Perimeter im Überblick

Veröffentlicht: 2024-07-17

In der Perimeterübersicht werden Diagramme und interaktive Visualisierungen angezeigt, mit denen Sie den Datenverkehr überwachen können, der über Verbindungen mit externen Endpunkten in Ihr Netzwerk ein- und ausströmt.

Video: Sehen Sie sich die entsprechende Schulung an: Überblick über Sicherheit, Netzwerk und Perimeter

Perimeterverkehr

Die Perimeter-Traffic-Diagramme bieten einen Überblick über den Geräteverkehr mit externen Verbindungen.

Eingehender Verkehr

Diese Anzahl zeigt die Gesamtmenge des eingehender Datenverkehr während des ausgewählten Zeitintervalls. Klicken Sie auf die Anzahl, um die Geschwindigkeit anzuzeigen, mit der Daten von externen Endpunkten eintreffen, und eine Aufschlüsselung nach Standort oder Konversation.

Ausgehender Verkehr

Diese Anzahl zeigt die Gesamtmenge des ausgehender Datenverkehr während des ausgewählten Zeitintervalls. Klicken Sie auf die Anzahl, um die Rate anzuzeigen, mit der Daten an externe Endpunkte übertragen werden, und eine Aufschlüsselung nach Standort oder Konversation.

Geräte, die eingehende Verbindungen akzeptieren

Diese Anzahl zeigt die Anzahl der Geräte an, die während des ausgewählten Zeitintervalls eingehende Verbindungen von externen Endpunkten akzeptiert haben. Klicken Sie auf die Anzahl, um eine Übersichtsseite für Gerätegruppe zu öffnen, auf der eine Liste der Geräte, Verkehrsdaten und Protokollaktivitäten angezeigt wird.

Eingehende Verbindungen

Diese Anzahl zeigt die Anzahl der eingehenden Verbindungen an, die von externen Endpunkten initiiert wurden. Klicken Sie auf die Anzahl, um eine detaillierte Ansicht dieser Konversationen zu öffnen.

Verdächtige eingehende Verbindungen

Dieses Zähldiagramm zeigt die Anzahl der Verbindungen an, die von verdächtigen externen Endpunkten initiiert wurden. ExtraHop identifiziert verdächtige Endpunkte durch Bedrohungsinformationen Daten. Klicken Sie auf das Diagramm, um eine gefilterte Ansicht dieser Konversationen zu öffnen.

Verdächtige ausgehende Verbindungen

Diese Anzahl zeigt die Anzahl der Verbindungen an, die interne Endpunkte mit verdächtigen externen Endpunkten initiiert haben. ExtraHop identifiziert verdächtige Endpunkte durch Bedrohungsinformationen Daten. Klicken Sie auf das Diagramm, um eine gefilterte Ansicht dieser Konversationen zu öffnen.

Ungewöhnliche Verbindungen

(Nur RevealX 360) Diese Anzahl zeigt die Anzahl der ausgehenden Verbindungen von Ihrem Netzwerk zu IP-Adressen an, die normalerweise nicht besucht werden oder in der Vergangenheit nicht besucht wurden. Klicken Sie auf das Diagramm, um eine gefilterte Ansicht dieser Konversationen zu öffnen.

Halo-Visualisierung

Die Halo-Visualisierung bietet zwei Ansichten Ihrer Netzwerkverbindungen zu externen Endpunkten: Cloud Services und Large Uploads.

Externe Endpunkte erscheinen auf dem äußeren Ring mit Verbindungen zu internen Endpunkten und erscheinen als Kreise in der Mitte der Visualisierung. Diese Visualisierungen ermöglichen es Ihnen, Ihre Prioritäten zu setzen Untersuchung für Verbindungen, bei denen ein hohes Risiko erkannt wurde, oder für hochwertige Geräte.

Um die Identifizierung von Endpunkten mit hohem Traffic zu erleichtern, nehmen innere und äußere Ringe mit steigendem Verkehrsaufkommen an Größe zu. In einigen Fällen kann die Größe der inneren Kreise und der äußeren Ringsegmente aus Gründen der Lesbarkeit erhöht werden. Klicken Sie auf einen Endpunkt, um genaue Verkehrsinformationen anzuzeigen.

Klicken Sie **Cloud-Dienste** um Verbindungen zwischen internen Endpunkten und Cloud-Dienstanbietern anzuzeigen. Cloud-Dienstanbieter und die Menge der gesendeten oder empfangenen Daten werden im Informationsfeld auf der rechten Seite angezeigt. Sie können zwischen Ansichten wechseln , die angezeigt werden **Ausgehende Bytes** an Anbieter und **Eingehende Byte** zu Ihrem Netzwerk.

Klicken Sie **Große Uploads** um Verbindungen zwischen internen und externen Endpunkten anzuzeigen, bei denen über 1 MB an Daten in einer einzigen Übertragung von Ihrem Netzwerk zu einem Externer Endpunkt übertragen wurden. Externe Endpunkte und die Menge der hochgeladenen Daten werden im Informationsfeld auf der rechten Seite angezeigt.

Hier sind einige Möglichkeiten, wie Sie mit diesen Halo-Visualisierungen interagieren können:

- Zeigen Sie mit der Maus auf Endpunkte oder Verbindungen, um die verfügbaren Hostnamen und IP-Adressen anzuzeigen.
- Zeigen Sie mit der Maus auf Endpunkte oder Verbindungen, um die entsprechenden Listenelemente auf der rechten Seite hervorzuheben. Zeigen Sie ebenfalls mit der Maus auf Listenelemente, um die entsprechenden Endpunkte und Verbindungen in der Halo-Visualisierung hervorzuheben.
- Klicken Sie in der Halo-Visualisierung auf Endpunkte oder Verbindungen, um den Fokus zu behalten und auf der rechten Seite präzise Verkehrsinformationen und Links für Ihre Auswahl anzuzeigen.
- Klicken Sie in der Halo-Visualisierung oder -Liste auf einen Externer Endpunkt, um die Gesamtmenge des eingehenden oder ausgehender Datenverkehr anzuzeigen, der mit dem Endpunkt und den verbundenen internen Endpunkten verknüpft ist .
- Klicken Sie in der Liste auf einen internen Endpunkt, um Geräteeigenschaften anzuzeigen und auf Links zu zugehörigen Informationen wie Erkennungen, Aufzeichnungen oder Paketen zuzugreifen.
- Klicken Sie in der Liste auf die Lupe neben einem Endpunkt, um die mit dem Endpunkt verknüpften Datensätze anzuzeigen.
- Wechseln Sie am Ende der Liste für Cloud-Dienste zwischen Ansichten, die Bytes Out und Bytes In für Ihr Netzwerk anzeigen.
- Passen Sie das Zeitintervall an, um Verbindungen zu bestimmten Zeiten anzuzeigen, z. B. unerwartete Aktivitäten am Abend oder am Wochenende.

Kartenvisualisierung

Die Registerkarte Geolocation bietet eine Weltkarte des Verkehrs zwischen internen Endpunkten und geografischen Standorten, die auf der Karte in einer kontrastierenden Farbe hervorgehoben sind. Die Intensität der kontrastierenden Farbe steht für das Verkehrsaufkommen an dieser Geolokation. Auf der Karte dargestellte Geolokationen werden auch im rechten Bereich aufgeführt.

Klicken Sie auf eine hervorgehobene Geolokalisierung auf der Karte oder der Liste, um die Gesamtmenge des eingehenden oder ausgehender Datenverkehr im Zusammenhang mit verbundenen internen Endpunkten anzuzeigen.

Hier sind einige Möglichkeiten, wie Sie mit den Geolokalisierungsdetails und der Kartenvisualisierung interagieren können:

- Klicken Sie in der Liste auf einen internen Endpunkt, um Geräteeigenschaften anzuzeigen und auf Links zu zugehörigen Informationen wie Erkennungen, Aufzeichnungen oder Paketen zuzugreifen.
- Klicken Sie auf die Lupe neben einem Endpunkt in der Liste, um die mit dem Endpunkt verknüpften Datensätze anzuzeigen.
- Wechseln Sie am Ende der Liste zwischen Ansichten, in denen Bytes Out und Bytes In to your Netzwerk angezeigt werden.
- Klicken Sie auf die Steuerelemente in der unteren rechten Ecke der Karte, um die Karte zu vergrößern und zu verkleinern oder die Karte an die ursprüngliche Position zurückzubringen, oder Sie können das Mausrad drehen.
- Klicken und ziehen Sie mit der Maus auf die Karte oder drücken Sie die Pfeiltasten auf Ihrer Tastatur, um die Kartenansicht neu zu positionieren.
- Passen Sie das Zeitintervall an, um den Verkehr zu bestimmten Zeiten anzuzeigen, z. B. unerwartete Aktivitäten am Abend oder am Wochenende.

Standortauswahl und Bericht über Sicherheitsoperationen

Auf dieser Seite können Sie die Websites angeben, von denen Sie Daten anzeigen möchten. Benutzer mit Zugriff auf das NDR-Modul können einen Security Operations Report erstellen, um die Ergebnisse zu teilen.

Seitenauswahl

Klicken Sie oben auf der Seite auf die Seitenauswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Traffic in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl zeigt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, werden in den Diagrammen und Geräteseiten, die Offlineseiten zugeordnet sind, möglicherweise keine oder nur begrenzte Daten angezeigt. Der Site-Selector ist nur von einem verfügbar Konsole.

(nur NDR-Modul) Sicherheitsbetriebsbericht

Der Security Operations Report enthält eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk. klicken **Bericht generieren** um das Zeitintervall und die Standorte anzugeben, die in den Bericht aufgenommen werden sollen, klicken Sie dann auf **Generieren** um eine PDF-Datei zu erstellen. klicken **Bericht planen** um einen Security Operations Report zu erstellen, der per E-Mail an die Empfänger gesendet wird gemäß die konfigurierte Frequenz.