Glossaire ExtraHop

Publié: 2024-04-10

AAA

AAA (Authentication, Authorization, and Accounting) est un cadre de sécurité qui inclut des protocoles d'accès réseau au niveau des applications tels que RADIUS, Diameter, TACACS et TACACS+.

ActiveMQ

ActiveMQ est un courtier de messages open-source d'Apache.

Cartes d'activités

Une carte dactivity est une représentation visuelle dynamique de l'activité du protocole L4-L7 entre les appareils de votre réseau. Vous pouvez consulter des informations en temps réel sur les appareils et les services qui communiquent entre eux sur votre réseau.

Analyse avancée

Les enregistrements, les paquets, les cartes d'activité, les détections et les graphiques contenant les métriques du protocole L2-L7 sont disponibles pour les appareils recevant ce niveau d'analyse. Donnez la priorité à un groupe ou ajoutez un équipement à la liste de surveillance pour spécifier quels appareils doivent faire l'objet d'une Analyse avancée.

AJP

Le protocole AJP (Apache JServ Protocol) est utilisé pour la communication entre un serveur Web Apache et un serveur dapplications.

Alerte

Une alerte est une configuration personnalisée de paramètres, tels qu'un intervalle de temps, une valeur métrique et des calculs métriques effectués sur les sources de données attribuées. Une alerte est générée lorsque les conditions configurées sont remplies. Les notifications peuvent être envoyées par des canaux tels que le courrier électronique ou le SNMP.

AMF

L'AMF (Action Message Format) est un format de codage des données transportées entre les clients et les serveurs Adobe Flash.

AppFlow

Le protocole AppFlow a été développé par Citrix. Ce protocole est une extension de la norme IPFIX pour la surveillance du trafic réseau. Vous pouvez collecter le trafic AppFlow avec le module ExtraHop NetFlow.

Demande

Dans le système ExtraHop, les applications sont des conteneurs définis par l'utilisateur que vous pouvez associer à plusieurs appareils et protocoles pour une vue unifiée des métriques intégrées. Ces conteneurs peuvent représenter des applications distribuées sur votre environnement réseau. Vous pouvez créer une application de base ou une application avancée via l'API Trigger. L'application All Activity par défaut est disponible pour tous les utilisateurs d'ExtraHop.

Surveillance des performances des applications

Les outils de surveillance des performances des applications (APM) permettent aux équipes de développement et d'application d'observer les performances des applications. Les données sont collectées par le biais d'agents logiciels qui s'exécutent sur les serveurs d'applications, les bases de données et les autres composants de l'application. Les agents peuvent être configurés pour collecter des données de transaction d'entrée et de sortie basées sur l'hôte, des entrées de suivi au niveau du code et des mesures d'utilisation des ressources telles que le processeur, la mémoire et le disque.

Visitez le site Web d'ExtraHop : Comment comparer les outils APM.

Carte des zones

Ce type de graphique ExtraHop affiche les valeurs métriques sous forme de ligne reliant les points de données au fil du temps, la zone située entre la ligne et l'axe étant colorée.

Actif

Les actifs sont les appareils et les groupes d'équipements de votre environnement, ainsi que les réseaux, applications et utilisateurs associés.

Chaîne d'attaque

(ExtraHop Reveal (x) uniquement) La plupart des attaques de réseau ont tendance à suivre des schémas ou des phases familiers. Ces phases peuvent être regroupées dans une chaîne dattacks afin de caractériser la progression d'une attaque. ExtraHop Reveal (x) détecte les comportements inhabituels du réseau associés aux différentes phases de la chaîne dattaques, notamment le commandement et le contrôle (C&C), la reconnaissance, l'exploit, le mouvement latéral et les actions sur un objectif.

Simulateur d'attaque

Un simulateur d'attaques, également connu sous le nom de simulation de brèches et d'attaques (BAS), est un outil qui permet aux analystes de créer une campagne de menaces qui imite des techniques d'attaque afin d' évaluer la couverture des outils de sécurité. Le système ExtraHop peut attribuer automatiquement le rôle de simulateur d'attaque aux appareils qui exécutent ces outils.

Journal d'audit

Le journal dac.audit du système ExtraHop fournit des données sur le fonctionnement du système, ventilées par composant. Par exemple, lorsque vous vous connectez au système ExtraHop, l'événement de réussite ou d'échec est enregistré sous forme d'entrée dans le journal dac.audit.

Graphique à barres

Ce type de graphique ExtraHop affiche la valeur totale des données métriques sous forme de barres horizontales.

Graphique Boxplot

Le diagramme à boîtes montre la variabilité d'une distribution de données métriques. Chaque diagramme à cases comprend trois ou cinq points de données. Avec cinq points de données, le diagramme à cases contient une case, des lignes de moustache supérieures et inférieures et une coche. Avec trois points de données, la ligne contient des lignes de moustache supérieures et inférieures, ainsi qu'une coche.

Filtre à paquets Berkeley (BPF)

Le filtre de paquets Berkeley (BPF) est un programme de filtrage des paquets réseau. La syntaxe BPF permet aux utilisateurs d'écrire des filtres qui explorent rapidement des paquets spécifiques pour afficher les informations essentielles.

Groupe intégré

Les groupes intégrés contiennent des appareils qui sont automatiquement regroupés en fonction de leur trafic de protocole réseau, tels que les clients CIFS, ou du rôle attribué à l'équipement, tel que les contrôleurs de domaine. Un équipement présentant plusieurs types de trafic peut apparaître dans plusieurs groupes intégrés. Vous pouvez sélectionner des groupes intégrés comme source métrique pour les graphiques, les alertes, les déclencheurs et les cartes d'activité.

Bundle

Les ensembles sont des documents au format JSON qui contiennent des informations sur la configuration système sélectionnée, telles que des déclencheurs, des tableaux de bord, des applications ou alertes. Vous pouvez créer un bundle, puis transférer ces configurations vers un autre système ExtraHop, ou enregistrer le bundle en tant que sauvegarde de vos personnalisations.

Les packs peuvent également être téléchargés depuis le site Web d'ExtraHop : Offres groupées de solutions ExtraHop.

Tableau en chandeliers

Ce type de graphique ExtraHop affiche les calculs de données pour une distribution des valeurs métriques dans le temps. À chaque intervalle de temps, une ligne affiche trois ou cinq points de données. Si la ligne comporte cinq points de données, elle contient un corps, un crochet central, une ligne d'ombre supérieure et une ligne d'ombre inférieure. Si la ligne comporte trois points de données, elle contient un crochet central.

CIFS

Le CIFS (Common Internet File System), également connu sous le nom de SMB (Server Message Block), est un protocole au niveau de l'application qui permet aux clients d'accéder aux fichiers d'un système de stockage rattaché au réseau (NAS), généralement dans un environnement Windows.

Cliente

Un client est une application ou un système qui accède à un service mis à disposition par un serveur.

Cluster

Un groupe du même type de magasins de disques ExtraHop réunis.

Diagramme à colonnes

Ce type de graphique ExtraHop affiche les valeurs métriques sous forme de barres verticales sur une période spécifiée.

Console

Une console ExtraHop (ou ECA) est un centre de commande pour une gestion centralisée. La console fournit une vue unifiée des données collectées à partir de capteurs, de magasins de disques et de magasins de paquets distribués dans les centres de données, les succursales et le cloud public. Anciennement appelé appareil de commande.

CORS

Le partage de ressources entre origines (CORS) vous permet d'accéder à l'API REST ExtraHop au-delà des limites du domaine et à partir de pages Web spécifiées sans que la demande passe par un serveur proxy. Vous pouvez configurer une ou plusieurs origines autorisées ou autoriser l' accès à l'API REST ExtraHop depuis n'importe quelle origine. Seuls les utilisateurs administratifs peuvent consulter et modifier les paramètres CORS.

Type métrique de comptage

Dans le système ExtraHop, ce type de métrique de niveau supérieur représente le nombre d'événements survenus au cours d'une période donnée. Vous pouvez visualiser les mesures de dénombrement sous forme de taux ou de dénombrement total.

Tableau de bord

Un tableau de bord est une page HTML personnalisable qui affiche différentes vues de votre réseau par le biais de widgets tels que des graphiques. Outre les tableaux de bord personnalisés, le système ExtraHop fournit les tableaux de bord intégrés suivants : tableau de bord des activités, tableau de bord réseau et tableau de bord de sécurité (Reveal (x) uniquement).

Base de données

Les bases de données relationnelles stockent, extraient et gèrent des informations structurées via un langage de système de gestion de base de données (DBMS).

Type métrique du jeu de données

Dans le système ExtraHop, ce type de métrique de niveau supérieur représente une distribution de données qui peut être calculée en percentiles.

Déduplication

Le système ExtraHop supprime les doublons de trames et de paquets L2 et L3 lorsque les métriques sont collectées et agrégées à partir de l'activité de votre réseau par défaut. La déduplication L2 supprime les trames Ethernet identiques (où l'en-tête Ethernet et l'intégralité du paquet IP doivent correspondre) ; la déduplication L3 supprime les paquets TCP ou UDP avec des champs d'ID IP identiques sur le même flux (où seul le paquet IP doit correspondre).

Métrique de détail

Les métriques détaillées vous fournissent une valeur métrique pour une clé spécifique, telle qu'une adresse IP client, une adresse IP de serveur, un URI, un nom d'hôte, un référent, un certificat ou une méthode. Lorsque vous passez d' une métrique de niveau supérieur dans le système ExtraHop à une métrique détaillée, vous pouvez avoir un aperçu de l'impact d'un équipement, d'une méthode ou d'une ressource spécifique sur le réseau.

Détections

Les détections sont des écarts inattendus par rapport aux modèles normaux de comportement de l'équipement ou de l'application. Le service ExtraHop Machine Learning identifie les détections à partir des données système ExtraHop stockées à l'aide d'un algorithme propriétaire qui combine la décomposition des séries chronologiques, l'apprentissage non supervisé, l'heuristique et l'expertise unique du domaine ExtraHop.

Appareil

Les appareils sont des points de terminaison de votre environnement qui ont été automatiquement découverts et classés par le système ExtraHop.

Découverte des appareils

La découverte d'appareils est le processus par lequel ExtraHop crée et gère une liste de périphériques actifs associés au trafic réseau surveillé. Le système ExtraHop peut découvrir et suivre les appareils par leur adresse MAC (L2 Discovery) ou par leur adresse IP (L3 Discovery). Lorsque L2 Discovery est activé, le système ExtraHop crée une entrée d'équipement pour chaque adresse MAC locale découverte sur le fil. Les adresses IP sont mappées à l' adresse MAC, mais les métriques sont stockées avec l'adresse MAC de l'équipement même si l'adresse IP change. Lorsque L3 Discovery est activé, le système ExtraHop crée et lie deux entrées pour chaque équipement local découvert : une entrée parent L2 avec une adresse MAC et une entrée enfant L3 avec les adresses IP et l'adresse MAC.

Groupe d'appareils

Les groupes d'appareils, également appelés groupes personnalisés, peuvent être statiques ou dynamiques. Vous devez identifier et attribuer manuellement des appareils individuels à un groupe statique. Vous

pouvez également configurer des règles pour attribuer automatiquement les appareils à un groupe dynamique.

DHCP

Le DHCP (Dynamic Host Configuration Protocol) est un protocole permettant de distribuer dynamiquement les paramètres de configuration réseau.

DICOM

La norme DICOM (Digital Imaging and Communications in Medicine) permet de stocker des images biomédicales et de les transmettre sur un réseau.

mode de découverte

Les enregistrements, les paquets, les détections et les informations relatives à l'activité du protocole sont disponibles pour les appareils en mode de découverte. Ajustez les priorités d'analyse pour faire passer un équipement ou un point de terminaison du mode de découverte au mode Analyse standard ou avancée.

Type de métrique de comptage distinct

Dans le système ExtraHop, ce type de métrique de niveau supérieur représente le nombre d' événements uniques survenus pendant un intervalle de temps sélectionné. La métrique de comptage distincte fournit une estimation du nombre d'éléments uniques placés dans un ensemble pendant l'intervalle de temps sélectionné. Les estimations sont calculées à l'aide de l'algorithme HyperLogLog.

DNS

Le DNS (Domain Name System) est le système de dénomination des hôtes et des ressources du réseau connectés à Internet. Les serveurs DNS mappent les adresses IP aux noms d'hôtes.

Lignes de base dynamiques

Les lignes de base dynamiques sont des lignes de tendance sur tableaux de bord qui vous aident à faire la distinction entre une activité normale et une activité anormale. Le système ExtraHop calcule des lignes de base dynamiques sur la base de données historiques. Pour générer des points de données sur une ligne de base dynamique, le système ExtraHop calcule la valeur médiane pour une période spécifiée.

Point final

Les points de terminaison sont des noms d'hôtes internes ou externes et des adresses IP observés par le système ExtraHop. Les points de terminaison internes sont situés sur votre réseau local ou distant, et les points de terminaison externes sont situés en dehors de votre réseau local ou distant.

ERSPAN

L'ERSPAN à distance encapsulé (ERSPAN) vous permet d'envoyer le trafic source d'un commutateur vers une destination située sur un autre commutateur, tout en franchissant une limite de couche 3.

Événement

Un événement représente une activité détectée depuis votre réseau ou depuis votre système ExtraHop. Les déclencheurs peuvent être écrits pour collecter les données associées à un événement afin de créer des métriques personnalisées.

Empreinte

Une empreinte digitale est un identifiant alphanumérique unique attribué à tous les capteurs, enregistreurs et magasins de paquets.

FIX

FIX (Financial Information eXchange) est un protocole qui fournit des informations sur l'échange en temps réel de transactions financières.

Débit

Un flux est un ensemble de paquets faisant partie d'une transaction unique entre deux points de terminaison. De la même manière que le système ExtraHop peut identifier les flux à partir de données filaires, les flux provenant de données de machines sur des réseaux distants peuvent être envoyés au système ExtraHop pour analyse.

Interface de flux

Une interface de flux est un regroupement local de trafic ou d'appareils sur un réseau de flux. Au lieu de consulter les informations de flux pour l'ensemble du réseau, vous pouvez consulter les informations de flux pour une interface spécifique du réseau.

réseau Flow

Un réseau de flux envoie des informations sur les flux observés sur l'équipement. Tout comme le système ExtraHop peut identifier les flux à partir de données filaires, le système ExtraHop peut recevoir des informations de flux provenant de périphériques réseau distants, également appelés exportateurs de flux.

sonde de débit

(ExtraHop Reveal (x) 360 uniquement) Un capteur de flux ExtraHop (EFC) collecte les données à partir des journaux de flux, plutôt que des paquets. Les capteurs permettent d'analyser et de visualiser toutes les données de votre réseau, de vos applications, de vos clients, de votre infrastructure et de votre entreprise. Les capteurs peuvent être connectés à une console ExtraHop pour une gestion centralisée et une vue unifiée des données collectées et stockées. Ils peuvent également être connectés à des magasins de disques et à des magasins de paquets pour un stockage supplémentaire et une analyse plus approfondie.

Stand Flow

Un Flow Stall est une métrique TCP du système ExtraHop qui mesure la congestion du réseau. Un blocage de flux est compté lorsque trois délais de retransmission (RTO) consécutifs sont observés sur un seul flux de données entre appareils. Un RTO représente un délai de 1 à 5 secondes lorsqu'un équipement attend de renvoyer des données qui auraient pu être perdues en raison d'une connexion encombrée.

FTP

Le protocole FTP (File Transfer Protocol) est un protocole réseau standard permettant de transférer des fichiers entre un client et un serveur.

Goodput

Goodput fait référence à la quantité de données utiles transférées sur la couche d' application L4 par unité de temps. Dans ce contexte, utile signifie que les retransmissions sont éliminées sous forme de paquets dupliqués, ainsi que toute surcharge liée au protocole ou toute autre donnée non liée à l'application trouvée sur le fil. Le Goodput est toujours inférieur au débit et correspond approximativement à la taille des octets de charge utile pour tout protocole exécuté sur TCP (tel qu'un fichier CIFS ou une requête HTTP) pendant le temps de transfert.

Graphique Heatmap

Ce type de graphique ExtraHop affiche une distribution des données métriques dans le temps, la couleur représentant une concentration de données.

Valeur élevée

La valeur élevée est une désignation désignant les appareils de votre réseau que vous ou le système ExtraHop pourriez considérer comme importants pour vos applications, vos flux de travail ou votre infrastructure professionnels. Un équipement est considéré comme ayant une valeur élevée si le système ExtraHop observe que l'équipement fournit une authentification ou fournit des services essentiels, ou si un utilisateur spécifie manuellement un équipement avec une valeur élevée.

Diagramme d'histogramme

Ce type de graphique ExtraHop affiche une distribution des données métriques sous forme de barres verticales ou de bacs.

HL7

Le HL7 (Health Level-7) est une norme pour l'échange d' informations de santé électroniques entre applications logicielles.

HTTP

Le protocole HTTP (Hypertext Transfer Protocol) est un protocole au niveau de l'application qui permet de récupérer des pages Web.

IBM MQ

IBM MQ est un protocole de mise en file d'attente de messages destiné aux produits IBM Enterprise et aux intergiciels de messagerie.

ICA

L'ICA (Independent Computing Architecture) est un protocole système Citrix qui transmet des données entre les clients et les serveurs.

ICMP

L'ICMP (Internet Control Message Protocol) est un protocole par lequel les périphériques réseau envoient des messages d'erreur et de requête.

Système de détection d'intrusion (IDS)

Les systèmes de détection d'intrusion (IDS) s'appuient sur un ensemble de règles contenant des signatures d'activités réseau dangereuses ou malveillantes. L'association d'une sonde IDS ExtraHop à une sonde de paquet ExtraHop permet au système ExtraHop d'identifier les activités malveillantes ou dangereuses sur la base des signatures IDS traditionnelles.

Enquête

Une investigation est un regroupement de détections géré par l'utilisateur qui permet aux utilisateurs de visualiser plusieurs détections sur une seule chronologie et une seule carte. Les enquêtes peuvent aider à déterminer si un comportement suspect constitue une menace valable et si une menace s'inscrit dans le cadre d'une campagne d'attaque plus vaste.

iDRAC

Le contrôleur d'accès à distance Dell intégré (iDRAC) fournit un accès à distance au système ExtraHop. Après avoir activé et configuré iDRAC, vous pouvez redémarrer le système, consulter les messages de la console et consulter les journaux de démarrage et de surveillance du matériel.

iSCSI

L'iSCSI (Internet Small Computer Systems Interface) est un protocole de niveau TCP qui permet d'envoyer des commandes SCSI via un réseau local (LAN) ou un réseau étendu (WAN).

Kerberos

Kerberos est un protocole de sécurité qui applique le chiffrement par clé secrète à l'authentification des clients et des serveurs.

L2

La couche de liaison de données dans le modèle OSI. Dans le système ExtraHop, les métriques L2 fournissent des informations sur la connexion entre deux appareils.

L3

La couche réseau du modèle OSI. Dans le système ExtraHop, les métriques L3 fournissent des informations d' adresse IP pour les nœuds qui communiquent sur le réseau surveillé.

L4 (TCP)

La couche de transport dans le modèle OSI. Dans le système ExtraHop, les métriques TCP (protocole de contrôle de transmission) L4 fournissent des informations sur le transfert fiable de paquets entre une source et une destination.

L7

La couche d'application dans le modèle OSI. Dans le système ExtraHop, les métriques L7 fournissent des informations sur l'interactivité avec les applications logicielles.

LDAP

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole indépendant du fournisseur qui gère et facilite l'accès à un annuaire distribué.

Lisez le billet de blog d'ExtraHop : Qu'est-ce que le LDAP, et qui en a besoin de toute façon ?

Alertes déclenchées par le niveau

Une alerte déclenchée par niveau est générée à des intervalles spécifiés tant que la valeur métrique reste supérieure au seuil configuré.

Graphique linéaire

Ce type de graphique ExtraHop affiche les valeurs métriques sous forme de ligne, qui relie une série de points de données au fil du temps.

Graphique à lignes et à colonnes

Ce type de graphique ExtraHop affiche les valeurs métriques sous forme de ligne, qui relie les points de données au fil du temps, avec la possibilité d'afficher une autre métrique sous forme de graphique à colonnes en dessous.

Tableau de liste

Ce graphique ExtraHop affiche les valeurs métriques dans une liste répartie sur plusieurs colonnes avec des sparklines facultatifs.

LLDP

Le protocole LLDP (Link Layer Discovery Protocol) est un protocole par lequel les périphériques réseau communiquent leur identité et leurs capacités.

LLMNR

LLMNR (Link-Local Multicast Name Resolution) est un protocole inclus dans les systèmes Microsoft Windows. Ce protocole est basé sur le format DNS (Domain Name System) et permet la résolution de noms pour les hôtes sur le même lien local en cas d'échec de la résolution de noms DNS.

Type métrique maximal

Dans le système ExtraHop, ce type de métrique de niveau supérieur est un point de données unique qui représente la valeur maximale pour une période spécifiée.

Memcache

Memcache est un protocole qui permet d'accéder à des systèmes de mise en cache d'objets de mémoire distribuée à hautes performances via une connexion TCP.

Métrique

Dans le système ExtraHop, une métrique est une mesure du comportement observé sur le réseau. Les métriques sont générées à partir du trafic réseau, puis chaque métrique est associée à une source. Le système ExtraHop fournit des métriques intégrées, ou par défaut, basées sur le trafic réseau observé à partir de Wire Data. Vous pouvez également créer des métriques personnalisées dans le système ExtraHop en écrivant un déclencheur pour collecter des métriques en fonction d'un événement spécifique.

Catalogue métrique

Le catalogue de métriques est un outil permettant de visualiser des informations sur les métriques intégrées et personnalisées dans le système ExtraHop. Vous pouvez également supprimer et modifier des métriques personnalisées via le catalogue de métriques.

explorateur de métriques

L'explorateur de métriques est un outil de configuration des graphiques de tableau de bord. Dans l' explorateur de mesures, vous pouvez ajouter plusieurs sources et mesures à un graphique et prévisualiser immédiatement l' affichage des données métriques.

Modbus

Modbus est un protocole de communication série utilisé dans l'automatisation industrielle .

MongoDB

MongoDB est une base de données de documents open-source qui fournit des performances, une disponibilité et une évolutivité.

Modules

Les modules offrent un ensemble de fonctionnalités du produit grâce à une combinaison de solutions, de composants et de services basés sur le cloud. Des modules sont disponibles pour la détection et la réponse réseau (NDR) et la surveillance des performances réseau (NPM), avec des modules supplémentaires pour les systèmes de détection d'intrusion (IDS) et l'analyse des paquets. Les administrateurs peuvent accorder aux utilisateurs un accès basé sur les rôles au module NDR, au module NPM ou aux deux.

MSMQ

MSMQ (Microsoft Message Queuing) est un protocole qui permet aux applications de s'envoyer des messages et des objets.

NaN

Acronyme pour « pas un chiffre ». Dans l'API Trigger, une propriété avec un type de données numérique s'affiche `NaN` si la valeur de la propriété n'est pas définie ou ne peut pas être représentée sous forme de nombre.

NAS

Le NAS (Network Attached Storage) est un référentiel de stockage au niveau des fichiers. Les clients peuvent accéder au référentiel via les protocoles SMB (Server Message Block) ou NFS (Network File System).

NBNS

NBNS ou NBT-NS (NetBIOS Name Service) est un système de dénomination pour les hôtes et les ressources du réseau.

NetFlow

Les technologies de flux telles que Netflow, IPFIX, sFlow et AppFlow collectent des données de trafic provenant de réseaux de flux extérieurs à votre source de données filaires et envoient les données à la sonde pour analyse.

Réseau

Dans le système ExtraHop, un réseau est le point d'entrée dans la capture du réseau, et des métriques sont collectées pour les attributs de capture du réseau, les alertes réseau et les détails du trafic réseau. Ces mesures fournissent un résumé de toutes les activités du réseau récupérées lors de la capture.

Octets du réseau

Un octet du réseau est une métrique qui affiche le débit du processus de capture ExtraHop .

Indicateurs de santé du réseau

(ExtraHop Reveal (x) uniquement) Les indicateurs de santé du réseau sont un ensemble de mesures qui vous montrent les tendances générales liées à l'état du réseau et à la sécurité. Les indicateurs de santé du réseau peuvent signaler des faiblesses ou des problèmes de performance du réseau ou des activités potentiellement suspectes. Ces statistiques se trouvent au bas de la page de présentation du réseau.

NFS

Le NFS (Network File System) est un protocole de système de fichiers distribué qui permet aux clients d'accéder aux fichiers d'un référentiel NAS (Network Attached Storage), généralement dans un environnement UNIX.

Nœud

Un espace de stockage des enregistrements ExtraHop individuel au sein d'un cluster.

Flux de données ouvert

Le service Open Data Stream (ODS) vous permet d'envoyer des données filaires à un système tiers distant, tel que MongoDB ou Kafka. Vous devez écrire un déclencheur pour identifier et collecter les données que vous souhaitez exporter et configurer les paramètres via les paramètres d'administration d' ExtraHop.

sonde de paquets

Une sonde danalysis de paquets collecte passivement une copie des données filaires non structurées (toutes les transactions sur votre réseau) et transforme ces données en données filaires structurées. Les capteurs permettent d'analyser et de visualiser toutes les données de votre réseau, de vos applications, de vos clients, de votre infrastructure et de votre entreprise. Les capteurs peuvent être connectés à une console ExtraHop pour une gestion centralisée et une vue unifiée des données collectées et stockées. Ils peuvent également être connectés à des magasins de disques et à des magasins de paquets pour un stockage supplémentaire et une analyse plus approfondie.

Paquets

La fonctionnalité Paquets vous permet de rechercher et de télécharger des paquets pour des transactions sélectionnées via une sonde ou une console. Cette fonctionnalité nécessite un stockage des paquets compatible.

Boutique de paquets

Un magasin de paquets ExtraHop collecte les paquets réseau bruts envoyés par une sonde de paquets connectée pour une récupération et un stockage à long terme. Les Packetstores vous permettent de récupérer rapidement tous les paquets correspondant à un ensemble de critères de recherche dans un intervalle de temps donné.

Participant

Les participants sont des terminaux qui participent en tant que délinquant ou victime à une détection.

Secret de transmission parfait (PFS)

Le Perfect Forward Secrecy (PFS) est une méthode de chiffrement qui permet des échanges de clés entièrement privées à court terme entre les clients et les serveurs. Vous pouvez octroyer une licence au système ExtraHop pour déchiffrer les sessions PFS SSL/TLS à partir des serveurs Windows sur lesquels le logiciel agent ExtraHop PFS est installé. Sans PFS, ces sessions ne pourraient pas être déchiffrées et les données issues de ces échanges seraient masquées.

PCAP

Le PCAP (capture de paquets) consiste en une interface de programmation d'applications (API) permettant de capturer le trafic réseau et de le stocker dans une base de données.

PCoIP

Le PCoIP (PC-over-IP) est un protocole qui transfère les pixels d'image compressés et chiffrés d'un serveur central vers un équipement PCoIP.

Diagramme circulaire

Ce graphique ExtraHop affiche les données métriques sous forme de portion ou de pourcentage d'un ensemble.

POP3

Le POP3 (Post Office Protocol) est un protocole standard au niveau de l' application qui transfère des messages électroniques entre un serveur et une application cliente via une connexion TCP.

Mise en miroir des ports

La mise en miroir de ports se produit lorsqu'un commutateur réseau envoie une copie des paquets réseau d'un port de commutateur (ou d'un VLAN complet) à une connexion de surveillance réseau sur un autre port de commutateur .

Protocole

Un protocole définit le format et l'ordre des messages échangés entre deux appareils ou plus, ainsi que les actions entreprises lors de la transmission et de la réception d'un message ou d'un autre événement.

Page de protocole

Une page de protocole est une page intégrée qui inclut des graphiques intégrés avec des indicateurs de haut niveau concernant vos actifs. Ces graphiques métriques peuvent être copiés dans vos tableaux de bord.

RDP

Le protocole RDP (Remote Desktop Protocol) est un protocole propriétaire de Microsoft permettant de communiquer entre un serveur hôte de session Remote Desktop et un client exécutant le logiciel Remote Desktop Connections. Le RDP est encapsulé et crypté dans le protocole TCP.

Enregistrer

Les enregistrements sont des informations structurées sur les flux et les transactions concernant les événements de votre réseau qui peuvent être envoyées à un espace de stockage des enregistrements compatible pour y être stockées. Vous pouvez ensuite rechercher des enregistrements à partir d'une sonde ou d'une console.

Format d'enregistrement

Un format dac.enregistrement est un schéma en lecture qui détermine la façon dont chaque enregistrement est affiché dans le système ExtraHop. Le système ExtraHop possède des formats d'enregistrement intégrés pour tous les types d'enregistrement intégrés, et bien que vous ne puissiez pas modifier un format d'enregistrement intégré, vous pouvez créer un format d'enregistrement personnalisé.

Types d'enregistrements

Les types d'enregistrement relient les enregistrements enregistrés au format d'enregistrement dans le système ExtraHop. Nécessite un espace de stockage des enregistrements compatible.

magasin de disques

Un espace de stockage des enregistrements collecte les enregistrements de transactions et de flux envoyés par une sonde connectée pour un stockage et une récupération à long terme. Vous pouvez consulter, enregistrer et rechercher les flux structurés et les informations de transaction concernant les événements de votre réseau à l'aide d'une interface utilisateur simple et unifiée, sans aucune modification de vos applications ou infrastructures existantes. Les magasins de disques ExtraHop sont disponibles sous forme de déploiements physiques ou virtuels ; le magasin d'enregistrements ExtraHop Cloud est fourni pour Reveal (x) 360 ; et les entrepôts de données tiers pris en charge incluent BigQuery et Splunk.

Redis

Redis est un serveur de structure de données open-source.

Région

Une région est tableau de bord composant contenant des widgets.

Délai de retransmission (RTO)

Un délai de retransmission (RTO) est une métrique du protocole TCP permettant de déterminer les performances du réseau . Les retransmissions TCP se produisent fréquemment sur le réseau. TCP lance un temporisateur de retransmission lorsqu'un segment sortant est transmis à une adresse IP. S'il n'y a aucun accusé de réception (ACK) avant l'expiration du délai, le segment est retransmis. Un RTO se produit lorsque l'expéditeur commence à manquer trop d'accusés de réception et arrête d'envoyer des segments pendant un certain temps. Les RTO peuvent représenter un délai de 1 à 5 secondes sur votre réseau. Plusieurs RTO au fil du temps peuvent entraîner des retards importants sur votre réseau.

Lisez le billet de blog d'ExtraHop : TCP RTOS : délais de retransmission et dégradation des performances des applications.

Révéler (x) 360

Reveal (x) 360 fournit une visibilité et une gestion basées sur le SaaS dans les environnements connectés sur site et dans le cloud. La console Reveal (x) 360 fournit une vue unique des données collectées par de multiples capteurs, magasins de paquets et magasins de disques, qui peuvent être distribuées dans les centres de données, les succursales et le cloud public.

Reveal (x) Enterprise

Reveal (x) Enterprise est une offre sur abonnement de produits ExtraHop qui incluent une sonde pour collecter les données de câblage et des composants supplémentaires en fonction du type de plan.

RFB

RFB (remote framebuffer) est un protocole d'accès à distance à une interface utilisateur graphique qui permet à un client de visualiser et de contrôler un système sur un autre ordinateur.

Score de risque

(ExtraHop Reveal (x) uniquement) Un indice de risque est un indicateur numérique de la gravité d'une détection . Les scores de risque sont basés sur plusieurs facteurs, tels que la position de la détection dans la chaîne dattaques, la vulnérabilité du protocole de détection et le niveau d'impact que la détection pourrait avoir sur le réseau. Le score est établi sur une échelle de 1 à 99, 99 étant le score le plus sévère.

RPC

Le MRPC (Microsoft Remote Procedure Call) est un mécanisme de communication permettant aux clients d'appeler une procédure à partir d'un programme situé sur un autre ordinateur, serveur ou réseau .

Capture de paquets à distance (RPCAP)

La capture de paquets à distance (RPCAP) est une implémentation logicielle pour le transfert de paquets similaire à une prise physique. Si vous souhaitez surveiller le trafic réseau pour les appareils qui ne sont pas directement connectés à votre flux de données filaire, vous pouvez transférer des paquets via le cloud et analyser ces données via le système ExtraHop.

RSPAN

L'analyseur de ports commutés à distance (RSPAN) permet de surveiller à distance plusieurs commutateurs sur un réseau commuté. Le RSPAN est un moyen de transférer le trafic d'une source SPAN sur un commutateur vers une destination SPAN sur un autre commutateur connecté via un tronc.

Note: RSPAN nécessite que les châssis source et de destination se trouvent dans le même domaine de couche 2.

RTCP

Le protocole RTCP (Real-time Transport Control Protocol) est un protocole qui surveille les statistiques relatives au streaming de données audio et vidéo transférées par le protocole RTP.

RTP

Le RTP (transport en temps réel) est un protocole qui définit le format de paquet normalisé pour le transfert en temps réel de flux audio et vidéo.

Journal de débogage

Le journal de débogage est un composant de l'éditeur de déclencheurs du système ExtraHop. Le journal de débogage affiche les exceptions et les résultats des instructions de débogage dans les scripts de déclencheur.

Type métrique de l'échantillon

Dans le système ExtraHop, ce type de métrique de niveau supérieur représente un résumé des données qui fournit une moyenne (moyenne) et un écart type sur une période spécifiée. Les métriques des ensembles d'échantillons résument généralement les données relatives à une métrique détaillée.

SDP

Le protocole SDP (Session Description Protocol) est un protocole qui définit les sessions de streaming multimédia.

capteur

Une sonde ExtraHop permet d'analyser et de visualiser toutes les données de votre réseau, de vos applications, de vos clients, de votre infrastructure et de votre entreprise. Une sonde d'analyse de paquets (ou EDA) collecte passivement une copie des données filaires non structurées (toutes les transactions de votre réseau) et transforme ces données en données filaires structurées. Un capteur de débit (ou EFC) collecte des données à partir des journaux de flux et n'est pris en charge que sur ExtraHop Reveal (x) 360. Les capteurs peuvent être connectés à une console ExtraHop pour une gestion centralisée et une vue unifiée des données collectées et stockées. Ils peuvent également être connectés à des magasins de disques et à des magasins de paquets pour un stockage supplémentaire et une analyse plus approfondie.

serveur

Un serveur est un système matériel dédié à l'hébergement d'un ou plusieurs services destinés aux utilisateurs ou aux clients du réseau. Dans le contexte du réseau IP (Internet Protocol), un serveur est un programme qui fonctionne comme un récepteur de socket.

SIP

Le protocole SIP (Session Initiation Protocol) est un protocole de signalisation qui contrôle les sessions de communication, telles que les appels vocaux pour les applications de téléphonie IP.

Site

Un site est un flux de données filaire analysé par le système ExtraHop qui représente une zone physique ou logique de votre réseau, telle qu'un centre de données, une succursale ou une charge de travail dans le cloud. Vous pouvez consulter les actifs, les détections et les autres données d'un site spécifique ou de plusieurs sites.

SMPP

Le SMPP (Short Messaging Peer-to-Peer) est un protocole au niveau de l'application qui transfère les données du service de messages courts (SMS) entre des entités de messagerie courte externes (ESME) et des centres de service de messages courts (SMSC).

SMTP

Le protocole SMTP (Simple Mail Transfer Protocol) est un protocole standard qui envoie, reçoit et relaie les messages électroniques entre les serveurs, les agents de transfert de courrier électronique et les applications clientes.

Type de métrique Snapshot

Dans le système ExtraHop, ce type de métrique de niveau supérieur représente un point de données qui représente un point unique dans le temps. Les métriques des instantanés incluent les ratios, les connexions actuelles et les connexions TCP établies.

SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole de couche 7 permettant de collecter , d'organiser, d'échanger et de modifier des informations sur les appareils gérés sur les réseaux IP.

La source

Les sources sont des ressources qui peuvent être attribuées à des graphiques, à des déclencheurs et à des alertes pour donner accès à des collections métriques.

SPAN

La mise en miroir de ports sur un commutateur Cisco Systems est généralement appelée Switched Port Analyzer (SPAN). SPAN copie le trafic et l'envoie vers une destination pour analyse du réseau.

SSH

Secure Shell (SSH) est un protocole qui transmet des informations de manière sécurisée sur un réseau.

SLL

Le protocole SSL (Secure Sockets Layer) est un protocole standard pour sécuriser les communications sur Internet. Pour établir un lien crypté entre un navigateur Web et un serveur, le serveur doit disposer d'un certificat SSL.

Analyse standard

Les enregistrements, les paquets, les détections, les cartes d'activité, l'activité des protocoles et les graphiques avec les mesures du débit et des paquets sont disponibles pour les appareils recevant une analyse standard. Ajustez les priorités d' analyse pour faire passer un équipement ou un point de terminaison d'une analyse standard à une analyse avancée .

Tableau de statut

Ce type de graphique ExtraHop affiche les valeurs métriques dans un graphique à colonnes, où la couleur des colonnes représente l'état et la gravité d'une alerte attribuée à la source et à la métrique sélectionnée dans le graphique.

STIX

(ExtraHop Reveal (x) uniquement) Structured Threat Information eXpression (STIX) est le langage et le format de sérialisation permettant de normaliser, de transmettre et de partager des données relatives aux données de renseignements sur les menaces cybernétiques. Le format STIX est généralement soutenu par la communauté et les plateformes de renseignements sur les menaces. Vous pouvez télécharger des fichiers STIX via le système ExtraHop ou l' API REST en tant que collecte des menaces personnalisée. Les collections de menaces personnalisées doivent être formatées dans STIX sous forme de fichiers TAR compressés, tels que .TGZ ou TAR.GZ.

Tableau graphique

Ce type de graphique ExtraHop affiche les valeurs métriques sur les lignes et les colonnes d'un tableau.

TAXI

TAXII (Trusted Automated Exchange of Intelligence Information) est un protocole permettant d' envoyer des renseignements sur les menaces via HTTPS.

TCP

Dans le système ExtraHop, les métriques TCP (Transmission Control Protocol) fournissent des informations sur le transfert fiable de paquets entre une source et une destination. Grâce aux métriques TCP, ExtraHop permet de savoir quels appareils sont connectés les uns aux autres, quand les appareils envoient des données, s'il y a des erreurs dans les données, par quels protocoles sont communiqués, etc.

TCP RST

Un paquet TCP RST est envoyé pour empêcher l'établissement d'une connexion TCP ou pour mettre fin de force à une connexion existante. Parfois, des réinitialisations sont envoyées lorsque l' équipement récepteur n'a pas réussi à ACK le paquet SYN ou qu'il n'a pas accusé réception d'un autre paquet envoyé et retransmis ultérieurement dans la transaction. Dans certains cas, les RST TRCP indiquent qu'une erreur s'est produite. Les volumes élevés de réinitialisations sortantes doivent être étudiés afin de déterminer s'ils correspondent à un comportement attendu ou s'ils indiquent un problème plus important.

Telnet

Telnet est un protocole de couche applicative pour les communications interactives orientées texte via une connexion de terminal virtuel.

Exposé sur les menaces

(ExtraHop Reveal (x) uniquement) Les briefings sur les menaces fournissent des conseils sur les menaces potentielles qui pèsent sur votre réseau, qu'il s'agisse d'événements de sécurité survenus à l'échelle du

secteur ou d'une analyse de votre réseau par apprentissage automatique. Les briefings sur les menaces peuvent inclure la détection de scans, d'exploits et d' indicateurs de compromission (IOC) liés à la menace.

Collecte des menaces

(ExtraHop Reveal (x) uniquement) Une collecte de menaces est un ensemble de données d' adresses IP, de noms d'hôtes et d'URI suspects qui permet à votre système Reveal (x) d'identifier les indicateurs de compromission et d'afficher les renseignements sur les menaces dans les graphiques et les enregistrements du système.

Renseignements sur les menaces

Les renseignements sur les menaces sont des données connues sur les adresses IP, les noms d'hôte et les URI suspects qui peuvent aider à identifier les risques pour votre entreprise. Ces ensembles de données, appelés collections de menaces, sont disponibles par défaut dans votre système Reveal (x) et auprès de sources gratuites et commerciales de la communauté de la sécurité.

sélecteur de temps

Le sélecteur de temps est un outil qui vous permet de spécifier un intervalle de temps pour la collecte et la présentation des données réseau dans le système ExtraHop. Il existe deux types de sélecteurs de temps : un sélecteur de temps global pour spécifier des intervalles de temps globaux et un sélecteur de temps de région pour spécifier les intervalles de temps régionaux dans un tableau de bord.

Horodatage

Un horodateur est un enregistrement numérique de l'heure à laquelle un événement particulier s'est produit. Dans le système ExtraHop, vous pouvez sélectionner l'horodateur par défaut ou configurer des horodatages externes tels que Gigamon ou Anue via le fichier de configuration en cours d'exécution.

Tinygram

Un tinygram est un petit paquet ou un segment TCP. Un tinygram est un paquet dont la charge utile est inférieure aux données d'en-tête de trame (L2-L4). En général, les tinygrams entraînent des ratios inefficaces entre les données d'en-tête de trame et les informations réellement utiles transitant sur le réseau. Les tinygrams peuvent contribuer à la congestion du réseau.

Lisez le billet de blog d'ExtraHop : Qu'est-ce qu'un Tinygram ?

Mesure métrique de haut niveau

Une métrique de haut niveau, ou métrique de base, vous donne une somme de données pour une période spécifiée. Les indicateurs de haut niveau vous fournissent une vue d'ensemble qui vous permet d'identifier ce qui se passe sur votre réseau. Vous pouvez ensuite accéder à une métrique de niveau supérieur pour afficher les métriques détaillées. Il existe différents types de mesures de haut niveau qui fournissent différentes informations, notamment le nombre, le jeu de données, le maximum, le sampleset et les types de mesures instantanés. Comprendre les types de métriques est essentiel pour écrire des déclencheurs et configurer des graphiques.

Top Set

Un topnset correspond aux 1 000 meilleures paires clé-valeur calculées pour l'intervalle de temps que vous spécifiez dans le sélecteur de temps. Un topnset n'est pas un ensemble de données complet car il ne représente que les valeurs-clés enregistrées pour un cumul d'agrégation spécifique (sur la base d'un intervalle de temps spécifié) et est limité à 1 000 clés par topnset.

Gâchette

Les déclencheurs sont des scripts personnalisés qui exécutent une action sur un événement prédéfini. Par exemple, vous pouvez écrire un déclencheur pour enregistrer une métrique personnalisée à chaque fois qu'une requête HTTP se produit, ou pour classer le trafic d'un serveur spécifique en tant que serveur dapplications.

Pour plus d'informations, consultez le Référence de l'API Trigger.

Réglage

Processus par lequel les détections de faible valeur sont supprimées d'une liste de détection. Une détection peut être réglée par un paramètre de réglage qui empêche la génération de la détection ou par une règle de réglage qui masque la détection en fonction du type de détection, des participants ou des propriétés de détection.

Tableau des valeurs

Ce graphique ExtraHop affiche la valeur totale d'une ou de plusieurs métriques. La sélection de plusieurs mesures affichera les valeurs métriques côte à côte.

Perte de paquets virtuels

La perte de paquets virtuels (VPL) fait référence à un phénomène qui affecte les applications totalement ou partiellement virtualisées. Le VPL crée des symptômes qui suggèrent une congestion du réseau et n'est souvent pas détecté par les outils traditionnels de surveillance du réseau et de gestion des performances des applications (APM). La VPL se produit lorsqu'un hyperviseur planifie le temps processeur pour un nombre excessif de machines virtuelles (VM) et empêche ces machines virtuelles de répondre assez rapidement aux accusés de réception TCP. Le VPL peut être détecté en combinant la connaissance des applications et une analyse TCP avancée.

VLAN

Un réseau local virtuel (VLAN) est un regroupement logique de trafic ou de périphériques sur un réseau. Les informations VLAN sont extraites des balises VLAN, si le processus de mise en miroir du trafic préserve les balises sur le port miroir.

Scanner de vulnérabilités

Les scanners de vulnérabilité sont des programmes qui recherchent des faiblesses dans les applications, les systèmes et les réseaux. Dans le système ExtraHop, un équipement qui envoie des requêtes HTTP associées à une activité de scanner connue se voit attribuer le rôle de scanner de vulnérabilités. Vous pouvez également désigner manuellement un équipement en tant que scanner en modifiant le rôle de l'équipement en Vulnerability Scanner.

Liste de surveillance

Les appareils individuels de la liste de surveillance bénéficient de la garantie Analyse avancée. En règle générale, les appareils de grande valeur sont ajoutés à la liste de surveillance. L'Analyse avancée est un niveau d'analyse dans lequel les enregistrements, les paquets, les cartes d'activité et les graphiques contenant des mesures du protocole L2-L7 sont disponibles pour les appareils. Vous pouvez supprimer des appareils de la liste de surveillance à tout moment.

Widget

Les widgets sont configurables tableau de bord composants qui peuvent être ajoutés à une région pour différentes fonctions. Les types de widgets sont les suivants : graphique, zone de texte, alerte, groupes d' activités et réseaux (consoles uniquement).

Données de câblage

Les données filaires sont créées lorsque les données en vol sont analysées lorsque le trafic est envoyé sur le réseau. Grâce à un traitement complet en temps réel, les données non structurées sont réassemblées en Wire Data structurées qui peuvent être analysées en temps réel. Les données filaires comprennent les données L2-L7 qui couvrent l'ensemble de la chaîne de livraison des applications et fournissent la visibilité la plus complète et la plus étendue.

WMI

WMI (Windows Management Instrumentation) est un ensemble d' extensions système Windows qui fournit une interface de système d'exploitation pour établir des sessions d'accès à distance.

WMAN

Le protocole WSMAN (Web Services Management) est une norme publique pour l' échange de données avec n'importe quel équipement informatique.

taille de fenêtre à zéro

Une taille de fenêtre à zéro est une métrique TCP du système ExtraHop qui mesure la congestion des applications . Lorsqu'un équipement annonce un message de taille de fenêtre à l'expéditeur pendant le transfert de données, cela signifie que l'équipement ne peut plus accepter de données car la fenêtre de réception de l'équipement (une mémoire tampon pour les données entrantes) est pleine. Le message de taille de fenêtre à zéro indique à l'expéditeur de suspendre le transfert de données jusqu'à nouvel ordre.