Scirius Documentation

Release 2.0.1

Stamus Networks

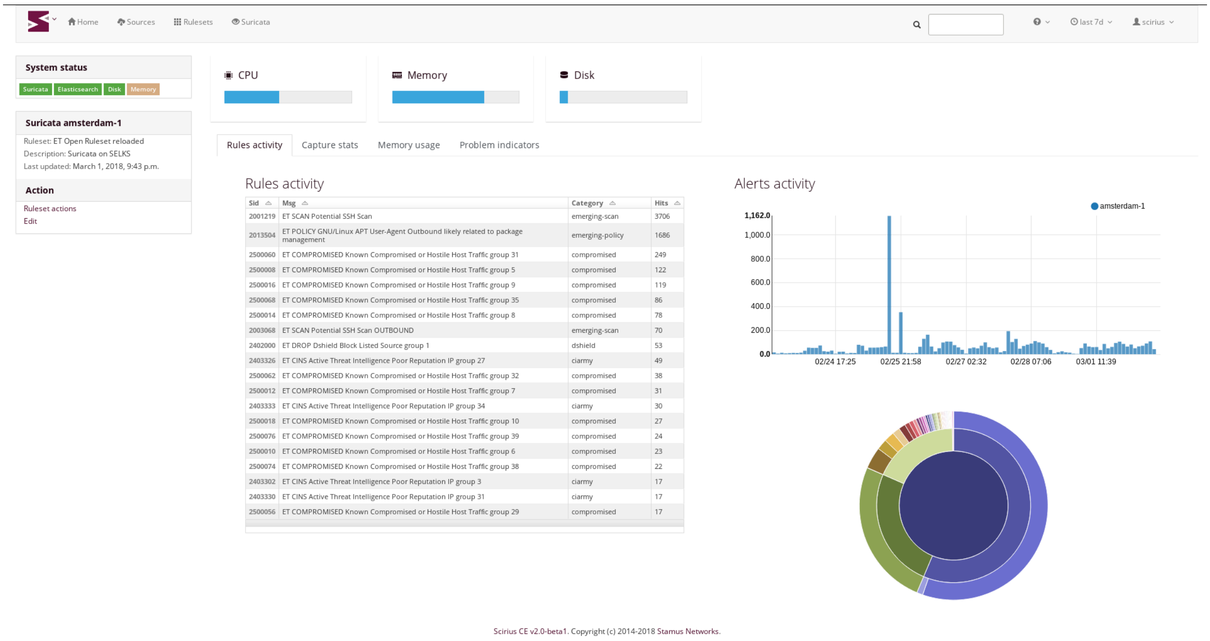
Apr 01, 2018

Contents:

CHAPTER 1

Introduction

Scirius Community Edition is a web interface dedicated to Suricata ruleset management. It handles the rules file and update associated files.



System status

Suricata Elasticsearch Disk Memory

Suricata amsterdam-1

Ruleset: ET Open Ruleset reloaded
Description: Suricata on SELKS
Last updated: March 1, 2018, 9:43 p.m.

Action

Ruleset actions
Edit

Rules activity

Sid	Msg	Category	Hits
2001219	ET SCAN Potential SSH Scan	emerging-scan	3706
2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	emerging-policy	1686
2500060	ET COMPROMISED Known Compromised or Hostile Host Traffic group 31	compromised	249
2500008	ET COMPROMISED Known Compromised or Hostile Host Traffic group 5	compromised	122
2500016	ET COMPROMISED Known Compromised or Hostile Host Traffic group 9	compromised	119
2500068	ET COMPROMISED Known Compromised or Hostile Host Traffic group 35	compromised	86
2500014	ET COMPROMISED Known Compromised or Hostile Host Traffic group 8	compromised	78
2003068	ET SCAN Potential SSH Scan OUTBOUND	emerging-scan	70
2402000	ET DROP Dshield Block Listed Source group 1	dshield	53
2403326	ET CINS Active Threat Intelligence Poor Reputation IP group 27	ciarmy	49
2500062	ET COMPROMISED Known Compromised or Hostile Host Traffic group 32	compromised	38
2500012	ET COMPROMISED Known Compromised or Hostile Host Traffic group 7	compromised	31
2403333	ET CINS Active Threat Intelligence Poor Reputation IP group 34	ciarmy	30
2500018	ET COMPROMISED Known Compromised or Hostile Host Traffic group 10	compromised	27
2500076	ET COMPROMISED Known Compromised or Hostile Host Traffic group 39	compromised	24
2500010	ET COMPROMISED Known Compromised or Hostile Host Traffic group 6	compromised	23
2500074	ET COMPROMISED Known Compromised or Hostile Host Traffic group 38	compromised	22
2403302	ET CINS Active Threat Intelligence Poor Reputation IP group 3	ciarmy	17
2403330	ET CINS Active Threat Intelligence Poor Reputation IP group 31	ciarmy	17
2500056	ET COMPROMISED Known Compromised or Hostile Host Traffic group 29	compromised	17

Scirius CE v2.0-beta1. Copyright (c) 2014-2018 Stamus Networks.

Scirius CE is developed by Stamus Networks and is available under the GNU GPLv3 license.

CHAPTER 2

Installation and setup

2.1 Installing Scirius CE

Scirius CE is an application written in Django. It requires at least Django 1.11 and has not yet support for Django 2.0.

Scirius CE also uses webpack to build CSS and JS bundles.

2.1.1 Dependencies

The easy way to install the dependencies is to use pip:

On Debian, you can run

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

You can then install django and the dependencies

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

To use the suri_reloader script which is handling suricata restart, you will also need pyinotify

```
pip install pyinotify
```

It has been reported that on some Debian system forcing a recent GitPython is required

```
pip install gitpython==0.3.1-beta2
```

You will also potentially needs the gitdb module

```
pip install gitdb
```

For npm and webpack, you need a stable version of npm and webpack version 3.11. On Debian you can do

```
sudo apt-get install npm
sudo npm install -g npm@latest webpack@3.11
npm install
```

2.1.2 Running Scirius CE

From inside the source directory, you can initiate Django database

```
python manage.py migrate
```

Authentication is by default in scirius so you will need to create a superuser account

```
python manage.py createsuperuser
```

Before starting the application you need to construct the bundles by running webpack

```
webpack
```

This step as to be done after each code update.

One of the easiest way to try Scirius CE is to run the Django test server

```
python manage.py runserver
```

You can then connect to `localhost:8000`.

If you need the application to listen to a reachable address, you can run something like

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

2.2 Suricata setup

Scirius CE is generating one single rules files with all activated rules. When editing the Suricata object, you have to setup the directory where you want this file to be generated and the associated files of the ruleset to be copied.

Scirius CE won't touch your Suricata configuration file aka `suricata.yaml`. So you have to update it to point to the directory where data are setup by Scirius CE. If you are only using rules generated by Scirius CE, you should have something looking like in your `suricata.yaml` file

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

To interact with Scirius CE, you need to detect when `/path/to/rules/scirius.reload` file are created, initiate a reload or restart of Suricata when it is the case and delete the reload file once this is done.

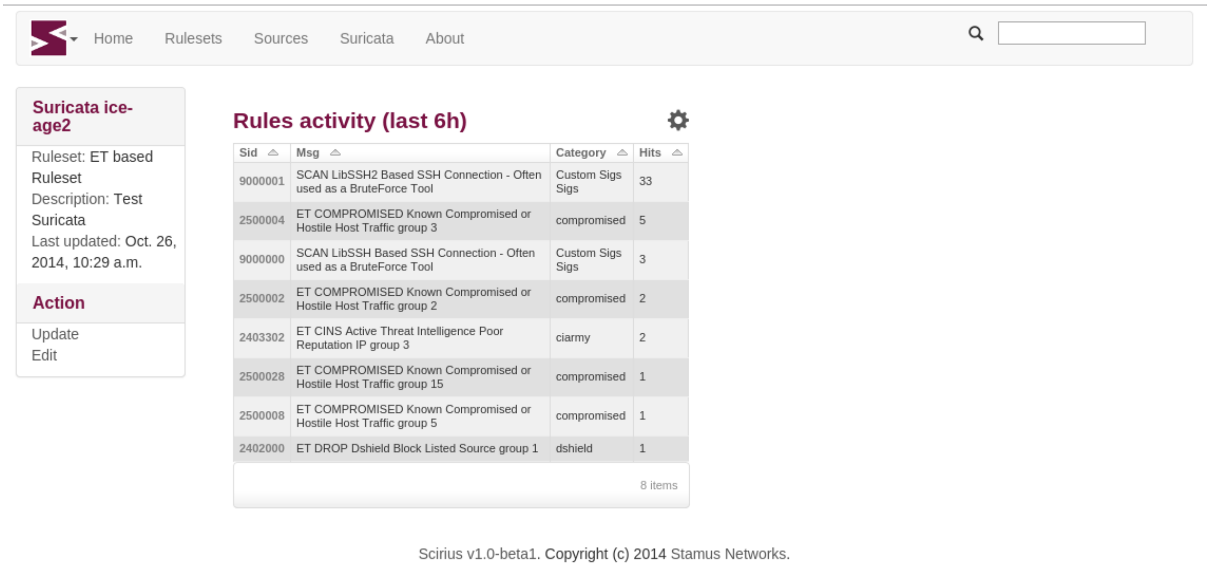
One possible way to do that is to use `suri_reloader` available in `suricata/scripts` directory. The syntax of `suri_reloader` can be something similar to

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

Use `-h` option to get the complete list of options. Please note that `suri_reloaded` uses the `service` command to restart or reload Suricata. This means you need a init script to get it working.

2.3 Link with Elasticsearch

If you are using Suricata with Eve logging and Elasticsearch, you can get information about signatures displayed in the page showing information about Suricata:



Suricata ice-age2

Ruleset: ET based Ruleset
Description: Test Suricata
Last updated: Oct. 26, 2014, 10:29 a.m.

Action

Update
Edit

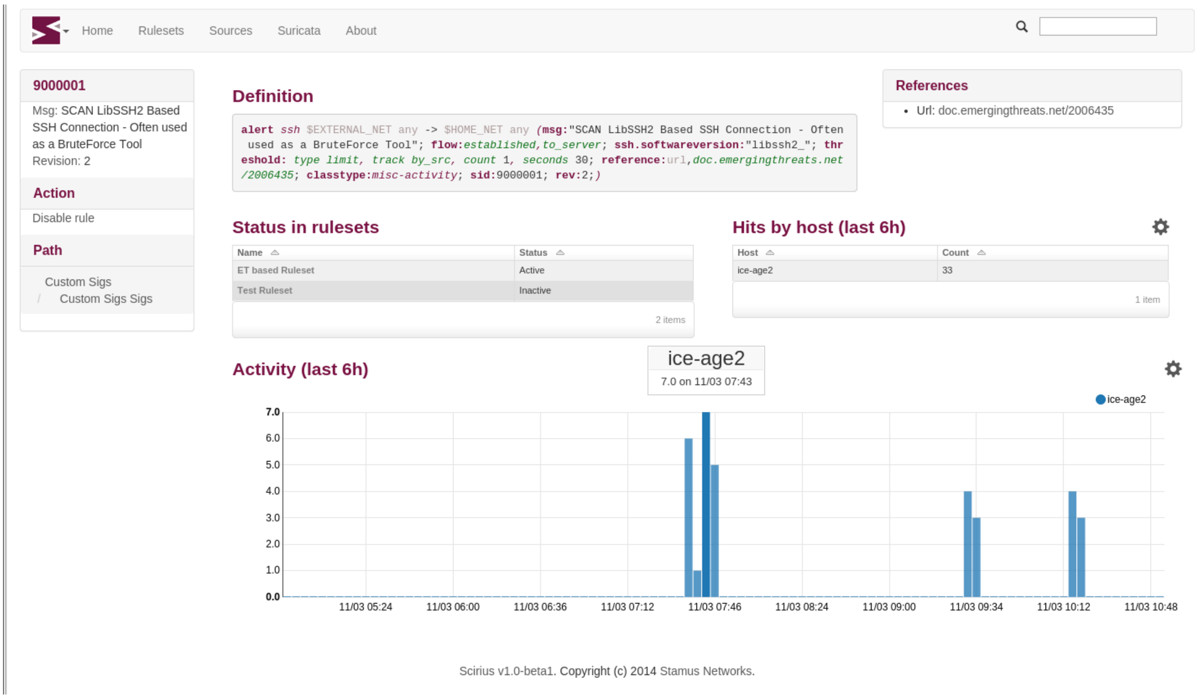
Rules activity (last 6h)

Sid	Msg	Category	Hits
9000001	SCAN LibSSH2 Based SSH Connection - Often used as a BruteForce Tool	Custom Sigs Sigs	33
2500004	ET COMPROMISED Known Compromised or Hostile Host Traffic group 3	compromised	5
9000000	SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool	Custom Sigs Sigs	3
2500002	ET COMPROMISED Known Compromised or Hostile Host Traffic group 2	compromised	2
2403302	ET CINS Active Threat Intelligence Poor Reputation IP group 3	ciarmy	2
2500028	ET COMPROMISED Known Compromised or Hostile Host Traffic group 15	compromised	1
2500008	ET COMPROMISED Known Compromised or Hostile Host Traffic group 5	compromised	1
2402000	ET DROP Dshield Block Listed Source group 1	dshield	1

8 items

Scirius v1.0-beta1. Copyright (c) 2014 Stamus Networks.

You can also get graph and details about a specific rule:



9000001

Msg: SCAN LibSSH2 Based SSH Connection - Often used as a BruteForce Tool
Revision: 2

Action

Disable rule

Path

Custom Sigs
/ Custom Sigs Sigs

Definition

```
alert ssh $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN LibSSH2 Based SSH Connection - Often
 used as a BruteForce Tool"; flow:established,to_server; ssh.softwareversion:"libssh2_"; thr
eshold: type limit, track by_src, count 1, seconds 30; reference:url,doc.emergingthreats.net
/2006435; classtype:misc-activity; sid:9000001; rev:2;)
```

References

- Url: doc.emergingthreats.net/2006435

Status in rulesets

Name	Status
ET based Ruleset	Active
Test Ruleset	Inactive

2 items

Hits by host (last 6h)

Host	Count
ice-age2	33

1 item

Activity (last 6h)

Scirius v1.0-beta1. Copyright (c) 2014 Stamus Networks.

To setup Elasticsearch connection, you can edit `settings.py` or create a `local_settings.py` file under `scirius` directory to setup the feature. Elasticsearch is activated if a variable names `USE_ELASTICSEARCH` is set to True in `settings.py`. The address of the Elasticsearch is stored in the `ELASTICSEARCH_ADDRESS` variable and uses the format `IP:port`.

For example, if your Elasticsearch is running locally, you can add to `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
```

Please note, that the name of the Suricata (set during edition of the object) must be equal to the `host` key present in Elasticsearch events. It can also be edited here: scirius -> suricata -> edit.

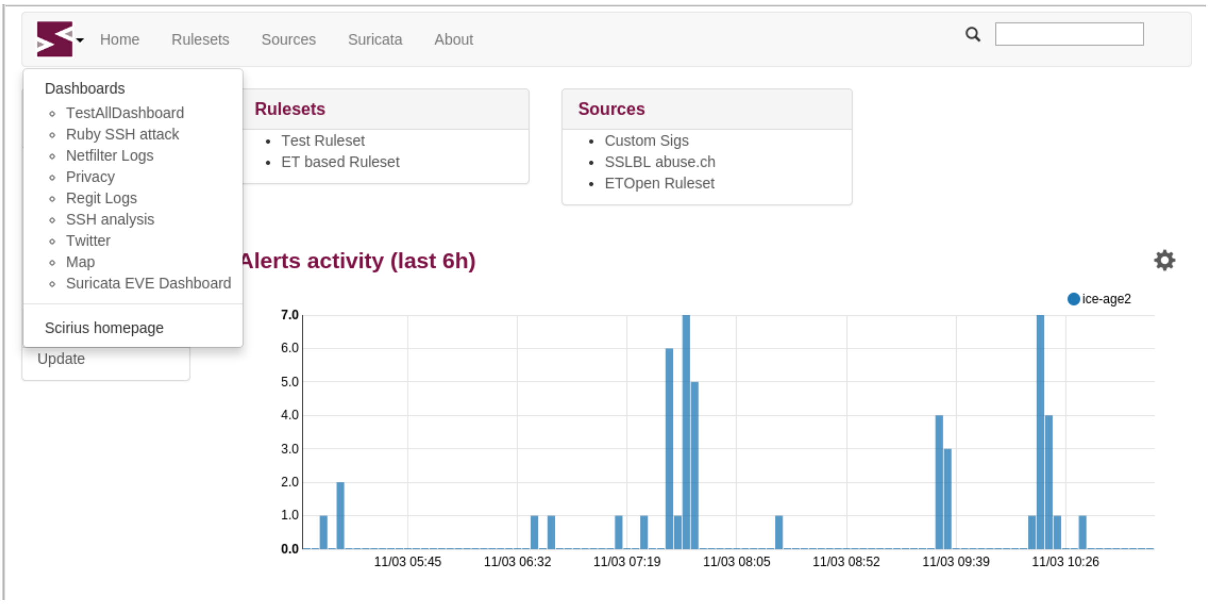
On logstash side, the only necessary thing is to make sure that the @timestamp is equal to the timestamp value provided in Suricata events. To do so and if you Suricata events are of type *SELKS* on can use

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

This is necessary to avoid glitch in the graphics generated by Scirius CE.

2.4 Link with Kibana

If you are using Kibana, it is possible to get links to your dashboards by clicking the top left icon:



To activate the feature, you need to edit your *local_settings.py* file:

```
KIBANA_URL = "http://localhost/"
USE_KIBANA = True
```

CHAPTER 3

Rulesets

3.1 Philosophy of Ruleset handling

Scirius allows you to define a `Ruleset` which is a set of rules defining the behaviour of Stamus Networks Suricata probes regarding detection and inspection. You can have as many Rulesets as you would like and you can attach a particular `Ruleset` to many `Appliances`.

A Ruleset is made of components selected in different `Sources`. Transformation such as removing some rules, altering content can be applied to the signatures in the ruleset before it is pushed to the network probe(s).

A Source is a set of files providing information to Suricata. For example, this can be EmergingThreats ruleset downloaded from the official ET URL (or any other URL) or uploaded locally.

When a Source containing Signatures is splitted in multiple files, the set of Signatures in each individual file is called a Category.

3.2 User actions logging

All actions done in ruleset management are logged. It is possible to access their history by using `Actions history` in the Stamus icon menu.

Optional comment are available for each action to allow users to interact with each other.

3.3 Ruleset management

The ruleset management encompasses both the `Rulesets` and `Sources` major menu options.

To create a ruleset, you thus must create a set of `Sources` and then link them to the ruleset. Once this is done, you can select which elements of the source you want to use. For example, in the case of a signature ruleset, you can select which categories you want to use and which individual signature you want do disable.

Once a Ruleset is defined, you can attach it to a Probe. To do that simply edit the Probe object and choose the Ruleset in the list.

3.4 Creating Source

There is two methods to create a Source. First one is to use predefined public sources and the second one via manual addition.

3.4.1 Public sources

Go to `Sources -> Add public source` (`Add` being in the `Actions` menu in the sidebar).

Choose a source and click on the `Add` button. In the popup you can select to which ruleset you want to add the source. In some cases there will be some fields like the secret key provided by the rules editors to be entered.

3.4.2 Manual addition

To create a Source go to `Sources -> Add custom source` (`Add` being in the `Actions` menu in the sidebar). Then set the different fields and click `Submit`.

A source of datatype `Signatures files in tar archive` has to follow some rules:

- It must be a tar archive
- All files must be under a `rules` directory

For example, if you want to fetch ETOpen Ruleset for Suricata 4.0, you can use:

- Name: ETOpen Ruleset
- URI: https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz

A source of datatype `Individual signature files` has to be a single file containing signatures.

For example, if you want to use SSL blacklist from abuse.ch, you can use:

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

A source of datatype `Other content` has to be a single file. It will be copied to Suricata rules directory using its name as filename.

If method is `HTTP URL`, you will see an `Optional authorization key` field. This field is optional and can be used to authenticate Scirius against the remote server. It adds an authorization header to HTTP request allowing authentication on a large number of third party services. This can be used in particular to import signatures from a MISP instance. See MISP documentation for more information.

3.5 Updating Source

To update a Source, you first need to select it. To do that, go to `Sources` then select the wanted Source in the array.

You can then click on `Update` in the menu in the sidebar. This step can take long as it can require some download and heavy parsing.

Once updated, you can browse the result by following links in the array.

3.6 Creating Ruleset

To create a Ruleset go to `Ruleset -> Add` (`Add` being in the `Actions` menu in the sidebar). Then set the name of the Ruleset and choose which Sources to use and click `Submit`.

You can select the Sources to use and the transformations to apply. For more informations about them, see *Rule transformations*.

3.7 Updating Ruleset

To update a Ruleset, you first need to select it. To do that, go to `Ruleset` then select the wanted Ruleset in the array.

You can then click on `Update` in the `Action` menu in the sidebar. This step can take long as it can require download of different Sources and heavy parsing.

3.8 Editing Ruleset

To edit a Ruleset, you first need to select it. To do that, go to `Ruleset` then select the wanted Ruleset in the array.

You can then click on `Edit` in the `Action` menu in the sidebar.

There is now different operations available in the `Action` menu

- Edit sources: select which sources of signatures to use in the Ruleset
- Edit categories: select which categories of signatures to use in the Ruleset
- Add rule to suppressed list: if a rule is in this list then it will not be part of the generated Ruleset
- Remove rule from suppressed list: this remove a rule from the previously mentioned list thus re-enabling it in the Ruleset

3.8.1 Edit Sources

To select which Sources to use, just select them via the checkbox and click on `Update sources`. Please note that selecting categories to enable is the next step in the process when you add a new source.

3.8.2 Edit Categories

To select which Categories to use, just select them via the checkbox and click on `Update categories`.

3.8.3 Add rule to suppressed list

Use the search field to find the rule(s) you want to remove, you can use the SID or any other element in the signature. Scirius will search the entered text in the definition of signature and return you the list of rules. You will then be able to remove them by clicking on the check boxes and clicking on `Add selected rules to suppressed list`.

3.8.4 Remove rule from suppressed list

To remove rules from suppressed list, simply check them in the array and click on `Remove select rules from suppressed list`.

3.9 Suppression and thresholding

Alert numbers for a particular signature can be controlled through suppression or thresholding.

Thresholding is usually used when number of alerts needs to be minimized - as for example maximum 1 alert per minute from that source or destination IP for that signature.

Suppression is used when the alerts need to be suppressed - aka do not generate alerts for that particular signature from that source or destination IP.

3.9.1 Suppress alerts

From any table displaying a list of alerts, click on the particular `sid` for the alerts that would need to be suppressed. This will display the rule page. There you can click on `Edit rule` under `Action` on the menu on the left hand side, then select `Suppress rule` in the same menu. From the rule page you can also reach the suppression creation page by being on the `Ip and Time stats` or `Advanced Data` tabs and clicking on the `x` next to the IP address.

On the new page you will be informed if there already is some threshold or suppression in effect for that particular signature. The available fields are:

- `Ruleset` for which ruleset this configuration applies
- `Track by` (mandatory field) to track by source or destination IP
- `Net` for which IP and/or particular network is that valid.

Choose the ruleset , source or destination (for that particular IP) and click `+Add`.

You can also choose to enforce the suppression for a whole network and/or use a list of IPs. You can add in the `Net` field like so:

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

You can verify the suppression by clicking on the `Rules info` tab. You will have an informational display about the status of the different (if any) threshold and suppression configurations. Alternatively you can also view that by clicking `Rulesets` and selecting the ruleset for which you have applied the particular suppression or threshold.

In order for the suppression to become active you need to `Push` the updated ruleset to the probes. See updating-appliances-ruleset on SEE and *Updating ruleset* on Scirius CE for complete instruction.

3.9.2 Threshold alerts

From any table displaying a list of alerts, click on the particular `sid` for the alerts that would need to be suppressed. This will display the rule page. There you can click on `Edit rule` under `Action` on the menu on the left hand side, then select `Threshold rule` in the same menu. From the rule page you can also reach the threshold creation page by being on the `Ip and Time stats` or `Advanced Data` tabs and clicking on the arrow down (next to the `x`) next to the IP address.

On the new page you will be informed if there already is some threshold or suppression in effect for that particular signature. The available fields are:

- `Type` type of the threshold. It can be:

  `limit` - limits the alerts to at most "X" times.

  `threshold` - minimum threshold for a rule before it generates an alert.

  `both` - both limiting and thresholding are applied.
- `Ruleset` for which ruleset this configuration applies
- `Track by` (mandatory field) to track by source or destination IP

- `Count` number of times the alert is generated.
- `Seconds` within that timespan

You can verify the thresholding by clicking on the `Rules info` tab. You will have an informational display about the status of the different (if any) threshold and suppression configurations. Alternatively you can also view that by clicking `Rulesets` and selecting the ruleset for which you have applied the particular suppression or threshold.

In order for the threshold to become active you need to `Push` the updated ruleset to the probes. See updating-appliances-ruleset on SEE and *Updating ruleset* on Scirius CE for complete instruction.

3.10 Rule transformations

There is three types of rules transformations. The first one *Action* allows the action of a particular rule to be changed - to drop, reject or filestore. Please note these actions requires advanced knowledge about rules and the rule keywords language. Second one is *Lateral* that modify the rules to detect lateral movement and third one is *Target* that update signatures by adding the target keyword.

Transformation are relative to a ruleset. But they can be set globally on a ruleset or set on a category or on a specific rule. So it is easy to handle exceptions.

3.10.1 Action transformation

Once you have a particular rule that you would like to transform - in the rule's details page on the left hand side panel under `Actions` click `Transform rule`. You will be presented with a few choices:

- Type of transformation to choose form:

  `drop` - (IPS mode) will convert the rule from alert to drop - aka IPS mode needs to be explicitly set up and configured before hand.

  `reject` - (IDPS/hybrid) will convert the rule from alert to reject meaning that when triggered a RST/or dst unreachable packets will be send to both the src and dst IP.

  `filestore` - will convert those rules only that have protocols allowing for file extraction - for example `alert http...` or `alert smtp`

- Choose a ruleset you wish the newly transformed rule to be added/registered in.

NOTE: A particular rule can be transformed only once.

NOTE: For using the `drop` functionality you need to have a valid IPS setup.

After you make the desired selection you can add in a comment for the purpose of accountability and click on `Valid`. You will have the details about the transformed rule in the `Information` tab. You can review and confirm the transformation and the ruleset it is add in alongside any comments.

Only rules that are active can be transformed. If a rule is not active in a particular ruleset it will not have the transformation or suppress/threshold options available on the left hand side panel. To make it active you can toggle the availability of that rule by clicking on the `Toggle availability` option on the left hand side panel menu.

The history tab of the rule details page will have any comments and changes to the transformed rule for traceability.

3.10.2 Lateral movement

Signatures are often written with the EXTERNAL_NET and HOME_NET variables and this means they won't match if both sides of a flow are in the HOME_NET. Thus, lateral movements are not detected. This transformation change EXTERNAL_NET to any to be able to detect lateral movements.

The option can have three values:

- No: the replacement is not done
- Yes: EXTERNAL_NET is replaced by any
- Auto: Substitution is done if signature verify some properties

3.10.3 Target keyword

Available since Suricata 4.0, the target keyword can be used to tell which side of a flow triggering a signature is the target. If this key is present then related events are enhanced to contain the source and target of the attack.

The option can have four values:

- Auto: an algorithm is used to determine the target if there is one
- Destination: target is the destination IP
- Source: target is the source IP
- None: no transformation is done

CHAPTER 4

Suricata management

4.1 Setup

The Suricata edit page allows you to setup the parameters of the Suricata.

The parameters are the following:

- Name: hostname of the probe, be sure it is matching value of *host* field in JSON events
- Descr: description of the suricata
- Rules directory: *scirius.rules* file will be created in this directory. Suricata must only use this file
- Suricata configuration file: used to detect some configuration settings
- Ruleset: choose the ruleset to use

4.2 Updating ruleset

To update Suricata ruleset, you can go to `Suricata -> Update` (`Update` being in the `Actions` menu). Then you have to select which action you want to do:

- Update: download latest version of the Sources used by the Ruleset
- Build: build a Suricata ruleset based on current version of the Sources
- Push: trigger a Suricata reload to have it running with latest build ruleset

You can also update the ruleset and trigger a Suricata reload by running

```
python manage.py updatesuricata
```

CHAPTER 5

Backup

To start a backup, run

```
python manage.py scbackup
```

To restore a backup and erase all your data, you can run

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

This will restore the latest backup. To choose another backup, indicate a backup filename as first argument. To get list of available backup, use

```
python manage.py listbackups
```

You can not restore a backup to a scirius which is older than the one where the backup has been done.

With default configuration file, the backup is done on disk in */var/backups* but other methods are available. As Scirius CE is using django-dbbackup application for backup and restore procedures, it benefits from all available methods in this application. This includes at least:

- FTP
- Amazon AWS
- Dropbox

Please see django-dbbackup configuration for more information on available methods and on their configuration.

Index