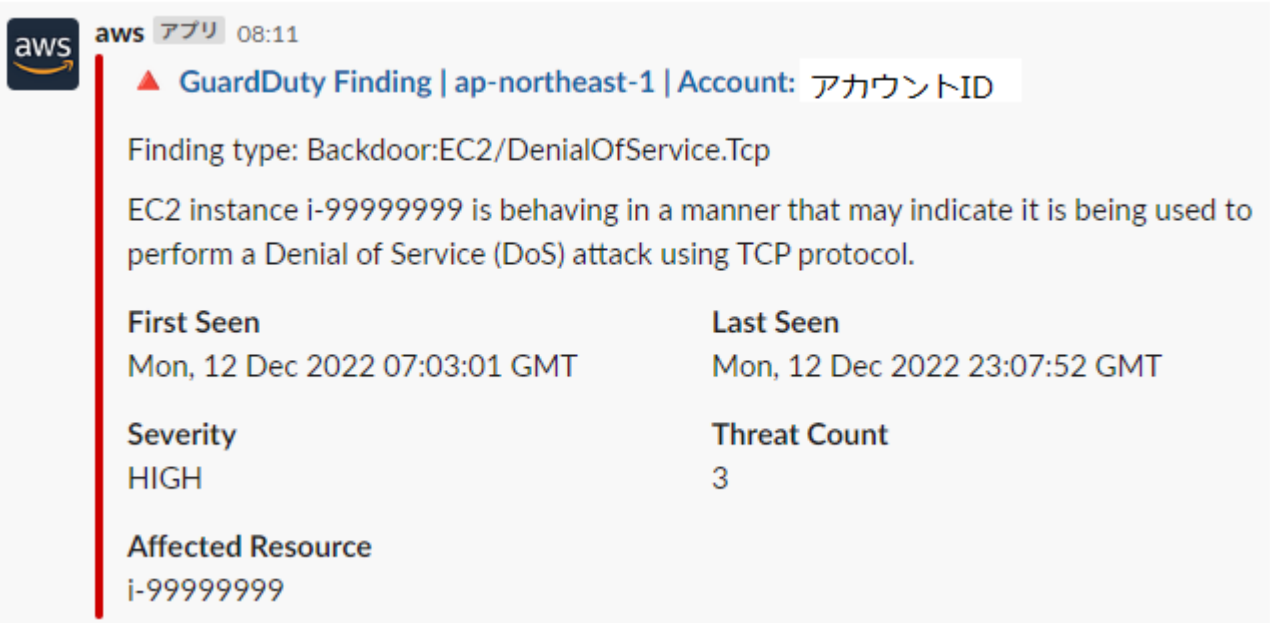
Amazon GuardDuty / AWS Security Hubの検知



- 検知の仕組みを導入した効果
  - メール通知は1日の受信件数が多くて見逃がすのでSlackへ
  - 全アカウントの検知内容を通知するチャンネルを用意

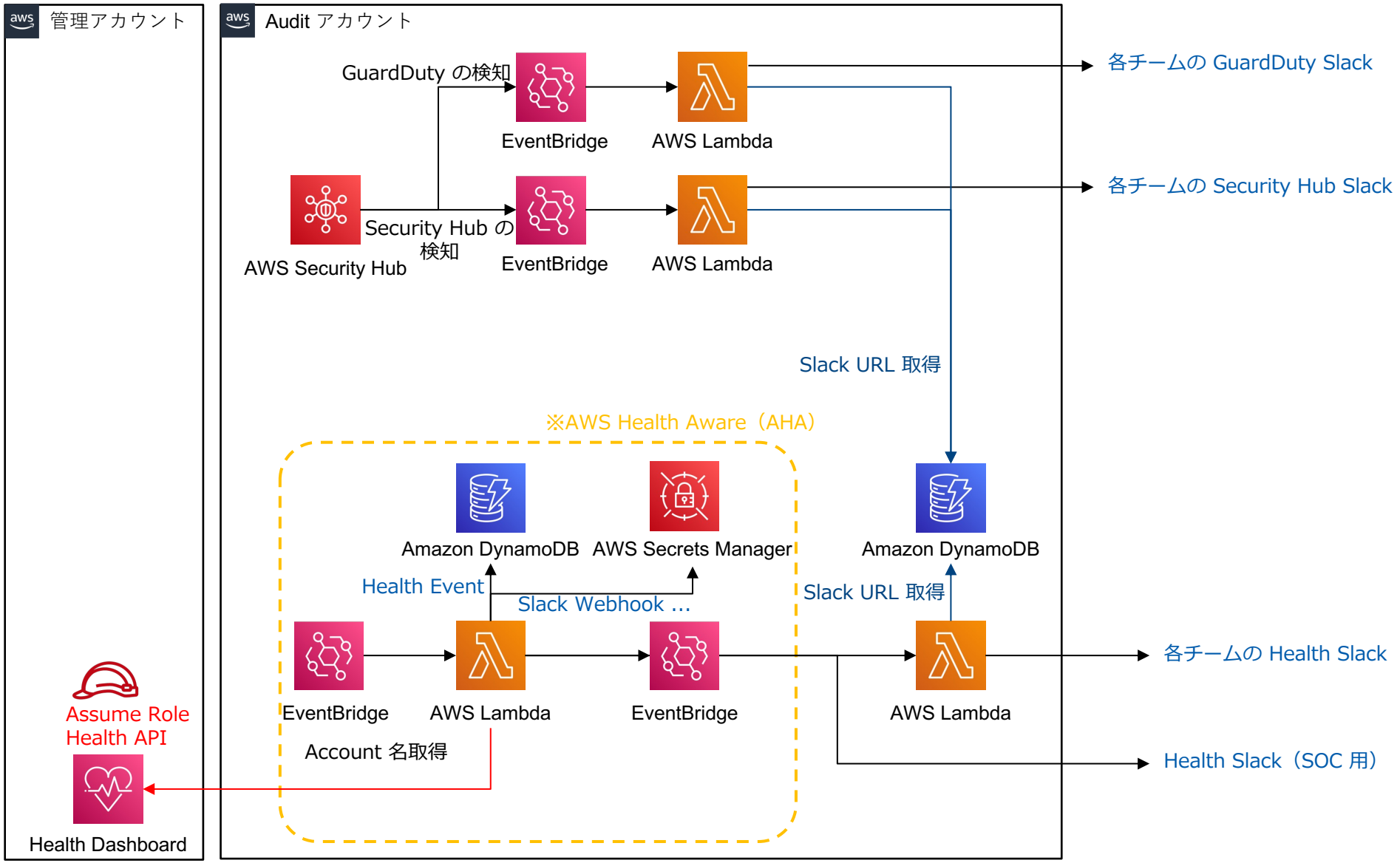
検知の課題

- 通知時にアカウントIDしか表示されない
  - 自チームが保有しているAWSアカウントに関する通知なのか、見てすぐわからないといった声が多数
- 各通知毎のSlackチャンネルに集約していた
  - AWS Health、Amazon GuardDuty、AWS Security Hubの通知を、それぞれ1つのSlackチャンネルにしていた
  - AWSアカウント数が増えるにつれて、情報がすぐ流れてしまうように



Slack通知のサンプル

各通知情報を各チームのSlackへ



※AWS Health Aware

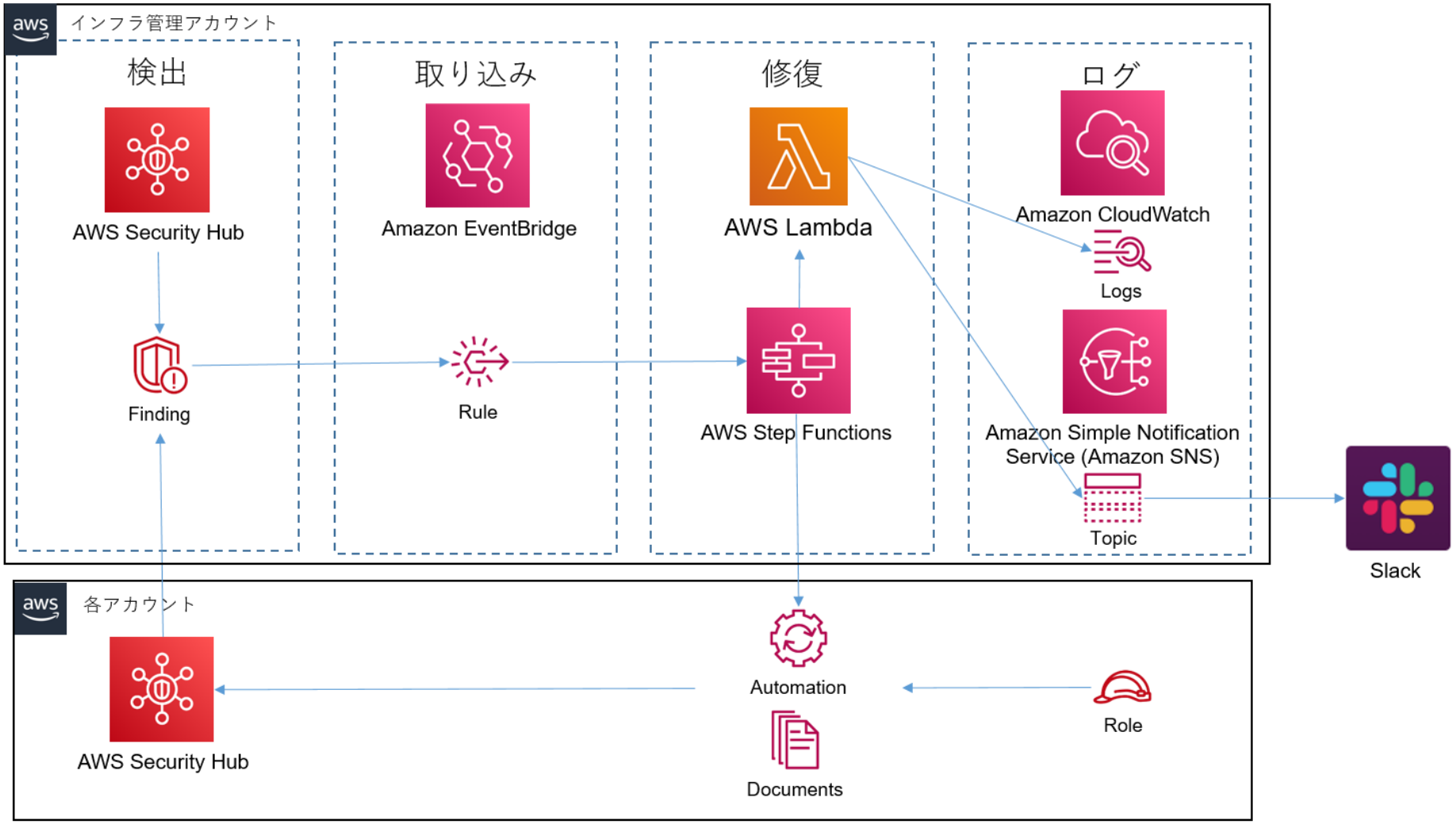
https://aws.amazon.com/jp/blogs/news/aws-health-aware-customize-aws-health-alerts-for-organizational-and-personal-aws-accounts/

弥生

AWS Security Hub検知の一部

ルールID	検知	アクション	統合ステータス	本番ステータス
CIS.1.12	ルートアカウントのアクセスキーが存在しないことを確認する	Slackへ通知	反映済	反映済
CIS.2.9	すべての VPC で VPC フロー ロギングを有効にする必要があります	Slackへ通知	反映済	反映済
APIGateway.1	API Gateway REST および WebSocket API の実行ログを有効にする必要があります	Slackへ通知	反映済	反映済
APIGateway.2	API Gateway REST API ステージは、バックエンド認証に SSL 証明書を使用するように構成する必要があります	Slackへ通知	反映済	反映済
APIGateway.4	API Gateway は WAF Web ACL に関連付ける必要があります	Slackへ通知	反映済	反映済
APIGateway.5	API Gateway REST API キャッシュ データは保存時に暗号化する必要があります	Slackへ通知	反映済	反映済
CloudFront.1	CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります	Slackへ通知	反映済	反映済
CodeBuild.1	CodeBuild GitHub または Bitbucket ソースリポジトリの URL は OAuth を使用する必要があります	Slackへ通知	反映済	反映済
CodeBuild.4	CodeBuild プロジェクト環境にはログ設定が必要です	Slackへ通知	反映済	反映済
DMS.1	Database Migration Service のレプリケーションインスタンスはパブリックであってはなりません	Slackへ通知	反映済	反映済
EC2.3	アタッチされた EBS ボリュームは保存時に暗号化する必要があります	Slackへ通知	反映済	―
EC2.4	停止した EC2 インスタンスは、指定された期間後に削除する必要があります	Slackへ通知	反映済	反映済
EC2.6	すべての VPC で VPC フロー ロギングを有効にする必要があります	Slackへ通知	反映済	反映済
EC2.8	EC2 インスタンスでは、Instance Metadata Service Version 2 (IMDSv2) を使用する必要があります	Slackへ通知	反映済	―
EC2.15	EC2 サブネットは、パブリック IP アドレスを自動的に割り当てるべきではありません	Slackへ通知	反映済	―
EC2.18	セキュリティグループは、許可されたポートのための無制限の着信トラフィックのみを許可する必要があります	Slackへ通知	反映済	反映済
EC2.19	セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません	Slackへ通知	反映済	反映済
EC2.20	AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります	Slackへ通知	反映済	反映済
EC2.23	EC2 Transit Gateway は VPC アタッチメントリクエストを自動的に受け付けるべきではありません	Slackへ通知	反映済	反映済
ECS.1	Amazon ECS タスク定義には、安全なネットワークモードとユーザー定義が必要です	Slackへ通知	反映済	反映済

AWS Security Hubの検知 / 自動修復



AWS Security Hubの検知 / 自動修復

ルールID	検知	アクション	統合ステータス	本番ステータス
CIS1.5	IAM パスワード ポリシーで少なくとも 1 つの大文字が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.6	IAM パスワード ポリシーで少なくとも 1 つの小文字が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.7	IAM パスワード ポリシーに少なくとも 1 つの記号が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.8	IAM パスワード ポリシーに少なくとも 1 つの数字が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.9	IAM パスワード ポリシーで最小パスワード長が 14 以上であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.10	IAM パスワードポリシーでパスワードの再使用が禁止されていることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.11	IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS4.1	0.0.0.0/0 からポート 22 への侵入を許可しません	該当のセキュリティグループを削除	反映済	反映済
CIS4.2	0.0.0.0/0 からポート 3389 への侵入を許可しません	該当のセキュリティグループを削除	反映済	反映済
CodeBuild.2	CodeBuild プロジェクトの環境変数には、クリアテキストの認証情報を含めないでください	Access/Secret KeyをSSMパラメータストアから読み込むよう変更	反映済	反映済
EC2.1	EBS スナップショットはパブリックであってはなりません	該当のスナップショットをプライベートへ変更	反映済	反映済
EC2.2	VPC のデフォルトのセキュリティグループはインバウンドトラフィックとアウトバウンドトラフィックを許可しません	インバウンド・アウトバウンドルール削除	反映済	反映済
EC2.7	EBS デフォルトの暗号化を有効にする必要があります	アカウントのリージョンごとのEBSのデフォルト暗号化設定を変更	反映済	反映済
IAM.7	IAM ユーザーのパスワード ポリシーには、強力な構成が必要です	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
lambda.1	Lambda 関数ポリシーはパブリックアクセスを禁止する必要があります	ポリシーを削除	反映済	反映済
RDS.1	RDS スナップショットはプライベートにする必要があります	該当のスナップショットをプライベートへ変更	反映済	反映済
RDS.2	RDS DBインスタンスはパブリックアクセスを禁止する必要があります	該当のインスタンスをプライベートへ変更	反映済	反映済
RDS.16	タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります	タグをスナップショットにコピーする設定を有効化に変更	反映済	反映済
RedShift.1	Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります	パブリックアクセスを無効化	反映済	反映済
RedShift.3	Amazon Redshift クラスターでは、自動スナップショットを有効にする必要があります	自動スナップショット設定の有効化	反映済	反映済
S3.1	S3 Block Public Access 設定を有効にする必要があります	アカウントレベルでのパブリックアクセスの禁止の設定を変更	反映済	反映済
S3.2	S3 バケットはパブリック読み取りアクセスを禁止する必要があります	バケットの設定をプライベートに変更	反映済	反映済
S3.3	S3 バケットはパブリック書き込みアクセスを禁止する必要があります	バケットの設定をプライベートに変更	反映済	反映済
S3.4	S3 バケットでは、サーバー側の暗号化を有効にする必要があります	バケットの暗号化設定を有効化	反映済	反映済
S3.5	S3 バケットには、SSLを使用するためのリクエストが必要です	バケットポリシーにHTTPS 経由のデータ送信のみを受け入れるポリシーを追加	反映済	反映済
S3.6	バケットポリシーで他の AWS アカウントに付与される S3 アクセス権限は制限する必要があります	バケットポリシーに拒否ポリシーを追加	反映済	反映済
S3.8	S3 ブロックパブリックアクセス設定は、バケットレベルで有効になっている必要があります	バケットの設定をプライベートに変更	反映済	反映済

AWS Security Hubの検知と自動修復

ルールID	検知	アクション	統合ステータス	本番ステータス
CIS.1.12	ルートアカウントのアクセスキーが存在しないことを確認する	Slackへ通知	反映済	反映済
CIS.2.9	すべての VPC で VPC フロー ロギングを有効にする必要があります	Slackへ通知	反映済	反映済
APIGateway.1	API Gateway REST および WebSocket API の実行ログを有効にする必要があります	Slackへ通知	反映	反映済
APIGateway.2	API Gateway REST API ステージは、バックエンド認証に SSL 証明書を使用するように構成する必要があります	Slackへ通知	反映	反映済
APIGateway.4	API Gateway は WAF Web ACL に関連付ける必要があります	Slackへ通知	反映済	反映済
APIGateway.5	API Gateway REST API キャッシュ データは保存時に暗号化する必要があります	Slackへ通知	反映	反映済
CloudFront.1	CloudFr	en		
CodeBuild.1	CodeBu			
CodeBuild.4	CodeBu			
DMS.1	Databas			
EC2.3	アタッチ			
EC2.4	停止した			
EC2.6	すべての			
EC2.8	EC2 イン			
EC2.15	EC2 サブ			
EC2.18	セキュリ			
EC2.19	セキュリ			
EC2.20	AWS Sit			
EC2.23	EC2 Tra			
EC5.1	Amazon			

ルールID	検知	アクション	統合ステータス	本番ステータス
CIS1.5	IAM パスワード ポリシーで少なくとも 1 つの大文字が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.6	IAM パスワード ポリシーで少なくとも 1 つの小文字が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.7	IAM パスワード ポリシーに少なくとも 1 つの記号が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.8	IAM パスワード ポリシーに少なくとも 1 つの数字が必要であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.9	IAM パスワード ポリシーで最小パスワード長が 14 以上であることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.10	IAM パスワードポリシーでパスワードの再使用が禁止されていることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS1.11	IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認する	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
CIS4.1	0.0.0.0/0 からポート 22 への侵入を許可しません	該当のセキュリティグループを削除	反映済	反映済
CIS4.2	0.0.0.0/0 からポート 3389 への侵入を許可しません	該当のセキュリティグループを削除	反映済	反映済
CodeBuild.2	CodeBuild プロジェクトの環境変数には、クリアテキストの認証情報を含めないでください	Access/Secret KeyをSSMパラメータストアから読み込むよう変更	反映済	反映済
EC2.1	EBS スナップショットはパブリックであってはなりません	該当のスナップショットをプライベートへ変更	反映済	反映済
EC2.2	VPC のデフォルトのセキュリティグループはインバウンドトラフィックとアウトバウンドトラフィックを許可しません	インバウンド・アウトバウンドルール削除	反映済	反映済
EC2.7	EBS デフォルトの暗号化を有効にする必要があります	アカウントのリージョンごとのEBSのデフォルト暗号化設定を変更	反映済	反映済
IAM.7	IAM ユーザーのパスワード ポリシーは、強力な構成が必要です	IAM パスワードポリシーを強力な構成に変更	反映済	反映済
lambda.1	Lambda 関数ポリシーはパブリック アクセスを禁止する必要があります	ポリシーを削除	反映済	反映済
RDS.1	RDS スナップショットはプライベートにする必要があります	RDSのスナップショットをプライベートへ変更	反映済	反映済
RDS.2	RDS DBインスタンスはパブリックアクセスを禁止する必要があります	パブリックアクセスを無効化	反映済	反映済
RDS.16	タグをスナップショットにコピーするように RDS DB インスタンスを構成する必要があります	タグをスナップショットにコピーするように変更を有効化に変更	反映済	反映済
RedShift.1	Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります	パブリックアクセスを無効化	反映済	反映済
RedShift.3	Amazon Redshift クラスターでは、自動スナップショットの保持期間を 7 日以上に設定する必要があります	スナップショットの保持期間の有効化	反映済	反映済
S3.1	S3 Block Public Access 設定を有効にする必要があります	アカウントレベルでのパブリックアクセスの禁止の設定	反映済	反映済
S3.2	S3 バケットはパブリック読み取りアクセスを禁止する必要があります	バケットの設定をプライベートに変更	反映済	反映済
S3.3	S3 バケットはパブリック書き込みアクセスを禁止する必要があります	バケットの設定をプライベートに変更	反映済	反映済
S3.4	S3 バケットでは、サーバー側の暗号化を有効にする必要があります	バケットの暗号化設定を有効化	反映済	反映済
S3.5	S3 バケットには、SSL を使用するためのリクエストが必要です	バケットポリシーにHTTPS 経由のデータ送信のみを受け入れるポリシーを追加	反映済	反映済
S3.6	バケットポリシーで他の AWS アカウントに付与される S3 アクセス権限は制限する必要があり	バケットポリシーに拒否ポリシーを追加	反映済	反映済
S3.8	S3 ブロックパブリックアクセス設定は、バケットレベルで有効になっている必要があります	バケットの設定をプライベートに変更	反映済	反映済

検知

自動修復

1年でここまで増加

2023年8月

自動修復27件、検知86件

2022年9月

自動修復8件、検知19件

弥生

検知・自動修復を啓蒙した結果

開発チームの
セキュリティ意識

認知度
Up

良い効果が出てきました

AWS Security Hubスコア

本番環境

18pt up

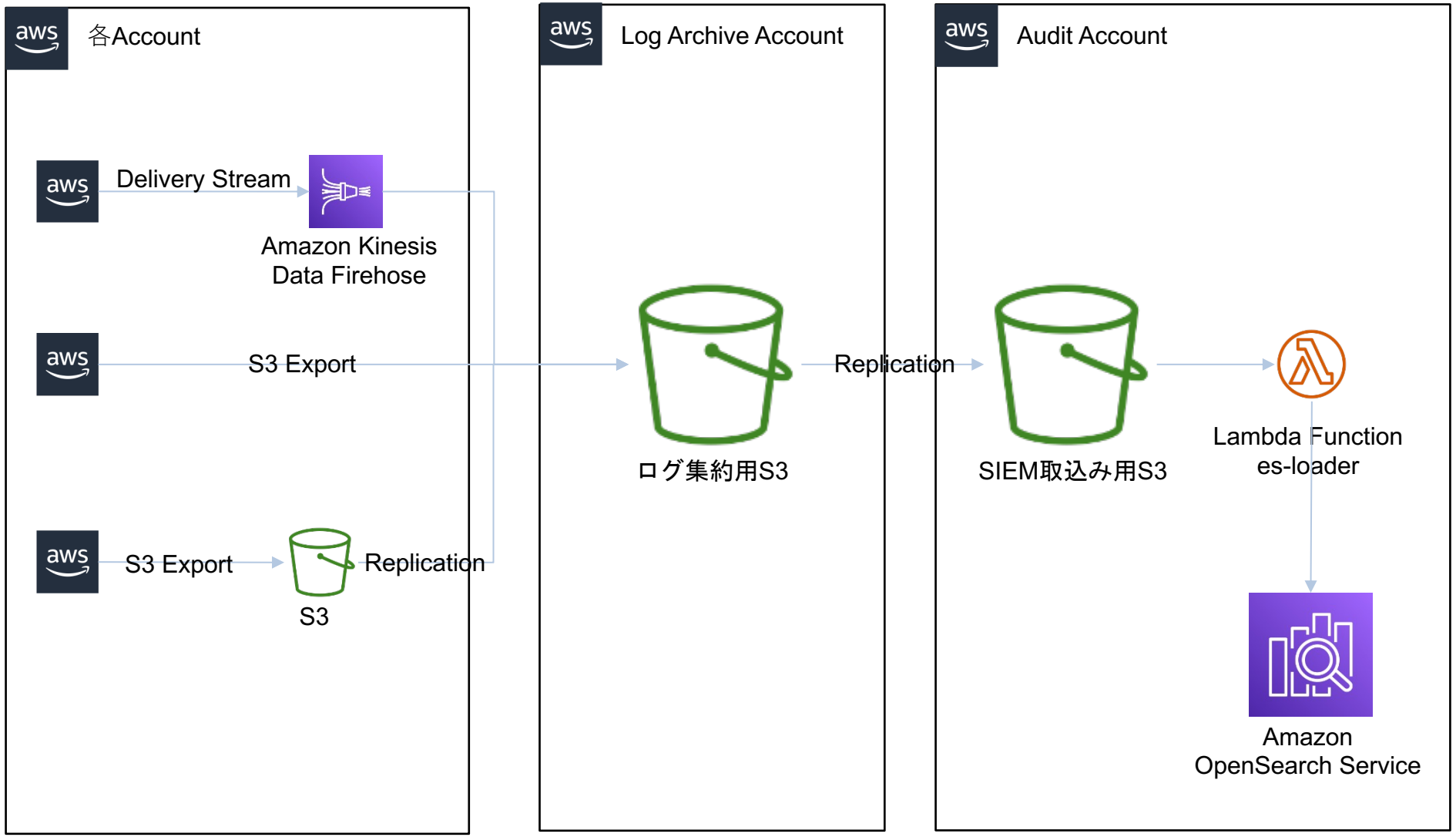
本番環境以外

28pt up

弥生


弥生のSIEM

SIEM on Amazon OpenSearch Service全体構成図



活用方法

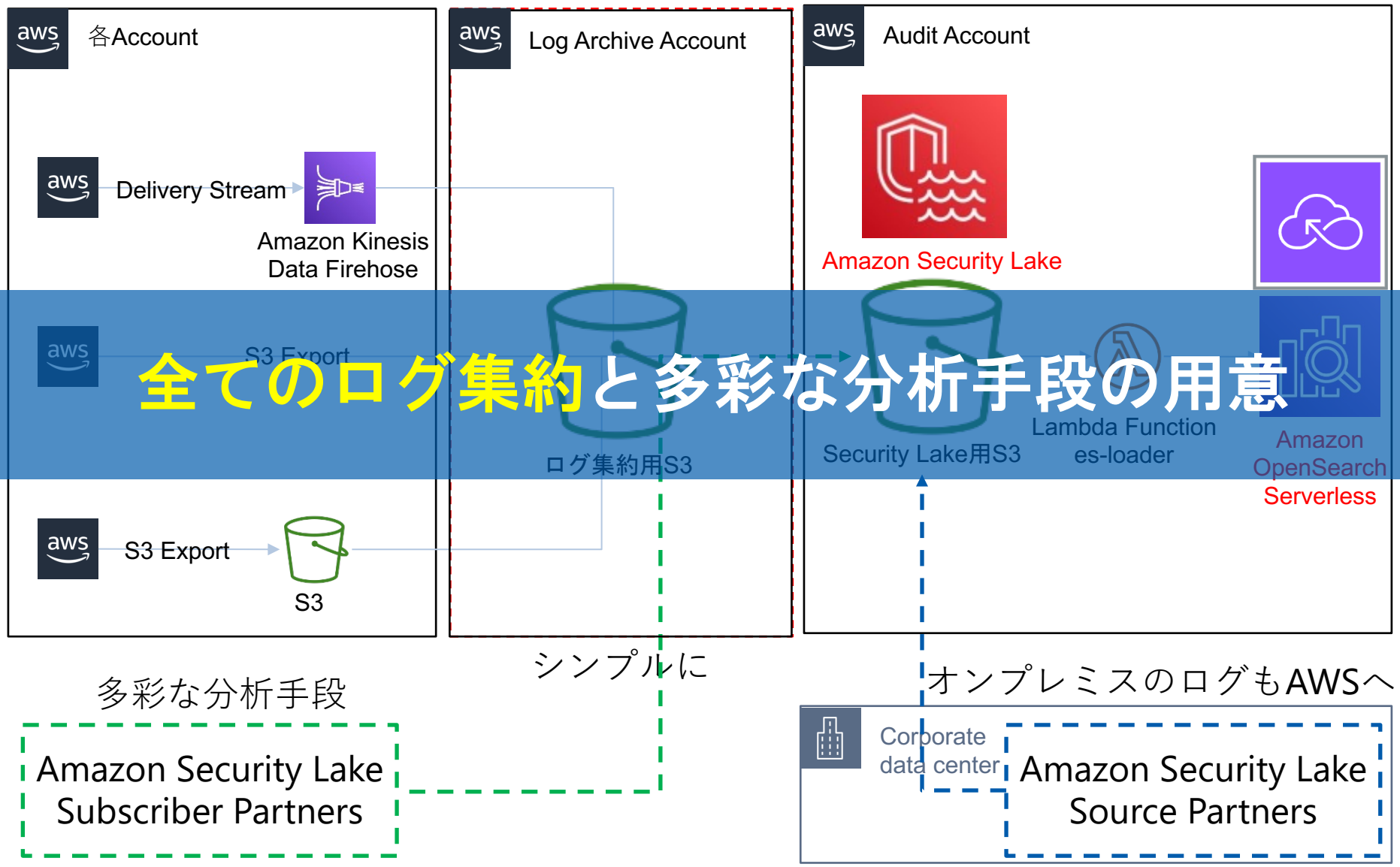
- 各種検知時
  - Amazon Guard Duty
    - Amazon Detectiveと共にCloudTrailやVPC Flow logsなどをSIEM環境で相関分析
  - AWS Security Hub
    - SIEM環境で主にCloudTrailを確認して、いつ、だれが、何をやったのか、を調査
- 障害発生時
  - VPC Flow logsやその他AWSのログ情報を相関分析

各AWSのアプリケーションログ＋オンプレ環境のログ分析も可能なSIEM環境へ

Amazon OpenSearch Serverless
Amazon Security Lake

- Amazon OpenSearch Serverless
  - 管理が容易
    - クラスタのサイジング、スケーリング、チューニング、およびシャードとインデックスのライフサイクル管理が不要
  - 速度
    - リソースを自動的にスケールし、高速なデータ取り込みレートとクエリ応答時間を一貫して維持
  - エコシステム
    - 同じOpenSearchクライアント、パイプライン、APIを使用して数秒で利用を開始できる
  - 費用対効果
    - 事前のリソースプロビジョニングは不要
- Amazon Security Lake
  - セキュリティに特化したデータレイクサービス
  - クラウド・オンプレミスおよびカスタムソースからのセキュリティデータをデータレイクに集約
  - セキュリティデータの制御・統制をしながら任意のツールと連携可能

SIEM on Amazon OpenSearchのアーキテクチャ変更



弥生

弥生のこれから

これからのセキュリティ＆ガバナンス

- セキュリティ＆ガバナンス向上へ向けた取り組み
  - AWS Security Hubのスコア向上→維持への仕組み
    - 各チームメンバーへのセキュリティ意識のさらなる醸成
  - SIEM環境の改善と全社展開
    - ログの集約（Amazon Security Lake）
    - 運用負荷軽減（Amazon OpenSearch Serverless）
    - 社内規程整備

AWS新サービス / ソリューションを積極的に活用

ご清聴ありがとうございました

弥生