概要

業界

- セキュリティ

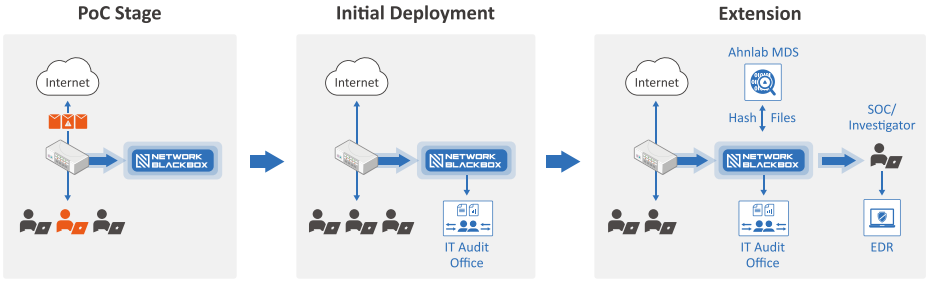
課題

- アナリスト間の情報交換はさまざまな方法（クラウド、Webメールなど）で行われるため、追跡とセキュリティ対策が困難
- クラウドストレージを使用したユーザーの特定

導入効果

- シャドーIT環境におけるIT監査の網羅性の向上
- インターネットを通じたファイル感染や内部情報漏洩へのリアルタイムな対応体制の構築
- 不正コンテンツの使用の検出およびポリシー違反の監査
- インシデント対応時間の短縮

PoCで個人情報の漏洩を検出した事例



今日のスピード感のあるビジネス環境では、サイバー攻撃の脅威が常に存在しており、金融業界は特に脆弱です。 最近、ある証券会社が概念実証 (PoC) による個人情報の漏洩を発見し、高度なサイバー攻撃に対する包括的なセキュリティソリューションの必要性が浮き彫りになりました。同社は、従来のセキュリティソリューションでは、この種の攻撃を検出して防止するには不十分であることに気付き、Quad Minersにソリューションを求めました。証券業界は規制が厳しく競争の激しい市場です。また密性の高い財務データを保護し、顧客の信頼を維持するためにはセキュリティが最も重要となります。 全米 No.1 の証券会社は、サイバー脅威から資産を保護し、顧客データの機密性を維持するための包括的なセキュリティ ソリューションの必要性を感じていました。

Quad Miners の Network Detection and Response (NDR) ソリューションは、PoC攻撃による個人情報漏洩の検出など、同社のセキュリティ課題に対処するために実装されました。 同社は、Advanced Persistent Threat (APT) を検出して迅速に対応し、データ侵害や経済的損失のリスクを最小限に抑えることができるソリューションに重要性を感じていました。

Quad MinersのNDRソリューションは、同社のセキュリティへの強い懸念に対処するだけでなく、APTソリューションと統合することでセキュリティ対応を拡充し柔軟性を提供しました。この統合により同社はセキュリティ体制を強化し、新たな脅威への先んじた対応を実現しました。

このケーススタディでは、同社がPoC攻撃による個人情報の漏洩を検出し対応するにあたって、どのようにQuad MinersのNDRソリューションが貢献したか、さらには同社がAPTソリューションの統合によってセキュリティ対応をどのように拡充しかのかを考察します。また、NDRソリューションの利点と、NDRソリューションが会社のより良い安全性と復旧能力を持つインフラの実現にどのように貢献したのかを説明します。

背景

アナリストの仕事の性質上、会社の基本要素を分析するためにはインターネットを安全に使用できるようにする必要があります。また同社では業務効率化のため、アナリストが会社からの許可なく別のアプリケーションを使用するシャドーITでの作業環境がありました。これらのアプリケーションの使用は機密データの窃取やマルウェアのネットワークへの導入などの可能性があるため、重大なセキュリティリスクに繋がります。
これの課題に対処するために、同社はシャドーITでの作業環境用のセキュリティポリシーを実装していました。しかし、セキュリティポリシーによるアプリケーションのサポートが制限されているため、セキュリティ対策には依然として穴がありました。さらに同社はDLP (Data Loss Prevention) ソリューションを導入していましたが、これらのソリューションでもアプリケーションのサポートが制限されていたため、さらに多くのセキュリティ上の脆弱性が生じていました。
Quad Miners の NDR ソリューションはこれらの課題に対処し、包括的なセキュリティプラットフォームを提供するために実装されました。このNDRソリューションにより、ネットワークトラフィックの完全な可視化、シャドーITアプリケーションによるものを含む、高度なサイバー脅威の検出および対応を実現しました。さらにこのソリューションは、セキュリティポリシーを拡張してより多くのアプリケーションやデバイスを対象とでき、セキュリティ対策の穴や脆弱性を最小限に抑えることに成功しました。

課題

証券業界では投資判断を下すために、判断材料となる情報をアナリスト間で交換することが不可欠です。しかし、情報交換はクラウドベースのアプリケーション、Webメール、SaaSでのファイル交換など、さまざまな方法で行われるため追跡と保護が困難となります。これはデータの損失や盗難のリスクを最小限に抑えるために、内部で使用されているアプリやコンテンツに関する情報を特定する必要があるため、セキュリティチームにとって大きな課題となります。
さらに、クラウドストレージを使用しているユーザーを特定するとセキュリティの課題がより複雑化します。同社はDLPソリューションを運用していますが、このソリューションではセキュリティポリシーによるアプリケーションサポートが制限されています。そのため、クラウドベースのアプリケーションを流れるデータを監視して保護することが難しくなり、重大なセキュリティリスクが生じます。
同社が直面しているもう1つの課題は、IT監査室からのフォローアップの遅れです。その結果セキュリティインシデント対して適時に対処できず、セキュリティの脆弱性とリスクがさらに高まる可能性があります。

ソリューション

Quad Miners の NDR ソリューションは、課題に対処するための包括的なセキュリティプラットフォームを提供し、以下のセキュリティ体制の強化に貢献しました。
Quad Miners の アプリケーションパーサ は、RSA や Darktrace などの競合他社より秀でており、情報漏洩を検出する概念実証 (PoC) ソリューションでした。 この機能により、同社はシャドー IT アプリケーションを含むさまざまなチャネルを通じて転送された機密データを特定できました。
Quad Miners の Network Blackbox は、ネットワーク トラフィックの完全な可視性を提供し、高度なサイバー脅威をリアルタイムで検出して対応できるようにしました。 Network Blackbox は、動的ファイル分析システムである Ahnlab MDS と統合され、インターネットトランザクション間のすべてのファイルをチェックします。 この統合により、同社は SOC のシステムと統合されたEndpoint Detection and Response (EDR) を使用して、潜在的な脅威に迅速に対応できるようになりました。
Network Blackbox は、同社がネットワーク トラフィックを監視し許可されていないクラウド ストレージを使用している人物を特定することにも貢献しました。 これにより、同社は認可されていないアプリケーションを使用していた従業員を特定し、セキュリティリスクを軽減するための適切な措置を講じることができました。

導入効果

Quad MinersのNDRソリューションを実装した後、同社のセキュリティ体制は大幅に改善されました。 RSA や Darktrace などの競合 PoC でしか利用できない アプリケーションパーサを提供することで、これまで見逃していた情報漏洩の検出が可能となりました。 Network Blackbox は動的ファイル分析システムである Ahnlab MDS とも統合され、インターネットトランザクション間のすべてのファイルをチェックし、SOC のシステムと EDR の統合を通じてリアルタイムで応答します。 これにより、悪意のあるファイルの感染やインターネットを介した内部情報の漏洩に対して、即時に対応する体制を確立することができました。
さらに、NDR ソリューションによってNetwork Blackbox を介したネットワーク トラフィックの監視が可能となり、許可されていないクラウドストレージを使用した人物を特定できました。 これにより、インターネット 網のパケットのフルキャプチャを通じて、不正なコンテンツの使用を検出し、ポリシー違反を監査する機能が提供され、シャドー IT 環境に対する 監査の網羅性が向上しました。 さらに、このソリューションがネットワークトラフィック全体を可視化することで、同社はインシデント対応時間を短縮し、セキュリティインシデントへのより効率的かつ効果的な対応を実現しました。 総じて、Quad Miners の NDR ソリューションは、同社がより包括的で効果的なセキュリティプラットフォームを実現し、サイバー脅威から顧客データを保護することに貢献しました。

サマリ

このケーススタディでは、Quad Miners は、シャドー IT 環境とセキュリティポリシーによるアプリケーションサポートの制限により、セキュリティ防御の盲点という課題に直面していた国内最大の証券会社に NDR ソリューションを提供しました。 NDR ソリューションは、ネットワーク トラフィックを完全に可視化し、同社が高度なサイバー脅威を検出して対応し、セキュリティの脆弱性と死角を最小限に抑えることを可能にしました。 その結果、同社は IT 監査の盲点を減らし、悪意のあるファイルの感染と内部情報漏洩に対するリアルタイムの対応システムを確立し、ネットワークトラフィック全体を可視化しインシデント対応時間を短縮することに成功しました。

セキュリティ企業がNDRソリューションを必要とする理由

セキュリティ企業は機密性の高い財務データを厳格な規制のもと扱っているため、サイバー攻撃者にとって格好の標的となっています。 Network Detection and Response (NDR) ソリューションは、同社がシャドー IT のアプリケーションによって引き起こされるものを含む、高度なサイバー脅威の検出と対応を実現する包括的なセキュリティ プラットフォームを提供します。 NDR ソリューションを実装することにより、同社は顧客データの機密性を維持し、セキュリティ侵害のリスクを軽減し、さらに規制要件を遵守することができます。