# Cisco Secure Cloud Analytics

## プライベートネットワーク、パブリッククラウド、およびハイブリッド環境のセキュリティを確保します。

**シスコ年次サイバーセキュリティ レポート (2017 年) によると、セキュリティアラートのうち調査が行われているのは 56% のみで、その半数以上は修復されていません。これらのアラートに対応するのは大変な業務であり、ほとんどの組織にはこの業務を継続するためのセキュリティスタッフがいません。あらゆる規模の企業は、パブリッククラウド環境とオンプレミス インフラストラクチャの安全性を確保するという課題に直面しています。**

誤検出の数を減らすことができるソリューションを使用して、パブリッククラウドのワークロードに効果的なセキュリティ対策を追加することは非常に重要なタスクです。しかし、パブリック クラウド インフラストラクチャはオンプレミス インフラストラクチャとは異なります。パブリッククラウドは、資産の変化率が非常に高いにもかかわらず、ネットワーク監視機能が低くなっています。誤検出の数を減らしながら効果的なセキュリティを提供するには、新しいアプローチが必要です。

従業員のクラウドクレデンシャルがフィッシングなどの方法で侵害されたとします。その従業員が別の国からログインを開始したかどうかを確認できますか。Cisco Secure Cloud Analytics (旧称 Stealthwatch Cloud) は、こうした種類の悪意のあるアクティビティをリアルタイムで特定するために必要な、実用的なセキュリティ インテリジェンスと可視性を提供します。セキュリティインシデントが壊滅的な侵害になる前に迅速に対応できます。

## メリット

- プライベートネットワークからパブリッククラウドまで、環境を可視化して実用的なインテリジェンスを獲得
- 高度な脅威とセキュリティ侵害の兆候を迅速に検出
- 運用オーバーヘッドを削減しながら、ビジネスに合わせてセキュリティを強化
- 基礎となる監視によってサポートされる信頼度の高いアラートにより、誤検出を大幅に削減
- パブリッククラウドを含め、企業全体で強力なセキュリティ態勢を実現

**Secure Cloud Analytics では、**プライベートネットワークからブランチオフィス、パブリッククラウドまで、**環境全体の外部および内部の脅威を検出できます。**Secure Cloud Analytics は、クラウドから提供される Software-as-a-Service (SaaS) ソリューションです。簡単に試して、購入でき、シンプルな運用とメンテナンスが可能です。データを受信する場合、追加の設定やデバイスの分類はほとんど必要ありません。すべての分析が自動化されています。

## エンティティモデリングによる環境の保護

脅威は絶えず進化しています。将来の攻撃を検出するには、攻撃に先んじるセキュリティが必要です。Secure Cloud Analytics では、ネットワーク上での動作に基づいて脅威を検出する、動作モデリングアプローチを使用します。たとえば、ドメインコントローラがファイル転送プロトコル (FTP) を使用してデータの転送を開始した場合、これがセキュリティ侵害の最初の兆候である可能性があります。Secure Cloud Analytics はこの動作をリアルタイムで検出し、アラートを表示します。

Secure Cloud Analytics では、動的学習を使用して、各デバイスとネットワークエンティティのモデル（シミュレーションの一種）を作成します。このモデルでは次のことが可能です。

- エンティティの動作に基づいてエンティティのロールを動的に決定し、そのロールと一致しないアクティビティを検出する
- データ伝送とアクセス特性の両方で、動作の異常と突然の変化を特定する
- エンティティが同様のデバイスとは異なる動作をする場合に検出する
- エンティティが組織のポリシー（プロトコルとポートの使用、デバイスとリソースのプロファイル特性、およびブラックリストに登録された通信など）に違反している場合を特定する
- 過去のアクティビティに基づいてホストまたはデバイスの動作を予測し、それらの予測に対して観察された動作を評価する

**これらの機能によって、Secure Cloud Analytics は、スタッフがログデータを手動で分析して原因を特定するのではなく、問題の修復により多くの時間を費やすことを可能にします。**

「組織のネットワークセキュリティを監視するより良い方法を探していました。このサービスにより、すべてのデバイスの可視性が大幅に向上します」。

米国行政府職員連合、
理事、Taylor Higley 氏

## パブリッククラウドでの脅威の検出

パブリッククラウドに移行する IT リソースの増加に伴い、クラウド資産を標的とする攻撃者を検出するための可視性が必要になります。さらに、使いやすく運用効率の高いソリューションも必要です。Secure Cloud Analytics のパブリック クラウド モニタリングは、Amazon Web Services（AWS）および Microsoft Azure 環境でワークロードの安全性を維持するために必要な可視性と脅威検出機能を提供します。

Amazon Virtual Private Cloud（VPC）フローログなど、AWS ネイティブのテレメトリのすべてのソースを使用して、ソフトウェアエージェントを使わずにクラウド内のすべてのアクティビティを監視します。Secure Cloud Analytics は、サービスの可用性を損なうことなく、数分でこれらの環境に導入できます。

Secure Cloud Analytics では、このデータを使用して、各クラウドリソースの動作をモデル化します。これをエンティティモデリングと呼びます。突然の動作の変化、悪意のあるアクティビティ、侵害の兆候を検出できます。

## プライベートネットワークも保護

Secure Cloud Analytics は、クラウド環境の保護に加えて、Cisco Secure Network Analytics SaaS（旧称 Stealthwatch Cloud Private Network Monitoring）を使用して、プライベートネットワークに拡張することもできます。これにより、単一のダッシュボードを使用して、ハイブリッド環境の可視性と脅威検出を実現できます。プライベートネットワークに接続されるデバイスの数は劇的に増加しています。セキュリティ担当者は、組織に脅威をもたらすかどうかは言うまでもなく、自社の環境内でどのようなエンティティが動作しているかを知るだけでも苦労しています。Secure Cloud Analytics では、攻撃がネットワーク、クラウド、またはその両方の環境で発生しているかどうかにかかわらず、リアルタイムで脅威を正確に検出できます。

## 環境を今すぐ保護

**リスクなしの無料トライアルで、今すぐ Secure Cloud Analytics をお試しください。**
**詳細については、https://www.cisco.com/go/secure-cloud-analytics を参照するか、最寄りのシスコアカウント担当者にお問い合わせください。**



CXX-XXXXXX-00 04/21