



USER'S GUIDE

Document version: 1.0

Document revision date: 15.02.2019

Table of Contents

1.	Introduction.....	5
1.1.	Document Purpose.....	5
1.2.	Target Audience.....	5
1.3.	Glossary	5
1.4.	References.....	5
2.	Overview.....	6
3.	Interface	8
3.1.	The DASHBOARD page.....	9
3.2.	The ATTACKS AND THREATS page	10
3.3.	The SENSORS page.....	12
3.4.	The THREAT POLICIES page	14
3.5.	The AUTOMATION page	14
3.6.	The SETTINGS page.....	15
3.6.1.	Users and roles	15
3.6.2.	Notifications	16
3.6.3.	Log	17
3.6.4.	Themes	18
3.6.5.	License	19
3.7.	Additional Menu.....	20
3.7.1.	About	21
3.7.2.	Documents.....	22
3.7.3.	Support	22
4.	Working with SNOWL.....	24
4.1.	User Authorization	24
4.2.	Working with Attacks and Threats	25
4.2.1.	Viewing Today's Attacks and Threats	25
4.2.2.	Viewing Historical Data of Attacks and Threats	26
4.2.3.	Sorting the List of Attacks and Threats.....	27
4.2.4.	Filtering the List of Attacks and Threats.....	27
4.2.4.1.	Applying Predefined Filter	27
4.2.4.2.	Deleting Predefined Filter.....	28
4.2.4.3.	Creating and Applying New Filter	29
4.2.4.4.	Saving New Filter as a Predefined One.....	30

4.2.4.5.	Using Additional Filtering Options.....	31
4.2.5.	Exporting the List of Attacks and Threats.....	32
4.2.6.	Viewing Detailed Information on Attacks and Threats	33
4.2.7.	Viewing Diagrams on Today's Attacks and Threats	34
4.2.7.1.	Diagrams on the Dashboard Page	34
4.2.7.2.	Diagrams on the Attacks and Threats Page	38
4.2.8.	Viewing Diagrams on Historical Data of Attacks and Threats	42
4.2.9.	Filtering Diagrams Data	44
4.3.	Working with Sensors.....	44
4.3.1.	Adding New Sensor.....	44
4.3.2.	Starting Sensor.....	45
4.3.3.	Stopping Sensor	46
4.3.4.	Restarting Sensor.....	46
4.3.5.	Changing Sensor Properties.....	46
4.3.6.	Deleting Sensor.....	47
4.3.7.	Configuring Sensor.....	48
4.3.8.	Viewing Sensor Activity Data	49
4.3.9.	Viewing Sensor Activity Diagrams	50
4.4.	Working with Threat Policies.....	51
4.4.1.	Adding New Threat Policy	51
4.4.2.	Copying Threat Policy	53
4.4.3.	Changing Threat Policy	54
4.5.	Working with Automatic Actions.....	55
4.5.1.	Adding New Automatic Action	55
4.5.2.	Changing Automatic Action	56
4.5.3.	Deleting Automatic Action	57
4.5.4.	Creating Filter	58
4.5.5.	Deleting Filter	58
4.6.	SNOWL Settings	58
4.6.1.	Adding New User	59
4.6.2.	Changing User's Personal Data	60
4.6.3.	Deleting User	61
4.6.4.	Configuring SNOWL for Sending Notifications	62
4.6.5.	Changing SNOWL Interface	64
4.6.6.	Getting New License	65

4.7.	Auxiliary Functions	66
4.7.1.	Viewing System Log	66
4.7.2.	Viewing System Documentation	67

1. Introduction

1.1. Document Purpose

The purpose of this document is to describe the capabilities provided to the user by **SNOWL**. This document covers the main business and technical scenarios and interface elements that allow working with threats and attacks, managing sensors, creating automatic rules, and so on.

1.2. Target Audience

The target audience of this document includes cyber security specialists involved in support of the protected resource.

1.3. Glossary

SNOWL	Hardware and software tools that provide protection of servers and network resources against different types of attacks.
Attack	Malicious use of a server or network resource.
Automatic action	Action that is automatically triggered upon detecting an attack.
Policy	Set of attacks and threats to be detected by a sensor.
Protected resource	A server/network resource which incoming traffic is protected by SNOWL .
Sensor	Attack and threat detector.
Threat	Suspected malicious use of a server or network resource.

1.4. References

Technical support	support@snowl.io
Q&A	snowl.io/dwqa-questions
Sales department	sales@snowl.io

2. Overview

SNOWL is designed to detect various types of malicious activity that can break security of a computer system and lead to theft of private information or financial resources and blocking the production processes. **SNOWL** can detect both network attacks against vulnerable services and malicious software activity (computer viruses, Trojan programs, worms, and so on).

SNOWL saves the detected events causing a threat and information on them for further analysis and provides instructions on corrective actions for a cyber security specialist. The archive of events is available only for users registered in the system.

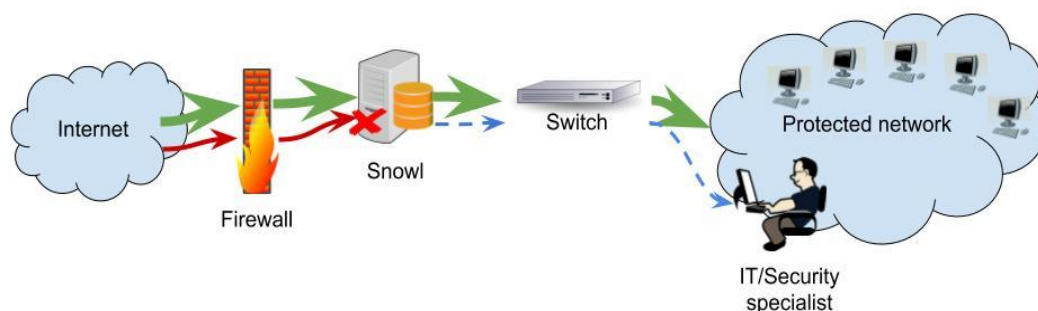
SNOWL provides advanced tools for visual analysis of the detected threats: various types of diagrams (including real-time diagrams) and a flexible event filtering system. It also provides tools for creating automatic actions that are triggered upon detecting an attack. This feature allows users to automate routine reactions, such as adding a blocking rule to a firewall.

Using **SNOWL**, a cyber security specialist can:

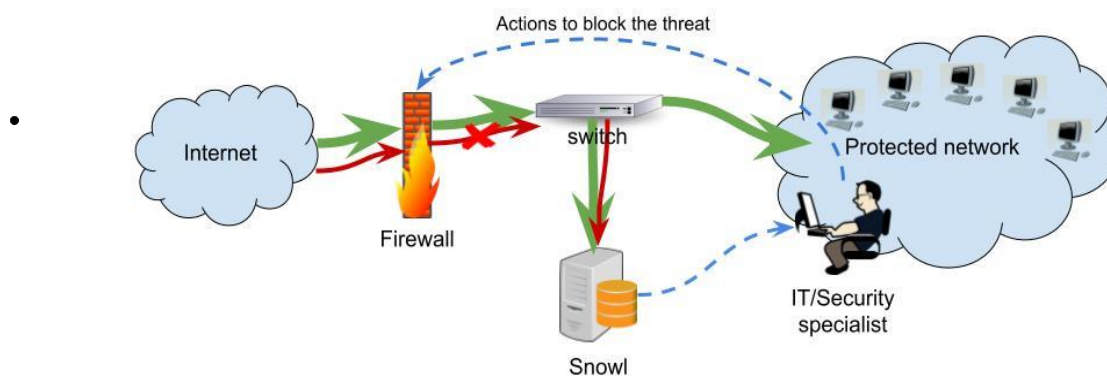
- Ensure security of servers/network resources that contain protected information.
- Monitor network threats.
- Identify the weakest and the riskiest systems.
- Quickly obtain information on the attack and instructions on further actions.
- In **SNOWL**, the attacks are detected using the **Snort** and **Suricata** sensors. **SNOWL** manages these sensors and processes all events coming from them.

Sensors can work in passive or active mode:

- In active mode, **SNOWL** can filter traffic:



In passive mode, **SNOWL** can apply the automatic actions:



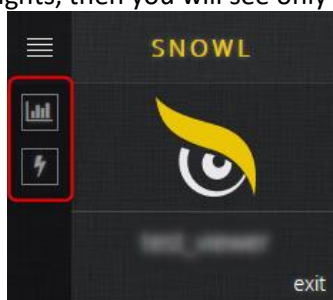
SNOWL also provides a cyber security specialist with the opportunity to specify types of events that should be detected by sensors. This functionality is called *threat policies*.

3. Interface

SNOWL contains many pages that have the following common features:



- | | |
|---|---|
| 1 | A button for hiding/showing the panel. |
| 2 | Buttons of the main menu.
If you don't have administrator rights, then you will see only two buttons in this menu: |



- | | |
|---|--|
| 3 | A link to the DASHBOARD page. |
| 4 | A link to the additional menu (About, Documents, Support). |
| 5 | Items of the additional menu. |
| 6 | A name of your user account. |
| 7 | A button for logging out. |
| 8 | System state widgets.
Clicking the Memory using / Disk using lines opens SENSOR MANAGEMENT PANEL . |

3.1. The DASHBOARD page

The **DASHBOARD** page is the main monitor of a cyber security specialist. The page is intended to estimate a state of the protected resource by viewing the most important diagrams. On this page, all diagrams are updated in real-time. You can see examples in the following sections:

[4.2.1, Viewing Today's Attacks and Threats](#)

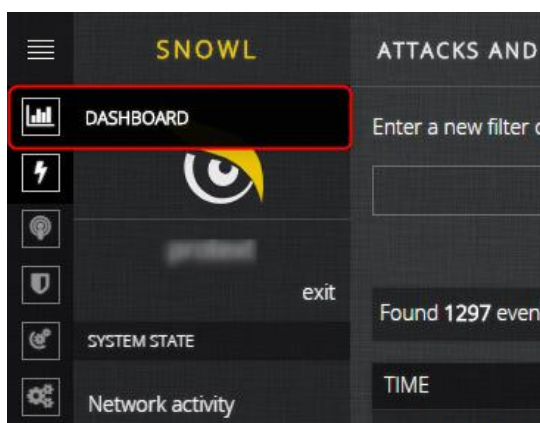
[4.2.6, Viewing Detailed Information on Attacks and Threats](#)

[4.2.4.5, Using Additional Filtering Options](#)

[4.2.7.1, Diagrams on the Dashboard Page](#)

[4.2.8, Viewing Diagrams](#)

- This page opens by default upon logging in to the system. To switch to this page from any other page,
- click **DASHBOARD** in the main menu:



The **DASHBOARD** page opens:



On this page, you can see the following diagrams:

MAP OF EXTERNAL ATTACKS

LAST THREATS

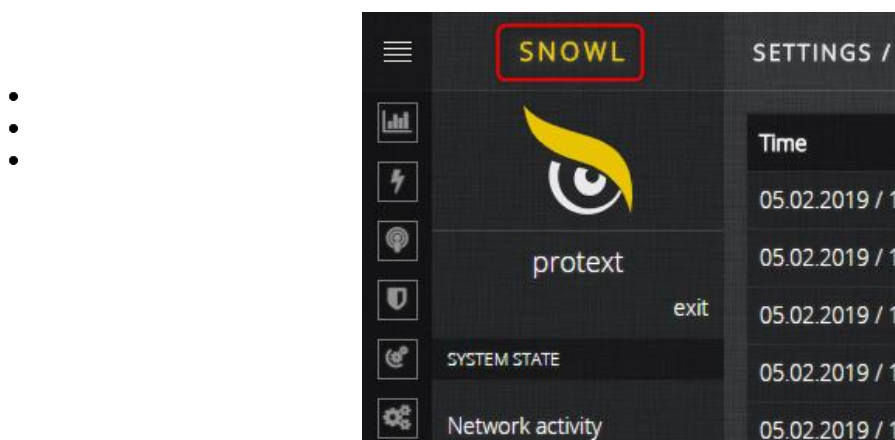
THREATS CLASSIFICATION

THREATS PRIORITY

THREATS IN TIMING

TOP ATTACKERS IP

You can also open the **DASHBOARD** page by clicking **SNOWL** in the left panel:



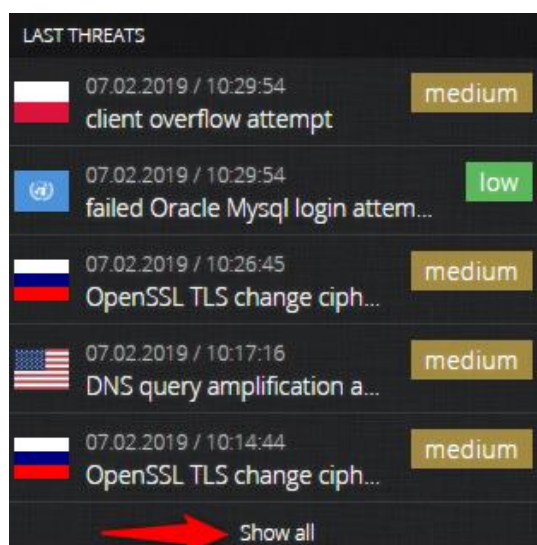
3.2. The ATTACKS AND THREATS page

The **ATTACKS AND THREATS** page is intended to view/sort/filter/export the list of attacks and threats and to view the diagrams on attacks and threats (see examples in section [4.2. Working with Attacks and Threats](#)).

To open the page, click **ATTACKS AND THREATS** in the main menu:



You can also open the **ATTACKS AND THREATS** page by clicking the **Show all** button in the **LAST THREATS** block of the **DASHBOARD** page:



The **ATTACKS AND THREATS** page opens:

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
28.01.2019 / 11:47:10	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 5	64.64.22.63	59684	192.168.1.10	22
28.01.2019 / 11:46:43	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 2	216.52.3.148	36893	192.168.1.10	22
28.01.2019 / 11:40:58	medium	PROTOCOL-VOIP	Sipicious User-Agent detected 3	185.53.91.44	5149	192.168.1.10	5060
28.01.2019 / 11:37:27	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 6	116.196.82.146	43334	192.168.1.10	22
28.01.2019 / 11:30:38	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 6	88.214.26.8	41402	192.168.1.10	22

By default, the page displays all today's attacks and threats. On this page, the following information is provided for each event:

TIME	Event registration time. By default, the list is sorted by this parameter (latest event on top).
PRIORITY	Event priority, which shows the event importance level: low/medium/high .
GROUP	Event group name.
THREAT	Event name, which is also a link to the event detailed information.
IP SRC	Source (attacker's) IP address.
PORT	Source (attacker's) port number.
IP DST	Destination IP address.
PORT	Destination port number.

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
28.01.2019 / 11:47:10	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 5	64.64.22.63	59684	192.168.1.10	22
28.01.2019 / 11:46:43	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 2	216.52.3.148	36893	192.168.1.10	22
28.01.2019 / 11:40:58	medium	PROTOCOL-VOIP	Sipivicious User-Agent detected 3	185.53.91.44	5149	192.168.1.10	5060
28.01.2019 / 11:37:27	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 6	116.196.82.146	43334	192.168.1.10	22
28.01.2019 / 11:30:38	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 6	88.214.26.8	41402	192.168.1.10	22

If similar attacks/threats occur several times within one day, then **SNOWL** will group them into one record. In this case, in the **THREAT** column of this record, you can see the number of events being grouped:

28.01.2019 / 12:36:10	medium	PROTOCOL-VOIP	Sipivicious User-Agent detected 2	185.53.91.44	5103	192.168.1.10	5060
-----------------------	--------	---------------	-----------------------------------	--------------	------	--------------	------

If you open the detailed information on the group of events, then, on the **Threat Timing** tab, you can see registration time of each event (for more information, see section [4.2.6, Viewing Detailed Information on Attacks and Threats](#)):

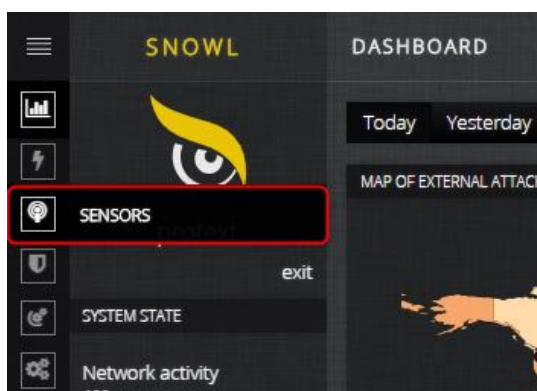
28.01.2019 / 12:36:10	medium	PROTOCOL-VOIP	Sipivicious User-Agent detected 2	185.53.91.44	5103	192.168.1.10	5060
<div>Threat Details Threat Timing</div> <div> 28.01.2019 / 12:36:10 28.01.2019 / 11:40:58 </div>							

3.3. The SENSORS page

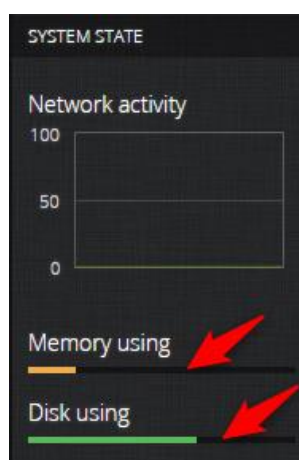
On the **SENSORS** page, all operations require administrator rights. If you don't have these rights, then you will not have the **SENSORS** item in the main menu.

The **SENSORS** page is intended to add new sensors to the protected resource and to maintain the previously added sensors (see examples in section [4.3, Working with Sensors](#)).

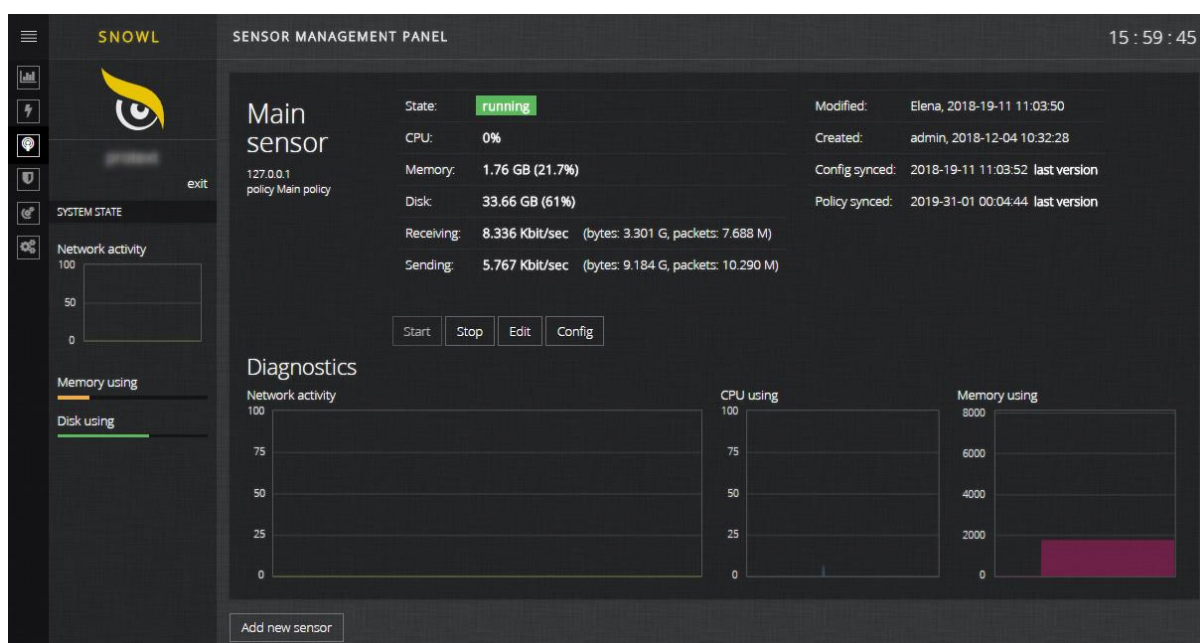
To open the page, click **SENSORS** in the main menu:



You can also open the **SENSORS** page by clicking the **Memory using/Disk using** lines in the **SYSTEM STATE** block of the left panel:



SENSOR MANAGEMENT PANEL opens:



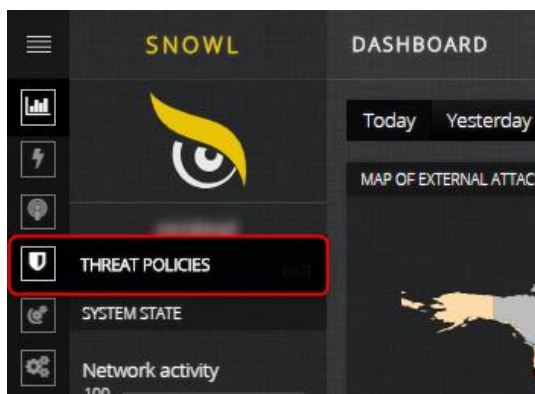
On this page, you can see widgets corresponding to sensors that are added to the protected resource.

3.4. The THREAT POLICIES page

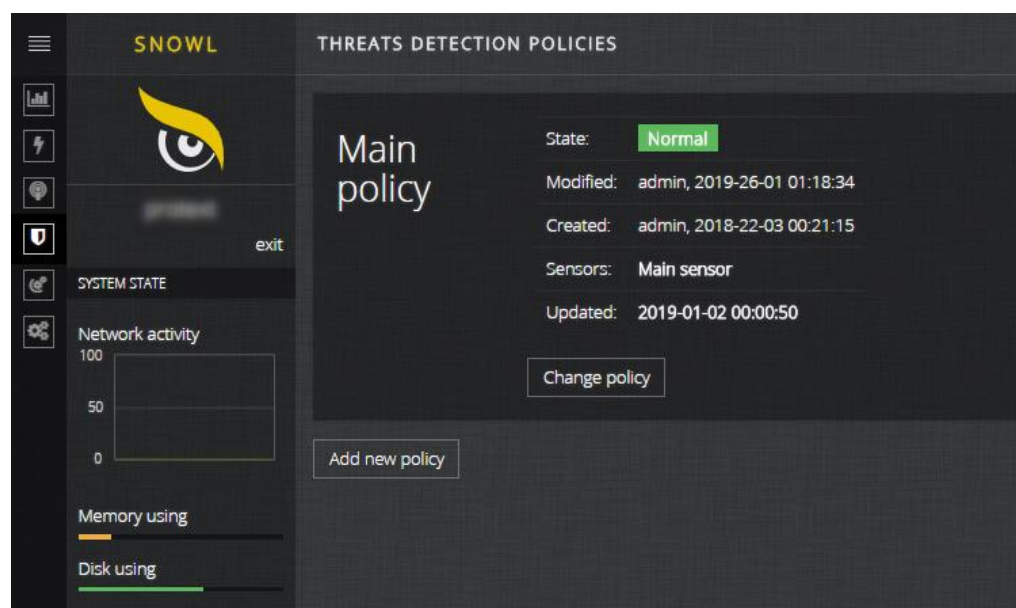
On the **THREAT POLICIES** page, all operations require administrator rights. If you don't have these rights, then you will not have the **THREAT POLICIES** item in the main menu.

The **THREAT POLICIES** page is intended to add new threat policies that can be further applied to sensors and to maintain the previously added policies (see examples in section [4.4, Working with Threat Policies](#)).

To open the page, click **THREAT POLICIES** in the main menu:



The **THREATS DETECTION POLICIES** page opens:



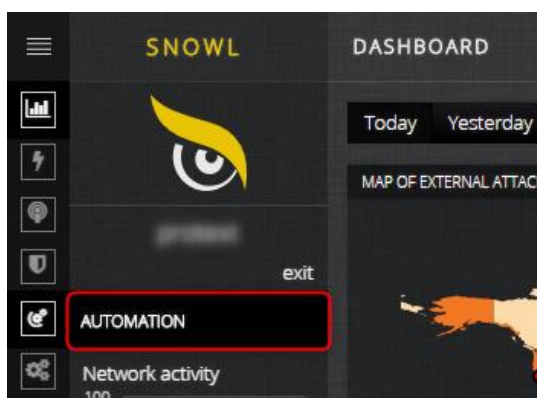
On this page, you can see widgets corresponding to threat policies that are added to **SNOWL**.

3.5. The AUTOMATION page

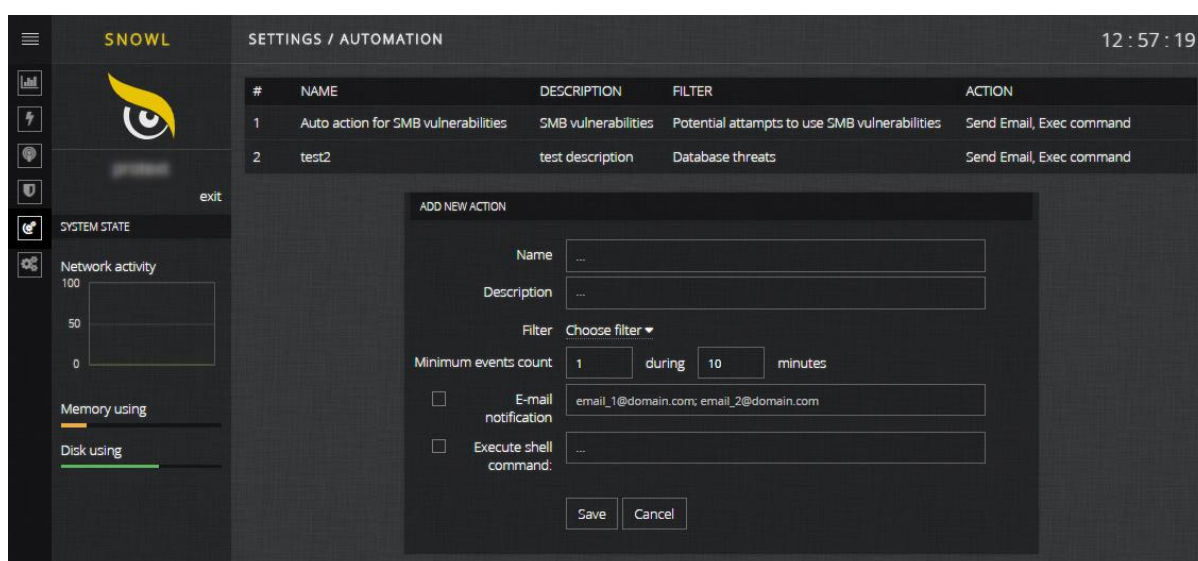
On the **AUTOMATION** page, all operations require administrator rights. If you don't have these rights, then you will not have the **AUTOMATION** item in the main menu.

The **AUTOMATION** page is intended to add new automatic actions and to maintain the previously added actions (see examples in section [4.5, Working with Automatic Actions](#)).

To open the page, click **AUTOMATION** in the main menu:



The **SETTINGS / AUTOMATION** page opens:



On this page, you can see the list of automatic actions and a window for adding a new automatic action.

3.6. The SETTINGS page

On the **SETTINGS** page, all operations require administrator rights. If you don't have these rights, then you will not have the **SETTINGS** item in the main menu.

3.6.1. Users and roles

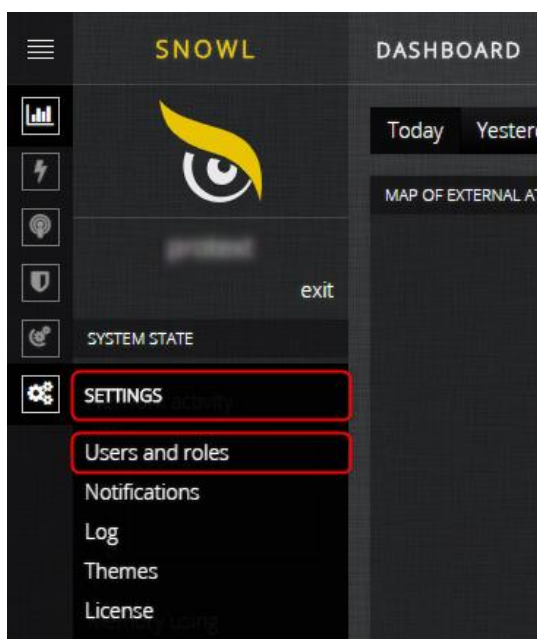
- The **Users and roles** page is intended to add new user accounts and to maintain the previously added accounts. You can see examples in the following sections:

[4.6.1, Adding New User](#)

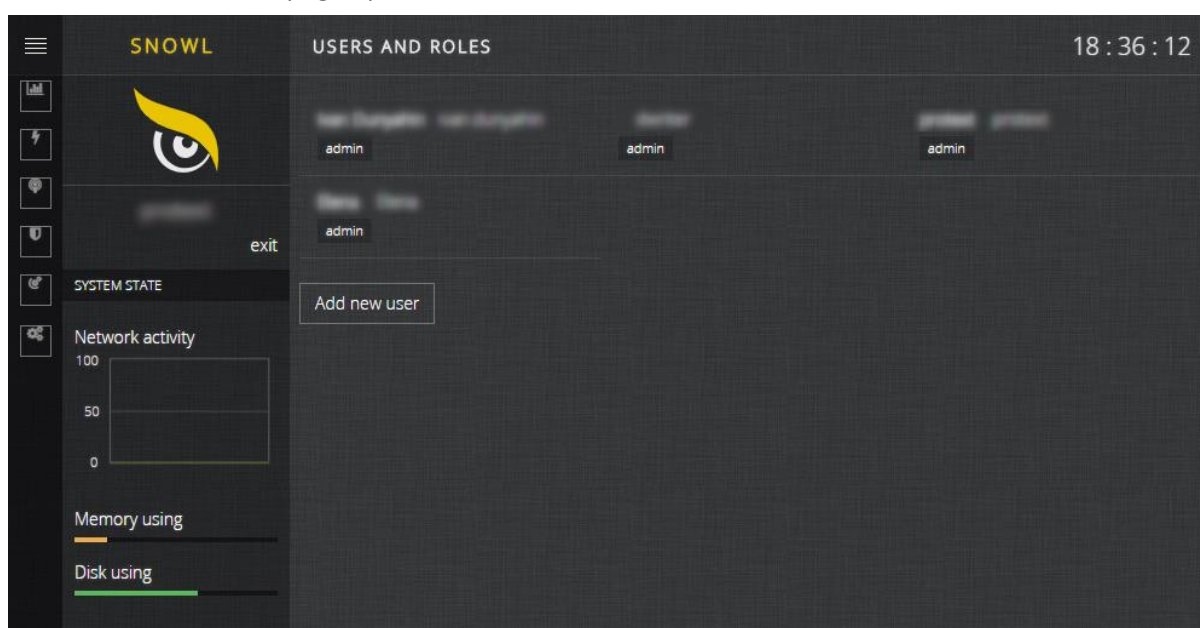
[4.6.2, Changing User's Personal Data](#)

[4.6.3, Deleting User](#)

To open the page, click **SETTINGS** in the main menu and **Users and roles** in the secondary menu:



The **USERS AND ROLES** page opens:

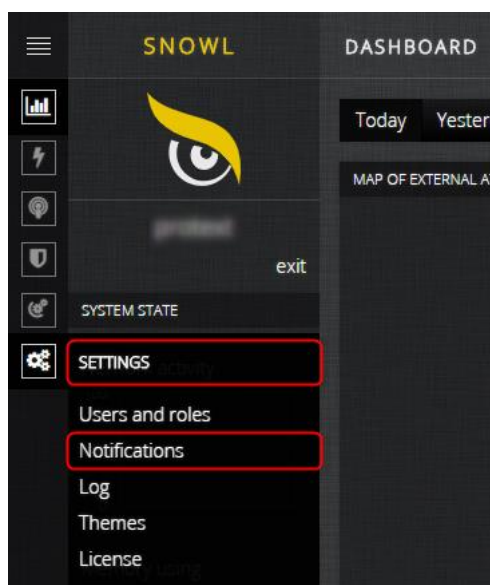


On this page, you can see the table containing accounts of all employees registered in **SNOWL**.

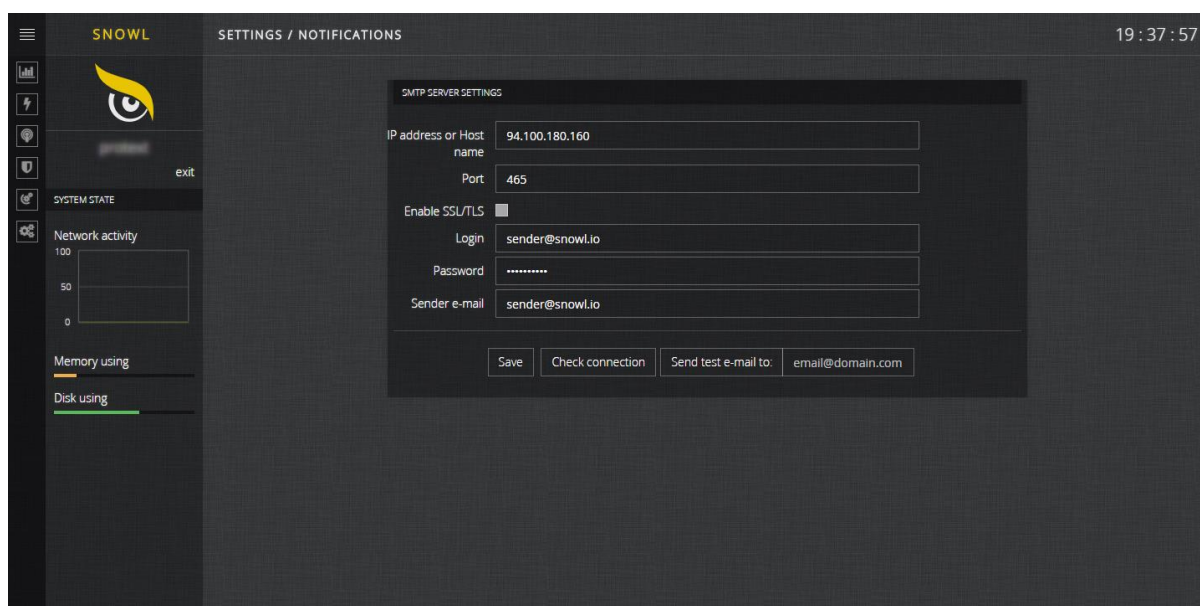
3.6.2. Notifications

The **Notifications** page is intended for configuring SMTP server and **SNOWL** for sending notifications to users (see examples in section [4.6.4, Configuring SNOWL for Sending Notifications](#)).

To open the page, click **SETTINGS** in the main menu and **Notifications** in the secondary menu:



The **SETTINGS / NOTIFICATIONS** page opens:

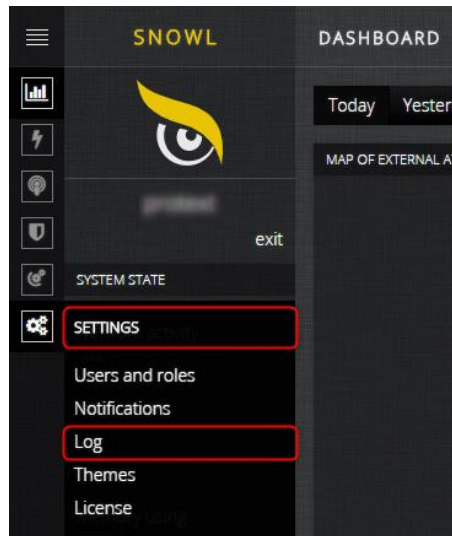


On this page, you can see a window for configuring SMTP server and **SNOWL** and checking connection after the configuration is done.

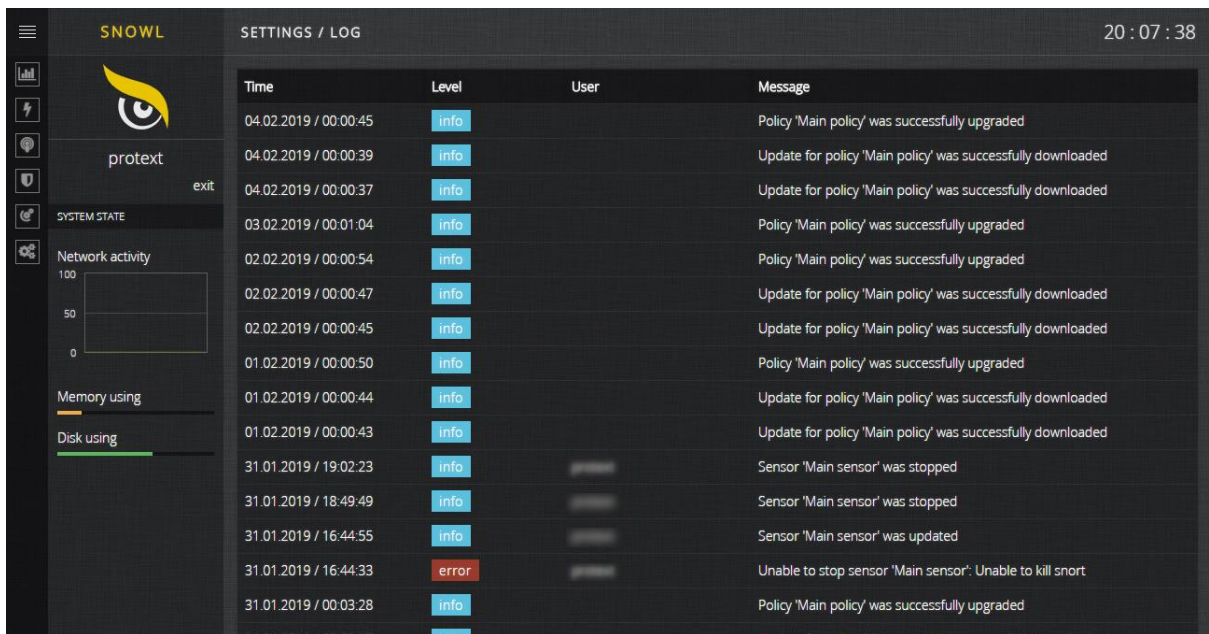
3.6.3. Log

The **Log** page is intended to view system messages (for more information, see section [4.7.1, Viewing System Log](#)).

To open the page, click **SETTINGS** in the main menu and **Log** in the secondary menu:



The **SETTINGS / LOG** page opens:



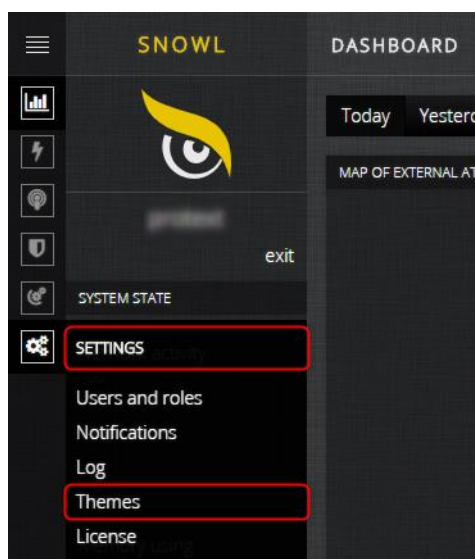
On this page, the following information is provided for each event:

Time	Time of an event that took place in SNOWL .
Level	Importance level of the event: info/warning/error .
User	Account of a user who caused the event.
Message	Description of the event.

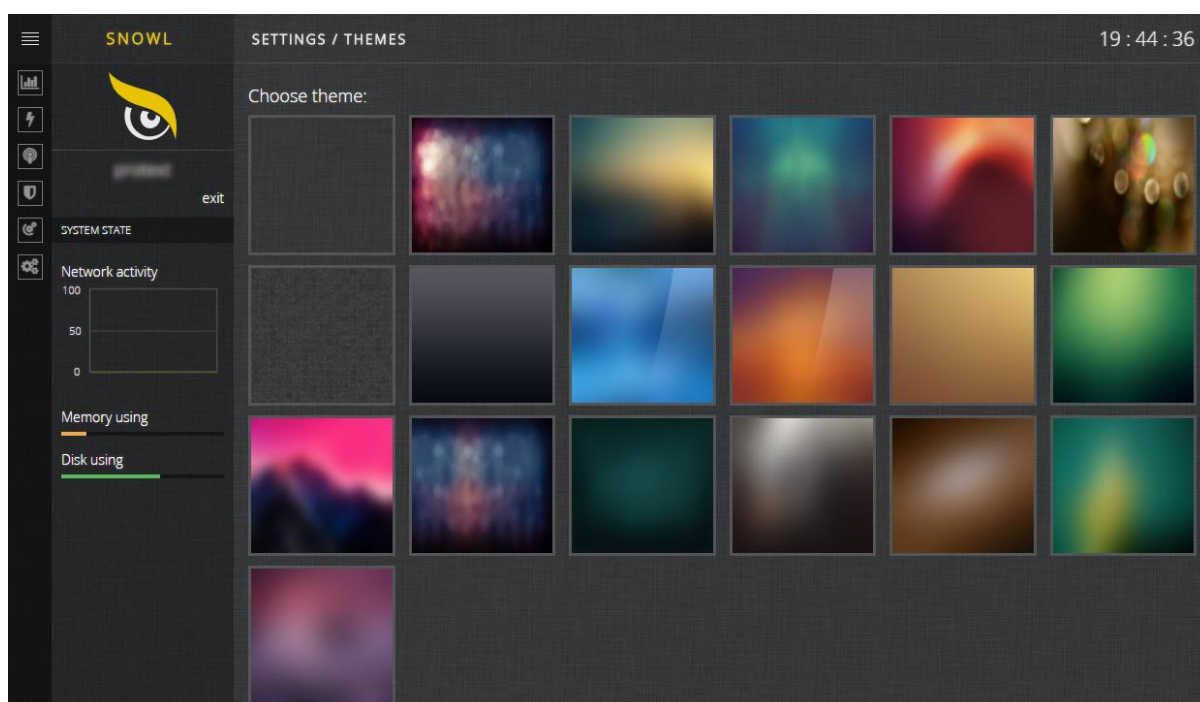
3.6.4. Themes

The **Themes** page is intended to change background themes of **SNOWL** (for more information, see section [4.6.5, Changing SNOWL Interface](#)).

To open the page, click **SETTINGS** in the main menu and **Themes** in the secondary menu:



The **SETTINGS / THEMES** page opens:

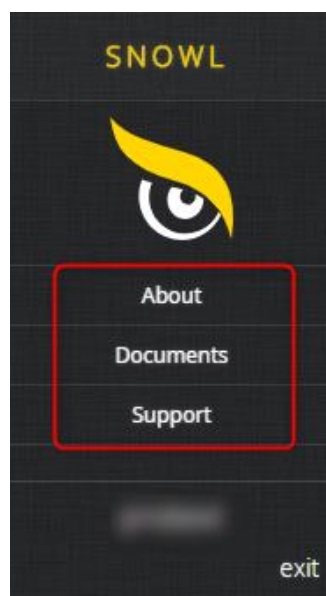


On this page, you can see a set of background themes that can be applied to **SNOWL**.

3.6.5. License

The **License** page is intended to view information on the current license, open a website for purchasing a new license, and upload the purchased license to **SNOWL** (for more information, see section [4.6.6, Getting New License](#)).

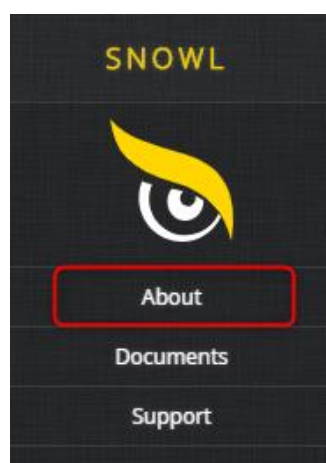
The additional menu opens:



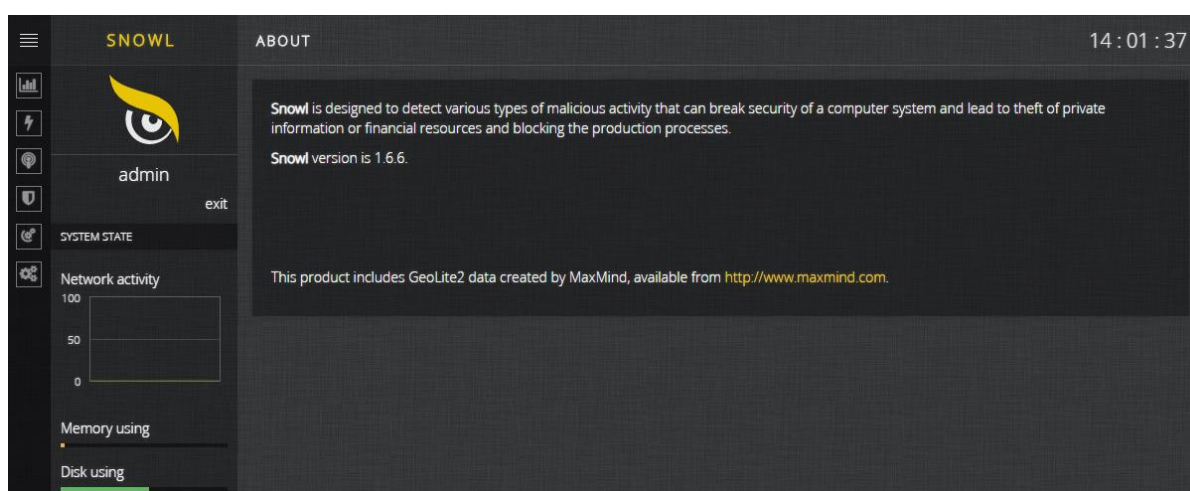
3.7.1. About

This page is intended to view information on **SNOWL** purpose and functions.

To open the page, click **About** in the additional menu:



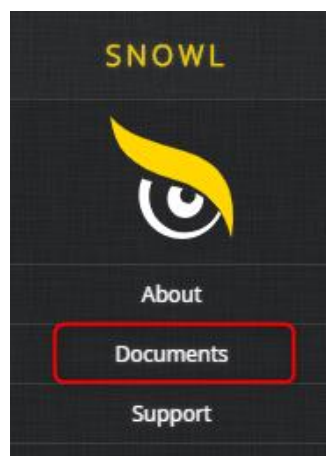
The **ABOUT** page opens:



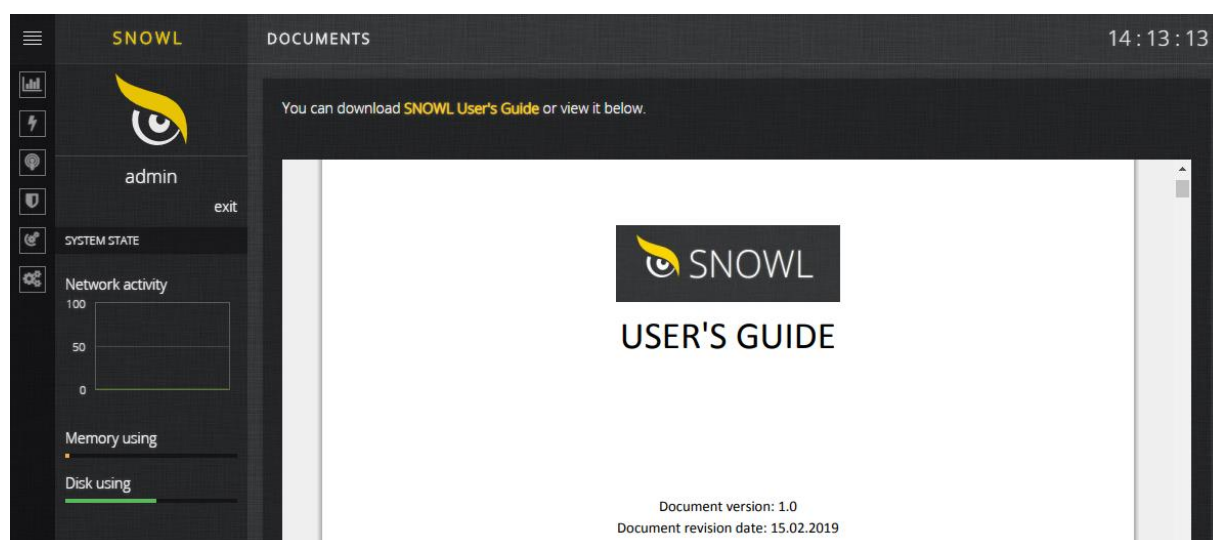
3.7.2. Documents

This page is intended to read or download guides on using and administrating **SNOWL**.

To open the page, click **Documents** in the additional menu:



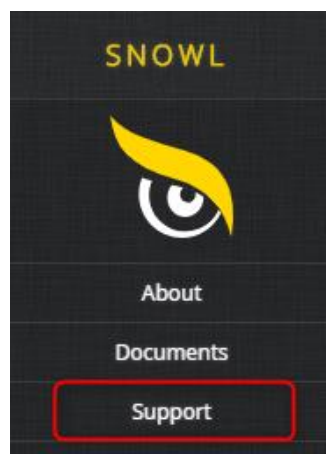
The **DOCUMENTS** page opens:



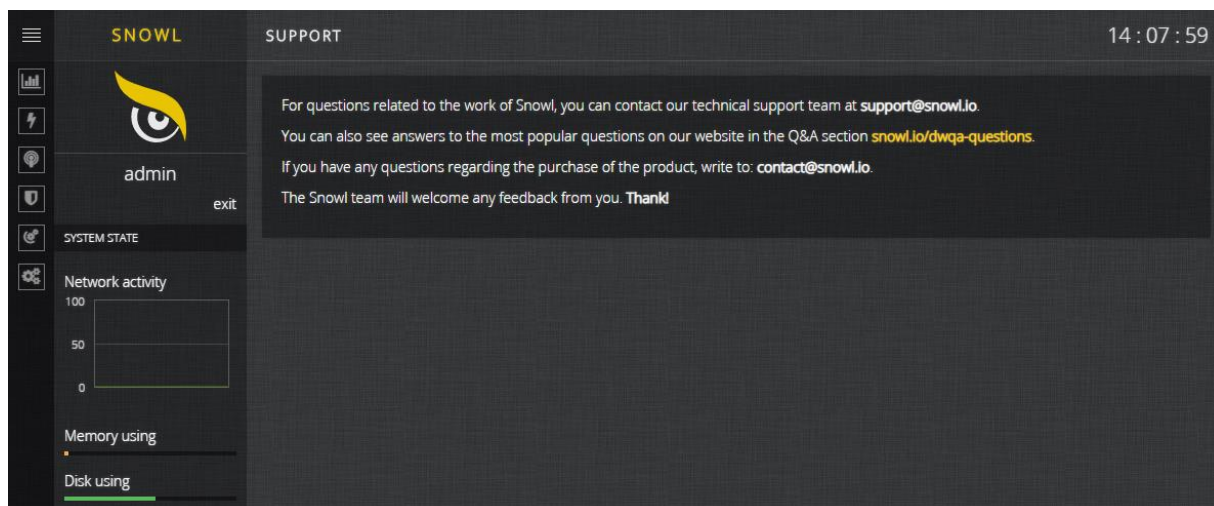
3.7.3. Support

This page is intended to view contacts of the **SNOWL** support team.

To open the page, click **Support** in the additional menu:



The **SUPPORT** page opens:



4. Working with SNOWL

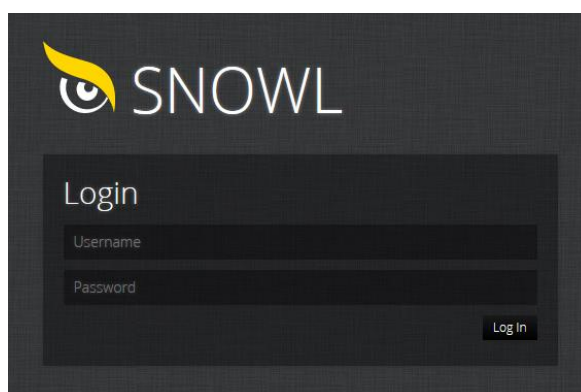
4.1. User Authorization

To start using **SNOWL**, log in. To do that, follow these steps:

Open the **SNOWL** web application in your browser (<https://<IP address>>, where **<IP address>** corresponds to the IP address of a server where **SNOWL** is installed).

Specify your credentials on the login page:

- 1.
- 2.

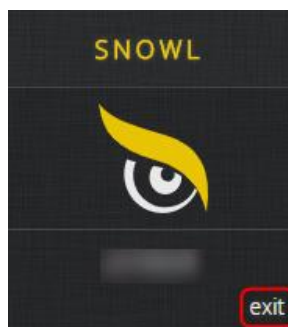


By default, your user name and password are equal to **admin** and **123456** respectively. We recommend that you change the credentials after the first logging in to the system. To do that, follow instructions in section [4.6.2, Changing User's Personal Data](#).

3. Click **Log in**. If both the user name and password are entered correctly, the **DASHBOARD** page opens. Welcome to **SNOWL**!



To log out, click **exit** under the owl's eye:



4.2. Working with Attacks and Threats

4.2.1. Viewing Today's Attacks and Threats

To view today's attacks and threats, click **ATTACKS AND THREATS** in the main menu:

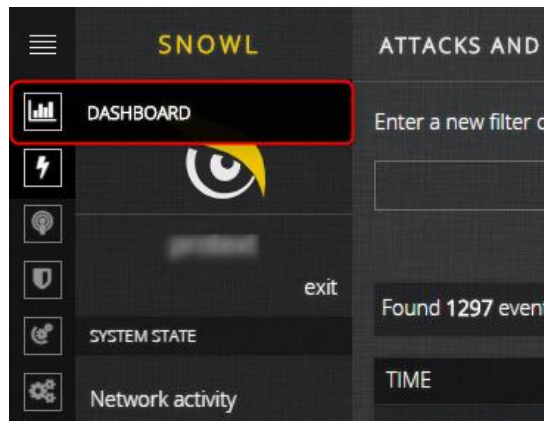


The **ATTACKS AND THREATS** page opens:

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
28.01.2019 / 11:47:10	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 5	64.64.22.63	59684	192.168.1.10	22
28.01.2019 / 11:46:43	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 2	216.52.3.148	36893	192.168.1.10	22
28.01.2019 / 11:40:58	medium	PROTOCOL-VOIP	Sipivicious User-Agent detected 3	185.53.91.44	5149	192.168.1.10	5060
28.01.2019 / 11:37:27	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 6	116.196.82.146	43334	192.168.1.10	22
28.01.2019 / 11:30:38	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler	88.214.26.8	41402	192.168.1.10	22

By default, the page displays all today's attacks and threats.

You can also view today's attacks and threats on the **DASHBOARD** page. The page opens by default upon logging in to the system. To switch to this page from any other page, click **DASHBOARD** in the main menu:



On the right part of the **DASHBOARD** page, in the **LAST THREATS** block, you can see a real-time list of the last five attacks and threats for today:



Clicking the **Show all** button leads you to the full list of today's attacks and threats on the **ATTACKS AND THREATS** page.

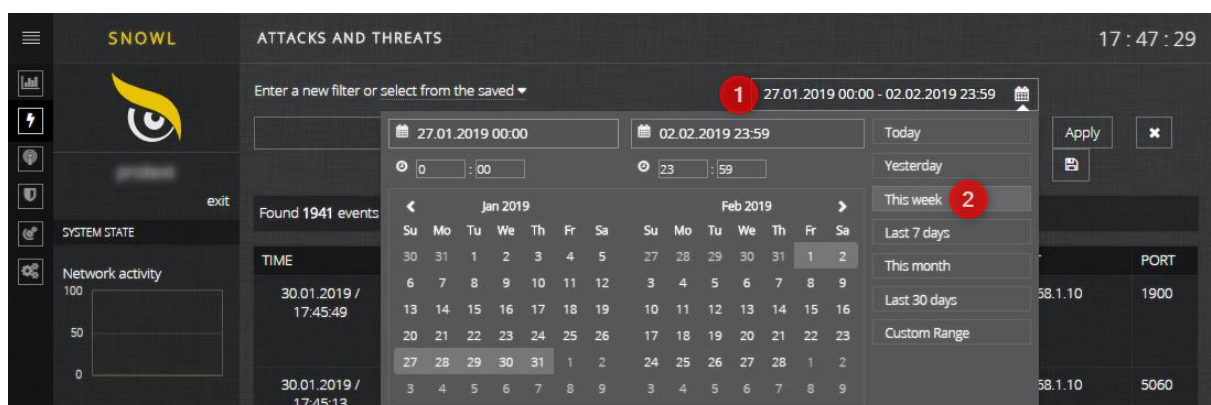
1. 4.2.2. Viewing Historical Data of Attacks and Threats

- To view historical data of attacks and threats, follow these steps:

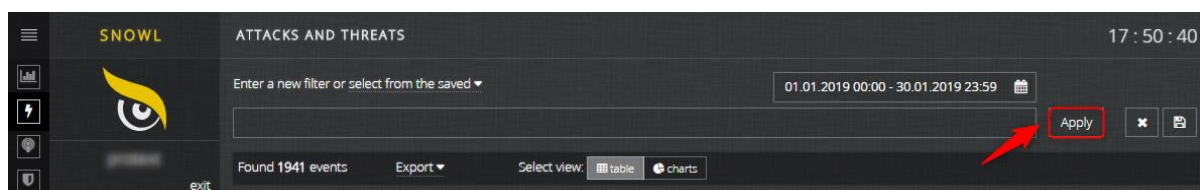
Click **ATTACKS AND THREATS** in the main menu. The page with today's attacks and threats opens.

In the top-right corner of the page, click the dates and select the observation period:

Yesterday, This week, Last 7 days, This month, Last 30 days or specify a custom range:



Click **Apply**:



3. The list of attacks and threats is updated according to the selected period.

4.2.3. Sorting the List of Attacks and Threats

By default, the list of attacks and threats is sorted by event registration time in order of arrival (latest event on top). However, you can sort the list by any other column. To do that, click **ATTACKS AND THREATS** in the main menu to open the list, then click the required column name. As a result, the list of attacks and threats is sorted by values of this column.

4.2.4. Filtering the List of Attacks and Threats

In **SNOWL**, filter is a Boolean expression containing the following parts:

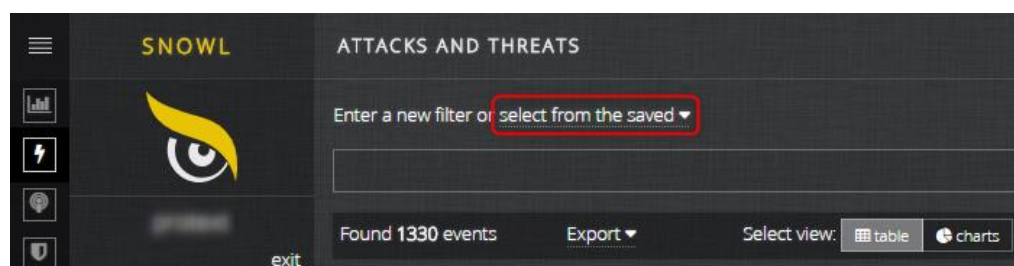
1. Event attribute name.
2. Sign of equality, inequality or comparison.
3. Event attribute value.
4. Example: **priority = low**.

One filter can contain several Boolean expressions combined by **AND/OR** operators, for example: **priority = low AND ip.dst = 192.168.1.10**.

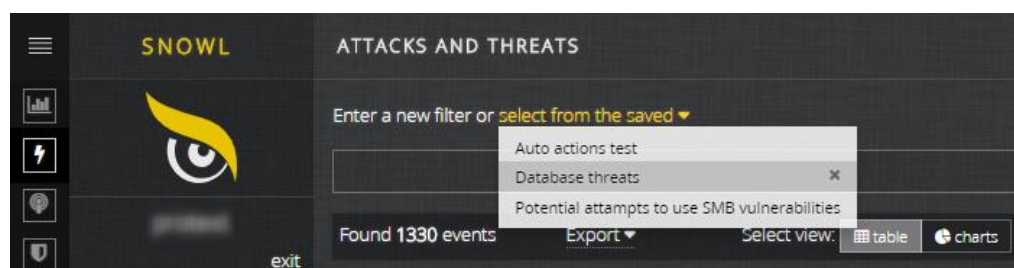
To filter the attacks and threats by the required conditions, you can either apply a predefined filter, create a new one or use additional filtering options.

4.2.4.1. Applying Predefined Filter

1. To apply one of the predefined filters, follow these steps:
2. Click **ATTACKS AND THREATS** in the main menu. The page with attacks and threats opens.
3. In the top-left corner of the page, click **select from the saved**:



In the drop-down list box, select the required filter:



The list of attacks and threats is filtered according to the selected conditions:

Database threats ▼ 30.01.2019 00:00 - 30.01.2019 23:59

group=ORACLE x or group=MYSQL x or group=SERVER-MSSQL x or group=SERVER-MYSQL x or group=SERVER-ORACLE x Apply X

Found 196 events Export Select view: table charts

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
30.01.2019 / 10:51:05	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	85.93.20.38	48071
30.01.2019 / 10:51:05	high	SERVER-MYSQL	mysql_log COM_CREATE_DB format string vulnerability exploit attempt	85.93.20.38	48071	192.168.1.10	3306
30.01.2019 / 10:51:05	medium	SERVER-MYSQL	client overflow attempt	85.93.20.38	48071	192.168.1.10	3306
30.01.2019 / 07:57:48	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	111.175.62.151	3798
30.01.2019 / 03:25:14	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	89.248.162.177	52294

To reset the filter, click X, then **Apply**:

Database threats ▼ 30.01.2019 00:00 - 30.01.2019 23:59

group=ORACLE x or group=MYSQL x or group=SERVER-MSSQL x or group=SERVER-MYSQL x or group=SERVER-ORACLE x Apply X

Found 846 events Export Select view: table charts

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
30.01.2019 / 20:59:56	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	85.93.20.38	29668
30.01.2019 / 20:59:56	medium	SERVER-MYSQL	client overflow attempt	85.93.20.38	29668	192.168.1.10	3306
30.01.2019 / 20:50:23	low	SERVER-MYSQL	failed Oracle	192.168.1.10	3306	58.218.213.79	3524

4.2.4.2. Deleting Predefined Filter

- To delete a predefined filter, follow these steps:
- Click **ATTACKS AND THREATS** in the main menu. The page with attacks and threats opens.

In the top-left corner of the page, click **select from the saved**:

Enter a new filter or select from the saved ▼

Found 1330 events Export Select view: table charts

In the drop-down list box, select the required filter and click X:

Enter a new filter or select from the saved ▼

Auto actions test

Database threats

Low priority

Potential attempts to use SMB vulnerabilities

Found 201 events

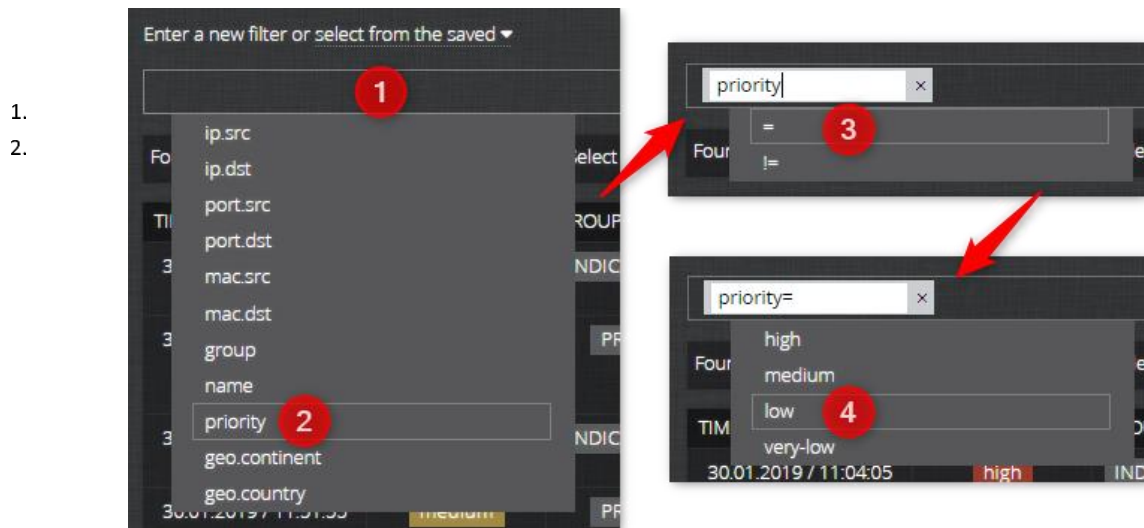
Click **Yes** to confirm the deletion.

4.2.4.3. Creating and Applying New Filter

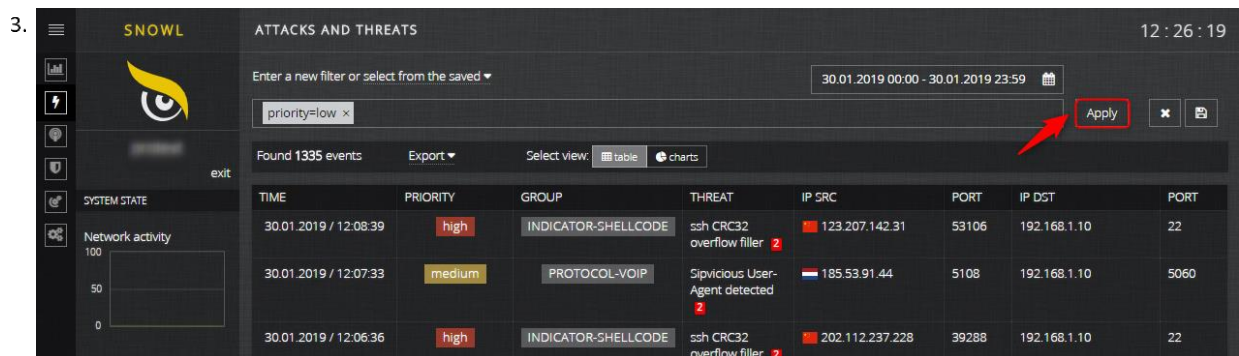
To create and apply a new filter, follow these steps:

Click **ATTACKS AND THREATS** in the main menu. The page with attacks and threats opens.

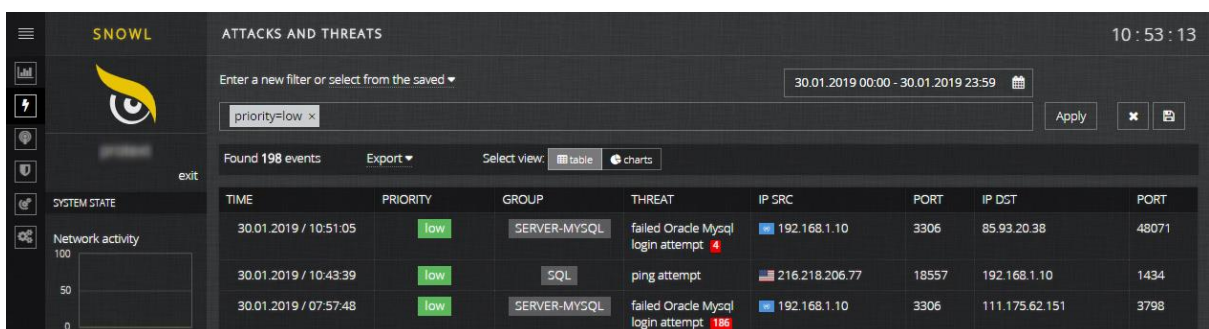
Click the field for entering a new filter (1) and successively select an attribute name (2), sign of equality/inequality/comparison (3), and attribute value (4) from the drop-down list boxes:



Click **Apply**:



The list of attacks and threats is filtered according to the selected conditions:



To reset the filter, click **X**, then **Apply**:

Found 198 events

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
30.01.2019 / 10:51:05	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	85.93.20.38	48071
30.01.2019 / 10:43:39	low	SQL	ping attempt	216.218.206.77	18557	192.168.1.10	1434
30.01.2019 / 07:57:48	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	111.175.62.151	3798

4.2.4.4. Saving New Filter as a Predefined One

To save a new filter as a predefined one, follow these steps:

Click **ATTACKS AND THREATS** in the main menu. The page with attacks and threats opens.

Create and apply a new filter (for more information, see section [4.2.4.3, Creating and Applying New Filter](#)).

- 1.
- 2.

Click the save icon:

Found 198 events

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
30.01.2019 / 10:51:05	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	85.93.20.38	48071
30.01.2019 / 10:43:39	low	SQL	ping attempt	216.218.206.77	18557	192.168.1.10	1434
30.01.2019 / 07:57:48	low	SERVER-MYSQL	failed Oracle Mysql login attempt	192.168.1.10	3306	111.175.62.151	3798

- 4.
- In the window that appears, specify a name for the created filter:

ENTER NAME OF THE FILTER:

Low priority

Save filter Cancel

As a result, the created filter is displayed in the list of predefined filters:

Found 1008 events

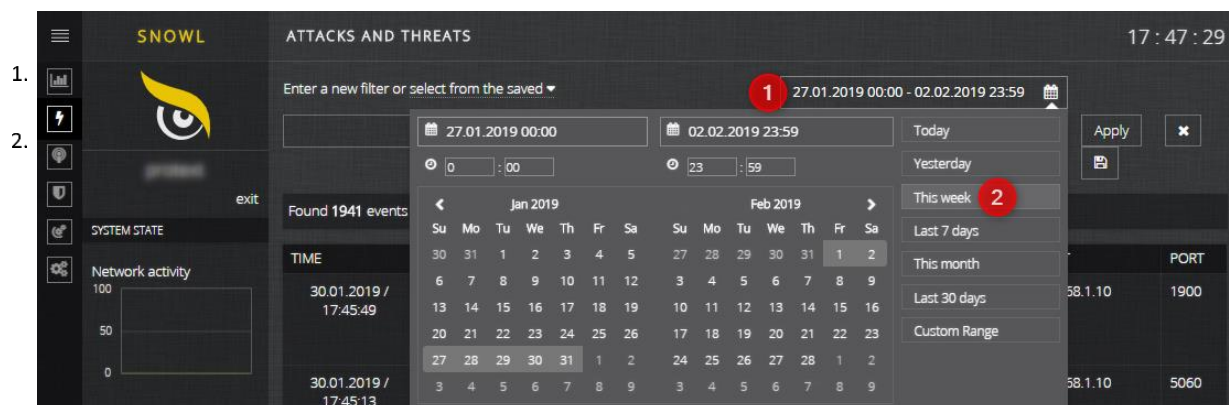
4.2.4.5. Using Additional Filtering Options

You can filter attacks and threats by period. To do that, follow these steps:

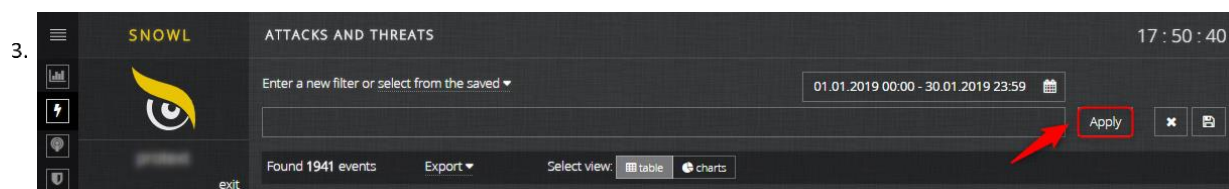
Click **ATTACKS AND THREATS** in the main menu. The page with today's attacks and threats opens.

In the top-right corner of the page, click the dates and select the observation period:

Yesterday, This week, Last 7 days, This month, Last 30 days or specify a custom range:



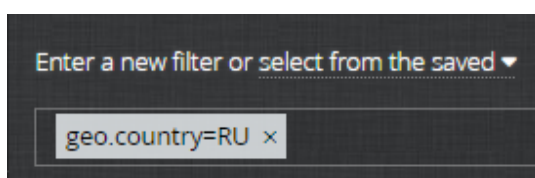
Click **Apply**:



The list of attacks and threats is updated.

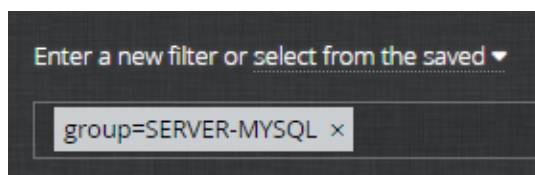
You can also filter attacks and threats using real-time diagrams on the **DASHBOARD** page:

- The **MAP OF EXTERNAL ATTACKS** diagram: clicking the country opens a list of attacks and threats filtered according to the selected country.



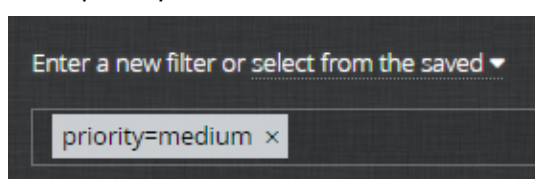
-

The **THREATS CLASSIFICATION** diagram: clicking the group name opens a list of attacks and threats filtered according to the selected group.



-

The **THREATS PRIORITY** diagram: clicking the bar opens a list of attacks and threats filtered according to the selected priority.



The **THREATS IN TIMING** diagram: clicking the point on the graph opens a list of attacks and threats filtered according to the selected time interval.

31.01.2019 06:30 - 31.01.2019 06:40

The **TOP ATTACKER'S IP** list: clicking the IP address opens a list of attacks and threats filtered according to the selected IP.

Enter a new filter or select from the saved ▼

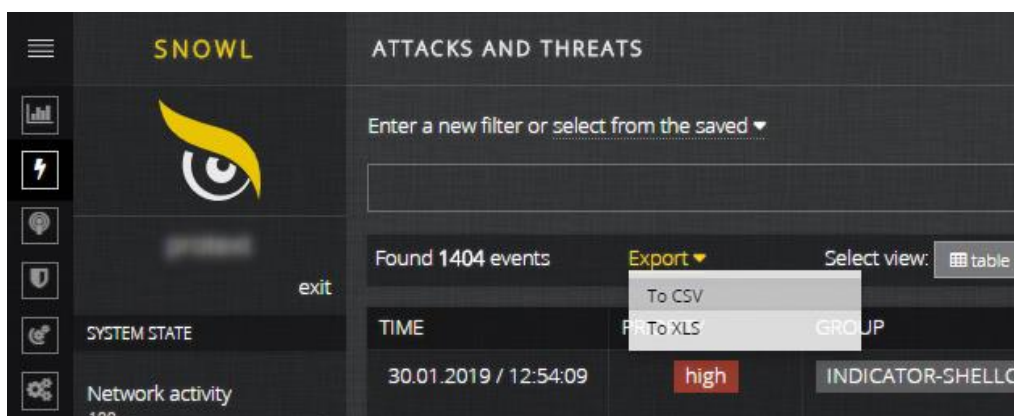
ip.src=88.214.26.8 x

4.2.5. Exporting the List of Attacks and Threats

To export the list of attacks and threats, follow these steps:

Click **ATTACKS AND THREATS** in the main menu. The page with all today's attacks and threats opens.

- Sort the events, apply filters or specify the required period to generate the list you want to export.
- Click **Export** and select either **CSV** or **XLS** file format:



The **Snowl-Export.xlsx** / **Snowl-Export.csv** file is saved on your computer. You can find this file in a folder that is configured for saving downloaded files in your browser.

Автосохранение		Snowl-Export.xlsx - защищенный просмотр - Excel																				Облачные ресурсы																									
Файл		Главная		Вставка		Разметка страницы		Формулы		Данные		Рецензирование		Вид		Справка		Команда		Что вы хотите сделать?		Облачные ресурсы																									
A1																																															
A		B		C		D		E		F		G		H		I		J		K		L		M		N		O		P		Q		R		S		T		U		V		W		X	
Id		Sensor Id		Timestamp		MAC src		IP src		Port src		MAC dst		IP dst		Port dst		Protocols		Generator		Signature		Signature		Class		Message		Priority		Geo: Cont		Geo: Cour		Geo: Sub1		Geo: Sub2		Geo: City		Geo: Latit		Geo: Longitude			
1		1273055		2		154879571		F07D6895:185.53.91.5143		00012E4D		192.168.1.5060		Ethernet/1		28993		2		PROTOCO		Sipvicious		medium		EU		NL										52382400		4899500							
2		1273056		2		154879585		F07D6895:139.162.5C.53290		00012E4D		192.168.1.161		Ethernet/1		1411		19		PROTOCO		public acc		medium		AS		SG										1366700		103800000							
3		1273057		2		154879585		F07D6895:139.162.5C.53290		00012E4D		192.168.1.161		Ethernet/1		1417		17		PROTOCO		request ui		medium		AS		SG										1366700		103800000							
4		1273058		2		15487960C		F07D6895:104.122.24.443		00012E4D		192.168.1.59730		Ethernet/1		43496		1		SERVER-V		Lets Encry		medium		EU		NL		NH				Amsterda		52350000		4916700									
5		1273059		2		15487960C		F07D6895:104.122.24.443		00012E4D		192.168.1.59732		Ethernet/1		43496		1		SERVER-V		Lets Encry		medium		EU		NL		NH				Amsterda		52350000		4916700									
6		1273060		2		15487969C		F07D6895:45.55.156.54122		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		NA		US		NJ				Clifton		40832600		-73869300									
7		1273061		2		154879691		F07D6895:46.18.3.47.58851		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		EU		UA		23				Zaporizhi		47850000		35283300									
8		1273062		2		154879691		F07D6895:51.68.198.35402		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		EU		FR								48858200		2338700									
9		1273063		2		154879695		F07D6895:88.214.26.38414		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		—										0		0									
10		1273064		2		154879711		F07D6895:45.55.156.54552		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		NA		US		NJ				Clifton		40832600		-73869300									
11		1273065		2		154879713		F07D6895:51.68.198.35770		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		EU		FR								48858200		2338700									
12		1273066		2		154879716		F07D6895:194.56.72.39788		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		AS		KG								0		0									
13		1273067		2		15487972C		F07D6895:31.186.53.32926		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		AS		CN								41000000		75000000									
14		1273068		2		154879721		F07D6895:106.12.36.48566		00012E4D		192.168.1.22		Ethernet/1		1325		14		INDICATO		ssh CRC32		high		AS		CN		BJ		Beijing		39928900		116388300											

Please note that the exported list of attacks and threats contains more data than you can see on the **ATTACKS AND THREATS** page. The following information is provided for each event:

Id	Event identifier.
Sensor id	Sensor identifier.
Timestamp	Date and time of event registration in the Unix-timestamp format.
MAC src	Source (attacker's) MAC address.

IP src	Source (attacker's) IP address.
Port src	Source (attacker's) port number.
MAC dst	Destination MAC address.
IP dst	Destination IP address.
Port dst	Destination port number.
Protocols	Network protocols.
Generator Id	Event generator identifier.
Signature Id	Signature identifier.
Signature Revision	Signature version.
Group	Event group name.
Threat	Event name.
Priority	Event priority, which shows the event importance level: low/medium/high .
Geo: Continent	Name of the attacker's continent.
Geo: Country	Name of the attacker's country.
Geo: Sub1	Name of the attacker's region.
Geo: Sub2	Name of the attacker's region (clarified).
Geo: Latitude	Attacker's latitude.
Geo: Longitude	Attacker's longitude.

4.2.6. Viewing Detailed Information on Attacks and Threats

To view detailed information on the attack/threat, follow these steps:

Click **ATTACKS AND THREATS** in the main menu. The page with attacks and threats opens.

1. For the attack/threat of your interest, click the value of the **THREAT** column. The **Threat Details** and **Threat Timing** tabs with detailed information appear:
- 2.

For each event, detailed information contains event description and instructions for a cyber security specialist.

- If you open detailed information on the group of events, then you can see registration time of each event on the **Threat Timing** tab.

To close the tabs, click the value of the **THREAT** column once again.

You can also view detailed information on an attack/threat using real-time diagrams on the **DASHBOARD** tab:

On the **MAP OF EXTERNAL ATTACKS** diagram, clicking the line displays a pop-up window with details of an attack/threat.

In the **LAST THREATS** block, clicking the attack/threat name also displays a pop-up window with details of an attack/threat.

For more information on these diagrams, see section [4.2.7.1, Diagrams on the Dashboard Page](#).

4.2.7. Viewing Diagrams on Today's Attacks and Threats

To monitor the current state of a protected resource, view the diagrams on today's attacks and

- threats. You can find the diagrams on the DASHBOARD and ATTACK AND THREATS pages.

4.2.7.1. Diagrams on the Dashboard Page

On the **DASHBOARD** page, the following diagrams are displayed: [MAP OF EXTERNAL ATTACKS](#), [LAST THREATS](#), [THREATS CLASSIFICATION](#), [THREATS PRIORITY](#), [THREATS IN TIMING](#), [TOP ATTACKERS IP](#). All the diagrams are updated in real-time.

MAP OF EXTERNAL ATTACKS

This diagram shows geographical distribution of attacks/threats.

1. Hovering over the country displays country name and the number of events coming from it:

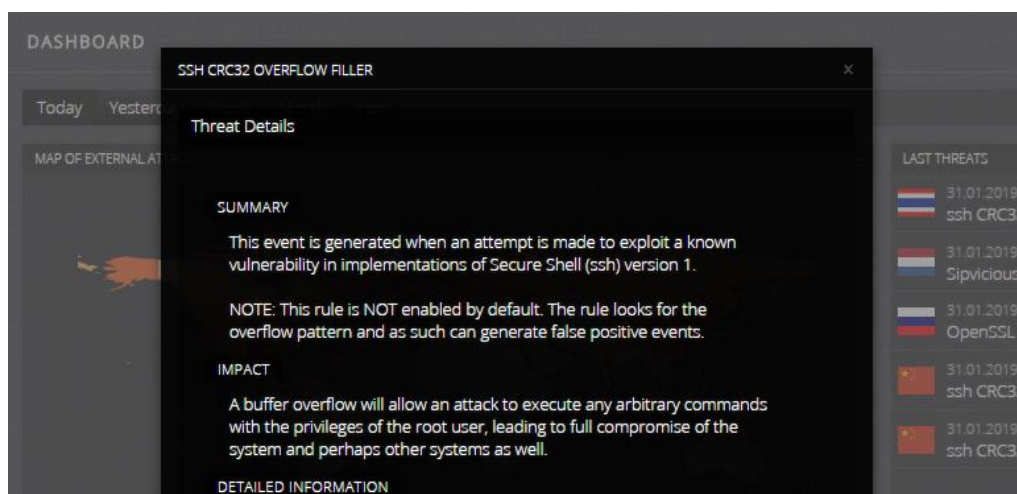


Colors of the countries differ according to the number of attacks coming from them: the more attacks, the more intense the red color is.

Clicking the country opens the list of attacks and threats filtered according to the selected country:

SNOWL		ATTACKS AND THREATS						11 : 20 : 56	
		Enter a new filter or select from the saved ▾						31.01.2019 00:00 - 31.01.2019 23:59	
		geo.country=RU x						Apply	
		Found 45 events						Select view: table charts	
		TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
		31.01.2019 / 11:15:49	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 3	85.192.171.23	59755	192.168.1.10	22
		31.01.2019 / 11:14:06	high	PUA-P2P	Bittorrent UTP peer	194.85.224.72	37999	192.168.1.10	1

Clicking the line displays a pop-up window with details of the appropriate attack/threat:

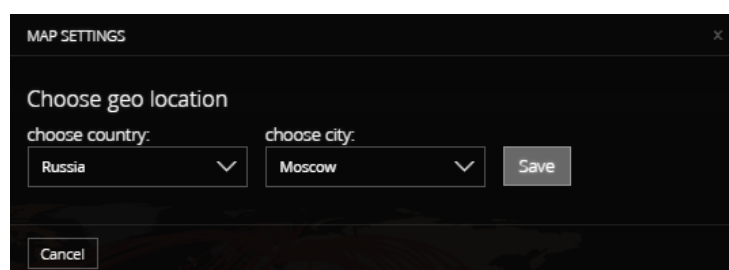


Color of line corresponds to the priority of the appropriate attack/threat.

To update this diagram to your location, click three dots in the top-right corner of the diagram:



After that select country and city where the protected resource is located and click **Save**:








The diagram is updated.

LAST THREATS

This is a list of the last five attacks/threats:

2.

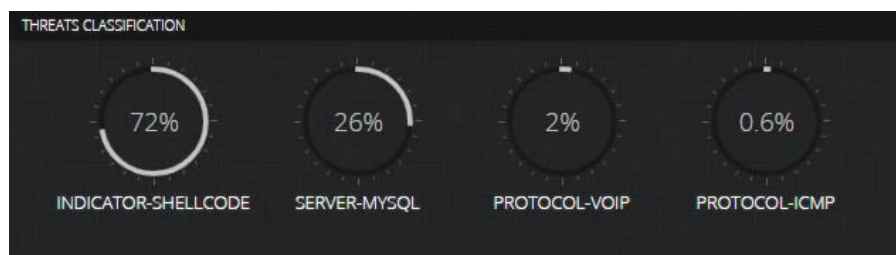
LAST THREATS		
	31.01.2019 / 11:45:05 ssh CRC32 overflow filler	high
	31.01.2019 / 11:44:20 ssh CRC32 overflow filler	high
	31.01.2019 / 11:44:20 ssh CRC32 overflow filler	high
	31.01.2019 / 11:44:09 ssh CRC32 overflow filler	high
	31.01.2019 / 11:43:53 ssh CRC32 overflow filler	high
Show all		

Clicking the attack/threat name displays a pop-up window with details on this attack/threat. Clicking the **Show all** button opens the full list of today's attacks and threats on the **ATTACKS AND THREATS** page.

THREATS CLASSIFICATION

3.

This diagram shows percentage ratio of the groups of attacks/threats:



Clicking the group name opens the list of attacks and threats filtered according to the selected group:

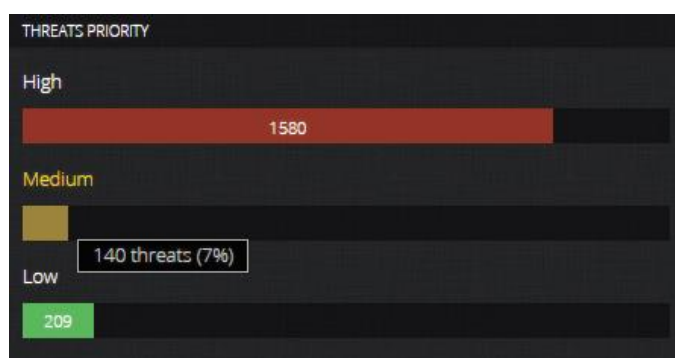
</

THREATS PRIORITY

This diagram is a bar chart that shows ratio of the priorities of attacks/threats.

Hovering over the bar displays the number and percentage of events within this priority:

4.



Clicking the bar opens the list of attacks and threats filtered according to the selected priority:

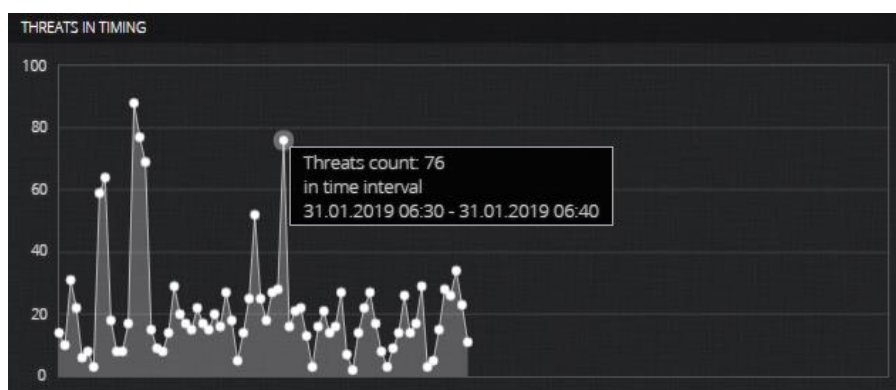
The screenshot shows the SNOWL interface with the 'ATTACKS AND THREATS' section. A filter 'priority=medium' is applied, showing 61 events. The table below lists the events:

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
31.01.2019 / 11:42:19	medium	SERVER-OTHER	OpenSSL TLS change cipher spec protocol denial of service	213.155.220.207	54749	192.168.1.10	443

5.

THREATS IN TIMING

This diagram is a graph that shows the number of attacks/threats in time. Hovering over the line displays the number of events and time interval:



Clicking the point on the graph opens the list of attacks and threats filtered according to the selected time interval:

The screenshot shows the SNOWL interface with the 'ATTACKS AND THREATS' section. A filter for the time interval '31.01.2019 06:30 - 31.01.2019 06:40' is applied, showing 1557 events. The table below lists the events:

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
31.01.2019 / 11:57:12	medium	PROTOCOL-VOIP	Sipicious User-Agent detected 2	185.53.91.44	5085	192.168.1.10	5060
31.01.2019 / 11:56:44	high	INDICATOR-SHELLCODE	ssh CRC32	192.52.242.143	59144	192.168.1.10	22

TOP ATTACKERS IP

This is a list of the most frequent attackers' IP addresses:

6.

TOP ATTACKER'S IP	
192.168.1.10	194
213.155.220.207	44
88.214.26.8	25
88.214.26.10	19
185.53.91.44	16
51.254.140.108	15

Clicking the IP address opens the list of attacks and threats filtered according to the selected IP:

The screenshot shows the SNOWL interface with the 'ATTACKS AND THREATS' section active. The filter 'ip.src=88.214.26.8' is applied, resulting in 18 events. The table below shows the details of the first event:

TIME	PRIORITY	GROUP	THREAT	IP SRC	PORT	IP DST	PORT
31.01.2019 / 11:46:11	high	INDICATOR-SHELLCODE	ssh CRC32 overflow filler 18	88.214.26.8	40957	192.168.1.10	22

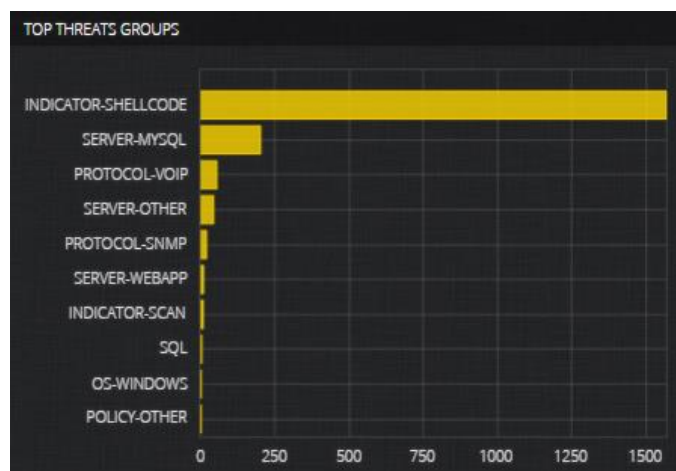
4.2.7.2. Diagrams on the Attacks and Threats Page

On the **ATTACKS AND THREATS** page, you can find the following diagrams: [TOP THREATS GROUPS](#), [TOP SOURCE IPS](#), [TOP DESTINATION IPS](#), [TOP THREATS](#), [THREATS PRIORITY](#), [PROTOCOLS](#), [TOP SOURCE PORTS](#), [TOP DESTINATION PORTS](#), [THREATS BY CONTINENTS](#), [THREATS BY COUNTRIES](#), [TOP](#)

1. [SOURCE MACS](#), [TOP DESTINATION MACS](#).

TOP THREATS GROUPS

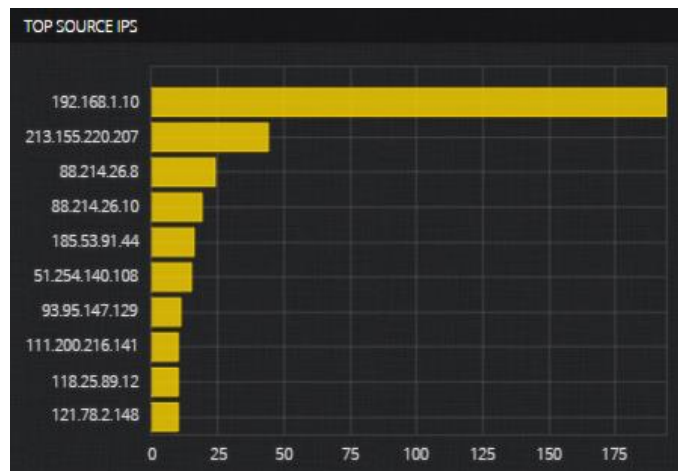
This diagram is a bar chart that shows ratio of the most frequent groups of attacks/threats:



TOP SOURCE IPS

This diagram is a bar chart that shows ratio of the most frequent attackers' IP addresses:

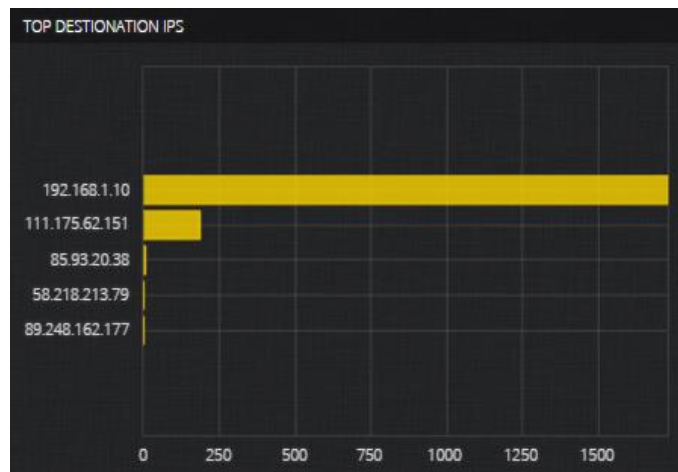
2.



TOP DESTINATION IPS

This diagram is a bar chart that shows ratio of the most frequent destination IP addresses:

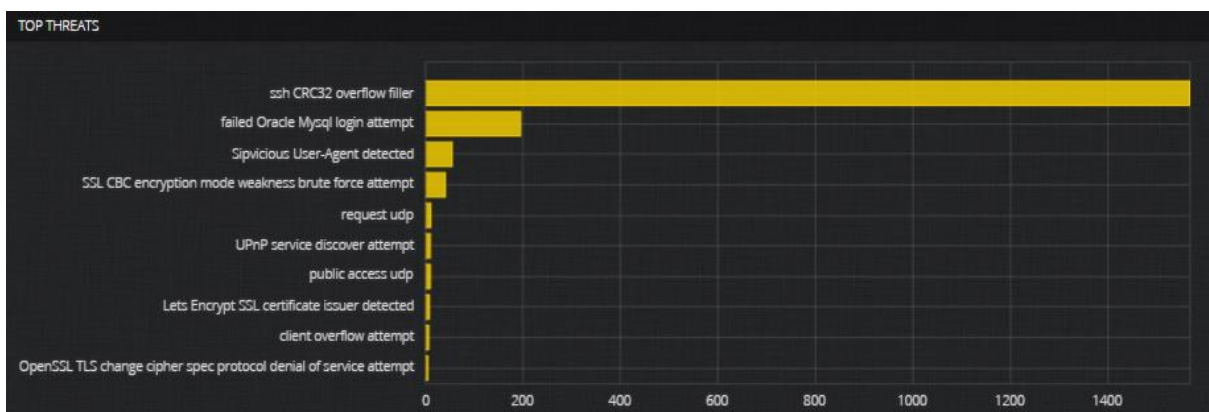
3.



4.

TOP THREATS

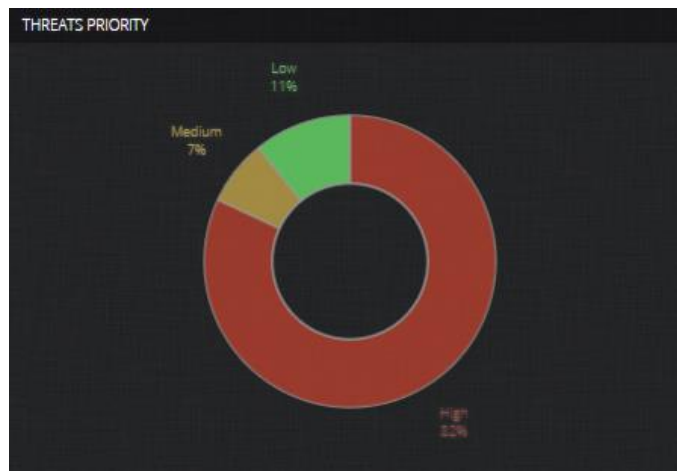
This diagram is a bar chart that shows ratio of the most frequent attacks/threats:



THREATS PRIORITY

This diagram is a pie chart that shows percentage ratio of priorities of the attacks/threats:

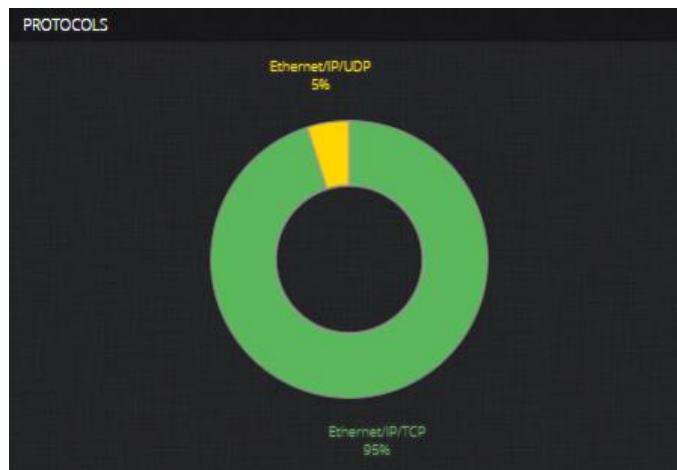
5.



PROTOCOLS

This diagram is a pie chart that shows percentage ratio of traffic protocols:

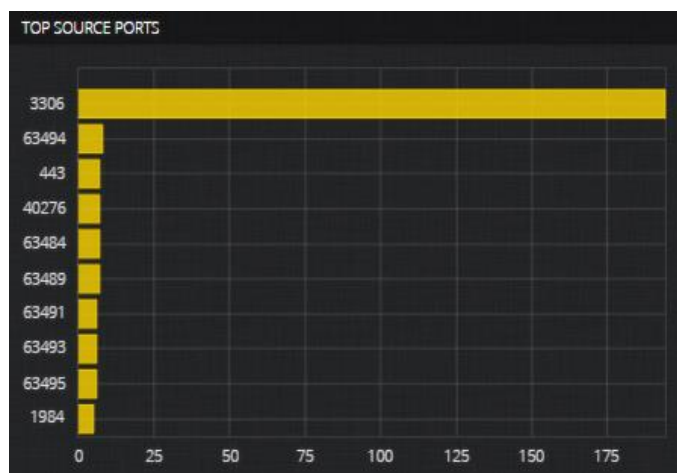
6.



7.

TOP SOURCE PORTS

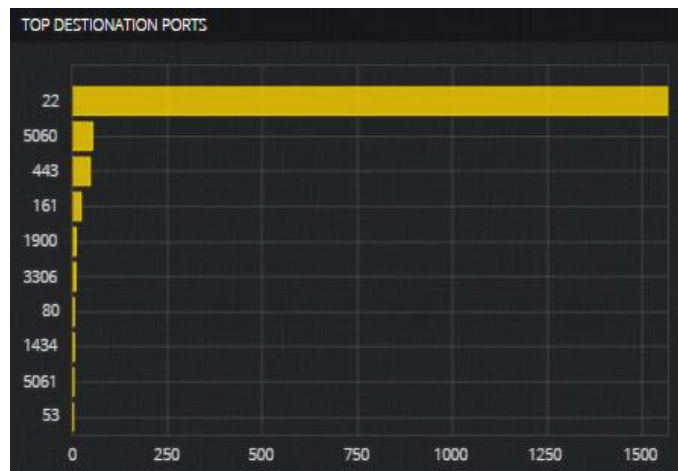
This diagram is a bar chart that shows ratio of the most frequent attackers' ports:



TOP DESTINATION PORTS

This diagram is a bar chart that shows ratio of the most frequent destination ports:

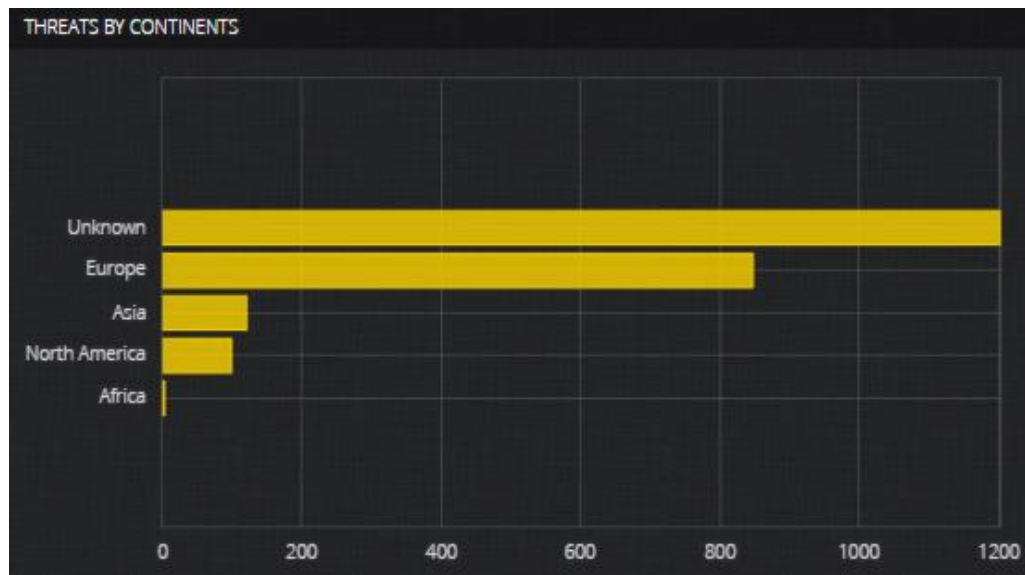
8.



THREATS BY CONTINENTS

This diagram is a bar chart that shows ratio of the attackers' continents:

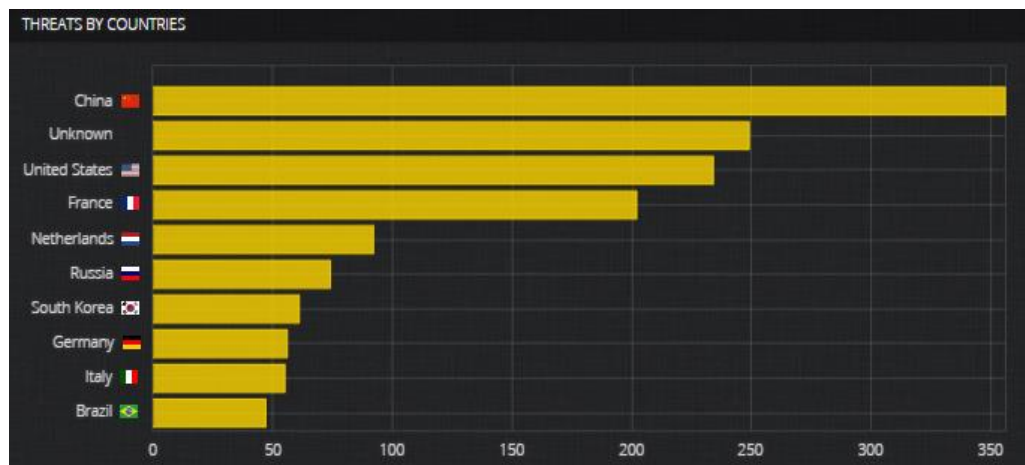
9.



10.

THREATS BY COUNTRIES

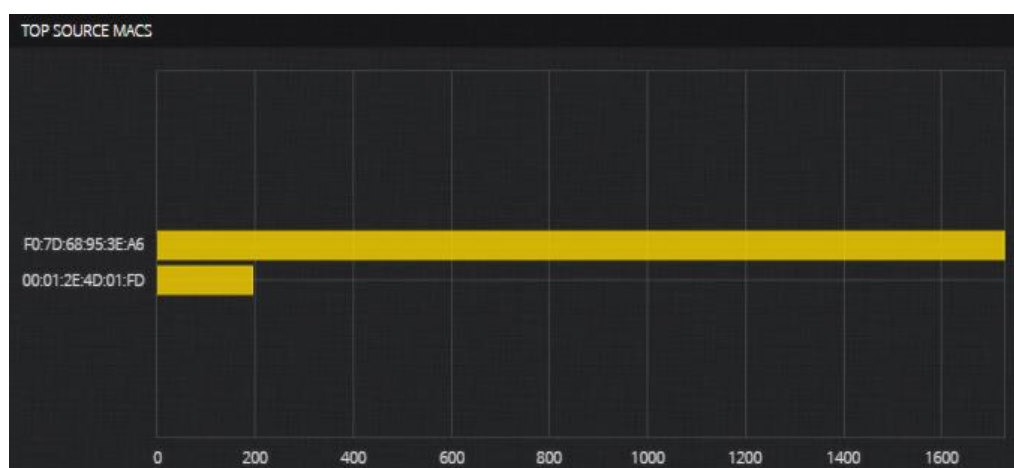
This diagram is a bar chart that shows ratio of the attackers' countries:



TOP SOURCE MACS

This diagram is a bar chart that shows ratio of the most frequent attackers' MAC addresses:

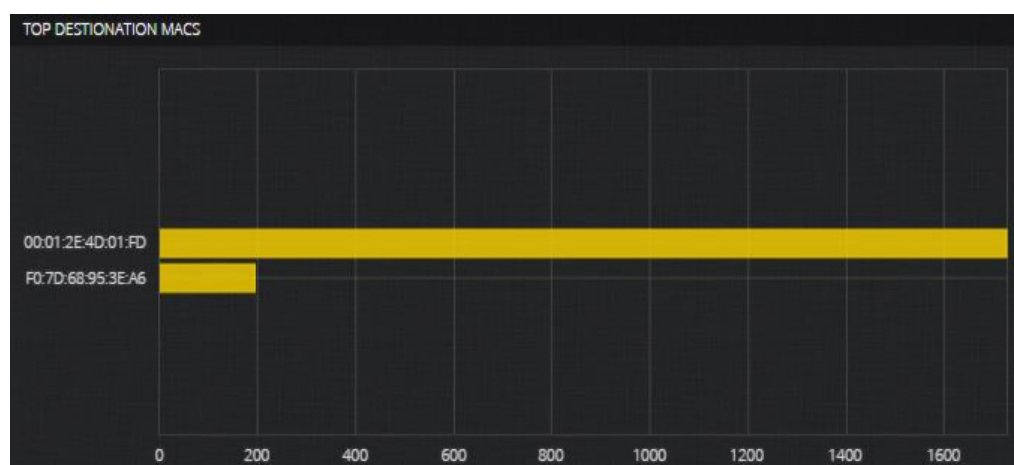
11.



TOP DESTINATION MACS

This diagram is a bar chart that shows ratio of the most frequent destination MAC addresses:

12.



4.2.8. Viewing Diagrams on Historical Data of Attacks and Threats

To analyze the state of a protected resource for a period in the past, view the diagrams on attacks and threats that occurred during the required period.

- You can find the diagrams on the **DASHBOARD** and **ATTACK AND THREATS** pages. By default, the diagrams show data for today. To select the required period, do the following:

For the **DASHBOARD** page:

- Click **DASHBOARD** in the main menu (this page opens by default upon logging in to the system).

- b. In the top-left corner of the page, select the required period: **Yesterday**, **Week**, **Month** or **Year**:



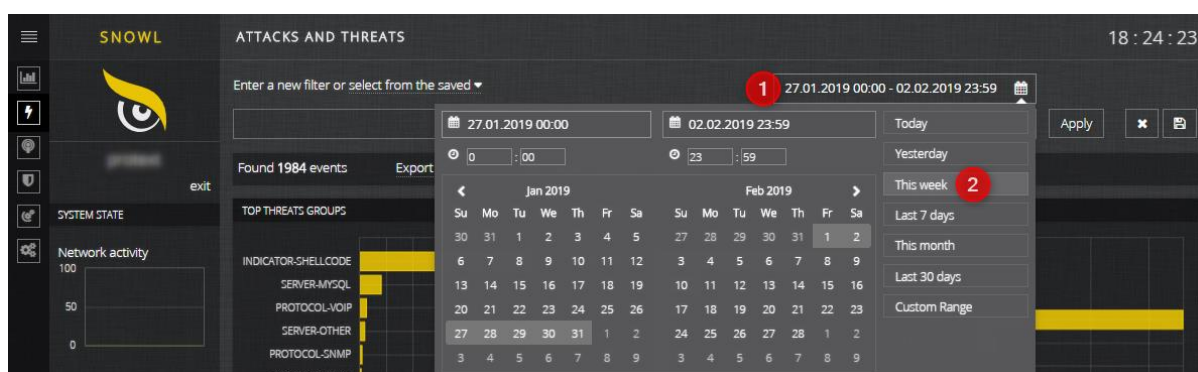
The diagrams are updated automatically.

For the **ATTACK AND THREATS** page:

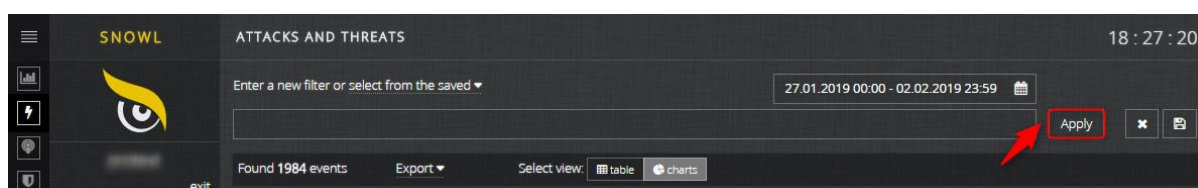
- a. Click **ATTACKS AND THREATS** in the main menu.
 b. Select the charts view:



- c. In the top-right corner of the page, click the dates and select the observation period: **Yesterday**, **This week**, **Last 7 days**, **This month**, **Last 30 days** or specify a custom range:



- d. Click **Apply**:



The diagrams are updated.

4.2.9. Filtering Diagrams Data

To filter data of the diagrams, you can use the same methods as described for the list of attacks and threats: [4.2.4, Filtering the List of Attacks and Threats](#).

4.3. Working with Sensors

These operations require administrator rights. If you don't have these rights, then you will not have the **SENSORS** item in the main menu.

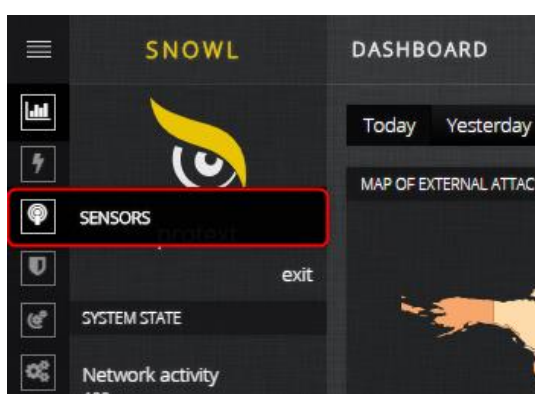
4.3.1. Adding New Sensor

Please note that before adding a new sensor to **SNOWL**, you should first install this sensor on a computer/server according to vendor instructions.

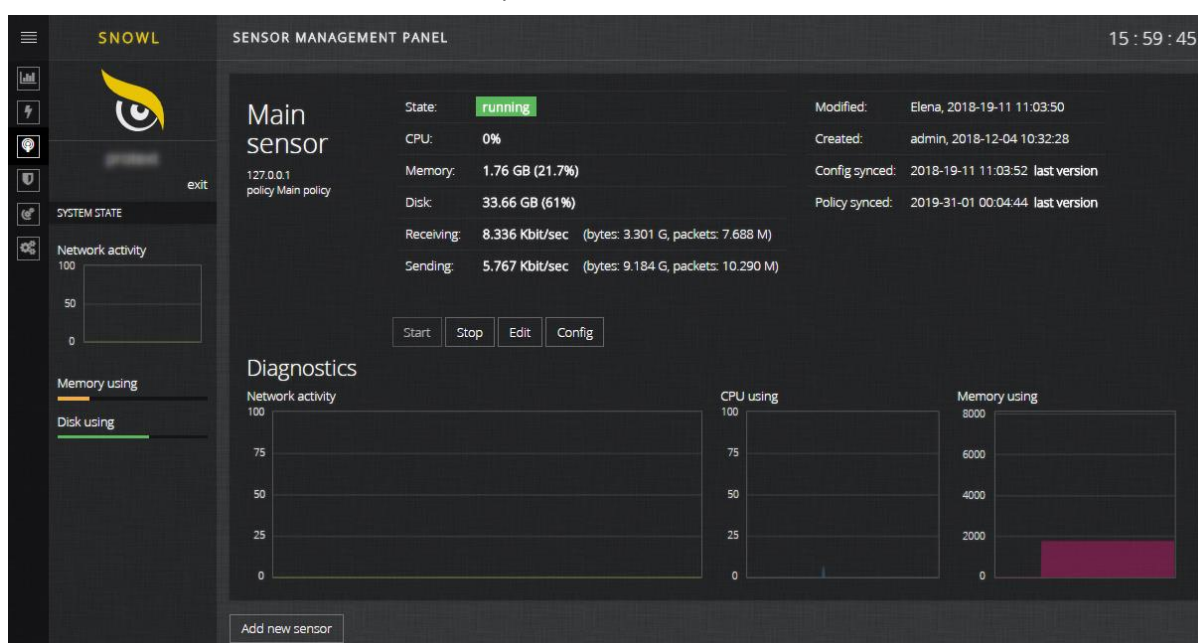
To add a new sensor to **SNOWL**, follow these steps:

Click **SENSORS** in the main menu:

1.



SENSOR MANAGEMENT PANEL opens:



In the bottom-left corner of the page, click **Add new sensor**.

A window for adding a new sensor appears:

2.

In the window for adding a new sensor, fill in the following fields:

3.

Name	Name of a new sensor.
Description	Description of a new sensor.
Address	IP address of a new sensor (obtained during sensor installation).
IDS	Type of a new sensor: Snort , Suricata or Other .
Interface	Physical network interface of a new sensor.
HomeNetwork	IP/mask of a new sensor.
Rule management	<p>If you want to use default management rules (free Snort Rule Set), then select the Snowl automatic manages the rules value. If you want to use custom management rules, then select the Custom rules value and specify paths to the following files:</p> <div data-bbox="525 1321 1303 1590"> </div>
Policy	Threat detection policy that should be applied to this sensor.

4.

Click **Save**.

1.

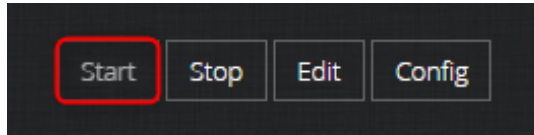
The new sensor is created.

4.3.2. Starting Sensor

To start a sensor, follow these steps:

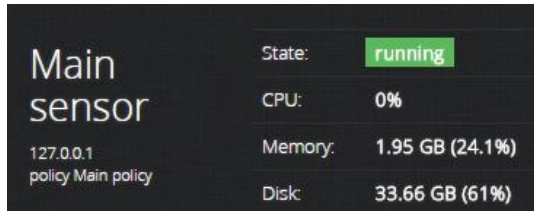
Click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens.

For the required sensor, click **Start**:



Sensor status is turned to **running**:

2.



4.3.3. Stopping Sensor

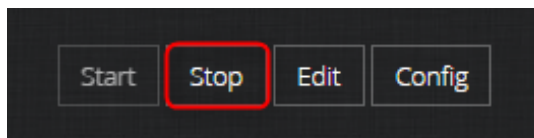
To stop a sensor, follow these steps:

Click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens.

For the required sensor, click **Stop**:

1.

2.



Sensor status is turned to **stopped**:



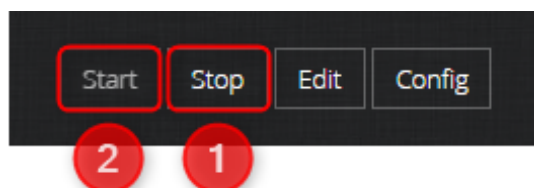
4.3.4. Restarting Sensor

1.

2. To restart a sensor, follow these steps:

Click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens.

For the required sensor, click **Stop**, then **Start**:



1.

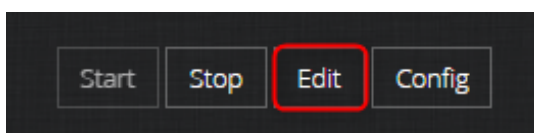
2.

4.3.5. Changing Sensor Properties

To change sensor properties, follow these steps:

Click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens.

For the required sensor, click **Edit**:



In the window that appears, edit the required fields and click **Update**:

3.

On **SENSOR MANAGEMENT PANEL**, in the **Modified** field, you can see information on the last update:

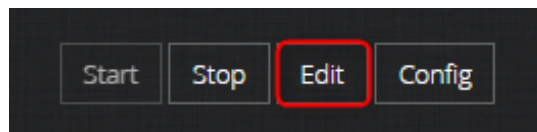
Main sensor <small>127.0.0.1 policy Main policy</small>	State:	running	Modified:	2019-31-01 16:44:55
	CPU:	0%	Created:	admin, 2018-12-04 10:32:28
	Memory:	1.32 GB (16.29%)	Config synced:	2019-31-01 16:44:58 last version
	Disk:	33.70 GB (61%)	Policy synced:	2019-01-02 00:01:47 last version
	Receiving:	20.162 Kbit/sec (bytes: 3.459 G, packets: 8.021 M)		
	Sending:	8.896 Kbit/sec (bytes: 9.288 G, packets: 10.579 M)		

4.3.6. Deleting Sensor

1. To delete a sensor, follow these steps:

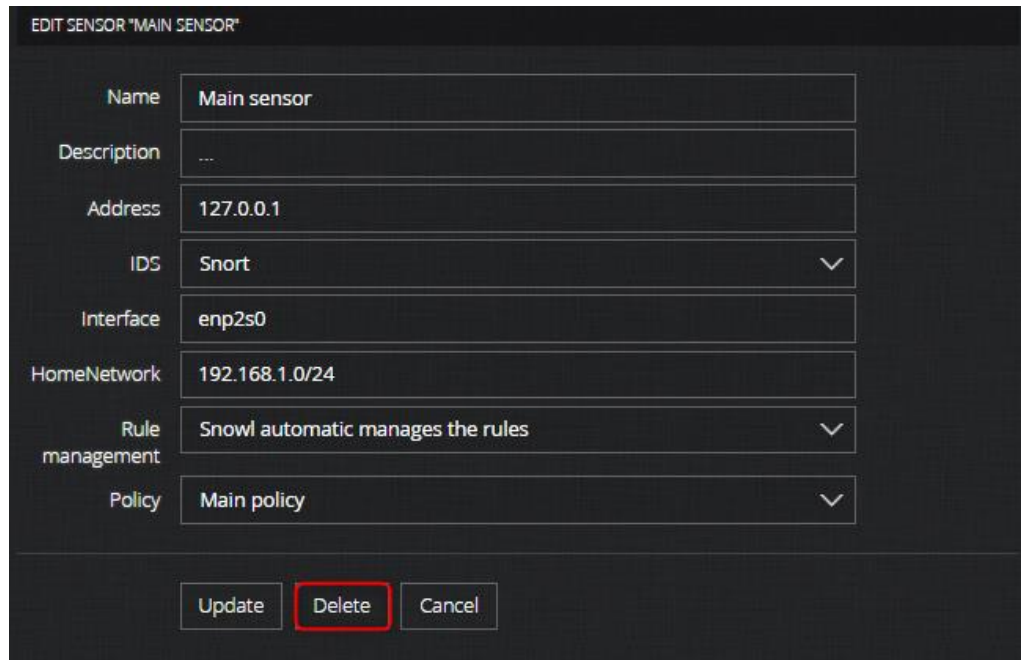
2. Click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens.

For the required sensor, click **Edit**:



In the window that appears, click **Delete**:

3.



EDIT SENSOR "MAIN SENSOR"

Name	Main sensor
Description	---
Address	127.0.0.1
IDS	Snort
Interface	enp2s0
HomeNetwork	192.168.1.0/24
Rule management	Snowl automatic manages the rules
Policy	Main policy

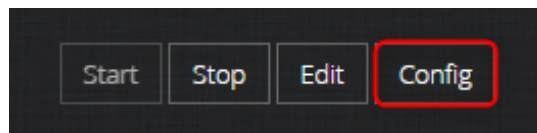
Update Delete Cancel

The sensor is deleted.

4.3.7. Configuring Sensor

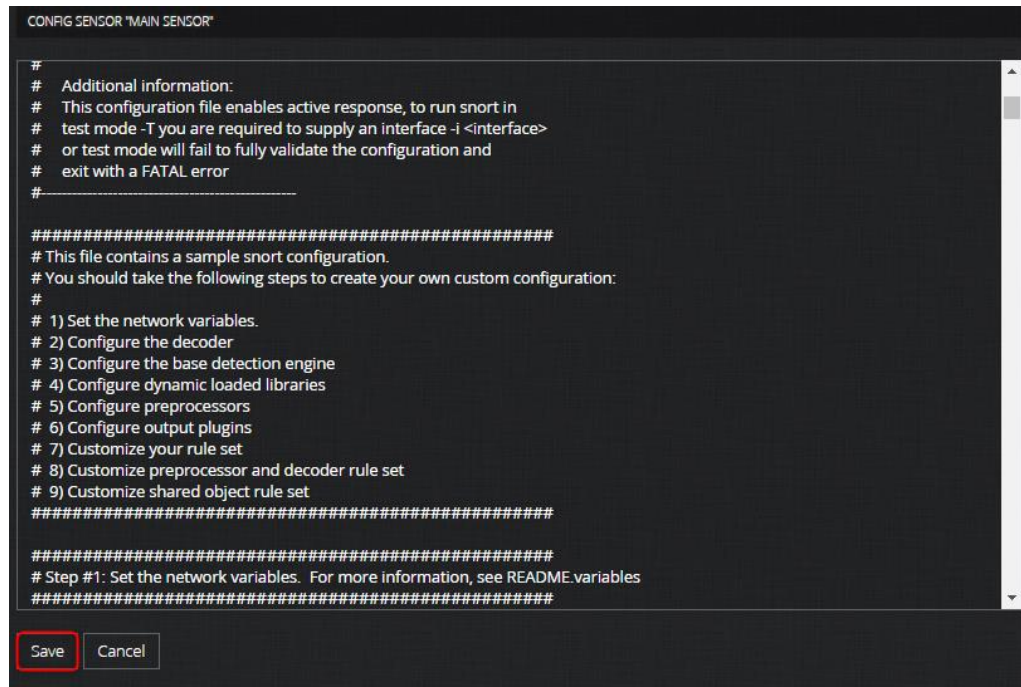
To change sensor configuration, edit the sample configuration file provided by vendor. To do that, follow these steps:

1. Click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens.
2. For the required sensor, click **Config**:



Edit the configuration file (for example, set network variables) and click **Save**:

3.

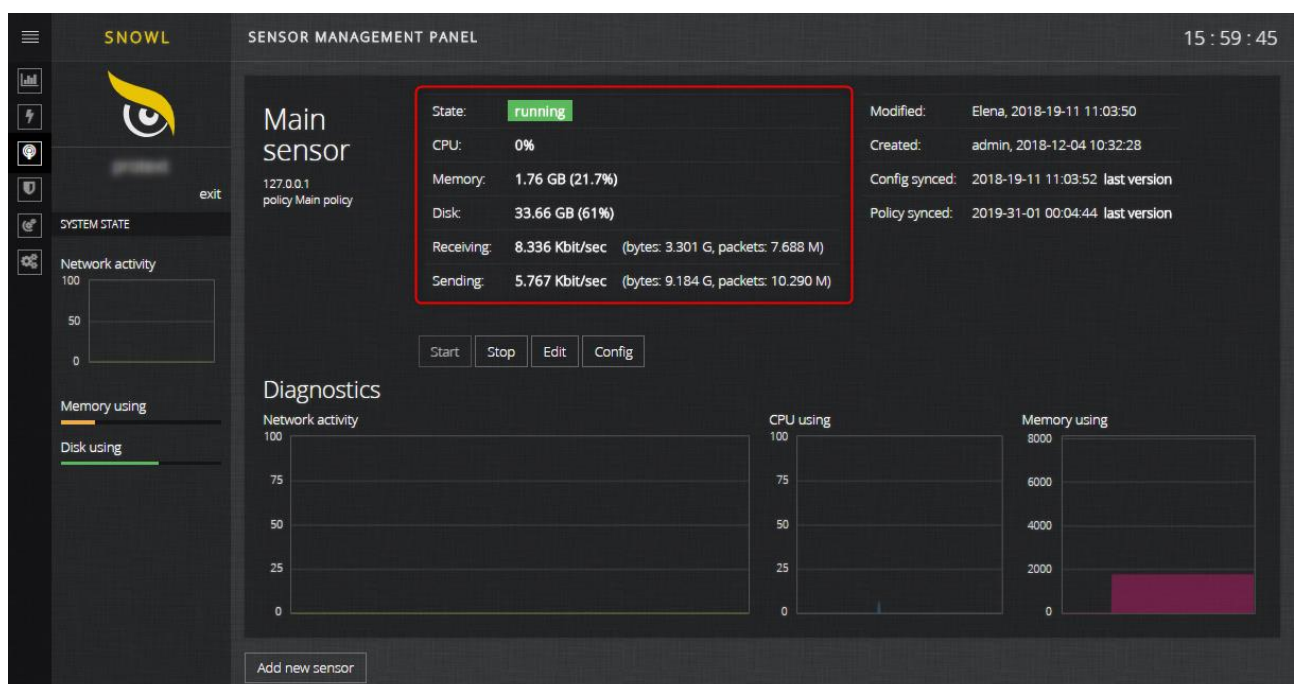


Sensor configuration is changed.

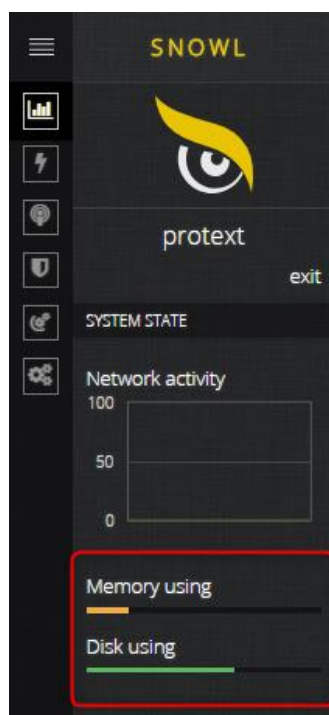
4.3.8. Viewing Sensor Activity Data

To view sensor activity data, click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens. You can view the following sensor activity parameters at the top of the widget:

- **State**
- **CPU**
- **Memory**
- **Disk**
- **Receiving**
- **Sending**



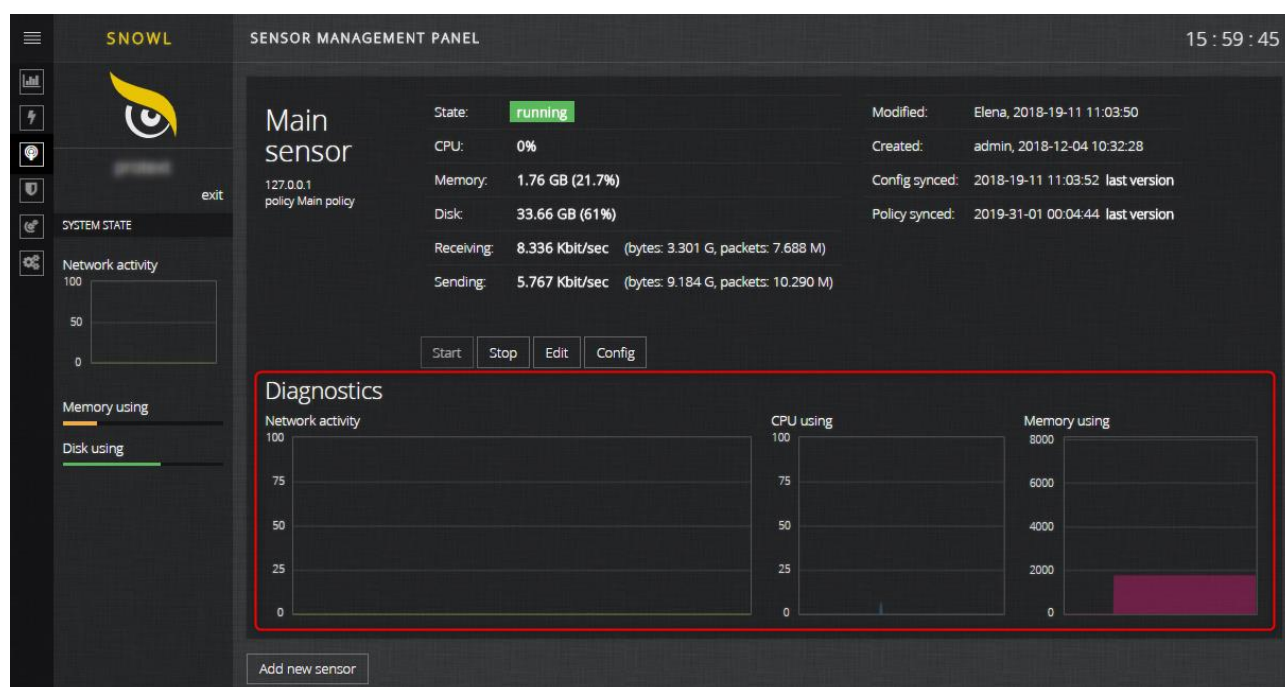
You can also monitor the **Memory using** and **Disk using** parameters in the left panel:



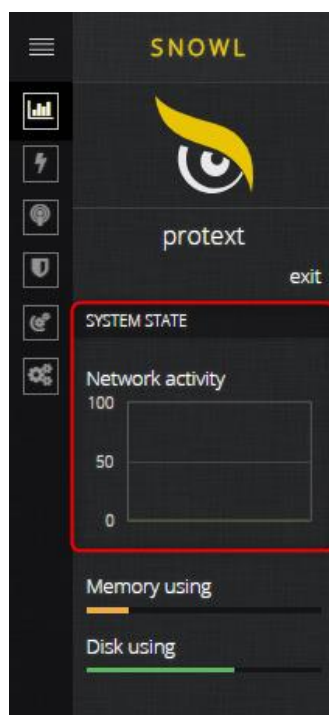
4.3.9. Viewing Sensor Activity Diagrams

To view sensor activity diagrams, click **SENSORS** in the main menu. **SENSOR MANAGEMENT PANEL** opens. You can view the following sensor activity diagrams at the bottom of the widget:

- **Network activity**
- **CPU using**
- **Memory using**



You can also monitor the **Network activity** diagram in the left panel:



4.4. Working with Threat Policies

These operations require administrator rights. If you don't have these rights, then you will not have the **THREAT POLICIES** item in the main menu.

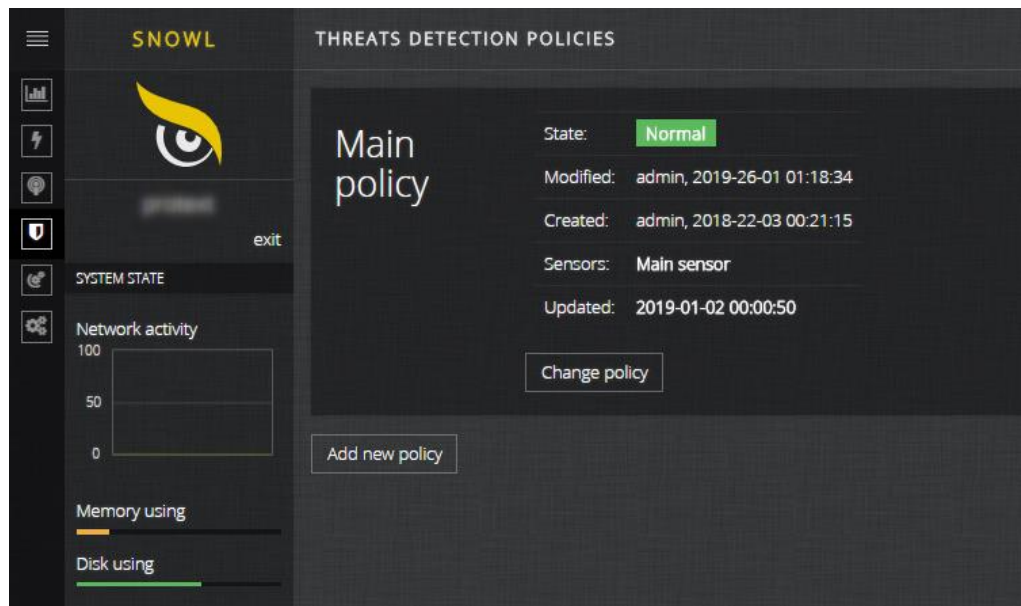
4.4.1. Adding New Threat Policy

1. To add a new threat policy, follow these steps:

Click **THREAT POLICIES** in the main menu:



The **THREATS DETECTION POLICIES** page opens:



In the bottom-left corner of the page, click **Add new policy**.

A window for adding a new policy appears:

2.

3.

In the window for adding a new policy, fill in the following fields:

Name	Name of a new threat policy.
Description	Description of a new threat policy.
Based on	If you select the Based on check box, then you can select an existing threat policy from a drop-down list box. In this case,

	properties of the new policy are copied from the selected one. The remaining fields in this form are hidden.
Rule urls	URLs for storing the rules files provided by vendor. If specified, SNOWL can automatically update the rules (update frequency is configured in the Auto updates field). If you fill in the Rule urls field, then do not fill in the Ruleset files field.
Ruleset files	Rules files that are provided by vendor or created. If you fill in the Ruleset files field, then do not fill in the Rule urls field.
IP blacklist urls	URLs for storing the IP blacklist files provided by vendor. If specified, SNOWL can automatically update the files (update frequency is configured in the Auto updates field). If you fill in the IP blacklist urls field, then do not fill in the IP blacklist files field.
IP blacklist files	IP blacklist files that are provided by vendor or created. If you fill in the IP blacklist files field, then do not fill in the IP blacklist urls field.
Auto updates	Update frequency of rules (if the Rule urls field is filled) and IP black lists (if the IP blacklist files field is filled).

Click **Save**.

4. The new threat policy is created.

4.4.2. Copying Threat Policy

To copy a threat policy, follow these steps:

1. Click **THREAT POLICIES** in the main menu. The **THREATS DETECTION POLICIES** page opens.
2. In the bottom-left corner of the page, click **Add new policy**.

A window for adding a new policy appears:

- 3.

In the window for adding a new policy, follow these steps:

- a. In the **Name** field, specify the name of a new threat policy.
- b. In the **Description** field, specify the description of a new threat policy.
- c. Select the **Based on** check box.
- d. In the **Based on** drop-down list box, select an existing threat policy.
- e. Click **Save**.

The new threat policy is created, and its properties are copied from the selected one.

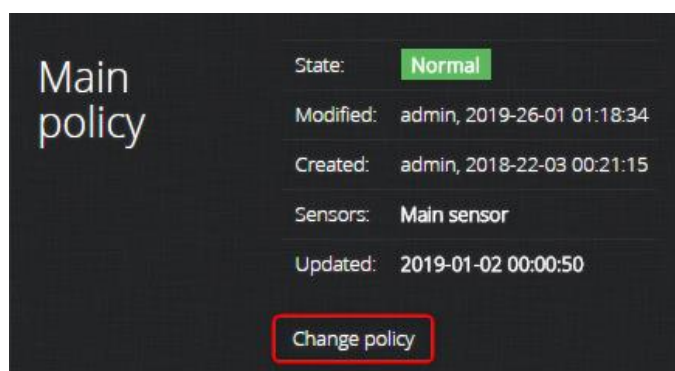
4.4.3. Changing Threat Policy

To change a threat policy, follow these steps:

Click **THREAT POLICIES** in the main menu. The **THREATS DETECTION POLICIES** page opens.

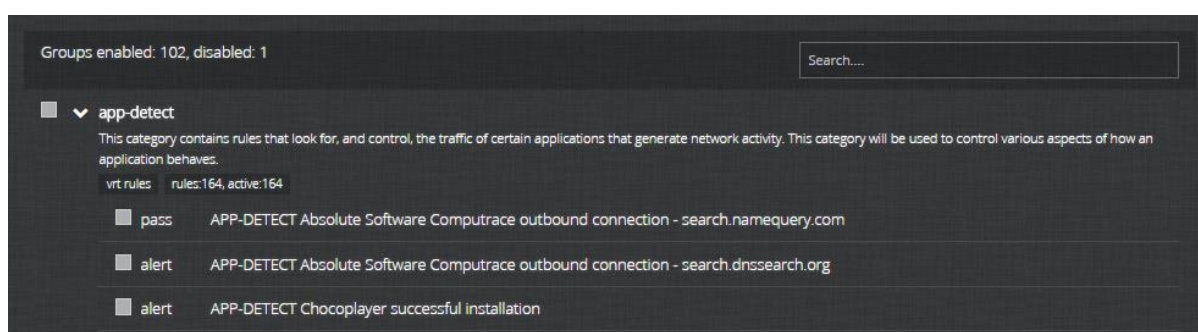
For the required policy, click **Change policy**:

- 1.
- 2.



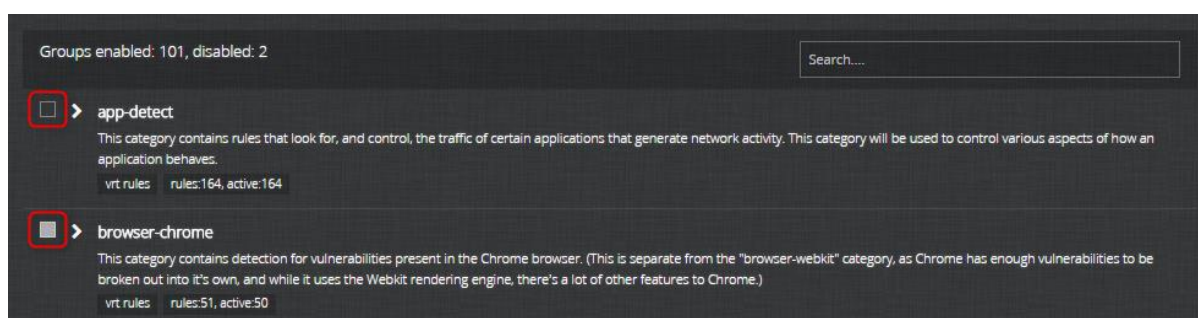
In the window that appears, you can see the list of categories. Each category includes rules that are automatically obtained by **SNOWL** from the corresponding files:

- 3.



You can make the following changes to the selected policy:

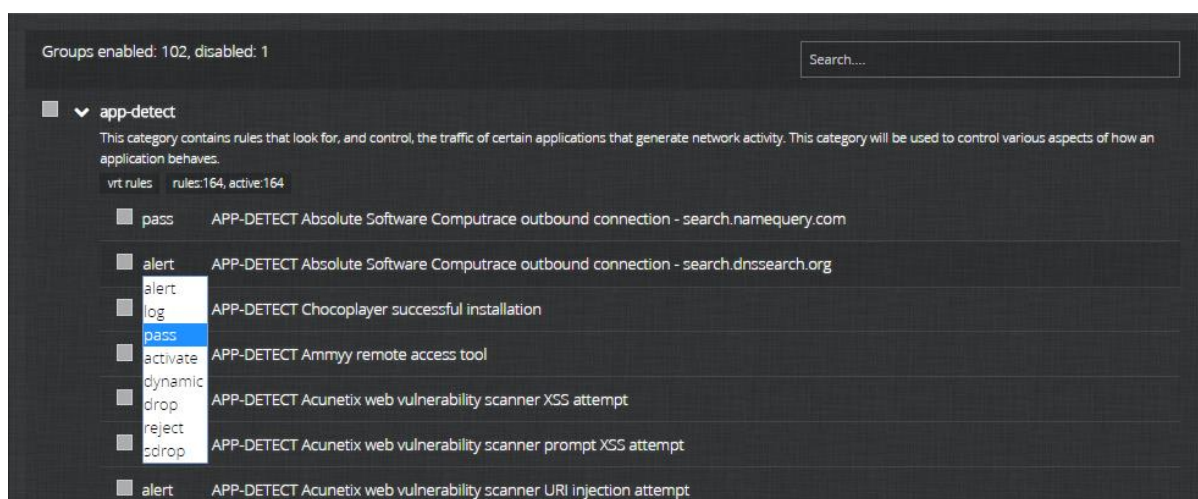
- **Turn on/off a category** (that is turn on/off all rules of this category). To do that, select or clear the check box next to the category name:



- **Turn on/off a rule**. To do that, select or clear the check box next to the rule name:



- **Change action mode of a rule.** To do that, click the rule name and select the required action:

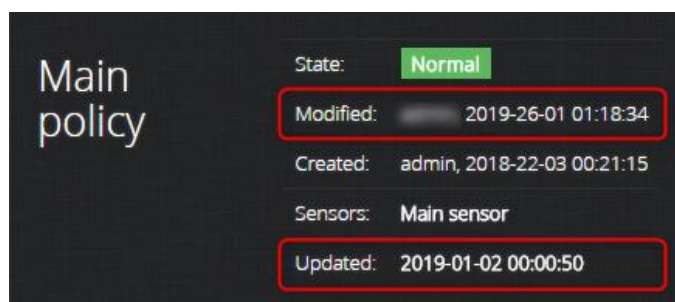


In the widget corresponding to a policy, you can see information on the last policy changes:

In the **Modified** field – manual changes made by user.

In the **Updated** field – automatic changes made by **SNOWL**.

•



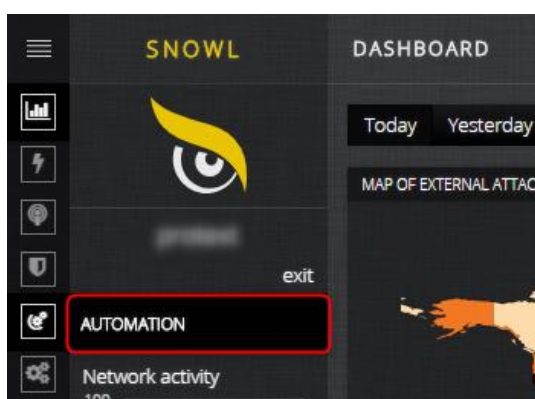
4.5. Working with Automatic Actions

These operations require administrator rights. If you don't have these rights, then you will not have the **AUTOMATION** item in the main menu.

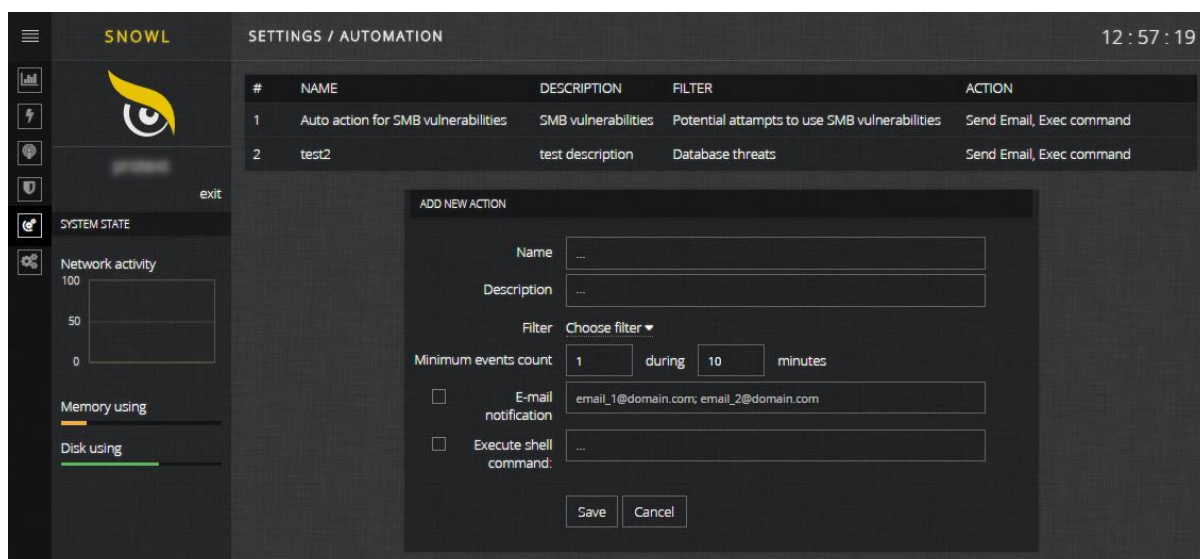
4.5.1. Adding New Automatic Action

To add a new automatic action, follow these steps:

Click **AUTOMATION** in the main menu:



The **SETTINGS / AUTOMATION** page opens:



In the window for adding a new automatic action, fill in the following fields:

2.	Name	Name of a new automatic action.
	Description	Description of a new automatic action.
	Filter	Rules for selecting threats/attacks that require an automatic action. Select one of the following filters in the drop-down list box: <ul style="list-style-type: none"> • Auto actions test • Database threats • Potential attempts to use SMB vulnerabilities If you need to create additional filters, see section 4.5.4, Creating Filter .
	Minimum events count	If the number of filtered threats/attacks is more than or equal to this value per X minutes (see the during minutes field), then the automatic action is applied.
	during minutes	Time interval during which the threshold number of threats/attacks is reached (see the Minimum events count field).
	Email notification	Email(s) for sending notifications. Before filling this field, make sure that SNOWL is configured to send notifications (for more information, see section 4.6.4, Configuring SNOWL for Sending Notifications).
3.	Execute shell command	Shell command or path to the executable file. Path example: <code>/home/john_doe/autoaction_test.sh --auto -quite</code> . This command is automatically applied upon detecting an event satisfying the predefined filter (the Filter field) and frequency (the Minimum events count and during minutes fields).

1. Click **Save**.

The new automatic action is created.

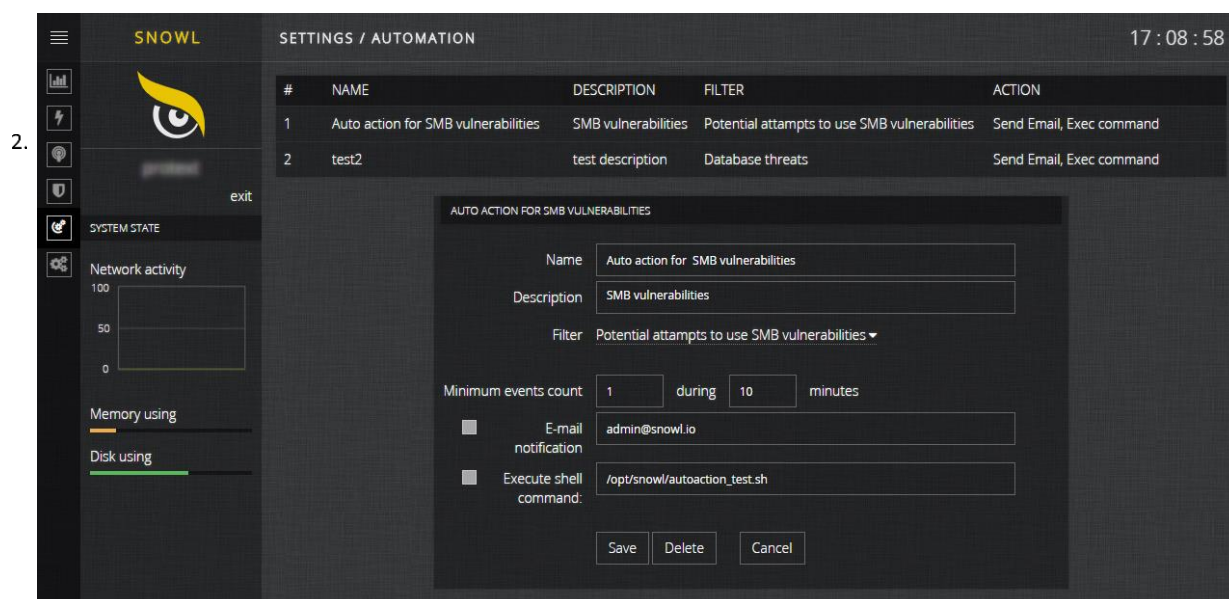
4.5.2. Changing Automatic Action

To change an automatic action, follow these steps:

Click **AUTOMATION** in the main menu. The **SETTINGS / AUTOMATION** page opens.

In the list of automatic actions, select the required one.

The window for changing the selected automatic action appears instead of the window for adding a new automatic action:



In the window for changing the selected automatic action, edit the required fields and click **Save**.

3.

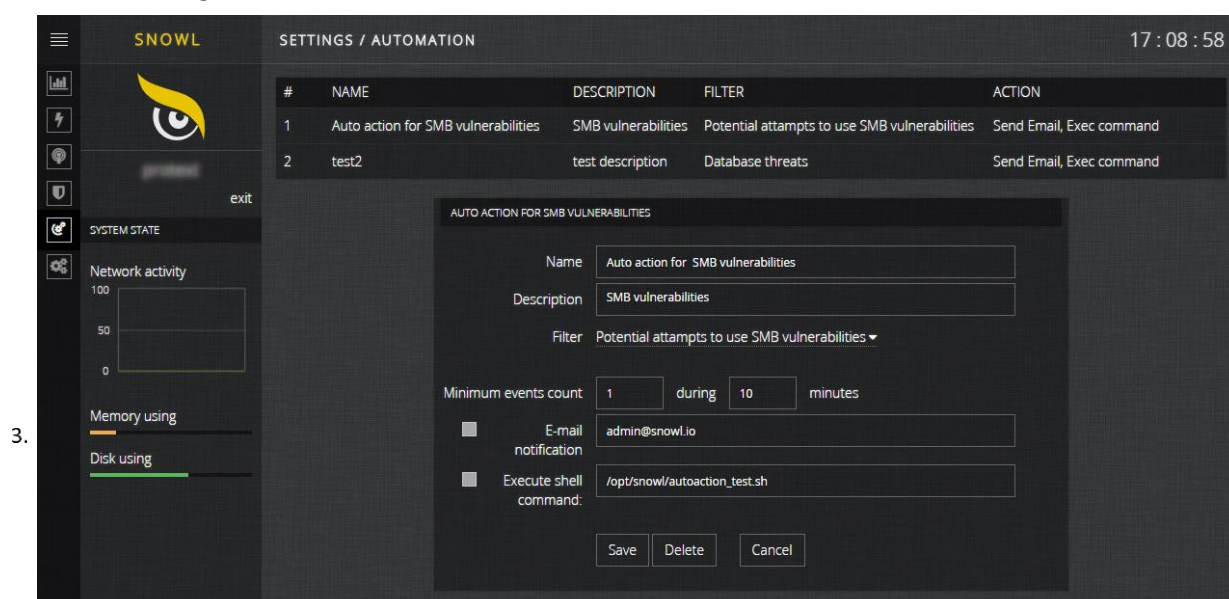
4.5.3. Deleting Automatic Action

To delete an automatic action, follow these steps:

1. Click **AUTOMATION** in the main menu. The **SETTINGS / AUTOMATION** page opens.

2. In the list of automatic actions, select the required one.

The window for changing the selected automatic action appears instead of the window for adding a new automatic action:



In the window for changing the selected automatic action, click **Delete**.

4.5.4. Creating Filter

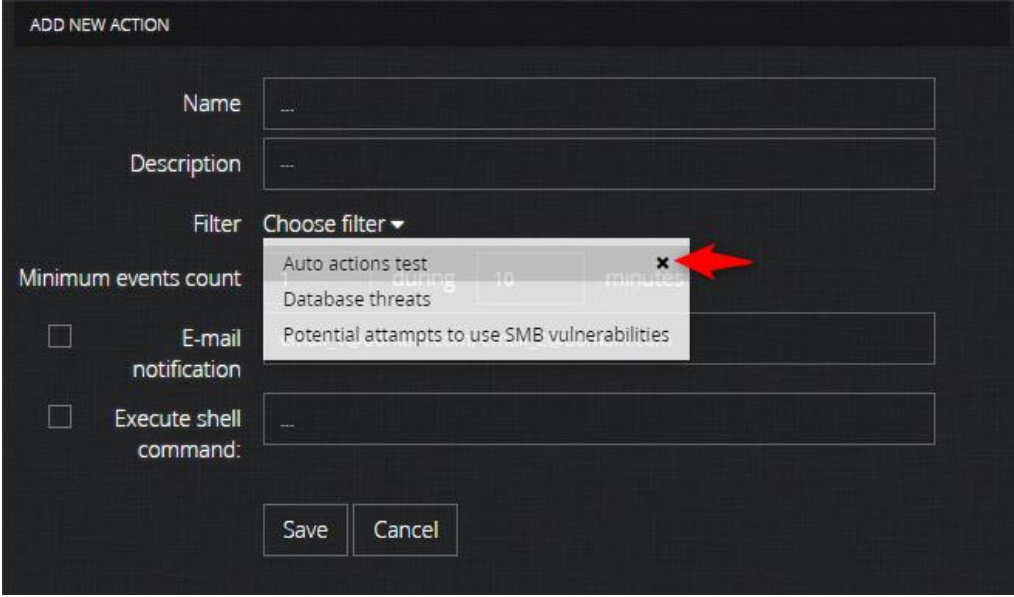
When you create an automatic action, a filter of threats/attacks should be selected. By default, **SNOWL** provides three predefined filters. You can create any filters you need using instructions in sections [4.2.4.3, Creating and Applying New Filter](#) and [4.2.4.4, Saving New Filter as a Predefined One](#).

4.5.5. Deleting Filter

To delete a filter that can be applied to an automatic action, follow these steps:

Click **AUTOMATION** in the main menu. The **SETTINGS / AUTOMATION** page opens.

In the **ADD NEW ACTION** window, click **Choose filter** in the **Filter** field, then click **X** next to the required filter:

- 1.
 - 2.
- 
- 3.
- Click **Yes** to confirm the deletion.

4.6. SNOWL Settings

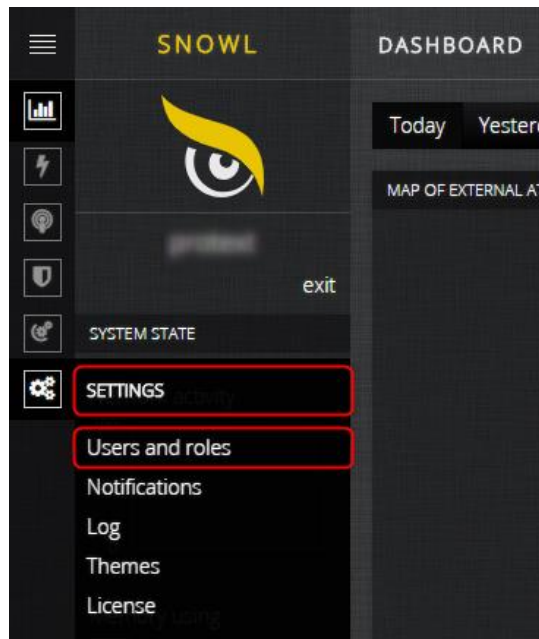
These operations require administrator rights. If you don't have these rights, then you will not have the **SETTINGS** item in the main menu.

4.6.1. Adding New User

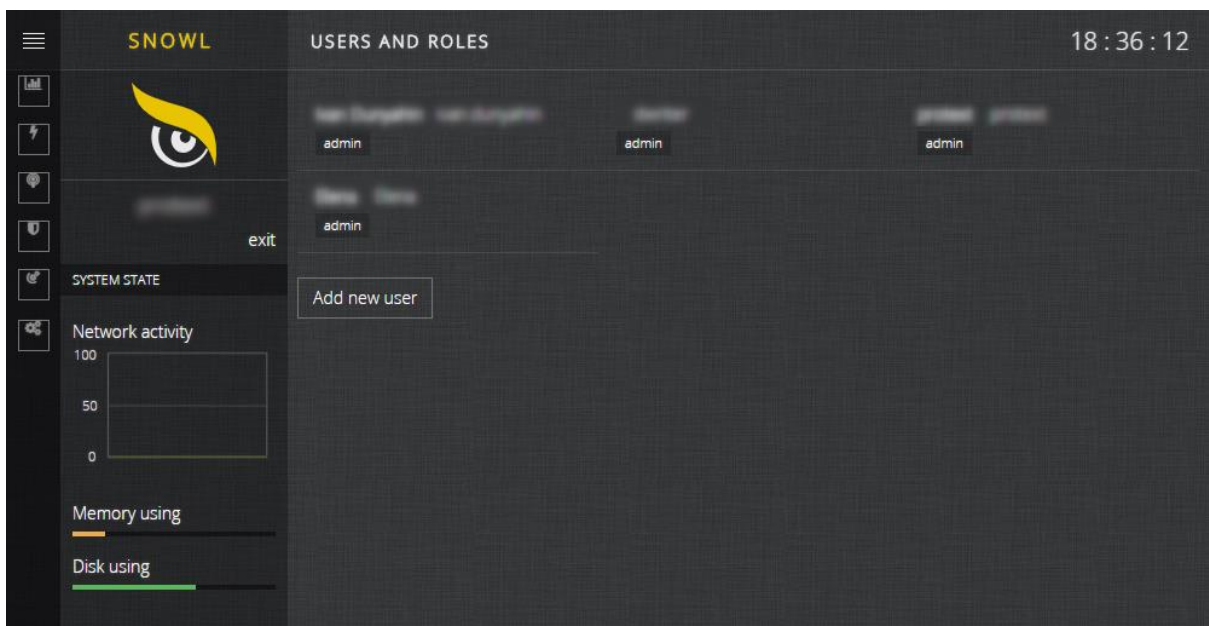
To add a new user, follow these steps:

Click **SETTINGS** in the main menu and **Users and roles** in the secondary menu:

1.



The **USERS AND ROLES** page opens:



Click **Add new user** under the table. The window for adding a new user appears:

2.

ADD NEW USER

First name

Last name

Username

Email

Group Viewer ▼

Password

Confirm

In the window for adding a new user, fill in the following fields:

3.

First name	User's first name.
Last name	User's last name.
Username	Account name.
Email	User's email.
Group	Group of rights: Admin or Viewer . For users having the Viewer group of rights, only two pages are available in the main menu: DASHBOARD and ATTACKS AND THREATS .
Password	Password for this account.
Confirm	Password for this account (repeatedly).

4.

Click **Create**.

The new user is created.

4.6.2. Changing User's Personal Data

1.

To change user's personal data, follow these steps:

2.

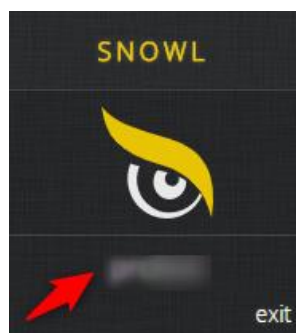
Click **SETTINGS** in the main menu and **Users and roles** in the secondary menu. The **USERS AND ROLES** page opens.

In the table containing accounts of all employees registered in **SNOWL**, click the required account. A window for changing the selected account appears.

In the window for changing the selected account, edit the required fields and click **Update**.

3.

To change your own account, you can click the account name under the owl's eye:



In the window that appears, edit the required fields and click **Save**.

4.6.3. Deleting User

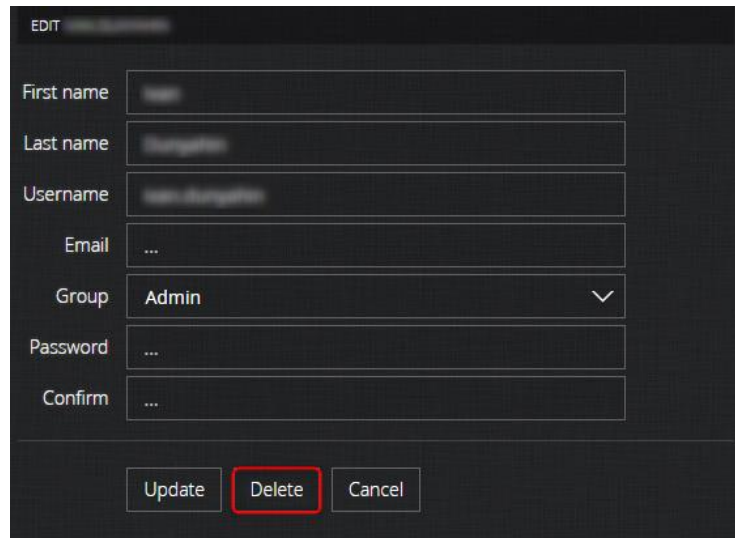
1. To delete an existing user, follow these steps:

2. Click **SETTINGS** in the main menu and **Users and roles** in the secondary menu. The **USERS AND ROLES** page opens.

In the table containing accounts of all employees registered in **SNOWL**, click the required account. The window for changing the selected account appears.

In the window for changing the selected account, click **Delete**.

3.



Click **OK** to confirm the deletion.

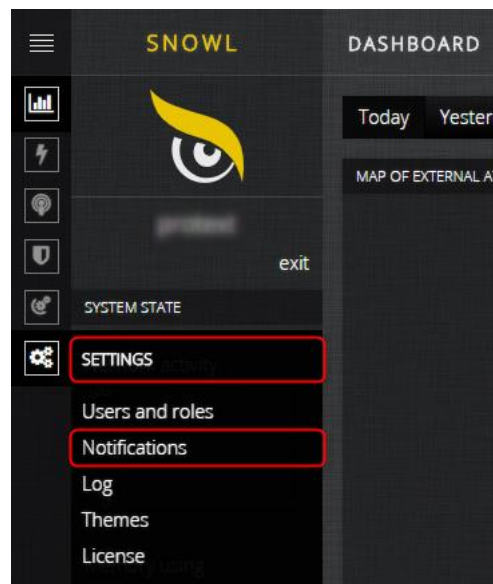
4.6.4. Configuring SNOWL for Sending Notifications

4.

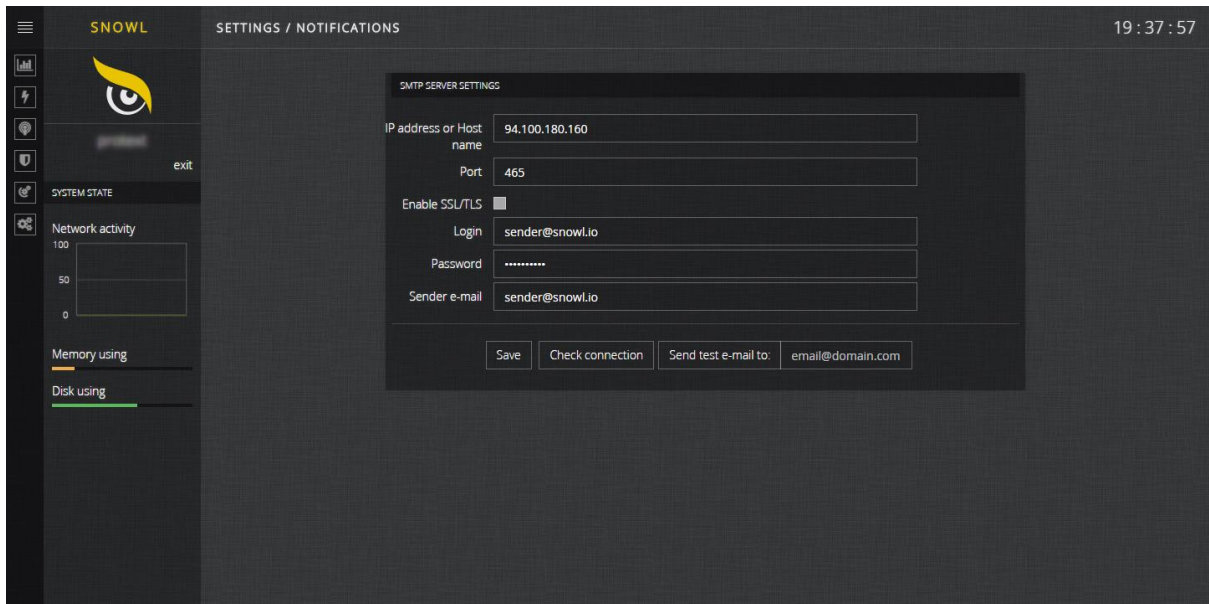
To enable **SNOWL** send email notifications as a part of automatic actions, follow these steps:

Click **SETTINGS** in the main menu and **Notifications** in the secondary menu:

1.



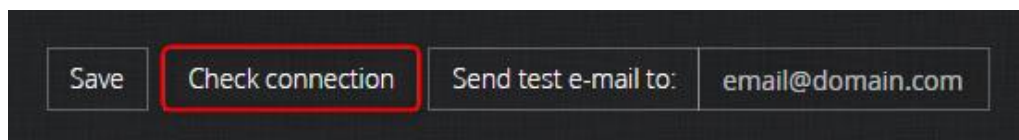
The **SETTINGS / NOTIFICATIONS** page opens:



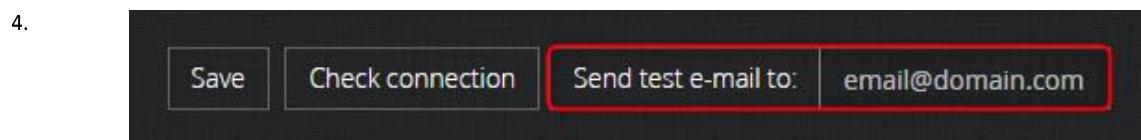
In the **SMTP SERVER SETTINGS** window, fill in the following fields:

2.	IP address or Host name	IP address or domain name of SMTP server.
	Port	Listening port of SMTP server that is used to send emails.
	Enable SSL/TLS	Select this check box if you need to use SSL/TLS encryption when interacting with SMTP server.
	Login	Login that is used for authentication on SMTP server when sending notification letters by SNOWL .
	Password	Password that is used for authentication on SMTP server when sending notification letters by SNOWL .
3.	Sender email	Email that is displayed when a user receives notification letter from SNOWL .

Click **Check connection** to ensure that SMTP server is configured properly:



You can also send a test email to check this. To send a test email, specify your email and click **Send test email to:**



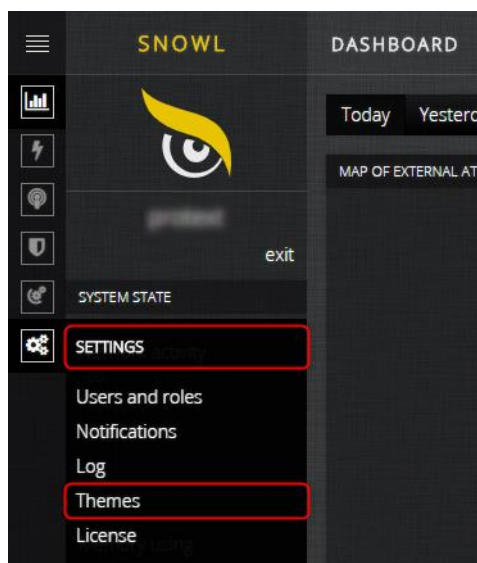
Click **Save**.

4.6.5. Changing SNOWL Interface

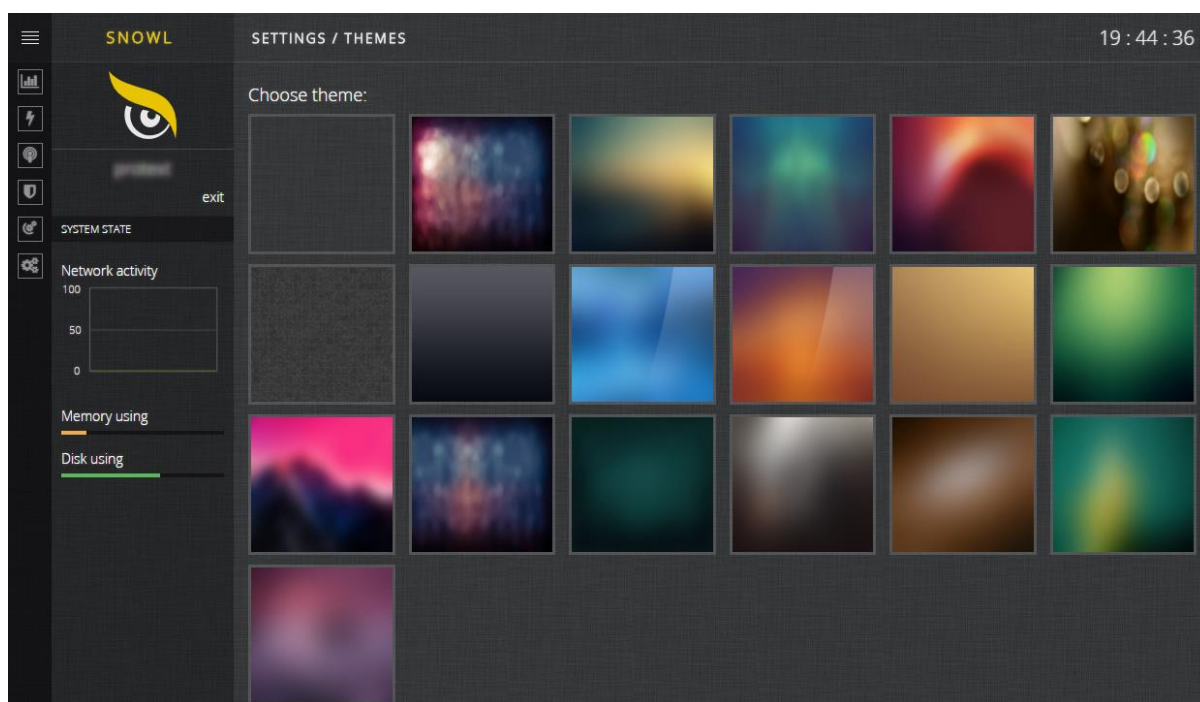
To change **SNOWL** interface, follow these steps:

Click **SETTINGS** in the main menu and **Themes** in the secondary menu:

1.

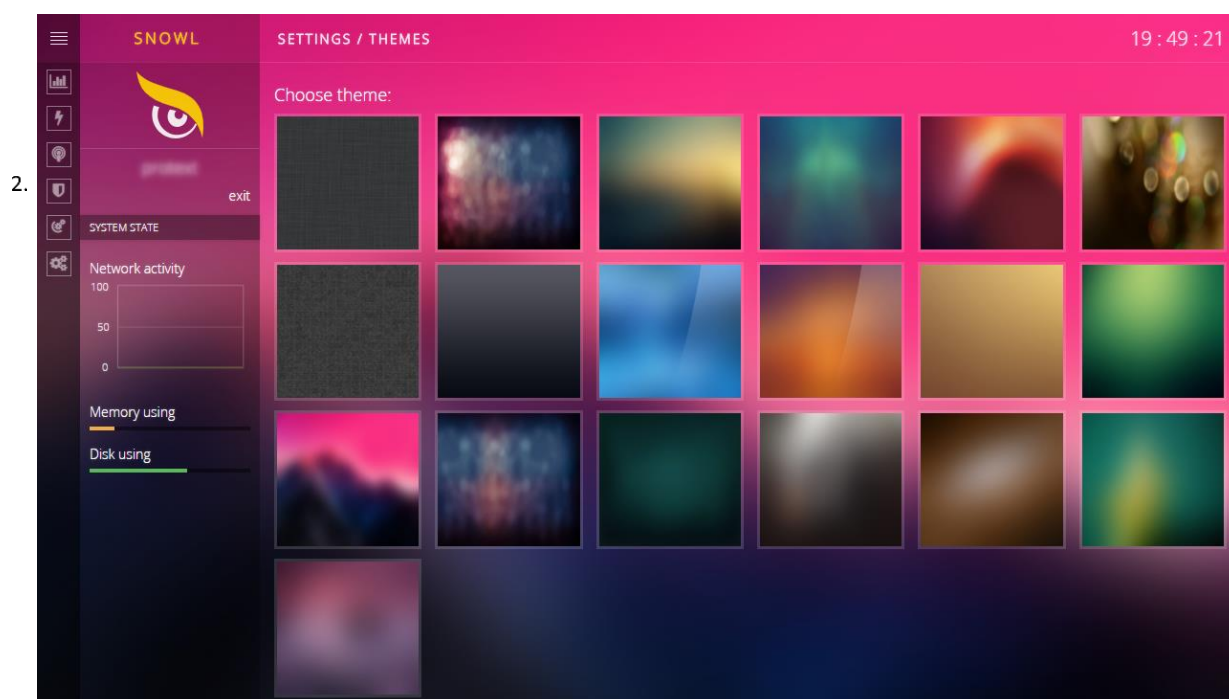


The **SETTINGS / THEMES** page opens:



Select a theme you want to apply.

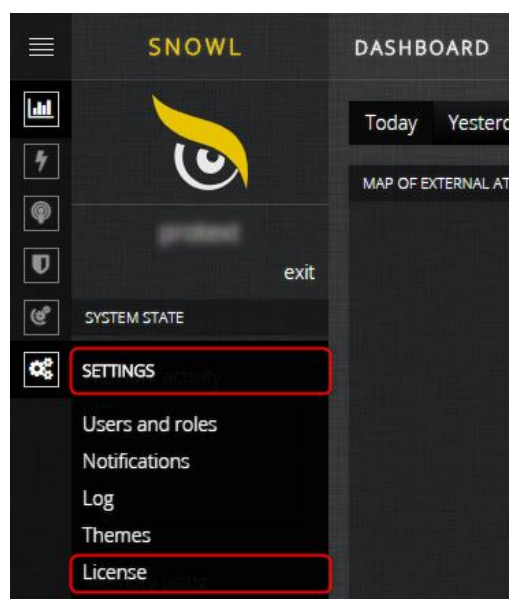
SNOWL is updated automatically:



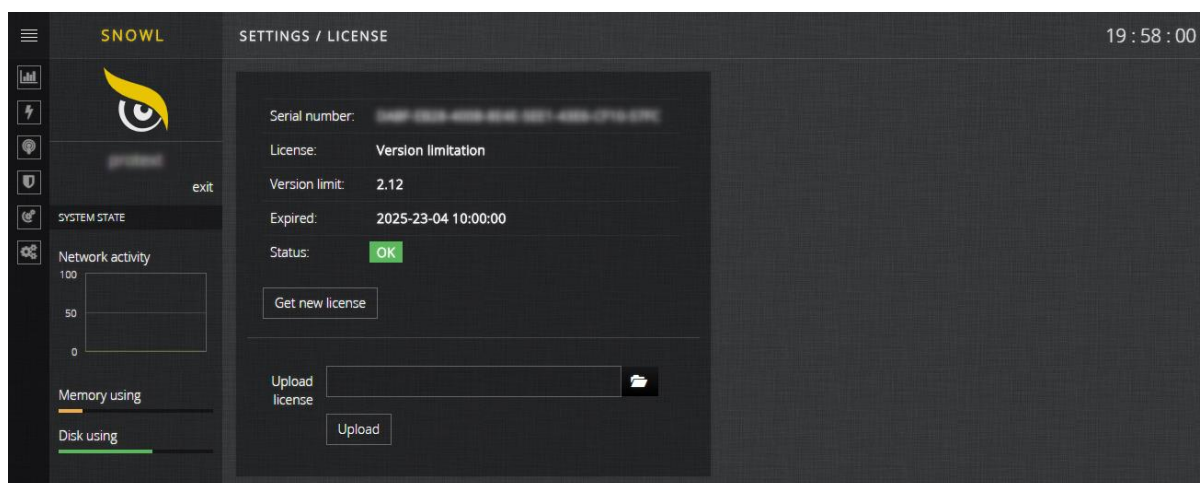
4.6.6. Getting New License

To get a new license, follow these steps:


1. Click **SETTINGS** in the main menu and **License** in the secondary menu:



The **SETTINGS / LICENSE** page opens:



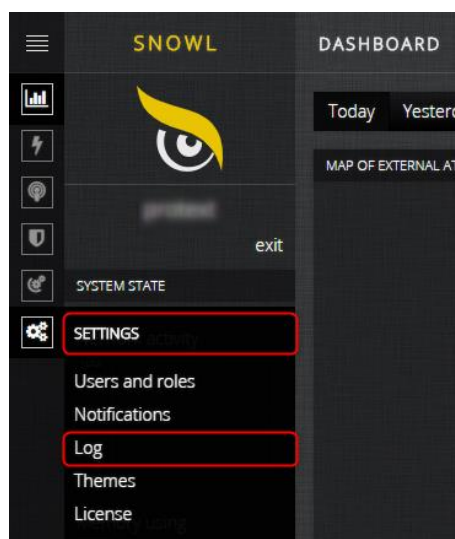
Click **Get new license** to purchase a license.

2. In the **Upload license** field, click  to select the purchased license file, then click **Upload**.
3. The new license is applied.

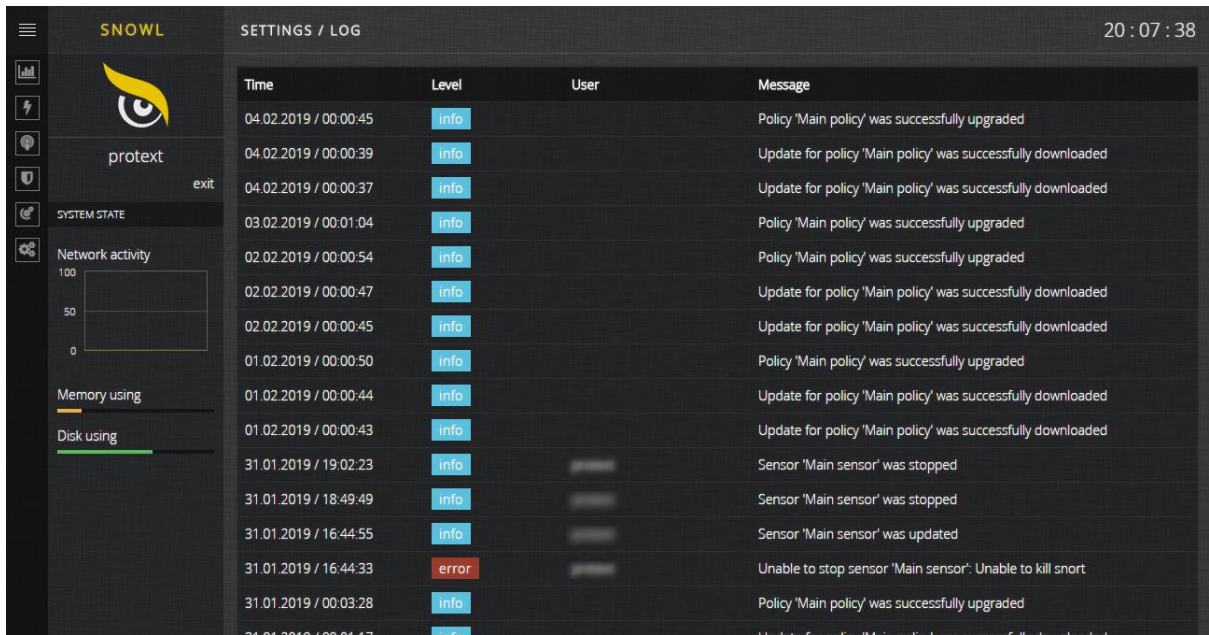
4.7. Auxiliary Functions

4.7.1. Viewing System Log

To view system log, click **SETTINGS** in the main menu and **Log** in the secondary menu:



The **SETTINGS / LOG** page opens:



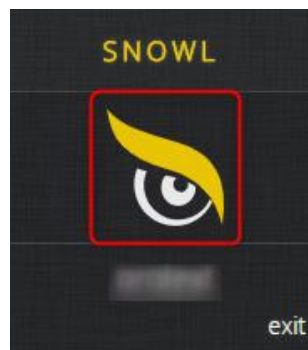
Time	Level	User	Message
04.02.2019 / 00:00:45	info		Policy 'Main policy' was successfully upgraded
04.02.2019 / 00:00:39	info		Update for policy 'Main policy' was successfully downloaded
04.02.2019 / 00:00:37	info		Update for policy 'Main policy' was successfully downloaded
03.02.2019 / 00:01:04	info		Policy 'Main policy' was successfully upgraded
02.02.2019 / 00:00:54	info		Policy 'Main policy' was successfully upgraded
02.02.2019 / 00:00:47	info		Update for policy 'Main policy' was successfully downloaded
02.02.2019 / 00:00:45	info		Update for policy 'Main policy' was successfully downloaded
01.02.2019 / 00:00:50	info		Policy 'Main policy' was successfully upgraded
01.02.2019 / 00:00:44	info		Update for policy 'Main policy' was successfully downloaded
01.02.2019 / 00:00:43	info		Update for policy 'Main policy' was successfully downloaded
31.01.2019 / 19:02:23	info		Sensor 'Main sensor' was stopped
31.01.2019 / 18:49:49	info		Sensor 'Main sensor' was stopped
31.01.2019 / 16:44:55	info		Sensor 'Main sensor' was updated
31.01.2019 / 16:44:33	error		Unable to stop sensor 'Main sensor': Unable to kill snort
31.01.2019 / 00:03:28	info		Policy 'Main policy' was successfully upgraded
31.01.2019 / 00:01:47	info		Update for policy 'Main policy' was successfully downloaded

4.7.2. Viewing System Documentation

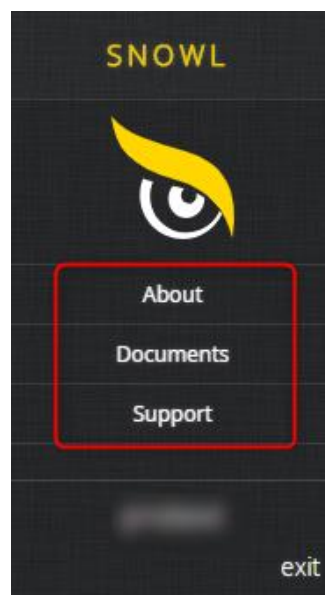
To view system documentation, follow these steps:

Click the owl's eye:

1.

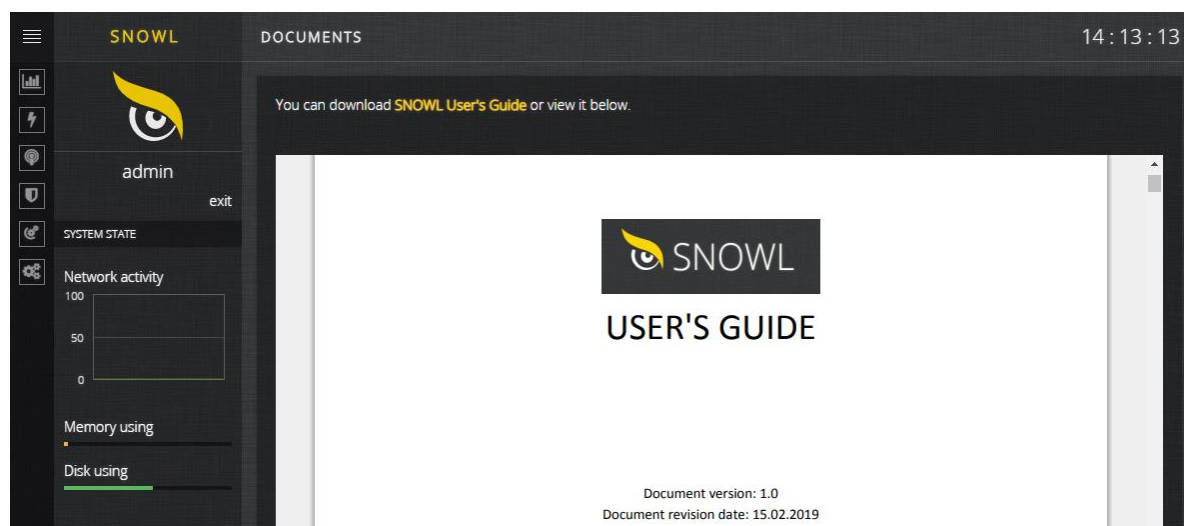


The additional menu opens:



In the additional menu, click **Documents**. The **DOCUMENTS** page opens:

2.



Select the required document.

You can either read the document in web browser or download it on your local computer.

3.