Secure Cloud Analytics でクラウドのセキュリティポスチャを管理 (旧 Stealthwatch Cloud)

クラウドでの成長に伴い企業が直面する主な課題

クラウドへの移行は複雑です。俊敏性を維持するために、企業は大挙してパブリッククラウドへの移行を進めてきました。パブリッククラウドでは、コンテナ化されたサーバレスなマネージド環境にワークロードを移行することで、より迅速で柔軟な導入が可能となるほか、効率が向上し、拡張性に優れた方法で業務を拡大できます。『Cisco Annual Internet Report』によると、2021 年には約 95% のワークロードがクラウドデータセンターで処理されると予想されています。組織とクラウドが成長を続ける中、コンプライアンスに関する懸念が増し、攻撃対象領域も拡大しています。**サイバーセキュリティ専門家の 94% が、 パブリッククラウドのセキュリティに関してある程度懸念を抱いていると回答しています** [1]。

クラウドの拡大に伴い、企業の**コンプライアンスの徹底と脅威リスク**に対する懸念は一段と高まっています。そのため、クラウドのセキュリティポスチャを適切に維持することが極めて重要です。過去 5 年間に一部の大手企業は、不適切なクラウド管理とリソース設定に起因する攻撃の犠牲になっています。機密性の高いワークロードとデータがクラウドに蓄積されるため、機密情報をモニタリング・保護するための適切なツールを用意することが非常に重要です。

IT 部門のタスクのほとんどはチーム間で分担されていますが、うまく連携が取れているとは言えません。脅威の検出や、ネットワーク攻撃と悪意のある動作のモニタリングは**セキュリティチーム**が、クラウドでのアプリケーションの迅速な構築と導入については**開発チーム**が担当しています。各チームがパブリッククラウドのさまざまな課題に別々に取り組んでおり、十分に連携が取れていないことも多々あります。組織が成熟してくると、セキュリティチームと開発チーム間の緊密な連携を実現するための戦略を追い求めるようになります。

68% の組織が、クラウドプラットフォームの設定不備がクラウド環境における最大の脅威であると考えています [1]。

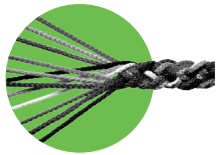
1. 2020 年クラウド セキュリティ レポート、サイバーセキュリティ インサイダー

パブリッククラウドリソースのモニタリングと保護

セキュリティチームは、Cisco Secure Cloud Analytics を使用することで、クラウドのワークロードを確実にモニタリング・保護することができます。また、クラウドネイティブな API ベースのソリューションを開発チームが想定した通りに使用することで、クラウド環境におけるセキュリティポスチャを迅速に評価できます。両チームは 1 つの直感的なソリューションを使用して、クラウドのワークロードに関する情報を共有し、攻撃される前にコンプライアンスや設定の問題を解決することができます。

利点

クラウド内の設定不備を悪用している可能性のある**高度な脅威を迅速に検出**



ライブイベントの表示によりクラウドのセキュリティポスチャを**強化 ・ 維持**

クラウドリソース内で発生しているアクティビティを**総合的に可視化**

セキュリティチームと開発チーム間のシームレスなコミュニケーションにより、セキュリティポリシーと設定を**迅速に修正**

Secure Cloud Analytics に、ユーザがクラウドポスチャを簡単に管理できる、柔軟性の高いイベントビューアが追加されました。その仕組みをご覧ください。

セキュリティチームと開発チーム間の連携強化

Secure Cloud Analytics により、クラウドポスチャ管理に最も関与している 2 チーム、つまりセキュリティチームと開発チーム間の連携が容易になります。セキュリティチームは、ネットワークのアラートのモニタリング、セキュリティホールの特定、アラームへの対処、クラウド環境内で検出された脅威への対応を担当します。一方開発チームは、これらの環境を実際に設定し、クラウドにおける強固な構造を構築・維持する役割を担っています。Secure Cloud Analytics には、自動検出機能、過去のイベントのドリルダウン機能があり、チーム間の連携が強化されます。また、さまざまなフィルタ機能を活用することで、セキュリティチームはクラウドの設定不備を簡単に特定できます。さらに、ウェブフックやサードパーティのプラットフォーム、シスコのその他のテクノロジーが統合されているため、セキュリティチームは調査結果を開発チームに簡単に伝達することができます。調査結果を受け取った開発チームは、クラウド インフラストラクチャの問題を解決し、すべてのリソースを適切に設定してセキュリティを確保します。自動修復オプション、ウェブフック、その他の統合など、さまざまな利点を活かすことで、両チームはクラウドセキュリティのポスチャの問題に迅速に対応できます。

業界標準や社内ルールに対応するためにコンプライアンスを徹底

Secure Cloud Analytics に、クラウドセキュリティのポスチャをモニタリングするイベントビューアが追加されました。このイベントビューアを使用して、アカウントや個々のリソースが業界のベストプラクティスやカスタムポリシーに準拠しているかどうかを調査できます。クエリモードに切り替えれば、さらに詳細な検索を実行することも可能です。組織が多数のアカウントを保有し、利用しているクラウド サービス プロバイダーの数が多い場合、可視性と一貫性を実現することは困難です。イベントビューアを活用することにより、セキュリティチームはすべてのクラウドアカウントに即座にアクセスし、リソースやルール、時間枠を指定してクエリを実行し、設定不備やその他のコンプライアンスの問題を絞り込むことができます。

パブリッククラウドのリソースのシームレスなモニタリングと保護

Secure Cloud Analytics は、基本設定やコンプライアンスルールだけでなく、悪意のあるアクティビティや脅威となり得る異常な動作を特定する、高精度の自動アラートを備えています。また、ダイナミック エンティティ モデリングと呼ばれるプロセスを使用しており、エンティティの動作に基づいてそのロールを決定し、動作の基準から逸脱したアクティビティに対してアラートを発します。「見えないものを守ることはできない」という言葉の通り、シスコは可視性が極めて重要であると考えています。エージェントレス型の Secure Cloud Analytics はマルチクラウド環境をサポートしており、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform など、主要なクラウドプラットフォームのモニタリングが可能です。EC2 インスタンス、AWS ロードバランサ、S3 バケット、NAT ゲートウェイなどのロールをすべて自動配置し、VPC や NSG フローログなどのクラウドネイティブなテレメトリを使用して、悪意のある可能性または有害である可能性のあるアクティビティを検出します。新しいアラートタブでは MITRE ATT&CK フレームワークへのマッピングが行われ、各アラートにコンテキスト情報が追加されます。たとえば、脅威の種類、攻撃者が使用している可能性のある手法、修復に最適なアクションに関する情報などです。また、「地理的に異常な API の使用」や「AWS Lambda 呼び出しの急増」といったクラウドの動作に特有な検出もあり、クラウド内の悪意のあるアクティビティにアラートを発するために特別に構築されています。Cisco SecureX プラットフォームが組み込まれているため、Umbrella や Talos などの他のアプリケーションに簡単に切り替えて詳細な調査を行ったり、常に脅威をブロックすることができます。

クラウドのポスチャの維持は、ビジネスにとって極めて重要です。Secure Cloud Analytics により、コンプライアンスを徹底して脅威から守り、クラウドセキュリティのポスチャの可視性と制御を強化することができます。

詳細はこちら

60 日間の無料トライアルに登録

2230031 | 05/21