

## 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。  
このコースでは、常時サーチすることになります。  
これは運用環境で最適な実例ではありませんが、データセット制限の性質により、これらのラボに必要となります。

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 5 - サーチ

### 説明

このラボでは Splunk サーチ言語でいくつかの基本サーチを実行できるようにします。


### 手順

**シナリオ:** 当社の Web サーバーにセキュリティ問題があると疑われる根拠があります。上司から SSH ログイン試行の失敗を検証するように依頼されます。

### タスク 1: 基本サーチを実行します。

1. 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。)
2. サーチバーで、サーチをタイプします: `error OR fail*`

**備考:** タイプすると、サーチアシスタントが提案を提供します。

3. タイムレンジピッカーが**常時**の時間範囲に設定されていることを確認し、**サーチ**ボタンをクリックします 。サーチを実行します。
4. サーチ結果をレビューします。あなたのサーチ単語が結果に強調表示されているのを確認します (強調表示されたテキストを見るためにはスクロールダウンするかイベント全列を表示をクリックしなければならない場合があります)。
5. ページネーションを使用してページをめくり、さらに結果を確認します。
6. 各イベントの下にホスト、ソース、ソースタイプの値が確認できます。ホスト値を見て、「web\_application」および「web\_server」ホスト両方のイベントが得られていることを確認します。

## 結果例

|   |                            |   |
|---|----------------------------|---|
| > | 5/21/18<br>11:06:40.000 PM | 59.36.99.70 -- [21/May/2018:23:06:40] "POST /cart/ <b>error</b> .do?msg=FormError&JSESSIONID=SD10SL3FF10ADFF89258 HTTP 1.1" 200 1799 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 874 |
|   |                            | host = web_application   source = access_30DAY.log   sourcetype = <a href="#">access_combined_wcookie</a>   |
| > | 5/21/18<br>10:56:31.000 PM | Mon May 21 2018 22:56:31 www1 sshd[1389]: <b>Failed</b> password for invalid user ubuntu from 223.213.255.255 port 4411 ssh2  |
|   |                            | host = web_server   source = linux_s_30DAY.log   sourcetype = linux_secure  |
| > | 5/21/18<br>10:56:18.000 PM | Mon May 21 2018 22:56:18 www1 sshd[3497]: <b>Failed</b> password for root from 223.213.255.255 port 8000 ssh2   |
|   |                            | host = web_server   source = linux_s_30DAY.log   sourcetype = linux_secure  |

## タスク 2: 新規サーチを開始します。結果を絞り込みます。

7. サーチをクリックして新規サーチを開始します。
8. 「fail\* AND password」を **All time** でサーチします。結果をレビューし、いくつかのイベントのポート値を確認します。確認したいのはこちらが開いている **SSH** ポート、ポート **22** にログインしようとしているユーザーです。
9. サーチ文字列の最後に以下をタイプします: 22
10. サーチボタンをクリックするか、**Enter** を押してサーチを実行します。
11. ポート **22** でのイベントだけではなく、**22** という数字を含むすべてのイベントが選択されているのが確認できます。

## 結果例

| i | Time                       | Event  |
|---|----------------------------|--|
| > | 5/21/18<br>10:56:31.000 PM | Mon May 21 2018 22:56:31 www1 sshd[1389]: <b>Failed</b> password for invalid user ubuntu from 223.213.255.255 port 4411 ssh2<br>host = web_server   source = linux_s_30DAY.log   sourcetype = linux_secure |
| > | 5/21/18<br>10:56:18.000 PM | Mon May 21 2018 22:56:18 www1 sshd[3497]: <b>Failed</b> password for root from 223.213.255.255 port 8000 ssh2<br>host = web_server   source = linux_s_30DAY.log   sourcetype = linux_secure                |
| > | 5/21/18<br>10:56:02.000 PM | Mon May 21 2018 22:56:02 www1 sshd[5001]: <b>Failed</b> password for invalid user tomcat from 192.188.106.240 port 22 ssh2<br>host = web_server   source = linux_s_30DAY.log   sourcetype = linux_secure   |

12. サーチの **22** という数を以下と置き換えます: "port 22"。必ず引用符を使用してください。
13. ここで全段階のイベントのみ確認できていることに注意してください。
14. 結果を全ページ確認します。ログイン失敗が多くあります。

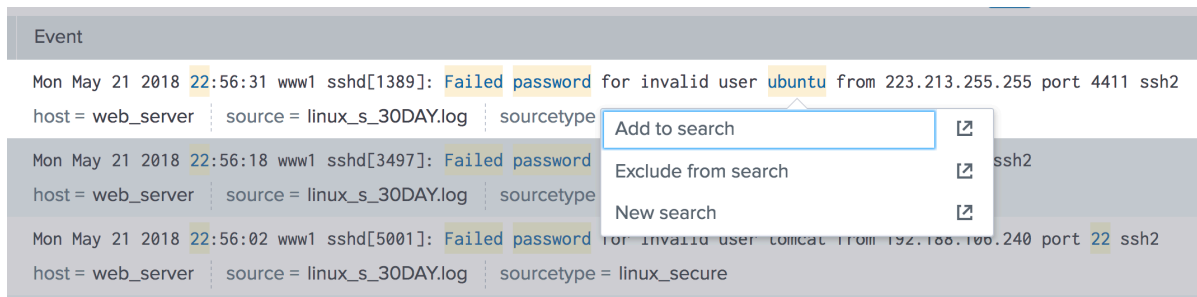
**備考:** 結果の上に、1ページに表示されるイベント数を変更できるメニュー項目があります。デフォルトでは、このオプションは**2ページにつき20**となっていますが、オプションをクリックして数を増減させることができます。

## タスク 3: タイムラインを使って結果の傾向を確認します。

15. 時間の経過に伴う傾向を見たいですか？
16. タイムラインの列の 1 つをクリックします。これらのイベントを確認します。
17. 他の列をクリックします。これらのイベントを確認します。時間内に類似のイベントの急上昇がみられる場合、システムが攻撃の対象となっている可能性があります。急上昇がない場合は、優良月です。任意で、返されたいくつかのイベントを見て、使用 IP アドレスまたはポートに何らかの類似性が見られるかを確認します (続くステップでもいくつかイベントの追加検証を行います)。

**タスク 4: サーチの出力を使用して結果を絞り込みます。**

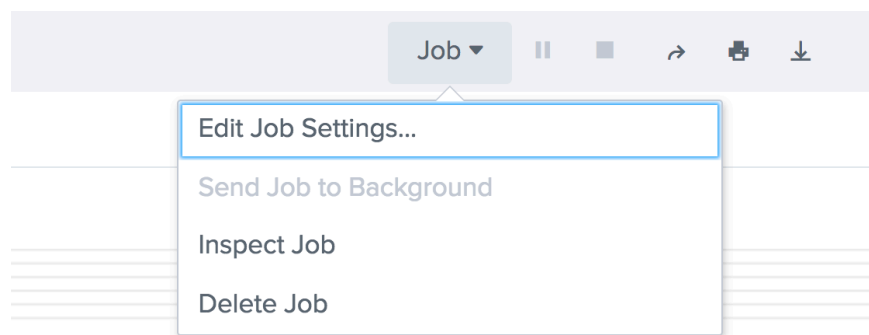
18. サーチ結果のユーザー名の 1 つをクリックします。ユーザーネームをクリックするとき、オプションメニューが表示されることに注意してください:



19. サーチに追加をクリックします。
20. タイムラインを見て、このユーザーに関するパスワード失敗のなんらかの急上昇がないかを確認します。
21. 急上昇を確認したら、タイムラインでその列をダブルクリックし、その時間範囲を拡大します。
22. そのユーザー名をもう一度結果内でクリックし、**サーチから削除**をクリックします。

**タスク 5: 結果を保存してシェアします (デフォルト保存時間を延長します。 デフォルト表示権限を全員に拡大します)。**

23. サーチボックスの右下にあるジョブメニューから、**ジョブ設定編集**を選択します。



24. そのジョブの**読み出し権限**を変更します。デフォルトは「プライベート」です。**全員**をクリックします。重要なサーチに関し、これにより他の人があなたの作業を活用することができます。
25. サーチの**寿命**を延長します。デフォルトではサーチは 10 分間保存されます。**7 日**をクリックします。サーチ結果へのリンクをコピー、またはリンクをブックマークできます。
26. **保存**をクリックしてサーチビューに戻ります。
27. ジョブリスト履歴を**アクティビティ > ジョブメニュー** (Splunk バーの右側、ブラウザウィンドウの一番上にある黒いバー) から表示します。

28. そのジョブのオーナー、イベント、期限切れ、ステータス、アクションを確認してください (ジョブが進行中の場合、アクションの下にある ■ ボタンを使用して停止することができます。またこれでジョブステータスを「完了」に設定します)。

**備考:** Splunkをプロダクション環境で使用している場合、いくつかのジョブが進行中である場合があります。すでに十分なデータを獲得している場合は、それらを完了してサーチジョブを停止できます。

29. 先ほど 7 日に有効期限を変更したサーチのサーチ基準 (青字) をクリックします。サーチが Search & Reporting App で再び開きます。

**備考:** このサーチを開いても再実行はされません。

30. アクティビティ > ジョブをもう一度クリックします。サーチを変更しなかったため、リストには一度だけ記載されます。
31. ブラウザの「戻る」ボタンをクリックしてサーチビューに戻ります。