業界初！

動作解析に基づくビジネスインテリジェンス

ExtraHop
See IT run.

EH6100アプライアンス
10G x 2ポート

リアルタイムでワイヤデータにアクセスすることで、新しい見識を得て、動作解析に基づいたより良い決定を下します

ITデータやビジネスデータのソースのなかで、ワイヤ上でトランザクションを行うソースほどリッチなものは他にありません。
ExtraHopが登場する前までは、こうした通信にアクセスし、重要な情報を抽出する容易な方法がありませんでした。
ExtraHopプラットフォームのリアルタイム・ストリーム・プロセッサは、生のパケットデータを構造化されたワイヤデータに変換するので、これまでは取得することが不可能だったイベント、傾向、トランザクションの詳細を取り出すことができます。このデータを柔軟なダッシュボードで可視化するか、データをElastic, MngoDB またはSplunkなどのサードパーティのデータストアにストリーミングします。

組織が解析のためにどのようにワイヤデータにアクセスしているかについては、下記の各ソリューションをお読みください。

● 使用事例

Heartbleed(ハートブリード) の脆弱性と試行の自動検出
Heartbleed(ハートブリード)が発表された日、あるネットワーク/セキュリティ運用チームはTLS Heartbeat Tracking(TLSハートブリード追跡)、Dashboards(ダッシュボード)、Client Identification(クライアント識別)およびGeomaps(ジオマップ)用のExtraHop Heartbleedバンドルを導入しました。このチームはサーバに不正アクセスしようとする悪意のある試行をリアルタイムで監視し、クライアント用のブロックポリシーを直ちに設定すると同時に、脆弱性のあるシステムにパッチを適用しました。

収入を支払取引と相関付ける
ある金融会社は、ExtraHop Application Inspection Trigger(アプリケーション・インスペクション・トリガー)を使用して、すべての個別の注文や業者毎の総収入、ならびに取引時間をSLAしきい値とともに表示させたことで、リアルタイムの購入傾向を特定することができました。ExtraHopにより、この金融会社はアーキテクチャ改善向けの予算を正当化するのに必要な見識を得ました。

データ持ち出しの検出
ある大規模な政府機関は、データ漏洩の原因を特定し、将来のあらゆるデータ持ち出しを検出する方法を必要としていました。セキュリティチームは、ExtraHopプラットフォームを使用して、漏洩の原因として異常なDNSアクティビティがある特定のマシンを割り出しました。今では、セキュリティチームは、セキュリティのモニタリングと解析に不可欠な要素としてExtraHopを使用しています。

ITビジネス解析
あるチームは、ExtraHopアプライアンスを使用することで、セキュアな支払処理セッションを解読し、取引履歴を照会して、サマリーデータとしては分からない特定の挙動(重複注文など)を調査しました。

医療ITセキュリティ
ある医療組織のITセキュリティチームは、デバイス、認証、ファイアウォールのリアルタイム・モニタリングのためのExtraHop Application Inspection Trigger(アプリケーション・インスペクション・トリガー)を導入することによって、専用のオンサイト監査機能を不要にすることができました。

ICD-9からICD-10の検出と監査
ある大手の医療提供組織は、ICD-10に準拠していることを保証するためにアプリケーション・ベンダやコンサルタントに頼っていましたが、継続的にセルフモニタリングや監査を行う方法がありませんでした。この組織は、ICD-9コードとICD-10コードの送受信を行うすべてのアプリケーションやインターフェースを発見・分類するために、ExtraHop ICD-9 – ICD-10 Detection and Auditバンドルを導入しました。このレベルの可視性は、コンプライアンス期限を保証し、誤ったコード使用による財政的な悪影響を回避するのに役立ちます。

クラウドアプリケーション発見と使用状況モニタリング
ある医療機器メーカーは、すべてのオンプレミスのアプリケーションとクラウドベースのアプリケーションを発見・モニタリングし、一連の許可されていないアプリケーションについての時間比較と使用状況の詳細を見始めました。このメーカーは、200人時間以上、SaaSアプリケーションのライセンスカウントと契約料金における年間$20,000の節減を提案しました。

リアルタイムの処方箋のモニタリングとアラート
ある医療提供組織は、その施設で発行されている処方箋についてのリアルタイム情報を見たいと思っていました。この組織は、HL7メッセージを解析するためのExtraHop Application Inspection Trigger(アプリケーション・インスペクション・トリガー)に加えて、傾向/アラート機能を使用して、オキシコンチンの偽造処方箋の出所を迅速に特定しました。処方箋に対するコンプライアンス/監査の回数はゼロになり、年間で$100,000以上節約されました。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

リアルユーザのモニタリング

ExtraHopは、ある技術サービス会社向けにエンドツーエンドのワークフロー追跡/レポートを作成しました。その結果、この会社のITチームは、ユーザが知覚した負荷時間の一因となっているのは何かを把握し、ユーザがどのようにサイトを体験しているかのリアルタイム解析を実施することが容易に行えるようになりました。

セキュリティ/　暗号化監査

入力SSLトラフィックと出力SSLトラフィックの両方を持つある大企業は、ExtraHopを使用して、ネットワーク上でのSSL挙動の全体を表示させることで、証明書がどのように使用されていたかを把握し、SSLハードウェア購入の計画を立て、使用されていない証明書を削除することができました。

TLS/SSモニタリング

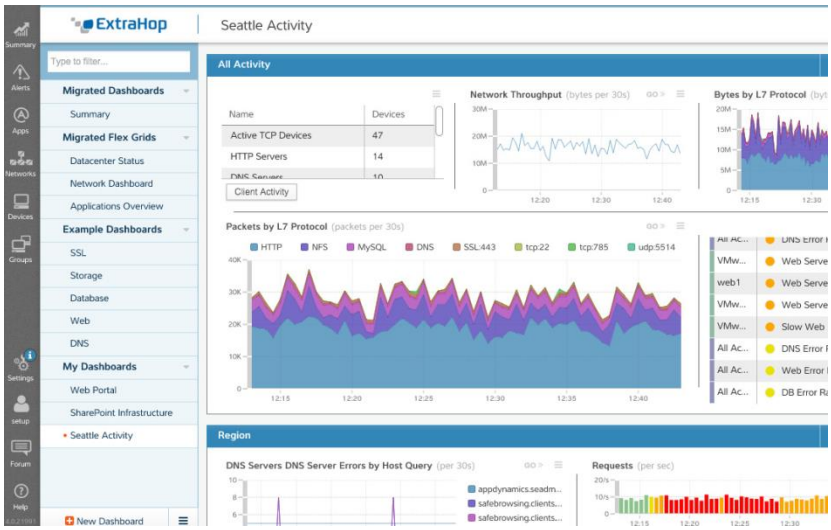
ある大手のウェブホスティング会社は、ExtraHopを使用して、ロードバランサとバックエンドサーバとの間のSSLトラフィックを継続的にモニタリングし、任意のトラフィックが適切に再暗号化されなかった場合はアラートを発報するようにしました。

RFIDのトラブルシューティング

ある大手のEコマース小売業者は、ExtraHopを使用して、パケット・キャプチャやオフライン解析を用いる必要なしに、大規模な倉庫におけるRFIDスキャン時間遅延の根本原因を突き止め、解決しました。動作は正常に戻り、小売業者は再びSLAに準拠することができるようになりました。

APIパフォーマンスの影響を把握する

あるオンライン旅行会社は、すべてのAPIの依存関係を分類・追跡して、その会社とパートナー会社がSLAを満たしているかどうかを確認するのを支援するために、ExtraHopを選択しました。この会社は、APIパフォーマンスの影響に対するプロアクティブな初期警告で、最初の1ヶ月だけで$200,000以上の節減を可能にしました。



テクノロジーパートナー

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

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。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp