Häufig gestellte Fragen zu erweiterten Bedrohungsinformationen

Veröffentlicht: 2024-08-07

Was ist erweiterte Bedrohungsinformationen?

Dank erweiterter Bedrohungsinformationen können Benutzer ausgewählte Daten mit ExtraHop teilen, um sie anhand einer größeren Sammlung von CrowdStrike-Bedrohungsindikatoren, gutartigen Endpunkten und anderen Netzwerkverkehrsinformationen zu überprüfen. Die Überprüfung der Daten anhand einer erweiterten Informationsbibliothek führt zu einer besseren Identifizierung bösartiger Endpunkte, einer verbesserten Erkennungsgenauigkeit und einer kontextbezogenen Anreicherung der Erkennungsinformationen, um eine schnelle und fundierte Bewertung von Erkennungen zu ermöglichen.

RevealX Enterprise-Benutzer müssen diesen Dienst aktivieren, indem sie ExtraHop Cloud Services aktivieren und in den Administrationseinstellungen erweiterte Bedrohungsinformationen aktivieren. Nach der Aktivierung kann das System auf Ihrem System beobachtete IP-Adressen, Domainnamen, Hostnamen, Datei-Hashes und URLs senden, um sie in Echtzeit anhand einer größeren Sammlung von Bedrohungsinformationen zu überprüfen. Diese Einstellung ist in revealX360 standardmäßig aktiviert und kann nicht deaktiviert werden. Eine vollständige Liste der Datentypen, die an ExtraHop Cloud Services gesendet werden, und um zu erfahren, wie die Daten zur Verbesserung der Bedrohungserkennung verwendet werden, finden Sie im Abschnitt Maschinelles Lernen von.

Wie sicher sind meine Daten?

Wenn du Melden Sie sich für erweiterte Bedrohungsinformationen an, sendet der ExtraHop-Sensor diese Metadaten über TLS 1.2- oder TLS 1.3-Verbindungen und Perfect Forward Secrecy (PFS) an ExtraHop Cloud Services. IP-Adressen, Domainnamen, Hostnamen, Datei-Hashes und URLs, die für erweiterte Bedrohungsinformationen an Cloud Services gesendet werden, werden sofort überprüft und dann verworfen.

Mehr darüber, wie ExtraHop Ihre Daten schützt, erfahren Sie in der Überblick über Sicherheit, Datenschutz und Vertrauen bei ExtraHop.

Warum sollte ich mich anmelden?

Hier sind die Möglichkeiten, wie Sie von erweiterten Bedrohungsinformationen profitieren können.

Die Macht der Cloud-Verarbeitung

Das cloudbasierte maschinelle Lernen von ExtraHop bietet Verarbeitungsmöglichkeiten, die weit über die Kapazität einzelner Sensoren hinausgehen. Wenn Sie sich für erweiterte Bedrohungsinformationen entscheiden, eröffnet sich eine riesige Bibliothek von Bedrohungsindikatoren, die auf Sensorebene nicht effizient angewendet werden konnten, aber mit der Rechenleistung der ExtraHop-Cloud-Ressourcen in Echtzeit verarbeitet werden können.

Zusätzliche CrowdStrike-Berichterstattung

Das ExtraHop-System bietet hochwertige Bedrohungssammlungen von CrowdStrike als Standardkomponente der integrierten Bedrohungsinformationen. Aufgrund von Verarbeitungseinschränkungen gibt es einen großen Rest der CrowdStrike-Intelligenz, der nicht in Sensoren enthalten sein kann. Wenn Sie sich für erweiterte Bedrohungsinformationen entscheiden, profitieren Sie von der zusätzlichen Rechenleistung der ExtraHop Cloud Services und ermöglichen eine viel größere Sammlung von CrowdStrike-Indikatoren, die Sie anhand Ihres Netzwerkverkehrs überprüfen können.

Mehr Informationen jetzt, weniger Untersuchung später

Bei der Bedrohungsanalyse geht es nicht nur darum, verdächtige IP-Adressen oder bösartige Datei-Hashes zu identifizieren. Es geht auch darum, Verkehr, der nicht verdächtig ist, schnell zu identifizieren. ExtraHop nutzt Netzwerkdaten, um gutartige Netzwerkaktivitäten zu klassifizieren

und das Geräusch harmloser Aktivitäten aus den Ermittlungsabläufen zu entfernen. Durch die Nutzung erweiterter Bedrohungsinformationen kann ExtraHop anhand einer möglichst großen Sammlung von Bedrohungsindikatoren und gutartigen Verhaltensmustern filtern, was Analysten sehen werden, und nur hochwertige, umsetzbare Informationen präsentieren.

Was ist der Unterschied zwischen erweiterter Bedrohungsanalyse und kollektiver Bedrohungsanalyse?

Daten gesendet an kollektive Bedrohungsanalyse wird einem anonymisierten Datenpool hinzugefügt und untersucht, um die Erkennung durch maschinelles Lernen zu verbessern, neue Angriffstypen zu identifizieren, Erkennungen für bösartige Datei-Hashes zu generieren und die Genauigkeit vorhandener Erkennungen zu verbessern. Daten, die mit Extended Threat Intelligence geteilt werden, werden sofort mit einer erweiterten Sammlung von Bedrohungsinformationen verglichen und anschließend verworfen.

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

Kann ich mich abmelden?

Dieser Dienst ist in revealX360 standardmäßig aktiviert und kann nicht deaktiviert werden. RevealX Enterprise-Systeme sind standardmäßig von der erweiterten Bedrohungsanalyse ausgeschlossen und können den Dienst in den Administrationseinstellungen aktivieren.

Die folgenden Einstellungen sind verfügbar:

- Ich bin damit einverstanden, IP-Adressen, Domainnamen, Hostnamen, Datei-Hashes und URLs an ExtraHop Cloud Services zu senden.
- Ich möchte keine IP-Adressen, Domainnamen, Hostnamen, Datei-Hashes und URLs an ExtraHop Cloud Services senden und verstehe, dass meine Daten nicht mit der vollständigen Sammlung von Bedrohungsinformationen verglichen werden.

Werden durch die Abmeldung alle auf Bedrohungsinformationen beruhenden Erkennungen gestoppt?

Nein. Wenn Sie die erweiterte Bedrohungsanalyse deaktivieren, wird nur verhindert, dass Ihre Daten mit einer vollständigen Sammlung von Bedrohungsinformationen verglichen werden. Netzwerkdaten werden weiterhin anhand von Bedrohungsinformationen aus lokalen Quellen überprüft, einschließlich integrierter Bedrohungssammlungen, hochgeladener STIX-Dateien und TAXII-Feeds. Beispielsweise werden Sie weiterhin Erkennungen sehen, die auf den integrierten CrowdStrike-Bedrohungssammlungen basieren.