napatech

ケーススタディ：最先端の脅威検知プラットフォームで問題事象の対処時間を短縮

ROHDE&SCHWARZ
Cybersecurity

業界における難題

ソフトウェアが全てを定義する世の中で、無数のエンドポイントとネットワークをあふれ出るとてつもなく大量のデータにより、アセットやリソースを保護する事の重要性は、組織にとってかつてなく深刻なものとなっています。Cybersecurity Ventures社によると、企業に対するサイバー攻撃はこのたった２年の間に15倍にも増加し、その損害は2015年の3億2500万ドルから2017年だけでも50億ドルを超えると予想されています。

脅威インテリジェンスプラットフォーム、及びセキュリティ情報・イベントマネジメントシステム（SIEM）はサイバー攻撃に対抗するセキュリティオペレーション（SecOps）チームにとって非常に貴重な手助けとなります。しかしながら、これらのツールはかなりの量のイベントデータを収集しますが、ネットワーク上で送受信された完全なパケットデータの記録は提供しません。このため、あらゆる疑わしいイベントを検知、優先順位付けして解決するためには、非常に深いレベルでの洞察が求められます。

課題

市場で最も高機能なイベント管理ツールの一つであるSplunkは様々な業界で、企業インフラストラクチャ内のセキュリティ、ネットワーク、サーバ資産からのデータ収集に活用されています。しかしながら、ネットワークセキュリティやパフォーマンス要件を満たすために必要な洞察を提供するには、Splunkによって記録された不自然な挙動は優先順位付けされた上で分析されなければなりません。このタスクには数十億のログの要約と順位付けが関連し、問題事象に対する反応時間が大きく遅延する一方でSecOpsチームを限界まで駆り立てます。

“93%のセキュリティ要員は、大量のアラートデータに圧倒されており、全ての潜在脅威に対して処理の優先順位を決める事が出来ません。”

インテルセキュリティ

ソリューション

この課題に取り組むために、Rohde & Schwarz CybersecurityはSplunkや他のイベント管理システムを活用した最新のネットワーク脅威検知プラットフォームを作るため、Napatechと協業しました。このプラットフォームはすべてのパケットを保持、記録する事で100%データの透明性と可視性を提供し、SecOpsチームに疑わしいイベントとその重大度を瞬時に洗い出せるツールを提供します。

課題

Splunkや類似する脅威インテリジェンスプラットフォームによって記録された異常なアクティビティは優先順位付けされ、解析されなければいけません。これには数十億のログが関連し、問題事象に対する反応時間が大きく遅延する一方でSecOpsチームを限界まで駆り立てます。

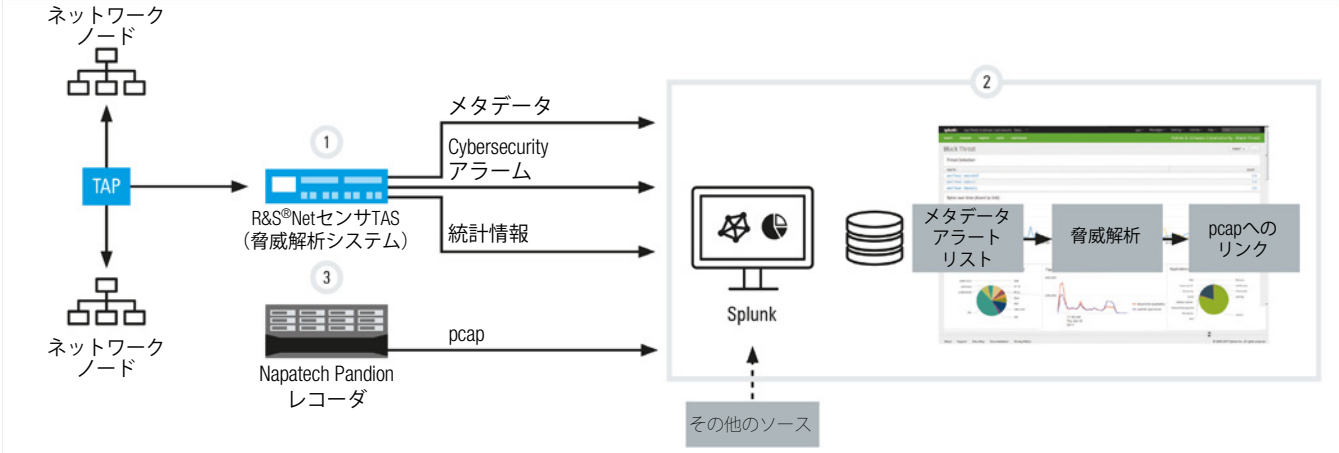
ソリューション

Rohde & Schwarz Cybersecurityは、SecOpsチームが細分化されたレベルで選択された問題事象をすばやく優先順位付けし調査できるようにするような、Splunkを活用した最新のネットワーク脅威検知プラットフォームを作るためにNapatechと協業しました。

利点

- 完全なトラフィック可視性
- 詳細なパケット履歴への即時アクセス
- 迅速な対処時間
- 既存のSplunkや類似する脅威インテリジェンスプラットフォームとのシームレスな統合

階層の深くに潜んだ脅威を検出するRohde & Schwarz CybersecurityおよびNapatechソリューション



ソリューションは3つの分岐を持ったアプローチをとります：

1. **R&Sネットセンサ TAS（脅威解析システム）**は、メタデータと統計情報抽出のためトラフィックにディープ・パケット・インスペクション（DPI）を行い、これらを既知の侵入検知システム（IDS）ルールとマッチさせます。TASはそれからSplunkなどの解析プラットフォームにこれらの解析結果を転送します。

2. **Splunk**はTASから得られたデータを表示し、トラフィックメタデータに基づいて、必要のある追加の脅威解析を行います。

3. **Napatech Pandion**レコーダはリアルタイムで40Gbpsまでの全データパケットをキャプチャし、記録します。大容量のPCAPリポジトリは長期間に渡ってデータを保持し、さらなる調査のためにSplunkがいつでも瞬時に必要なデータを抽出できるようにします。

ケース

TASから疑わしいドメイン名とともに通知されたSplunkイベントをセキュリティエンジニアが調査しているというシナリオについて考察します。対応するファイアウォールからのイベントは、解決したアドレスへの接続が試みられたことを示していました。

このアクティビティをさらに調査するために、エンジニアはSplunkでイベントをクリック、Pandionワークフローを利用して、ほんの数秒間でこのアドレス解決とそれに続く接続に関連するフルパケットレコードを見ることができます。

この情報がない場合、イベントを報告するかまたは無視するかの判断基準は推測だけになってしまいます。パケットデータを分析することで、 エンジニアは疑わしいアドレスに実際に何が送信/受信されたか、有害なドキュメントがダウンロードされたか否か、そしてインフラ外に送信された情報があるかどうか、正確に判断可能です。

利点

この情報に基づき、セキュリティエンジニアはSplunkイベントに関する重大度とその影響をすぐに判断でき、イベントの全容を理解して即座に必要な対処を施すことができます。

一般的なIDSとフルDPI、そして強力なフォレンジック性能を組み合せる事で、プラットフォームは検知のためのシグネチャが登録済みの既知の脅威はもちろん、典型的なセキュリティツールでは検知しにくい新たな例外をも企業が検知することを可能にします。これによって可視性が増大し、問題事象への対処時間は劇的に短縮されます。

主な付加価値：

- 完全なトラフィック可視性
- 詳細なパケット履歴への即時アクセス
- 迅速な対処時間
- 既存のイベント管理システムとのシームレスな統合

DN-1137 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
ntapacsales@napatech.com