Navigieren im ExtraHop-System

Veröffentlicht: 2024-09-26

Das ExtraHop-System bietet Zugriff auf Netzwerkaktivitätsdaten und Erkennungsdetails über eine dynamische und hochgradig anpassbare Benutzeroberfläche.

Dieses Handbuch bietet einen Überblick über die globale Navigation und die Steuerelemente, Felder und Optionen, die im gesamten System verfügbar sind. siehe Einführung in das ExtraHop-System um zu erfahren, wie das ExtraHop-System Ihre Daten sammelt und analysiert.

Video: Sehen Sie sich die entsprechende Schulung an: Vollständiger Lernpfad zu den UI-Grundlagen

Unterstützte Browser

Die folgenden Browser sind mit allen ExtraHop-Systemen kompatibel. Wenden Sie die von Ihrem Browser bereitgestellten Barrierefreiheits- und Kompatibilitätsfunktionen an, um über technische Hilfsmittel auf Inhalte zuzugreifen.

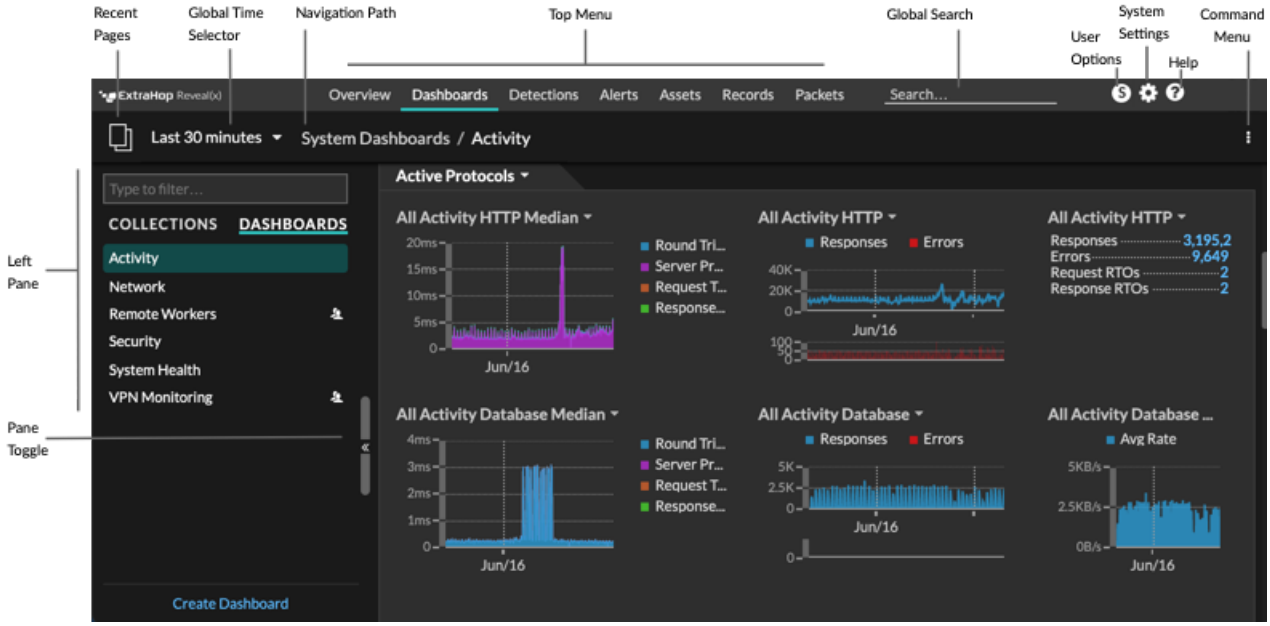
- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Wichtig: Internet Explorer 11 wird nicht mehr unterstützt. Wir empfehlen Ihnen, die neueste Version aller unterstützten Browser zu installieren.

Layout und Menüs

Globale Navigationselemente befinden sich oben auf der Seite und enthalten Links zu den Hauptabschnitten des Systems. In jedem Abschnitt enthält der linke Bereich Links zu bestimmten Seiten oder Daten.

Die folgende Abbildung zeigt sowohl globale Navigationselemente als auch Navigationselemente im linken Bereich.



Hier sind Definitionen der einzelnen globalen Navigationselemente:

Übersichtsseiten

Auf Übersichtsseiten können Sie schnell den Umfang verdächtiger Aktivitäten in Ihrem Netzwerk bewerten, sich über Protokollaktivitäten und Geräteverbindungen informieren und den ein- und ausgehender Datenverkehr in Ihrem Netzwerk untersuchen.

- Sehen Sie sich das an Überblick über die Sicherheit für Informationen über Sicherheitserkennungen in Ihrem Netzwerk.
- Sehen Sie sich das an Überblick über das Netzwerk für Informationen über aktive Geräte in Ihrem Netzwerk.
- Sehen Sie sich das an Perimeter im Überblick für Informationen über den Verkehr, der in und aus Ihrem Netzwerk fließt.

Armaturenbretter

klicken **Armaturenbretter** um Dashboards zur Überwachung aller Aspekte Ihres Netzwerk oder Ihrer Anwendungen anzuzeigen, zu erstellen oder zu teilen. System-Dashboards geben Ihnen einen sofortigen Überblick über die Aktivitäten und potenziellen Sicherheitsbedrohungen in Ihrem Netzwerk.

Warnmeldungen

klicken **Warnmeldungen** um Informationen zu jeder Alarm anzuzeigen, die während des Zeitintervalls generiert wurde.

Erkennungen

Wenn dein Paket oder Fluss Sensor ist mit dem ExtraHop Machine Learning Service verbunden, die Top-Level-Navigation zeigt die **Erkennungen** Speisekarte. Klicken Sie **Erkennungen** um anhand Ihrer wire data identifizierte Erkennungen anzuzeigen. Sie können auf gespeicherte Erkennungen zugreifen, auch wenn Ihre Sensor ist vom Machine Learning Service getrennt.

Hinweis: Erkennungen durch maschinelles Lernen erfordern eine Verbindung zu ExtraHop Cloud Services.

Vermögenswerte

Klicken Sie **Vermögenswerte** um alle Anwendung, Netzwerk oder Gerät zu finden, die vom ExtraHop-System erkannt wurden. Sie können Protokollmetriken für Ihre Ressourcen, aktiven Benutzer oder Netzwerkaktivitäten nach Protokoll anzeigen.

Rekorde

Wenn Ihr ExtraHop-System mit einem konfiguriert ist Recordstore, die Navigation auf oberster Ebene zeigt das Datensatzmenü. Klicken Sie **Rekorde** um alle gespeicherten Datensätze für das aktuelle Zeitintervall abzufragen. Datensätze sind strukturierte Informationen über Transaktionen, Nachrichten und Netzwerkflüsse.

Pakete

Wenn Ihr ExtraHop-System mit einem konfiguriert ist Packetstore, die Navigation auf oberster Ebene zeigt das Menü Pakete. Klicken Sie **Pakete** um alle gespeicherten Pakete für das aktuelle Zeitintervall abzufragen.

Globales Suchfeld

Geben Sie den Namen eines beliebigen Geräts, eines Hostnamens oder einer IP-Adresse, einer Anwendung oder eines Netzwerk ein, um eine Übereinstimmung auf Ihrem Gerät zu finden Sensor oder Konsole. Wenn Sie einen verbundenen Recordstore haben, können Sie nach gespeicherten Datensätzen suchen. Wenn Sie einen verbundenen Packetstore haben, können Sie nach Paketen suchen.

Hilfesymbol

Sehen Sie sich die Hilfeinformationen für die Seite an, die Sie gerade betrachten. Um auf die aktuellsten und umfassendsten ExtraHop-Dokumentationen zuzugreifen, besuchen Sie die ExtraHop Documentation Webseite.

Symbol „Systemeinstellungen“

Greifen Sie auf Systemkonfigurationsoptionen wie Trigger, Alarme, geplante Berichte und benutzerdefinierte Geräte zu und klicken Sie, um das ExtraHop-System und die Version anzuzeigen. Klicken Sie **Hinweise zum System** um eine Liste der Funktionen in der aktuellsten Version und aller Systemhinweise wie ablaufende Lizenzen oder verfügbare Firmware-Upgrades.

Symbol für Benutzeroptionen

Loggen Sie sich ein und melden Sie sich von Ihrem ab Sensor oder Konsole, ändere dein Passwort, wähle das Display-Thema, eine Sprache einstellen und greifen Sie auf API-Optionen zu.

Fenster umschalten

Reduzieren oder erweitern Sie den linken Bereich.

Globaler Zeitselektor

Ändern Sie das Zeitintervall um Anwendung- und Netzwerkaktivitäten anzuzeigen, die vom ExtraHop-System für einen bestimmten Zeitraum beobachtet wurden. Das globale Zeitintervall wird auf alle Metriken im System angewendet und ändert sich nicht, wenn Sie zu verschiedenen Seiten navigieren.

Letzte Seiten

Sehen Sie sich in einem Drop-down-Menü eine Liste der zuletzt besuchten Seiten an und treffen Sie eine Auswahl, um zu einer vorherigen Seite zurückzukehren. Wiederholte Seiten werden dedupliziert und komprimiert, um Platz zu sparen.

Navigationspfad

Sehen Sie sich an, wo Sie sich im System befinden, und klicken Sie auf einen Seitennamen im Pfad , um zu dieser Seite zurückzukehren.

Dropdownmenü im Befehlsmenü

Klicken Sie hier, um auf bestimmte Aktionen für die Seite zuzugreifen, die Sie gerade betrachten. Zum Beispiel, wenn Sie klicken **Armaturenbretter** oben auf der Seite das Befehlsmenü ⋮ bietet Aktionen zum Ändern der Dashboard-Eigenschaften oder zum Erstellen eines neuen Dashboard.

Beginnen Sie mit der Datenanalyse

Beginnen Sie Ihre Reise zur Datenanalyse mit dem ExtraHop-System, indem Sie die unten aufgeführten grundlegenden Workflows befolgen. Sobald Sie sich mit dem ExtraHop-System vertraut gemacht haben, können Sie komplexere Aufgaben wie das Installieren von Bundles und das Erstellen von Triggern erledigen.

Im Folgenden finden Sie einige grundlegende Möglichkeiten, mit dem ExtraHop-System zu navigieren und mit diesem zu arbeiten, um Netzwerkaktivitäten zu analysieren.

Überwachen Sie Kennzahlen und untersuchen Sie interessante Daten

Gute Ausgangspunkte sind die Dashboard zur Netzwerkaktivität und Dashboard zur Netzwerkleistung, die Ihnen Zusammenfassungen wichtiger Kennzahlen zur Anwendungsleistung in Ihrem Netzwerk zeigen. Wenn Sie einen Anstieg des Datenverkehrs, Fehler oder Serververarbeitungszeit feststellen, können Sie mit den Dashboard-Daten interagieren, um bohren Sie nach unten und ermitteln Sie, welche Clients, Server, Methoden oder andere Faktoren zu der ungewöhnlichen Aktivität beigetragen haben.

Anschließend können Sie die Leistungsüberwachung oder Problembehandlung fortsetzen, indem Sie ein benutzerdefiniertes Dashboard erstellen um eine Reihe interessanter Metriken und Geräte zu verfolgen.

Schauen Sie sich Folgendes an Komplettlösungen um mehr über die Überwachung von Daten in Dashboards zu erfahren:

- Überwachen Sie die Leistung Ihrer Website in einem Dashboard
- Überwachen Sie DNS-Fehler in einem Dashboard
- Überwachen Sie den Zustand der Datenbank in einem Dashboard

Suchen Sie nach einem bestimmten Gerät und untersuchen Sie zugehörige Metriken und Transaktionen

Wenn Sie einen langsamen Server untersuchen möchten, können Sie suche nach dem Server im ExtraHop-System anhand des Gerätenamens oder der IP-Adresse und untersuchen Sie dann die Aktivität des Servers auf einer Protokollseite. Gab es einen Anstieg an Antwortfehlern oder Anfragen? War die Serververarbeitungszeit zu hoch oder hat sich die Netzwerklatenz auf die Datenübertragungsrate ausgewirkt? Klicken Sie auf der Geräteseite auf verschiedene Protokolle, um weitere vom ExtraHop-System gesammelte Metrik Daten zu untersuchen. Aufschlüsselung nach Peer-IP-Adressen um zu sehen, mit welchen Clients oder Anwendungen der Server gesprochen hat.

Wenn Ihr ExtraHop-System mit einem verbunden ist Recordstore, Sie können ganze Transaktionen untersuchen, an denen der Server beteiligt war Erstellen einer Datensatzabfrage.

Schauen Sie sich Folgendes an Komplettlösungen um mehr über das Erkunden von Metriken und Datensätzen zu erfahren:

- Erkunden Sie Metriken im ExtraHop-System, um DNS-Fehler zu untersuchen
- Datensätze abfragen, um fehlende Webressourcen zu finden

Verschaffen Sie sich einen Überblick über Änderungen an Ihrem Netzwerk, indem Sie nach Protokollaktivitäten suchen

Sie können Ihr Netzwerk von oben nach unten betrachten, indem Sie sich die integrierten Protokollgruppen ansehen. Eine Protokollgruppe ist eine Sammlung von Geräten, die vom ExtraHop-System auf der Grundlage des über die Leitung beobachteten Protokollverkehrs automatisch gruppiert werden. Sie können beispielsweise neue oder stillgelegte Server finden, die aktiv über ein Protokoll kommunizieren, indem Sie eine Aktivitätskarte erstellen.

Wenn Sie eine Sammlung von Geräten finden, die Sie weiter überwachen möchten, können Sie ein Geräte-Tag hinzufügen oder benutzerdefinierter Gerätename damit diese Geräte im ExtraHop-System leichter auffindbar sind. Du kannst auch eine benutzerdefinierte Gerätegruppe erstellen oder ein benutzerdefiniertes Dashboard um die Aktivität von Gerätegruppe zu überwachen.

Erweiterte Workflows zur Anpassung Ihres ExtraHop-Systems

Nachdem Sie sich mit den grundlegenden Arbeitsabläufen vertraut gemacht haben, können Sie Ihr ExtraHop-System anpassen, indem Sie Warnmeldungen einrichten, benutzerdefinierte Metriken erstellen oder Bundles installieren.

Benachrichtigungen einrichten

Warnmeldungen Verfolgen Sie bestimmte Messwerte, um Sie über Verkehrsabweichungen zu informieren, die auf ein Problem mit einem Netzwerkgerät hinweisen könnten. Einen Schwellenwertalarm konfigurieren um Sie zu benachrichtigen, wenn eine überwachte Metrik einen definierten Wert überschreitet. Konfigurieren Sie eine Trendwarnung um Sie zu benachrichtigen, wenn eine überwachte Metrik von den normalen, vom System beobachteten Trends abweicht.

Erstellen Sie einen Auslöser, um benutzerdefinierte Metriken und Anwendungen zu erstellen

Trigger sind benutzerdefinierte Skripts , die bei einem vordefinierten Ereignis eine Aktion ausführen. Trigger müssen geplant werden, um sicherzustellen, dass ein Auslöser die Systemleistung nicht negativ beeinflusst.

Schauen Sie sich Folgendes an Komplettlösungen um mehr über das Erkunden von Metriken und Datensätzen zu erfahren:

- Erstellen Sie einen Auslöser, um benutzerdefinierte Metriken für HTTP 404-Fehler zu sammeln
- Erstellen Sie einen Auslöser, um Antworten auf NTP-Monlist-Anfragen zu überwachen