Häufig gestellte Fragen zur gemeinsamen Bedrohungsanalyse

Veröffentlicht: 2023-09-13

Was ist kollektive Bedrohungsanalyse?

Die kollektive Bedrohungsanalyse ermöglicht es Benutzern, ausgewählte Daten mit ExtraHop zu teilen , um die Genauigkeit von Erkennungen zu verbessern, wie z. B. Command-and-Control (C&C) Beaconing.

Standardmäßig werden alle an den ExtraHop Cloud Service gesendeten Daten, die einen Netzwerkteilnehmer eindeutig identifizieren könnten (z. B. eine IP-Adresse oder ein Benutzername), mit einem Schlüssel verschlüsselt, der auf dem Sensor und auf die ExtraHop keinen Zugriff hat.

Reveal (x) Enterprise-Benutzer können Daten an den Machine Learning Service senden, indem sie ExtraHop Cloud Services in den Administrationseinstellungen aktivieren. Das System kann beispielsweise externe Klartext-IP-Adressen, Domainnamen und Hostnamen senden, die mit dem erkannten verdächtigen Verhalten in Verbindung stehen. Diese Einstellung ist in Reveal (x) 360 standardmäßig aktiviert und kann nicht deaktiviert werden. Eine vollständige Liste der Datentypen, die an den ExtraHop Machine Learning Service gesendet werden, und Informationen darüber, wie die Daten zur Verbesserung der Bedrohungserkennung verwendet werden, finden Sie im Abschnitt Machine Learning der Überblick über Sicherheit, Datenschutz und Vertrauen bei ExtraHop.

Indem Sie sich für die Weitergabe dieser Klartextdaten entscheiden, tragen Sie zu einem großen Community-Datensatz bei, der zum Nutzen aller analysiert werden kann — insbesondere zu Ihrem eigenen. Dieser Datensatz enthält sowohl Klartextdaten als auch anonymisierte Metadaten im Zusammenhang mit Bedrohungen, die von ExtraHop erkannt wurden.

Wie sicher sind meine Daten?

Wenn du Opt-In, um ExtraHop die externen Klartext-IP-Adressen, Hostnamen und Domainnamen zu senden Der ExtraHop-Sensor wird in Ihrem Netzwerk beobachtet und sendet diese Metadaten über TLS 1.2- oder TLS 1.3-Verbindungen und Perfect Forward Secrecy (PFS) an den Machine Learning Service. Sowohl übertragene als auch ruhende Daten werden sicher in einem verschlüsselten, hochgeschützten Datenspeicher gespeichert.

In der Übersicht über Sicherheit, Datenschutz und Vertrauen von ExtraHop erfahren Sie mehr darüber, wie ExtraHop Ihre Daten schützt.

Warum sollte ich mich anmelden?

Hier sind die Möglichkeiten, wie Sie davon profitieren, zur kollektiven Forschung und Analyse beizutragen.

Verbessern Sie den Kontext Ihrer Erkennungen

Das cloudbasierte maschinelle Lernen von ExtraHop kann Klartextdaten bei der Analyse verdächtigen Verhaltens nutzen. Umfangreiche Daten ermöglichen Erkennungen mit höherer Zuverlässigkeit.

Nehmen wir zum Beispiel die Website eines lokalen Coffeeshops mit schlecht konfigurierter Webanalyse. Diese Website kontaktiert häufig einen externen Analyseserver mit Leistungsstatistiken. Der Webseiten-Traffic kann in Ihrem Netzwerk während eines 30-sekündigen Rapid Beacons erkannt werden — ein Verhalten, das auch häufig bei bösartigen Command-and-Control (C&C) -Beacons beobachtet wird. Durch den Zugriff auf den externen Klartext-Hostnamen und die IP-Adresse des Analyseservers, der mit der Erkennung verknüpft ist, kann das ExtraHop-System jedoch besser feststellen, ob das Rapid Beaconing mit einer bekannten bösartigen Quelle verknüpft ist. Der verbesserte Kontext hilft ExtraHop, Sie darüber zu informieren, wenn der Traffic bösartig ist, und reduziert Fehlalarme.

Helfen Sie dabei, neuartige Angriffe auf Ihr Netzwerk zu stoppen

ExtraHop führt Big-Data-Analysen durch, um nach heimlichen und fortschrittlichen Angriffen zu suchen, die einzelne Unternehmen möglicherweise übersehen. Der gesamte Kundenstamm wird automatisch und sofort vor jeder neu identifizierten Bedrohung geschützt.

ExtraHop könnte beispielsweise beobachten, dass Geräte in mehreren Netzwerken umgekehrte SSH-Tunnel zu einer verdächtigen IP-Adresse einrichten. Bei weiterer Analyse scheint die verdächtige IP-Adresse einen C&C-Server zu hosten, der Verhaltensweisen zeigt, die zuvor mit einer bekannten Bedrohungsgruppe in Verbindung gebracht wurden. ExtraHop aktualisiert sofort alle bereitgestellten Sensoren mit Erkennungen zum Schutz aller mit der Cloud verbundenen Bereitstellungen vor der neu identifizierten Bedrohung.

Verbessern Sie Modelle für maschinelles Lernen in Ihren Erkennungen

ExtraHop nutzt Daten aus der Community, um Algorithmen für maschinelles Lernen zu trainieren und neue Modelle für maschinelles Lernen zu entwickeln, die darauf ausgelegt sind, Angriffe auf Benutzernetzwerke zu erkennen. Wir verfeinern auch unser Verständnis von gutartigen Verhaltensmustern, indem wir beobachten, wie sich Verhaltensweisen in Netzwerken verschiedener Branchen, Größen und geografischer Standorte manifestieren.

Kann ich mich abmelden?

In den Sensoren von Reveal (x) Enterprise können Sie die Standardeinstellung deaktivieren, die eine kollektive Bedrohungsanalyse ermöglicht.

Detektoren, die die kollektive Bedrohungsanalyse unterstützen, zeigen allen Benutzern in den Ansichten Nach Erkennungstyp gruppieren und Erkennungsdetails eine Erinnerungsbenachrichtigung an. Administratoren können sich dafür entscheiden, die Produkterinnerungen auszublenden.

Die folgenden Einstellungen sind verfügbar:

- Tragen Sie externe IP-Adressen, Domainnamen und Hostnamen für die kollektive Bedrohungsanalyse bei
- Tragen Sie nicht zur kollektiven Bedrohungsanalyse bei
- Tragen Sie nicht zur kollektiven Bedrohungsanalyse bei und zeigen Sie keine Produkterinnerungen an