ランサムウェアの
リアルタイム
検出・阻止に！

Cisco Tetration Analytics®とExtraHopによるデータセンターのリアルタイム性能管理・可視化と、ランサムウェアの阻止に業界唯一のソリューション！

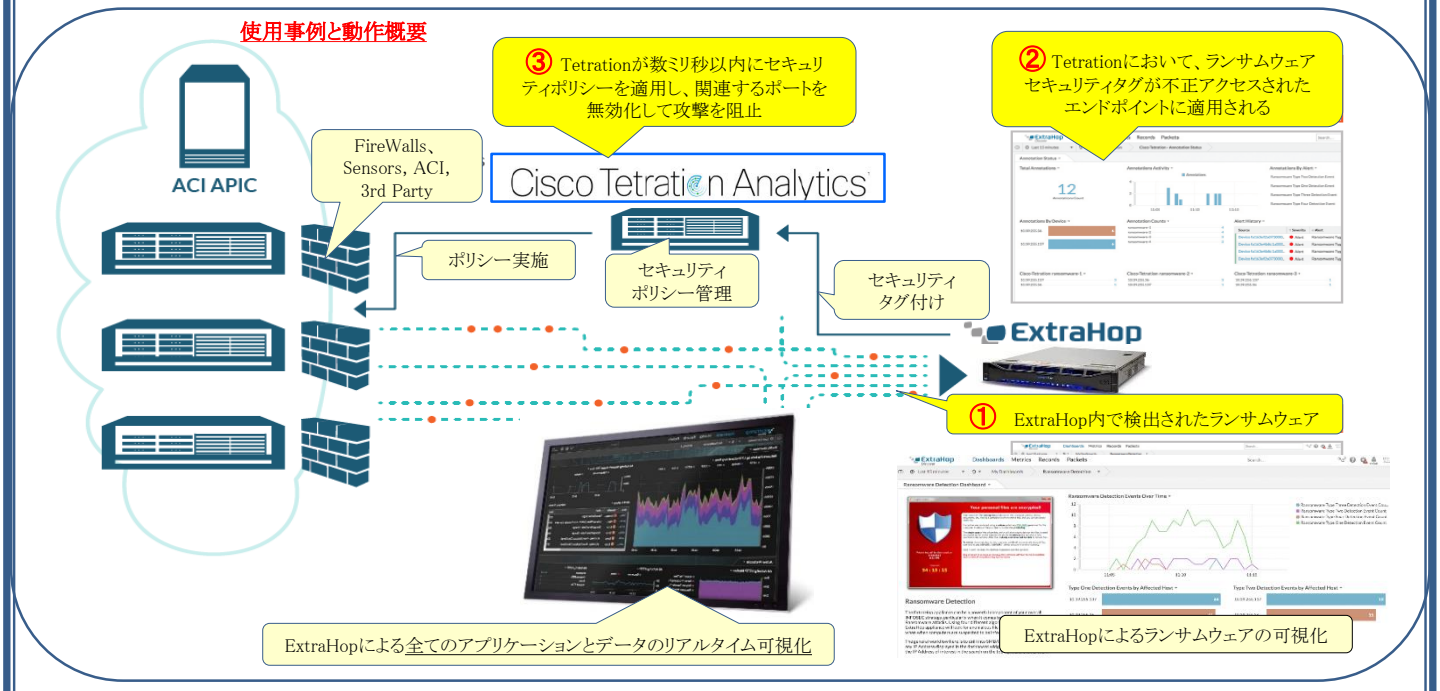
2017 BEST OF Interop ITX

リアルタイムワイヤデータ解析のトップリーダであるExtraHopのアプリケーション(L7)可視性および機械学習機能を、Tetrationのパワフルなセキュリティポリシー施行と組み合わせることによって、ランサムウェアやブルートフォースログイン試行のような脅威に対して、迅速な措置を講じます。

● 動作原理

Cisco Tetration Analytics®とExtraHopの統合ソリューションは、パワフルな見識やブルートフォース・ログイン、ランサムウェア攻撃、期限切れの証明書を始めとするインシデントを検出する機能を提供します。アプリケーションの間を流れるパケットの詳細解析により、セキュリティ問題をリアルタイムで確実に検出します。

その絶好の例としては、ランサムウェア攻撃を検出し、不正アクセスされたホストにタグ付けする機能があります。その後、Tetrationは、そのホスト上で制限付きセキュリティポリシーを施行することができます。この統合は、ExtraHopランサムウェア検出トリガによりTetration REST APIを呼び出し、カスタムタグを適用することによって、実現します。



主なメリット

Cisco Tetration Analytics™とExtraHopを統合したソリューションは、データセンタからクラウド、ネットワークエッジに至るまで、脅威検出やセキュリティポリシーの実施を提供し、以下のシナリオに容易、且つ迅速に実現します。

- **ブルートフォースログイン:** データーベーストラフィック内のスパイク(トラフィックの急上昇)を検出し、スパイクがブルートフォースログイン試行に起因するものであるかどうかを判断し、特定のテーブルクエリまで試行の場所を突き止めます。
- **ランサムウェア攻撃:** 共通インターネットファイルシステム(CIFS)トラフィックを調査してランサムウェアを識別し、不正アクセスされたホストに自動的にタグ付けして攻撃の拡散を阻止します。
- **期限切れの証明書:** Cisco Tetration Analytics™ プラットフォームは、顧客が期限切れの証明書を識別するのを支援します。ExtraHopは、この可視性を一歩前進させ、証明書が期限切れになった特定の1つまたは複数のサーバを識別します。

業界で最も的を絞った正確で迅速なセキュリティポリシーの施行

Cisco Tetration Analytics™ とExtrahop Open Data Streamの統合では、ゼロトラスト実装を簡略化し、異常なネットワーク挙動を検出し、施行ポリシーを自動的にトリガするために、ExtraHopのリアルタイムのアプリケーションレイヤ可視性をCisco Tetrationの自動化ポリシー施行と組み合わせ、最終的には、異常なネットワークトラフィックパターンの背後にある特定のアクティビティを明らかにするリアルタイムのアプリケーションレベルの可視性によって、有益なコンテキストの新しいレイヤを提供します。

これにより、トラフィック挙動を解析・ベースライン化することが可能になり、セキュリティポリシーやマイクロセグメンテーション計画を強固なものにすることができます。更に、データベースサーバ及び外部クライアントからアプリケーションサーバを分けるエンドポイントにおいて即、且つ自動的に適切なファイアウォールポリシーを適用し、業界で最も的を絞った正確で迅速なセキュリティポリシー施行を用いてランサムウェアのような主要な脅威を阻止します。

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

Rev A

Tetration Analytics™

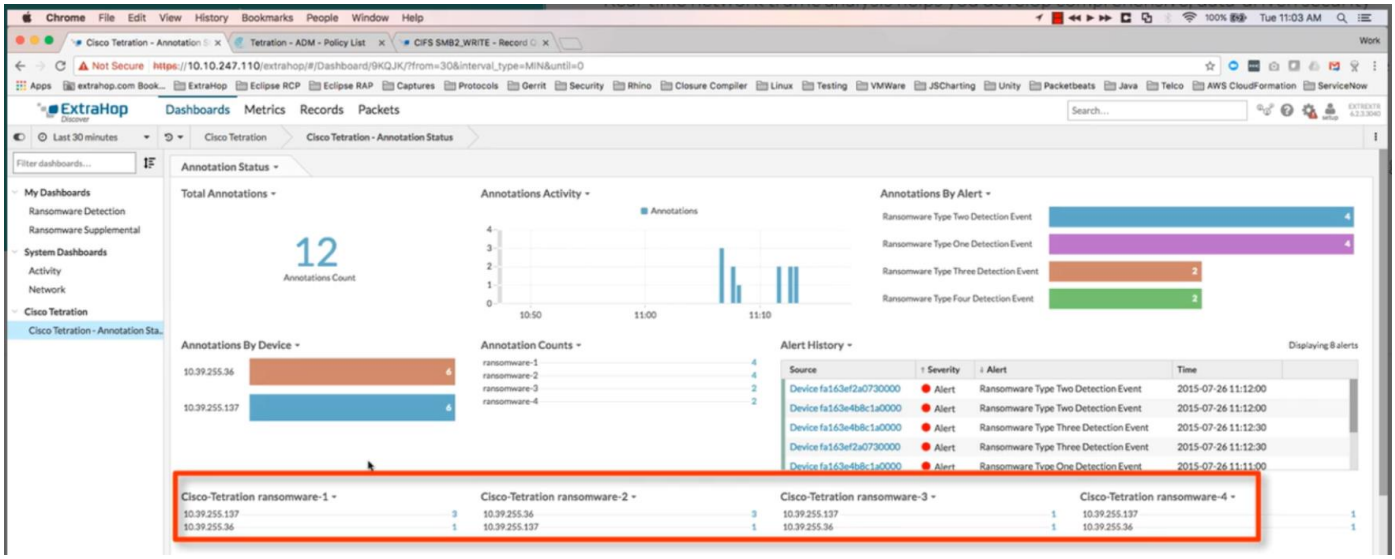
● Cisco Tetration Analytics®とExtraHopによる業界唯一のセキュリティソリューション！

Tetrationは、エンドポイントセンサ、ACI、又はサードパーティのファイアウォールにおいてセキュリティポリシーを適用することができます。これらのセキュリティポリシーは、カスタムのタグ付けにより強化することで、追加のコンテキストを提供することができます。
ExtraHopのL7アプリケーションレイヤ可視性と組み合わせたTetrationのエンドポイントセンサマシンメトリック(L2-L4)は、他に類を見ない詳細なコンテキストを提供し、セキュリティポリシー実施のためのより良いカスタムのタグ付けをサポートします。

＊ExtraHopプラットフォームは、伝送中の全てのデータ(全てのクライアント、ネットワーク、アプリケーション、インフラのアクティビティ)を解析して、リアルタイムのセキュリティの見識からなる豊富な情報源を提供します。

事例

アプリケーションレベルの攻撃（例: ランサムウェア）	・ExtraHopが、不正アクセスされたホストにタグ付けする ・Tetrationが、そのホスト上で制限付きセキュリティポリシーを施行する ・ExtraHopランサムウェア検出トリガが、Tetration REST APIを呼び出して、カスタムタグを適用する
ブルートフォースログイン	ユーザは、データベーストラフィック内のスパイクを検出することと、トラフィックのスパイクがブルートフォースログイン試行に起因するものであるかどうかを判断することの両方を行うことができ、それと共に特定のテーブルが照会される
ランサムウェア	CIFSトラフィックを調査してランサムウェアを見つけ、不正アクセスされたホストに自動的にタグ付けして攻撃の拡散を阻止する
証明書の監査	・証明書が期限切れになった特定の1つまたは複数のサーバを識別する ・不正な証明書を識別する
暗号の監査	暗号スイートが弱い特定の1つまたは複数のサーバを識別する
ネットワークフォレンジック	ユーザは、インシデントの状況を判断するために詳細なアプリケーショントランザクションおよびパケットにアクセスすることができる



● ExtraHopとの統合により、Tetrationユーザーはデータベーストラフィックの急上昇（スパイク）を検出し、照会されている特定のテーブルとともに、ブルートフォースログイン試行によるトラフィックスパイクかどうかを判断できるようになります。 又、ExtraHopはTetrationタグを適用して、関係するクライアントとサーバーを識別します。 更に、Tetrationはセキュリティポリシーを実行して、リスクの高いクライアントとサーバーを分離します。

Tetrationユーザは、ExtraHopプラットフォームのCIFSトラフィックの詳細な分析により、Ransomwareの攻撃をリアルタイムで検出し、停止させることもできます。 ExtraHopがRansomware攻撃を検出すると、侵害されたホストを特定するためにTetrationタグが適用され、セキュリティポリシーの適用によってすぐに隔離されます。更に、ExtraHopは不正な証明書や期限切れの証明書や弱い暗号を識別するためにネットワーク上で監査を実行し、影響を受けるサーバーを識別するためにTetrationタグを適用して、ユーザーによる是正措置を可能にします。

ExtraHop Networks社について

ExtraHop Networks社（アメリカ、シアトル）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、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。

Cisco TetrationとExtraHopの統合の詳細については、
www.extrahop.com/company/tech-partnersをご覧ください。

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

EH3000アプライアンス
10G x 2ポート

Cisco UCS向けExtraHopプラットフォーム

ExtraHop

ExtraHop
See IT run.

Cisco UCS環境内のワイヤデータを解析することによって ITオペレーション・インテリジェンスを得る

ExtraHopプラットフォームは、エンタープライズ・データセンタ内のUCSプラットフォームおよびブランチオフィス内のUCS-Eと連携することが証明されています。
また、ExtraHopは、Citrix VDIの導入をサポートし、XenDesktop、XenApp、NetScalerに対してCitrix Readyであることが確認されています。

- ExtraHopを用いると、ITチームは、これまではタップされていなかったCisco UCS(Unified Computing System：ユニファイド・コンピューティング・システム)環境内の豊富なワイヤデータにアクセスすることによって、ITオペレーション・インテリジェンスを得ることができます。

  ワイヤデータにより、ITチームはパフォーマンスや効率を最適化し、エンドユーザのアクティビティをモニタし、ビジネス・インテリジェンスを提供することができます。

  ExtraHopプラットフォームは、動的でスケーラブルな非侵入型のアプローチを使用しており、エンタープライズ・データセンタ内のUCSプラットフォームとブランチオフィス内のUCS-Eの両方と連携することが証明されている唯一のソリューションです。

- メリット

  ・重要なIT/ビジネスの疑問に答える
  ・仮想化およびプライベートクラウドへの取り組みをサポートする
  ・ユーザに影響を与える前に潜在的な問題を解決する
  ・問題のトラブルシューティングをより迅速に行う
  ・エージェントやプロファイラなしで、データベースのパフォーマンスをモニタする
  ・自動的な発見・分類によって迅速な導入

- 層にまたがる見識によって問題を迅速に解決する

従来のモニタリングツールは、リソース使用率（CPU、メモリ、ディスクI/O）を測定します。ところが、これらの測定値では、特に高度に仮想化された環境において、ユーザが体験するアプリケーションパフォーマンスについてはほとんど明らかになりません。
一方、ITチームはリソース使用率データのみを使用して、実際にアプリケーションがどうなっているかについての全体像を明らかにしなければなりません。

ExtraHopでは、UCS環境におけるパフォーマンスをモニタするより良いアプローチを採用しています。

まず、セッション、フロー、トランザクションをネットワークトラフィックのコピーからパッシブに再構築します。次に、ネットワーク、ウェブ、VDI、ミドルウェア、ストレージの各層から有益なL2-L7パフォーマンスメトリックを抽出します。これにより、ITチームは、プロアクティブになって問題を迅速に解決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得ることができます。

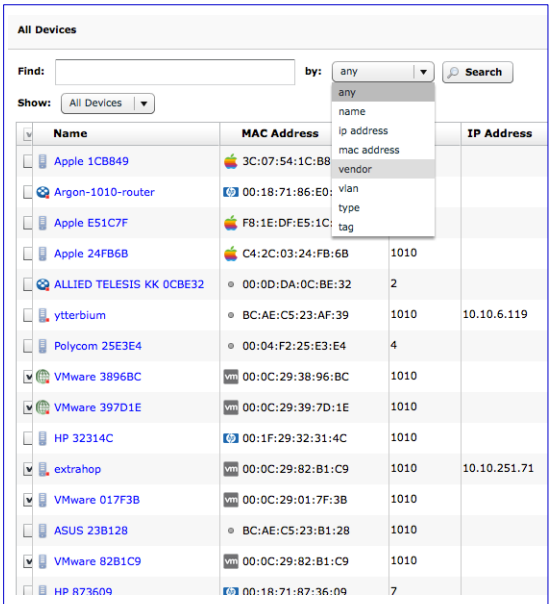
・各層にまたがって相関付けられたトランザクション・モニタリングにより、遅さの根本原因を突き止める
・エラー、メソッド、URI、保存したプロシージャ、ファイル名など、問題を解決するのに必要なアプリケーションレベルの詳細を得る
・エンドユーザに影響を及ぼす前に、リアルタイムのダッシュボードと初期警告アラートによって、新たな問題にプロアクティブに対応する
・従来のモニタリングベンダが自社ツールに組み込むものだけでなく、「なだれの中から雪片を見つける」ためのカスタムメトリックを数分で定義し、関心があるメトリックを提供する

- すべてのアプリケーションに対する動的かつ継続的なモニタリング

Cisco UCSの導入には、それぞれが80Gbpsのバックプレーンを有する、数百のシャーシ内の数千のブレードサーバ上で動作する数万ものVMを含む場合があります。ExtraHopは、こうした動的な環境に適応し、すべてのアプリケーション通信をモニタするように拡張することができる唯一のソリューションです。

・ネットワーク上に現れるアプリケーションやVMを自動的に発見・分類
・テクノロジープラットフォームに関係なく、すべて（自社製、市販）のアプリケーションをモニタ
・すべてのトランザクションをリアルタイムでモニタ（サンプリングや合成トランザクションは不要）
・ベンダに関係なく、すべてのストレージシステムをモニタ

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

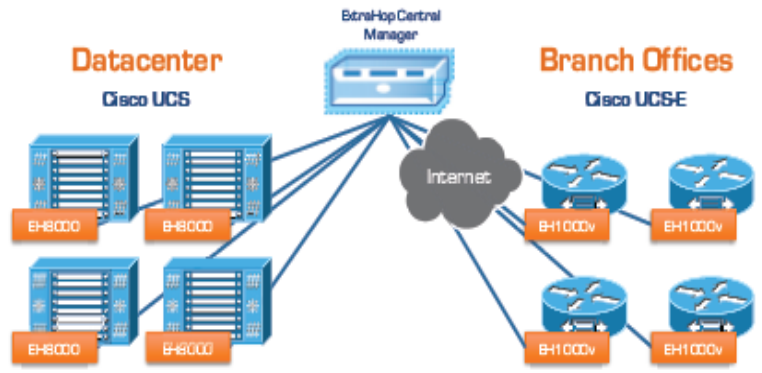


ExtraHopは、アプリケーションやデバイスを自動的に発見・分類します。

ORACLE

IBM DB2 MySQL PostgreSQL Informix SQL Server SYBASE

ExtraHopは、Oracle、IBM DB2、IBM Informix、Microsoft SQL Server、MySQL、PostgreSQL、Sybase ASE、Sybase IQを始めとする、多数のリレーショナルデータベース管理システムのモニタリングを提供します。



ExtraHopにより、ITチームはUCS環境全体からリアルタイムの見識を得ることができます。

● IT/ビジネスの疑問に答える

UCS環境には、有益なITオペレーション・インテリジェンスを提供することができる豊富なワイヤデータがあります。

ExtraHopは、セッション、フロー、トランザクションをリアルタイムで再構築してから、トランザクションペイロード全体を調べることによって、以下のような重要な疑問に答えるための見識を提供します。

・機密ファイルや機密フォルダにアクセスすることでポリシーに違反しているのはどのユーザか?
・この新しいアプリケーションは以前のバージョンと比べてどのように動作するか?
・失敗したAPIウェブサービスコールはどれか?/失敗したのはなぜか?
・デフォルトの上限1MBを超えているために保存されていないのはどのmemcached キーか?
・最新のソフトウェアアップデートによる悪影響を受けているのはどのタイプのクライアントデバイスか?
・アプリケーションはトランザクションを複製しているか?/複製している場合、影響を受けているのは誰か?

● IT/ビジネスの疑問に答える

ExtraHopはCiscoと連携して、UCSとUCS-Eの両方についてExtraHopプラットフォームをテスト・認証しました。

その結果として、ExtraHopプラットフォームはエージェントやプローブを必要とせずに迅速に導入できるだけでなく、エンタープライズ・データセンタ内のUCSプラットフォームおよびブランチオフィス内のUCS-Eと連携することが証明された唯一のソリューションとなっています。

・コンフィグレーションを必要とせずに直ちに可視性を得る
・UCS-Eブレードサーバを動作させているブランチオフィスをモニタ
・システムにオーバーヘッドを課さず、アプリケーションに障害を与えることがない、安心できるパッシブなネットワークベースのアプローチ
・アプリケーションコードを変更することなしに容易にカスタマイズ可能なモニタリング
・迅速な導入

● 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しています。

ExtraHopはwww.extrahop.com/discovery から無償でお試しいただけます。

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