ExtraHop Glossary

Published: 2022-12-08

AAA

AAA (Authentication, Authorization, and Accounting) is a security framework that includes application-level network access protocols such as RADIUS, Diameter, TACACS, and TACACS+.

ActiveMQ

ActiveMQ is an open-source, message broker from Apache.

Activity maps

An activity map is a dynamic visual representation of the L4-L7 protocol activity between devices in your network. You can view real-time information about which devices and services are talking to each other across your network.

Advanced Analysis

Records, packets, activity maps, detections, and charts with L2-L7 protocol metrics are available for devices receiving this analysis level. Prioritize a group or add a device to the watchlist to specify which devices should receive Advanced Analysis.

AJP

AJP (Apache JServ Protocol) is used for communication between an Apache web server and an application server.

Alert

An alert is a custom configuration of settings, such as a time interval, metric value, and metric calculations that occur on assigned data sources. An alert is generated when configured conditions are met. Notifications can be sent through channels such as email or SNMP.

AMF

AMF (Action Message Format) is a format for encoding data transported between Adobe Flash clients and servers.

AppFlow

The AppFlow protocol was developed by Citrix. This protocol is an extension of the IPFIX standard for monitoring network traffic. You can collect AppFlow traffic with the ExtraHop NetFlow module.

Application

In the ExtraHop system, applications are user-defined containers that you can associate with multiple devices and protocols for a unified view of built-in metrics. These containers can represent distributed applications on your network environment. You can create a basic application or an advanced application through the Trigger API. The default All Activity application is available to all ExtraHop users.

Application Performance Monitoring

Application performance monitoring (APM) tools enable development and application teams to observe the performance of applications. Data is collected through software agents that run on application servers, databases, and other application components. The agents can be configured to gather host-based ingress and egress transaction data, code-level stack trace inputs, and resource usage metrics such as CPU, memory, and disk.

Visit the ExtraHop website: How to compare APM tools.

Area chart

This ExtraHop chart type displays metric values as a line that connects data points over time, with the area between the line and axis filled in with color.

Asset

Assets are devices and device groups in your environment, as well as related networks, applications, and users.

Atlas Remote Analysis

Through this service, ExtraHop analysts can perform an unbiased analysis of your network data and report on areas in your IT infrastructure where improvements can be made.

Attack chain

(ExtraHop Reveal(x) only) Most network attacks tend to follow familiar patterns or phases. These phases can be assembled into an attack chain to characterize the progression of an attack. ExtraHop Reveal(x) detects unusual network behavior associated with different attack chain phases, including command and control (C&C), reconnaissance, exploit, lateral movement, and actions on objective.

Attack simulator

An attack simulator, also known as a breach and attack simulation (BAS), is a tool that enables analysts to build a threat campaign that emulates attack techniques to evaluate security tool coverage. The ExtraHop system can automatically assign the Attack Simulator role to devices that run these tools.

Audit log

The audit log on the ExtraHop system provides data about the operations of the system, broken down by component. For example, when you log in to the ExtraHop system, the successful or failed event is logged as an entry to the audit log.

Bar chart

This ExtraHop chart type displays the total value of metric data as horizontal bars.

Boxplot chart

The box plot chart displays variability for a distribution of metric data. Each box plot includes three or five data points. With five data points, the box plot contains a box, upper and lower whisker lines, and a tick mark. With three data points, the line contains upper and lower whisker lines, and a tick mark.

Berkeley Packet Filter (BPF)

Berkeley Packet Filter (BPF) is a program for filtering network packets. The BPF syntax enables users to write filters that quickly drill down on specific packets to see the essential information.

Built-in group

Built-in groups contain devices that are automatically grouped together based on their network protocol traffic, such as CIFS clients, or by the role assigned to the device, such as Domain Controllers. A device with multiple types of traffic might appear in more than one built-in group. You can select built-in groups as a metric source for charts, alerts, triggers, and activity maps.

Bundle

Bundles are JSON-formatted documents that contain information about selected system configuration, such as triggers, dashboards, applications, or alerts. You can create a bundle and then transfer those configurations to another ExtraHop system, or save the bundle as a backup of your customizations.

Bundles can also be downloaded from the ExtraHop website: ExtraHop Solution Bundles.

Candlestick chart

This ExtraHop chart type displays data calculations for a distribution of metric values over time. A line at each time interval displays three or five data points. If the line has five data points, it contains a body, middle tick mark, an upper shadow line, and a lower shadow line. If the line has three data points, it contains a middle tick mark.

CIFS

CIFS (Common Internet File System), also known as SMB (Server Message Block), is an application-level protocol that provides client access to files on a network attached storage (NAS) repository, typically in a Windows environment.

Client

A client is an application or system that accesses a service made available by a server.

Cluster

A group of the same type of ExtraHop recordstores that are joined together.

Column chart

This ExtraHop chart type displays metric values as vertical bars over a specified time period.

Console

An ExtraHop console (or ECA) is a command center for centralized management. The console provides a unified view of data collected from sensors, recordstores, and packetstores that are distributed across data centers, branch offices, and the public cloud. Previously referred to as a Command appliance.

CORS

Cross-origin resource sharing (CORS) allows you to access the ExtraHop REST API across domain-boundaries and from specified web pages without requiring the request to travel through a proxy server. You can configure one or more allowed origins or you can allow access to the ExtraHop REST API from any origin. Only administrative users can view and edit CORS settings.

Count metric type

In the ExtraHop system, this top-level metric type represents the number of events that occurred over a specific time period. You can view count metrics as a rate or a total count.

Dashboard

A dashboard is a customizable HTML page that displays different views of your network through widgets such as charts. In addition to custom dashboards, the ExtraHop system provides the following built-in dashboards: Activity dashboard, Network dashboard, and Security dashboard (Reveal(x) only).

Database

Relational databases store, retrieve, and manage structured information through a database management system (DBMS) language.

Dataset metric type

In the ExtraHop system, this top-level metric type represents a distribution of data that can be calculated into percentiles values.

Deduplication

The ExtraHop system removes duplicate L2 and L3 frames and packets when metrics are collected and aggregated from your network activity by default. L2 deduplication removes identical Ethernet frames (where the Ethernet header and the entire IP packet must match); L3 deduplication removes TCP or UDP packets with identical IP ID fields on the same flow (where only the IP packet must match).

Detail metric

Detail metrics provide you with a metric value for a specific key, such as a client IP address, server IP address, URI, hostname, referrer, certificate, or method. When you drill down from a top-level metric in the ExtraHop system to a detail metric, you can gain insight into how a specific device, method, or resource is affecting the network.

Detections

Detections are unexpected deviations from normal patterns in device or application behavior. The ExtraHop Machine Learning service identifies detections from stored ExtraHop system data with a proprietary algorithm that combines time series decomposition, unsupervised learning, heuristics, and ExtraHop unique domain expertise.

Device

Devices are endpoints in your environment that have been automatically discovered and classified by the ExtraHop system.

Device discovery

Device discovery is the process by which ExtraHop builds and maintains a list of active devices associated with monitored network traffic. The ExtraHop system can discover and track devices by their MAC address (L2 Discovery) or by their IP addresses (L3 Discovery). When L2 Discovery is enabled, the ExtraHop system creates a device entry for every local MAC address discovered over the wire. IP addresses are mapped to the MAC address, but metrics are stored with the device MAC address even if the IP address changes. When L3 Discovery is enabled, the ExtraHop system creates and links two entries for each local discovered device: an L2 parent entry with a MAC address and an L3 child entry with IP addresses and the MAC address.

Device group

Device groups, also known as custom groups, can be either static or dynamic. You must manually identify and assign individual devices to a static group. Alternatively, you can configure rules to automatically assign devices to a dynamic group.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol for dynamically distributing network configuration parameters.

DICOM

DICOM (Digital Imaging and Communications in Medicine) is a standard for storing biomedical images and transmitting those images over a network.

Discovery Mode

Records, packets, detections, and information about protocol activity are available for devices in Discovery Mode. Adjust analysis priorities to elevate a device or endpoint from Discovery Mode to Standard or Advanced Analysis.

Distinct count metric type

In the ExtraHop system, this top-level metric type represents the number of unique events that occurred during a selected time interval. The distinct count metric provides an estimate of the number of unique items placed into a set during the selected time interval. Estimates are calculated with the HyperLogLog algorithm.

DNS

DNS (Domain Name System) is the naming system for network hosts and resources that are connected to the Internet. DNS servers map IP addresses to hostnames.

Dynamic baselines

Dynamic baselines are trend lines on dashboards that help you distinguish between normal and abnormal activity. The ExtraHop system calculates dynamic baselines based on historical data. To generate data points on a dynamic baseline, the ExtraHop system calculates the median value for a specified period of time.

Endpoint

Endpoints are internal or external hostnames and IP addresses observed by the ExtraHop system. Internal endpoints are located on your local or remote network, and external endpoints are located outside of your local or remote network.

ERSPAN

Encapsulated Remote SPAN (ERSPAN) enables you to send source traffic on one switch to a destination on another switch, while traversing a Layer 3 boundary.

Event

An event represents activity detected from your network or from your ExtraHop system. Triggers can be written to collect the data associated with an event to create custom metrics.

Fingerprint

A fingerprint is a unique, alphanumeric identifier assigned to all sensors, recordstores, and packetstores.

FIX

FIX (Financial Information eXchange) is a protocol that provides information about the real-time exchange of financial transactions.

Flow

A flow is a set of packets that are part of a single transaction between two endpoints. Similar to how the ExtraHop system can identify flows from wire data, flows from machine data on remote networks can be sent to the ExtraHop system for analysis.

Flow interface

A flow interface is a local grouping of traffic or devices on a flow network. Instead of looking at flow information for the entire network, you can look at flow information for a specific interface on the network.

Flow network

A flow network sends information about flows seen across the device. Similar to how the ExtraHop system can identify flows from wire data, the ExtraHop system can receive flow information from remote network devices, also called flow exporters.

Flow sensor

(ExtraHop Reveal(x) 360 only) An ExtraHop flow sensor (EFC) collects data from flow logs, instead of from packets. Sensors provides the ability to analyze and visualize all of your network, application, client, infrastructure, and business data. Sensors can be connected to an ExtraHop console for centralized management and a unified view of collected and stored data. They can also be connected to recordstores and packetstores for additional storage and deeper analysis.

Flow Stall

A Flow Stall is a TCP metric in the ExtraHop system that measures network congestion. A Flow Stall is counted when there are three consecutive retransmission timeouts (RTOs) observed on a single flow of data between devices. An RTO represents a 1-5 second delay as a device waits to resend data that might have been lost over a congested connection.

FTP

FTP (File Transfer Protocol) is a standard network protocol for transferring files between a client and a server.

Goodput

Goodput refers to the amount of useful data that is transferred over the L4 application layer per unit time. In this context, useful means that retransmissions are discarded as duplicate packets along with any protocol overhead or other non-application data found on the wire. Goodput is always lower than the throughput, and roughly corresponds to the size of the payload bytes for any protocol running on TCP (such as a CIFS file or HTTP request) over the transfer time.

Heatmap chart

This ExtraHop chart type displays a distribution of metric data over time, where color represents a concentration of data.

High value

High value is a designation for devices on your network that you or the ExtraHop system might consider significant to your business applications, workflows, or infrastructure. A device is considered high value if the ExtraHop system observes the device providing authentication or essential services, or if a user manually specifies a device as high value.

Histogram chart

This ExtraHop chart type displays a distribution of metric data as vertical bars, or bins.

HL7

HL7 (Health Level-7) is a standard for exchanging electronic health information between software applications.

HTTP

HTTP (Hypertext Transfer Protocol) is an application-level protocol that retrieves web pages.

IBM MQ

IBM MQ is a message-queuing protocol for IBM enterprise and message middleware products.

ICA

ICA (Independent Computing Architecture) is a Citrix system protocol that transmits data between clients and servers.

ICMP

ICMP (Internet Control Message Protocol) is a protocol that network devices send error and query messages through.

Investigation

An investigation is a user-managed grouping of detections that enable users to view multiple detections in a single timeline and map. Investigations can help determine whether suspicious behavior is a valid threat and if a threat is part of a larger attack campaign.

iDRAC

The Integrated Dell Remote Access Controller (iDRAC) provides remote access to the ExtraHop system. After you enable and configure iDRAC, you can power cycle the system, view console messages, and review hardware monitoring and boot logs.

iSCSI

iSCSI (Internet Small Computer Systems Interface) is a TCP-level protocol that allows SCSI commands to be sent over a local-area network (LAN) or wide-area network (WAN).

Kerberos

Kerberos is a security protocol that applies secret-key cryptography to client and server authentication.

L2

The data link layer in the OSI model. In the ExtraHop system, L2 metrics provide information about the connection between two devices.

L3

The network layer in the OSI model. In the ExtraHop system, L3 metrics provide IP address information for nodes that communicate over the monitored network.

L4 (TCP)

The transport layer in the OSI model. In the ExtraHop system, L4 TCP (Transmission Control Protocol) metrics provide information about the reliable transfer of packets between a source and destination.

L7

The application layer in the OSI model. In the ExtraHop system, L7 metrics provide information about interactivity with software applications.

LDAP

LDAP (Lightweight Directory Access Protocol) is a vendor-neutral protocol that maintains and provides easy access to a distributed directory.

Read the ExtraHop blog post: What Is LDAP, and Who Needs It Anyway?

Level-triggered alerts

A level-triggered alert is generated at specified intervals for as long as the metric value remains above the configured threshold.

Line chart

This ExtraHop chart type displays metric values as a line, which connects a series of data points over time.

Line & column chart

This ExtraHop chart type displays metric values as a line, which connects data points over time, with the option to display another metric as a column chart underneath.

List chart

This ExtraHop chart displays metric values in a list across multiple columns with optional sparklines.

LLDP

The Link Layer Discovery Protocol (LLDP) is a protocol that network devices communicate their identity and capabilities through.

LLMNR

LLMNR (Link-Local Multicast Name Resolution) is a protocol that is included in Microsoft Window systems. This protocol is based on the Domain Name System (DNS) format and enables name resolution for hosts on the same local link when DNS name resolution fails.

Maximum metric type

In the ExtraHop system, this top-level metric type is a single data point that represents the maximum value from a specified time period.

Memcache

Memcache is a protocol that provides access to high-performance, distributed memory object caching systems over a TCP connection.

Metric

In the ExtraHop system, a metric is a measurement of observed network behavior. Metrics are generated from network traffic, and then each metric is associated with a source. The ExtraHop system provides built-in, or default, metrics based on observed network traffic from wire data. You can also create custom metrics in the ExtraHop system by writing a trigger to collect metrics based on a specific event.

Metric Catalog

The Metric Catalog is a tool for viewing information about built-in and custom metrics in the ExtraHop system. You also can delete and edit custom metrics through the Metric Catalog.

Metric Explorer

The Metric Explorer is a tool for configuring dashboard charts. In the Metric Explorer, you can add multiple sources and metrics to a chart and immediately preview how metric data will appear.

Modbus

Modbus is a serial communication protocol used in industrial automation.

MongoDB

MongoDB is an open-source document database that provides performance, availability, and scalability.

MSMQ

MSMQ (Microsoft Message Queuing) is a protocol that enables applications to send messages and objects to each other.

NaN

Acronym for not a number. In the Trigger API, a property with a numeric data type displays `NaN` if the property value is undefined or cannot be represented as a number.

NAS

NAS (Network Attached Storage) is a file-level storage repository. Clients can access the repository through SMB (Server Message Block) or NFS (Network File System) protocols.

NBNS

NBNS or NBT-NS (NetBIOS Name Service) is a naming system for network hosts and resources.

NetFlow

Flow technologies such as Netflow, IPFIX, sFlow, and AppFlow collect traffic data from flow networks outside your wire data feed and send the data to the sensor for analysis.

Network

In the ExtraHop system, a network is the entry point into the network capture, and metrics are collected for network capture attributes, network alerts, and network traffic details. These metrics provide a summary of all network activity retrieved in the capture.

Network bytes

A network byte is a metric that displays the throughput rate of the ExtraHop capture process.

Network health indicators

(ExtraHop Reveal(x) only) Network health indicators are a set of metrics that show you general trends related to network and security health. Network health indicators might signal weaknesses or issues in network performance or potentially suspicious activity. These metrics can be found at the bottom of the Network Overview page.

NFS

NFS (Network File System) is a distributed file system protocol that provides client access to files on a network attached storage (NAS) repository, typically in a UNIX environment.

Node

An individual ExtraHop recordstore within a cluster.

Open Data Stream

The open data stream (ODS) service enables you to send wire data to a remote third-party system, such as MongoDB or Kafka. You must write a trigger to identify and collect the data you want to export and configure settings through the ExtraHop Administration settings.

Packet sensor

A packet sensor passively collects a copy of unstructured wire data—all of the transactions on your network—and transforms this data into structured wire data. Sensors provides the ability to analyze and visualize all of your network, application, client, infrastructure, and business data. Sensors can be connected to an ExtraHop console for centralized management and a unified view of collected and stored data. They can also be connected to recordstores and packetstores for additional storage and deeper analysis.

Packets

The Packets feature enables you to search for and download packets for selected transactions through a sensor or a console. This feature requires a supported packetstore.

Packetstore

An ExtraHop packetstore collects raw, network packets sent from a connected packet sensor for long-term retrieval and storage. Packetstores enable you to quickly retrieve all packets that match a set of search criteria within a given time interval.

Participant

Participants are endpoints that are participating as an offender or victim in a detection.

Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy (PFS) is an encryption method that enables short-term, completely private key exchanges between clients and servers. You can license the ExtraHop system to decrypt PFS SSL/TLS sessions from Windows servers where the ExtraHop PFS agent software is installed. Without PFS, those sessions could not be decrypted, and the data from those exchanges would be obscured.

PCAP

PCAP (packet capture) consists of an application programming interface (API) for capturing network traffic and storing it to a database.

PCoIP

PCoIP (PC-over-IP) is a protocol that transfers compressed and encrypted image pixels from a central server to a PCoIP device.

Pie chart

This ExtraHop chart displays metric data as a portion or percentage of a whole.

POP3

POP3 (Post Office Protocol) is a standard application-level protocol that transfers email messages between a server and a client application over a TCP connection.

Port mirroring

Port mirroring occurs when a network switch sends a copy of network packets from one switch port (or an entire VLAN) to a network monitoring connection on another switch port.

Protocol

A protocol defines the format and the order of messages exchanged between two or more devices, as well as the actions taken on the transmission and receipt of a message or other event.

Protocol page

A protocol page is a built-in page that includes built-in charts with top-level metrics about your assets. These metric charts can be copied to your dashboards.

RDP

RDP (Remote Desktop Protocol) is a proprietary Microsoft protocol for communicating between a Remote Desktop Session Host server and a client running Remote Desktop Connections software. RDP is encapsulated and encrypted within TCP.

Record

Records are structured flow and transaction information about events on your network that can be sent to a supported recordstore for storage. Then, you can query for records from a sensor or a console.

Record format

A record format is a schema on read that determines how each record is displayed in the ExtraHop system. The ExtraHop system has built-in record formats for all built-in record types, and although you cannot modify a built-in record format, you can create a custom record format.

Record types

Record types link stored records with the record format in the ExtraHop system. Requires a supported recordstore.

Recordstore

A recordstore collects transaction and flow records sent from a connected sensor for long-term storage and retrieval. You can view, save, and search the structured flow and transaction information about events on your network with a simple, unified UI, with no modifications to your existing applications or infrastructure. ExtraHop recordstores are available as physical or virtual deployments; the ExtraHop Cloud Recordstore is provided for Reveal(x) 360; and supported third-party data warehouses include BigQuery and Splunk.

Redis

Redis is an open-source, data structure server.

Region

A region is a dashboard component that contains widgets.

Retransmission Timeout (RTO)

A retransmission timeout (RTO) is a TCP protocol metric for determining network performance. TCP retransmissions occur on the network frequently. TCP starts a retransmission timer when an outbound segment is handed down to an IP address. If there is no acknowledgment (ACK) before the timer expires, the segment is retransmitted. An RTO occurs when the sender begins missing too many acknowledgments and stops sending segments for a period of time. RTOs can represent a 1-5 second delay on your network. Multiple RTOs over time can represent significant delays on your network.

Read the ExtraHop blog post: TCP RTOs: Retransmission Timeouts & Application Performance Degradation.

Reveal(x) 360

Reveal(x) 360 provides SaaS-based visibility and management across on-premises and cloud-based connected environments. The Reveal(x) 360 console provides a single view of data collected from multiple sensors, packetstores, and recordstores, which can be distributed across data centers, branch offices, and the public cloud.

Reveal(x) Enterprise

Reveal(x) Enterprise is a subscription-based offering of ExtraHop products that include a sensor to collect wire data and additional components based on the plan type.

RFB

RFB (remote framebuffer) is a protocol for remote access to a graphical user interface that allows a client to view and control a system on another computer.

Risk score

(ExtraHop Reveal(x) only) A risk score is a numeric indicator of the severity of a detection. Risk scores are based on several factors, such as where the detection falls in the attack chain, the vulnerability of the detection protocol, and the level of impact the detection could have on the network. Scoring is on a scale from 1-99, with 99 being the most severe.

RPC

MRPC (Microsoft Remote Procedure Call) is a communication mechanism for clients to call a procedure from a program located on another computer, server, or network.

Remote packet capture (RPCAP)

Remote packet capture (RPCAP) is a software implementation for packet forwarding that is similar to a physical tap. If you want to monitor network traffic for devices that are not directly connected to your wire data feed, you can forward packets through the cloud and analyze that data through the ExtraHop system.

RSPAN

Remote Switched Port Analyzer (RSPAN) provides remote monitoring of multiple switches across a switched network. RSPAN is a way to get traffic from a SPAN source on one switch to a SPAN destination on another switch that is connected via a trunk.

Note: RSPAN requires that the source and destination chassis are in the same Layer 2 domain.

RTCP

RTCP (Real-time Transport Control Protocol) is a protocol that monitors statistics for streaming audio and video data transferred by the RTP protocol.

RTP

RTP (Real-time Transport) is a protocol that defines the standardized packet format for the real-time transfer of streaming audio and video.

Debug Log

The debug log is a component of the Trigger Editor in the ExtraHop system. The debug log displays exceptions and output from debug statements in trigger scripts.

Sampleset metric type

In the ExtraHop system, this top-level metric type represents a summary of data that provides a mean (average) and standard deviation over a specified time period. Sampleset metrics typically summarize data about a detail metric.

SDP

The Session Description Protocol (SDP) is a protocol that defines multimedia streaming sessions.

Sensor

An ExtraHop sensor provides the ability to analyze and visualize all of your network, application, client, infrastructure, and business data. A packet sensor (or EDA) passively collects a copy of unstructured wire data—all of the transactions on your network—and transforms this data into structured wire data. A flow sensor (or EFC) collects data from flow logs and is only supported on ExtraHop Reveal(x) 360. Sensors can be connected to an ExtraHop console for centralized management and a unified view of collected and stored data. They can also be connected to recordstores and packetstores for additional storage and deeper analysis.

Server

A server is a hardware system dedicated to hosting one or more services for users or clients on the network. In the context of Internet Protocol (IP) networking, a server is a program that operates as a socket listener.

SIP

SIP (Session Initiation Protocol) is a signaling protocol that controls communication sessions, such as voice calls for IP-based telephony applications.

Site

A site is a wire data feed analyzed by the ExtraHop system that represents a physical or logical area of your network, such as a data center, branch office, or cloud workload. You can view assets, detections, and other data from a specific site or across multiple sites.

SMPP

SMPP (Short Messaging Peer-to-Peer) is an application-level protocol that transfers Short Message Service (SMS) data between External Short Messaging Entities (ESME) and Short Message Service Centers (SMSC).

SMTP

SMTP (Simple Mail Transfer Protocol) is a standard protocol that sends, receives, and relays email messages between servers, email transfer agents, and client applications.

Snapshot metric type

In the ExtraHop system, this top-level metric type represents a data point that represents a single point in time. Snapshot metrics include ratios, current connections, and established TCP connections.

SNMP

The Simple Network Management Protocol (SNMP) is a layer-7 protocol for collecting, organizing, exchanging, and modifying information about managed devices on IP networks.

Source

Sources are assets that can be assigned to charts, triggers, and alerts to provide access to metric collections.

SPAN

Port mirroring on a Cisco Systems switch is generally referred to as Switched Port Analyzer (SPAN). SPAN copies traffic and sends it to a destination for network analysis.

SSH

Secure Shell (SSH) is a protocol that securely transmits information over a network.

SSL

SSL (Secure Sockets Layer) is a standard protocol for securing communication over the Internet. To establish an encrypted link between a web browser and a server, the server must have an SSL certificate.

Standard Analysis

Records, packets, detections, activity maps, protocol activity, and charts with throughput and packet metrics are available for devices receiving Standard Analysis. Adjust analysis priorities to elevate a device or endpoint from Standard Analysis to Advanced Analysis.

Status chart

This ExtraHop chart type displays metric values in a column chart, where the color of the columns represents the status and severity of an alert assigned to the source and metric selected in the chart.

STIX

(ExtraHop Reveal(x) only) Structured Threat Information eXpression (STIX) is the language and serialization format for standardizing, conveying, and sharing data about cyber threat intelligence data. The STIX format is commonly supported by the threat intelligence community and platforms. You can upload STIX files through the ExtraHop system or the REST API as a custom threat collection. Custom threat collections must be formatted in STIX as TAR or TAR.GZ files.

Table chart

This ExtraHop chart type displays metric values across rows and columns in a table.

TCP

In the ExtraHop system, TCP (Transmission Control Protocol) metrics provide information about the reliable transfer of packets between a source and destination. Through TCP metrics, ExtraHop provides visibility into which devices are connected to each other, when devices send data, if there are errors in the data, what protocols are communicated through, and so on.

TCP RST

A TCP RST packet is sent to prevent a TCP connection from being established or to forcibly terminate an existing connection. Sometimes resets are sent when the receiving device failed to ACK the SYN packet, or it failed to acknowledge another packet sent and retransmitted later in the transaction. In some cases, TRCP RSTs indicates that an error occurred. High volumes of outbound resets should be investigated to determine if they are expected behavior or indicative of a larger issue.

Telnet

Telnet is an application-layer protocol for interactive text-oriented communications over a virtual terminal connection.

Threat briefing

(ExtraHop Reveal(x) only) Threat briefings provide guidance about potential threats to your network from both industry-wide security events and machine-learning analysis of your network. Threat briefings might include detections of scans, exploits, and indicators of compromise (IOC) that are related to the threat.

Threat collection

(ExtraHop Reveal(x) only) A threat collection is a data set of suspicious IP addresses, hostnames, and URIs that enables your Reveal(x) system to identify indicators of compromise and display threat intelligence in system charts and records.

Threat intelligence

Threat intelligence is known data about suspicious IP addresses, hostnames, and URIs that can help identify risks to your organization. These data sets, called threat collections, are available by default in your Reveal(x) system and from free and commercial sources in the security community.

Time Selector

The Time Selector is a tool that enables you to specify a time interval for the collection and presentation of network data in the ExtraHop system. There are two types of Time Selectors: a Global Time Selector for specifying global time intervals and a Region Time Selector for specifying region time intervals in a dashboard.

Timestamp

A timestamp is a digital record of the time a particular event occurred. In the ExtraHop system, you can select the default timestamp, or configure external timestamps such as Gigamon or Anue through the Running Configuration file.

Tinygram

A tinygram is a small packet or TCP segment. A tinygram is a packet where the payload is smaller than the frame header (L2-L4) data. In general, tinygrams lead to inefficient ratios of frame header data to actual useful information going across the network. Tinygrams can contribute to network congestion.

Read the ExtraHop blog post: What is a Tinygram?

Top-level metric

A top-level, or base, metric gives you a sum of data for a specified time period. Top-level metrics provide you with a big-picture value to help identify what is happening on your network. You can then drill down on a top-level metric to view detail metrics. There are different types of top-level metrics that provide different information, which include count, dataset, maximum, sampleset, and snapshot metric types. Understanding metrics types is essential to writing triggers and configuring charts.

Topnset

A topnset is the top 1,000 key-value pairs calculated for the time interval you specify in the Time Selector. A topnset is not a complete data set because a topnset only represents the key-values that are recorded for a specific aggregation roll up (based on a specified time interval), and is limited to up to 1,000 keys per topnset.

Trigger

Triggers are custom scripts that perform an action upon a pre-defined event. For example, you can write a trigger to record a custom metric every time an HTTP request occurs, or to classify traffic for a particular server as an application server.

For more information, see the Trigger API Reference.

Tuning

The process by which low-value detections are removed from a detection list. A detection can be tuned by a tuning parameter that suppresses the detection from being generated, or by a tuning rule that hides the detection based on detection type, participants, or detection properties.

Value chart

This ExtraHop chart displays the total value for one or more metrics. Selecting more than one metric will display the metric values side-by-side.

Virtual packet loss

Virtual packet loss (VPL) refers to a phenomenon that affects fully or partially virtualized applications. VPL creates symptoms that suggests network congestion and is often undetected by traditional network monitoring and application performance management (APM) tools. VPL occurs when a hypervisor schedules CPU time for an excessive number of virtual machines (VMs) and prevents those VMs from responding fast enough to TCP acknowledgments. VPL can be detected by a combination of application awareness and advanced TCP analysis.

VLAN

A Virtual Local Area Network (VLAN) is a logical grouping of traffic or devices on a network. VLAN information is extracted from VLAN tags, if the traffic mirroring process preserves the tags on the mirror port.

Vulnerability Scanner

Vulnerability scanners are programs that search applications, systems, and networks for weaknesses. In the ExtraHop system, a device that sends HTTP requests associated with known scanner activity is assigned the Vulnerability Scanner role. You can also manually designate a device as a scanner by changing the device role to Vulnerability Scanner.

Watchlist

Individual devices on the watchlist are guaranteed Advanced Analysis. Typically, high-value endpoints are added to the watchlist. Advanced Analysis is an analysis level where records, packets, activity maps, and charts with L2-L7 protocol metrics are available for devices. You can remove devices from the watchlist at any time.

Widget

Widgets are configurable dashboard components that can be added to a region for different functions. Widget types are chart, text box, alert, activity groups, and networks (consoles only).

Wire data

Wire data is created when data in flight is analyzed as traffic is sent over the network. Through real-time full-stream processing, unstructured data is reassembled into structured wire data that can be analyzed in real time. Wire data encompasses L2-L7 data that spans the entire application delivery chain and provides the most comprehensive, wide-reaching visibility.

WMI

WMI (Windows Management Instrumentation) is a set of Windows system extensions that provides an operating system interface for establishing remote access sessions.

WSMAN

WSMAN (Web Services Management) protocol is a public standard for exchanging data with any computer device.

Zero Window

A Zero Window is a TCP metric in the ExtraHop system that measures application congestion. When a device advertises a Zero Window message to the sender device during data transfer, this means that the device can no longer accept data because the device's receive window (a buffer for incoming data) is full. The Zero Window message tells the sender to pause data transfer until further notice.