Audit-Log-Daten an einen Remote-Syslog-Server senden

Veröffentlicht: 2024-04-09

Das Audit-Log sammelt Daten über den Betrieb des ExtraHop-Systems, aufgeschlüsselt nach Komponenten. Das im System gespeicherte Protokoll hat eine Kapazität von 10.000 Einträgen, und Einträge, die älter als 90 Tage sind, werden automatisch entfernt. Sie können diese Einträge in den Administrationseinstellungen anzeigen oder die Audit-Log-Ereignisse zur Langzeitspeicherung, Überwachung und erweiterten Analyse an einen Syslog-Server senden. Alle protokollierten Ereignisse sind in der folgenden Tabelle aufgeführt.

Die folgenden Schritte zeigen Ihnen, wie Sie das ExtraHop-System so konfigurieren, dass Audit-Log-Daten an einen Remote-Syslog-Server gesendet werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Status und Diagnose auf **Prüfprotokoll**.
3. Klicken **Syslog-Einstellungen konfigurieren**.
4. Geben Sie im Feld Ziel die IP-Adresse des Remote-Syslog-Servers ein.
5. Wählen Sie im Dropdownmenü Protokoll **TCP** oder **UDP**. Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.
6. Geben Sie im Feld Port die Portnummer für Ihren Remote-Syslog-Server ein. Standardmäßig ist dieser Wert auf 514 festgelegt.
7. Klicken **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind. Wenn die Einstellungen korrekt sind, sollten Sie in der Syslog-Log-Datei auf dem Syslog-Server einen Eintrag sehen, der dem folgenden ähnelt:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

8. Klicken **Speichern**.
9. Optional: Ändern Sie das Format von Syslog-Meldungen.

   Standardmäßig entsprechen Syslog-Meldungen nicht RFC 3164 oder RFC 5424. Sie können Syslog-Meldungen jedoch so formatieren, dass sie konform sind, indem Sie die laufende Konfiguration ändern.

   a) Klicken **Admin**.
   b) Klicken **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken **Konfiguration bearbeiten**.
   d) Füge einen Eintrag hinzu unter `auditlog_rsyslog` wo der Schlüssel ist `rfc_compliant_format` und der Wert ist entweder `rfc5424` oder `rfc3164`.

      Das `auditlog_rsyslog` Der Abschnitt sollte dem folgenden Code ähneln:

      ```
      "auditlog_rsyslog": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```

   e) Klicken **Aktualisieren**.
   f) Klicken **Erledigt**.
10. Optional: Ändern Sie die Zeitzone, auf die in den Syslog-Zeitstempeln verwiesen wird.

    Standardmäßig verweisen Syslog-Zeitstempel auf die UTC-Zeit. Sie können Zeitstempel jedoch so ändern, dass sie auf die ExtraHop-Systemzeit verweisen, indem Sie die laufende Konfiguration ändern.

a) Klicken **Admin**.
b) Klicken **Config ausführen (ungespeicherte Änderungen)**.
c) Klicken **Konfiguration bearbeiten**.
d) Füge einen Eintrag hinzu unter `auditlog_rsyslog` wo der Schlüssel ist `syslog_use_localtime` und der Wert ist `true`.

   Das `auditlog_rsyslog` Der Abschnitt sollte dem folgenden Code ähneln:

```
"auditlog_rsyslog": {
    "syslog_destination": "192.168.0.0",
    "syslog_ipproto": "udp",
    "syslog_port": 514,
    "syslog_use_localtime": true
}
```

e) Klicken **Aktualisieren**.
f) Klicken **Erledigt**.

Nächste Schritte
Nachdem Sie bestätigt haben, dass Ihre neuen Einstellungen erwartungsgemäß funktionieren, behalten Sie Ihre Konfigurationsänderungen bei, indem Sie die laufende Konfigurationsdatei speichern.

Audit-Log-Ereignisse

Die folgenden Ereignisse auf einem ExtraHop-System generieren einen Eintrag im Audit-Log.

Kategorie	Ereignis
Vereinbarungen	• Eine EULA- oder POC-Vereinbarung wird vereinbart
API	• Ein API-Schlüssel wird erstellt • Ein API-Schlüssel wird gelöscht • Ein Benutzer wird erstellt. • Ein Benutzer wird geändert.
Sensormigration	• Eine Sensormigration wird gestartet • Eine Sensormigration war erfolgreich • Eine Sensormigration ist fehlgeschlagen
Browsersitzungen	• Eine bestimmte Browsersitzung wird gelöscht • Alle Browsersitzungen werden gelöscht
Cloud-Dienste	• Status eines angeschlossenen Sensor wird abgerufen
Konsole	• Ein Sensor wird mit einer Konsole verbunden • Ein Sensor wird von einer Konsole getrennt • Ein ExtraHop-Recordstore oder Packetstore stellt eine getunnelte Verbindung zu einer Konsole her • Die Konsoleninformationen sind festgelegt • Ein Konsolen-Spitzname ist festgelegt • Einen Sensor aktivieren oder deaktivieren • Der Sensor wird aus der Ferne betrachtet

Kategorie	Ereignis
	• Eine Lizenz für einen Sensor wird von einer Konsole überprüft • Eine Lizenz für einen Sensor wird von einer Konsole festgelegt
Armaturenbretter	• Ein Dashboard wird erstellt • Ein Dashboard wird umbenannt • Ein Dashboard wird gelöscht • Ein Dashboard-Permalink, auch Kurzcode genannt, wird geändert • Die Optionen zum Teilen von Dashboards wurden geändert
Datenspeicher	• Die erweiterte Datenspeicherkonfiguration wurde geändert • Der Datenspeicher wird zurückgesetzt • Ein Datenspeicher-Reset wurde abgeschlossen • Anpassungen werden gespeichert • Anpassungen werden wiederhergestellt • Anpassungen werden gelöscht
Erkennungen	• Ein Erkennungsstatus wird aktualisiert • Ein Erkennungsbeauftragter wird aktualisiert • Erkennungsnotizen werden aktualisiert • Ein externes Ticket wird aktualisiert • Eine Tuning-Regel wird erstellt • Eine Tuning-Regel wird gelöscht • Eine Tuning-Regel wird geändert • Eine Beschreibung der Tuning-Regel wird aktualisiert • Eine Tuning-Regel ist aktiviert • Eine Tuning-Regel ist deaktiviert • Eine Tuning-Regel wird erweitert
Ausnahmedateien	• Eine Ausnahmedatei wird gelöscht
ExtraHop Recordstore Records	• Alle ExtraHop Recordstore-Datensätze werden gelöscht
ExtraHop-Recordstore-Cluster	• Ein neuer ExtraHop-Recordstore-Knoten wird initialisiert • Ein Knoten wird zu einem ExtraHop-Recordstore-Cluster hinzugefügt • Ein Knoten wird aus einem ExtraHop-Recordstore-Cluster entfernt • Ein Knoten tritt einem ExtraHop-Recordstore-Cluster bei • Ein Knoten verlässt einen ExtraHop-Recordstore-Cluster • Ein Sensor oder eine Konsole ist mit einem ExtraHop-Recordstore verbunden

Kategorie	Ereignis
	• Ein Sensor oder eine Konsole ist von einem ExtraHop-Recordstore getrennt • Ein ExtraHop-Recordstore-Knoten wurde entfernt oder fehlt, aber nicht über eine unterstützte Schnittstelle
ExtraHop Aktualisierungsservice	• Eine Entdeckungskategorie wird aktualisiert • Eine Erkennungsdefinition wird aktualisiert • Ein Erkennungsauslöser wird aktualisiert • Eine Ransomware-Definition wird aktualisiert • Erkennungsmetadaten werden aktualisiert • Erweiterter Erkennungsinhalt wird aktualisiert
Firmware	• Die Firmware wurde aktualisiert
Globale Richtlinien	• Die globale Richtlinie für die Bearbeitungssteuerung von Gerätegruppe wurde aktualisiert
Integrationen	• Eine Integration wird aktualisiert
Lizenz	• Eine neue statische Lizenz wird angewendet • Die Lizenzserverkonnektivität wird getestet • Ein Produktschlüssel ist auf dem Lizenzserver registriert • Eine neue Lizenz wird beantragt
Loggen Sie sich in das ExtraHop-System ein	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
Loggen Sie sich über SSH oder REST API ein	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
Module	• Die Zugriffskontrolle für das NDR-Modul ist aktiviert • Die Zugriffskontrolle für das NPM-Modul ist aktiviert
Netzwerk	• Eine Netzwerkschnittstellenkonfiguration wird bearbeitet • Der Hostname oder DNS Einstellung wurde geändert • Eine Netzwerkschnittstellenroute wird geändert
Offline-Erfassung	• Eine Offline-Capture-Datei wird geladen
PCAP	• Eine Paketerfassungsdatei (PCAP) wird heruntergeladen
Fernzugriff	• Der Fernzugriff für das ExtraHop Support Team ist aktiviert

Kategorie	Ereignis
	• Der Fernzugriff für das ExtraHop Support Team ist deaktiviert • Fernzugriff für ExtraHop Support ist aktiviert • Der Fernzugriff für ExtraHop Support ist deaktiviert
RPCAP	• Eine RPCAP-Konfiguration wird hinzugefügt • Eine RPCAP-Konfiguration wird gelöscht
Config ausführen	• Die laufende Konfigurationsdatei ändert sich
SAML-Identitätsanbieter	• Ein Identitätsanbieter wird hinzugefügt • Ein Identitätsanbieter wird geändert • Ein Identitätsanbieter wird gelöscht
SAML-Anmeldung	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
SAML-Privilegien	• Eine Privilegienstufe wird gewährt • Eine Privilegienstufe wurde verweigert
SSL-Entschlüsselung	• Ein SSL-Entschlüsselungsschlüssel wird gespeichert
SSL-Sitzungsschlüssel	• Ein PCAP-Sitzungsschlüssel wird heruntergeladen
Kundendienst-Konto	• Das Support-Konto ist deaktiviert • Das Support-Konto ist aktiviert • Der Support-SSH-Schlüssel wird neu generiert
Unterstützungsskript	• Ein Standard-Support-Skript wird ausgeführt • Ein früheres Unterstützungsskript-Ergebnis wird gelöscht • Ein Support-Skript wird hochgeladen
Syslog	• Remote-Syslog-Einstellungen werden aktualisiert
System- und Servicestatus	• Das System wird gestartet • Das System wird heruntergefahren • Das System wird neu gestartet • Der Bridge-, Capture- oder Portal-Prozess wird neu gestartet • Ein Systemdienst ist aktiviert (z. B. SNMP, Webshell, Management, SSH) • Ein Systemdienst ist deaktiviert (z. B. SNMP, Webshell, /management, SSH)
Systemzeit	• Die Systemzeit ist eingestellt • Die Systemzeit wurde geändert

Kategorie	Ereignis
	• Die Systemzeit ist rückwärts eingestellt • NTP-Server sind eingerichtet • Die Zeitzone ist eingestellt • Eine manuelle NTP-Synchronisierung wird angefordert
Systembenutzer	• Ein Benutzer wird hinzugefügt • Benutzermetadaten werden bearbeitet • Ein Benutzer wird gelöscht • Ein Benutzerkennwort ist gesetzt • Ein anderer Benutzer als der `setup` Benutzer versucht, das Passwort eines anderen Benutzers zu ändern • Ein Benutzerkennwort wird aktualisiert
TAXII-Feeds	• Ein TAXII-Feed wird hinzugefügt • Ein TAXII-Feed wird geändert • Ein TAXII-Feed wird gelöscht
Informationsgespräche über Bedrohungen	• Ein Bedrohungsübersicht wird archiviert • Eine Bedrohungsübersicht wird wiederhergestellt
ExtraHop Packetstore	• Ein neuer ExtraHop-Paketstore wird initialisiert • Ein Sensor oder eine Konsole ist mit einem ExtraHop-Packetstore verbunden • Ein Sensor oder eine Konsole ist von einem ExtraHop-Packetstore getrennt • Ein ExtraHop-Paketstore wird zurückgesetzt
Tendenzen	• Ein Trend wird zurückgesetzt
Trigger	• Ein Auslöser wird hinzugefügt • Ein Auslöser wird bearbeitet • Ein Auslöser wird gelöscht
Benutzergruppen	• Eine lokale Benutzergruppe wird erstellt • Eine lokale Benutzergruppe wird gelöscht • Eine lokale Benutzergruppe ist aktiviert • Eine lokale Benutzergruppe ist deaktiviert