AWS FOR SECURITY

AWS サービスで実現するセキュリティ
～初めの一歩から大規模環境まで～

アマゾン ウェブ サービス ジャパン合同会社

AWS 環境を管理するセキュリティ担当者のお悩み

- システムごとに**サーバーレス・コンテナなど**様々な技術が使われていてセキュリティの検討が追いついていない
- 利用している **AWS サービス数が多く**、リスクが把握しきれない
- 環境ごとに**ログが点在し**、各現場ごとに個別ルールで収集されている
- 管理すべき **AWS アカウントが多数存在**する

etc.

AWS の脅威検知とインシデント対応サービスを活用し、
包括的な脅威やリスクを可視化することから始めてみませんか？

AWS の脅威検知とインシデント対応のサービス

セキュリティ監視と脅威検知

AWS 内のワークロードの
アイデンティティ、ネットワーク
アクティビティと統合

Amazon GuardDuty
脅威と
異常なふるまいを検出

Amazon Macie
機微情報の検出

Amazon Inspector
脆弱性管理

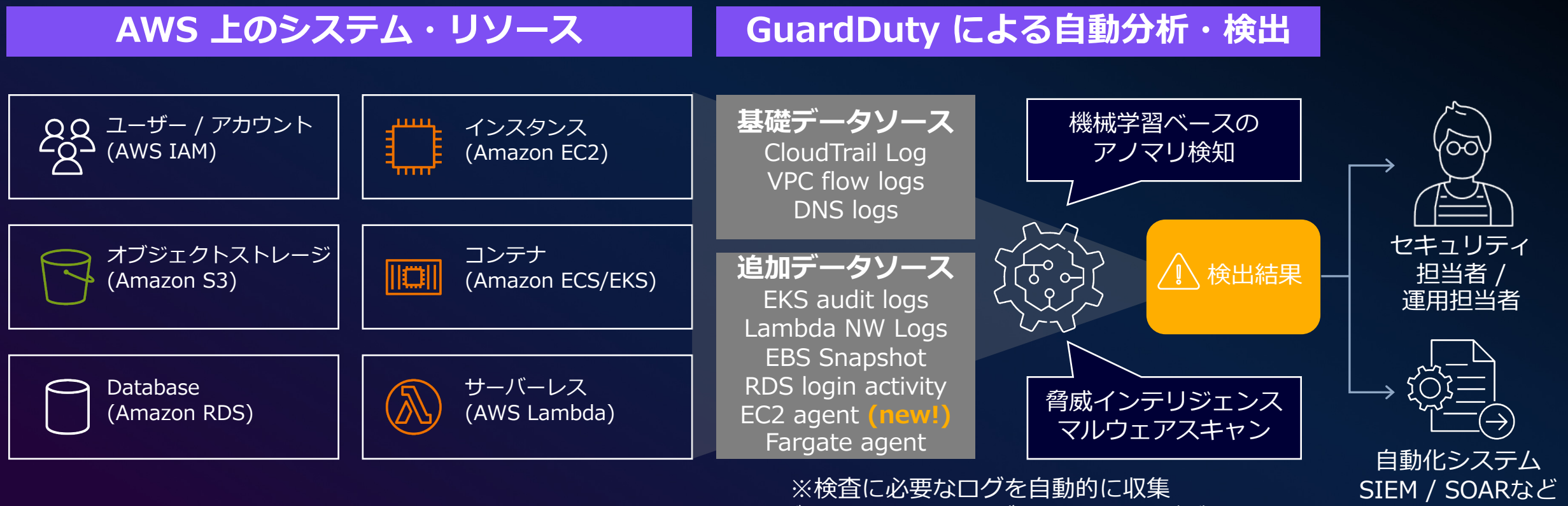
AWS Security Hub
脅威の一元管理

Amazon Detective
イベントと
検出結果の調査

Amazon Security Lake
ログの正規化と
一元管理

Amazon GuardDuty

ワンクリックで自動的にログを分析し、AWS アカウントとワークロードに対する
不審なアクティビティを継続的にモニタリングすることができる脅威検知サービス



※検査に必要なログを自動的に収集
ユーザー側での事前のログ有効化は不要だが、
脅威検出後の調査に必要なログは別途取得を推奨

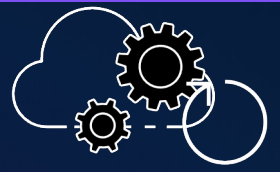
AWS Security Hub

セキュリティのベストプラクティスのチェックを行い、アラートを集約し、
自動修復を可能にするクラウドセキュリティ体制管理サービス

セキュリティのベストプラクティスからの逸脱を自動チェック

フレームワークや標準に準拠した
コントロールが用意されているため
必要なものを有効化する

- AWS FSBP
- CIS AWS Foundational Benchmark
- NIST SP 800-53
- PCI DSS
- AWS リソースタグ付け標準



AWS 環境

ユーザーのMFAは有効済？	PASSED
S3アクセスログは有効済？	PASSED
SQS キューは暗号化済？	FAILED
コンテナは非特権モード？	PASSED

アラートの集約・対応

Security Hub 検出結果

AWS Service 検出結果

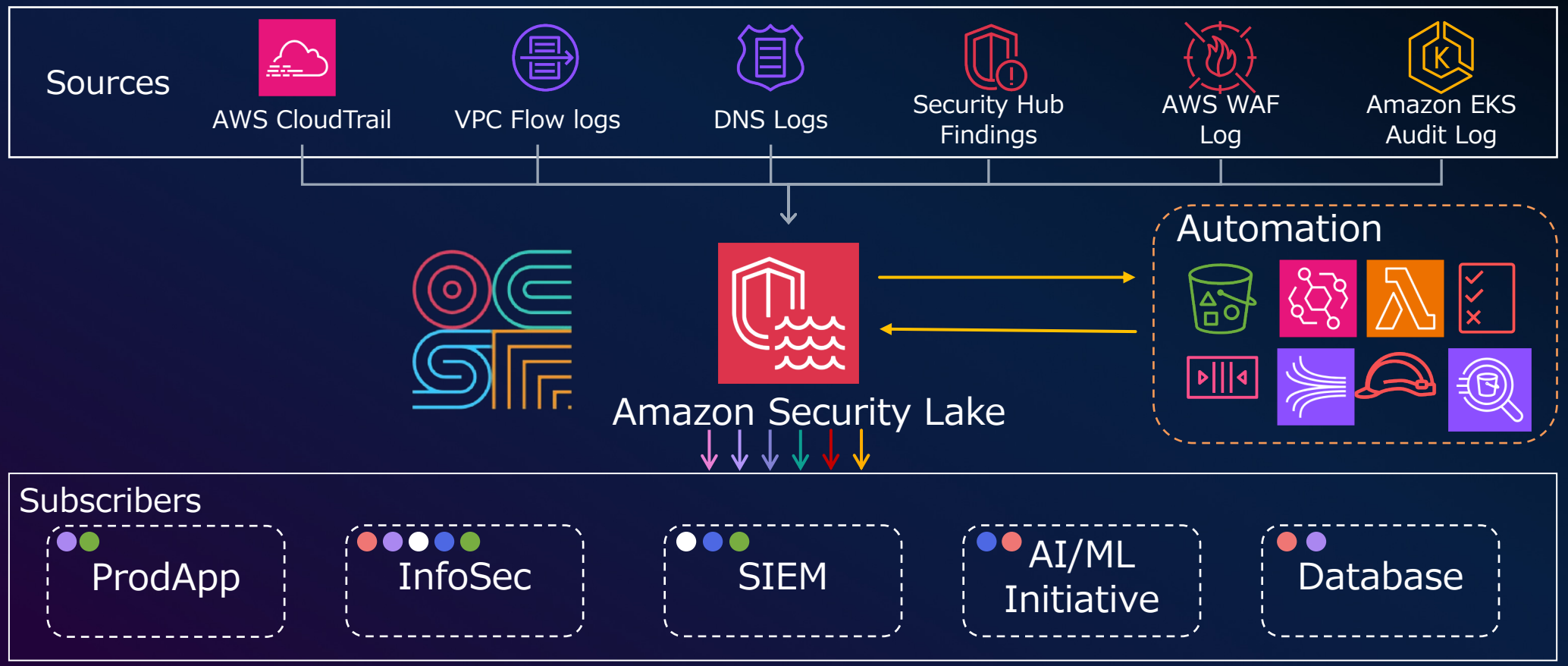
3rd party 検出結果

統合ダッシュボード
インサイト

対応自動化

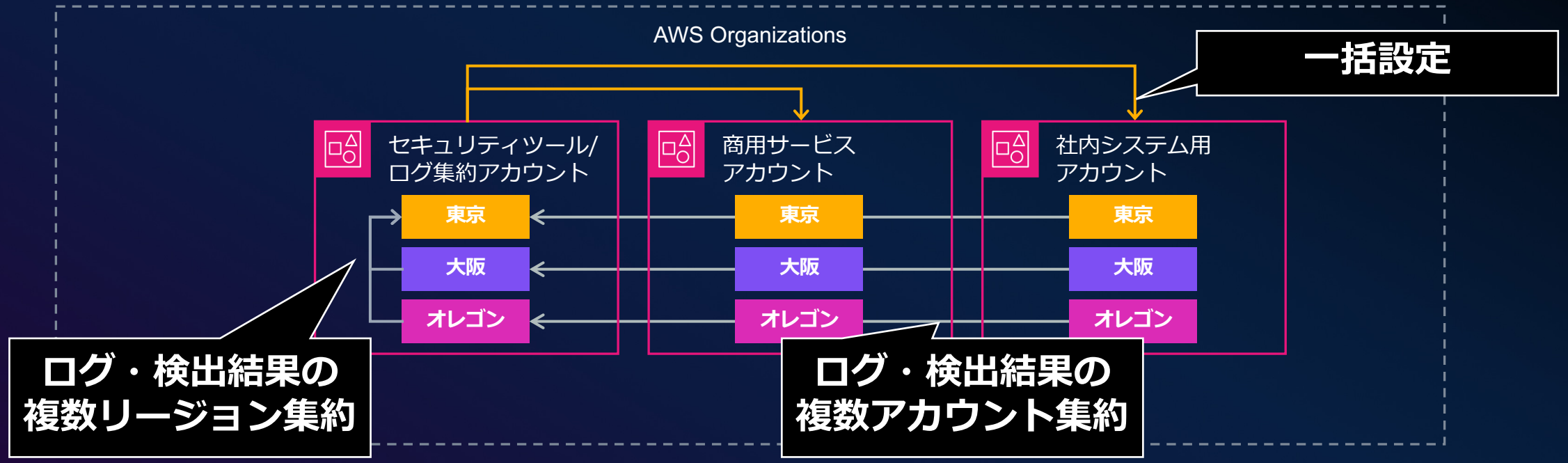
Amazon Security Lake

複数のワークロードにまたがるセキュリティログを自動的に収集し保存、
分析へと繋げる



大規模な環境でもスケールするアプローチを

AWS Organizations と連携し、複数の AWS アカウント・リージョンにまたがる
セキュリティサービス設定・ログを一元的に管理



※ セキュリティアカウントとログ集約アカウントは分離を推奨（参考）
※ Amazon GuardDuty は各リージョンごとにセットアップが必要
※ Amazon GuardDuty のリージョン集約は各リージョンの検出結果を AWS Security Hub に連携することで実現

Key Takeaways

AWS の脅威検知とインシデント対応サービスを活用し、
包括的な脅威やリスクを可視化することから始めてみませんか？

- Amazon GuardDuty で**サーバーレス・コンテナなどのワークロードを包括的に**モニタリング
- AWS Security Hub で多様なリソースのセキュリティポスチャを**継続チェック**
- Amazon Security Lake で**組織内に分散するセキュリティログ**を**自動的に収集**
- AWS Organizations との統合を活用し**マルチアカウント・マルチリージョンの管理**を効率化

Thank you!