Scirius 用户手册

V 2.0.0

原著：Stamus Networks

日期：2018 年 4 月 1 日

翻译：resehist

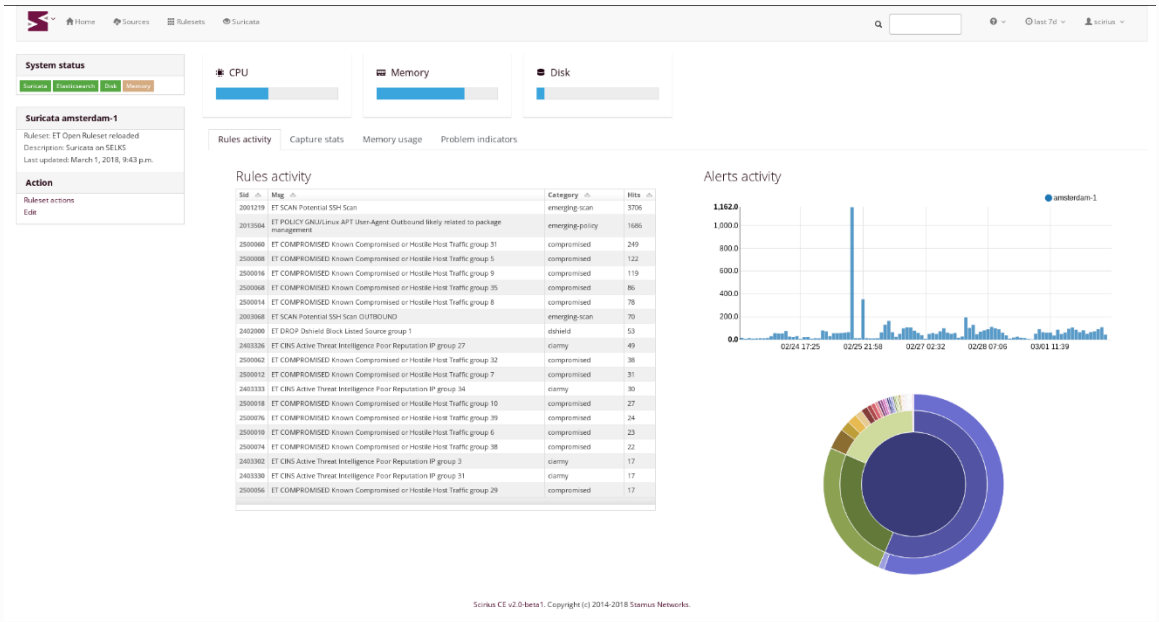
支持：360 Meshfire Team

日期：2018 年 9 月 29 日

目录

1、介绍

Scirius Community Edition 是一个专用于 Suricata 规则集管理的 Web 界面。它可以管理规则文件和更新相关文件。



Scirius CE 由 Stamus Networks 开发，通过 GNU GPLv3 许可证。

2、安装和设置

2.1 安装 Scirius CE

Scirius CE 是一个用 Django 编写的应用程序。它至少需要 Django 1.11 并且还不支持 Django 2.0。

Scirius CE 还使用 webpack 来构建 CSS 和 JS 包。

2.1.1 依赖

安装依赖项的简单方法是使用 pip：

在 Debian 上，你可以运行

```
aptitude install python-pip python-dev
```

然后，您可以安装 django 和依赖项

```
pip install -r requirements.txt
```

要使用处理 suricata restart 的 suri_reloader 脚本，您还需要 pyinotify

```
pip install pyinotify
```

据反馈，在一些 Debian 系统中强制要求较新版本的 GitPython

```
pip  install  gitpython == 0.3 。1 - beta2
```

您还可能需要 gitdb 模块

```
pip  install  gitdb
```

对于 npm 和 webpack，您需要稳定版本的 npm 和 webpack 3.11 版。在 Debian 上你可以使用下面命令

```
sudo  apt - get  install  npm
sudo  npm  install  - g  npm @latest  webpack @ 3 。11
npm  install
```

2.1.2 运行 Scirius CE

从源目录内，您可以启动 Django 数据库

```
python manage.py syncdb
```

默认情况下，身份验证在 scirius 中，因此您需要创建一个超级用户帐户。

在启动应用程序之前，您需要通过运行 webpack 来构建 bundle

```
webpack
```

此步骤将在每次代码更新后完成。

尝试 Scirius CE 的最简单方法之一是运行 Django 测试服务器

```
python manage.py runserver
```

然后你可以连接到 `localhost:8000`。

如果您需要应用程序来侦听可访问的地址，您可以运行类似的地址

```
python manage.py runserver 192.168.1.1:8000
```

2.2 Suricata 设置

Scirius CE 会生成一个包含所有已激活规则的规则文件。编辑 Suricata 对象时，必须设置要生成此文件的目录以及要复制的规则集的关联文件。

Scirius CE 不会改变您的 Suricata 配置文件 `suricata.yaml`。所以你必须更新它以指向 Scirius CE 设置数据的目录。如果您只使用 Scirius CE 生成的规则，则应该在 `suricata.yaml` 文件中看起来像

```
default-rule-path: /path/to/rules
rule-files:
 - scirius.rules
```

要与 Scirius CE 交互，您需要检测何时 `/path/to/rules/scirius.reload` 创建文件，在这种情况下启动重新加载或重新启动 Suricata，并在完成后删除重新加载文件。

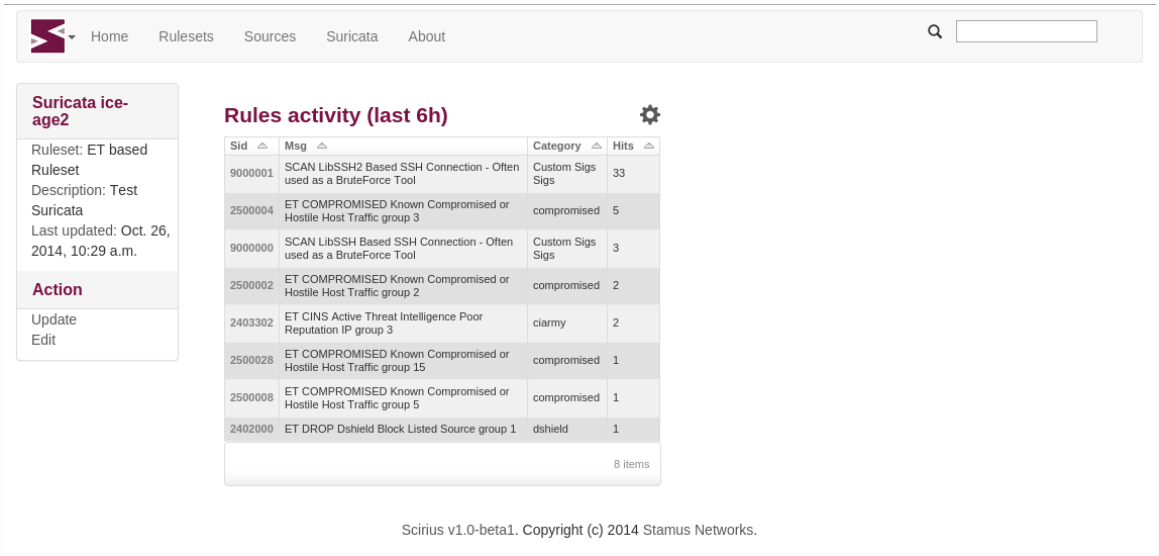
一种方法是使用 `suricata/scripts` 目录中的 `suri_reloader` 脚本 `suri_reloader` 的语法可以类似于

```
suri_reloader -p /path/to/rules  -l /var/log/suri-reload.log  -D
```

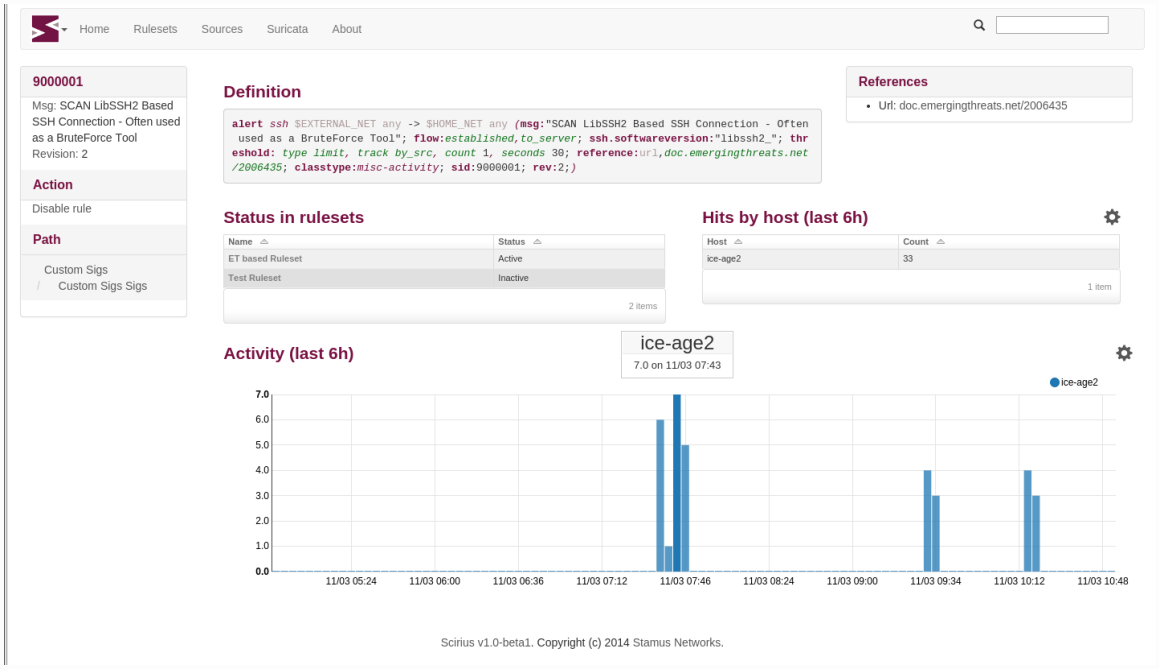
使用 `-h` 选项获取完整的选项列表。请注意， `suri_reloaded` 使用该 `service` 命令重新启动或重新加载 Suricata。这意味着您需要一个 init 脚本才能使其正常工作。

2. 3 连接 Elasticsearch

如果您使用 Suricata 的 Eve 日志记录和 Elasticsearch，则可以获取 Suricata 中有关签名的信息，并展示在页面中：



您还可以获取有关特定规则的图表和详细信息：



要设置 Elasticsearch 连接，您可以在 `scirius` 目录下编辑 `settings.py` 或创建 `local_settings.py` 文件以设置该功能。如果 `settings.py` 中的变量名称 `USE_ELASTICSEARCH` 设置为 True，则激活 Elasticsearch 。Elasticsearch 的地址存储在 `ELASTICSEARCH_ADDRESS` 变量中并使用该格式 `IP:port` 。

例如，如果您的 Elasticsearch 在本地运行，则可以添加到 `local_settings.py`

```
USE_ELASTICSEARCH = True
ELASTICSEARCH_ADDRESS = "127.0.0.1:9200"
ELASTICSEARCH_VERSION = 2 # In 1, 2, 5 set depending on ES major version
```

请注意，Suricata 的名称（在对象编辑期间设置）必须等于 Elasticsearch 的 `host`。它也可以在这里编辑：scirius - > suricata - >edit。

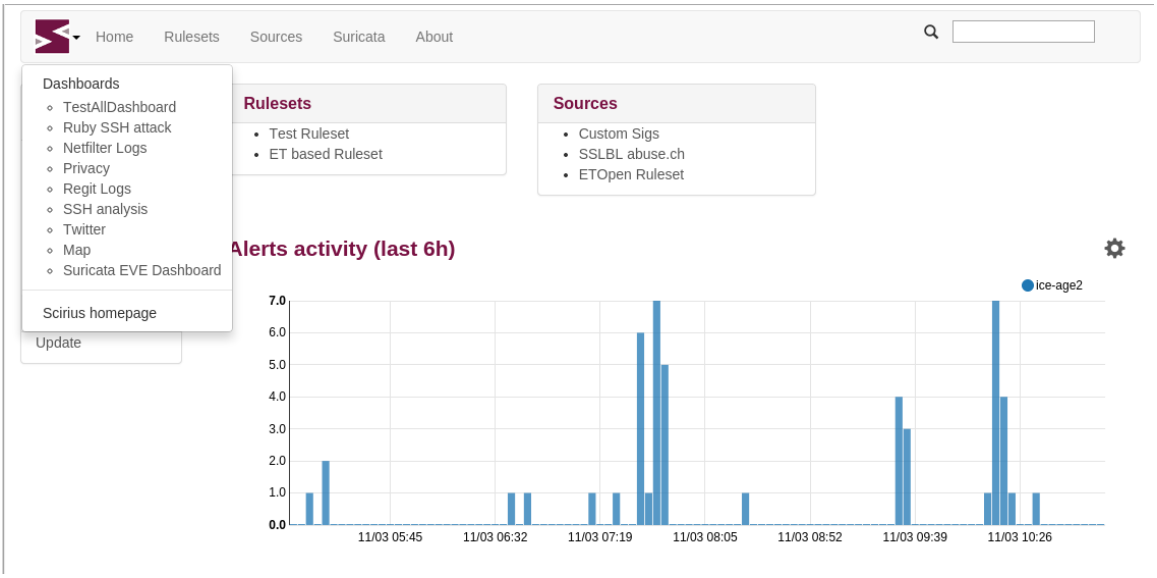
在 logstash 端，唯一必要的是确保@timestamp 等于 Suricata 事件中提供的时间戳值。为此，如果 Suricata 事件属于 *SELKS* 类型，则可以使用

```
filter {
  if [type] == "SELKS" {
    date {
      match => [ "timestamp", "ISO8601" ]
    }
  }
}
```

这对于避免 Scirius CE 生成的图形出现故障是必要的。

2.4 连接 Kibana

如果您使用的是 Kibana，可以通过单击左上角的图标获取指向仪表板的链接：



要激活该功能，您需要编辑 *local_settings.py* 文件：

```
KIBANA_URL  =  “http: // localhost /”
USE_KIBANA  =  True
```

3 管理账户

此菜单选项允许用户管理 - 编辑/创建和删除不同的用户帐户，更改用户详细信息和密码。在此菜单中，您还可以查看当前可用用户的列表以及这些帐户的设置。

3.1 添加/创建用户

要添加/创建新用户：在左上角单击 Stamus Networks 徽标下拉图标 - > 。`Manage Accounts`

在 `User Management pageActionAdd` ，点击 `Action` 面板- >点击 `Add`。

3.2 编辑用户

要编辑现有用户，请执行以下操作：在左上角单击 Stamus Networks 徽标下拉图标 - > `Manage Accounts`

在 `User Management PageUsers listUsername` ，在 `Users list` - >点击你要编辑的用户 `Username` 。

在 `Actions` 面板中 - >单击 `Edit user`。

3.3 更改用户密码

要更改用户密码：在左上角单击 Stamus Networks 徽标下拉图标 - > 。`Manage Accounts`

在 `User Management PageUsers listUsername` ，在 `Users list` - >点击其密码要改变用户的 `Username`。

在 `Actions` 面板中 - >单击 `Change user password`。

3.4 删除用户

要删除用户：在左上角单击 Stamus Networks 徽标下拉图标 - > `Manage Accounts`。

在 `User Management PageUsers listUsername` ，在 `Users list` - >单击要删除的用户 `Username`。

在 `Actions` 面板中 - >单击 `Delete user`。

3.5 用户权限：

有三个级别的权限：

- 允许活动用户连接到 Scirius 但只具有读取权限
- 员工用户可以在 Scirius 中行动（设备编辑，规则集推送，...）
- 超级用户具有完全不受限制的访问权限，包括在本地数据库中编辑用户身份验证设置和用户创建。

要处理权限级别：在左上角单击 Stamus Networks 徽标下拉图标 - > `Manage Accounts`。

在 `User Management PageUsers listUsername`，在 `Users list` - >点击其权限级别要更改用户的 `Username`。

在 `Actions` 面板- >点击 `Edit user`，并通过启用/禁用 `Active`，`Staff User`，`Superuser` 复选框设置权限级别。

4 规则集

4.1 规则集处理的哲学

Scirius 允许您定义一个 `Ruleset`，Ruleset 是一组规则定义了 Stamus Networks Suricata 探测器检测和检查的规则行为。您可以拥有任意数量的规则集，并且可以将特定的 `Ruleset` 加到许多 `Appliances`。

规则集由不同的 `Sources` 中选择的组件组成。如删除某些规则，更改签名中的内容, 然后再将其推送到网络探测器。

Source 是一组向 Suricata 提供信息的文件。例如，这可以是从官方 ET URL（或任何其他 URL）下载或在本地上载的 EmergingThreats 规则集。

当包含签名的源在多个文件中拆分时，每个单独文件中的签名集称为类别。

4.2 用户操作记录

记录规则集管理中执行的所有操作。可以使用 Stamus 图标菜单 `Actions history` 访问其历史记录。

每个 Action 都可操作，以允许用户交互使用。

4.3 规则集管理

规则集管理包含 `Rulesets` 和 `Sources` 两个主菜单选项。

因此，要创建规则集，必须创建一组 `Sources` 然后将它们链接到规则集。完成此操作后，您可以选择要使用的源的哪些元素。例如，对于签名规则集，您可以选择要使用的类别以及要禁用的单个签名。

定义规则集后，可以将其附加到 Probe。为此，只需编辑 Probe 对象并在列表中选择 Ruleset。

4.4 创建源

有两种方法可以创建 Source。第一个是使用预定义的公共源，第二个是通过手动添加。

4.4.1 公共资源

转到 `Sources -> Add public sourceAddActions`（`Add` 位于 `Actions` 侧栏中的菜单中）。

选择一个来源，然后单击 `Add` 按钮。在弹出窗口中，您可以选择要添加源的规则集。在某些情况下，会有一些字段，例如要输入的规则编辑器提供的密钥。

4.4.2 手动添加

要创建源，请转到 `Sources -> Add custom sourceAddActionsSubmit`（位于侧栏中的 菜单中），然后设置不同的字段并单击。

数据类型 `Signatures files in tar archive` 的来源必须遵循一些规则：

- 它必须是 tar 存档
- 所有文件必须位于 `rules` 目录下

例如，如果要为 Suricata 4.0 获取 ETOpen Ruleset，可以使用：

- 名称：ETOpen 规则集
- URI：https：//rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz

数据类型源 `Individual signature files` 必须是包含签名的单个文件。

例如，如果您想使用来自 abuse.ch 的 SSL 黑名单，您可以使用：

- 名称：SSLBL abuse.ch
- URI：https：//sslbl.abuse.ch/blacklist/sslblacklist.rules

数据类型 `Other content` 的来源必须是单个文件。它将使用其名称作为文件名复制到 Suricata 规则目录。

如果是方法 `HTTP URL`，您将看到一个 `Optional authorization key` 字段。此字段是可选字段，可用于针对远程服务器对 Scirius 进行身份验证。它为 HTTP 请求添加了一个授权标头，允许对大量第三方服务进行身份验证。这可以特别用于从 MISP 实例导入签名。有关更多信息，请参阅 MISP 文档。

4.5 更新源

要更新源，首先需要选择它。为此，请转到 `Sources` 然后在数组中选择所需的 Source。

然后，您可以单击 `Update` 侧栏中的菜单。此步骤可能需要很长时间，因为它可能需要一些下载和大量解析。

更新后，您可以通过弹出的链接浏览结果。

4.6 创建规则集

要创建规则集，请转到 `Ruleset -> Add` （ `Add` 位于侧栏中的 `Actions` 菜单中）。然后设置规则集的名称并选择要使用的源并单击。

您可以选择要使用的源和要转换的规则。有关它们的更多信息，请参阅规则转换。

4.7 更新规则集

要更新规则集，首先需要选择它。为此，请转到 `Ruleset` 然后在数组中选择所需的 Ruleset。

然后，您可以单击侧栏中 `Update` 的 `Action` 菜单。此步骤可能需要很长时间，因为它可能需要下载不同的源和重度解析。

4.8 编辑规则集

要编辑规则集，首先需要选择它。为此，请转到 `Ruleset` 然后在数组中选择所需的 Ruleset。

然后，您可以单击侧栏中 `Action` 菜单中的 `Edit` 。

现在 `Action` 菜单中有不同的操作

- 编辑源：选择要在规则集中使用的签名源
- 编辑类别：选择要在规则集中使用的签名类别
- 将规则添加到抑制列表：如果规则在此列表中，则它不会是生成的规则集的一部分
- 从被抑制列表中删除规则：这将从前面提到的列表中删除规则，从而在规则集中重新启用它

4.8.1 编辑源

要选择要使用的源，只需通过复选框选择它们，然后单击 `Update sources`。请注意，选择要启用的类别是添加新源时过程的下一步。

4.8.2 编辑类别

要选择要使用的类别，只需通过复选框选择它们，然后单击 `Update categories`。

4.8.3 将规则添加到抑制列表

使用搜索字段查找要删除的规则，可以使用签名中的 SID 或任何其他元素。Scirius 将在签名定义中搜索输入的文本，并返回规则列表。然后，您可以通过单击复选框 `Add selected rules to suppressed list` 并单击来删除它们。

4.8.4 从被抑制列表中删除规则

要从抑制列表中删除规则，只需在阵列中检查它们并单击 `Remove select rules from suppressed list` 即可。

4.9 抑制和阈值

可以通过抑制或阈值控制特定签名的警报数量。

当需要最小化警报数时，通常使用阈值处理 - 例如，来自该签名的源或目标 IP 的每分钟最多 1 个警报。

当需要抑制警报时使用抑制 - 也就是说不从该源或目标 IP 生成针对该特定签名的警报。

4.9.1 抑制警报

从显示警报列表的任何表中，单击 `sid` 需要抑制的警报的特定内容。这将显示规则页面。在那里，您可以单击 `Action` 左侧菜单下的 `Edit rule` ，然后在同一菜单中选择 `Suppress rule` 。在规则页面中，您还可以通过在 `Ip and Time stats` 或 `Advanced Data` 选项卡上单击 IP 地址旁边的 `x` 抑制创建页面。

在新页面上，如果对该特定签名已经存在某些阈值或抑制，您将被告知。可用字段是：

- `Ruleset` 适用于此配置的规则集
- `Track by` （必填字段）按源或目标 IP 进行跟踪
- `Net` IP 和/或特定网络的有效性。

选择规则集，源或目标（针对该特定 IP），然后单击`+Add`。

您还可以选择对整个网络强制执行抑制和/或使用 IP 列表。您可以像这样在`Net`字段中添加：

```
10.10.10.0/24,1.1.1.1,2.2.2.2
```

您可以通过单击`Rules info`选项卡来验证抑制。您将获得有关不同（如果有）阈值和抑制配置状态的信息显示。或者，您也可以通过单击并选择已应用特定抑制或阈值的规则集来查看该视图。

为了使抑制变为活动状态，您需要`Push`更新探针的规则集。有关完整说明，请参阅 SEE 上的 updates -appliances-ruleset 和 Scirius CE 上的更新规则集。

4.9.2 门限警报

从显示警报列表的任何表中，单击`sid`需要抑制的警报的特定内容，这将显示规则页面。在那里，您可以单击`Action`左侧菜单下的`Edit rule`，然后在同一菜单中选择`Threshold rule`。在规则页面中，您还可以通过`Ip and Time stats`或`Advanced Data`选项卡上单击 IP 地址旁边的向下箭头（旁边）来访问阈值创建页面。

在新页面上，如果对该特定签名已经存在某些阈值或抑制，您将被告知。可用字段是：

- `Type`阈值的类型。有以下 3 种：

  `limit` - 将警报限制为最多“X”次。

  `threshold` - 规则生成警报之前的最低阈值。

  `both` - 应用限制和阈值。
- `Ruleset` 适用于此配置的规则集
- `Track by` （必填字段）按源或目标 IP 进行跟踪
- `Count` 生成警报的次数。

- `Seconds` 在那个时间跨度内

您可以通过单击 `Rules info` 选项卡来验证阈值。您将获得有关不同（如果有）阈值和抑制配置状态的信息显示。或者，您也可以通过单击 `Rulesets` 并选择已应用特定抑制或阈值的规则集来查看该视图。

要使阈值变为活动状态，您需要 `Push` 更新探针的规则集。有关完整说明，请参阅 SEE 上的 updates -appliances-ruleset 和 Scirius CE 上的更新规则集。

4.10 规则转换

有三种类型的规则转换。第一个 *Action* 允许更改特定规则的操作 - 删除，拒绝或文件存储。请注意，这些操作需要有关规则和规则关键字语言的高级知识。第二个是 *Lateral*，它修改规则以检测横向移动，第三个是 *Target*，它通过添加 target 关键字来更新签名。

转换与规则集相关。但是它们可以在规则集上全局设置，也可以在类别或特定规则上设置。因此很容易处理异常。

4.10.1 动作转换

一旦您有一个特定的规则，您想要转换 - 在左侧面板的规则的详细信息页面下 `Actions` 单击 `Transform rule`。您将看到一些选择：

- 选择形式的转换类型：

  `drop` - （IPS 模式）将规则从警报转换为丢弃 - 也需要事先明确设置和配置 IPS 模式。

  `reject` - （IDPS / hybrid）会将规则从 alert 转换为 reject，这意味着当触发 RST /或 dst 不可达数据包时，将发送到 src 和 dst IP。

  `filestore` - 将仅转换那些具有允许文件提取的协议的规则 - 例如 `alert http...` 或 `alert smtp`。

- 选择您希望添加/注册新转换的规则的规则集。

注意：特定规则只能转换一次。

注意：要使用此 `drop` 功能，您需要具有有效的 IPS 设置。

完成所需的选择后，您可以添加注释以进行问责，然后单击 `Valid`。您将在 `Information` 选项卡中获得有关已转换规则的详细信息。您可以查看并确认转换及其添加的规则集以及任何注释。

只能转换活动的规则。如果规则在特定规则集中未处于活动状态，则它将不具有左侧面板上可用的转换或抑制/阈值选项。要使其处于活动状态，您可以通过单击左侧面板菜单上的选项 `Toggle availability` 来切换该规则的可用性。

规则详细信息页面的历史记录选项卡将对已转换的规则进行任何注释和更改以进行跟踪。

4.10.2 横向移动

签名通常使用 EXTERNAL_NET 和 HOME_NET 变量编写，这意味着如果流的两端都在 HOME_NET 中，它们将不匹配。因此，未检测到横向运动。这种转换将 EXTERNAL_NET 改为任何能够检测横向运动的。

该选项可以有三个值：

- No：不替换
- Yes：EXTERNAL_NET 由 any 替换
- Auto：如果签名验证某些属性，则完成替换

4.10.3 目标关键字

自 Suricata 4.0 起可用，目标关键字可用于指示触发签名的流的哪一侧是目标。如果存在此密钥，则会增强相关事件以包含攻击的源和目标。

该选项有四个值：

- Auto：如果存在目标，则使用算法确定目标
- Destination：目标是目标 IP
- Source：目标是源 IP
- None：没有进行转换

5 Hunt

5.1 介绍

Hunt 是一个专门用于签名和事件可视化和调优的界面。它可以通过 Scirius Enterprise 顶级菜单中的 `Hunt` 链接进入。

Hunt 使用向下钻取方法来选择事件。通过单击字段值旁边的放大镜图标，可以简单地添加警报事件中包含的协议元数据的过滤器。

一旦定义了复合过滤器，用户就可以基于它采取行动。该操作将被用于与复合过滤器匹配的所有未来事件。

在 Community Edition 中，只能使用在 suricata 中创建抑制和阈值的字段。目前仅限于 `src_ip` 和 `dest_ip`。

在 Enterprise Edition 中，Stamus 探针可以为使用任意协议元数据的过滤器应用操作。

5.2 页面

可以通过左侧菜单中的单击访问页面。从一个页面跳到另一个页面将保持过滤器不受影响，允许分析师在可用的不同视图之间切换。

5.3 仪表板

此页面显示一个仪表板，其中包含可在警报中看到的最有趣的数据和协议元数据的统计信息。

5.4 签名

如果已创建签名 ID 的过滤器，此页面将显示签名或签名页面的列表。

5.5 提醒

此页面以列表形式显示各个警报事件。可以扩展事件以查看包括有关它的元数据的所有详细信息。

5.6 动作

此页面显示操作列表。列表已排序，过滤器按升序应用。

可以重新排序动作以调整过滤器的相应优先级。为此，只需单击操作右侧的三个点并填写表单即可。

5.7 历史

此页面显示用户在 Scirius 实例上执行的修改的历史记录。

5.8 首页

链接到 Scirius 主页。

5.9 动作

5.9.1 抑制

抑制操作将在匹配事件到达存储之前将其删除。

在 Scirius CE 中，需要具有签名 ID 和源或目标 IP 的过滤器才能创建操作。

对于 Stamus 探针，可以使用任何字段。

5.9.2 门槛

阈值操作仅在达到定义的阈值时保持警报。

在 Scirius CE 中，需要具有签名 ID 的过滤器才能创建操作。

在 Scirius EE 和 Stamus 探针中，可以使用任何字段。

5.9.3 标签

一个*标签*可以根据过滤器进行设置。它将在所有匹配事件上设置，并允许轻松分类。

目前有 2 个值：

- 信息：信息足够好，不会被压制，以防万一
- 相关：事件是相关的，需要进行调查

所有未标记的事件都可以在 *Untagged* 标签下找到。如果正确设置了已定义的操作，则应该是新签名或未引用的行为。所以应该进行调查和分类。

标记操作仅适用于 Scirius EE 和 Stamus 探针。

5.9.4 标记和保持

一个*标签，并保持*动作类似于*标签*的动作，但匹配的事件将不会受到任何后来的行动处理发现的行动来抑制或 thesholded。

标记和保持操作仅适用于 Scirius EE 和 Stamus 探针。

5.10 键盘快捷键

5.10.1 标签过滤

这是完整的清单：

- *A*：显示所有事件
- *R*：仅显示相关事件
- *I*：仅显示信息事件
- *U*：仅显示未标记的事件

6 Suricata 管理

6.2 设置

Suricata 编辑页面允许您设置 Suricata 的参数。

参数如下：

- 名称：探测器的主机名，确保它与 JSON 事件中的*主机*字段的值匹配
- 描述：suricata 的描述
- 规则目录：将在此目录中创建 *scirius.rules* 文件。Suricata 必须只使用此文件
- Suricata 配置文件：用于检测某些配置设置
- 规则集：选择要使用的规则集

6.2 更新规则集

要更新 Suricata 规则集，您可以转到 `Suricata -> Update`（在 `Actions` 菜单中 `Update`）。然后你必须选择你想要做的动作：

- Update：下载规则集使用的源的最新版本
- Build：基于当前版本的源构建 Suricata 规则集
- Push：触发 Suricata 重新加载以使其与最新的构建规则集一起运行

您还可以通过运行更新规则集并触发 Suricata 重新加载

```
python manage.py updatesuricata
```

7 备份

要开始备份，请运行

```
python manage.py scbackup
```

要恢复备份并清除所有数据，您可以运行

```
python manage.py screstore
python manage.py migrate
```

这将恢复最新的备份。要选择其他备份，请将备份文件名指定为第一个参数。要获取可用备份列表，请使用

```
python manage.py listbackups
```

您无法将备份还原到比已完成备份的 scirius 更旧的 scirius。

使用默认配置文件，备份在*/ var / backups 中的*磁盘上。由于 Scirius CE 使用 django-dbbackup 应用程序进行备份和还原过程，因此它可以从此应用程序中的所有可用方法中受益。这包括至少：

- FTP
- Amazon AWS
- Dropbox

有关可用方法及其配置的更多信息，请参阅 django-dbbackup 配置。