napatech

ケーススタディ：Splunk を完全かつシームレスなネットワークの可視化に活用する

Splunk とは

Splunk は主要なマシンデータ用ソフトウェアプラットフォームで、ユーザはリアルタイムで業務上のインテリジェンスを得ることができます。そのミッションはマシンにより生成されたビッグデータの膨大なストリームを管理する際に生じる課題および機会に対処することです。

課題：
何十億ものログを克服

市場で最も多様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。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的に分析する必要があります。

このタスクは一般的にセキュリティおよびネットワークオペレーションセンター (SOC および NOC) により管理され、何十億ものログ通知から優先度の高い対処可能なイベントを生成しています。しかしながら、Splunk 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データの完全な記録は提供しません。そのため、SOC および NOC には疑わしく見えるイベントを裏付けて解決する方法が必要です。

「不正確および誤った情報への対応に費やしている時間の平均コストは、年間 127 万ドルになります。」

Ponemon Institute Survey

ソリューション：
Splunk / Pandion の統合

これこそが、まさにNapatech Pandion が支援できる点です。Pandion は 、Splunk イベントやその他のツールで観測された不自然な挙動と一致する、完全かつ継続的なパケットキャプチャを提供します。以下に示すように、全データはディスクに保存され、オペレーションスタッフによるさらなる詳細な調査に使用できます。

ケース 1

最初のケーススタディでは、金融サービス企業に勤める SOC セキュリティエンジニアが、疑わしいドメイン名とともにSuricataから送信された Splunk イベントを調査しています。

課題

Splunk はかなりの量のデータを収集しますが、ネットワーク上で送受信されたデータの完全な記録は提供しません。そのため、セキュリティおよびネットワークオペレーションセンタには疑わしく見えるイベントを調査するツールが必要です。

ソリューション

Splunk / Pandion の統合により、全てが記録され、ディスクに保存されるので、データに直接アクセスしてさらに調査することができます。

利点

業界をリードする検索速度により、Pandion は数秒で洞察を提供するので、Splunk ユーザはイベントの全貌を把握して修正を行えます。Pandion は既存の Splunk ソリューションとシームレスに統合できるので、企業は過去の投資を活用できます。

DN-1038 Rev. 1

napatech
pandion

Splunk

ファイアウォールからの対応するイベントは、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、SOC エンジニアは Splunk でイベントをクリック、Pandion ワークフローを使用し、ほんの数秒間でこのアドレス解決とそれに続く接続に対応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、イベントをレポート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、SOC 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、実際に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。Splunk イベントの重要度および影響は、憶測や不完全な情報に頼ることなく解決可能です。

ケース 2

2 番目のケーススタディでは、ソーシャルメディアに勤める NOC アナリストが Splunk で遅延/応答なしのアプリケーションアラートを見つけ、懸念される問題箇所を正確に特定する必要がありました。このような調査は、時間がかかり複雑である場合があります。しかし Pandion / Splunk 統合により、NOC アナリストはイベントをクリック、パケットを検索するだけで、どのインフラ領域（ネットワーク、サーバまたはデータベース）に問題がありそうか、すばやく判断できます。避けられないことですが、上記インフラ領域の各担当者は自身が担当するドメインしか監視していないので、「何も問題はない」と申し立てる傾向があります。しかし上記ソリューションを使用すれば、生パケットデータは最終的に組織のどの部門がイベントに対処する必要があるか示し、根本的な原因分析を提供します。

ケース 3

3 番目のケーススタディでは、大手の防衛請負企業で働く調査担当者が、ネットワークセキュリティデバイスが Splunk に疑わしい SSL トラフィックを示すアラートを送信したことに気づきました。このケースでは、サーバはheartbleed バグに脆弱である可能性があります。つまり、クリアテキストのユーザ名やパスワードを含む最近の Web 取引の情報がメモリから読み取られるかもしれません。調査担当者は Splunk でイベントをクリックしパケットを分析することで、直接以下を判断できます：

1. バグが悪意のある第三者に利用されたかどうか
2. 脆弱性により盗まれた実際の情報は何か

「一組織は一週間あたり平均 17,000 近いマルウェアアラートを受信する可能性があります。このようなアラートに対処する時間は組織の経済的リソースおよび IT セキュリティ部門にとって重大な損失です。」

Ponemon Institute Survey

利点

ご覧のように、Pandion のワークフローは簡単です。Splunk でイベントをクリックすることで、オペレーションユーザは Splunk イベントに対応する完全なネットワークパケットのトレースを迅速に得ることが可能です。業界をリードする検索速度により、Pandion は数秒で回答を提供するので、Splunk ユーザはイベントの全貌を把握して、必要な修正を即座に行うことができます。

Pandion は既存の Splunk ソリューションとシームレスに統合できるので、企業は過去の投資を活用し、かなりの費用削減を実現できます。

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

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

Napatech Korea
韓国 ソウル
Tel. +82 2 6001 3545

ntapacsales@napatech.com
www.napatech.com