splunk>

Splunk 基本 1 ラボ実習

ラボ表記規則:

`[sourcetype=db_audit]` または `[cs_mime_type]` はソースタイプまたはフィールド名を指します。

備考: ラボ作業が個人のコンピュータまたはバーチャルマシンで実施された場合、ラボ環境は提供されません。 運用環境でのラボ作業は**決して実施しない**でください。

ラボマニュアルは示されるデータタイプ別にソースタイプを参照しています:

タイプ	ソースタイプ	関連のフィールド
ウェブアプリケーション	access_combined_wcookie	action、bytes、categoryId、clientip、itemId、JSESSIONID、productId、referer、referer_domain、status、useragent、file
データベース	db_audit	Command、Duration、Type
Web サーバー	linux_secure	COMMAND、PWD、pid、process

ラボモジュール 13 - アラートの作成

警告: このラボは無料ライセンスでは機能しません。
このラボはトライアルライセンスが無料ライセンスに変換されていない場合にのみ実行してください。

備考: このラボ文書には2つのセクションがあります。
最初のセクションには解答の記載がない指示が含まれます。
次のセクションには予想されるサーチ文字列 (解答) が赤で記載された指示が含まれます。
このコースはSplunk内部データを使用しており、管理者アカウントが必要です。

説明
このラボ実習では、Splunk インターフェースに表示されるアラートを作成して起動します。

シナリオ: セキュリティ上の理由から、Splunk サーチヘッドでのログイン試行の失敗をモニタリングする必要があります。注意を向けるのは管理者アカウントでのログイン失敗のみです。1 分以内に 2 回以上ログイン試行に失敗すると通知を受け取るよう設定します。

タスク 1:ユーザーアカウントを変更してサンプルサーチを実行します。

1. **ユーザー名 > ログアウト**メニューを使用して Splunk Enterprise をログアウトします。
2. ユーザー名に「`admin`」、パスワードに「`WrongPassword`」と入力します。

© 2018 Splunk Inc. All rights reserved.

3. 次に、ユーザー名「admin」とモジュール 3 で選択したパスワードを入力します。
4. サーチビューに移動します。（**ホーム** App にいる場合は、画面左側にある列から**サーチ & レポート**をクリックしてください。サーチビューへは、画面一番上の緑のバーにある**サーチ**メニューをクリックしてもアクセスすることができます。）
5. 「ログイン試行」のアクションが admin のユーザー名に対して**過去 15 分**間にわたり「失敗情報」を返すイベントを_audit インデックスでサーチします。

結果例:

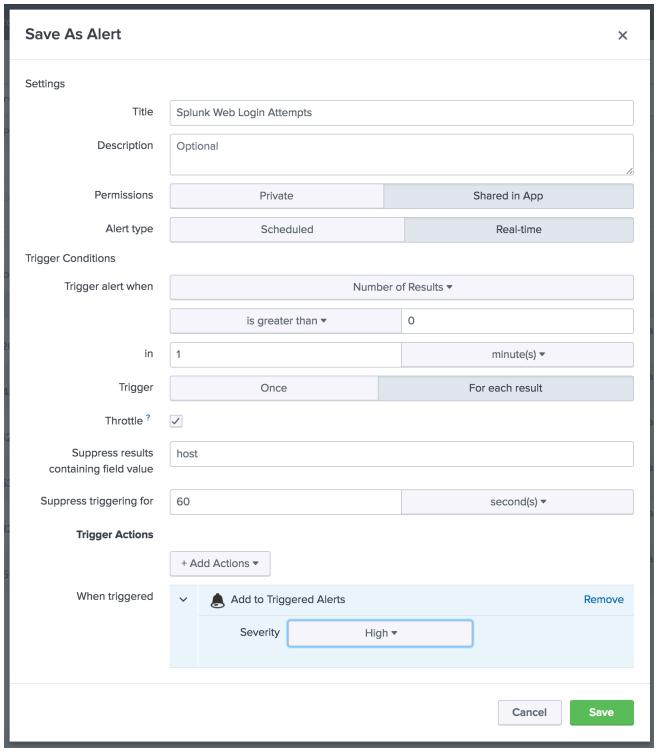
i	Time	Event
>	5/22/18 3:23:37.220 PM	Audit:[timestamp=05-22-2018 15:23:37.220, user=admin, action=login attempt, info=failed, src=127.0.0.1][n/a] host = cbreshears-MBP-B120D source = audittrail sourcetype = audittrail

タスク **2:** アラートを作成します。

6. **名前を付けて保存**メニューから**アラート**を選択します。
7. アラートにタイトルを付けます: Splunk Web Login Attempts
8. **権限**については、**App でシェア**を選択します。
9. **アラートタイプ**は、**リアルタイム**を選択します。
10. **次の条件の時にアラートを生成**では、**結果数**を選択します。
11. 結果数を 0 **より大きい**に設定します。
12. **イン**フィールドは 1 **分**に設定する必要があります。
13. **生成条件**には、**各結果に対して**を選択します。
14. **抑制**チェックボックスを確認します。
15. **フィールド値を含む結果を抑制**には「host」と入力します。
16. **抑制トリガー**が「60」秒に設定されていることを確認してください。
17. **アクション追加**をクリックし、**生成アラートに加える**を選択します。
18. **重大度**を**高**に設定します。

例:

© 2018 Splunk Inc. All rights reserved.



19. **保存**をクリックし、**アラート表示**をクリックします。

タスク 3: アラートをテストします。

20. **管理者 > ログアウト**メニューを使用して Splunk Enterprise をログアウトします。
21. ユーザー名に「`admin`」、パスワードに「`WrongPassword`」を 1 列に 3 回入力します。
22. 次にユーザー名「`admin`」と正しいパスワードを入力します。
23. Splunk バーから**アクティビティ > 作動したアラート**をクリックします。
24. **サーチ & レポート**が、**App** 用に選択されていることを確認します。

例:

	Time	Fired alerts	App	Type	Severity	Mode	Actions
☐	2018-05-22 15:30:03 PDT	Splunk Web Login Attempts	search	Real-time	High	Per Result	View results | Edit search | Delete

25. 作動したアラートの**結果表示**リンクをクリックし、アラートを引き起こしたイベントを確認します。

© 2018 Splunk Inc. All rights reserved.

splunk>

Splunk 基本 1 ラボ実習

ラボ表記規則:

`[sourcetype=db_audit]` または `[cs_mime_type]` はソースタイプまたはフィールド名を指します。

備考: ラボ作業が個人のコンピュータまたはバーチャルマシンで実施された場合、ラボ環境は提供されません。 運用環境でのラボ作業は**決して実施しない**でください。

ラボマニュアルは示されるデータタイプ別にソースタイプを参照しています:

タイプ	ソースタイプ	関連のフィールド
ウェブアプリケーション	access_combined_wcookie	action、bytes、categoryId、clientip、itemId、JSESSIONID、productId、referer、referer_domain、status、useragent、file
データベース	db_audit	Command、Duration、Type
Web サーバー	linux_secure	COMMAND、PWD、pid、process

ラボモジュール 13 - アラートの作成 (ソリューション付)

警告: このラボは無料ライセンスでは機能しません。
このラボはトライアルライセンスが無料ライセンスに変換されていない場合にのみ実行してください。

備考: このラボ文書には2つのセクションがあります。
最初のセクションには解答の記載がない指示が含まれます。
次のセクションには予想されるサーチ文字列 (解答) が赤で記載された指示が含まれます。
このコースはSplunk内部データを使用しており、管理者アカウントが必要です。

説明
このラボ実習では、Splunk インターフェースに表示されるアラートを作成して起動します。

シナリオ: セキュリティ上の理由から、Splunk サーチヘッドでのログイン試行の失敗をモニタリングする必要があります。注意を向けるのは管理者アカウントでのログイン失敗のみです。1 分以内に 2 回以上ログイン試行に失敗すると通知を受け取るよう設定します。

タスク 1:ユーザーアカウントを変更してサンプルサーチを実行します。

1. **ユーザー名 > ログアウト**メニューを使用して Splunk Enterprise をログアウトします。
2. ユーザー名に「admin」、パスワードに「WrongPassword」と入力します。

© 2018 Splunk Inc. All rights reserved.

3. 次に、ユーザー名「admin」とモジュール 3 で選択したパスワードを入力します。
4. サーチビューに移動します。（**ホーム** App にいる場合は、画面左側にある列から**サーチ & レポート**をクリックしてください。サーチビューへは、画面一番上の緑のバーにある**サーチ**メニューをクリックしてもアクセスすることができます。）
5. 「ログイン試行」のアクションが admin のユーザー名に対して**過去 15 分**間にわたり「失敗情報」を返すイベントを_audit インデックスでサーチします。

   (index=_audit action="login attempt" info=failed user=admin)

結果例:

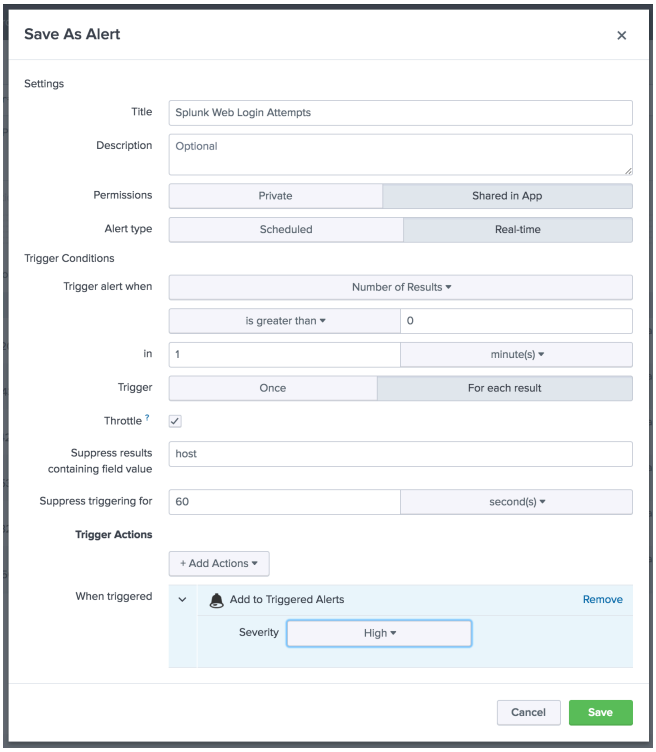
i	Time	Event
>	5/22/18 3:23:37.220 PM	Audit:[timestamp=05-22-2018 15:23:37.220, user=admin, action=login attempt, info=failed, src=127.0.0.1][n/a] host = cbreshears-MBP-B120D source = audittrail sourcetype = audittrail

タスク **2:** アラートを作成します。

6. **名前を付けて保存**メニューから**アラート**を選択します。
7. アラートにタイトルを付けます: Splunk Web Login Attempts
8. **権限**については、**App でシェア**を選択します。
9. **アラートタイプ**は、**リアルタイム**を選択します。
10. **次の条件の時にアラートを生成**では、**結果数**を選択します。
11. 結果数を 0 **より大きい**に設定します。
12. **イン**フィールドは 1 **分**に設定する必要があります。
13. **生成条件**には、**各結果に対して**を選択します。
14. **抑制**チェックボックスを確認します。
15. **フィールド値を含む結果を抑制**には「host」と入力します。
16. **抑制トリガー**が「60」秒に設定されていることを確認してください。
17. **アクション追加**をクリックし、**生成アラートに加える**を選択します。
18. **重大度**を**高**に設定します。

例:

© 2018 Splunk Inc. All rights reserved.



19. **保存**をクリックし、**アラート表示**をクリックします。

タスク 3: アラートをテストします。

20. **管理者 > ログアウト**メニューを使用して Splunk Enterprise をログアウトします。
21. ユーザー名に「`admin`」、パスワードに「`WrongPassword`」を 1 列に 3 回入力します。
22. 次にユーザー名「`admin`」と正しいパスワードを入力します。
23. Splunk バーから**アクティビティ > 作動したアラート**をクリックします。
24. **サーチ & レポート**が、**App** 用に選択されていることを確認します。

例:

	Time	Fired alerts	App	Type	Severity	Mode	Actions
☐	2018-05-22 15:30:03 PDT	Splunk Web Login Attempts	search	Real-time	High	Per Result	View results | Edit search | Delete

25. 作動したアラートの**結果表示**リンクをクリックし、アラートを引き起こしたイベントを確認します。

© 2018 Splunk Inc. All rights reserved.