パロアルトネットワークスが考える「クラウドセキュリティ」とは

PRISMA
BY PALO ALTO NETWORKS

クラウドセキュリティスペシャリスト
泉　篤彦

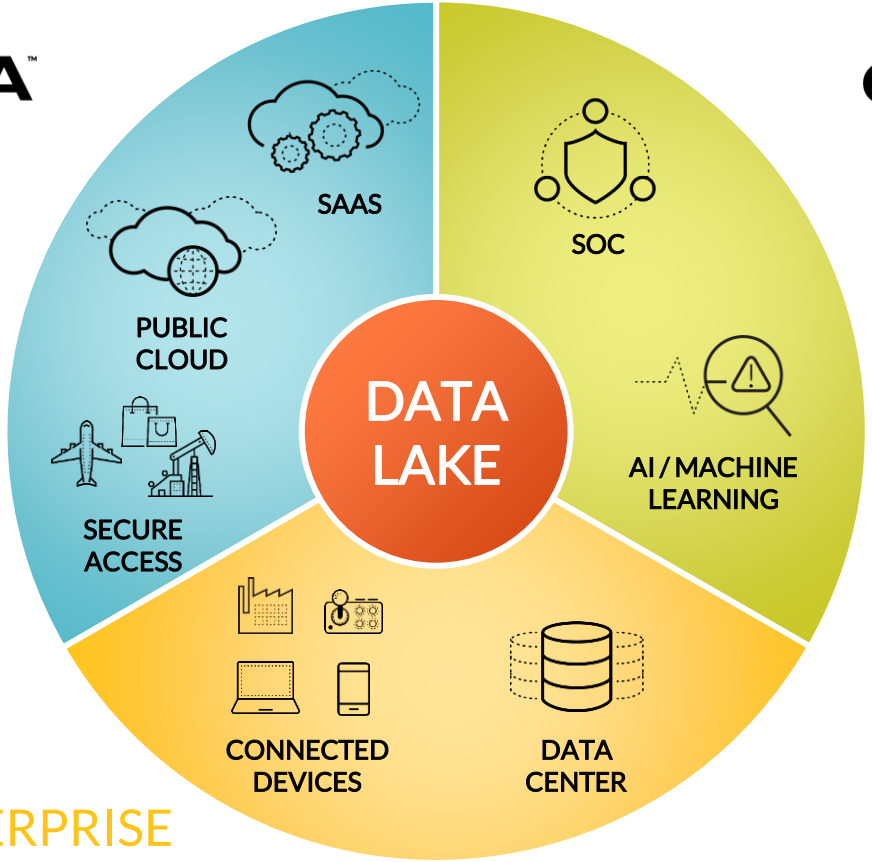
目まぐるしく進化するクラウド環境をより安全に

PRISMA™

CORTEX™

SECURE
THE CLOUD

SECURE
THE FUTURE



SECURE
THE ENTERPRISE

PRISMA™ BY PALO ALTO NETWORKS

RedLockからPrisma Public Cloudへ

PRISMA 製品名	現行 製品名
Prisma Access	GP cloud service GlobalProtect cloud service (GPCS)
Prisma SaaS	AP Aperture + GP cloud service GPCS
Prisma Public Cloud	RL RedLock
VM-Series	VM-Series VM-Series

PRISMA BY PALO ALTO NETWORKS

クラウドセキュリティのテーマと関連製品

テーマ	ユースケース	Prisma Access	Prisma Public Cloud	Prisma SaaS	その他の関連製品
モバイルセキュリティ	• モバイルセキュリティ(働き方改革) • BYODセキュリティ • リモートVPNやプロキシの撤廃	◉			PA-Series、VM-Series
拠点セキュリティ	• MPLSの負荷軽減/撤廃 • SD-WANソリューションとの併用 • 海外含む拠点のFW機器撤廃	◉			PA-Series、VM-Series
ゼロトラスト クラウドセキュリティ	• プロキシ/CASBの更改 • ゼロトラストイニシアチブ	◉	●	●	
クラウドガバナンス& コンプライアンス	• 環境横断でのアセット/設定管理 • GDPR等の各種規制対応		◉	◉	VM-Series
クラウドデータ保護	• クラウド上の情報漏洩防止		◉	◉	
クラウド脅威防御	• セグメンテーションと脅威防御 • クラウドのホスト/ネットワーク保護 • セキュリティ調査の迅速化		◉		VM-Series、Traps
DevOpsセキュリティ	• コンテナイメージの脆弱性スキャン • IaCセキュリティ • CI/CDパイプラインの継続的監視		◉		VM-Series Twistlock、PureSec

PRISMA BY PALO ALTO NETWORKS

パブリッククラウドでのセキュリティで考慮すべきポイントとは

クラウドの責任共有とは

パブリッククラウドのセキュリティに関しての質問で多い「オンプレミスとの違いは？」「クラウドベンダーが全て管理してくれるのでは？」

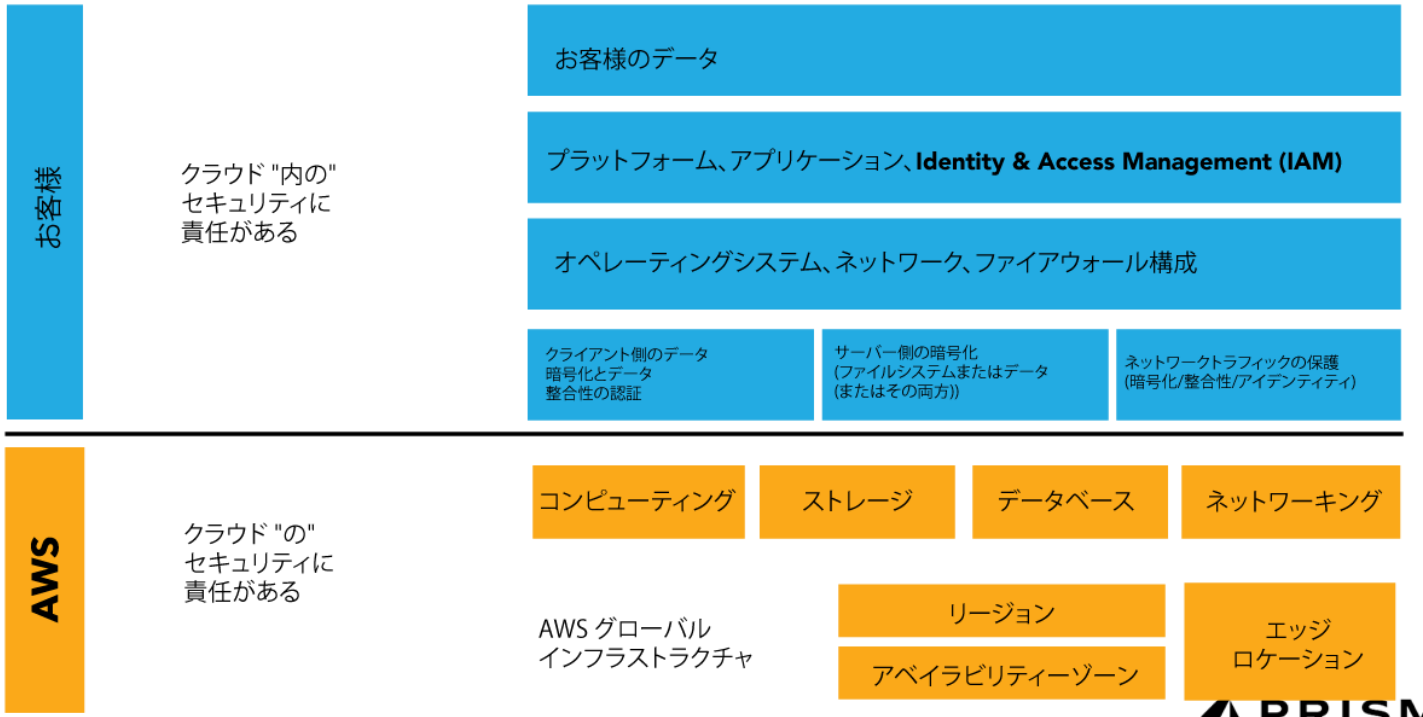
責任共有モデル

お客様自身でセキュリティを担保する必要があります

PRISMA BY PALO ALTO NETWORKS

アマゾン ウェブ サービス（AWS）の責任共有モデル

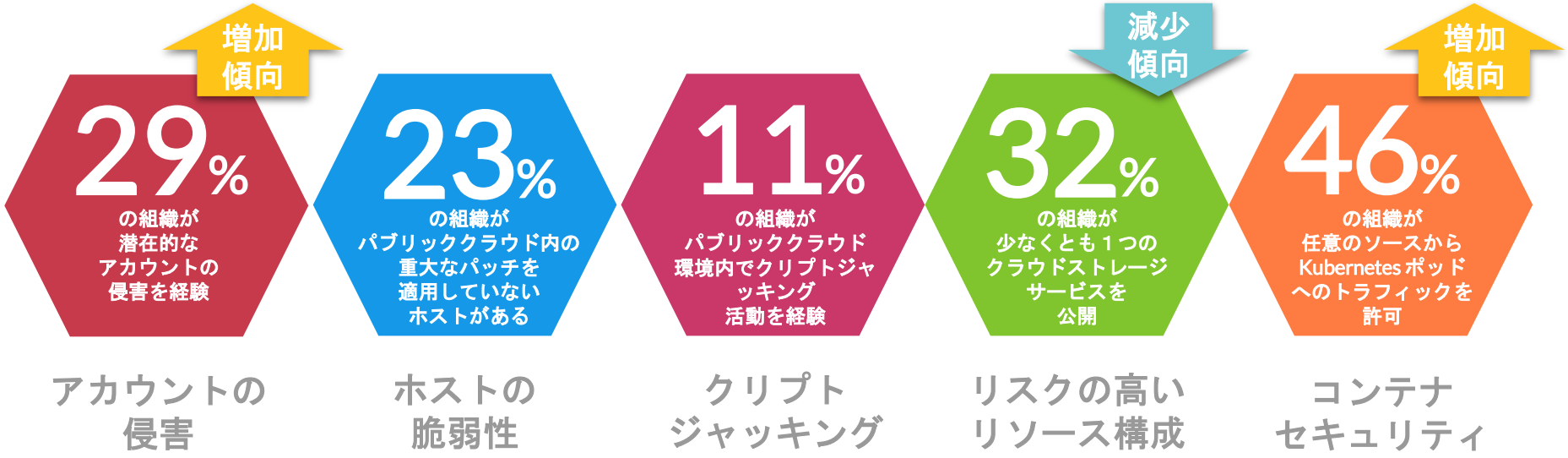
AWS は、AWS クラウドで提供されるすべてのサービスを実行する**インフラストラクチャの保護に責任を負います**。お客様は、ゲストオペレーティングシステムの管理 (更新やセキュリティパッチなど)、インスタンスにインストールしたアプリケーションソフトウェアまたはユーティリティの管理、AWS より各インスタンスに提供される**ファイアウォール (セキュリティグループと呼ばれる) の構成に責任を負います**。



PRISMA BY PALO ALTO NETWORKS

パブリッククラウド特有の脅威とは

クラウドインシデントの特徴



5つの主要なクラウドセキュリティの傾向:
組織がクラウドにおけるリスクを減らす上で役立つベストプラクティス
https://www.paloaltonetworks.jp/company/in-the-news/2018/unit-42-cloud-security-trends-tips

9 | © 2019 Palo Alto Networks, Inc. All Rights Reserved.

PRISMA
BY PALO ALTO NETWORKS

外部からの攻撃＋内部セキュリティの監視＝クラウド環境を全方位で防御

外部からの攻撃による漏洩

VPC

次世代仮想ファイアウォール
VM-Series

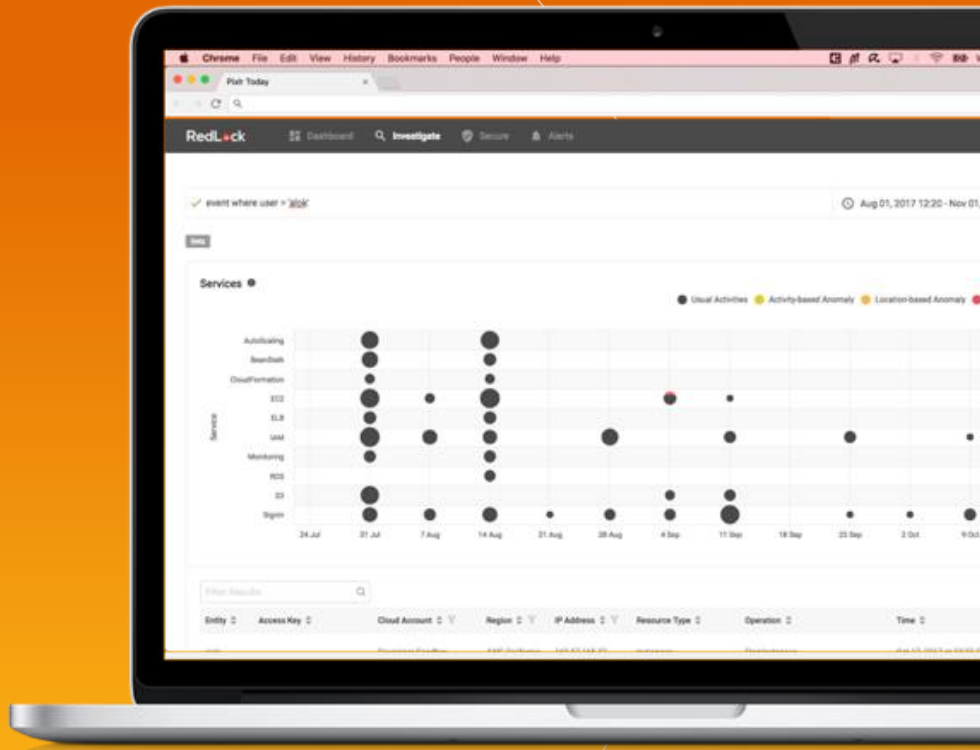
APIベースのセキュリティ
コンプライアンス
PPC

API

内部からのセキュリティ設定の甘さによる漏洩

PRISMA
BY PALO ALTO NETWORKS

Demo



paloalto NETWORKS

クラウド開発現場で発生している問題点とは

部門ごとにパブリック環境を契約していて、全社でどのくらい利用されているのかも把握していない

社内パブリッククラウドにガバナンスをPPCで実現

全社でどのくらい利用されているか把握していない

正しくセキュリティ設定がされているか管理したい

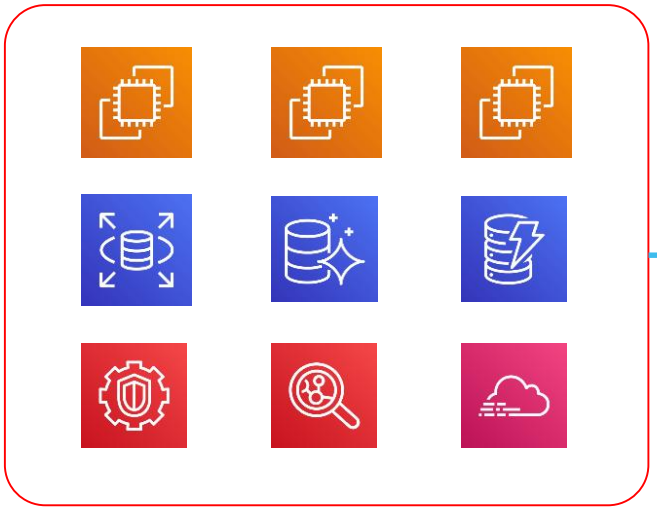
サービス事業部

各事業本部

海外拠点

業界的にコンプライアンスが厳しいので、うちの環境がどの程度基準を満たしているかを確認する方法がない

各種コンプライアンス標準から環境を診断



API

PCI DSS — 80%

GDPR — 35%

NIST SP800 — 60%

ISO27001 — 90%

SOC 2 — 28%

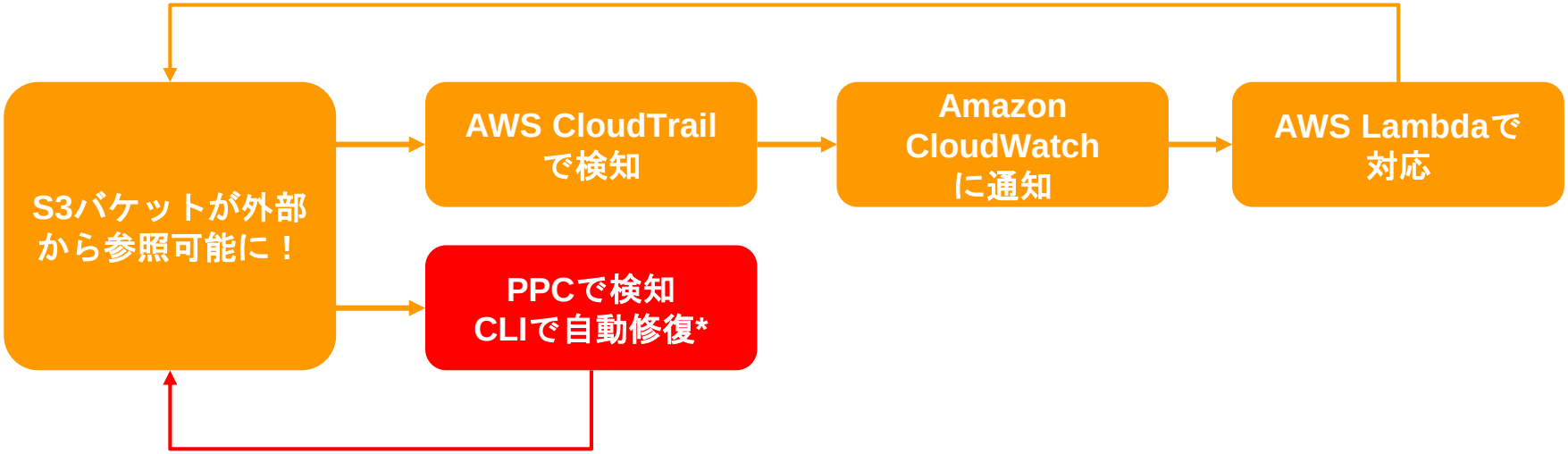
お客様のIaaS、PaaS環境を各種コンプライアンス標準に照らし合わせてチェックを行い、どの程度AWSセキュリティ設定が準拠しているかを客観的に診断します。

またその結果をレポートとしてPDF形式で任意のタイミングで出力することも可能です。

PRISMA
BY PALO ALTO NETWORKS

アラートが多すぎて、全てに対応することができない

検知から自動修復までをPPCのみで実現



AWS内のインシデントを発見から自動修復までをワンストップで定義可能。しかもAWS Lambdaなどのコードを書く必要もなく、誰でも自動修復までのバッチ処理をPPCのみで定義が可能。これによりアラートの数も大幅に削減でき、工数の削減が可能。

＊全ポリシーのうち一部のみが自動修復(オートレメディエーション)に対応
AWS

PRISMA BY PALO ALTO NETWORKS

AWSが提供するセキュリティ、ロギング
サービスだけで対応している
それでもPPCは必要？

複数のAWSネイティブセキュリティをワンストップで提供　さらに...

AWS

- VPCフローログ
- AWS Config
- Amazon CloudTrail
- Amazon GuardDuty
- Amazon Inspector

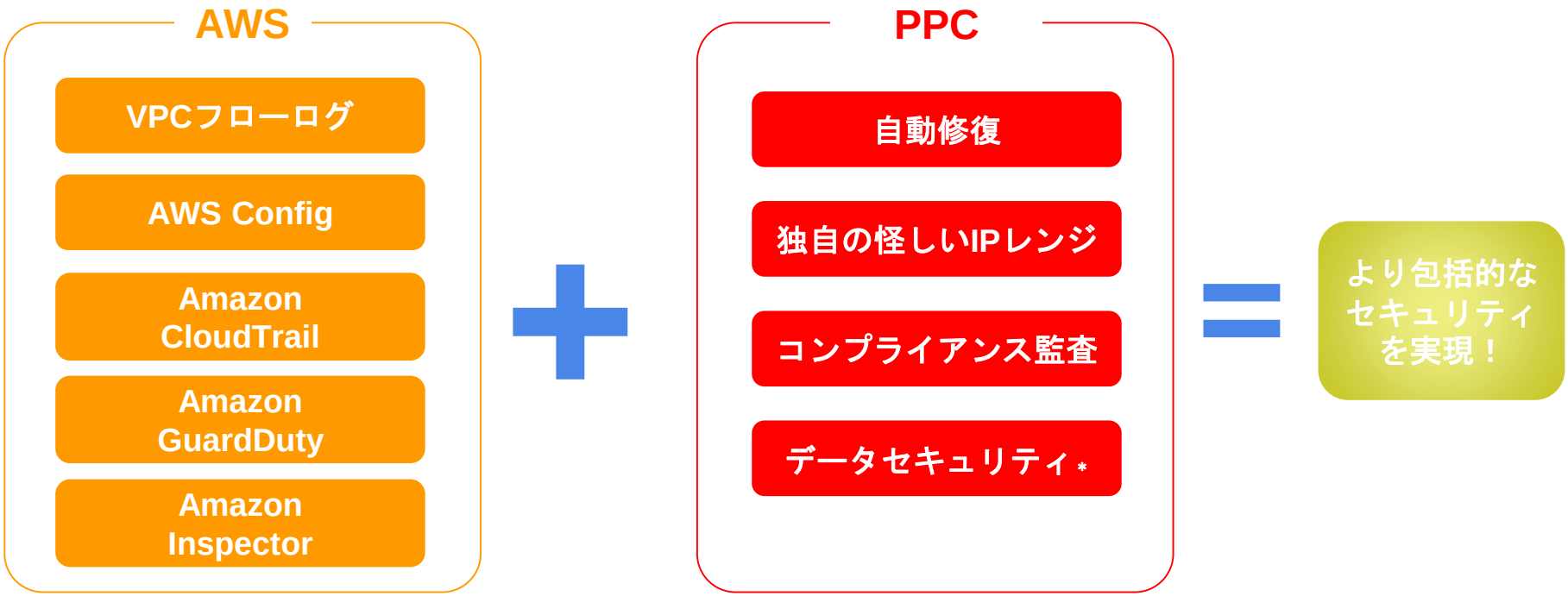
AWSが提供する豊富なネイティブセキュリティをすべて理解し、それらの情報を総合的に判断し正しい対応をするのは容易ではありません。

またその判定が担当者によって違う場合もあります。

PPCはそれらのネイティブセキュリティからの情報を統合的かつ機会的に判定し、アラートとして通知することが可能です。

PRISMA BY PALO ALTO NETWORKS

AWSネイティブセキュリティ＋PPC独自ポリシー



AWSネイティブセキュリティ統合だけでなく、さらにPPC(パロアルト)が独自の見地を追加することにより、より広範囲で包括的なセキュリティをご提供します。

＊提供予定

国内事例のご紹介

カブドットコム証券株式会社様事例

カブドットコム株式会社
システムリスク管理室長
石川　陽一様

PPC導入背景

これまで自社で運用してきた次世代のFintechプラットフォーム基盤をAWSに移行することを決定し、AWS上のセキュリティ標準選定を検討。PPCの持つ豊富なセキュリティ監査機能やコンプライアンス標準による金融監査基準にも対応可能と判断し採用を決定。
また、少ないメンバーで日々増え続けるログ監視も問題となっており、対応の自動化も必要となってきていた。

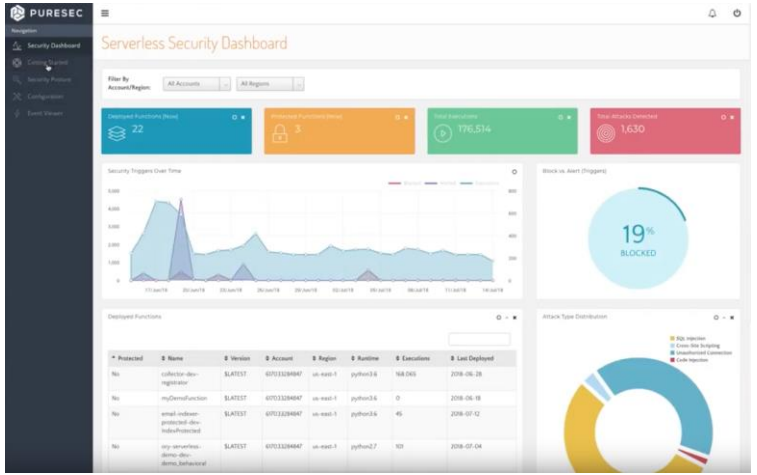
PPC導入後の姿

- FISCに準拠するための自社コンプライアンス標準もPPCの持つPCI DSSテンプレートを参考にしてカスタマイズ可能と判断。そのコンプライアンス標準を各AWSアカウント環境に適用することにより、人的な対応ではなく機械化による均一的な監査の実施を目指す。
- 自社で検討決定したAWSに対するセキュリティ標準をRedLock Query Language(RQL)に落とし込み、監査の自動化を実現する。
- 最終的にはPPCの持つ自動修復機能を活用してアラートへの対応も機械化、自動化する予定
- アーキテクト人材育成を一から自社で行うよりも、Prisma Public Cloudの持つポリシーを参考にすることによりパブリッククラウドセキュリティポイントの理解を効率的に達成する。

PRISMA
BY PALO ALTO NETWORKS

Prisma Public Cloudロードマップ

コンテナ/サーバーレスセキュリティの2企業の買収を発表



Twistlock

PURESEC

PRISMA
BY PALO ALTO NETWORKS

PPC
パートナープログラムのご紹介

Prisma Public Cloudによるソリューション提供パートナープログラム

既に展開しているクラウドソリューションにPPCを統合して以下のような メニューをお客様に提供可能なパートナー様を募集中

- パブリッククラウド診断サービス
- パブリッククラウド環境の継続的な監視、レポートの提供
- お客様ポリシーに合わせたコンプライアンス監査およびコンサルティングの提供
- SOCサービス提供、IRやフォレンジックの提供

PRISMA
BY PALO ALTO NETWORKS