業界初！

ExtraHop

セキュリティ&コンプライアンス・ソリューション

ExtraHop
See IT run.

EH6000アプライアンス
10G x 2ポート

● 「セキュリテイ脅威」の識別、データ漏洩の特定、コンプライアンス監査の簡易化に必要なITオペレーション・インテリジェンス

ExtraHopのセキュリティ&コンプライアンス・ソリューションは、モニターするのが困難なメトリックを含むその他のメトリックを最新の方法で提供します（下記）。

・SSLトランザクションレート、移動中にすべての機密データが暗号化されていることを保証する
・期限切れまたは弱いSSL証明書および暗号、強い暗号化が広範に使用されていることを保証する
・VDI環境内のプリンタチャネルおよびUSBチャネルを通過するデータ、ロックダウン環境が実際にロックダウンしていることを保証する
・ユーザ、ファイルパス、名前、頻度、データレート、パフォーマンス毎の追跡を含むファイルアクセスのレポート、機密データの保護を保証する
・認証サーバ上での高強度/低強度のブルートフォース攻撃
・DNS TXTレコードからのデータの引き出し(データを抽出する一般的な手段)
・スーパーユーザ・アカウントのアクティビティ、データベースにアクセスする許可を得た人だけがデータベースにアクセスしていることを保証する

● ExtraHopは、情報セキュリティ/ITチームがセキュリティおよびコンプライアンスの能力を高めるための効率的、且つ効果的な方法を提供します。

ExtraHopは、ワイヤ上のすべての通信を解析することによって、データ漏洩を特定し、IPS/IDSが識別しない脅威を識別し、適切な暗号化を保証し、監査中のコンプライアンスを証明するのに必要な可視性を提供します。

ExtraHopのワイヤデータ解析は、SIEM(セキュリティ情報イベント管理)ベンダあるいは他のログファイルシステムまたはマシンデータ解析システムと容易に統合することができます。

● 機密データへの無許可アクセスをモニターする

ExtraHopは、ワイヤを通過するすべてのトランザクションをパッシブに解析するので、ITチームは、ユーザおよびクライアント毎のデータベース、ストレージ、電子メール、ディレクトリサービスのアクティビティの完全なレコードを即時に得ることができます。

・失敗したディレクトリサービスへのログイン試行に基づいてアラートを生成する
・グループポリシーに従って、公開アプリケーションへの無許可アクセスをモニターする
・特定のストレージパーティション上の機密データへの無許可アクセスを追跡する
・ユーザがロックダウンVDI環境内のUSBチャネルおよびプリンタチャネル上でデータを渡しているかどうかを確認する

● IDSシグネチャがない脅威を識別する

ExtraHopは、地理的データ、履歴データ、層間データを含むコンテキスト的な可視性を提供することによってIDS/IPSを強化するので、ITチームは疑わしいアクティビティを容易に特定・阻止することができます。

・パフォーマンスメトリック、関連するクライアントIPアドレスを有する色分けされたアラートを含む動的なジオマップを表示する
・少なくとも30日間の遡及を含む履歴の傾向を表示することによって、疑わしいアクティビティを特定する
・相関付けられたウェブ、VDI、データベース、ストレージ、DNS、LDAPの通信を表示することによって、イベントの内容を把握する

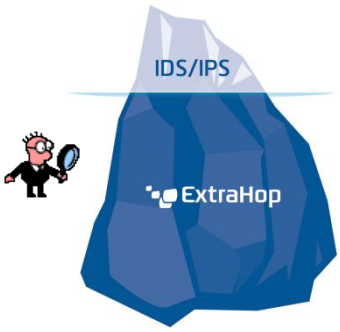
コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

● HIPAAコンプライアンス監査の簡易化・コスト削減

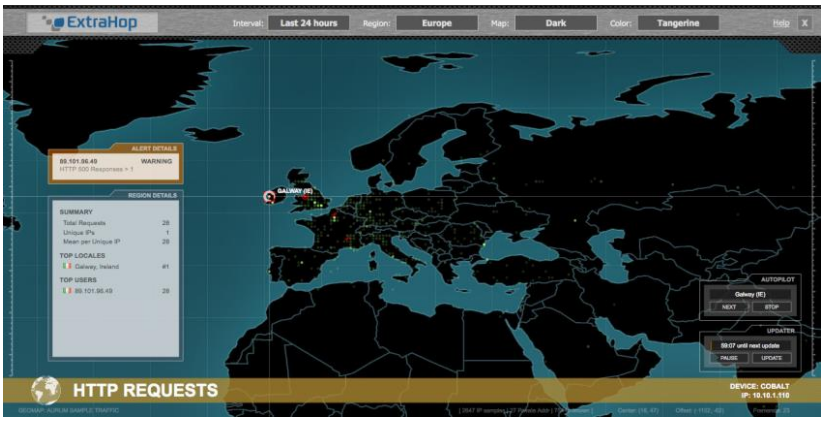
＊HIPAA: United States Health Insurance Portability and Accountability Act of 1996（米国における医療保険の相互運用性と説明責任に関する法令）の略称

平均すると、セキュリティ監査/査定コンサルティングサービスには1～4ヵ月かかり、1回で$150,000～$480,000のコストがかかります。
これは高価なだけではなく、数少ないITスタッフを他の重要なプロジェクトから奪うことになります。ExtraHopからの完全なレコードがあれば、ITチームは主要な要件に対するコンプライアンスを容易に証明することができます。

・すべてのSSLトランザクションを示して、移動中の継続的な暗号化を証明し、有効期限、暗号およびキーの強度を含め、環境全体において使用されている証明書キーに対するコンプライアンスを保証する
・暗号化を使用しなければならないすべてのシステムが実際に暗号を使用していることを確認する
・ユーザによる機密ディレクトリに対するすべての読取り/書込みを示すレポートを作成する
・すべてのデータベースにおいてスーパーユーザのアクティビティを追跡する



シグネチャを使用するIDS/IPSとは異なり、ExtraHopは、コンテキスト（傾向や実際のアクティビティ履歴）を情報セキュリティ/ITチームに提供することによって、脅威を識別します。



ExtraHopは、エラーやその他のイベントの色分けされたアラートを含め、ユーザの地理的位置を明らかにします。

SSL Client: Certificates

Subject	Count ▼	Expires (UTC)	Bytes In	Bytes Out
localhost.localdomain:RSA_2048	7,456	Wed Dec 20 2023	2.0MB	1.9MB
unknown-host-10-10-255-5.sea.l.extrahop.com:RSA_2048	3,680	Thu Aug 4 2022	894.8KB	981.1KB
unknown-host-10-10-254-100.sea.l.extrahop.com l.extrahop.com e...	3,680	Tue Sep 26 2023	1.1MB	981.1KB
www.extrahop.com:RSA_2048	535	Sun Nov 11 2012	338.6KB	201.9KB
forum.extrahop.com:RSA_2048	524	Thu Nov 22 2012	293.1KB	133.0KB
*.google.com:RSA_1024	478	Fri Jun 7 2013	1.1MB	324.7KB

ExtraHopにより、ITチームは、キー強度や証明書の期限を含め、SSL暗号化を容易に監査することができます。

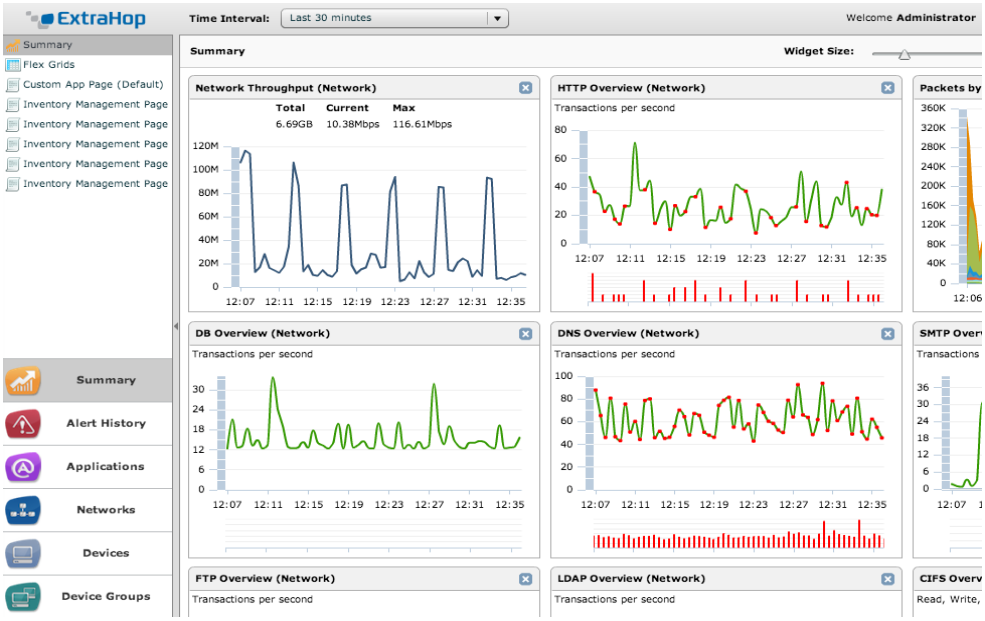
ExtraHopは、通常のAレコードボリュームをTXTレコードボリュームと比較することによって、DNSを介したTCP/IPトンネリングをモニターします。

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

● 6つのセキュリテイソリューションをカバー

ExtraHopプラットフォームはオープンかつ拡張可能で、情報セキュリティ/ITチームが固有の環境に適したその他のカスタムメトリック、アラート、ダッシュボードを作成するのを可能にします。他に類を見ないExtraHopセキュリティ&コンプライアンス・ソリューションは、ExtraHopプラットフォームの柔軟性とパワーを示す6つのユースケースをカバーします(下表)。

ロックダウンVDIモニタリング	セキュアなCitrix VDI環境では、機密データの漏洩を防止するためにUSBチャネルおよびプリンタチャネルはロックダウンされています。ExtraHopは、ユーザおよびクライアントの詳細とともに、保護されたチャネルを通過するすべてのデータにフラグを立てることによって、これらの測定値の継続的な監査を提供します。
SSL暗号化監査	従来であれば、暗号化が最新であり、使用中であることを確認するには、サーバの詳細なロギングが必要になります。ExtraHopはITチームが、ロギングなしで、弱いSSLキーおよび証明書の有効期限を容易に特定することを可能にします。
ストレージアクセスのモニタリング	ExtraHopはネットワーク接続されたストレージシステム上の機密データの継続的なモニタリングを提供するので、ITチームはすべての読取り/書込みのクライアントIP、ユーザ名、ファイルパスを確認することができます。また、ExtraHopは無許可ユーザによる失敗したログイン/ファイルアクセス試行を追跡します。
認証へのブルートフォース攻撃に対するアラート	ExtraHopは、LDAP成功率/失敗率、失敗した試行の合計数、ユーザ毎の試行失敗の頻度をモニタリングすることによって、認証サーバへの高強度/低強度の攻撃を特定します。
DNSを介したTCP/IPトンネリングの検出	DNSを介したTCP/IPトンネリングを使用するマルウェアおよびデータ取り出しの試行を検出します。ExtraHopはDNSレコードタイプを取り出すので、ITチームは通常のAレコードを異常なTXTレコードと比較することができます。
データベース・スーパーユーザ・アカウントの追跡	ルートやSAなどのスーパーユーザ・アカウントにより、悪意のあるユーザが自分のトラックを隠し、損害を与えることが容易になります。ExtraHopは、クライアントおよびサーバの詳細とともに、MySQL、Microsoft SQL Server、その他のデータベースへのスーパーユーザ・ログインを追跡するので、ITチームは迅速に対策を講じることができます。



● ExtraHop Networks社について

ExtraHopはリアルタイムのワイヤデータ解析におけるグローバルリーダーです。ExtraHopオペレーション・インテリジェンス・プラットフォームは、完全な双方向のトランザクション・ペイロードを含む、あらゆるL2-L7通信を解析します。
この革新的なアプローチは、今日の複雑で動的なIT環境におけるアプリケーションのパフォーマンス、アベイラビリティ、セキュリティに不可欠な、相関性がある層間可視性を提供します。

セキュリティ&コンプライアンス・ソリューションはディスカバリ・エディションで実現できます。
無償版の仮想アプライアンスはwww.extrahop.com/discoveryからダウンロードできます。

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

業界初！

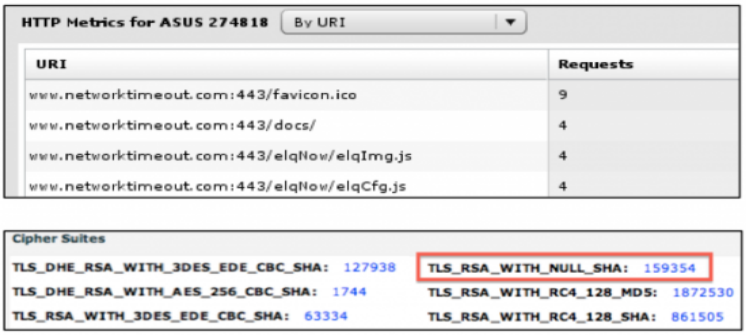
ExtraHop

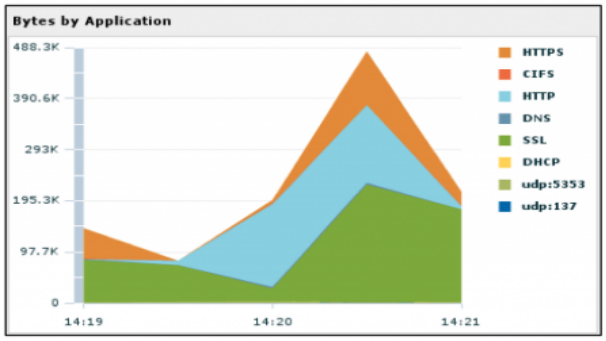
ExtraHop
See IT run.

EH6000アプライアンス
10G x 2ポート

SSLで保護されたトラフィックの復号化と分析をリアルタイムで実行！

SSL Decryption





- ExtraHopのSSL拡張キットはSSLで保護されたトラフィックの復号化と分析をリアルタイムで実行し、ITチームは、セキュリティで保護された環境内でアプリケーションのパフォーマンスを管理したり、暗号、キーの長さや証明書の監査が可能になります。

企業がよりアプリケーショントラフィックのSSL暗号化を導入にするにつれて、セキュアな環境でネットワークやアプリケーションのパフォーマンスをモニターすることが困難になっており、従来のソフトウェアによるSSL復号化では、この増え続ける負荷に追従できません。

（＊ 2011年5月のパロアルトネットワークスのアプリケーション利用とそのリスクに関するレポートによると、ビジネス･アプリケーションの40％以上は、SSLを使用することができ、ネットワークトラフィックの約36％は、SSL暗号化で保護されています。）

- セキュアな環境でリアルタイムパフォーマンスをモニター

ExtraHop SSL拡張キットは、持続的な20Gbpsのまでの速度でリアルタイムにSSLで保護されたトラフィックを復号化し、分析するために暗号化アクセラレーションハードウェアを用いて、このセキュアトラフィックの可視性を復元します。

SSL拡張キットにより、ITチームは前例のない結果を得ることができます。

- 復号化、及び殆どの暗号スイートに関して、SSLで保護されたトラフィックを分析
- 20Gbpsのバルクの復号化を実行する専用のハードウェアにSSL復号化をオフロードすることで、1024ビットキーに対しては最高毎秒200,000SSLハンドシェイク 、2048ビットキーについては最高毎秒35,000 SSLハンドシェイクが可能です。
- NIST(米国国立標準技術研究所)が推奨する2048ビットキーまでの可変キー長をサポート
- 暗号の監査、キーの長さ、および証明書を含む、より簡単な暗号化管理のためのSSLエンベロープ解析を提供

Best of INTEROP WINNER 2013 Cloud Computing & Virtualization

Gartner 2013 CoolVendor

VALUE LEADER EMA Radar for AAPM: Q1-2013 (Small/Medium Deployments)

Networking Innovation Award

WASHINGTON'S BEST WORKPLACES 2013

テクノロジーパートナー

Microsoft splunk> ARISTA f5 CISCO keynote CITRIX SevOne

- ExtraHop Networks社について

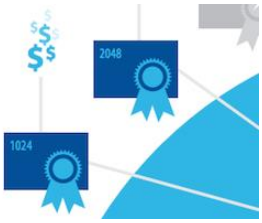
ExtraHopは、ITをよりアジャイルかつプロアクティブにするのに必要なリアルタイムのオペレーション・インテリジェンスを提供します。アドビ(Adobe)、アラスカ航空(Alaska Airlines)、コンカー(Concur)、エクスペディア(Expedia)、マイクロソフト(Microsoft)を始めとする世界で最も成功しているIT組織は、ExtraHopを使用して50万台以上のデバイスを管理し、毎日1兆を超えるトランザクションをモニターしています。

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

業界初！

ExtraHopとSSL 証明書管理

EH6000アプライアンス
10G x 2ポート



- SSL証明書の管理は、ITオペレーションチームに重くのしかかる、日常的、且つ重要な多くのIT管理タスクの一つです。
- ExtraHopは、これらのタスクを容易にし、ITチームがセキュリティやパフォーマンスの問題にプロアクティブに対処するのに役立ちます。

SSL証明書管理

Microsoftが1024ビット未満のRSAキーをブロックする「パッチチューズデー」の更新を発表したとき、システム管理者は慌てて、基準に達していないキーサイズを使用している証明書を探しました。

状況

Microsoftが1024ビット未満の暗号を使用しているSSLキーをブロックする「パッチチューズデー」の更新を発表したとき、システム管理者は慌ててコンプライアンスを確認しなければなりませんでした。

更新後、基準に達していないキー長を使用していたすべてのWindowsサーバとWindowsクライアントでは、IEで暗号化されたウェブサイトへのアクセスがブロックされたり、Microsoft ExchangeやOutlook電子メールで暗号化や署名の暗号化ができなくなったりするなどの問題が発生しました。この更新は、よく知られている認証機関ならびに内部の認証機関の証明書に影響を及ぼすことになりました。

Microsoftは、サーバ上でログを有効にした後、しばらくしてからチェックを行って、基準に達していないキーサイズを使用している証明書を特定することを推奨していますが、このソリューションは大規模なエンタープライズ環境では完全に実現可能なものではありませんでした。

代替策

Microsoftは、キーが 1024 ビット未満である RSA 証明書が使用されているかどうかを確認するには、主に以下の 4 つの方法を推奨しています。

・証明書および証明のパスを手動で確認する
・CAPI2 ログを使用する
・証明書テンプレートを確認する
・この更新プログラムがインストールされているコンピューター上でログを有効にする

アプリケーションが動作しているかどうかを判断する重要なインフラサービスを管理する場合、問題を解決する前に更新を適用するのは全くの問題外です。CAPI2ログを有効にすると、レジストリ編集、フィルタクエリ、旧式の待機(old-fashioned waiting)が必要になります。
コンプライアンスの保証は、手動での修正によるものではなく、簡単で検証可能なものである必要があります。

ExtraHopは、ネットワークを通過するすべてのトランザクションでSSLエンベロープ解析を実行するので、システム管理者はキーサイズ、有効期限、その他の重要な詳細を容易に確認することができます。ログは必要ありません。

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

● ソリューション

ExtraHopがあれば、SSL証明書管理は簡単です。

「Activity Groups」ビューには、ネットワーク上で通信しているすべてのSSLサーバとSSLクライアントがリストアップされた2つのグループがあります。これらのデバイスは自動的に発見・分類されます。SSL Serverアクティビティグループと SSL Clientアクティビティグループには、SSLセッションの詳細やSSLバージョンの内訳を含む豊富な情報があります。

「Certificates」をクリックすることにより、ExtraHopシステムはネットワークを通過する証明書のリストを生成します。

ヘッダーバーとテキストボックスを使用して、これらの証明書のソートやフィルタリングを行うことができます。512のフィルタを使用すると、非準拠SSL証明書のリストが生成され、すぐに利用可能な情報が数時間・数日ではなく数分で提供されます。

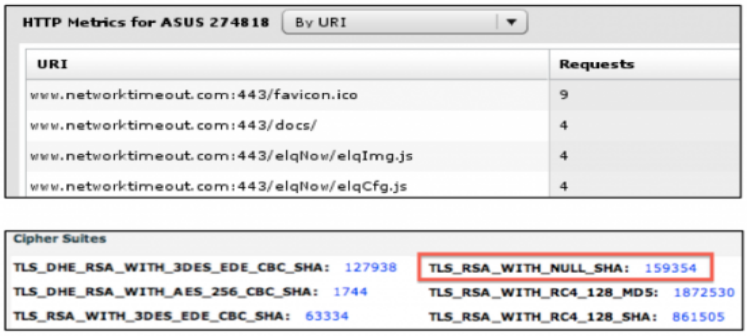
ExtraHopはSSL証明書、DNS、ディレクトリサービスや認証、その他のルーチンのITタスクの管理を容易にします。その結果として、障害対応コストを減少し、よりセキュア且つ信頼性の高い環境の構築が可能になります。

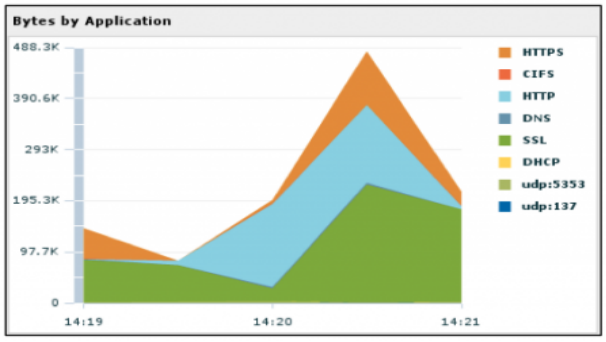
● メリット

SSL証明書は最新のビジネスアプリケーションにとって非常に重要です。
SSL証明書はクラウドベースのサービス、サーバ間の通信、ユーザ認証を有効にしますが、Extra Hopは、SSL証明書管理を容易にし、管理コストを削減します。

ExtraHopにより、エンタープライズで使用中のすべてのSSL証明書をキーサイズや有効期限も含めて把握することが容易になります。

システム管理者は、ログを有効にしたり、証明書テンプレートを手動で調べたりする必要なしに、問題を迅速に見つけて解決するのに必要となるすべての証明書情報を包括的に得ることができます。





● ExtraHop Networks社について

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