napatech

ケーススタディ：IBM® QRadar®でネットワークフォレンジックを強化

IBM

業界の問題点

悪意のある攻撃を特定するまでの平均時間は229日間です。そして攻撃を阻止するため、これに対処する平均時間は82日間です*。これらの統計結果は、迅速かつ完全に脅威を検出すること、つまりトラフィック全体を常時監視することの重要性を明確に実証しています。ただし、大半のセキュリティソリューションは発生する攻撃をリアルタイムで検出するために設計されており、多くの場合、対処に必要な証拠を取得、保持することは不可能です(特に攻撃が何か月、或いは何年も前に発生した場合)。その結果、多くの企業が思い知らされているように、壊滅的な事態に陥ることがあります。

こうした問題に対処するため、IBM®は企業が異常を検知して高度な脅威を発見するのに役立つ最新のセキュリティプラットフォームであるQRadar® SIEMを開発しました。

クライアントの課題

QRadar®SIEMの開発にあたり、IBM®はこのプラットフォームですべてのネットワークデータを取得、保存して、攻撃を受けた際にはエンドユーザーに対し、証拠を完全な状態で妥協なく確実に提供する必要がありました。

これを実現するために、IBM®はすべてのデータを欠けることなくリアルタイムでキャプチャでき、侵害が発生した時には選択したデータをインシデントのフォレンジック調査のために速やかに取得できる技術を持った協業者を業界で探していました。

IBM®には、強力な実績と、この業界に対する深い造詣、そして議論の余地のない最高の技術を持ったパートナーが必要だったのです。すべての要件を満たす唯一の候補者であるNapatechが選ばれたのは自然な成り行きでした。

「Napatechを使用すれば睡眠時間を削る必要はありません。エンジニアリングチームとテクノロジの素晴らしい統合により、当社はNapatechによる世界クラスの製品提供に対して絶対的な信頼を置いています。」

IBMセキュリティ部門
フォレンジック最高技術責任者
Russel Couturier 博士

課題

IBM® はQRadar® SIEMプラットフォームで100%のネットワークデータを確実に捕捉および取得し、サイバーセキュリティ侵害が発生した場合には、妥協なく正確な証拠をエンドユーザーに確実に提供できる必要がありました。

ソリューション

Napatechは戦略的パートナーとして選定され、必要とされる最高のテクノロジを提供しました。これにより確実に、すべてのデータが欠けることなくリアルタイムでキャプチャされ、侵害が発生した場合に選択したデータをインシデントのフォレンジック調査用に速やかに取得できます。

利点

- 全証拠の可用性を保証
- 超高速データ抽出
- 並外れて長いデータ保持期間
- 全体的でインテリジェントなトラフィックへの洞察

* Ponemon Institute

当社のソリューション

IBM®は解析装置の性能を向上するために以前からNapatechのテクノロジを導入しており、これによって100%のネットワークデータがリアルタイムで確実にキャプチャされていました。今回、完全なネットワーク履歴がオンデマンドで利用できることを保証するため、新たにNapatechのディスク書き込みテクノロジが統合されました。これにより確実に、すべてのパケットがナノ秒の精度で記録され、素早く簡単にデータが抽出できるようになりました。結果として、QRadar® SIEMは所定のインシデントの全体像を(ほぼ正確な概要ではなく)完全な形でを即座に再構築できます。

利点

このソリューションを採用することにより、IBM®は並外れた高水準のデータ完全性を備えた最先端のセキュリティプラットフォームを提供し、エンドユーザーに対し、必要なときにはいつでもすべてのデータが簡単に利用できるという確信と安心を与えることができました。
含まれている主要な利点:

- ゼロパケットロス - 全証拠の可用性を保証
- 重要情報を超高速抽出
- 全体的でインテリジェントなトラフィックへの洞察

追加された機能

システムパフォーマンスを最適化し、プラットフォーム全体でのシームレスな統合を確保するため、以下のような特注の追加機能が開発されました。

- **2倍のパフォーマンス向上**
  物理的にトラフィックを分割し、フローを適切なCPUコアに直接送信することで、2倍のパフォーマンス向上が達成されました。これにより、フォレンジック調査に必要な大量のデータ分析が容易になりました。

- **固有のセッションID**
  複数のSIEMコンポーネントから通知されるすべての情報を紐付けるメカニズムとして固有のセッションIDが設計されました。これにより、ネットワークパケットと再構築された情報間のインテリジェントなリンクが提供されます。所定の通信セッションのすべてのパケットを固有のIDに関連付けることにより、特定のパケットを瞬時に取得できます。

- **保持期間の延長**
  1つのネットワークに複数のネットワークレコーディング機器を組み込むことで、検索時の性能に影響を与えずに保持期間を延長することができました。これによりフォレンジック調査の時間枠が拡大、エンドユーザーは完全に拡張可能なストレージソリューションを利用できます。

Napatech Pandion

データ量が多大なとき、その関連性はなによりも重要です。Pandionネットワークレコーダーを使用すると、すべてのトラフィックをリアルタイムで捕捉し、オンデマンドで関連するデータのみを取得できます。

Napatech Pandionは、さまざまなイーサネットインターフェイスオプションを利用可能なNapatech SmartNICと構成変更可能なストレージ、それとNapatech Pandionソフトウェアによって構成されています。

Pandionは、10年以上にわたって業界実績のあるNapatech FPGAテクノロジ上に構築されており、100%のキャプチャとディスク書き込みを、最先端のセキュリティ分析およびコンプライアンスアプリケーションにお届けします。

詳細はこちら:
www.napatech.com/products/napatech-pandion/

さらにケーススタディを見る:
www.napatech.com/resources/case-studies

DN-1111 Rev. 1-JA

ヨーロッパ・中東・アフリカ
Napatech A/S
デンマーク コペンハーゲン

Tel. +45 4596 1500
info@napatech.com
www.napatech.com

北米
Napatech Inc.
マサチューセッツ州 ボストン
カリフォルニア州ロスアルトス
ワシントンD.C.

Tel. +1 888 318 8288
info@napatech.com
www.napatech.com

アジア太平洋
Napatech China/South Asia
台湾 台北
Tel. +886 2 28164533 Ext. 319

ナパテックジャパン株式会社
日本 東京
Tel. +81 3 5326 3374
ntjapansales@napatech.com