ExtraHop Glossar

Veröffentlicht: 2024-04-10

AAA

AAA (Authentication, Authorization, and Accounting) ist ein Sicherheitsframework, das Netzwerkzugriffsprotokolle auf Anwendungsebene wie RADIUS, Diameter, TACACS und TACACS+ umfasst.

ActiveMQ

ActiveMQ ist ein Open-Source-Nachrichtenbroker von Apache.

Karten mit Aktivitäten

Eine Aktivitätsdiagramm ist eine dynamische visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Sie können Echtzeitinformationen darüber anzeigen, welche Geräte und Dienste in Ihrem Netzwerk miteinander kommunizieren.

Erweiterte Analyse

Aufzeichnungen, Pakete, Aktivitätskarten, Erkennungen und Diagramme mit L2-L7-Protokollmetriken sind für Geräte verfügbar, die diese Analysestufe erhalten. Priorisieren Sie eine Gruppe oder fügen Sie ein Gerät zur Beobachtungsliste hinzu, um festzulegen, welche Geräte Erweiterte Analyse erhalten sollen.

AJP

AJP (Apache JServ Protocol) wird für die Kommunikation zwischen einem Apache-Webserver und einem Anwendungsserver verwendet.

Warnung

Eine Alarm ist eine benutzerdefinierte Konfiguration von Einstellungen, z. B. einem Zeitintervall, einem Metrikwert und Metrikberechnungen, die für zugewiesene Datenquellen durchgeführt werden. Eine Alarm wird generiert, wenn die konfigurierten Bedingungen erfüllt sind. Benachrichtigungen können über Kanäle wie E-Mail oder SNMP gesendet werden.

AMF

AMF (Action Message Format) ist ein Format zur Kodierung von Daten, die zwischen Adobe Flash-Clients und -Servern übertragen werden.

AppFlow

Das AppFlow-Protokoll wurde von Citrix entwickelt. Dieses Protokoll ist eine Erweiterung des IPFIX-Standards zur Überwachung des Netzwerkverkehrs. Sie können AppFlow-Verkehr mit dem ExtraHop NetFlow-Modul sammeln.

Bewerbung

Im ExtraHop-System sind Anwendungen benutzerdefinierte Container, die Sie mehreren Geräten und Protokollen zuordnen können, um eine einheitliche Ansicht der integrierten Messwerte zu erhalten. Diese Container können verteilte Anwendungen in Ihrer Netzwerkumgebung darstellen. Sie können über die Trigger-API eine Basisanwendung oder eine erweiterte Anwendung erstellen. Die Standardanwendung All Activity ist für alle ExtraHop-Benutzer verfügbar.

Überwachung der Anwendungsleistung

Tools zur Überwachung der Anwendungsleistung (Application Performance Monitoring, APM) ermöglichen es Entwicklungs- und Anwendungsteams, die Leistung von Anwendungen zu beobachten. Daten werden über Softwareagenten gesammelt , die auf Anwendungsservern, Datenbanken und anderen Anwendungskomponenten ausgeführt werden. Die Agenten können so konfiguriert werden, dass sie hostbasierte Eingangs- und Ausgangstransaktionsdaten, Stack-Trace-Eingaben auf Codeebene und Messwerte zur Ressourcennutzung wie CPU, Arbeitsspeicher und Festplatte sammeln.

Besuchen Sie die ExtraHop-Website: So vergleichen Sie APM-Tools..

Flächendiagramm

Dieser ExtraHop-Diagrammtyp zeigt Metrik Werte als Linie an, die Datenpunkte im Laufe der Zeit verbindet, wobei der Bereich zwischen der Linie und der Achse farbig ausgefüllt ist.

Vermögenswert

Ressourcen sind Geräte und Gerätegruppen in Ihrer Umgebung sowie zugehörige Netzwerke, Anwendungen und Benutzer.

Angriffskette

(Nur ExtraHop Reveal (x)) Die meisten Netzwerkangriffe folgen in der Regel bekannten Mustern oder Phasen. Diese Phasen können zu einer Angriffskette zusammengefasst werden, um den Verlauf eines Angriffs zu charakterisieren. ExtraHop Reveal (x) erkennt ungewöhnliches Netzwerkverhalten im Zusammenhang mit verschiedenen Phasen der Angriffskette, darunter Command and Control (C&C), Aufklärung, Exploit, laterale Bewegung und zielgerichtete Aktionen.

Angriffssimulator

Ein Angriffssimulator, auch bekannt als Breach and Attack Simulation (BAS), ist ein Tool , mit dem Analysten eine Bedrohungskampagne erstellen können, die Angriffstechniken emuliert, um die Reichweite von Sicherheitstools zu bewerten. Das ExtraHop-System kann Geräten, auf denen diese Tools ausgeführt werden, automatisch die Rolle des Angriffssimulators zuweisen.

Audit-Protokoll

Das Audit-Log auf dem ExtraHop-System enthält Daten über den Betrieb des Systems, aufgeschlüsselt nach Komponenten. Wenn Sie sich beispielsweise beim ExtraHop-System anmelden, wird das erfolgreiche oder fehlgeschlagene Ereignis als Eintrag im Audit-Log protokolliert.

Balkendiagramm

Dieser ExtraHop-Diagrammtyp zeigt den Gesamtwert der Metrik Daten als horizontale Balken an.

Boxplot-Diagramm

Das Boxplot-Diagramm zeigt die Variabilität für eine Verteilung Metrik Daten. Jeder Boxplot enthält drei oder fünf Datenpunkte. Bei fünf Datenpunkten enthält das Boxplot ein Kästchen, obere und untere Whiskerlinien sowie ein Häkchen. Bei drei Datenpunkten enthält die Linie obere und untere Whiskerlinien sowie ein Häkchen.

Berkeley-Paketfilter (BPF)

Berkeley Packet Filter (BPF) ist ein Programm zum Filtern von Netzwerkpaketen. Die BPF-Syntax ermöglicht es Benutzern, Filter zu schreiben, die schnell nach bestimmten Paketen suchen, um die wichtigsten Informationen zu sehen.

Integrierte Gruppe

Integrierte Gruppen enthalten Geräte, die automatisch anhand ihres Netzwerkprotokollverkehrs gruppiert werden, z. B. CIFS-Clients, oder anhand der dem Gerät zugewiesenen Rolle, z. B. Domänencontroller. Ein Gerät mit mehreren Verkehrsarten kann in mehr als einer integrierte Gruppe vorkommen. Sie können integrierte Gruppen als Metrikquelle für Diagramme, Benachrichtigungen, Auslöser und Aktivitätskarten auswählen.

Bündel

Bundles sind Dokumente im JSON-Format, die Informationen zur ausgewählten Systemkonfiguration enthalten, z. B. Trigger, Dashboards, Anwendungen oder Warnungen. Sie können ein Paket erstellen und diese Konfigurationen dann auf ein anderes ExtraHop-System übertragen oder das Paket als Backup Ihrer Anpassungen speichern.

Bundles können auch von der ExtraHop-Website heruntergeladen werden: ExtraHop Lösungspakete.

Candlestick-Diagramm

Dieser ExtraHop-Diagrammtyp zeigt Datenberechnungen für eine Verteilung von Metrikwerten über die Zeit an. Eine Linie zeigt in jedem Zeitintervall drei oder fünf Datenpunkte an. Wenn die Linie fünf Datenpunkte hat, enthält sie einen Körper, ein mittleres Häkchen, eine obere Schattenlinie und eine untere Schattenlinie. Wenn die Linie drei Datenpunkte hat, enthält sie ein mittleres Häkchen.

CIFS

CIFS (Common Internet File System), auch bekannt als SMB (Server Message Block), ist ein Protokoll auf Anwendungsebene, das Client-Zugriff auf Dateien in einem Netzwerkspeicher ermöglicht (NAS) Repository, normalerweise in einer Windows-Umgebung.

Kunde

Ein Client ist eine Anwendung oder ein System, das auf einen Dienst zugreift, der von einem Server zur Verfügung gestellt wird.

Cluster

Eine Gruppe derselben Art von ExtraHop-Plattenläden, die miteinander verbunden sind.

Säulendiagramm

Dieser ExtraHop-Diagrammtyp zeigt Metrikwerte als vertikale Balken über einen bestimmten Zeitraum an.

Konsole

Eine ExtraHop-Konsole (oder ECA) ist eine Kommandozentrale für die zentrale Verwaltung. Die Konsole bietet eine einheitliche Ansicht der Daten, die von Sensoren, Datensatzspeichern und Paketspeichern gesammelt wurden, die über Rechenzentren, Zweigstellen und die Public Cloud verteilt sind. Früher als Command Appliance bezeichnet.

CORS

Cross-Origin Resource Sharing (CORS) ermöglicht Ihnen den Zugriff auf die ExtraHop REST API über Domaingrenzen hinweg und von bestimmten Webseiten aus, ohne dass die Anfrage über einen Proxyserver übertragen werden muss. Sie können einen oder mehrere zulässige Ursprünge konfigurieren oder den Zugriff auf die ExtraHop REST API von einem beliebigen Ursprung aus zulassen. Nur Administratorbenutzer können CORS-Einstellungen anzeigen und bearbeiten.

Metriktyp zählen

Im ExtraHop-System stellt dieser Metriktyp der obersten Ebene die Anzahl der Ereignisse dar , die in einem bestimmten Zeitraum aufgetreten sind. Sie können die Zählmetriken als Rate oder als Gesamtzahl anzeigen.

Armaturenbrett

Ein Dashboard ist eine anpassbare HTML-Seite, auf der mithilfe von Widgets wie Diagrammen verschiedene Ansichten Ihres Netzwerk angezeigt werden. Zusätzlich zu den benutzerdefinierten Dashboards bietet das ExtraHop-System die folgenden integrierten Dashboards: Aktivitäts-Dashboard, Netzwerk-Dashboard und Sicherheits-Dashboard (nur Reveal (x)).

Datenbank

Relationale Datenbanken speichern, abrufen und verwalten strukturierte Informationen über eine Datenbankmanagementsystem-Sprache (DBMS).

Metriktyp des Datensatzes

Im ExtraHop-System stellt dieser Metriktyp der obersten Ebene eine Verteilung von Daten dar , die in Perzentilwerte berechnet werden können.

Deduplizierung

Das ExtraHop-System entfernt standardmäßig doppelte L2- und L3-Frames und -Pakete, wenn Metriken aus Ihrer Netzwerkaktivität gesammelt und aggregiert werden. Die L2-Deduplizierung entfernt identische Ethernet-Frames (bei denen der Ethernet-Header und das gesamte IP-Paket übereinstimmen müssen). Die L3-Deduplizierung entfernt TCP- oder UDP-Pakete mit identischen IP-ID-Feldern im selben Fluss (wobei nur das IP-Paket übereinstimmen muss).

Metrik im Detail

Detailmetriken bieten Ihnen einen Metrikwert für einen bestimmten Schlüssel, z. B. eine Client-IP-Adresse, eine Server-IP-Adresse, einen URI, einen Hostnamen, einen Referrer, ein Zertifikat oder eine Methode. Wenn Sie von einer Top-Level-Metrik im ExtraHop-System zu einer Detail-Metrik gelangen, können Sie sich einen Überblick darüber verschaffen, wie sich ein bestimmtes Gerät, eine Methode oder eine Ressource auf das Netzwerk auswirkt.

Erkennungen

Erkennungen sind unerwartete Abweichungen von normalen Mustern im Gerät- oder Anwendungsverhalten. Der ExtraHop Machine Learning-Dienst identifiziert Erkennungen anhand von gespeicherten ExtraHop-Systemdaten mithilfe eines proprietären Algorithmus, der Zeitreihenzerlegung, unbeaufsichtigtes Lernen, Heuristik und das einzigartige Fachwissen von ExtraHop kombiniert.

Gerät

Geräte sind Endpunkte in Ihrer Umgebung, die vom ExtraHop-System automatisch erkannt und klassifiziert wurden.

Erkennung von Geräten

Die Geräteerkennung ist der Prozess, bei dem ExtraHop eine Liste der aktiven Geräte erstellt und verwaltet, die mit dem überwachten Netzwerkverkehr verknüpft sind. Das ExtraHop-System kann Geräte anhand ihrer MAC-Adresse (L2 Discovery) oder anhand ihrer IP-Adressen (L3 Discovery) erkennen und verfolgen. Wenn L2 Discovery aktiviert ist, erstellt das ExtraHop-System einen Geräteeintrag für jede lokale MAC-Adresse, die über das Kabel erkannt wurde. IP-Adressen werden der MAC-Adresse zugeordnet, aber Metriken werden zusammen mit der MAC-Adresse des Gerät gespeichert, auch wenn sich die IP-Adresse ändert. Wenn L3 Discovery aktiviert ist, erstellt und verknüpft das ExtraHop-System zwei Einträge für jedes lokal erkannte Gerät: einen übergeordneten L2-Eintrag mit einer MAC-Adresse und einen untergeordneten L3-Eintrag mit IP-Adressen und der MAC-Adresse.

Gerätegruppe

Gerätegruppen, auch als benutzerdefinierte Gruppen bezeichnet, können entweder statisch oder dynamisch sein. Sie müssen einzelne Geräte manuell identifizieren und einer statischen Gruppe zuweisen. Alternativ können Sie Regeln konfigurieren, um Geräte automatisch einer dynamischen Gruppe zuzuweisen.

DHCP

DHCP (Dynamic Host Configuration Protocol) ist ein Protokoll zur dynamischen Verteilung von Netzwerkkonfigurationsparametern.

DICOM

DICOM (Digital Imaging and Communications in Medicine) ist ein Standard für die Speicherung biomedizinischer Bilder und die Übertragung dieser Bilder über ein Netzwerk.

Entdeckungsmodus

Aufzeichnungen, Pakete, Erkennungen und Informationen zur Protokollaktivität sind für Geräte im Entdeckungsmodus verfügbar. Passen Sie die Analyseprioritäten an, um ein Gerät oder einen Endpunkt vom Erkennungsmodus in den Modus Standard oder Erweiterte Analyse zu versetzen.

Eindeutiger Zähler-Metriktyp

Im ExtraHop-System stellt dieser Metriktyp der obersten Ebene die Anzahl der eindeutigen Ereignisse dar, die während eines ausgewählten Zeitintervalls aufgetreten sind. Die Kennzahl für die eindeutige Anzahl bietet eine Schätzung der Anzahl der eindeutigen Elemente, die während des ausgewählten Zeitintervalls in einem Satz platziert wurden. Schätzungen werden mit dem HyperLogLog-Algorithmus berechnet.

DNS

DNS (Domain Name System) ist das Benennungssystem für Netzwerkhosts und Ressourcen, die mit dem Internet verbunden sind. DNS-Server ordnen IP-Adressen Hostnamen zu.

Dynamische Basislinien

Dynamische Basislinien sind Trendlinien auf Dashboards die Ihnen helfen, zwischen normaler und abnormaler Aktivität zu unterscheiden. Das ExtraHop-System berechnet dynamische Basislinien auf der Grundlage historischer Daten. Um Datenpunkte auf einer Dynamische Basislinie zu generieren, berechnet das ExtraHop-System den Medianwert für einen bestimmten Zeitraum.

Endpunkt

Endpunkte sind interne oder externe Hostnamen und IP-Adressen, die vom ExtraHop-System beobachtet werden. Interne Endpunkte befinden sich in Ihrem lokalen oder Remote-Netzwerk, und externe Endpunkte befinden sich außerhalb Ihres lokalen oder Remote-Netzwerks.

ERSPAN

Encapsulated Remote SPAN (ERSPAN) ermöglicht es Ihnen, Quelldatenverkehr auf einem Switch an ein Ziel auf einem anderen Switch zu senden und dabei eine Layer-3-Grenze zu überschreiten.

Ereignis

Ein Ereignis steht für Aktivitäten, die in Ihrem Netzwerk oder in Ihrem ExtraHop-System erkannt wurden. Trigger können geschrieben werden, um die mit einem Ereignis verknüpften Daten zu sammeln und benutzerdefinierte Metriken zu erstellen.

Fingerabdruck

Ein Fingerabdruck ist eine eindeutige, alphanumerische Kennung, die allen Sensoren, Plattenspeichern und Paketspeichern zugewiesen wird.

FIX

FIX (Financial Information eXchange) ist ein Protokoll, das Informationen über den Austausch von Finanztransaktionen in Echtzeit bereitstellt.

Durchfluss

Ein Fluss ist ein Satz von Paketen, die Teil einer einzelnen Transaktion zwischen zwei Endpunkten sind. Ähnlich wie das ExtraHop-System Datenflüsse anhand von wire data identifizieren kann, können Datenflüsse aus Maschinendaten in entfernten Netzwerken zur Analyse an das ExtraHop-System gesendet werden.

Flow-Schnittstelle

Eine Flussschnittstelle ist eine lokale Gruppierung von Verkehr oder Geräten in einem Flussnetz. Anstatt die Flussinformationen für das gesamte Netzwerk zu betrachten, können Sie sich die Flussinformationen für eine bestimmte Schnittstelle im Netzwerk ansehen.

Flow-Netzwerk

Ein Flussnetz sendet Informationen über Flüsse, die auf dem Gerät gesehen werden. Ähnlich wie das ExtraHop-System Datenflüsse anhand von wire data identifizieren kann, kann das ExtraHop-System Flussinformationen von entfernten Netzwerkgeräten, auch Flow-Exportern genannt, empfangen.

Durchflusssensor

(Nur ExtraHop Reveal (x) 360) Ein ExtraHop Flusssensor (EFC) sammelt Daten aus Flow-Logs statt aus Paketen. Sensoren bieten die Möglichkeit, all Ihre Netzwerk-, Anwendung-, Client-, Infrastruktur- und Geschäftsdaten zu analysieren und zu visualisieren. Sensoren können an eine ExtraHop-Konsole angeschlossen werden, um eine zentrale Verwaltung und eine einheitliche Ansicht der gesammelten und gespeicherten Daten zu ermöglichen. Sie können auch mit Schallplatten- und Paketspeichern verbunden werden, um zusätzlichen Speicherplatz und tiefere Analysen zu ermöglichen.

Flow Stall

Ein Flow Stall ist eine TCP-Metrik im ExtraHop-System, die Netzwerküberlastung misst. Ein Flow-Stall wird gezählt, wenn bei einem einzelnen Datenfluss zwischen Geräten drei aufeinanderfolgende Retransmission Timeouts (RTOs) beobachtet werden. Ein RTO steht für eine Verzögerung von 1-5 Sekunden, da ein Gerät darauf wartet, Daten erneut zu senden, die möglicherweise aufgrund einer überlasteten Verbindung verloren gegangen sind.

FTP

FTP (File Transfer Protokoll) ist ein Standard-Netzwerkprotokoll für die Übertragung von Dateien zwischen einem Client und einem Server.

Gut gemacht

Goodput bezieht sich auf die Menge nützlicher Daten, die pro Zeiteinheit über die L4-Anwendungsschicht übertragen werden. In diesem Zusammenhang bedeutet nützlich, dass Neuübertragungen zusammen mit dem Protokoll-Overhead oder anderen anwendungsfremden Daten, die auf der Leitung gefunden wurden, als doppelte Pakete verworfen werden. Goodput ist immer niedriger als der Durchsatz und entspricht in etwa der Größe der Nutzdaten-Bytes für jedes Protokoll, das über TCP läuft (z. B. eine CIFS-Datei oder eine HTTP-Anfrage), während der Übertragungszeit.

Heatmap-Diagramm

Dieser ExtraHop-Diagrammtyp zeigt eine Verteilung der Metrik Daten über die Zeit, wobei die Farbe eine Datenkonzentration darstellt.

Hoher Wert

Ein hoher Wert ist eine Bezeichnung für Geräte in Ihrem Netzwerk, die Sie oder das ExtraHop-System als wichtig für Ihre Geschäftsanwendungen, Workflows oder Infrastruktur erachten könnten. Ein Gerät gilt als hoher Wert, wenn das ExtraHop-System beobachtet, dass das Gerät Authentifizierung oder wichtige Dienste bereitstellt, oder wenn ein Benutzer manuell ein Gerät mit hoher Wert angibt.

Histogramm-Diagramm

Dieser ExtraHop-Diagrammtyp zeigt eine Verteilung von Metrik Daten als vertikale Balken oder Abschnitte an.

HL7

HL7 (Health Level-7) ist ein Standard für den Austausch von elektronischen Gesundheitsinformationen zwischen Softwareanwendungen.

HTTP

HTTP (Hypertext Transfer Protocol) ist ein Protokoll auf Anwendungsebene, das Webseiten abruft.

IBM MQ

IBM MQ ist ein Message-Queuing-Protokoll für IBM Enterprise- und Message-Middleware-Produkte.

ICA

ICA (Independent Computing Architecture) ist ein Citrix-Systemprotokoll, das Daten zwischen Clients und Servern überträgt.

ICMP

ICMP (Internet Control Message Protocol) ist ein Protokoll, über das Netzwerkgeräte Fehler - und Abfragemeldungen senden.

Einbruchmeldesystem (Intrusion Detection System)

Intrusion Detection Systems (Intrusion Detection System) basieren auf einer Reihe von Regeln, die Signaturen für unsichere oder böswillige Netzwerkaktivitäten enthalten. Durch die Kopplung eines ExtraHop IDS-Sensors mit einem ExtraHop-Paketsensor kann das ExtraHop-System böswillige oder unsichere Aktivitäten anhand herkömmlicher IDS-Signaturen identifizieren.

Untersuchung

Eine Untersuchung ist eine benutzerverwaltete Gruppierung von Erkennungen, die es Benutzern ermöglicht, mehrere Erkennungen in einer einzigen Zeitleiste und Karte anzuzeigen. Mithilfe von Untersuchungen kann festgestellt werden, ob verdächtiges Verhalten eine legitime Bedrohung darstellt und ob eine Bedrohung Teil einer größeren Angriffskampagne ist.

iDRAC

Der Integrated Dell Remote Access Controller (iDRAC) ermöglicht den Fernzugriff auf das ExtraHop-System. Nachdem Sie iDRAC aktiviert und konfiguriert haben, können Sie das System aus- und wieder einschalten, Konsolenmeldungen anzeigen und Hardwareüberwachungs- und Startprotokolle überprüfen.

iSCSI

iSCSI (Internet Small Computer Systems Interface) ist ein Protokoll auf TCP-Ebene, mit dem SCSI-Befehle über ein lokales Netzwerk (LAN) oder ein Weitverkehrsnetzwerk (WAN) gesendet werden können.

Kerberos

Kerberos ist ein Sicherheitsprotokoll, das geheime Schlüsselkryptografie auf die Client- und Serverauthentifizierung anwendet.

L2

Die Datenverbindungsschicht im OSI-Modell. Im ExtraHop-System liefern L2-Metriken Informationen über die Verbindung zwischen zwei Geräten.

L3

Die Netzwerkschicht im OSI-Modell. Im ExtraHop-System stellen L3-Metriken IP-Adressinformationen für Knoten bereit, die über das überwachte Netzwerk kommunizieren.

L4 (TCP)

Die Transportschicht im OSI-Modell. Im ExtraHop-System liefern L4-TCP-Metriken (TCP) Informationen über die zuverlässige Übertragung von Paketen zwischen einer Quelle und einem Ziel.

L7

Die Anwendungsschicht im OSI-Modell. Im ExtraHop-System liefern L7-Metriken Informationen über die Interaktivität mit Softwareanwendungen.

LDAP

LDAP (Lightweight Directory Access Protocol) ist ein herstellerneutrales Protokoll, das ein verteiltes Verzeichnis verwaltet und einen einfachen Zugriff darauf ermöglicht.

Lesen Sie den ExtraHop-Blogbeitrag: Was ist LDAP und wer braucht es überhaupt?

Durch Level ausgelöste Warnmeldungen

Eine vom Alarmschwelle wird in bestimmten Intervallen generiert, solange der Metrikwert über dem konfigurierten Schwellenwert bleibt.

Liniendiagramm

Dieser ExtraHop-Diagrammtyp zeigt Metrikwerte als Linie an, die eine Reihe von Datenpunkten im Laufe der Zeit verbindet.

Linien- und Säulendiagramm

Dieser ExtraHop-Diagrammtyp zeigt Metrikwerte als Linie an, die Datenpunkte im Laufe der Zeit verbindet, mit der Option, eine weitere Metrik als Säulendiagramm darunter anzuzeigen.

Diagramm auflisten

Dieses ExtraHop-Diagramm zeigt Metrikwerte in einer Liste über mehrere Spalten mit optionalen Sparklines an.

LLDP

Das Link Layer Discovery Protocol (LLDP) ist ein Protokoll, über das Netzwerkgeräte ihre Identität und Fähigkeiten kommunizieren.

LLMNR

LLMNR (Link-Local Multicast Name Resolution) ist ein Protokoll, das in Microsoft Windows-Systemen enthalten ist. Dieses Protokoll basiert auf dem DNS-Format (Domain Name System) und ermöglicht die Namensauflösung für Hosts auf demselben lokalen Link, wenn die DNS-Namensauflösung fehlschlägt.

Maximaler Metrik Typ

Im ExtraHop-System ist dieser Metriktyp der obersten Ebene ein einzelner Datenpunkt, der den Maximalwert aus einem bestimmten Zeitraum darstellt.

Memcache

Memcache ist ein Protokoll, das den Zugriff auf leistungsstarke, verteilte Speicherobjekt-Caching-Systeme über eine TCP-Verbindung ermöglicht.

Metrisch

Im ExtraHop-System ist eine Metrik eine Messung des beobachteten Netzwerkverhaltens. Metriken werden aus dem Netzwerkverkehr generiert, und dann wird jede Metrik einer Quelle zugeordnet. Das ExtraHop-System bietet integrierte oder standardmäßige Messwerte, die auf dem beobachteten Netzwerkverkehr anhand von wire data basieren. Sie können auch benutzerdefinierte Metriken im ExtraHop-System erstellen, indem Sie einen Auslöser schreiben, um Metriken auf der Grundlage eines bestimmten Ereignis zu sammeln.

Metrischer Katalog

Der Metric Catalog ist ein Tool zum Anzeigen von Informationen über integrierte und benutzerdefinierte Metriken im ExtraHop-System. Sie können benutzerdefinierte Metriken auch über den Metrikkatalog löschen und bearbeiten.

Metric Explorer

Der Metric Explorer ist ein Tool zur Konfiguration von Dashboard-Diagrammen. Im Metrik Explorer können Sie mehrere Quellen und Metriken zu einem Diagramm hinzufügen und sofort eine Vorschau anzeigen, wie Metrikdaten angezeigt werden.

Modbus

Modbus ist ein serielles Kommunikationsprotokoll, das in der industriellen Automatisierung verwendet wird.

MongoDB

MongoDB ist eine Open-Source-Dokumentendatenbank, die Leistung, Verfügbarkeit und Skalierbarkeit bietet.

Modul

Module bieten eine Reihe von Produktfunktionen durch eine Kombination aus Lösungen, Komponenten und Cloud-basierten Diensten. Module sind für Network Detection and Response (NDR) und Network Performance Monitoring (NPM) erhältlich, mit zusätzlichen Modulen für Intrusion Detection Systems (Intrusion Detection System) und Packet Forensics. Administratoren können Benutzern rollenbasierten Zugriff auf das NDR-Modul, das NPM-Modul oder beide gewähren.

MSMQ

MSMQ (Microsoft Message Queuing) ist ein Protokoll, das es Anwendungen ermöglicht, Nachrichten und Objekte aneinander zu senden.

NaN

Abkürzung für keine Zahl. In der Trigger-API wird eine Eigenschaft mit einem numerischen Datentyp angezeigt `NaN` wenn der Eigenschaftswert undefiniert ist oder nicht als Zahl dargestellt werden kann.

NAS

NAS (Network Attached Storage) ist ein Speicher-Repository auf Dateiebene. Clients können über die Protokolle SMB (Server Message Block) oder NFS (Network File System) auf das Repository zugreifen.

NBNS

NBNS oder NBT-NS (NetBIOS Name Service) ist ein Benennungssystem für Netzwerkhosts und Ressourcen.

NetFlow

Flow-Technologien wie Netflow, IPFIX, sFlow und AppFlow sammeln Verkehrsdaten von Flussnetzwerken außerhalb Ihres Kabeldatenfeeds und senden die Daten zur Analyse an den Sensor.

Netzwerk

Im ExtraHop-System ist ein Netzwerk der Einstiegspunkt in die Netzwerkerfassung, und es werden Metriken für Netzwerkerfassungsattribute, Netzwerkwarnungen und Netzwerkverkehrsdetails gesammelt. Diese Metriken bieten eine Zusammenfassung aller Netzwerkaktivitäten, die bei der Erfassung abgerufen wurden.

Netzwerk-Bytes

Ein Netzwerkbyte ist eine Metrik, die die Durchsatzrate des ExtraHop-Capture-Prozesses anzeigt.

Indikatoren für den Netzwerkstatus

(Nur ExtraHop Reveal (x)) Netzwerkintegritätsindikatoren sind eine Reihe von Kennzahlen, die Ihnen allgemeine Trends in Bezug auf den Netzwerk- und Sicherheitsstatus aufzeigen. Netzwerkintegritätsindikatoren können auf Schwächen oder Probleme bei der Netzwerkleistung oder auf potenziell verdächtige Aktivitäten hinweisen. Diese Metriken finden Sie unten auf der Netzwerkübersichtsseite.

NFS

NFS (Network File System) ist ein verteiltes Dateisystemprotokoll, das Client-Zugriff auf Dateien in einem Netzwerk Attached Storage (NAS) -Repository ermöglicht, typischerweise in einer UNIX-Umgebung.

Knoten

Ein einzelner ExtraHop-Recordstore innerhalb eines Cluster.

Datenstrom öffnen

Mit dem Open Data Stream (ODS) -Dienst können Sie wire data an ein externes Drittanbietersystem wie MongoDB oder Kafka senden. Sie müssen einen Auslöser schreiben, um die Daten, die Sie exportieren möchten, zu identifizieren und zu sammeln und Einstellungen über die ExtraHop-Administrationseinstellungen zu konfigurieren.

Paketsensor

Ein Paketsensor sammelt passiv eine Kopie der unstrukturierten Kabeldaten — also aller Transaktionen in Ihrem Netzwerk — und wandelt diese Daten in strukturierte wire data um. Sensoren bieten die Möglichkeit, all Ihre Netzwerk-, Anwendung-, Client-, Infrastruktur- und Geschäftsdaten zu analysieren und zu visualisieren. Sensoren können an eine ExtraHop-Konsole angeschlossen werden, um eine zentrale Verwaltung und eine einheitliche Ansicht der gesammelten und gespeicherten Daten zu ermöglichen. Sie können auch mit Schallplatten- und Paketspeichern verbunden werden, um zusätzlichen Speicherplatz und tiefere Analysen zu ermöglichen.

Pakete

Mit der Paketfunktion können Sie über einen Sensor oder eine Konsole nach Paketen für ausgewählte Transaktionen suchen und diese herunterladen. Für diese Funktion ist ein unterstützter Packetstore erforderlich.

Paketshop

Ein ExtraHop-Paketspeicher sammelt rohe Netzwerkpakete, die von einem angeschlossenen Paketsensor gesendet werden, um sie langfristig abzurufen und zu speichern. Mit Packetstores können Sie innerhalb eines bestimmten Zeitintervalls schnell alle Pakete abrufen, die einer Reihe von Suchkriterien entsprechen.

Teilnehmer

Teilnehmer sind Endpunkte, die als Täter oder Opfer an einer Erkennung teilnehmen.

Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy (PFS) ist eine Verschlüsselungsmethode, die einen kurzfristigen, vollständig privaten Schlüsselaustausch zwischen Clients und Servern ermöglicht. Sie können das ExtraHop-System für die Entschlüsselung von PFS-SSL/TLS-Sitzungen von Windows-Servern lizenzieren, auf denen die ExtraHop PFS-Agent-Software installiert ist. Ohne PFS könnten diese Sitzungen nicht entschlüsselt werden, und die Daten aus diesen Austauschen wären verdeckt.

PCAP

PCAP (Packet Capture) besteht aus einer Anwendungsprogrammierschnittstelle (API) zur Erfassung des Netzwerkverkehrs und dessen Speicherung in einer Datenbank.

PCoIP

PCoIP (PC-over-IP) ist ein Protokoll, das komprimierte und verschlüsselte Bildpixel von einem zentralen Server auf ein PCoIP-Gerät überträgt.

Kreisdiagramm

Dieses ExtraHop-Diagramm zeigt Metrik Daten als Teil oder Prozentsatz eines Ganzen an.

POP3

POP3 (Post Office Protokoll) ist ein Standardprotokoll auf Anwendungsebene , das E-Mail-Nachrichten zwischen einem Server und einer Client-Anwendung über eine TCP-Verbindung überträgt.

Port-Spiegelung

Port-Mirroring tritt auf, wenn ein Netzwerk-Switch eine Kopie von Netzwerkpaketen von einem Switch-Port (oder einem gesamten VLAN) an eine Netzwerküberwachungsverbindung an einem anderen Switch-Port sendet.

Protokoll

Ein Protokoll definiert das Format und die Reihenfolge von Nachrichten, die zwischen zwei oder mehr Geräten ausgetauscht werden, sowie die Aktionen, die beim Senden und Empfangen einer Nachricht oder eines anderen Ereignis ergriffen werden.

Protokollseite

Eine Protokollseite ist eine integrierte Seite, die integrierte Diagramme mit wichtigen Kennzahlen zu Ihren Vermögenswerten enthält. Diese Metrikdiagramme können in Ihre Dashboards kopiert werden.

RDP

RDP (Remote Desktop Protokoll) ist ein proprietäres Microsoft-Protokoll für die Kommunikation zwischen einem Remote Desktop Session Host-Server und einem Client, auf dem die Remote Desktop Connections-Software ausgeführt wird. RDP ist in TCP gekapselt und verschlüsselt.

Rekord

Datensätze sind strukturierte Fluss- und Transaktionsinformationen über Ereignisse in Ihrem Netzwerk , die zur Speicherung an einen unterstützten Recordstore gesendet werden können. Anschließend können Sie Datensätze von einem Sensor oder einer Konsole abfragen.

Format des Datensatzes

Ein Datensatzformat ist ein Schema beim Lesen, das bestimmt, wie jeder Datensatz im ExtraHop-System angezeigt wird. Das ExtraHop-System verfügt über integrierte Datensatzformate für alle integrierten Datensatztypen, und obwohl Sie ein integriertes Datensatzformat nicht ändern können, können Sie ein benutzerdefiniertes Datensatzformat erstellen.

Arten von Datensätzen

Datensatztypen verknüpfen gespeicherte Datensätze mit dem Datensatzformat im ExtraHop-System. Erfordert einen unterstützten Recordstore.

Plattenladen

Ein Recordstore sammelt Transaktions- und Flussdatensätze, die von einem angeschlossenen Sensor gesendet werden, um sie langfristig zu speichern und abzurufen. Sie können die strukturierten Fluss- und Transaktionsinformationen zu Ereignissen in Ihrem Netzwerk mit einer einfachen, einheitlichen Benutzeroberfläche anzeigen, speichern und durchsuchen, ohne Änderungen an Ihren vorhandenen Anwendungen oder Ihrer Infrastruktur vornehmen zu müssen. ExtraHop Recordstores sind als physische oder virtuelle Bereitstellungen verfügbar; der ExtraHop Cloud Recordstore wird für Reveal (x) 360 bereitgestellt, und zu den unterstützten Data Warehouses von Drittanbietern gehören BigQuery und Splunk.

Redis

Redis ist ein Open-Source-Datenstrukturserver.

Region

Eine Region ist ein Dashboard Komponente, die Widgets enthält.

Timeout für die erneute Übertragung (RTO)

Ein Retransmission Timeout (RTO) ist eine TCP-Protokollmetrik zur Bestimmung der Netzwerkleistung. TCP-Neuübertragungen finden im Netzwerk häufig statt. TCP startet einen Timer für die erneute Übertragung, wenn ein ausgehendes Segment an eine IP-Adresse weitergegeben wird. Wenn vor Ablauf des Timers keine Bestätigung (ACK) erfolgt, wird das Segment erneut übertragen. Ein RTO tritt auf, wenn der Absender anfängt, zu viele Bestätigungen zu verpassen und das Senden von Segmenten für einen bestimmten Zeitraum unterbricht. RTOs können eine Verzögerung von 1-5 Sekunden in Ihrem Netzwerk bedeuten. Mehrere RTOs im Laufe der Zeit können zu erheblichen Verzögerungen in Ihrem Netzwerk führen.

Lesen Sie den ExtraHop-Blogbeitrag: TCP-RTOs: Zeitüberschreitungen bei der erneuten Übertragung und Leistungseinbußen bei Anwendungen.

Enthüllen (x) 360

Reveal (x) 360 bietet SaaS-basierte Transparenz und Verwaltung für lokale und cloudbasierte verbundene Umgebungen. Die Reveal (x) 360-Konsole bietet eine zentrale Ansicht der Daten, die von mehreren Sensoren, Packetstores und Recordstores gesammelt wurden und über Rechenzentren, Zweigstellen und die Public Cloud verteilt werden können.

Enthülle (x) Enterprise

Reveal (x) Enterprise ist ein abonnementbasiertes Angebot von ExtraHop-Produkten, die je nach Tariftyp einen Sensor zur Erfassung von wire data und zusätzliche Komponenten enthalten.

RFB

RFB (Remote Framebuffer) ist ein Protokoll für den Fernzugriff auf eine grafische Benutzeroberfläche, das es einem Client ermöglicht, ein System auf einem anderen Computer anzusehen und zu steuern.

Risikobewertung

(Nur ExtraHop Reveal (x)) Eine Risikoscore ist ein numerischer Indikator für den Schweregrad einer Erkennung. Risikobewertungen basieren auf verschiedenen Faktoren, z. B. der Position der Erkennung in der Angriffskette, der Schwachstelle des Erkennungsprotokolls und dem Ausmaß der Auswirkungen, die die Erkennung auf das Netzwerk haben könnte. Die Bewertung erfolgt auf einer Skala von 1 bis 99, wobei 99 am schwerwiegendsten ist.

RPC

MRPC (Microsoft Remote Procedure Call) ist ein Kommunikationsmechanismus, mit dem Clients eine Prozedur von einem Programm aufrufen können, das sich auf einem anderen Computer, Server oder Netzwerk befindet.

PCAP aus der Ferne (RPCAP)

Remote PCAP (RPCAP) ist eine Softwareimplementierung für die Paketweiterleitung, die einem physischen Tap ähnelt. Wenn Sie den Netzwerkverkehr für Geräte überwachen möchten, die nicht direkt mit Ihrem Kabeldatenfeed verbunden sind, können Sie Pakete über die Cloud weiterleiten und diese Daten über das ExtraHop-System analysieren.

RSPAN

Der Remote Switched Port Analyzer (RSPAN) ermöglicht die Fernüberwachung mehrerer Switches in einem Switching-Netzwerk. RSPAN ist eine Möglichkeit, Traffic von einer SPAN-Quelle auf einem Switch zu einem SPAN-Ziel auf einem anderen Switch zu leiten, der über einen Trunk verbunden ist.

Hinweis: RSPAN erfordert , dass sich das Quelle- und das Zielchassis in derselben Layer-2-Domäne befinden.

RTCP

RTCP (Real-Time Transport Control Protocol) ist ein Protokoll, das Statistiken für Streaming-Audio- und Videodaten überwacht, die über das RTP-Protokoll übertragen werden.

RTP

RTP (Real-time Transport) ist ein Protokoll, das das standardisierte Paketformat für die Echtzeitübertragung von Streaming-Audio und Video definiert.

Debug-Protokoll

Das Debug-Log ist eine Komponente des Trigger-Editors im ExtraHop-System. Das Debug-Protokoll zeigt Ausnahmen und Ausgaben von Debug-Anweisungen in Triggerskripten an.

Metrik Typ des Probensatzes

Im ExtraHop-System stellt dieser Metriktyp der obersten Ebene eine Zusammenfassung von Daten dar, die einen Mittelwert (Durchschnitt) und eine Standardabweichung über einen bestimmten Zeitraum liefert. Stichprobenmetriken fassen in der Regel Daten zu einer Detail-Metrik zusammen.

SDP

Das Session Description Protocol (SDP) ist ein Protokoll, das Multimedia-Streaming-Sitzungen definiert.

Fühler

Ein ExtraHop-Sensor bietet die Möglichkeit, all Ihre Netzwerk-, Anwendung-, Client-, Infrastruktur- und Geschäftsdaten zu analysieren und zu visualisieren. Ein Paketsensor (oder EDA) sammelt passiv eine Kopie unstrukturierter Kabeldaten — also aller Transaktionen in Ihrem Netzwerk — und wandelt diese Daten in strukturierte wire data um. Ein Flusssensor (oder EFC) sammelt Daten aus Flussprotokollen und wird nur auf ExtraHop Reveal (x) 360 unterstützt. Sensoren können an eine ExtraHop-Konsole angeschlossen werden, um eine zentrale Verwaltung und eine einheitliche Ansicht der gesammelten und gespeicherten Daten zu ermöglichen. Sie können auch mit Schallplatten- und Paketspeichern verbunden werden, um zusätzlichen Speicherplatz und tiefere Analysen zu ermöglichen.

Server

Ein Server ist ein Hardwaresystem, das dazu dient, einen oder mehrere Dienste für Benutzer oder Clients im Netzwerk zu hosten. Im Kontext von Internet Protocol (IP) -Netzwerken ist ein Server ein Programm, das als Socket-Listener fungiert.

SIP

SIP (Session Initiation Protokoll) ist ein Signalisierungsprotokoll, das Kommunikationssitzungen wie Sprachanrufe für IP-basierte Telefonieanwendungen steuert.

Seite

Ein Standort ist ein wire data Datenfeed, der vom ExtraHop-System analysiert wird und einen physischen oder logischen Bereich Ihres Netzwerk darstellt, z. B. ein Rechenzentrum, eine Zweigstelle oder eine Cloud-Workload. Sie können Ressourcen, Erkennungen und andere Daten von einem bestimmten Standort oder von mehreren Standorten aus anzeigen.

SMPP

SMPP (Short Messaging Peer-to-Peer) ist ein Protokoll auf Anwendungsebene, das SMS-Daten (Short Message Service) zwischen External Short Messaging Entities (ESME) und Short Message Service Centers (SMSC) überträgt.

SMTP

SMTP (Simple Mail Transfer Protokoll) ist ein Standardprotokoll, das E-Mail-Nachrichten zwischen Servern, E-Mail-Übertragungsagenten und Client-Anwendungen sendet, empfängt und weiterleitet.

Snapshot-Metriktyp

Im ExtraHop-System stellt dieser Metriktyp der obersten Ebene einen Datenpunkt dar, der einen einzelnen Zeitpunkt darstellt. Zu den Snapshot-Metriken gehören Verhältnisse, aktuelle Verbindungen und etablierte TCP-Verbindungen.

SNMP

Das Simple Network Management Protokoll (SNMP) ist ein Layer-7-Protokoll zum Sammeln, Organisieren, Austauschen und Ändern von Informationen über verwaltete Geräte in IP-Netzwerken.

Quelle

Quellen sind Ressourcen, die Diagrammen, Triggern und Alerts zugewiesen werden können, um Zugriff auf Metriksammlungen zu gewähren.

SPAN

Die Portspiegelung auf einem Cisco Systems Switch wird allgemein als Switched Port Analyzer (SPAN) bezeichnet. SPAN kopiert den Datenverkehr und sendet ihn zur Netzwerkanalyse an ein Ziel.

SSH

Secure Shell (SSH) ist ein Protokoll, das Informationen sicher über ein Netzwerk überträgt.

SSL

SSL (Secure Sockets Layer) ist ein Standardprotokoll zur Sicherung der Kommunikation über das Internet. Um eine verschlüsselte Verbindung zwischen einem Webbrowser und einem Server herzustellen, muss der Server über ein SSL-Zertifikat verfügen.

Standardanalyse

Aufzeichnungen, Pakete, Erkennungen, Aktivitätskarten, Protokollaktivitäten und Diagramme mit Durchsatz- und Paketmetriken sind für Geräte verfügbar, die Standardanalyse empfangen. Passen Sie die Analyseprioritäten an, um ein Gerät oder einen Endpunkt von der Standardanalyse zur erweiterten Analyse hochzustufen.

Status-Diagramm

Dieser ExtraHop-Diagrammtyp zeigt Metrikwerte in einem Säulendiagramm an, wobei die Farbe der Spalten den Status und den Schweregrad einer Alarm darstellt, die der Quelle und der im Diagramm ausgewählten Metrik zugewiesen ist.

STIX

(Nur ExtraHop Reveal (x)) Structured Threat Information eXpression (STIX) ist die Sprache und das Serialisierungsformat für die Standardisierung, Übertragung und den Austausch von Daten über Cyber-Bedrohungsdaten. Das STIX-Format wird häufig von der Bedrohungsinformationen Community und den Plattformen unterstützt. Sie können STIX-Dateien über das ExtraHop-System oder die REST-API als benutzerdefinierte Bedrohungssammlung hochladen. Benutzerdefinierte Bedrohungssammlungen müssen in STIX als komprimierte TAR-Dateien wie .TGZ oder TAR.GZ formatiert werden.

Tabellen-Diagramm

Dieser ExtraHop-Diagrammtyp zeigt Metrikwerte in Zeilen und Spalten in einer Tabelle an.

TAXII

TAXII (Trusted Automated Exchange of Intelligence Information) ist ein Protokoll für den Versand von Bedrohungsinformationen über HTTPS.

TCP

Im ExtraHop-System liefern TCP-Metriken (TCP) Informationen über die zuverlässige Übertragung von Paketen zwischen einer Quelle und einem Ziel. Mithilfe von TCP-Metriken bietet ExtraHop einen Überblick darüber, welche Geräte miteinander verbunden sind, wann Geräte Daten senden, ob es Fehler in den Daten gibt, über welche Protokolle kommuniziert wird usw.

TCP RST

Ein TCP-RST-Paket wird gesendet, um zu verhindern, dass eine TCP-Verbindung hergestellt wird, oder um eine bestehende Verbindung gewaltsam zu beenden. Manchmal werden Resets gesendet, wenn das empfangende Gerät das SYN-Paket nicht als ACK bestätigen konnte oder wenn es ein anderes Paket nicht bestätigt hat, das zu einem späteren Zeitpunkt in der Transaktion gesendet und erneut übertragen wurde. In einigen Fällen weist TRCP RSTs darauf hin, dass ein Fehler aufgetreten ist. Große Mengen an ausgehenden Resets sollten untersucht werden, um festzustellen, ob es sich um ein erwartetes Verhalten handelt oder ob sie auf ein größeres Problem hinweisen.

Telnet

Telnet ist ein Protokoll auf Anwendungsebene für interaktive textorientierte Kommunikation über eine virtuelle Terminalverbindung.

Bedrohungsinformation

(nur ExtraHop Reveal (x)) Threat Briefings bieten Hinweise zu potenziellen Bedrohungen für Ihr Netzwerk, die sich sowohl aus branchenweiten Sicherheitsereignissen als auch aus maschinellen Lernanalysen Ihres Netzwerk ergeben. Bedrohungsinformationen können die Erkennung von Scans, Exploits und Indicators of Compromise (Kompromittierungsindikatoren) beinhalten, die mit der Bedrohung in Zusammenhang stehen.

Erfassung von Bedrohungen

(Nur ExtraHop Reveal (x)) Eine Bedrohungssammlung ist ein Datensatz mit verdächtigen IP-Adressen, Hostnamen und URIs, der es Ihrem Reveal (x) -System ermöglicht, Indikatoren für eine Gefährdung zu identifizieren und Bedrohungsinformationen in Systemdiagrammen und Aufzeichnungen anzuzeigen.

Bedrohungsinformationen

Bedrohungsinformationen sind bekannte Daten über verdächtige IP-Adressen, Hostnamen und URIs, anhand derer Risiken für Ihr Unternehmen identifiziert werden können. Diese Datensätze, die als Bedrohungssammlungen bezeichnet werden, sind standardmäßig in Ihrem Reveal (x) -System und in der Sicherheits-Community aus kostenlosen und kommerziellen Quellen verfügbar.

Zeitselektor

Der Zeitselektor ist ein Tool, mit dem Sie ein Zeitintervall für die Erfassung und Präsentation von Netzwerkdaten im ExtraHop-System angeben können. Es gibt zwei Arten von Zeitselektoren: einen Global Zeitselektor zur Angabe globaler Zeitintervalle und einen Region Zeitselektor zur Angabe von Regionszeitintervallen in einem Dashboard.

Zeitstempel

Ein Zeitstempel ist eine digitale Datensatz der Zeit, zu der ein bestimmtes Ereignis eingetreten ist. Im ExtraHop-System können Sie den Standardzeitstempel auswählen oder externe Zeitstempel wie Gigamon oder Anue über die laufende Konfigurationsdatei konfigurieren.

Tinygramm

Ein Tinygram ist ein kleines Paket oder ein TCP-Segment. Ein Tinygram ist ein Paket, bei dem die Nutzlast kleiner ist als die Frame-Header-Daten (L2-L4). Im Allgemeinen führen Tinygramme zu ineffizienten Verhältnissen zwischen Frame-Header-Daten und tatsächlich nutzbaren Informationen, die über das Netzwerk übertragen werden. Tinygramme können zur Netzwerküberlastung beitragen.

Lesen Sie den ExtraHop-Blogbeitrag: Was ist ein Tinygram?

Metrik auf oberster Ebene

Eine Metrik der obersten Ebene oder Basismetrik gibt Ihnen eine Summe von Daten für einen bestimmten Zeitraum. Top-Level-Metriken bieten Ihnen einen Gesamtwert, anhand dessen Sie erkennen können, was in Ihrem Netzwerk passiert. Anschließend können Sie eine detaillierte Analyse einer Metrik auf oberster Ebene durchführen, um detaillierte Kennzahlen anzuzeigen. Es gibt verschiedene Arten von Top-Level-Metriken, die unterschiedliche Informationen liefern, darunter die Metriktypen Anzahl, Datensatz, Maximum, Sampleset und Snapshot. Das Verständnis der Metriktypen ist für das Schreiben von Triggern und das Konfigurieren von Diagrammen unerlässlich.

Oberster Satz

Ein Topnset sind die 1.000 wichtigsten Schlüssel-Wert-Paare, die für das Zeitintervall berechnet wurden, das Sie in der Zeitselektor angeben. Ein Topnset ist kein vollständiger Datensatz, da ein Topnset nur die Schlüsselwerte darstellt, die für einen bestimmten Aggregations-Rollup (basierend auf einem bestimmten Zeitintervall) aufgezeichnet wurden, und auf bis zu 1.000 Schlüssel pro Topnset begrenzt ist.

Auslöser

Trigger sind benutzerdefinierte Skripten, die bei einem vordefinierten Ereignis eine Aktion ausführen. Sie können beispielsweise einen Auslöser schreiben, um bei jeder HTTP-Anforderung eine benutzerdefinierte Metrik Datensatz oder um den Datenverkehr für einen bestimmten Server als Anwendungsserver zu klassifizieren.

Weitere Informationen finden Sie in der Trigger-API-Referenz.

Tuning

Der Vorgang, bei dem Erkennungen mit geringem Wert aus einer Erkennungsliste entfernt werden. Eine Erkennung kann durch einen Optimierungsparameter, der verhindert, dass die Erkennung generiert wird, oder durch eine Optimierungsregel, die die Erkennung basierend auf Erkennungstyp, Teilnehmern oder Erkennungseigenschaften ausblendet, optimiert werden.

Wertetabelle

Dieses ExtraHop-Diagramm zeigt den Gesamtwert für eine oder mehrere Metriken. Wenn Sie mehr als eine Metrik auswählen, werden die Metrikwerte nebeneinander angezeigt.

Virtueller Paketverlust

Virtual Paket Loss (VPL) bezieht sich auf ein Phänomen, das vollständig oder teilweise virtualisierte Anwendungen betrifft. VPL verursacht Symptome, die auf eine Netzwerküberlastung hindeuten, und werden von herkömmlichen Tools zur Netzwerküberwachung und zum Anwendung Performance Management (APM) häufig nicht erkannt. VPL tritt auf, wenn ein Hypervisor die CPU-Zeit für eine übermäßige Anzahl von virtuellen Maschinen (VMs) plant und verhindert, dass diese VMs schnell genug auf TCP-Bestätigungen reagieren. VPL kann durch eine Kombination aus Anwendungsbewusstsein und fortschrittlicher TCP-Analyse erkannt werden.

VLAN

Ein Virtual Local Area Network (VLAN) ist eine logische Gruppierung von Verkehr oder Geräten in einem Netzwerk. VLAN-Informationen werden aus VLAN-Tags extrahiert, wenn der Datenverkehrsspiegelungsprozess die Tags auf dem Mirror-Port beibehält.

Schwachstellen-Scanner

Schwachstellenscanner sind Programme, die Anwendungen, Systeme und Netzwerke nach Schwachstellen durchsuchen. Im ExtraHop-System wird einem Gerät, das HTTP-Anfragen sendet , die mit bekannten Scanneraktivitäten verknüpft sind, die Rolle Vulnerability Scanner zugewiesen. Sie können ein Gerät auch manuell als Scanner festlegen, indem Sie die Geräterolle in Vulnerability Scanner ändern.

Beobachtungsliste

Für einzelne Geräte auf der Beobachtungsliste ist eine erweiterte Analyse garantiert. In der Regel werden hochwertige Geräte zur Beobachtungsliste hinzugefügt. Erweiterte Analyse ist eine Analyseebene, auf der Datensätze, Pakete, Aktivitätskarten und Diagramme mit L2-L7-Protokollmetriken für Geräte verfügbar sind. Sie können Geräte jederzeit von der Beobachtungsliste entfernen.

Widgets

Widgets sind konfigurierbar Dashboard Komponenten, die einer Region für verschiedene Funktionen hinzugefügt werden können. Widget-Typen sind Diagramm, Textfeld, Alarm, Aktivitätsgruppen und Netzwerke (nur Konsolen).

Drahtdaten

Drahtdaten werden erstellt, wenn Flugdaten analysiert werden, während der Verkehr über das Netzwerk gesendet wird. Durch die Full-Stream-Verarbeitung in Echtzeit werden unstrukturierte Daten wieder zu strukturierten wire data zusammengesetzt, die in Echtzeit analysiert werden können. Wire Data umfasst L2-L7-Daten , die die gesamte Anwendungsbereitstellungskette umfassen und die umfassendste und weitreichendste Transparenz bieten.

WMI

WMI (Windows Management Instrumentation) ist eine Reihe von Windows-Systemerweiterungen, die eine Betriebssystemschnittstelle zum Einrichten von Fernzugriffssitzungen bereitstellen.

FRAU

Das WSMAN-Protokoll (WSMAN) ist ein öffentlicher Standard für den Datenaustausch mit jedem Computergerät.

Zero Window

Ein Zero Window ist eine TCP-Metrik im ExtraHop-System, die Anwendungsüberlastung misst. Wenn ein Gerät während der Datenübertragung eine Zero-Window-Meldung an das Sendergerät sendet, bedeutet dies, dass das Gerät keine Daten mehr annehmen kann, da das Empfangsfenster des Geräts (ein Puffer für eingehende Daten) voll ist. Die Zero Window Window-Nachricht weist den Absender an, die Datenübertragung bis auf weiteres zu unterbrechen.