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 10 - レポートとダッシュボードの作成

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。

説明

このラボでは、Buttercup Games 組織メンバーのためのレポートとダッシュボードを構築します。

手順

シナリオ: セキュリティチームはよからぬことをたくらんでいると思われる IP のレポートを望んでいます。

タスク **1:** **統計カウント関数を使用して、Buttercup Games ウェブアプリケーションの禁止されたページにアクセスしようとしているユーザーのレポートを入手します。**

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。)

備考: **このコースでは、常時メインインデックスを使用して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。

2. 禁止されたステータス (403) のすべてのウェブアプリケーションイベントを返すサーチを入力します。

結果例:

i	Time	Event
>	5/21/18 11:15:37.000 PM	67.133.102.54 - - [21/May/2018:23:15:37] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD2SL4FF6ADFF4958 HTTP 1.1 " 403 2282 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 773 host = web_application | source = access_30DAY.log | sourcetype = access_combined_wcookie
>	5/21/18 11:07:46.000 PM	91.205.189.15 - - [21/May/2018:23:07:46] "GET /cart.do?action=remove&JSESSIONID=SD0SL7FF8ADFF4960 HTTP 1.1" 403 720 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (compatible; NetcraftSurveyAgent/1.0/cc-prepass-https; +info@netcraft.com)" 378 host = web_application | source = access_30DAY.log | sourcetype = access_combined_wcookie
>	5/21/18 10:43:51.000 PM	76.169.7.252 - - [21/May/2018:22:43:51] "GET /oldlink?&JSESSIONID=SD4SL6FF8ADFF4960 HTTP 1.1" 403 3640 "http://www.buttercupgames.com/oldlink" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 122 host = web_application | source = access_30DAY.log | sourcetype = access_combined_wcookie

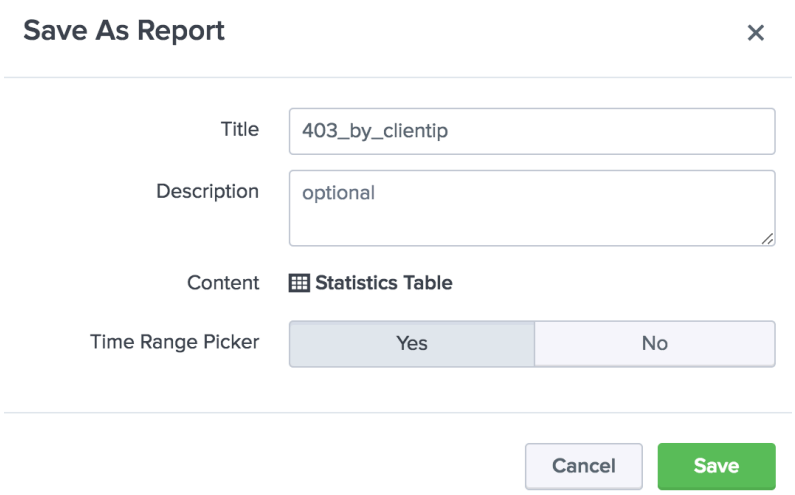
3. 「Stats Count」関数を使用して「clientip」別にイベントをカウントし、そのカウントの名前を「attempts」に変更します。

結果例:

clientip	attempts
107.3.146.207	11
108.65.113.83	3
109.169.32.135	4
110.138.30.229	2
110.159.208.78	3
111.161.27.20	2

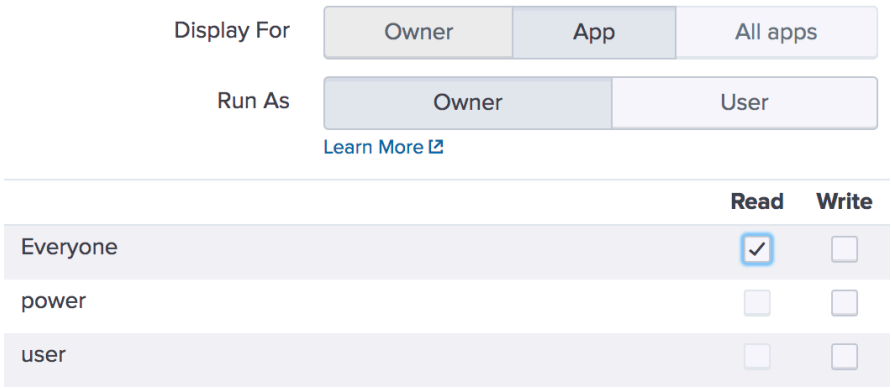
4. 「Sort」コマンドを使用して結果を表示し、最も「attempts」回数が多い「clientip」が最初に表示されるようにします。
5. 最も「attempts」回数の多い「clientip」について、「attempts」の合計数はいくつですか？ これはクイズモジュールに登場する可能性があります。
6. **名前をつけて保存**メニュー (タイムレンジピッカーの上) を使用して**レポート**を選択します。
7. そのレポートに対し「403_by_clientip」と**タイトル**を入力して**保存**をクリックします。

例:



8. **権限**リンクを使用して App 用のレポートを表示し、オーナーとして実行することで、全員が読めるようにします。 **保存**をクリックします。

例:



9. 入手可能なレポートのリストへは、画面一番上の緑のバーにある**レポート**メニューオプションを使用してアクセスできます。
10. 「403_by_clientip」レポートがリストにあることに注目してください。 レポートタイトルをクリックしてレポートを実行します。

シナリオ: CFO はあなたにプロダクトセールスの現状を 1 つの場所で確認できるダッシュボードの作成を依頼します。

タスク 2: 統計関数を使用して、販売されたプロダクトの視覚エフェクトを作成し、それらをダッシュボードに追加します。

---

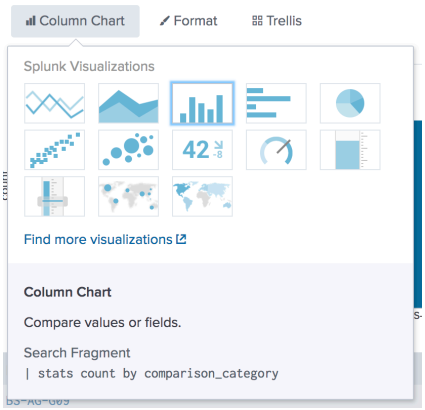
11. 新しいサーチビューに移動します。(サーチビューへは、画面一番上のバーにある**サーチ**メニューをクリックしてアクセスします。)
12. アイテムが正常に購入されたすべてのウェブアプリケーションイベントを常に返すサーチを入力します。アイテムが正常に購入されると「success.do」ファイルが使用され、200 ステータスが返されることを覚えておいてください。
13. 「Stats Count」関数を「by」で使用し、productId ごとにイベントをカウントします。

結果例:

productId	count
BS-AG-G09	935
CU-PG-G06	935
DB-SG-G01	1319
DC-SG-G02	1308
FI-AG-G08	988
FS-SG-G03	1155

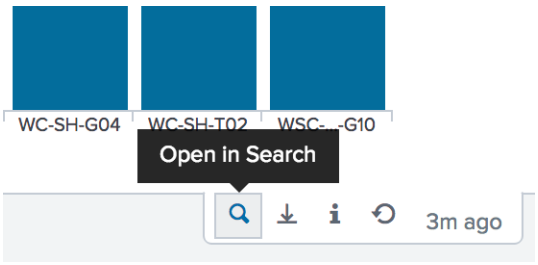
14. **視覚エフェクト**タブを選択して視覚エフェクト選択肢から**棒グラフ**選択します。

例:



15. **名前をつけて保存**メニューを使用して**ダッシュボードパネル**を選択します。
16. これらの値でダッシュボードを保存します:
    - ダッシュボード: *新規*
    - ダッシュボードのタイトル: *セールスダッシュボード*
    - パネルタイトル: *プロダクトセールス*
17. 保存したら、**ダッシュボードを表示**をクリックします。
18. グラフの棒にポインターを合わせてインタラクションを確認し、パネルの下にあるツールに留意します。

例:

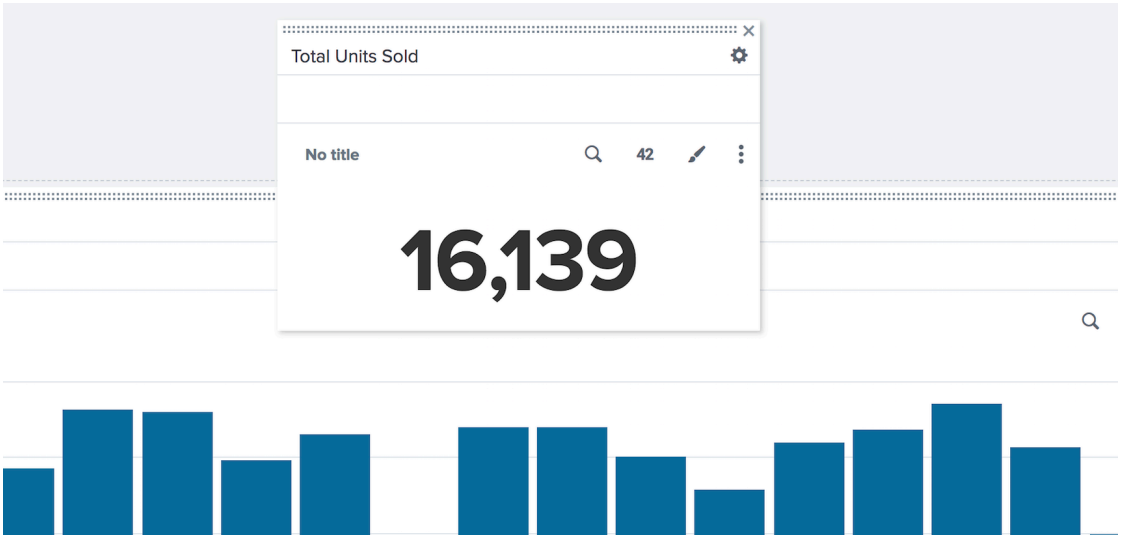


19. パネルの下にある**サーチで開く**アイコンを使用してサーチビューを開き、サーチを実行します。
20. サーチから「By」を削除し、販売されたプロダクトの総数を返します。
21. **視覚エフェクト**タブを選択して **Splunk 視覚エフェクト**メニューから**単一値**視覚エフェクトを選択します。
22. **名前をつけて保存**メニューを使用して**ダッシュボードパネル**を選択します。
23. これらの値でダッシュボードを保存します:
    - ダッシュボード: *既存*
    - ダッシュボードのタイトル: *セールスダッシュボード*

- パネルタイトル: *販売ユニット総数*

24. 保存したら、**ダッシュボードを表示**をクリックします。
25. 「販売ユニット総数」パネルは CFO が一番見たいアイテムに違いありません。 ダッシュボードの一番上にある**編集**ボタンをクリックします。
26. 「販売ユニット総数」パネルの一番上にあるバーをクリックしてホールドし、ダッシュボードの一番上へパネルをドラッグします。 配置したら**保存**をクリックします。

例:



27. CFO にとって有益と思われるパネルは他に何がありますか？前に実行したいくつかのサーチに戻り、それらをダッシュボードに追加します。

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 10 - レポートとダッシュボードの作成 (ソリューション付)

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。

説明

このラボでは、Buttercup Games 組織メンバーのためのレポートとダッシュボードを構築します。

手順

シナリオ: セキュリティチームはよからぬことをたくらんでいると思われる IP のレポートを望んでいます。

タスク **1:統計カウント関数を使用して、Buttercup Games ウェブアプリケーションの禁止されたページにアクセスしようとしているユーザーのレポートを入手します。**

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。)

備考: **このコースでは、常時メインインデックスを使用して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。

2. 禁止されたステータス (403) のすべてのウェブアプリケーションイベントを返すサーチを入力します。
   (index=main sourcetype=access_combined_wcookie status=403)

結果例:

i	Time	Event
>	5/21/18 11:15:37.000 PM	67.133.102.54 - - [21/May/2018:23:15:37] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD2SL4FF6ADFF4958 HTTP 1.1 " 403 2282 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 773 host = web_application | source = access_30DAY.log | sourcetype = access_combined_wcookie
>	5/21/18 11:07:46.000 PM	91.205.189.15 - - [21/May/2018:23:07:46] "GET /cart.do?action=remove&JSESSIONID=SD0SL7FF8ADFF4960 HTTP 1.1" 403 720 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (compatible; NetcraftSurveyAgent/1.0/cc-prepass-https; +info@netcraft.com)" 378 host = web_application | source = access_30DAY.log | sourcetype = access_combined_wcookie
>	5/21/18 10:43:51.000 PM	76.169.7.252 - - [21/May/2018:22:43:51] "GET /oldlink?&JSESSIONID=SD4SL6FF8ADFF4960 HTTP 1.1" 403 3640 "http://www.buttercupgames.com/oldlink" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 122 host = web_application | source = access_30DAY.log | sourcetype = access_combined_wcookie

3. 「Stats Count」関数を使用して「clientip」別にイベントをカウントし、そのカウントの名前を「attempts」に変更します。

(index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip)

結果例:

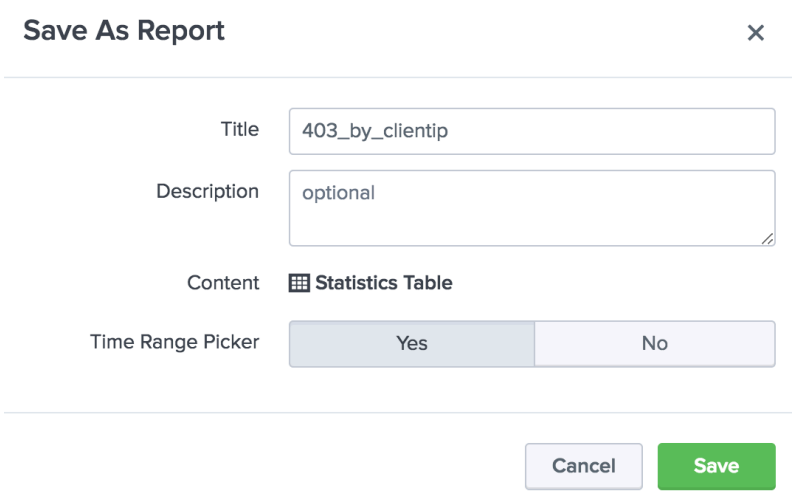
clientip	attempts
107.3.146.207	11
108.65.113.83	3
109.169.32.135	4
110.138.30.229	2
110.159.208.78	3
111.161.27.20	2

4. 「Sort」コマンドを使用して結果を表示し、最も「attempts」回数が多い「clientip」が最初に表示されるようにします。

   (index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip | sort -attempts)

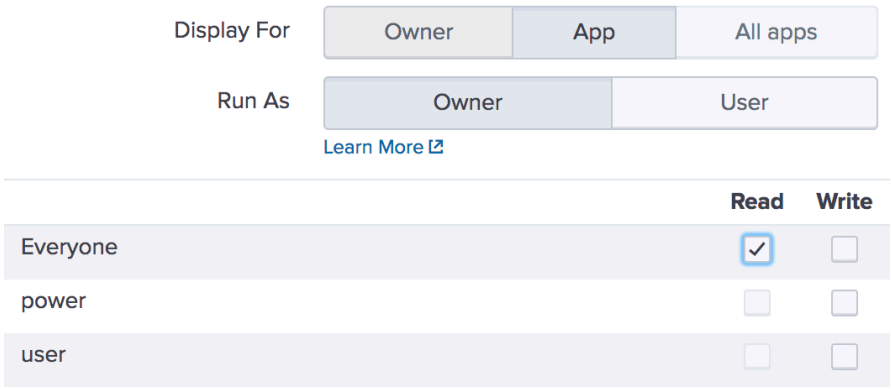
5. 最も「attempts」回数の多い「clientip」について、「attempts」の合計数はいくつですか？ これはクイズモジュールに登場する可能性があります。 (100)
6. **名前をつけて保存**メニュー (タイムレンジピッカーの上) を使用して**レポート**を選択します。
7. そのレポートに対し「403_by_clientip」と**タイトル**を入力して**保存**をクリックします。

例:



8. **権限**リンクを使用して App 用のレポートを表示し、オーナーとして実行することで、全員が読めるようにします。 **保存**をクリックします。

例:



9. 入手可能なレポートのリストへは、画面一番上のバーにある**レポート**メニューオプションを使用してアクセスすることができます。
10. 「403_by_clientip」レポートがリストにあることに注目してください。 レポートタイトルをクリックしてレポートを実行します。

シナリオ: CFO はあなたにプロダクトセールスの現状を 1 つの場所で確認できるダッシュボードの作成を依頼します。

タスク 2: 統計関数を使用して、販売されたプロダクトの視覚エフェクトを作成し、それらをダッシュボードに追加します。

---

11. 新しいサーチビューに移動します。(サーチビューへは、画面一番上のバーにある**サーチ**メニューをクリックしてアクセスします。)
12. アイテムが正常に購入されたすべてのウェブアプリケーションイベントを常に返すサーチを入力します。アイテムが正常に購入されると「success.do」ファイルが使用され、200 ステータスが返されることを覚えておいてください。

    (index=main sourcetype=access_combined_wcookie file=success.do status=200)
13. 「Stats Count」関数を「by」で使用し、productId ごとにイベントをカウントします。

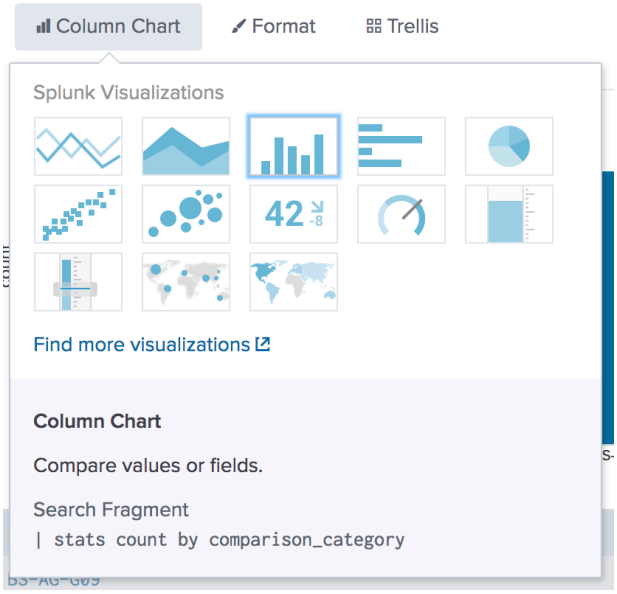
(index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count by productId)

結果例:

productId	count
BS-AG-G09	935
CU-PG-G06	935
DB-SG-G01	1319
DC-SG-G02	1308
FI-AG-G08	988
FS-SG-G03	1155

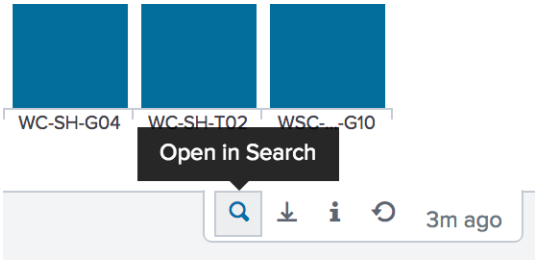
14. **視覚エフェクト**タブを選択して視覚エフェクト選択肢から**棒グラフ**選択します。

例:



15. **名前をつけて保存**メニューを使用して**ダッシュボードパネル**を選択します。
16. これらの値でダッシュボードを保存します:
    - ダッシュボード: *新規*
    - ダッシュボードのタイトル: *セールスダッシュボード*
    - パネルタイトル: *プロダクトセールス*
17. 保存したら、**ダッシュボードを表示**をクリックします。
18. グラフの棒にポインターを合わせてインタラクションを確認し、パネルの下にあるツールに留意します。

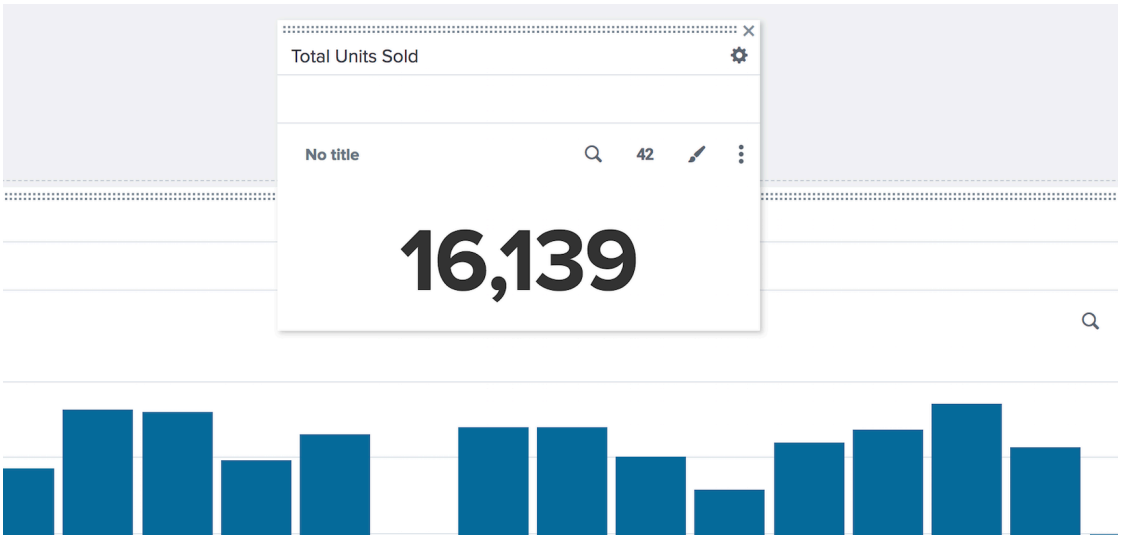
例:



19. パネルの下にある**サーチで開く**アイコンを使用してサーチビューを開き、サーチを実行します。
20. サーチから「By」を削除し、販売されたプロダクトの総数を返します。

    (index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count)
21. **視覚エフェクト**タブを選択して **Splunk 視覚エフェクト**メニューから**単一値**視覚エフェクトを選択します。
22. **名前をつけて保存**メニューを使用して**ダッシュボードパネル**を選択します。
23. これらの値でダッシュボードを保存します:
    - ダッシュボード: *既存*
    - ダッシュボードのタイトル: *セールスダッシュボード*
    - パネルタイトル: *販売ユニット総数*
24. 保存したら、**ダッシュボードを表示**をクリックします。
25. 「販売ユニット総数」パネルは CFO が一番見たいアイテムに違いありません。 ダッシュボードの一番上にある**編集**ボタンをクリックします。
26. 「販売ユニット総数」パネルの一番上にあるバーをクリックしてホールドし、ダッシュボードの一番上へパネルをドラッグします。 配置したら**保存**をクリックします。

例:



27. CFO にとって有益と思われるパネルは他に何がありますか？前に実行したいくつかのサーチに戻り、それらをダッシュボードに追加します。