



SOC Workflow for ELK Community Edition Guide

v.3.7.4

2020

© 2020 SOC Prime Inc.

All rights reserved. This product and documentation related are protected by copyright and distributed under licenses restricting their use, copying, distribution, and decompilation. No part of this product or documentation related may be reproduced in any form or by any means without the prior written authorization of SOC Prime. While every precaution has been taken in the preparation of this book, SOC Prime assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

Contents

SOC Workflow overview	4
SOC Workflow Installation	5
Creating new Alerts in SOC Workflow App	8
Test alerts in SOC Workflow App	8
Alerts enrichment with the Playbooks	9
Interface overview	10
Navigation Panel	10
Cases	10
Cases by Stage	10
Cases by Priority	11
Cases by SLA	11
Cases Timeline	11
Cases Flow	12
Alerts	13
Alerts by Stage	13
Alerts by Priority	13
Alerts by SLA	13
Alerts Timeline	13
Alert Flow	14
Events	14
Playbooks	15
Incidents Investigation	16
Case creation	16
Case Info	19
Actions with the Case	20
How to Update	22

SOC Workflow overview

SOC Workflow App helps Security Analysts and Threat Hunters explore suspicious events, look into raw events arriving at Elastic stack and view Saved Searches saved by teammates. Carry out investigations based on automatically generated alerts from SIEM, EDR, IDS arriving at Elastic stack, Elastic Machine Learning alerts and Threat Intelligence data enrichments from Anomali ThreatStream & MISP.



SOC Workflow Installation

To install SOC Workflow for your Kibana:

- 1) **Copy the file `soc_workflow-xxxxx.zip` to Kibana server and run the command:**

```
/usr/share/kibana/bin/./kibana-plugin install file:///PATH_TO_FILE/soc_workflow-xxxxx.zip
```

Wait until the installation finishes, it may take a few minutes to optimize and cache browser bundles.

If you get an error: "Plugin installation was unsuccessful due to error "Incorrect Kibana version in plugin [soc_workflow]. Expected [6.6.0]; found [6.6.1]", please open zip archive and modify file `./kibana/soc_workflow/package.json`: put version of your Kibana to field "version".

- 2) **Restart Kibana** to apply the changes.

In case after restart Kibana you don't see any changes, go to `/usr/share/kibana/optimize`. Delete all files in the folder 'optimize' including subfolders and restart Kibana. This will make Kibana refresh its cache.

- 3) SOC Workflow Application is using indices:
 - "alerts_ecs*" - for events that need to be investigated by SOC. That could be correlation events generated by logstash or scripts;
 - "alerts_logs*" - for workflow stages and comments history;
 - "case_ecs*" - is used to store cases;
 - "case_logs*" - for case stages and comments history;
 - "soc_app_users" - for the custom list of users in case you are using non-local users.
 - "playbook" - for playbooks.

Create index templates for these indices from files:

- `index_template_alerts_case_logs.txt`
- `index_template_ecs_new.txt`
- `Index_template_playbook.txt`
- `Index_template_sigma_doc.txt`
- `playbooks_to_elastic.txt`

- 4) **Configure users.** If you are using local users, created in Kibana you can skip this point. If you are using a non-local user (like Active Directory) you need to configure the application to take users from custom index since AD users are not stored in Elastic indices. Edit file



`/usr/share/kibana/plugins/soc_workflow/config/user_source.json`, set index `"soc_app_users"` to `"user_source"` field.

Modify file `user_source.json`:

```
{
  "_example_of_user_source": "security OR soc_app_users",
  "user_source": "soc_app_users"
}
```

Create a separate index for users that will be used in application run command:

```
POST soc_app_users/doc
{
  "user_name": "shortusername",
  "user_type": "usertype",
  "user_email": "useremail@company.com",
  "user_full_name": "Full Name"
}
```

Field `"user_full_name"` will be displayed in the application.

5) Load SIGMA documents to the index `"sigma_doc"`. To fill sigma docs to index enter the folder `resources/ELK_import_export`. Modify the script `es_config.py`, put there Elasticsearch hostname, user and password. Run command:

```
python /PATH_TO_FILE/ELK_import_export/import_es_index.py
```

Indices will be created and filled with Sigma rules.

You should have the elasticsearch module, for python 2.7 install it using the command:

```
pip install elasticsearch
```

6) **Add playbooks to the index** from the application or add your own ones in the same format. Run commands in Dev Tools Kibana console from the file `playbooks_to_elastic.txt`.
Playbook format:

```
"@timestamp": "1530687175111",
"playbook_name" : "Playbook",
"playbook_body" : "PUT HERE TEXT OF YOUR PLAYBOOK IN HTML CONVERTED TO BASE64"
```

7) **Configure external commands** to run scripts/commands and make lookups to the 3rd parties services.

Edit file `/usr/share/kibana/plugins/soc_workflow/config/data_actions.json`

```
{
  "Menu": [{
    "Submenu": [{
      "name": "Command 1",
      "command": "/bin/sh /opt/scripts/script1.sh \"[[value]]\""
    }]
  },
  {
    "name": "Command 2",
    "command": "/usr/bin/python2.7 /opt/scripts/scripts2.py -v \"[[value]]\""
  },
  {
    "name": "Lookup: Google",
    "link": "https://www.google.com/search?q=[[value]]"
  }
]
```

Where:

- “name” is the display name of the command;
- “command” is the command line command to execute;
- [[value]] is the field value from the alert/case that is sent to the command;
- “link” is the link for drill-down. Put [[value]] to the appropriate place in the link to send field value from the alert/case.

All scripts and commands are run from the kibana user. Make sure that all scripts and folders have appropriate owner and rights.

Put the full path to the tools, for example for python put “/usr/bin/python2.7” path.

The output of the script/command is displayed in web console and saved to workflow logs.

Make sure that your script/command gives readable and short output for further investigation in SOC App.

8) **Copy predefined scripts for data enrichment and response** from folder “scripts_app” to Kibana `/opt/scripts`. And run commands:

```
chown -R kibana:kibana /opt/scripts
chmod +x /opt/scripts/*.sh
```

- 9) Now you can use the SOC Workflow plugin.

Creating new Alerts in SOC Workflow App

There are several ways to create an alert in SOC Workflow App:

- 1) Configure Logstash output for specific events, or newly created events (call correlated events), to put them in the index alerts_ecs*. You can use any of correlated scenarios from the SOC Prime Threat Detection Marketplace (TDM) <https://tdm.socprime.com/>. Please contact sales@socprime.com to get an appropriate subscription level to TDM.
- 2) Create watcher and configure output to index alerts_ecs*. In case if watcher triggers appropriate alert it will be created in SOC Workflow App. Please refer to TDM to get watchers with output to index.
- 3) You can create an alert manually by creating a document in index alerts_ecs*. Or by using any custom script.

Test alerts in SOC Workflow App

You can manually create test alerts in the SOC Workflow App.

Navigate to Kibana → Dev Tools → Console and create a test event. The minimum required parameters are:

For SOC Workflow App v.1.8.3

```
POST alerts_ecs-2019.01.31/doc
{
  "message": "<alert message>",
  "tags": [
    "<tag1>"
  ],
  "@timestamp": "2019-01-31T03:49:56.143Z",
  "event.severity": "7",
  "event.labels": "Queued"
}
```




For SOC Workflow App v.2 and higher:

```
POST alerts_ecs-2019.03/doc
{
  "message": "<message>",
  "tags": [
    "correlated"
  ],
  "@timestamp": "2019-03-26T03:49:56.143Z",
  "event": {
    "severity": "7",
    "labels": "Queued"
  }
}
```

The following information will be displayed in the Alert info:

- Priority - the min value is 1, the max value is 10;
- Message - the alert message;
- Tags;
- Logstash @timestamp,
- Logstash @timestamp UTC.

Alerts enrichment with the Playbooks

To enrich an alert with the Playbook edit the file:

kibana/plugins/soc_workflow/config/playbook_alert_links.json

Set the value of an alert message:

```
{
  "<playbook name>": [
    "<alert message 1>"
    "<alert message 2>"
  ]
}
```

Where the playbook name is the name of playbook;

Alert message 1, alert message 2 - alert names in the index alert-ecs.

After that, each generated alert will have an additional link to the playbook, which will help to see the process of investigation for operators.



Interface overview

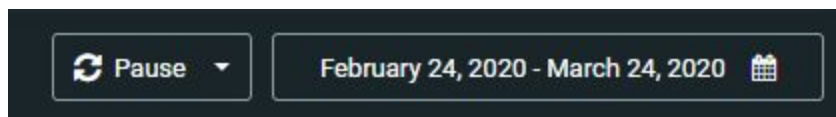
SOC Workflow App helps Security Analysts and Threat Hunters explore suspicious events, look into raw events arriving at Elastic stack and view Saved Searches saved by teammates. Carry out investigations based on automatically generated alerts from SIEM, EDR, IDS arriving at Elastic stack, Elastic Machine Learning alerts and Threat Intelligence data enrichments from Anomali ThreatStream & MISP.

Navigation Panel

The Navigation panel consists of the menu buttons to switch between Cases, Alerts, and Events, Playbooks drop-down menu, the button to switch between the Dark and Light theme, and SOC Prime logo.



Under the Navigation panel, there is the Screen update interval drop-down menu and the Calendar.



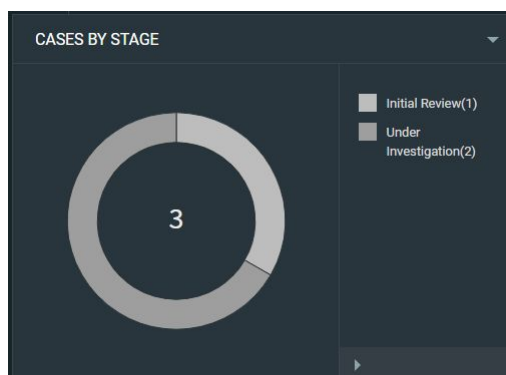
Click the drop-down menu to select the screen update interval - 5 sec, 10 sec, 30 sec, 60 sec, or pause the update.

Click the Calendar to select the time range for information to display - today, yesterday, last 30 days, this month, last month, or select the custom range. Click Apply to save the changes, click Cancel to discard.

Cases

Click the Cases button on the Navigation panel to move to the Cases page. It consists of dashlets with diagrams, Cases Timeline dashlets, and Case Flow list.

Cases by Stage



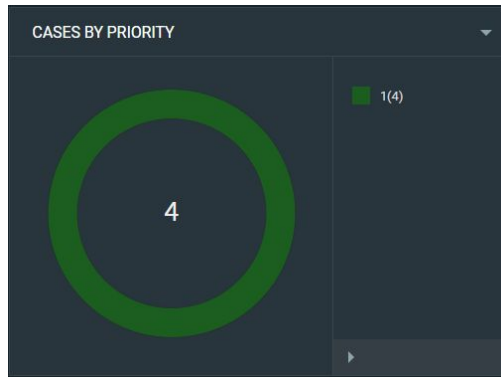
The **Cases by Stage** diagram dashlet displays the total number of cases for the selected period and their workflow stages. Put the pointer over the diagram section to see the percentage and the number of cases of the selected stage.

Click **Legend** to view the detailed information about the number of cases on each stage. Click the stage name to remove it from the diagram, it will not be displayed on the dashlet and its percentage will not be calculated.

Note:

The option of **adding and editing Stages** is not available for Free version users.

Cases by Priority



The **Cases by Priority** diagram dashlet displays the total number of cases for the selected period and their priority level. Put the pointer over the diagram section to see the percentage and the number of cases of the selected priority level.

Click **Legend** to view the detailed information about the number of cases on each priority level. Click the priority level name to remove it from the diagram, it will not be displayed on the dashlet and its percentage will not be calculated.

Cases by SLA



The **Cases by SLA** diagram dashlet displays the total number of cases for the selected period and their SLA (low < 10 min, medium 10-15 min, high >10 min). Put the pointer over the diagram section to see the percentage and the number of cases of the selected SLA.

Click **Legend** to view the detailed information about the number of cases. Click the SLA name to remove it from the diagram, it will not be displayed on the dashlet and its percentage will not be calculated.

Cases Timeline

The Cases Timeline Dashlet displays the daily number of cases and their stages for the selected time range.



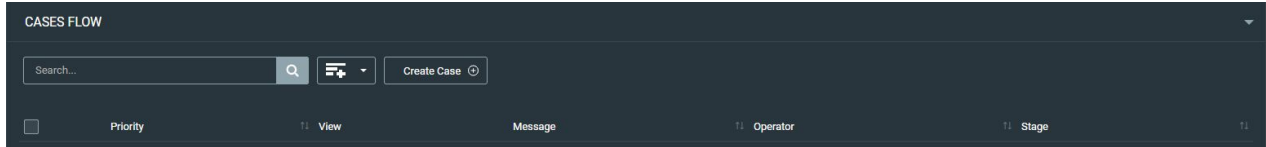
Cases Flow

The Cases Flow List displays the created cases sorted by time of creation.



The following Case information is displayed: case priority, view case button, message, SOC operator, case stage:

Click the Add field button to add additional fields to be displayed. Select the fields from the drop-down menu.



To create a new Case, click the Create Case button.

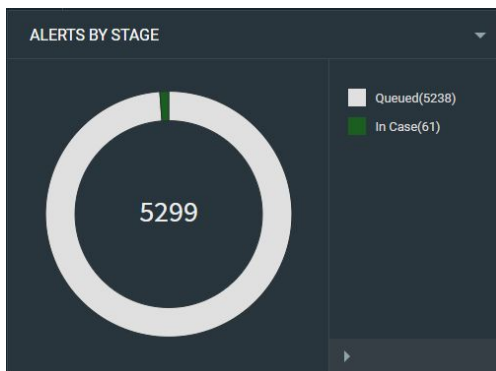
To sort the cases, click the ↕ icon.

Use Search to find the case you are interested in, the list of cases containing your search query will be displayed.

To select all cases displayed on the page, mark the Select All checkbox. To select one case, mark the checkbox in the case line.

Alerts

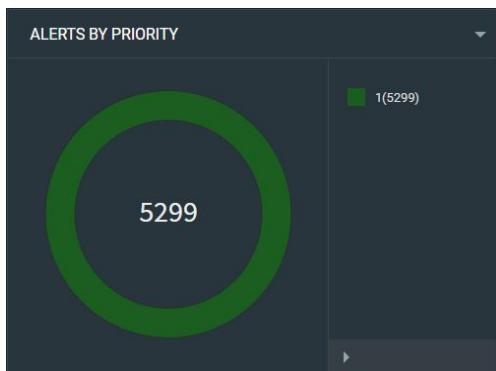
Alerts by Stage



The **Alerts by Stage** diagram dashlet displays the total number of alerts for the selected period and their workflow stages. Put the pointer over the diagram section to see the percentage and the number of alerts of the selected stage.

Click Legend to view the detailed information about the number of alerts on each stage. Click the stage name to remove it from the diagram, it will not be displayed on the dashlet and its percentage will not be calculated.

Alerts by Priority



The **Alerts by Priority** diagram dashlet displays the total number of alerts for the selected period and their priority level. Put the pointer over the diagram section to see the percentage and the number of alerts of the selected priority level.

Click **Legend** to view the detailed information about the number of alerts on each priority level. Click the priority level name to remove it from the diagram, it will not be displayed on the dashlet and its percentage will not be calculated.



Alerts by SLA

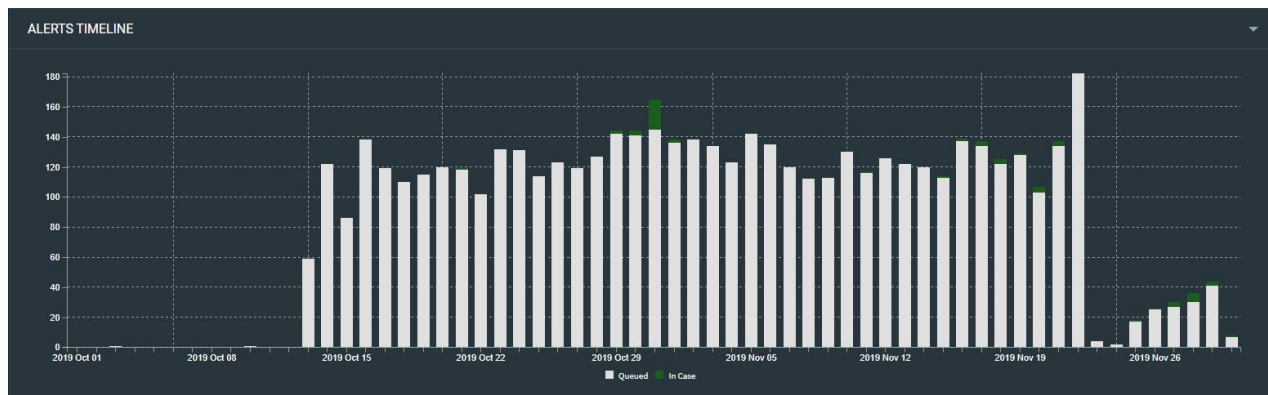


The **Alerts by SLA** diagram dashlet displays the total number of alerts for the selected period and their SLA (low < 10 min, medium 10-15 min, high >10 min). Put the pointer over the diagram section to see the percentage and the number of alerts of the selected SLA.

Click **Legend** to view the detailed information about the number of alerts. Click the SLA name to remove it from the diagram, it will not be displayed on the dashlet and its percentage will not be calculated.

Alerts Timeline

The Alerts Timeline dashlet displays the daily number of alerts and their stages for the selected time range.

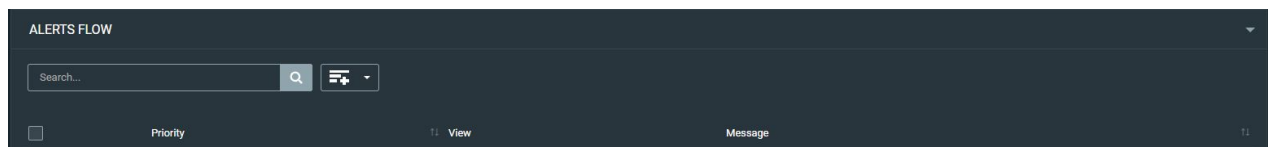


Alert Flow

The Alert Flow list displays the triggered alerts. By default, the list is sorted by time of creation.

The following Alert information is displayed: alert priority, view, message.


Click the Add field button to add additional fields to be displayed. Select the fields from the drop-down menu.



To sort the alerts, click the  icon.

Use Search to find the alert you are interested in, the list of alerts containing your search query will be displayed.



To select all alerts displayed on the page, mark the Select All checkbox. To select one alert, mark the checkbox in the alert line. Click the  icon to create a case or add the alert(s) to the existing case.

Events

Select a saved search from the drop-down list and specify the search time range to view the events information on your query. Click Select to perform the search. Enter your query to look for events containing your search query.

Note:

The option **Share Link** using a saved search link generated in the Kibana Discover from documents is not available for Free version users.

Playbooks

Click the Playbooks drop-down list to view available playbooks.

Start input the name of the playbook you are interested in and the list of playbooks containing your search query will be displayed.

Click the playbook name to open it.

Note:

The option of **editing, removing and adding Playbooks** is not available for Free version users.

Incidents Investigation

The investigation proceeds using SOC Workflow Application is embedded in Kibana WEB UI as a separate menu item. SOC Workflow App contains a set of tools to organize incidents workflow and a dashboard with analytics required to organize and measure work with information security incidents.

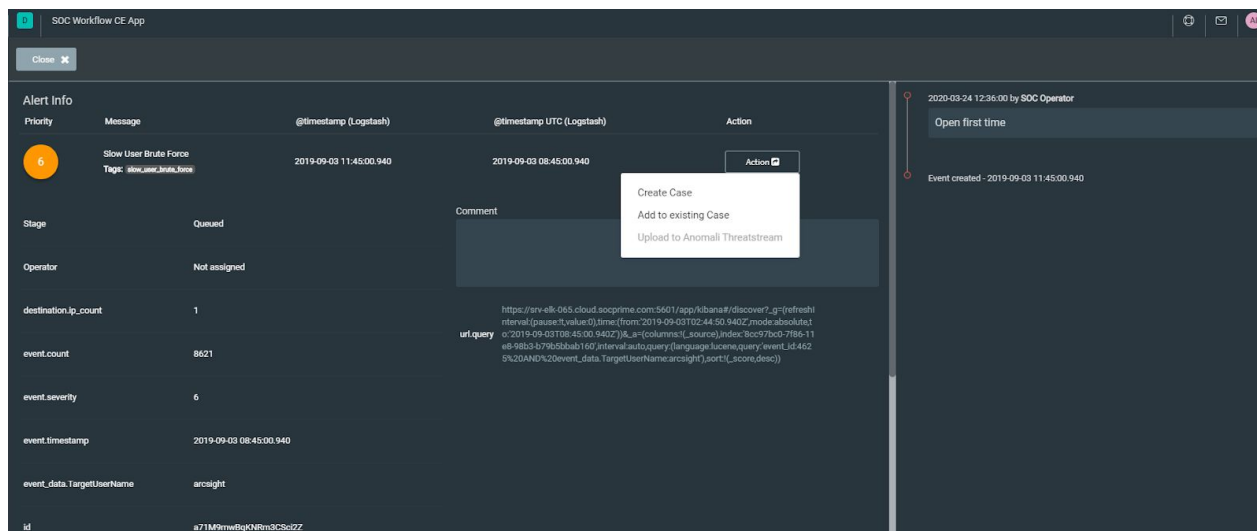
There are a number of common steps that are usually followed to handle the cybersecurity incidents effectively and make a basis for investigation approach. Following a cybersecurity incident, it is important to update the incident investigation/response approaches and related documents as an incident lesson learning activity.

General incident Workflow:

- 1) Alert is fixed in the monitoring system.
- 2) The case is created based on alert information.
- 3) Changing of case status or/and priority.
- 4) Closing the case.

Case creation

To create a Case, first, review the Alert by double-clicking on the Alert. After reviewing and defining the complexity of the alert, click the Action button and select Create case.



The screenshot displays the SOC Workflow CE App interface. On the left, an 'Alert Info' panel shows details for a 'Slow User Brute Force' alert. The alert has a priority of 6, a message 'Slow User Brute Force', and tags 'slow_user_brute_force'. It was received at 2019-09-03 11:45:00.940. The alert is in the 'Queued' stage, with no operator assigned. The 'event_count' is 8621, 'event_severity' is 6, and 'event_timestamp' is 2019-09-03 08:45:00.940. The 'event_data.TargetUsername' is 'arcsight'. The 'id' is 'a71M9mwBgKNRm3CS0Z7'.

On the right, a timeline shows the alert was created on 2019-09-03 11:45:00.940. A modal window is open over the 'Action' button, offering three options: 'Create Case', 'Add to existing Case', and 'Upload to Anomali Threatstream'.

The 'url.query' parameter is visible in the 'event_data' section, containing a complex Kibana discovery query for the 'arcsight' source.



CREATE CASE [X]

Case name:
Slow User Brute Force

Priority:
6

Operator:
[]

Stage:
[]

Comment:
Comment

Source IP:
Source IP

Destination IP:
Destination IP

Device product:
Device product

Playbooks:
[]

Events Id:
a71M9mwBqKNRm3CSc2Z

event count:
8621

Select Additional fields:
[]

[Cancel] [Save]

- ← Select Case Priority level
- ← Select the SOC Operator.
- ← Select Stage: Initial Review, Under Investigation, Closed.
- ← Fill in the comment field.
- ← Select additional fields if needed.
- ← Click the Save button.

Note:

The number of **Stages** is **strongly limited** in the SOC Workflow Free version.

In case several alerts require similar reaction, SOC operator can:

ALERTS FLOW

Search... [Q] [Filter]

Priority	View	Message
<input checked="" type="checkbox"/> 6	Alert	Slow User Brute Force
<input checked="" type="checkbox"/> 6	Alert	Regular Slow User Brute Force (Last 7 Days)
<input type="checkbox"/> 6	Alert	Slow User Brute Force
<input type="checkbox"/> 6	Alert	Slow User Brute Force

- 1) Tick checkboxes on the left of the alerts' names.
- 2) Click the [Menu] button to proceed with the cases.
- 3) Take actions with all selected incidents as one action.

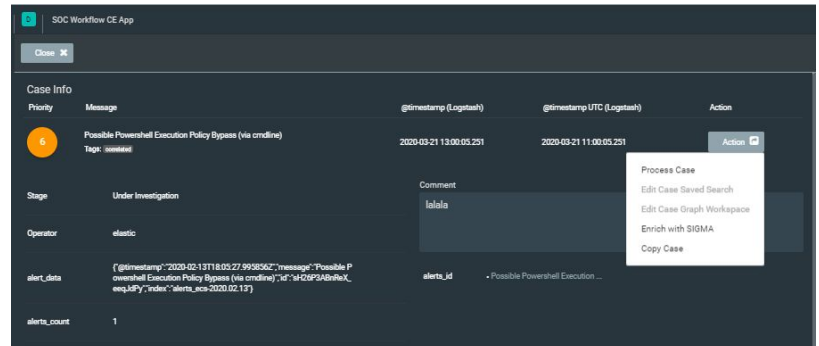


During the investigation, SOC operator logs operations in comments and changes the state of the Incident Case from Initial Review stage to the Close stage or Under investigation stage if he needs more time to investigate the incident.

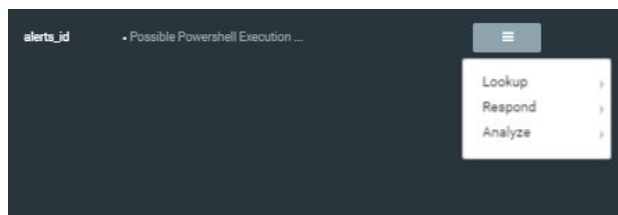
Case Info

Double click the case to open it and view the details, add information or process the case. The following information and actions are available:

- Case priority,
- Case message with tags,
- @timestamp (Logstash),
- @timestamp UTC (Logstash),
- Stage,
- Operator,
- device.vendor,
- ecs_version,
- event.organization_id,
- event.severity,
- event.type,
- Id,
- index,
- @version,
- message,
- source.hostname,
- tags,
- Comment,
- alerts.id.



Put the pointer over the field to see the additional actions menu:



Enrichment: Enrichment examples;

Lookup: pre-configured lookup, e.g. CyberChef, Google;

Analyze: Virus Total, URLSCAN.IO, Anomali Threatstream, Detonate File. Detonate URL.

Note:

The additional actions menu is not available for the following fields: Case priority, Case message with tags, @timestamp (Logstash), @timestamp UTC (Logstash), and Comment.

Note:

The number of additional actions is **strongly limited** in the SOC Workflow Free version.

Actions with the Case

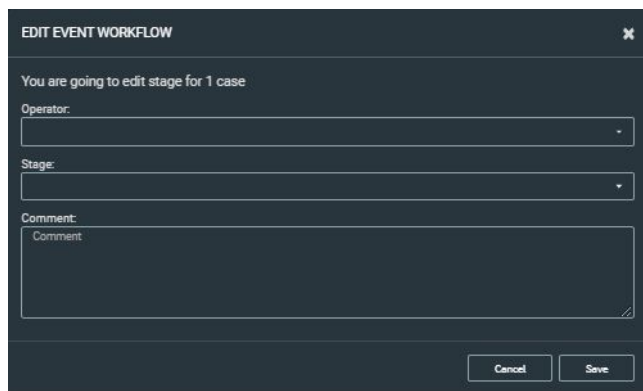


- 1) Click the Action button.
- 2) Select Process Case.

Note:

The options of adding and editing **Case Saved Search** and **Case Graph Workspace** are not available for Free version users.

Process Case:

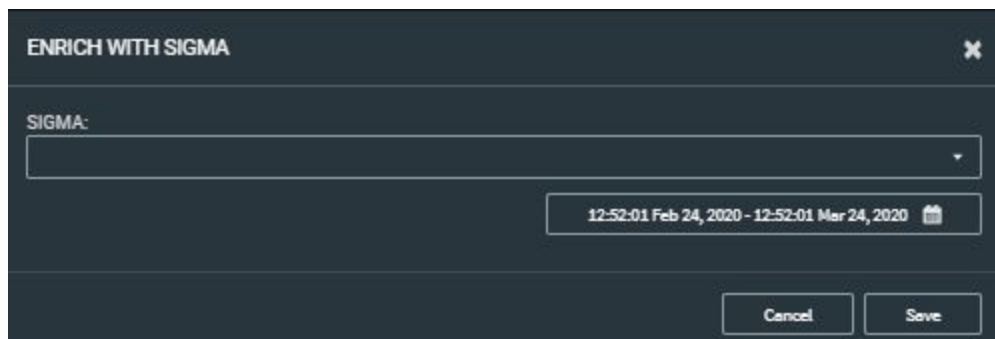


- 1) Select the SOC Operator.
- 2) Select the stage for the selected incident.
- 3) Provide a comment which can explain the chosen stage.
- 4) Click the Save button.

Note:

The options of adding and editing **SOC Operators** and **Stages** are not available for Free version users.

Enrich the Case with SIGMA:



- 1) Click the Action button.
- 2) Select the needed time range using the calendar.
- 3) Select SIGMA from the drop-down list.
- 4) Click the Save button.
- 5) View the User Action information in the pop-up window.

Now your Case is enriched with SIGMA and the User Action log is displayed on the Activity Feed panel.

Note:

The number of user Action Logs is limited for Free version users. Only **five** action logs are displayed on the Activity Feed panel.

Copy Case:

To create a new Case with similar information, click Action → Copy Case. In the pop-up window, remove or edit the fields by selecting relevant information from the drop-down menus.

How to Update

1. Backup all config files in folder /usr/share/kibana/plugins/soc_workflow/config/.
2. Remove folder /usr/share/kibana/plugins/soc_workflow/.
3. Install application from new version archive.
4. Remove Kibana cache - all files and subfolders in folder /usr/share/kibana/optimize/. Do not delete the folder "optimize".
5. Update or add new templates for data if needed.
6. Copy back upped configuration files to folder /usr/share/kibana/plugins/soc_workflow/config/.
7. Restart Kibana. Restarting Kibana may take a while since rebuilding the cache.

If you have SOC Workflow App version older than 1.5.7 please contact dev@socprime.com