

Fiverrは複数のツールをOrca Securityに置き換え、AWSアセットの即時かつ完全な視認性を確保しています。



「数分以内にAWSアカウントを完全に可視化しました。Orcaの実装前は視認性ゼロでした。今では必要なものすべてを見ることができます。さらに、1つのツールであらゆることができるようになりました」



Shahar Maor
情報セキュリティ最高責任者 (CISO)
Fiverr

クラウドセキュリティの課題

- ✗ AWS全体で発生していた状況について、完全なコンテキストを理解する方法がない
- ✗ AWSとオープンソースツールでは時間がかかり、効果がない
- ✗ 誰も確認する時間がない数千のアラートの洪水

クラウドセキュリティの結果

- ✓ ディープクラウド・インスペクション (DCI) は、マルウェア、設定ミス、「秘密」、弱いパスワード、PIIを特定
- ✓ 1週間あたりの作業時間とDevOpsへの依存度を減らし、アセットを見落とさない
- ✓ アラートの優先順位は環境コンテキストに基づいて決まり、それをSlackにプッシュして解決

急速なグローバル展開で大規模なAWSクラウドセキュリティが必要に

2010年に設立され、テルアビブに本社を置く Fiverr (NYSE:FVRR) は、フリーランスによるサービス向けの巨大なオンライン・グローバルマーケットプレイスです。そのプラットフォームでは、フリーランスの人々が世界中の顧客にサービスを提供する一方で、企業側はカタログを閲覧したり検索を行ったりするだけで必要なサービスを見つけることができます。

Fiverrのプラットフォームは550万社以上の企業に提供されており、5,000万件以上の取引をサポートしました。多くの人々がプラットフォームにアクセスする場合、安全なAWSインフラを維持することが不可欠です。

FiverrのCISOであるShahar Maor氏は、クラウド環境の保護が複雑な作業であることを知っていました

Shahar Maor氏は次のように述べています。「私はFiverrが雇った初めてのフルタイムのセキュリティ専門家でした。しかし、セキュリティの保護はFiverrの企業文化にすでに深く浸透していました」

Maor氏による最初のAWSインフラ分析では、外部のベクター、ハッカー、悪意のあるボット、ウイルスから攻撃される可能性が指摘されました。しかし、Maor氏はクラウド環境には見た目以上のものがあることを知っていました。

「組織では多くの場合、周辺環境を保護すればそれで十分であるとみなされ、クラウドインフラは見落とされがちです。プラットフォーム自体の設定ミスが問題になる可能性があります。もっと明確なクラウドネイティブのインフラがあれば、それは誤解であることが分かります。クラウド環境の保護には多くの複雑性が伴うのです」

Maor氏は、弱いパスワードを設定しているプラットフォームユーザーの脆弱性、またAWSサーバーでマルウェアが実行される可能性について懸念していました。「高価値の資産に対して最初にリスクマッピングを行ったとき、盲点が存在することは明らかでした。さらに、手作業で多くの時間を監視に費やして資産（特にAWS S3バケット）が流出していないことを確認していました。それは非常に面倒でした」

深い視認性が必要なすべてのAWSアセットに理想的なソリューション

Maor氏は具体的な要件を念頭に置いて、AWSのクラウドセキュリティソリューションを見つけることにしました。「AWS環境を完全に可視化すると同時に、マルウェアのスキャン、設定ミスの特特定、PIIの保護をしてくれるソリューションを必要としていました」

「組織では多くの場合、周辺環境を保護すればそれで十分であるとみなされ、クラウドインフラは見落とされがちです」

Shahar Maor
情報セキュリティ最高責任者
Fiverr

最適なクラウドセキュリティツールは特定のリスクに対する包括的なソリューションであり、IT、DevOps、エンジニアリングの全体に実用的なインサイトと価値を提供します。AWSのセキュリティソリューションに必要な追加の目標と要件が含まれます。

- 管理するエージェントがありません。
- 管理するエージェントが無い
- 完全な視認性。アセットの見落としが発生しない
- PIIを検索し保護
- サーバーのヘルスチェックを実施
- 脆弱なパスワードを特定
- 設定ミスを検索
- 既存コードに残る「秘密」を探す
- S3バケットなど露出アセットの監視
- PCIを中心とした規制遵守の簡略化

「AWS環境を完全に可視化すると同時に、マルウェアのスキャン、設定ミスの特定、PIIの保護を可能にするソリューションが必要でした」

Shahar Maor
情報セキュリティ最高責任者
Fiverr

ネイティブツーリング、レガシースキャナー、エージェントベースのアプローチはカットしていません

Maor氏は、Fiverrのクラウド環境には多くの利用可能なクラウドセキュリティツールでは満たせない独自の要件が存在することを理解していました。「Amazon InspectorやGuardDutyなどのネイティブツールは基本的な機能を提供しますが、ロジックをインシデントと関連付けたり、発生している状況を完全に理解する訳ではありません。ログを分析し、データの意味を理解するために時間を費やす必要があります。オープンソースツールと同じように、何もしないよりはマシですが、チームのアクションにつながる結果を届けるワークフローがありません」

Maor氏はスキャナーとエージェントベースのツールが非常に限定されていることを付け加えています。「一部の商用ツールは脆弱性対策のためにサーバーをスキャンしますが、それだけです。要するに、これらのツールはより多くの作業を生み出しますが、効果的に機能するためにはドメインの専門知識と追加のツールが必要です」

1つのツールですべてを実行

Maor氏は、Orca SecurityをFiverrのAWSインフラ内に潜むリスクを減らすワンストップショップとみなしています。「OrcaはFiverrのデータセンターにおけるリスクを緩和する全体的なソリューションを提供します。AWSをスキャンするOrca独自の方法が当社にとって最も適していることが判明し、DevOpsチームにもまぎりました。さらに、1つのツールであらゆることができるようになりました」

Orca SideScanning™はエージェントの必要性を排除しパフォーマンスへの影響もありません

個々の仮想マシンでセキュリティエージェントを実行する場合、継続的な管理が必要です。Orcaはそのアプローチの代わりにSaaSサービスとして、顧客のAWS、Azure、GCPワークロードのランタイムブロックストレージへの読み取り専用アクセスにより実行されます。スナップショットからビットとバイトを再構成し、オペレーティングシステム、アプリケーション、データに対するバーチャルな読み取り専用ビューを構築します。その後、脆弱性とリスクをスキャンします。

Maor氏は次のように述べています。「Orcaは非常に軽量であり、ネットワークへの影響は一切ありません。インスタンス自体に干渉することなく視認性が得られます。Orcaはシンプルにコピーを作成し、それを読み、分析し、その後で確認のためにダッシュボードに提示します」

ノイズがなく一目で分かる高価値アラート

Orca Securityの特許取得済みSideScanning™テクノロジーは、お客様の環境でのすべてのアセットを自動的に検出します。これにより、セキュリティチームは危険なリソース、脆弱性、マルウェア、設定ミスを即時に可視化します。Orcaはこうした情報と環境メタデータを組み合わせることにより、効果的な優先順位付けを可能にするコンテキストの範囲内でアラートを送信します。

「Orcaは、誰も読まない、または確認する時間がない膨大なログと数千のアラートを作成する代わりに、脅威に対する注意を喚起するための一目で分かる実用的なアラートをリアルタイムで送信します。すべての重要な結果についてSlackアラートを受け取ります。Orcaが新しい脆弱性を発見した場合、すぐに知ることができます」

規制コンプライアンスを簡素化

さらに、Orca Securityは規制コンプライアンスを簡素化します。「PCIでは当社の環境をスキャンする必要があります。またサーバーレスであるため、独自の課題が提示されます。OrcaのソリューションではEKSとECSの両方のコンテナをスキャンし、PCIに良好なカバレッジを提供します」

Orca Securityは、脅威に対する注意を喚起するための一目で分かる実用的なアラートをリアルタイムで送信します。Orcaが新しい脆弱性を発見した場合、すぐに知ることができます」

Shahar Maor
情報セキュリティ最高責任者
Fiverr

最小限の労力で完全な視認性

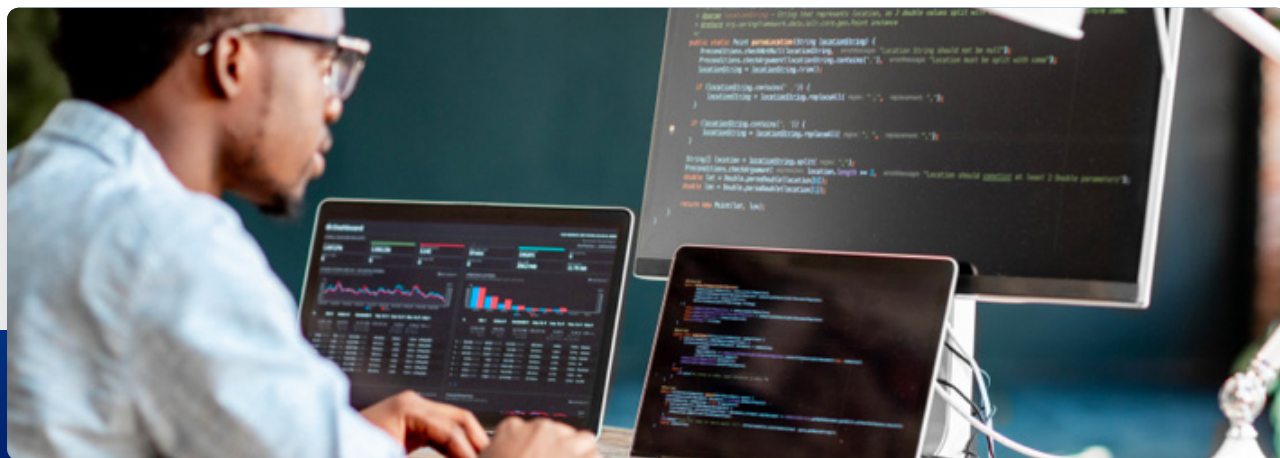
実装直後、OrcaはMaor氏のチームが対処できる範囲の脆弱性を検出しました。「Orca Securityは、貴重なインサイトとFiverrのセキュリティポスチャーを拡張する機能を提供してくれます。Orcaの実装前は視認性がゼロでした。今では必要なもののすべてを見ることができます」

Maor氏は、この出来事を通じてOrca Securityが必要不可欠なものであることを確認しました。また、Maor氏は次のように述べています。「OrcaとCASBの両方が実装されていますが、次の更新ではインサイトを提供していないCASBを削除する予定です。「エンドツーエンドでのAWSの生産環境の監視はOrcaだけに頼ることになります」

1週間あたりの作業時間を削減し、DevOpsに頼る必要もありません

現在、Maor氏がクラウドのセキュリティ作業に費やす時間は半分になりました。「Orcaの導入により、クラウドセキュリティのメンテナンスと管理にあてていた毎週数時間の作業が不要になりました。さらに、DevOpsのサポートに頼る必要もありません」

さらにボーナスとして、Maor氏は推奨事項と専門知識をOrca Securityのチームに頼ることができます。「Orcaチームにはセキュリティの幅広いバックグラウンドと実用的な知識があり、驚くべきアジリティと柔軟性が備わっています。当社は、Orcaがもたらしてくれる膨大な価値をすでに見いだしつつあります。また、OrcaをAWSの主要なセキュリティプラットフォームとして使用し、成長できることが非常に楽しみです」



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、プラスト半径に基づいてリスクを優先させます。



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

