業界唯一！

防衛機関向けExtraHopプラットフォーム

サイバー攻撃を含むリアルタイムコンテキスト解析が可能な業界唯一の状況認識・可視化装置

ネットワークは、任務の目標を達成し、命を救うためのリアルタイムデータが最も豊富なソースですが、状況認識のために当該の伝送中のデータを取り出すことは今までは不可能でした。

ExtraHopプラットフォームは、伝送中のデータを理解するので、防衛機関は、より効果的に任務の成功を確実にすることができます。ワイヤデータを調査することができるので、チームは、問題をより迅速に修復し、パフォーマンスを最適化し、システムをセキュリティ保護し、統合・移行イニシアチブを計画することが可能です。

● 環境内のあらゆるものを発見する

あらゆるものがワイヤ上でトランザクションを行っています。ExtraHopはこの伝送中のデータを解析するので、ユーザはあらゆるデバイスやアプリケーションをリアルタイムで確認することができます。プラットフォームの自動発見/分類機能により、防衛機関の職員が主導権を取り戻し、大規模で動的な異種環境を管理します。

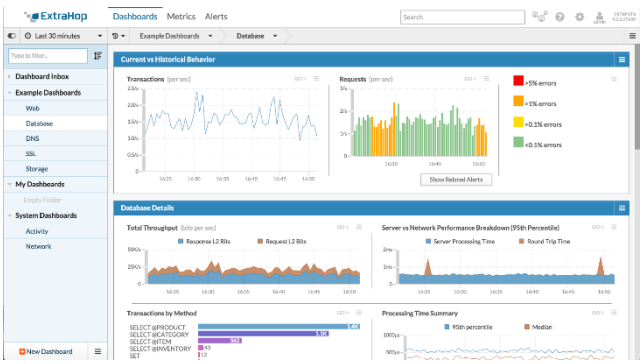
「ExtraHopプラットフォームにより、DoD(国防総省)のクライアントは環境に対する新しい視点を得ることができます。

これは、現状の環境をベースライン化することから、ハイブリッドクラウドにおけるパフォーマンスとセキュリティに関する完全な状況認識を提供することまで、サイバードメインを映す鏡となっています。」

カート・L・ホッジズ(Kurt L. Hodges)
元DoD(国防総省)

● 主な導入メリット

・サイバーハンター/保護チームが異常を特定し、詳細な調査が可能
・禁止されたポート、プロトコル、サービスの使用を監視
・ネットワーク上で通信しているデバイスを自動的に発見し、それらのデバイスの依存関係をマッピング
・エンドツーエンドの可視性により、仮想デスクトップやアプリ(例えばCitrix)の提供を改善
・最大40Gbpsのリアルタイム解析により、大規模で動的な環境をサポート
・セキュリティの弱点や攻撃を特定する
・IT資産を容易に追跡し、依存関係をマッピングする
・動的な仮想化環境における可視性を得る
・エージェントなしで簡単に導入



● 他に類を見ない可視性を得る

ExtraHopはすぐに利用可能な見識を提供できるので、任務チームは環境内の隠れた問題の切り分け・診断を行うことができます。又、ワイヤデータは信頼できる経験的な情報源であり、ワイヤ上でそのデータを観測していれば、何かが起こったことが分かります。

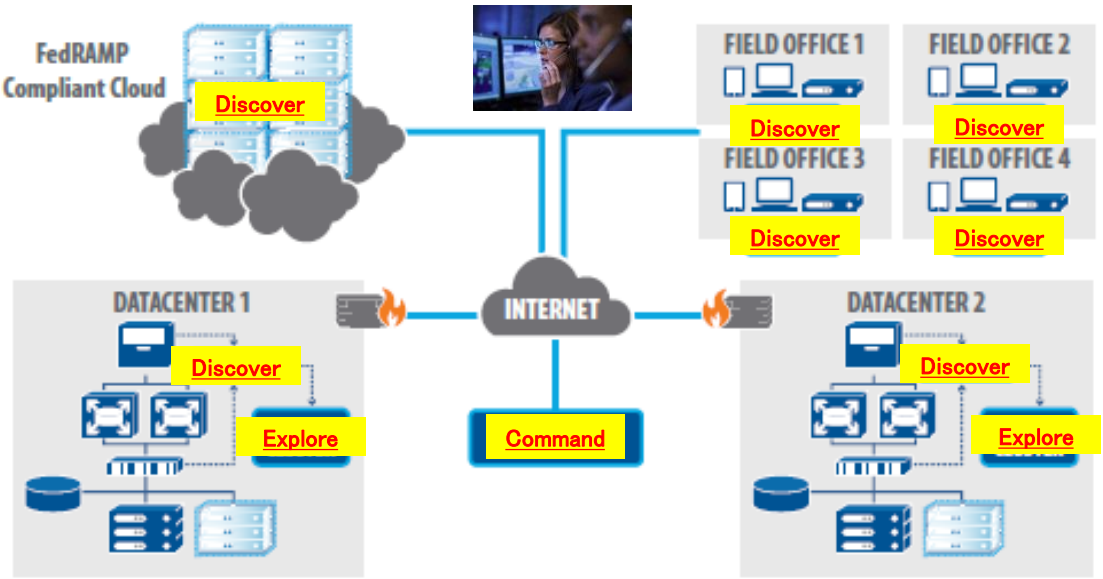
・ドリルダウンして、特定のユーザやデバイスについてのトランザクション詳細を確認する
・重要なサーバからの全てのアウトバウンド接続を監視する
・複数の技術的なレイヤにわたってアクティビティを相関付ける
・信頼できる共有のデータソースを全てのチームに持たせる
・カスタムのメトリックを数分で定義・実装する

● ターンキー解析によってワイヤデータを調査する

ExtraHopにより、チームはワイヤデータを容易に調査してリアルタイムの問題を見つけ、履歴アクティビティを詳細に調べることができます。

・セキュリティインシデントに迅速に対応し、フォレンジック調査を実施する
・誰でもビッグデータ解析を使用することができる – データサイエンティストは不要
・セキュリティやプライバシーの規制に対するコンプライアンスを保証する
・Elastic、Splunk、LogRhythm、Arcsight、AppDynamicsなどの他のプラットフォームにワイヤデータのメトリックを送る

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



● ExtraHop Discover アプライアンスは、ExtraHopプラットフォームの中核となるものです。タップまたはミラーポートからネットワークトラフィックをDiscoverアプライアンスに供給すると、Discoverアプライアンスは、パケットをリアルタイム解析のための構造化されたワイヤデータに変換します。

処理能力

	スループット	監視対象サーバ
物理	最大40Gbps	最大5,500
仮想	最大10Gbps	最大3,000
クラウド	最大10Gbps	最大3,000

● ExtraHop Explore アプライアンスは、Discoverアプライアンスからトランザクション/フローレコードを受信し、それらのレコードに多次元解析用のインデックスを付けます。ユーザは、そこからいつでも見識を検索・調査・ピボット・抽出することができます。

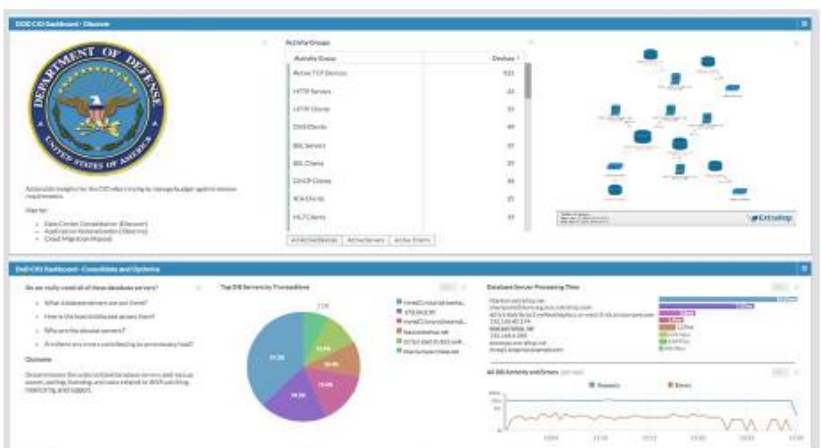
● ExtraHop Command アプライアンスは、データセンタ、クラウド、支店におけるDiscoverアプライアンスからのすべてのデータストリームを統合します。ユーザは、すべてのデータを一箇所でまとめて閲覧・管理することができます。

● 防衛機関の最終結果

ExtraHopプラットフォームは、DoD(国防総省)のサイバーハント、保護、ITの各チームにとっての戦力増強手段です。
このプラットフォームにより、防衛機関は、すぐに利用可能なリアルタイムの見識のために、最も豊富なデータソース(ネットワーク上で伝送中のデータ)を取り出すことができます。

ExtraHopにより、サイバー/ITチームは、IT環境内のあらゆるものを発見・観測・解析することができます。それがネットワーク上で通信している限り、ExtraHopプラットフォームはそれを検出・分類します。一例として、防衛機関は、すべてのアウトバウンド接続を監視し、ネットワーク上の禁止されたポート、プロトコル、サービスを検出することができます。職員は、詳細を掘り下げ、ウェブ、データベース、認証、ストレージトランザクションなどについての詳細を調査することもできます。Extrahopのワイヤデータ解析を用いれば、不要なデータをふるい落として、データから決定までの流れをより一層加速することができます。

デバイス、ポート、プロトコル、サービス(PPS)をパッシブに発見・調査します。



Passively discover and explore devices, ports, protocols, and services (PPS).

ExtraHop Networks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め、全てのL2-L7通信を解析します。これにより、今日の複雑で動的なIT環境に必須である、相関付けられた層間の可視性を実現します。

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