三十三回 「アップデート紹介とちょっぴり
DIVE DEEP する AWS の時間」- SECURITY 編 -

Amazon GuardDuty

2023 夏

Yuki Yoshida

Solution Architect
Amazon Web Services Japan G.K.

自己紹介

名前: 吉田 裕貴 (よしだ ゆうき)
所属: アマゾンウェブサービスジャパン合同会社
DNBソリューション本部
ISV/SaaSソリューショングループSaaSソリューション部
ソリューションアーキテクト
経歴:
EC や FinTech 領域で AWS 環境の管理を担当
AWS Authorized Instructor として有償トレーニングを提供

好きなAWSサービス：
Amazon GuardDuty

本日ご紹介する内容について

Amazon GuardDuty が標準機能に加えて追加で利用できる各種 Protection について概要と検知のデモを交えた機能紹介をします。

Amazon GuardDuty そのものの機能についての説明は時間の都合上割愛します。

Agenda

- Amazon GuardDuty EKS Protection
- Amazon GuardDuty Lambda Protection
- Amazon GuardDuty Malware Protection
- Amazon GuardDuty RDS Protection
- Amazon GuardDuty S3 Protection

Amazon GuardDuty Protection 機能

Protection 一覧

プロテクション名	概要
GuardDuty EKS Protection	Amazon EKS クラスターへの脅威検知をするために利用できる機能
GuardDuty Lambda Protection	AWS Lambda 関数への脅威検知をするために利用できる機能
GuardDuty Malware Protection	Amazon EC2 インスタンスとコンテナワークロードにアタッチされた Amazon EBS ボリュームに対する追加のマルウェアスキャンのために利用できる機能
GuardDuty RDS Protection	Amazon Aurora データベースへの不審なログインを検知するために利用できる機能
GuardDuty S3 Protection	Amazon S3 バケット内のデータのセキュリティリスクを特定するために、オブジェクトレベルの API オペレーションを モニタリングする機能

Amazon GuardDuty は、基本的なログデータソースに加えて、他の AWS サービスからの追加データを使用して、潜在的なセキュリティ脅威を監視および分析できます。
Protection 機能は、 GuardDuty の脅威検出機能を強化し、追加の保護機能を有効にすることで得られる機能です。

Amazon GuardDuty EKS Protection

Amazon GuardDuty EKS Protection

Amazon EKS クラスターへの不正なアクティビティを監視

設定の問題

- ダッシュボードが公開されていないか？
- デフォルトのサービスアカウントへの管理者権限付与されていないか？
- Anonymous ユーザーへの権限付与されていないか？

不正アクセス

- データの探索、取得、変更の送信元が
  - Tor (匿名通信)
  - 漏洩した認証情報使用
  - 不正な IP アドレス

などではないか？

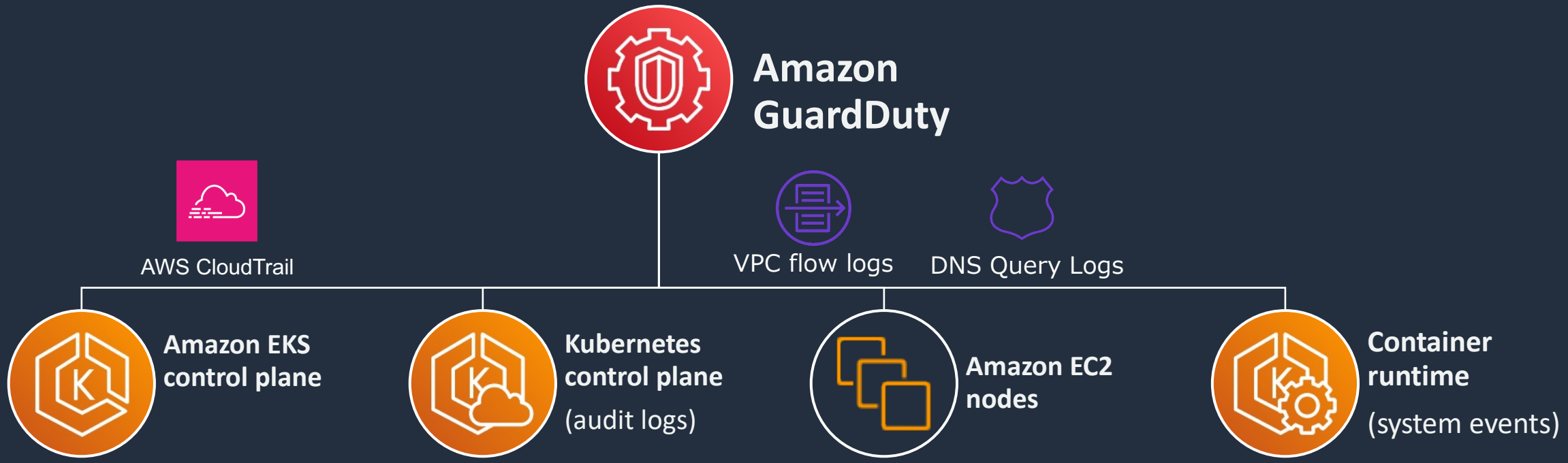
疑わしいふるまい

- Kubernetes の System Pod 内で実行されていないか？
- 機密性の高いホストパスへマウントされていないか？
- 特権権限のコンテナ起動されていないか？

Amazon GuardDuty は、Amazon EKS の監査ログを分析することにより Amazon EKS クラスタのコントロールプレーンのアクティビティを継続的に監視します

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/kubernetes-protection.html

EKS Audit Log Monitoring の仕組み



EKS Runtime Monitoring

EKS Runtime Monitoring

Amazon EKS クラスターのランタイムイベントを監視

ノードとコンテナのランタイムに対する脅威検出

- セキュリティエージェントを介して Amazon EKS を監視する
- ファイルアクセス、プロセス実行、ネットワーク接続などコンテナ実行時のアクティビティを可視化する
- コンテナ環境からの特権昇格の試みを検出する

- 既知のコンテナ攻撃技術に合わせて 20 種類以上※1 の行為検出を追加提供します
- セキュリティエージェントを追加でデプロイする必要があります

[1]GuardDuty EKS 監査ログモニタリングと組み合わせると、Amazon EKS デプロイに対する脅威を特定するように調整された検出が 50 件以上になります。

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty-eks-runtime-monitoring.html

Amazon GuardDuty Lambda Protection

Amazon GuardDuty Lambda Protection

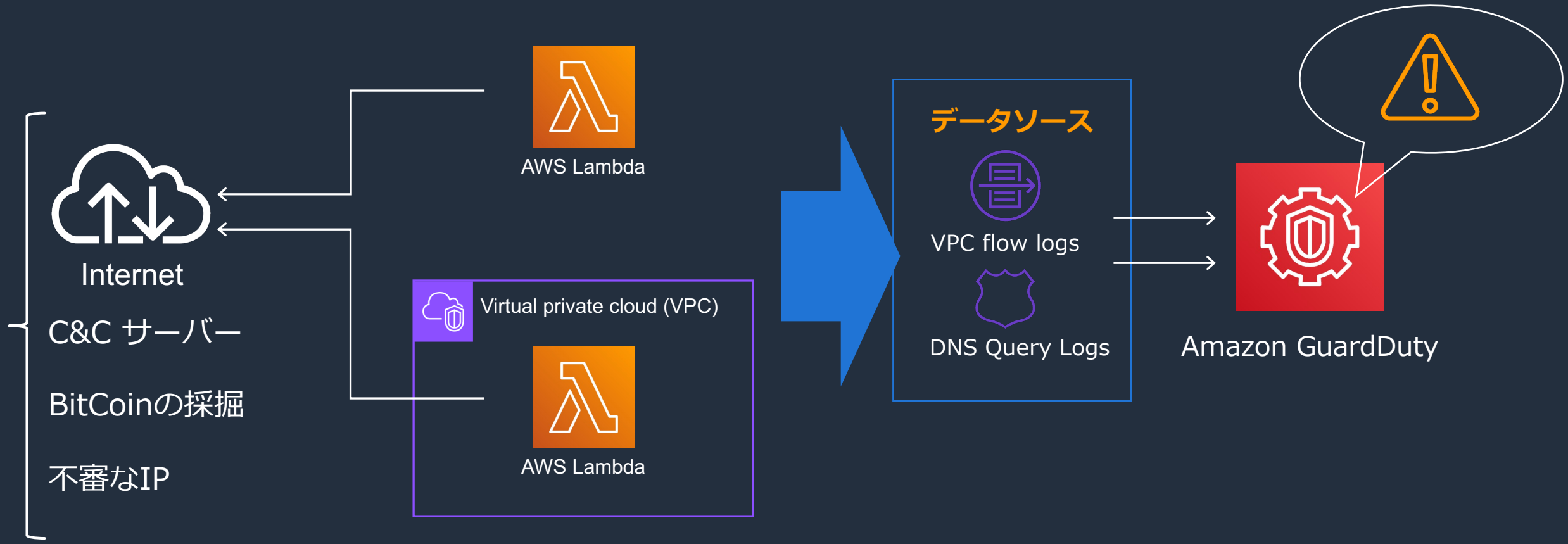
AWS Lambda に対する脅威のプロアクティブな検出を提供

疑わしいふるまい
• 既知の C&C サーバに関連する IP アドレスを問い合わせをしている • 仮想通貨関連の活動に関連する IP アドレスを問い合わせしている • マルウェアによって盗まれたデータを保持しているとされるリモートホストと通信している

- AWS Lambda 関数を呼び出すことによって生成されたネットワークアクティビティログを監視します
- Amazona VPC ネットワークを使用する AWS Lambda の場合 VPC フローログを追加で有効にする必要はありません

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/lambda-protection.html

Amazon GuardDuty Lambda Protection の仕組み



Amazon GuardDuty Malware Protection

Amazon GuardDuty Malware Protection の対象範囲

Amazon EC2 対象範囲

Amazon EC2 instances

Amazon ECS

Amazon EKS

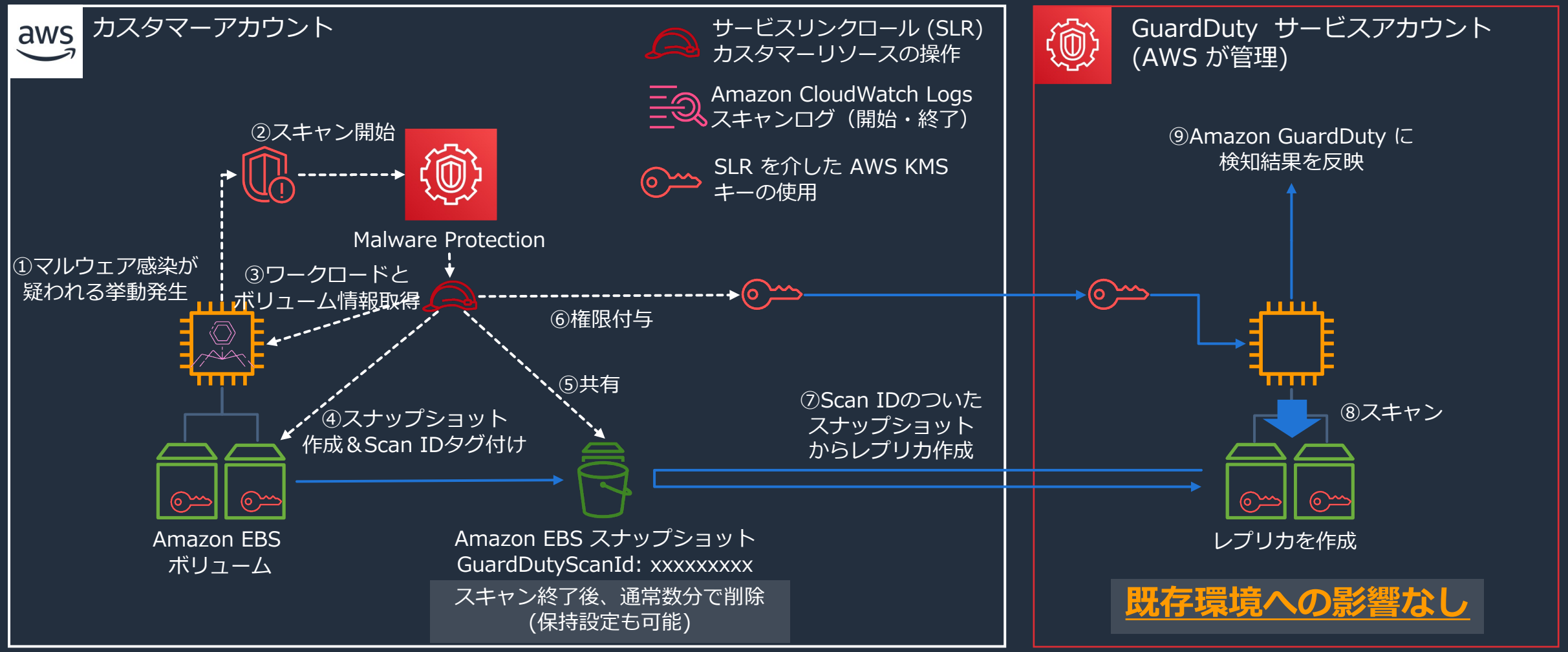
Amazon EC2 上で独自に管理しているコンテナ

マルウェアスキャンの実行タイミング

- Amazon GuardDuty が潜在的に感染した可能性のある Amazon EC2 インスタンスの活動を検知すると自動的にスキャン開始
- 一つの Amazon EC2 インスタンスにおけるスキャン間隔は 24 時間
- Amazon GuardDuty による検出が複数回あったとしても、前回のスキャンから 24 時間未満であれば追加のスキャンは開始されない

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/malware-protection.html

Amazon GuardDuty Malware Protection仕組み



エージェントレス＆性能影響を生じないスキャンを実施

Amazon GuardDuty RDS Protection

Amazon GuardDuty RDS Protection

Amazon Relational Database Service への疑わしいログインを検知

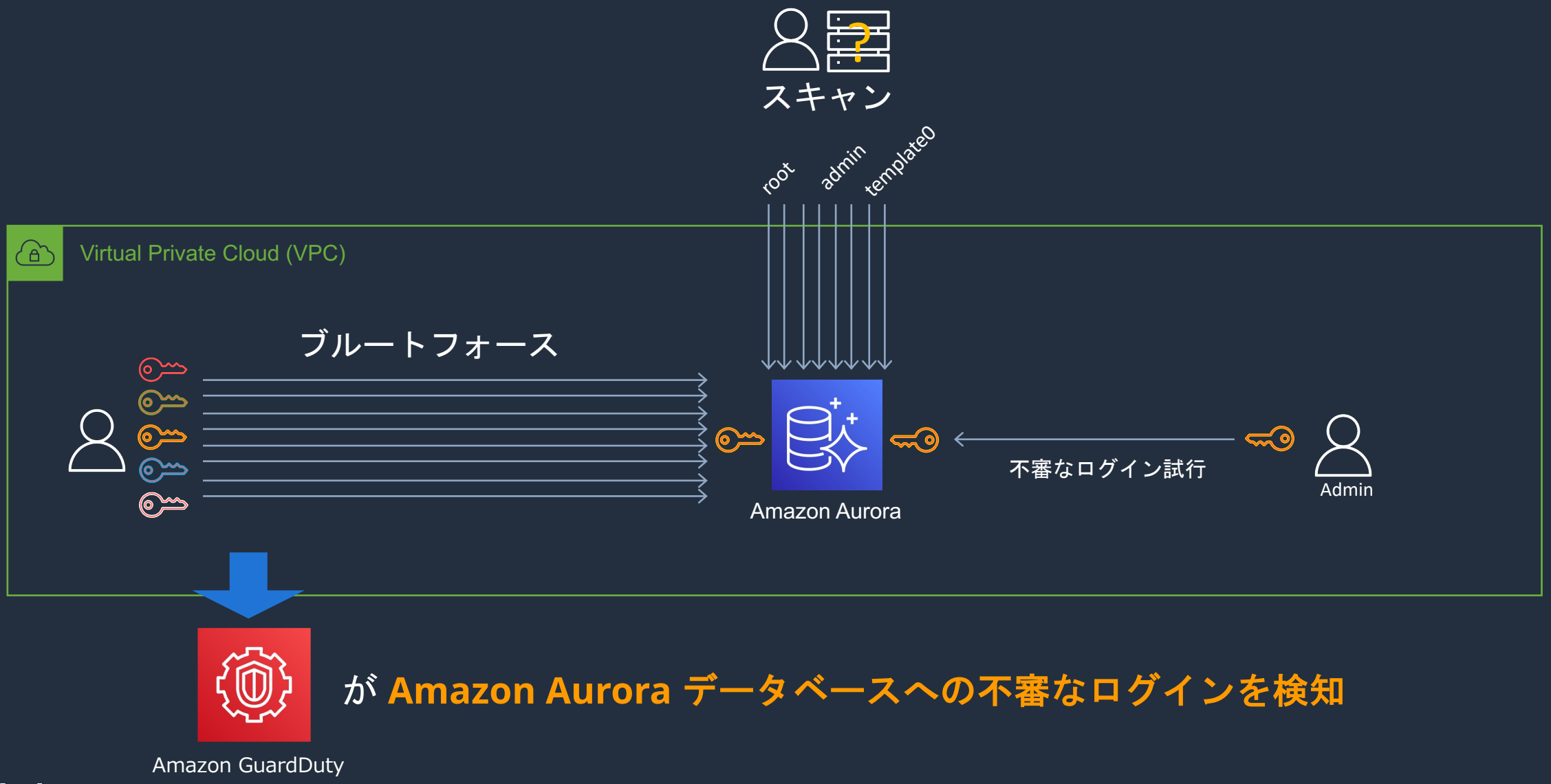
異常なログイン動作の検出

- DB ユーザーが異常な方法でログインに成功
- 異常な方法でのログインの失敗

- 手動で有効化することで利用できます
- RDS Protection は次の Aurora データベースのバージョンをサポートしています。
- サポートされている Amazon Aurora データベースバージョンはドキュメント※1 を参照

[1] https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/rds-protection.html

Amazon GuardDuty RDS Protection の仕組み



が **Amazon Aurora データベースへの不審なログインを検知**

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/rds-protection.html

Amazon GuardDuty S3 Protection

Amazon GuardDuty S3 Protection

Amazon S3 内のデータに対する脅威のプロアクティブな検出を提供

- アカウント内の全ての Amazon S3 バケットを、自動的に継続的に監視する
- 新規に Amazon GuardDuty を有効化すると、自動的に有効化される

ポリシー

- バケットが公開されていないか？
- S3 パブリックアクセスが有効になっていないか？
  ブロックパブリックアクセスの無効化がされていないか？
- ロギングが停止されていないか？
- ルートアカウントが使用されていないか？

不正アクセス

- データの探索、取得、変更の送信元が
  - Tor (匿名通信)
  - 漏洩した認証情報使用
  - 不正な IP アドレス

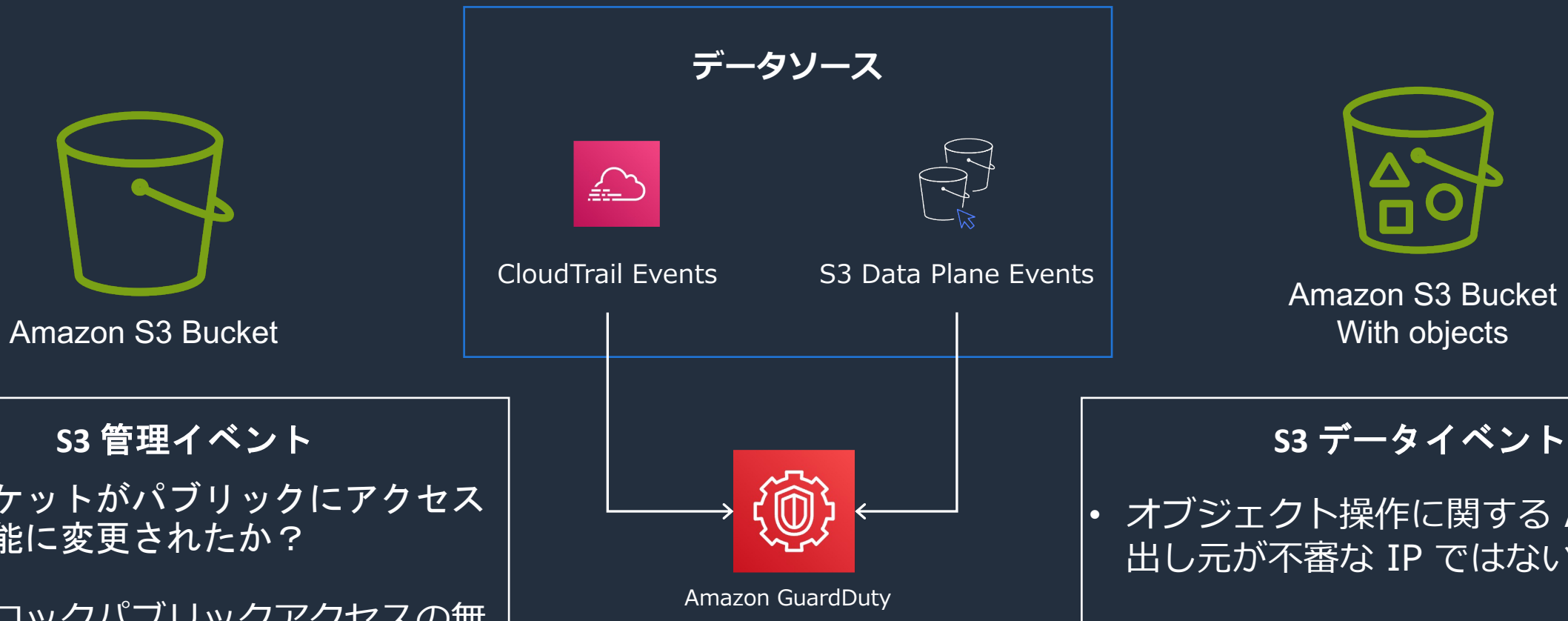
などではないか？

異常なふるまい

- 攻撃者が侵入を試みるためにがネットワークからデータを収集しようとしていないか？
- 攻撃者が悪意のあるデータや不正なデータを書き込もうとしていないか？
- 攻撃者が侵入を試みるためにツールを使ったアクセスをしていないか？

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/s3-protection.html

Amazon GuardDuty S3 Protection の仕組み



S3 管理イベント

- バケットがパブリックにアクセス可能に変更されたか？
- ブロックパブリックアクセスの無効化がされたか？

S3 データイベント

- オブジェクト操作に関する API 呼び出し元が不審な IP ではないか？

S3 Protection を有効にすることを強く推奨しています

Appendix
検出結果タイプ

各 Protection 機能の検出結果タイプ

各 Protection 機能が生成する検出結果タイプの完全な一覧は下記ドキュメントを確認してください。

- Kubernetes 監査ログの検出結果タイプ
- EKS Runtime Monitoring の検出結果タイプ
- Lambda Protection の検出結果タイプ
- Malware Protection の検出結果のタイプ
- RDS Protection の検出結果タイプ
- S3 の検出結果タイプ

Thank you!