Häufig gestellte Fragen zur kollektiven Gefahrenanalyse

Veröffentlicht: 2024-08-07

Was ist kollektive Bedrohungsanalyse?

Mithilfe der kollektiven Bedrohungsanalyse können Benutzer ausgewählte Daten mit ExtraHop teilen, um die Genauigkeit von Erkennungen wie Command-and-Control (C&C) Beaconing zu verbessern und neue Erkennungen zu generieren, z. B. die Identifizierung bösartige Datei Datei-Hashes.

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.

RevealX Enterprise-Benutzer können Daten an den Machine Learning Service senden, indem sie ExtraHop Cloud Services aktivieren und sich in den Administrationseinstellungen für die kollektive Bedrohungsanalyse entscheiden. Das System kann beispielsweise Domainnamen, Hostnamen, Datei-Hashes und externe IP-Adressen senden. Diese Einstellung ist in revealX360 standardmäßig aktiviert und kann nicht deaktiviert werden. Eine vollständige Liste der an den ExtraHop Machine Learning Service gesendeten Datentypen und Informationen darüber, wie die Daten zur Verbesserung der Bedrohungserkennung verwendet werden, finden Sie im Abschnitt Maschinelles Lernen der Überblick über Sicherheit, Datenschutz und Vertrauen bei ExtraHop.

Indem Sie sich dafür entscheiden, diese Klartext-Daten zu teilen, 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 zu Bedrohungen, die von ExtraHop erkannt wurden.

Wie sicher sind meine Daten?

Wenn du Melden Sie sich für eine kollektive Bedrohungsanalyse an Der ExtraHop-Sensor sendet diese Metadaten über TLS 1.2- oder TLS 1.3-Verbindungen und Perfect Forward Secrecy (PFS) an den Machine Learning Service. Sowohl Daten während der Übertragung als auch Daten im Ruhezustand werden sicher in einem verschlüsselten, hochgeschützten Datenspeicher gespeichert.

Weitere Informationen darüber, wie ExtraHop Ihre Daten schützt, finden Sie in der Überblick über Sicherheit, Datenschutz und Vertrauen bei ExtraHop.

Warum sollte ich mich anmelden?

Hier sind die Möglichkeiten, wie Sie von einem Beitrag zur kollektiven Forschung und Analyse profitieren.

Verbessern Sie den Kontext Ihrer Erkennungen

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

Nehmen wir zum Beispiel die Website eines lokalen Coffeeshops , das über schlecht konfigurierte Webanalysen verfügt. Diese Website wendet sich häufig an einen externen Analyseserver mit Leistungsstatistiken. Der Webseiten-Traffic könnte in Ihrem Netzwerk erkannt werden, wenn es 30 Sekunden lang Rapid Beacons sendet — ein Verhalten, das auch häufig bei bösartigen Command-and-Control-Beacons (C&C) beobachtet wird. Durch den Zugriff auf den externen Klartext-Hostnamen und die IP-Adresse des Analyseservers, die mit der Erkennung verknüpft sind, kann das ExtraHop-System jedoch besser feststellen, ob das Rapid Beaconing an eine bekannte bösartige Quelle gebunden ist. Ein verbesserter Kontext hilft ExtraHop, Ihnen mitzuteilen, wann 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 Reverse-SSH-Tunnel zu einer verdächtigen IP-Adresse einrichten. Bei einer weiteren 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 Machine-Learning-Modelle bei 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.

Was ist der Unterschied zwischen erweiterter Bedrohungsanalyse und kollektiver Bedrohungsanalyse?

Daten, die zur kollektiven Bedrohungsanalyse gesendet werden, werden einem anonymisierten Datenpool hinzugefügt und untersucht, um die Erkennung durch maschinelles Lernen zu verbessern, neue Angriffstypen zu identifizieren, bösartige Datei-Hashes zu erkennen und die Genauigkeit vorhandener Erkennungen zu verbessern. Daten geteilt mit erweiterte Bedrohungsinformationen wird sofort mit einer erweiterten Sammlung von Bedrohungsinformationen verglichen und dann verworfen.

Beide Dienste werden in RevealX 360 automatisch aktiviert, aber RevealX Enterprise-Administratoren müssen sich in den Administrationseinstellungen anmelden.

Kann ich mich abmelden?

In den RevealX Enterprise-Sensoren können Sie die Standardeinstellung deaktivieren, die eine kollektive Bedrohungsanalyse ermöglicht.

Melder, die eine kollektive Bedrohungsanalyse unterstützen, zeigen allen Benutzern eine Erinnerungsbenachrichtigung in den Ansichten Nach Entdeckungstyp gruppieren und Entdeckungsdetails an. Administratoren können sich dafür entscheiden, die produktinternen Erinnerungen auszublenden.

Die folgenden Einstellungen sind verfügbar:

- Tragen Sie Domainnamen, Hostnamen, Datei-Hashes und externe IP-Adressen zur kollektiven Bedrohungsanalyse bei
- Tragen Sie nicht zur kollektiven Bedrohungsanalyse bei
- Tragen Sie nicht zur kollektiven Bedrohungsanalyse bei und zeigen Sie keine produktinternen Erinnerungen an