業界初！

ケーススタディ（大手金融サービス会社）

ExtraHop
See IT run.

次世代ネットワーク・パフォーマンス・モニタリング

“ユニバーサル・ペイロード解析機能”（業界初！）

EH6100アプライアンス
10G x 2ポート

● どうすれば、非常にセキュアな環境において、ネットワーク、インフラ、パフォーマンスが相関付けられた可視性を安全に得られるか?

問題:
数十億ドル規模の金融サービス会社は、PCI標準やSEC規制に違反することなく、ある特定の記録を保持する必要があり、パケットキャプチャや手作業での事後解析に関連する計算コストや労働コストを削減したいと考えていました。

目標:
指定されたデータセットのリアルタイム解析、データ自体のセキュリティを維持しながら、アラートを設定し、異常や傾向を抽出することができること。

ソリューション:
この会社は、ExtraHop SSL Decryption(SSL復号化)、Precision Packet Capture(高精度のパケットキャプチャ)、Alerts(アラート)、Dashboards(ダッシュボード)を使用して、ネットワーク全体のパフォーマンス・メトリックについてリアルタイム解析を実施することで、プロビジョニングコストを削減し、データセキュリティを危険にさらすことなく、解析をチームと共有しました。

結果:
ネットワーク・マネージャは、撤去されたと思っていたのに依然としてアクティブであった43台のDNSサーバを発見しました。
これが会社にコストを負担させ、システム内に大きいセキュリティホールをあけていました。

● 問題

数十億ドル規模の大手金融サービス会社のネットワーク・マネージャは、ネットワーク上のすべての通信を相関付けたL2-L7解析が、迅速かつ事前対応型のネットワーク問題の特定や解決までの時間の鍵であるということを知っていました。課題は、大規模で非常にセキュアな環境内のネットワークに関する完全なビューを得ることであり、この環境では、アプリケーションの75パーセント以上が暗号化され、厳しいコンプライアンス・ポリシーの対象となっていました。

ネットワーク・マネージャは、大規模に復号を実行することができ、以前のプローブのように環境を混乱させることがないソリューションを必要としており、また、プロトコル・アナライザを用いてキャプチャすることによる収集/ふるい分けの手間やリスクがない可視性を必要としていました。こうしたトレースを取得するには、事前承認を得ることを要求されただけでなく、適切な防御と廃棄も要求されました。
この部署には3つの主な課題がありました。

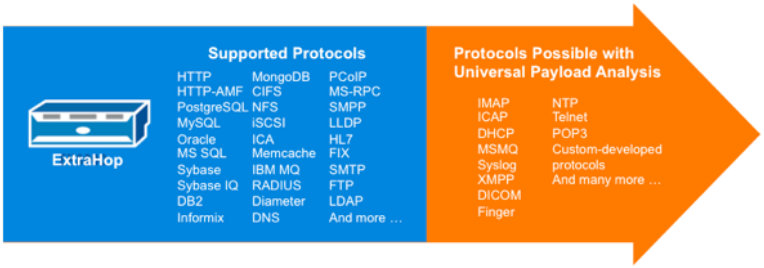
・解析用に自動発見、分類、並べ替え、組み合わせを行うことが可能な詳細な情報にアクセスする
・機能停止時のパケットキャプチャによる収集/ふるい分けの時間や保存にかかるコスト
・サーベンス・オクスリー法、PCI基準またはSEC規制に違反するリスクなしに履歴データを保持する

現行のソリューションとデータセットは最適とは言えませんでした。NetFlowとSNMPデータは若干の基本的な見識を与えていましたが、これは拡張性があまりなく、どのシステムが別のシステムに話しかけているか、交換されるバイト、ドロップ、フレーム・メトリックならびに基本的なリソース使用率しか示しませんでした。

Netflowは他の詳細を求めて戻る機会を提供せず、すべてのレイヤ4-7情報を見逃している一方で、依然として大量のストレージを消費していました。TCPダンプはフォレンジック解析には非常に有益であることが分かっていましたが、Wiresharkのような任意のパケットキャプチャ解析は必要なデータボリュームに合わせて拡張することができず、管理チェーンからの承認を必要としました。

ネットワーク・チームにパケット解析以外の選択肢がなかったとき、コストのかかる要件は、書面による許可を得てから、パケットアナライザをシステムにインストールし、パケットキャプチャを行い、次いでパケットアナライザをアンインストールし、解析後にパケットトレースファイルを安全に破壊することでした。どのようなITパフォーマンス問題の場合でも、アプリケーション・デベロッパー、ストレージ・チーム、DBAははるかに高性能でサイロ化されたツールを持っており、通常、ネットワークに問題があると考えていました。

アプリケーションプロトコルと
ユニバーサルペイロード解析による動作の可視化。



日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY
(TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp

目標

・ネットワーク上のすべての層にわたる通信を収集・可視化する
・階層化アーキテクチャを反映するカスタマイズ可能なダッシュボード
・傾向化と時間比較により、パターンを発見することができる
・組織内で広くダッシュボードを共有することができる
・アプリケーションの変更がどのようにネットワークや他のインフラに影響を及ぼすかを示す

NetFlow、SNMP、およびレポートはある程度の情報を提供していましたが、その情報を調べるのは困難でした。これは他の詳細を求めて戻る機会を提供せず、非常に多くのストレージを消費するものでした。インターフェース毎の約45メガバイトのNetFlow情報に対し、この会社は毎日8～10ギガバイトを保存する必要がありました。

ソリューション

この会社は当初、Citrix解析用にExtraHopを購入しましたが、ネットワーク・チームはExtraHopにはパワフルなネットワーク解析機能もあることに気付きました。実際、ExtraHopはパケットキャプチャ・システムではなく、リアルタイム・ストリーム・プロセッサであるので、セキュアで複雑な環境でコンプライアンスや規制のニーズを満たす理想的なソリューションでした。

ネットワーク・チームはまず、すべてのアクティブなシステムが自動分類されるトップレベルビューからダッシュボードの作成に取りかかり、次いで、ネットワーク上で通信しているシステムの実際の会話を測定しました。ネットワーク・チームは初めて、Netflowを越えて、FTPサーバが話しかけている相手は誰かだけでなく、どのメソッドが使用されていたか、特定のメッセージのレート、レスポンスタイム、トランザクションのサイズはいくつだったかも相関付けることができました。

ネットワーク・チームは、アプリケーションとネットワーク・アーキテクチャ内のほぼすべての層とプロトコルに対して同じことを行いました。時系列の比較により、チームは、前の日、前の週、前の月の同じ時間に同じネットワークがどのように動作していたか、何が通信していたかをすぐに理解することができました。このタイプの状況認識により、インシデントの特定と対応までの時間が60パーセント以上改善されました。

このベースライン化が完了すると、チームはより事前対応型になり始めました。チームは、ExtraHopを用いて、ワイヤ上で特定のデータベースエラーが観測されたときにパケットキャプチャを始動させるApplication Inspection Trigger(アプリケーション・インスペクション・トリガー)をすぐに作成しました。

ExtraHopのPrecision Packet Capture(高精度のパケットキャプチャ)には継続的なリング・バッファがあるので、インベントが発生した時間にさかのぼり、そのイベントの作成に関連するパケットのみを抽出することができます。

エラーイベントが発生したとき、ネットワーク・チームは高精度のパケットキャプチャを解析し、それをExtraHopのデータベース解析とともにDBチームに持って行きました。結局、エラーはテスト中のアプリケーションコードの更新によって引き起こされていたということが分かりました。アプリケーションが時折、同じデータベース呼出しを同じトランザクション内で2回行っていたことがパケットキャプチャにより確認されました。このことが特定されていなければ、この顧客対応アプリケーションに重大な影響が及んでいたことでしょう。

結果

インシデント対応までの時間を60パーセント以上改善しただけでなく、ネットワーク・マネージャは、撤去されたと思っていたのに依然としてアクティブであった43台のDNSサーバを発見しました。

これは、再利用や電力の点で会社にコストを負担させていただけでなく、大きなセキュリティホールをあけていました。また、1日1回ではなく1時間に1回実行され、平均して帯域幅の30パーセントをバックホールリンク上で消費していたストレージ・バックアップ・プロセスも発見されました。この問題は、特定のトラフィックタイプのレイヤ7の可視性とファイル名そのものによって特定されました。
ネットワーク・マネージャにとっての最大の収穫は、事後対応状態から事前対応状態に移行したので、自分と自分のチームが同じスタッフでより多くのより良質の仕事ができるようになったということです。

テクノロジーパートナー

Microsoft splunk> ARISTA f5 CISCO keynote CITRIX SevOne FireEye amazon web services Partner Network TECHNOLOGY PARTNER Gigamon ixia FIREMON

ExtraHop Networksについて

ExtraHopは、ITをよりアジャイルかつプロアクティブにするのに必要なリアルタイムのオペレーション・インテリジェンスを提供します。アドビ(Adobe)、アラスカ航空(Alaska Airlines)、コンカー(Concur)、エクスペディア(Expedia)、マイクロソフト(Microsoft)を始めとする世界で最も成功しているIT組織は、ExtraHopを使用して50万台以上のデバイスを管理し、毎日1兆を超えるトランザクションをモニターしています。

日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp