Übermitteln Sie einen benutzerdefinierten Datensatz, um verdächtige Portaktivitäten zu überwachen

Veröffentlicht: 2023-09-14

Die ExtraHop-Plattform kann Ihnen dabei helfen, Transparenz und Echtzeitzugriff auf frühe Angriffsindikatoren in Ihrem Netzwerk zu erlangen. Eine proaktive Sicherheitsmaßnahme, die Sie ergreifen können, ist die Überwachung von Ports, die Sie für anfällig für Trojaner und andere Malware halten.

Da 12345 beispielsweise eine leicht zu merkende Sequenz ist, wird diese Nummer häufig bei der Konfiguration einer Standard-Portnummer für einen Server oder ein Programm ausgewählt, sodass dieser Portwert ein beliebtes Ziel für Angreifer ist.

In dieser exemplarischen Vorgehensweise schreiben Sie einen Auslöser, der jede Transaktion über einen verdächtigen Portwert in einen Datensatz festschreibt. Anschließend erstellen Sie eine Abfrage, um die gesammelten Datensätze anzuzeigen.

Voraussetzungen

- Sie benötigen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto, das über System- und Zugriffsadministrationsrechte verfügt.
- Ihr ExtraHop-System muss mit einem Recordstore verbunden sein.
- Ihr Netzwerk muss so konfiguriert sein, dass Verkehr über Port 12345 zugelassen wird.
- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie die Rekorde und Auslöser.
- Machen Sie sich mit den Prozessen zur Erstellung von Triggern vertraut, indem Sie die Komplettlösung für Trigger.

Schreiben Sie den Auslöser

In den folgenden Schritten schreiben Sie einen Auslöser, der nach Serververkehr über Port 12345 sucht und dann einen benutzerdefinierten Datensatz jeder Transaktion in einen Recordstore.

1. Melden Sie sich bei einem ExtraHop-System an, das mit einem Recordstore verbunden ist.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Auslöser**.
3. klicken **Erstellen**.
4. In der Name Feld, Typ `Verdächtige Port-Aktivität`.
5. In der Ereignisse Feld, wählen **FLOW_CLASSIFY**.
6. Fügen Sie im rechten Bereich den folgenden Triggercode zum Editor hinzu:

```
if (Flow.server && Flow.server.port === 12345) {
    commitRecord('Trojan', {
        description: 'Possible NetBus or other trojan',
        protocol:Flow.l7proto
    });
}
```

   Um alle Transaktionen über den Port zu erfassen, ruft der Auslöser die Flow-Klasse auf. Der Auslöser gibt „Trojan“ als Datensatztyp an und fügt dem Datensatzinhalt zwei Eigenschaften hinzu: eine Beschreibung und das Protokoll der Transaktion, falls bekannt.
7. klicken **Speichern**.

8. klicken **Erweiterte Optionen anzeigen** und wählen Sie dann **Allen Geräten zuweisen**.

   Wichtig: Wenn Sie Ihre eigenen Trigger erstellen, weisen Sie Trigger nur den Geräten zu, von denen Sie Messwerte sammeln müssen, um die Leistungseinbußen Ihrer Trigger auf das ExtraHop-System zu minimieren.

9. klicken **Speichern und schließen**, und lassen Sie den Auslöser dann mindestens zehn Minuten lang laufen.

Abfragen und Anzeigen der benutzerdefinierten Datensätze

In den folgenden Schritten suchen Sie nach den benutzerdefinierten Datensätzen, die an den Recordstore übergeben wurden, und erstellen eine gespeicherte Datensatzabfrage auf der Grundlage der Suchkriterien.

1. Klicken Sie in der obersten Navigationsleiste auf **Rekorde**.
2. Aus dem **Beliebiger Datensatztyp** Drop-down-Menü, wählen **Trojanische**.
3. klicken **Aufzeichnungen ansehen**.
4. Aus dem **Felder** Drop-down-Menü, wählen **Alles auswählen**.
5. Klicken Sie auf **Ausführliche Ansicht**  Ikone.
   Im Inhaltsbereich werden die benutzerdefinierten Datensatzfelder angezeigt. Zusätzlich zu den im Auslöser angegebenen Beschreibungs- und Protokollfeldern enthält der Datensatz die folgenden Eigenschaften:

   - Flow-ID
   - Client
   - Kundenadresse
   - Client-Port
   - Server
   - Server-AddR
   - Server-Port

6. Klicken Sie auf **Speichern** Symbol 🖫 von oben rechts auf der Seite.
7. In der Name Feld, Typ `Mögliche Trojaner`, und klicken Sie **Speichern**.

Überprüfen Sie die Aufzeichnungen Malware Malware-Indikatoren

Wenn Ihr System von einem Malware-Angriff betroffen ist oder Sie von neuer Malware erfahren, die im Umlauf ist, können Sie in Ihren Aufzeichnungen nachsehen, ob Ihr System angegriffen wurde.

Wenn Sie beispielsweise erfahren, dass ein neuer Trojaner häufig über Port 12345 gesendet wird, können Sie die gespeicherte Abfrage Mögliche Trojaner öffnen, die Sie oben erstellt haben, und nach der folgenden Aktivität suchen:

- Transaktionen, die über unerwartete Protokolle erfolgen. Sie könnten beispielsweise erwarten, dass IMAP-Verkehr über Port 12345 angezeigt wird, aber kein SSH-Verkehr.
- Transaktionen, die über nicht klassifizierte Protokolle erfolgen und in den Abfrageergebnissen als tcp:12345 angezeigt werden. Nicht klassifizierte Protokolle werden vom ExtraHop-System nicht erkannt und können verdächtig sein .
- Client-IP-Adressen, die mit Transaktionen über unerwartete oder nicht klassifizierte Protokolle verknüpft sind, und wenn die IP-Adresse aus einem nicht vertrauenswürdigen Gebietsschema stammt.
- Zeitstempel der Transaktionen, die Sie für fragwürdig halten und die außerhalb der Geschäftszeiten stattfanden.

Durch die Eingrenzung verdächtiger Transaktionen können Sie feststellen, ob Sie ein Malware-Problem haben , sodass Sie mit der Lösung beginnen können.