Orca Securityは、セキュリティ、DevOps、コンプライアンスのための1つのツールを提供します。

「開発者に『セキュリティについて考えたことがありませんでしたか？』などのようなことを尋ねることはできません。AWSで新しいVMを開始する際、教えていただけますか、そうするとスキャンできますと尋ねることはできます。そのマシンにエージェントをデプロイしてもらえますか？より良い機能が必要です。Orcaは組織の摩擦を排除することにより、その良い方法を提供します。」

Erwin Geirnaert
クラウド セキュリティ アーキテクト
NGDATA

クラウドセキュリティの課題

- 頻繁にエージェントを使用せずに、頻繁に変化するエージェントにはAWSアセットのグローバルなリアルタイムビューが必要
- 顧客アセットと企業の知的財産が保護されていることを確認
- デベロッパーの作業方法と統合するツールが必要

クラウドセキュリティの結果

- すべてのNGDATAアセットをリアルタイムで完全に把握
- Jiraと統合し、脆弱性改善プロセスを自動化
- デベロッパーとの組織的摩擦を取り除き、DevSecOpsアプローチに移行

データインサイトを通じ、企業が個人的な顧客体験を提供するのを助けるNGDATA

NGDATAは金融サービス、通信、ユーティリティ、ホスピタリティなどのデータ主導型産業のブランドが、つながった顧客体験を提供するのを支援します。AI駆動CDPとデジタルトランスフォーメーションサービスは、Customer DNAを通じて人々をあらゆるビジネスの中心に置き、動作から継続的に学び、世界中のブランドに魅力的な体験を提供します。NGDATAはベルギーのゲントに本社を置き、米国、ヨーロッパ、アジア太平洋にもオフィスを持ちます。

ソフトウェアプラットフォームはオンプレミスにインストールしたり、プライベートクラウドにデプロイすることができますが、すべての製品開発作業はクラウドで行います。NGDATAはShift Left Securityのクラウドセキュリティアーキテクト Erwin Geirnaert氏と契約し、クラウド環境に秩序を提供し、脆弱性を特定して排除し、良いセキュリティポスチャを維持する手順を実行しています。

Orca Securityは従来型のセキュリティスキャンには不可能だったことを成し遂げた

Geirnaert氏の最初の事業は、可能な限り迅速に現在の環境の状態を特定する従来型の浸透テストでした。このスキャンは、常に変化するクラウドエステートの一時的なスナップショットに過ぎないため、ほんの少ししか役に立ちませんでした。しかし、認証スキャナーでさえ、何をスキャンすればいいのかわからなければ、ギャップが生じます。「クラウドネイティブのアプローチでは機能しません」とGeirnaert氏は述べています。

そして、Sumo Logicのダッシュボードに取り込んだAmazonのログから、スキャンするIP範囲の情報を得ようとしました。その結果、困ったことが起きました。

「クラウドインフラの脆弱性を見つけるには、従来の浸透テストは意味がありません。Orcaによる最初のスキャンは、本当に目を見張りました。存在を知らなかったマシンや、機密情報やインターネットに接続されているサービスが入ったマシンが見つかりました。」

Erwin Geirnaert
クラウド セキュリティ アーキテクト
NGDATA

Geirnaert氏は、OrcaがDevSecOpsの動力を有効にする方法を説明しています。「開発者はAWSコンソールにアクセスする権利があるため、読み取り専用ポリシーを使用してOrcaを添付することができます。デプロイ、適用、インストールする必要はありません。AWSを設定し、Orcaプラットフォームに信頼してスキャンするだけです。読み取り専用ポリシーを添付して実行するのに約5分かかります。そして、Orcaの細かいスキャンから結果がすぐに得られることがわかります。」

「コンプライアンスビューで、開発者は『セキュリティ姿勢に影響を与えるようなAmazonのセキュリティ設定を見落としてないか』と問うことができます。これを設定し、有効にし、使用し、実行する必要があることがすぐにわかります。Orcaはコンプライアンスも更新しています。脆弱性が見つからなくても、それだけで多くの情報が得られるので、セキュリティ会社に指示を仰ぐ必要はないのです。Orcaは、当社がすべきこと、またその方法について教えてくれます」とGeirnaert氏は述べています。

> Orcaを使用すると、さまざまなユーザーにさまざまな役割へのアクセスを許可できます。CISOはコンプライアンスに興味を持っています。セキュリティエンジニアは、脆弱性とアラートを検討します。開発者は、ダッシュボードから問題である理由を理解できます。
>
> **Erwin Geirnaert**
> クラウド セキュリティ アーキテクト
> NGDATA

AWS APIに接続し、NGDATAのすべてのアセットをリアルタイムで確認できるツールを探し出すことができます。このようなツールは、重大な脆弱性と、PIIや知的財産がリスクにさらされているかどうかが明らかにする必要があります。このクエストにおいて、GeirnaertはOrca Securityを発見しました。

「Orcaによる最初のスキャンは、本当に目を見張りました。存在を知らなかったマシンや、機密情報やインターネットに接続されているサービスが入ったマシンが見つかりました。」と彼は述べています。Orcaは、すべてのIPアドレスと仮想マシンの毎日スキャンを設定しています。たとえインターネットに接続されていない場合でも、すべてのIPアドレスを毎日スキャンしています。「お客様の資産、そしてNGDATA自身の知的財産を確実に保護するために、当社は自社が持っているものを完全に理解する必要があります。」

DevOpsの変革的なツールであるOrca

NGDATAの開発者は、世界中に広がっています。Geirnaert氏は、「彼らに「セキュリティについて考えたことがありますか？」と尋ねることはできません。AWSで新しいVMを開始する際、スキャンができるよう教えていただけますか、と尋ねることはできます。そのマシンにエージェントをデプロイしてもらえますか？」より良い機能が必要です。Orcaは、組織の摩擦をすべて取り除くことで、その良い方法を提供します。

「DevOpsアプローチ、そしてクラウドネイティブやサーバーレス化が、開発者をセキュリティのチャンピオンに育成することなくセキュリティを向上させると強く信じています。すでに機能する方法と統合するツールで、有効にする必要があります。」

規制とセキュリティのフレームワークへのコンプライアンスを促進します

Geirnaert氏がNGDATAに入社した当初、インターネットセキュリティセンターのAWS向けコンプライアンスフレームワークに基づき、ベストプラクティスのリストを作成しました。プロジェクト管理ツールのような100アイテムリストを使用してタスクを割り当てます。リストが必要ではなくなりました。

「Orcaを起動すると、コンプライアンス要件を動的に確認します。以前はSumo Logicを使いチェックを実施していました。AWS CloudTrailのログインからのイベントを見る時には、ダッシュボードにキャプチャして表示していました。今ではOrcaのダッシュボードで自動的にすぐにすべてが確認できます。」

GDPRコンプライアンスは、サーバーとファイルでOrcaがPIIを探しているため、簡単にできます。Orcaは隠されたPIIや、PIIがあるような場所を見つけるのに役立ちます。セキュリティ担当者として、Geirnaert氏は本番環境にアクセスできないため、Orcaは通常では得られないレベルの視認性を提供します。PIIに関しては、問題のパッチや緩和に役立ちます。

Orcaは監査プロセスも簡素化します。「PIIが保存されている場所を簡単に検索することができます。すべてのドキュメントが得られるため、監査が簡単に求める証拠を見せることができます。」とGeirnaert氏は述べています。

Orca Securityについて

Orca Securityは、特許出願中のSideScanning™テクノロジーを活用し、AWS、Azure、GCP向けにクラウド全体のワークロードのディープなセキュリティとコンプライアンスを提供します。クラウドプロバイダへ読み取り専用及び影響のない統合を瞬時に行った後、Orca Securityは脆弱性、マルウェア、設定の誤り、横方向の動きのリスク、認証のリスク、安全ではない高リスクデータを検出し、エージェントをデプロイせずに根本的な問題、アクセス可能性、ブラスト半径に基づいてリスクを優先させます。

orca security

最初のクラウドアカウントに数分で接続し、
ご自身の目でお確かめください：orca.securityを見る

© Copyright Orca Security 2021この資料で参照されているすべての商標、サービスマーク、商号はそれぞれの所有者に帰属します。