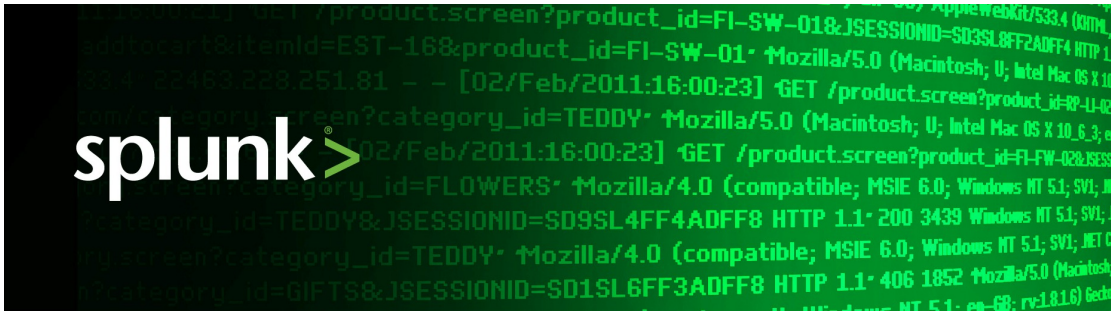


Splunk® Enterprise 6.5.0

Splunk Enterprise 方案

生成时间：2016 年 9 月 26 日，下午 10:28

Table of Contents

概述

关于这些方案

本手册包含运维智能使用案例的分步走查。

创建登录失败仪表板

审查方案并设定一个目标

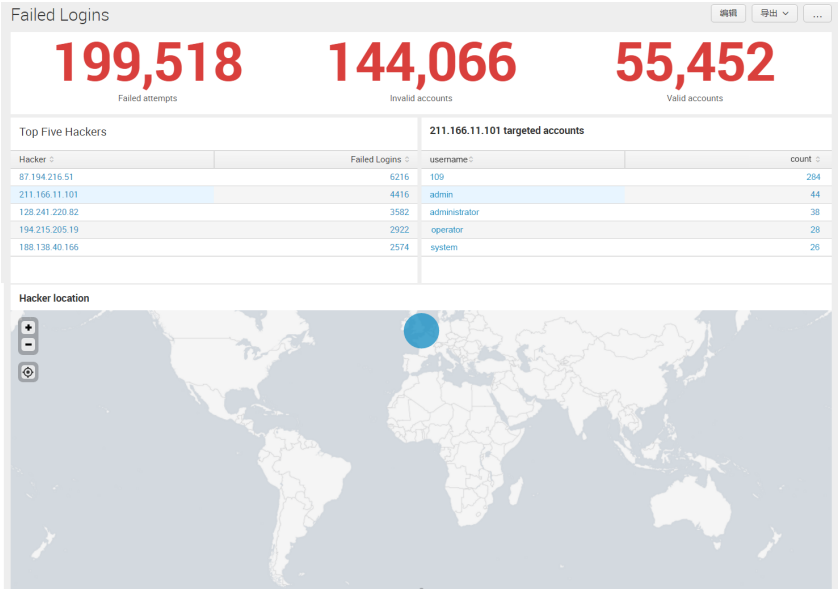
了解如何创建一个仪表板来监视可疑的网站活动。

方案

该方案基于典型的 IT 操作和安全监视用例。使用失败的登录尝试和 IP 地址来追踪黑客活动。监视顶级黑客的位置和目标用户帐户。

目标

构建一个仪表板以帮助您大致监视黑客活动。该方案告诉您如何创建一个像这样的仪表板。



该仪表板显示关键信息。

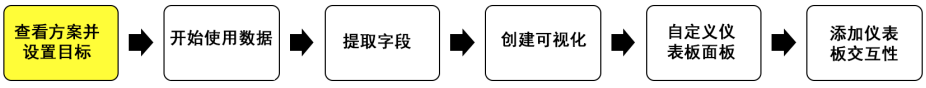
- 有效和无效帐户的失败登录尝试计数。
- 链接到失败的登录尝试的前五名黑客 IP 地址。

仪表板还包括交互功能。

- 一张显示选定的黑客所瞄准的用户帐户的动态填充列表。
- 一张显示选定的黑客位置的动态绘制地图。

步骤

通过这些步骤来达到目标。



前提条件

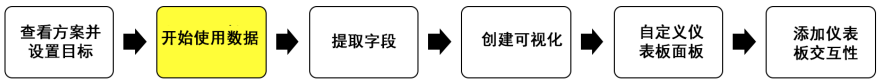
在进行下一步之前，请确保您有以下的资源。

- **正在运行的 Splunk 平台实例**
  - Splunk Enterprise
  - Splunk Cloud
  - Splunk Cloud 免费试用版
- **教程样本数据**
  - 下载 tutorialdata.zip 文件。
  - 在继续之前使用以下一个选项将教程数据上传到 Splunk 平台实例。

实例类型	后续步骤
◦ Splunk Enterprise ◦ 自助式 Splunk Cloud 部署	按照这些教程上传指令将数据导入 Splunk 平台。
◦ 管理的 Splunk Cloud 部署	提出请求数据上传的支持问题。

满足前提条件后，进入下一步骤开始使用数据。

开始使用数据



在这种情况下，黑客似乎进行了许多次登录到系统的尝试，但均失败。在新的数据集中跟踪登录尝试。

开始使用数据。

- 查看数据中的事件模式，以确定特定类型的事件。
- 运行搜索以分离出与特定事件模式匹配的事件。

第 1 部分：查看样本数据中的事件

教程数据有一个来源默认字段。开始使用此字段搜索数据。

- 注意：搜索结果可能会有所不同，具体取决于您将样本数据导入 Splunk 平台实例的时间。

前提条件

- 上载教程样本数据。有关更多详细信息，请参阅之前的方案步骤。

步骤

1. 在**所有时间**范围内运行以下搜索。

   ```
   source="tutorialdata.zip:*"
   ```

   此搜索返回教程数据包中不同日志文件的大量事件。在搜索结果的第一页中，您可能不会看到任何登录失败事件。

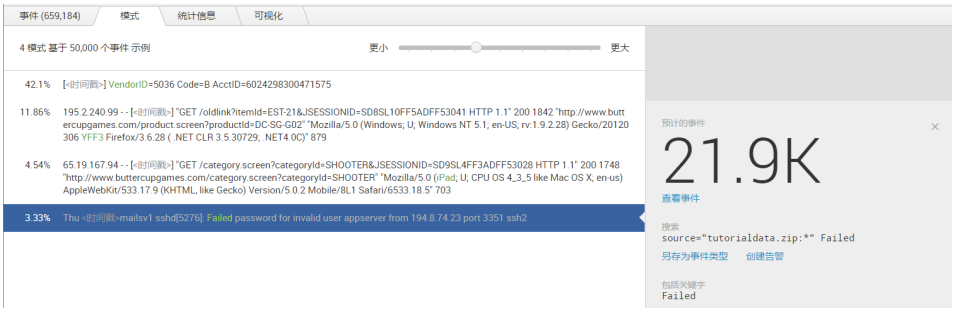
第 2 部分：在数据集中查找事件模式

使用**模式**选项卡来查看数据集中的常用事件模式。您可能会找到一个可用于搜索的登录错误事件。

- 注意：搜索结果可能会有所不同，具体取决于您将样本数据导入 Splunk 平台实例的时间。

步骤

1. 选择**模式**选项卡。选择此选项卡在初始搜索结果中为事件模式生成二次搜索。
2. 注意，**模式**选项卡显示两个事件模式。其中一种模式表示失败的密码尝试。



如果**较小/较大**滑块滑到与上文显示的默认设置不同的位置，您可能会看到更多或更少的模式。使用默认设置以获得相同的结果。

3. 选择失败的登录模式查看以下详细信息。
   - 定义事件模式的关键字。
   - 返回此模式中所表示事件的搜索。

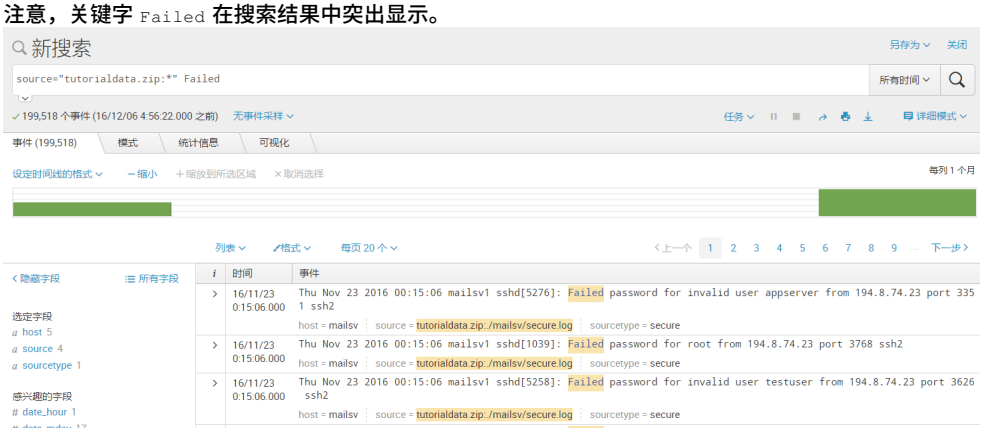
模式选项卡是检查数据集的一种方法。您也可以使用以下选项。

- 查看在**字段**边栏中返回的字段。研究字段摘要和运行预先构建的搜索。
- 在“数据透视表”中打开搜索以使用基于搜索数据的表格和图表。

第 3 部分：在模式中查找事件

步骤

1. 在“模式”选项卡中，选择**查看事件**。搜索使用适合模式的搜索字符串来运行。搜索会分离出符合该模式的事件。
2. 注意，关键字 `Failed` 在搜索结果中突出显示。



3. 同时注意，事件左边的字段边栏包括 `sourcetype` 字段。

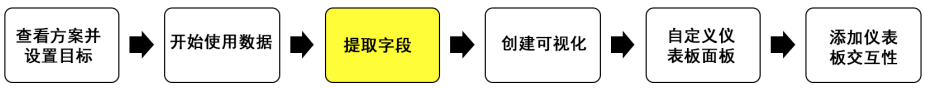
   该字段只有一个值，这意味着由该搜索返回的所有事件具有相同的 `sourcetype` 值。

   因为所有的事件都具有相同的 sourcetype，所以下面的搜索会返回相同的事件。

```
sourcetype=secure failed
```

方案的下一部分将介绍如何从事件中标识和提取字段。

提取字段



仪表板面板的可视化由搜索结果驱动。在构建失败的登录仪表板之前，请确保您拥有为每个面板运行搜索所需要的所有字段。

该方案步骤介绍如何使用字段。

- 查看您正在创建的失败的登录仪表板面板。
- 确定生成仪表板面板所需的字段。
- 确定这些字段是否存在于数据中，或是否必须提取出来。
- 使用“字段提取器”创建字段提取。

第 1 部分：查看目标

您正在构建的失败的登录仪表板需要有以下面板。

- 失败的登录尝试计数。
- 按失败的登录计数排序的前几位黑客。
- 目标用户帐户和在对其进行登录尝试的黑客。
- 地图上的黑客位置。

第 2 部分：确定必填字段

每个仪表板面板都使用一个特定的搜索。根据您正在构建的面板，可能需要提取新的字段来运行搜索。

仪表板面板	如何实现它	需要任何字段吗？
失败的登录尝试计数，按有效和无效帐户细分	使用 `stats count` 以获得事件计数。	否。您可以在事件中搜索“无效”或“有效”，来区分有效和无效的帐户。
黑客排名列表	使用 `top <fieldname>` 命令来列出黑客排名。	**是**。黑客是由事件中的 IP 地址确定的，所以 IP 地址字段是必填的。
目标用户	使用 `stats count` 设计钻取搜索来为每个黑客 IP 地址聚合目标用户帐户。	**是**。为每个黑客聚合目标用户帐户需要上面提到的用户名字段和 IP 地址字段。
在世界地图上对黑客进行定位	使用 `iplocation` 和 `geostats` 命令将 ip 地址转换为在地图上绘制的位置。	**是**。使用上文提及的 IP 地址字段。

第 3 部分：检查所需字段是否可用

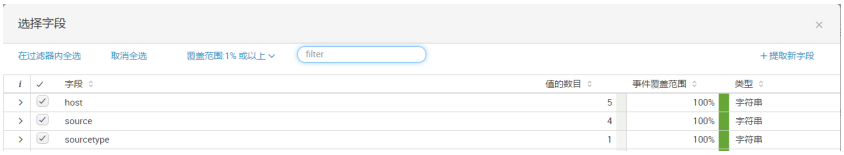
您已确定您需要用户名和 IP 地址字段。检查这些字段是否在数据中可用。如果不可用，则提取它们。

1. 运行以下搜索：`sourcetype=secure failed`
2. 检查字段边栏。

   此处显示**选定的字段**和**感兴趣的字段**类别中的字段。这些列表不会始终包括从搜索结果中获得的每个字段。

3. 注意，不会显示任何具有 IP 地址或用户名的值的字段。
4. 请确保通过选择**全部字段**，这些字段不显示。

   这将打开**选择字段**对话框。您可以查看该搜索中提取的所有字段的详细信息。



5. 查看**选择字段**对话框，并注意，IP 地址和用户名字段未被提取。

接下来的步骤介绍如何提取所需字段。

第 4 部分：字段提取 - 选择示例事件

1. 在**选择字段**对话框中，单击**提取新字段**。“字段提取器”打开。

2. 注意，字段提取器指示您正在为安全的 sourcetype 提取字段。

   “字段提取器”进行的所有字段提取都必须与 sourcetype 相关联。“字段提取器”从搜索获取 sourcetype。当 sourcetype 不可用时，“字段提取器”会在第一步提示您提供一个 sourcetype。

   字段提取也可以与特定的主机和来源值相关联，但是字段提取器仅启用 sourcetype 字段提取。
3. 选择一个示例事件。
4. 单击**下一步**来选择要从事件中提取的字段。
5. 选择使用正则表达式来提取字段，并单击**下一步**。

第 5 部分：字段提取 - 选择要提取的字段

在**选择字段**“字段提取器”这步允许您在示例事件中突出显示您想提取的字段值。您可以从相同事件中提取多个字段。

1. 提取用户名字段。

   在每个事件中，用户名都会出现在错误消息的结尾，`Failed password for invalid user <username>`。要提取用户名字段，突出显示在示例事件中显示的用户名，并指示它是一个称为 `username` 的新字段的示例值。

2. 单击**添加提取**。
   “字段提取器”尝试从示例事件中提取字段。您可以在页面底部附近的预览表中查看结果。
3. 提取 IP 地址字段。

   为此，将事件中的 IP 地址突出显示为新的 `clientip` 字段的值。

4. 单击**添加提取**。更新预览表以显示“字段提取器”如何查找并提取第二个字段的值。在您添加两个字段提取之后，预览表外观应与此类似。

5. 单击**下一步**来验证字段提取并保存它们。

第 6 部分：验证并保存字段提取

1. 通过查看**匹配**和**不匹配**来检查字段提取是否成功。您也可以查看为 `username` 和 `clientip` 提取字段创建的选项卡。
2. （可选）如果您发现任何错误，请删除事件中不正确地突出显示的值。
3. 在验证字段提取之后，请单击**下一步**。

   提取字段。打开**保存**步骤。

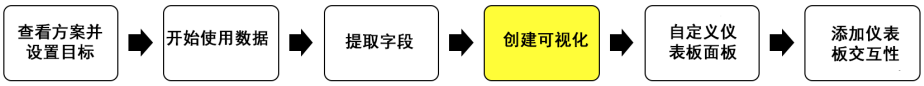
4. 将字段提取的**权限**更改为**所有应用**。

   如果您保持**所有者**的默认值不变，则您使用这些提取创建的其他任意仪表板将只能为您所用。该步骤允许您选择通过角色来为提取设置权限。目前保持默认权限（**每个人**的读取权限和**管理员**的写入权限）。

5. 单击**完成**来保存提取。

方案的下一部分将介绍如何构建可视化。

创建可视化



您现在有能帮助构建失败的登录仪表板中的可视化的字段。

开始构建仪表板。

- 使用搜索来生成单值可视化。
- 搜索保存为报表并添加到仪表板。

第 1 部分：搜索验证失败事件

构建的第一个仪表板面板显示登录失败计数。该面板将登录失败划分为以下两类。

- 有效帐户的登录失败。
- 要获取帐户数据的失败尝试。

步骤

1. 从**搜索和报表**应用为登录失败事件运行此搜索。

```
sourcetype=secure failed
```

第 2 部分：创建单值可视化

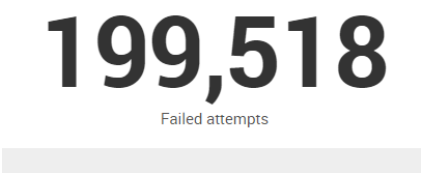
1. 尚未格式化搜索结果以生成一个可视化。修改搜索以聚合登录失败事件并生成一个计数。

```
sourcetype=secure failed | stats count
```

2. 运行搜索，然后选择**可视化**选项卡。
3. 从“可视化挑选器”选择**单值可视化**。

显示单值可视化。

4. 选择自定义可视化的**格式**。
5. 在**常规**设置面板中，将“失败的尝试”添加到**标题**字段。可视化现在如下所示：



显示的计数值可以改变。

第 3 部分：将可视化保存为报表

1. 选择**另存为 > 报表**。
2. 配置报表。使用以下设置。

   标题：选择标题。
   时间范围挑选器：否。

3. 单击**保存**。

第 4 部分：添加报表到仪表板

1. 在下一屏幕中，选择**添加到仪表板**。
2. 选择**新建**来创建新的仪表板。
3. 提供一个仪表板标题。例如，“失败的登录”。
4. 选择**报表操纵的面板**。
5. 单击**保存**。

您已拥有具有一个面板的仪表板。该面板显示失败的验证总数。除了总计数外，您还可以添加显示有效和无效帐户失败计数的面板。

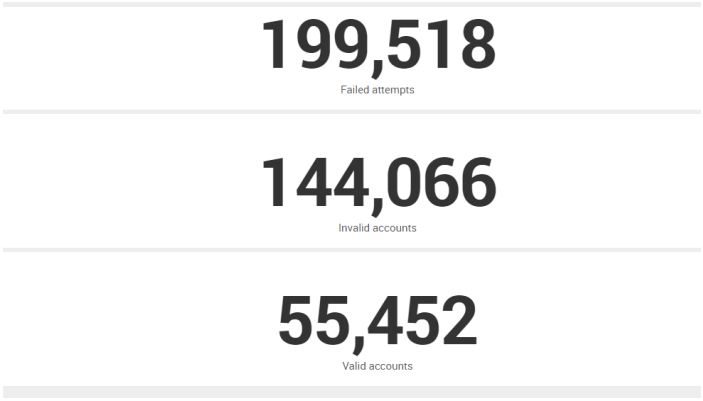
第 5 部分：生成额外的可视化

生成显示无效和有效帐户登录失败的单值可视化。

1. 按照前面的步骤来运行搜索，创建一个单值可视化，并添加标题。为两个新的可视化使用下面的搜索字符串和标题。

可视化显示	搜索	标题
无效帐户的登录失败	`sourcetype=secure failed "invalid user" | stats count`	无效帐户
有效帐户的登录失败	`sourcetype=secure failed NOT "invalid user" | stats count`	有效帐户

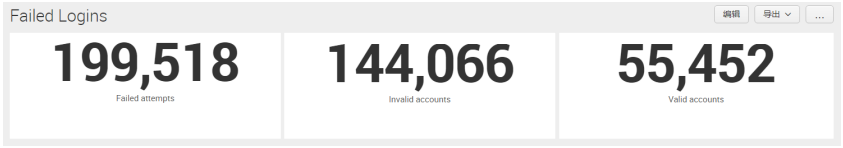
2. 每个可视化保存为报表并添加到仪表板。仪表板面板现在如下例所示。显示的计数可能会有所不同。



第 6 部分：开始自定义仪表板布局

为了节省空间，将所有的仪表板面板放在一行中。

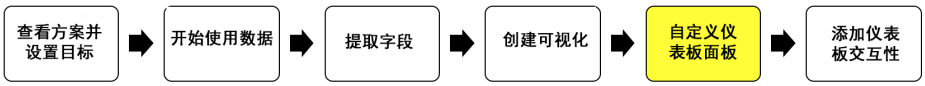
1. 选择**编辑 > 编辑面板**。
2. 单击并拖动面板，将它们放在一行中。



3. 单击**完成**。

方案的下一部分将介绍如何添加更多的自定义设置。

自定义仪表板面板



仪表板面板现在显示有关失败的登录的信息。除了每个值的标题，虽然，它们不包括太多的上下文。

自定义面板以便它们更容易进行大致解释。

- 更新单值可视化来根据严重程度以颜色标记值。
- 使用“简单 XML”简化面板布局。

第 1 部分：使用颜色来显示值的严重程度

为每个面板重复这些步骤。

1. 从仪表板中，选择**编辑 > 编辑面板**。
   在编辑模式中打开面板。
2. 单击其中一个面板的画笔图标。打开**格式**菜单。
3. 在**颜色**设置面板中，设置**使用颜色**为**是**。显示可配置的颜色和范围。
4. 在这种情况下，超过 10,000 次失败的登录是一个严重的问题。在该级别或更高级别的计数应以红色显示。调整所有的默认范围，以符合下列设置。

5. 关闭“格式”编辑器。

第 2 部分：简化仪表板

在一个面板中显示三个单值可视化来指示它们是密切相关的。编辑 XML 源代码来更改布局。

步骤

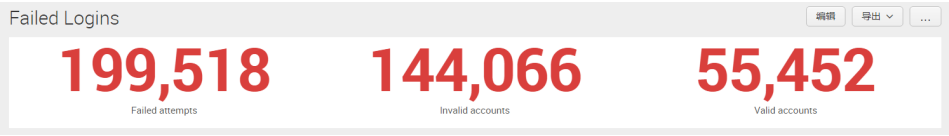
1. 从仪表板中，选择**编辑 > 编辑来源**，打开 XML 编辑器。
2. 注意，在 XML 源代码中，每个面板都是通过以下标记分离的。
   `<panel></panel>`
3. 通过删除面板之间的 `</panel>` 和 `<panel>` 标记，将所有的可视化放在一个面板中。

   第一个 `<panel>` 和最后一个 `</panel>` 标记保持不动。
   编辑的 XML 代码应如下所示。

```
<dashboard>
  <label>Failed Logins</label>
  <row>
    <panel>
      <single>
        <search>
          <query>sourcetype=secure failed | stats count</query>
        </search>
        <option name="colorBy">value</option>
        <option name="colorMode">none</option>
        <option name="drilldown">all</option>
        <option name="numberPrecision">0</option>
        <option name="rangeColors">["0x65a637","0x6db7c6","0xf7bc38","0xf58f39","0xd93f3c"]</option>
        <option name="rangeValues">[0,3000,7000,10000]</option>
        <option name="showSparkline">1</option>
        <option name="showTrendIndicator">1</option>
        <option name="trendColorInterpretation">standard</option>
        <option name="trendDisplayMode">absolute</option>
        <option name="underLabel">Failed attempts</option>
        <option name="unitPosition">after</option>
        <option name="useColors">1</option>
        <option name="useThousandSeparators">1</option>
        <option name="linkView">search</option>
      </single>
      <single>
        <search>
          <query>sourcetype=secure failed "invalid user"  | stats count</query>
        </search>
        <option name="colorBy">value</option>
        <option name="colorMode">none</option>
        <option name="drilldown">all</option>
        <option name="numberPrecision">0</option>
        <option name="rangeColors">["0x65a637","0x6db7c6","0xf7bc38","0xf58f39","0xd93f3c"]</option>
        <option name="rangeValues">[0,3000,7000,10000]</option>
        <option name="showSparkline">1</option>
```

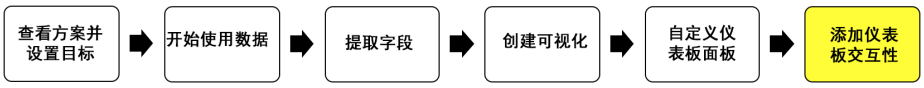
```
        <option name="showTrendIndicator">1</option>
        <option name="trendColorInterpretation">standard</option>
        <option name="trendDisplayMode">absolute</option>
        <option name="underLabel">Invalid accounts</option>
        <option name="unitPosition">after</option>
        <option name="useColors">1</option>
        <option name="useThousandSeparators">1</option>
        <option name="linkView">search</option>
      </single>
      <single>
        <search>
          <query>sourcetype=secure failed  NOT "invalid user" | stats count</query>
        </search>
        <option name="colorBy">value</option>
        <option name="colorMode">none</option>
        <option name="drilldown">all</option>
        <option name="numberPrecision">0</option>
        <option name="rangeColors">["0x65a637","0x6db7c6","0xf7bc38","0xf58f39","0xd93f3c"]</option>
        <option name="rangeValues">[0,3000,7000,10000]</option>
        <option name="showSparkline">1</option>
        <option name="showTrendIndicator">1</option>
        <option name="trendColorInterpretation">standard</option>
        <option name="trendDisplayMode">absolute</option>
        <option name="underLabel">Valid accounts</option>
        <option name="unitPosition">after</option>
        <option name="useColors">1</option>
        <option name="useThousandSeparators">1</option>
        <option name="linkView">search</option>
      </single>
    </panel>
  </row>
</dashboard>
```

4. 单击**保存**。三个可视化现在显示在同一个仪表板面板上。



转到下一步以完成仪表板。

添加仪表板交互性



您几乎已完成全部练习！

仪表板需要交互功能，以便用户可以找到关于黑客和目标帐户的更多详细信息。通过添加以下三个面板完成仪表板。

- 一张显示验证尝试失败次数最多的前五名黑客的 IP 地址的表格。
- 一张显示选定的黑客所瞄准的用户帐户的钻取表。
- 一张显示与选定的黑客的 IP 地址相关联的位置的钻取地图。

第 1 部分：添加显示前五名黑客的表格

1. 运行搜索以生成登录失败次数最多的前五名 IP 地址的表格。`sourcetype=secure failed | top 5 clientip`
2. 选择**统计**选项卡来查看结果表。注意，该表包括一个百分比列。最后两列命名为 `clientip` 字段和失败的登录计数。
3. 调整搜索以删除百分比列，并重命名最后两列。`sourcetype=secure failed | top 5 clientip showperc=f | rename clientip as "Hacker" count as "Failed Logins"`
4. 运行更新后的搜索并检查**统计**选项卡。现在新的表格只有您想要的两栏以及更具描述性的栏目标题。
5. 选择**另存为 > 仪表板面板**。
6. 将面板添加到现有的“失败的登录”仪表板，面板标题使用**前五名黑客**。
7. 单击**保存**。
8. 单击**查看仪表板**。
   仪表板现在包含一张显示前五名黑客 IP 地址的表格。

第 2 部分：从黑客表中设置钻取

在这种情况下，用户可能想要关于表中列出的黑客的更多信息。使表格更具互动性，以便用户可以单击一个黑客的 IP 地址来查看黑客的目标用户帐户列表。

您可以使用钻取来实现该互动。按照接下来的步骤在表格和列出目标用户帐户的新面板之间设置钻取。

步骤

1. 从仪表板中，选择**编辑** > **编辑来源**，打开 XML 仪表板源代码。
2. 滚动到页面底部，找到“前 5 名黑客”表格的 XML。
3. 创建一个钻取，使用令牌来捕获用户在表中选择的黑客的 IP 地址。

   为此，立即在 `<search>...</search>` 标记下方添加以下 XML。

```
<drilldown>
  <set token="hackerip">$click.value$</set>
</drilldown>
```

4. 注意，XML 代码定义了一个新的令牌 "hackerip"。该令牌像一个编程变量。设置令牌为从单击的表行中捕获一个值。您可以参考使用符号 `$hackerip$` 的搜索中的令牌。
5. 单击**保存**返回到仪表板。

第 3 部分：添加新表

此时，“前 5 名黑客”表格有设置来捕获用户选择的 IP 地址的钻取和令牌。现在您可以为目标帐户添加一个表格。驱动新表的搜索使用捕获的令牌值来显示该 IP 地址的目标帐户。

步骤

1. 从仪表板中，选择**编辑** > **编辑面板** > **添加面板**。打开面板选项列表。
2. 选择**新建** > **统计表**来创建新表。打开表格设置面板。
3. 使用设置面板来添加以下表格组件。
   - **标题：**$Hackerip$ 的目标帐户
   - **搜索字符串：**

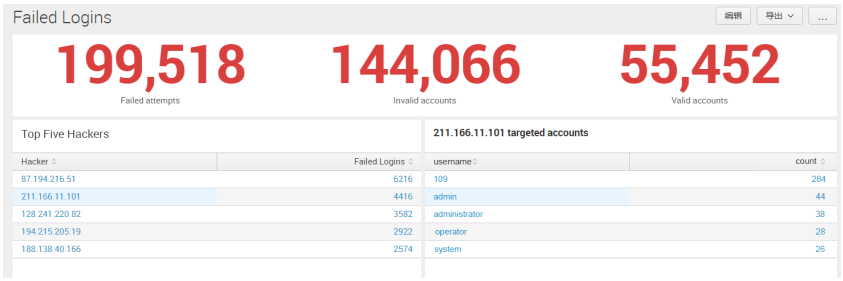
     ```
     sourcetype=secure clientip="$hackerip$" | stats count by username | sort -count
     ```

   注意，新的搜索查找其中 `clientip` 字段包含 `$hackerip$` 令牌值的事件。搜索也通过 `username` 来聚合事件，并以递减的顺序对它们进行排序。
4. 单击**添加到仪表板**并关闭表格设置面板。
   新面板现在会显示在仪表板底部。它仍未显示任何数据，因为只有当用户单击“前 5 名黑客”表格中的一个 IP 地址时才会填充该面板。
5. 单击“前 5 名黑客”表格中的一个 IP 地址来试着钻取。应该填充新表。

第 4 部分：调整仪表板布局和表格显示

在仪表板中为最后一个面板留出空间。

1. 选择**编辑** > **编辑面板**。单击并拖动新面板，以便显示在“前 5 名黑客”面板的右侧。
2. 单击右上角的**完成**来提交编辑。
3. 为下一个面板留出更多的空间。为此，调整目标帐户面板来显示较少的行。
   1. 选择**编辑** > **编辑面板**。
   2. 单击目标帐户面板中的画笔图标。打开“格式”菜单。
   3. 将**每页显示行数**设置更改为 5。
   4. 关闭“格式”菜单。现在对齐底部面板，并为最后一个面板留出空间。
4. 单击右上角的**完成**来提交编辑。
5. 更新后的仪表板外观现在应如下所示。



第 5 部分：创建显示黑客位置的钻取地图

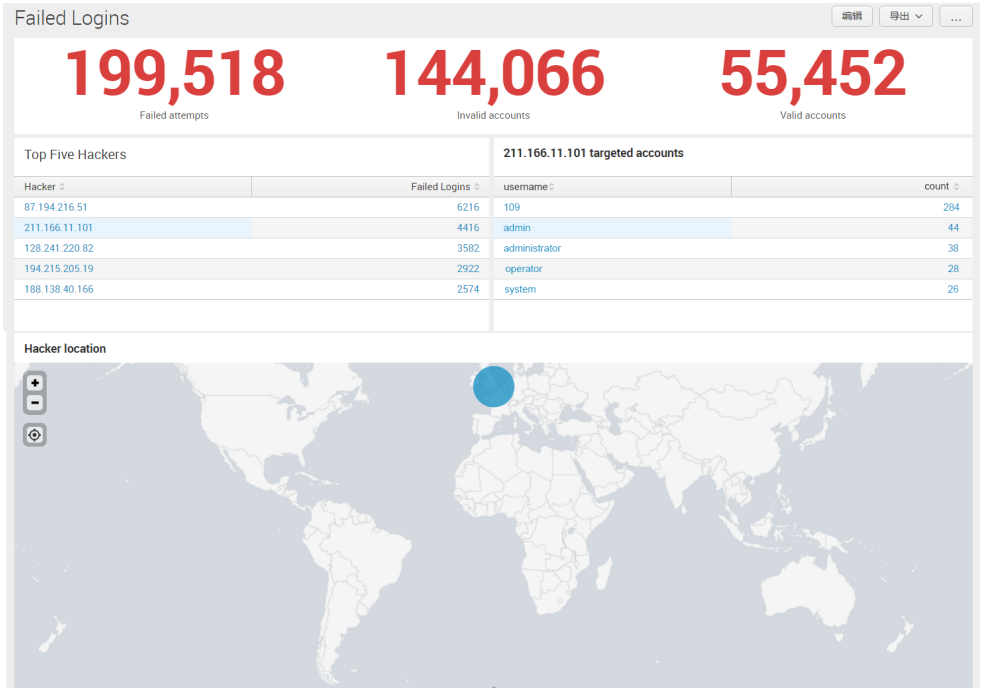
向仪表板添加最终的面板以在地图上显示黑客的 IP 地址。新面板使用来自“前 5 名黑客”面板的钻取来生成地图。

步骤

1. 选择**编辑 > 编辑面板 > 添加面板**。打开面板选项列表。
2. 选择**新建 > 地图**。添加以下面板设置。

   标题：黑客位置
   搜索字符串：`sourcetype=secure failed clientip="$hackerip$" | dedup clientip | iplocation prefix=cip_ clientip | geostats latfield=cip_lat longfield=cip_lon count`

   注意，该搜索查找其中 `clientip` 字段包含从“前 5 名黑客”表格中选择的 `$hackerip$` 值的事件。它也会删除 `clientip` 字段的重复值，并为黑客的 IP 地址生成纬度和经度坐标。具有同一纬度和经度的搜索计数事件。
3. 单击**添加到仪表板**。
4. 关闭表格设置面板，并单击**完成**以保存编辑。
5. 通过单击“前 5 名黑客”表格中的 IP 地址来尝试新的钻取。应该填充“目标帐户”和“黑客位置”面板。完成的仪表板如下所示。



结论

恭喜！您现在有一个提供多种信息一览的互动仪表板。

要了解关于该方案中包括的概念和工具的更多信息，请参阅下面的资源。

如欲了解	请参阅
• 编写搜索	*搜索手册*

• 转换和其他命令	*搜索参考*
• 字段和字段提取	*知识管理器手册*
• 创建和编辑可视化 • 创建和编辑仪表板 • 钻取互动 • 简单 XML • 令牌	*仪表板和可视化*
• 额外的自定义仪表板实现示例	仪表板示例应用