Micro Focus Security ArcSight SOAR

Software Version: 3.0.0

ArcSight SOAR User's Guide

Document Release Date: December 2020
Software Release Date: December 2020

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About ArcSight SOAR

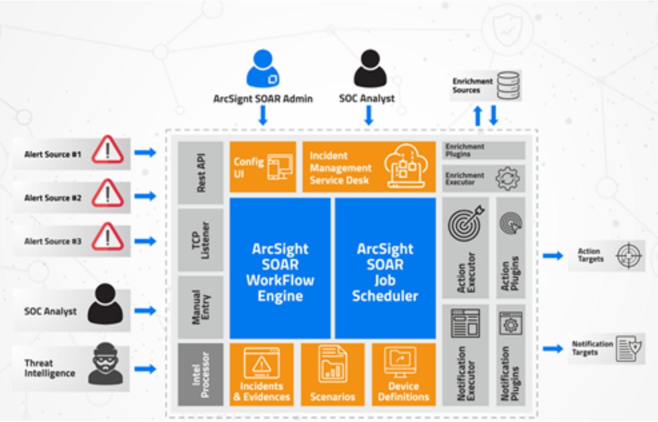
ArcSight SOAR is a leading Security Orchestration, Automation and Response Platform (SOAR) which combines orchestration of both technology and people, automation and incident management into a seamless experience. ArcSight SOAR helps security teams improve their efficiency in responding to cyberattacks in security operations.

- **Attack speed**: Attacks keep getting faster every day. Modern attacks are almost entirely automated.
- **Attack volume**: An average organization would get more than 300 cyber alerts per day (IDC). Investigating and responding to an alert would take around 8 full hours.
- **Disparate tools**: SOC analysts use 15, up to 20 different tools throughout their daily jobs to investigate and respond to attack alerts. Tier-1 analysts are not able to investigate (and use the tools) and they are merely expensive human filters.
- **No single pane of glass**: There is no trail of investigation and response activities and there isn’t a proper answer to “who is working on which case and doing what” at any point in time on the SOC floor.
- **Lack of KPIs and metrics**: As most SOCs lack the practice of investigation and response, it is almost impossible to come up with relevant, easy-to-collect KPIs and metrics. Getting a grip on who needs more training, SLA adherence, incident backlog trends, etc. is difficult and intuitive-only.
- **Cyber Security Skill Shortage**: Currently, the cybersecurity sector is facing a severe expert shortage. As the market sits now, there are 350,000 vacant positions in the U.S. alone and the industry shortfall will rise to a stunning 3.5 million cyber expert vacancies.

ArcSight SOAR helps CSOC teams improve their efficiency in responding to cyber-attacks using various and diverse forms of automation. ArcSight SOAR also helps SOC managers better govern their business by providing insight and accountability to SOC processes.

How SOAR Works

Following figure shows the general working mechanism of SOAR:



SOAR’s process starts after the alert sources are configured. The following paragraphs describe how it works.

Receiving Alerts

After the alert sources are created and configured, SOAR starts to listen to the configured ports and get alert messages from these sources. These alert messages are usually brief; they include useful information such as the type of alert, time of event, count of base events that produced the alert, and the severity of the alert. Context of the alert messages depends on the alert source’s type and its rules configured on its own administration interface.

Getting Base Events

After an alert is received and if auto-enrichment is available and enabled for its source type, SOAR requests more details from the alert source. Getting base events can be controlled under Parameters tab of Configuration menu, e.g., ArcSightAutoEnrichEnabled), SOAR requests more details from the alert source. Enrichment basically means getting more details for an alert.

When an alert is created, the alert source (SIEM) usually keeps various base events that produced that alert. For example, if a “**Remote Port Scan Detected**” alert is created, the SIEM would have a number of events each of which is a separate log entry received by the alert source, from systems under attack or probe. SOAR gets these base events since they contain useful information (time of each event, attacker username, attacker remote address, , etc.). These information are displayed on the incident’s page in SOAR, which is created and bound to that alert. In addition to displaying, various data is automatically added to incident’s scope. Please see the "Incident Management Service Desk" on page 40for more information.

Creating and Dispatching Incidents

Using the data from the alert (not the base events), SOAR creates an incident and links it to the alert. Incident’s severity is set to a value using the severity mappings of the alert’s source. For example, if the alert has a severity of Medium, SOAR looks for the mappings and may decide to set the incident’s severity to “**Urgent**”.

As soon as the incident is created, it needs to be assigned to a user or user group. For this, SOAR executes the playbooks called “**incident dispatch playbooks**”. If these playbooks cannot find an assignee, SOAR leaves the incident as unassigned. More than one dispatch playbooks may find an assignee, but SOAR only executes the first one matching.

Dispatch playbooks might change incident’s severity, add watchers or labels. Please see the Dispatch section for more information.

Executing Playbook

After the incident is created and dispatched, SOAR starts to execute the playbooks defined in the system.

Each playbook has a number of conditions to match the alert received. All matching playbooks are executed sequentially and in their rank order. Higher rank playbooks are executed earlier. Please see the "Managing Playbooks" on page 24 Chapter for details.

Each executed playbook can run a number of enrichment operations and queue actions in an arbitrary order.

Enrichments are synchronous; playbook execution waits for their completion before continuing with the next operation.

Actions are always asynchronous. There’s a separate queue of actions, manageable in the SOAR’s administration interface (Action and Rollback Queue tab of the Status menu). Completed actions are moved from the queue to the Alerts tab of Status menu. A completed action can be either automatically or manually rolled back, if the action’s capability supports rollback operation. Please see the sections explaining playbook creation under "Managing Playbooks" on page 24 Chapter.

Note that, not all action capabilities support rollback.

After all playbooks are executed, SOAR tries to keep the alert’s incident open except the following conditions:

- If an executed playbook’s “Incident auto-close mode” is specified as “Close if there are no actions for approval” (please see the "Managing Playbooks" on page 24 Chapter). SOAR makes sure that all actions created by the playbook are not targeting any integration with approval users set. If this condition matches, the incident is closed, otherwise no status changes are made.
- If an executed playbook’s “Incident auto-close mode” is specified as “Close if actions created”: The incident will be closed if the playbook created any actions.
- If an executed playbook’s source code contains a call to SOAR.closeTicket() : In this case, the incident is closed no matter the other exceptions are. This has the highest precedence.

User Interface

ArcSight SOAR user interface consists of the following menu items:

- Dashboard: It shows a summary of information about the incident status, recent incidents, incident distribution among the assignees, number of alerts, your integrations and alert sources, etc. This is the first page that is shown whenever you login to SOAR user interface. You can refer to the "Dashboard and Reports" on page 46 chapter for its usage details and full list of data sources.
- Incidents: It allows you to manage your incidents. You can see the list of incidents and their descriptions, require enrichments and perform actions on the incidents and more. Please refer to the "Incident Management Service Desk" on page 40 for more information.
- Playbooks: It allows you to create, delete, edit, enable/disable playbooks. A playbook includes conditions, actions and notifications. When the created alert in SOAR meets the defined conditions, the playbook starts to execute on the alert’s incident and perform the actions and/or send the notifications as defined in the playbook. Please refer to the "Managing Playbooks" on page 24 chapter for more information.
- Status: It allows you to see the action and rollback queues, alerts, actions, message queues, and logs generated by your configured system. Please refer to the "System Status" on page 21 chapter for more information.
- Reports: It allows you to create reports about incidents and analysts.
- Configuration: This menu contains all the configuration elements required by your

SOAR to work properly. You will use it to create and edit integrations, alert sources, users, credentials and more. Please refer to the "Integrations" on page 9 chapter for more information.

There is a notification icon (a bell picture) on top right part of the screen. It gives information about the incident notifications. There is also a Capital Letter or avatar and a username next to it. When you click it, it informs you about the user who logged in.

Preferences screen has an additional field for selecting themes and layouts. You can select any theme from the list. **Dark** is the default theme. You can select any layout in which you want to work for. Default is Tier 1 layout.

In a typical list screen (displayed below) there are four common sections which always reside in every list screen.

In the upper right part of the screen, there is a search box. You can enter the desired word(s) for selecting the desired lines and reducing the length of the list.

Next to it, there is a column selection section. You can select the columns you want to display or not.

In the lower left part of the screen, there is a list of number of items that will be displayed at one page. You can change the number of items by selecting from the list. The numbers vary according to the type of the list.

In the lower right part of the screen, there is a pagination section. If the list consists of more than one page, you can go to the desired page by page number or previous or next buttons.

Selection information are not stored, so when you log out, your choices will be reset.

Managing Configurations

To configure your alert sources and edit the rules, use the **Alert Sources** tab under the **Configuration** menu.

Configuring Alert Sources

On this tab you can see the list of alert source configurations defined previously along with their recent alert times. Here, you can create and edit your alert source configurations.

To create an alert source configuration, click on the “**Create Alert Source Configuration**” button.

You might see differences in the fields of this editor for some alert source types (as you select it from the Type combo box list).The following table describes all the possible fields.

Value	**Description**
Name	Name of the alert source
Type	Type of the alert source. It could be one of the alert source types listed above.
Address	IP address of the alert source to which SOAR connects when it wants to get data.
Key	A unique, auto-generated key which is used as a shared token to make sure the remote IP addresses (“Allowed IP addresses”) are correct. The value of this field should be included in the messages coming from those remote IP addresses. See the appendices for more information on configuring this key on different security managers and platforms.
Allowed IP addresses	Any alert coming from the IP addresses specified in this field will be processed and others will be discarded. For most alert source types SOAR opens a TCP port (or a web service API endpoint) and waits for some alert sources to connect. This field along with the “Key” field is to improve your system’s security. The combination of these two fields prevents a potential attacker from feeding your system with fake events and causing damages.
Alert Severity	Severity of alert sources. Define the severities according to the priorities of tickets produced by the alert source. Use the “Add” button to create each severity. While adding the severities, you can specify the default severity by selecting the checkbox under the “Default” column.

Configuration Content	This area shows default configuration definitions for some type of alert sources, such as IBM Security QRadar but it is not required for many alert sources. It depends on which alert source you are trying to interact with. If there are some required data for the alert source configuration, this area shows a template and ask you to edit it if needed. You can see alert source specific configurations in “Alert Guides”.
Credential	Credentials defined on the system to be used for the alert source.
Show alert parameters by default	Shows the default alert parameters defined for the selected device type on the system.
Trust Invalid SSL Certificates	Select if you want SOAR to connect anyways to an alert source ignoring warnings for untrusted SSL certificates. You may have installed alert sources with self-signed SSL certificates, which SOAR does not trust and deny connecting by default. Therefore, if you do not select this checkbox, SOAR still gets the brief alert, but cannot get more details on the alert.

You can edit the alert source configurations by clicking the **Edit** buttons in the list of configurations. To remove a configuration from the system, click the **Delete** button.

For detailed information see the related Integration Guides.

Configuring SOAR as Alert Source and Internal Alerts

ArcSight SOAR creates internal alerts for some cases, such as when an action is failed permanently or a integration becomes unavailable since its firewall is not reachable, etc.

These internal alerts are generated for the following event types: action and rollback failures, auto-enrichment failures, when an integration becomes offline/online, breach of ticket resolution/first response SLAs, and custom/arbitrary alerts created by playbooks.

Integrations

To create, manage and configure your security integrations and platforms, use the **Integrations** tab under the **Configuration** menu.

A list of integrations configured previously along with their action and rollback queue sizes, and their availability statuses are displayed in the Integrations page.

You can edit the integration attributes by clicking on the **Edit** buttons in the list of integrations. To remove an integration from the system, click the **Delete** button.

Creating Integration

To create and configure a integration click the **Create Integration** button. The following integration editor shows up:

Value	**Description**
Name	Name of the Integration.
Type	Type of the Integration.
Address	IP address of the integration.
Configuration	Depending on the integration type, you may select and enter various configuration commands on the black window. Please see the below Changing Integration Configuration section for details.
Credential	Credentials to be used to connect this integration. Credentials are defined in Credentials menu.
Trust Invalid SSL Certificates	Select if you want SOAR to connect anyways to an integration ignoring warnings for untrusted SSL certificates.
Require Approval From	When a user is selected here, action items need to be approved by this user before executing it for the integrations.
Notify	When a user is selected here, actions done will be notified to this items need to this user.
Tags	It is used to group integrations. This allows creating actions on a number of integrations having the same tag. You may want to create an action for all integrations that have a specified tag such as “block offender IP address on all firewalls that are used to manage WiFi networks”.

You may want to specify some more parameters for integrations of some types. In this case select the “**Show Additional Parameters**” checkbox located at the very bottom of the integration editor.

Here are the descriptions for these additional parameters:

Value	Description
Maintenance	Maintenance is supported by all integrations to which SOAR connects using the SSH protocol. It is essentially a generic SSH integration action script. It is best used in conjunction with Check Point Firewall integration for activating/installing a previously saved but not activated firewall policy. You can select a maintenance frequency or type your own cron job (for a scheduled maintenance) by selecting the “Custom Cron Value” option in the combobox.
Host Key	SSH public key of the remote integration; it is only used for integrations connected with SSH. If this field is not empty, provided SSH key will be validated using the key provided. This check is required to prevent man-in-the-middle attacks.
Batch Size	SOAR can send multiple action queue items to the integrations in a single connection. This field specifies the maximum number of action queue items that will be sent in each execution. For example, if you provided “Batch Size” as “10” and there are 25 action queue items waiting for that integrationd, SOAR will send these items in 3 separate execution (10 + 10 + 5). Its default value is 1. This is a feature to avoid causing excessive system load on the remote integrations when executing actions. A bigger batch size may create overhead on the integration thus failing all entries. So you need to be careful when increasing this value.
Max Postpone	Maximum number of action retries. If any action cannot be executed for any reason, such as connection failures, authentication problems or another SOAR internal problem, it will automatically be retried later. There are a number of global configuration parameters to configure how and when it will retry, but, after a number of retries specified in this field, SOAR will give up and mark the action as failed. Default value is 6 (in hours).
Connection Limit	Maximum number of concurrent connections for the integration. Default value is 5.
Max Action Retry	Maximum action retry count for the integration. Default value is 5
Max Rollback Retry	. Maximum rollback retry count for the integration. Default value is 5.

Changing Integration Configuration

Integration configurations are specific information about individual integrations. The following is an example integration configuration for an Active Directory integration:

Note: For the configuration details of each integration type, please refer to the Integration Guides.

Testing the Integration

As you notice, there is a **Test** button in the **integration** editor. When pressed, it immediately triggers the availability check for the integration and if anything fails, a detailed error message will be displayed. For example, in the case of a Check Point Firewall integration, SOAR needs a credential to work with the integration, if a proper credential is not available, you will see an error regarding this.

If the administrator of the remote integration accidentally deletes the credential that SOAR uses, SOAR will no longer be able to create actions on the integration. In this case, the integration will be shown as offline (and an internal alert will be created) and the error message will be logged into the error log. If you want to see the exact error message, you need to click on the **Test** button.

A successful test will mark the integration as online.

Flushing Queues

To Flush the Ques, select **Flush Queue** button under the **Actions** column of the integrations list. Following is the basic flow in SOAR:

1. Alert is received.

2. Matched playbooks run.

3. Action and rollback queue objects are created (waiting for execution in the queue).

4. Actions/rollbacks in the action/rollback queues are executed and saved.

If you click the **Flush Queue** button, SOAR will not wait for the execution scheduler (which consumes action/rollback queue objects) and executes these actions/rollbacks as soon as you click the button.

Integration Credentials

In order to manage the credentials to connect to integrations, use the **Credentials** tab under **Configuration** menu. After you click on this tab, the main page for the credential configurations, where you can create and edit the credentials is displayed. In this page, you can see the credential names and the last date and modifier of any modification performed on the credential information.

Creating Credentials

To create a credential set, click on the **Create Credential** button.

Select **Type** from the list (****Internal Credential** or **External Credential**). Internal credentials are stored in SOAR’s database table. External credentials are stored in integrations such as Cyberark Central Credential Provider. Enter a name for the credential set in the **Name** field (this name will be shown to select a credential while you are creating entities such as integrations and alert sources in SOAR). Provide the username, password and private key (if needed) in the related fields of the editor.

You can always edit the previously created credentials by clicking on the **Edit** buttons in the list of credentials. To remove a credential from the system, click on the **Delete** button, but you cannot remove the credentials used in the integrations.

User Roles

The user roles define the permissions granted for a user and each user on SOAR must have a role.

In order to manage the roles, use the **Roles** tab under **Configuration** menu.

In this page, you can see the name of the user role, permissions assigned to that role, and the last date and modifier of any modification performed on the user role information.

Creating Roles

To create a user role, click on the **Create User Role** button.

You must specify the user role attributes as follows:

Value	Description
Role Name	Name of the user role. Consider giving an explanatory name that hints about the permission level of the user, e.g., Full Administrator, Monitoring Operator, etc.

You can always edit the previously created user roles by clicking on the **Edit** buttons in the list of user roles. To remove a user role from the system, click on the **Delete** button.

User Groups

You can create user groups to make some operations easier. These operations may include assigning an incident, specifying watchers for an incident, or assigning operator tasks to these user groups so that each user in the group is involved in that operation.

In order to manage the user groups, use the **User Groups** tab under **Configuration** menu. If you click on this tab, the page to create and edit the is displayed.

In this page, you can see the name of the user group, its users, and the last date and modifier of any modification performed on the user group information.

Creating Groups

To create a user group, click on the **Create User Group** button.

You must specify the user attributes as follows:

Value	Description
Name	Name of the user group. Provide an explanatory name which gives a hint about what the user group is created for.
Users	Select the users to be included in this user group.
AvSOAR	You can select an avSOAR for the group by clicking on the “Choose File” button. Any image will work. It is recommended to select image files with sizes of 200 x 200 pixels.

You can always edit the previously created user roles by clicking on the **Edit** buttons in the list of user roles. To remove a user role from the system, click on the **Delete** button.

Access Control Lists

Access Control Lists (ACLs) are used to control the access of the users or user groups to ATAR objects. These objects include action capabilities, credentials, custom scripts, enrichment capabilities, enrichment plugins, integrations and integration types. You may want a specific group of users to access to some integrations for example. In these cases you need to edit the access controls managed under **Access Control Lists** tab.

When you click on the **Access Control Lists** tab under the **Configuration** menu, a welcome page is displayed.

In this list you can see the SOAR objects, users or user groups who can access those objects, and the last user and last modification date of an access control edit.

You can search for objects in this list using the **Search** text field located at top right corner of the list. The list will be updated as you type. The search term will be searched in the names of objects (first column of the list).

You can edit an access control by clicking on the **Edit** button under the **Actions** column; and the editor is displayed.

You can only edit the **Allow Access For** and **Users/Groups** fields. By default, SOAR has created the object list with the **Anyone** option. If you want to narrow down the users for an object, just edit the related object and specify the users or groups for the option you selected in the **Allow Access For** field, which can be **Only selected users/groups** or **Anyone except selected users/groups**.

After editing an **Access Control List** item, **Clear** button appears in the **Actions** column of that item. You can not remove an **Access Control List** item from the list. By clicking on the **Clear** button under the **Actions** column, you can reset value of the **Access** column.

Lists

Lists are used as lookup tables in SOAR. SOAR can store values of various types in the lists. To access Lists, click on the **Lists** tab under **Configuration** menu.

On this page you can see name, content type and size of the lists, whether the lists are exclusions, actions/enrichments are allowed or not, and the last user and last modification date of a list edit.

You can search for a list using the **Search** text field located at top right corner of the page. The page will be updated as you type. The search term will be searched in the names of lists (first column).

You can always edit a list by clicking on the **Edit** button for the desire list. To remove a list from the system, click on the **Delete** button. You can also download a list as a text file (txt) to your computer using the **Download** buttons.

Creating Lists

In order to create a new list click on the **Create List** button.

You should specify the list attributes as explained below.

- List Name: Name of the list
- Content type: Type of data in the list. It can be one of the following:
    - Computer Name
    - Email Address
    - File
    - File Name
    - Hash
    - Host
    - Keyword
    - MAC address
    - Network address (IP and/or Hostname)
    - Process
    - Rule name
    - Unknown
    - URL
    - Username
- Contents: Enter the list’s content one line at a time and click on **Save** button for each line.
- Use as exclusion list: Specifies whether the list will be an exclusion list. When you select this checkbox, you can choose whether the contents of this list to be exempt from the action and enrichment activities or not. If selected, two additional options are displayed:
    - Actions: Set to **Allowed** if performing actions will be allowed on the contents of the list. Otherwise, set to **Not Allowed**.

- ○ Enrichments: Set to **Allowed** if performing enrichments will be allowed on the contents of the list. Otherwise, set to **Not Allowed**.

Example use cases: You may define a list to hold the IP addresses of your data center.

When you mark it as an exclusion list and select **Not Allowed** in the **Actions** field, SOAR will not take any actions for the servers listed if they involve in an incident. For example, your play book may contain a step to block all IP addresses on the incident scope, however it will not block those addresses defined in the list. Or, as another example, you may define a list of VIP usernames. When you mark it as an exclusion list and select **Not Allowed** both in **Actions** and **Enrichments** fields, SOAR will not take actions or perform enrichments on these VIP users.

Exclusion list control is performed before Approval request.

Incidents

Incident configuration is used to define statuses, severities, priorities, incident types and labels for the incidents generated by your alert sources. In order to manage the incident configurations, use the Incidents tab under the Configuration menu.

You can see the following sub-tabs on this page:

- Statuses
- Severities
- Types
- Labels

The following sections explain each configuration.

Statuses

You can define your own statuses for the incidents, such as **Finished** or **Expired**.

Incident statuses support colors likewise labels and severities.

When you click on the **Incidents** tab,a configuration page for Statuses is displayed.

To create an incident status, click on the **Create Status** button. The following status editor shows up:

Value	Description
Status Name	Name of the incident status. Provide a short and explanatory name, e.g., Open, Closed, InProgress.
Open Status	This allows to select whether the incident will be in an open or closed state during the incident progress. For example, it is in open state when the incident is re-opened, or in closed state when the incident is expired.
Suggested Colors	Color of the status..

You can always edit the previously created incident statuses by clicking on the “**Edit**” buttons in the list of statuses. To remove a status from the system, click on the “**Delete**” button.

Severities

Incident severities are labels representing the severity of an incident. You can define and rank them as you want.

You can change the rank of a severity in the priorities list by editing the **Rank** column.

You can always edit the previously created incident severities by clicking on the **Edit** buttons in the list of severities. To remove a severity from the system, click on the **Delete** button.

To create an incident severity, click on the **Create Severity** button.

You should specify the severity attributes as explained in the following table:.

Value	Description
Name	Name of the incident severity.
Color	Select a color from the color palette..
Response/Resolution Time	These fields are optional and they provide what should be the response and resolution periods for an incident of a specific severity. For example, for the incidents of severity “Critical”, you may require shorter times for its response and resolution.

When you select the **Show Additional Parameters** checkbox, there will appear the following fields:

Parameter	Description
Resolution breach alert frequency time units	It is the frequency of notifications which are sent after the resolution of the incidents of this severity has passed the “Resolution Time”.

Response breach alert frequency time units	It is the frequency of notifications which are sent after the response time for incidents of this severity has passed the “Response Time”.

Incident Types -DEPRECATED-

Incident types are assigned to an incident when the incidents go through the playbooks. According to the outcomes of playbooks, an incident will be of these incident types. If no manual operation is needed on an incident (as decided by the playbooks), it will have INCIDENT as its type.

You can create your own incident types if you want SOAR to assign some specific types to the incidents having special backgrounds. To create a type, click on the **Create Incident Type** button.

In order to create a new list click on the **Create List** button see the parameter descriptions as follows:

Value	**Description**
Type Definition	Explanation of the incident type, e.g., for which incidents this type can be used.
Visible Name	Visible Name Provide a name for this incident type to be shown when selecting an incident type on the other pages of SOAR.
Severities/Default Severity	Select possible severities for this type. When an incident is opened by SOAR and related playbooks are executed, the default severity is assigned to the incident.
Statuses/Default Open/Closed Status	Select possible statuses for this type. When an incident is opened by SOAR and related playbooks are executed, the default status is assigned to the incident. When is it closed, the value in the “Default Closed Status” will be the status of incident.
Allow Incident Reopen	Select this checkbox if you want the incident of this type can be reopened after it is closed.
Custom Fields	Optionally, you can add your own fields to the incident to be shown in the Incidents page. Click on the “Create” button within the “Custom Fields” area, and type the name of field, select its type (text/date) and select whether this field will be visible, editable and shown on the Incidents page when you select incidents of this ticket type. After you provide the values for the fields click on the “Save” button, and your field will be added as a row within the “Custom Fields” area. You can edit or delete it using the “Edit” and “Delete” buttons, and add as many fields as you want.

After you provide all the fields with desired values, click on the “**Save**” button on the “**Incident Type Editor**”. The type will be shown in the list of incident types.

You can always edit the previously created incident types by clicking on the “**Edit**” buttons in the list of types.

Labels

Labels are your own special tags to mark the incidents.

To create an incident label, click on the **Create Label** button.

You can always edit the previously created incident labels by clicking on the **Edit** buttons in the list of labels. To remove a label from the system, click on the **Delete** button.

Customization Library

All plugin scripts, email templates, query templates, etc. can be seen and managed under Customization Library.

You can use **Integration**, **Integration Type** and **Script Type** dropdowns on top of the page to filter existing customizations

In order to add a new customization, you need to click **Create New Customization** and select the **Name**, **Description** and **Script** values.

You can **Edit**, **Reset Lookup** and **Download** buttons to manage customizations. **Lookup** shows there this customization is used across SOAR. **Reset** resets the content of customization to out-of-the-box version.

Document Repository

Document repository is the place to store documents and images which will be linked to incidents if needed. For instance, you can add incident handling guides for your SOC analysts and link these documents automatically when such incident is created on SOAR.

To add a document to repository, click on the **Upload Document** button. You need to provide **Title** and **Description** and select the file to be uploaded.

Report Templates

You can prepare your own Report template in JasperReports and upload it to SOAR in order to get your own customized reports.

To add a report template, click on the **Create Report Template** button. You need to provide **Report Type Name** and select the file to be uploaded.

Scope Item Properties

With ArcSight SOAR 3.0, it is possible to create your own scope item property types and use them in your workflows. In order to define a new scope item property, click **Create Scope Item Property** button and fill the **Name** and **Data Type** fields. Scope item property can possibly be a:

- Number
- Text
- Json
- Percentage
- Boolean

GeoIP Database

SOAR can keep scope items' country information as scope item property using MaxMind GeoIP database. In order to utilize this feature, complete the following steps:

1. Create an account on https://dev.maxmind.com/geoip/geoip2/geolite2/ and download the GeoLite2-Country database (Binary)
2. Copy **GeoLite2-Country.mmdb** file into SOAR server using SFTP
3. Edit **/opt/SOAR/conf/SOAR.properties** file and add a parameter as: **SOAR.ip2country.geolite-db=path_to_GeoLite2-Country.mmdb**
4. Restart the "SOAR service".

System Status

Using the **Status**you can check the action and rollback queues, alerts, actions, process queues, and logs generated by your configured system. When you click on the **Status** menu, the following page shows up:

It has the following tabs to monitor SOAR's status:

- Alerts
- Action and Rollback Queues
- Action History
- Enrichment History
- Process Queues
- Troubleshooting

Alerts

Alerts tab lets you see alerts generated by your system. To manage alerts, click on the **Alerts** tab in **Status** menu.

You can select an alert source in the **Alert Source** combo box and see the alerts only generated by the selected source. You can also narrow down the alert list by providing a time interval (Start/End Dates) and specific parameters (Alert Parameters) that are included in the alerts’ context.

You can see more details on an alert by clicking on the **View Alert Details** button under the **Actions** column. You can also see the alert parameters as JSON arguments by clicking on the **View Alert Parameters as JSON**. By clicking on the **Display Incident** button, you will be taken to the incident’s page which has been created by SOAR for that alert.

You can use the **Process Again** button if you want SOAR to re-run the playbooks (the basic and advanced ones) on an alert. Note that **Process Again** button will not have any effect for the alerts with offender information if they have been processed previously.

Action and Rollback Queues

SOAR has a mechanism to manage actions to be executed on the integration, called queuing. This section explains the action and rollback queues.

When SOAR receives an alert, alert is processed according to playbooks and SOAR decides the action and target integration.

SOAR adds this action process or rollback process to **Action and Rollback Queues** list which you can ignore approve or clear items. In order to filter list based on process type,Integration type etc. you can use buttons on the top of the list.

Action History

Action History tab lets you display and search logs of executed actions and rollback operations. To manage action history, click on the **Action History** tab in **Status** menu.

The page allows you to filter the action list by the following criteria:

- **Stage**: Stage of the action. Available values are **Executed Actions** and **Rollback Actions**.
- **Device**: You can select a device defined on your system to see the actions only performed on that device.
- **Playbook**: You can select a playbook defined on your system to see the actions only performed as a result of that playbook.
- **Status**: Status of the action. Available values are **All, Successful** and **Failed**.
- **Start/End Dates**: You can refine the action list by providing start and end dates of actions using the calendar buttons at both fields.
- **Action Value (Contains)**: A value to filter the action list where the action text contains this value.

There is a **"Refresh"** button on top right of the **"Stage"** field. You can click on this button to update the filtered actions list at that moment, or choose one of the predefined intervals in the button's dropdown list to update the list automatically at the selected interval.

There is also a **"Download"** button on top right of the list view. You can download your filtered action list as a CSV file to your computer using this button.

Enrichment History

Enrichment History tab lets you display and search logs of executed enrichments. To manage enrichment history, click on the **Enrichment History** tab in **Status** menu.

The page allows you to filter the action list by the following criteria as well as date:

- **Device**: You can select a device defined on your system to see the enrichments only performed on that device.
- **Submitters**: You can filter by users/automation.
- Status: Status of the enrichment. Available values are **All**, **Completed**, **Failed**, **Long Running**, **Not Started**, **In Progress** and **Excluded.**

There is a **“Refresh”** button on top right. For each entry there’s also a **Result** column that will include a **“Show”** button to display the raw result of the enrichment.

Process Queues

Process Queues tab contains the following queue sub-tabs:

- **Alert Queue**: Lists the alerts received from any alert source that are saved in the SOAR database (including base events for applicable alert sources) and waiting to be processed (create/update incidents, execute playbooks).

  You can use “Clear” button at the very end of queue list to clear the items in the respective queue

Troubleshooting

Troubleshooting Download button under this menu lets you to download a zip archive comprised of the following files:

- actionInternals.txt
- pgLocks.csv
- pgStatActiviy.csv
- pgStats.csv
- threatDump.txt

Managing Playbooks

A playbook is basically a way to tell ArcSight SOAR what to do on a given incident. SOAR performs actions, enrichments and/or sends tasks and notifications based on the playbooks defined in the Playbooks menu. You may create, modify, delete, enable or disable playbooks on this page.

Playbook’s are made of several different components and all of them execute with an order. Although specific rules are mentioned in each section as a general rule SOAR will execute the lowest ranking - therefore highest priority - item first. You can edit the rank via the **Rank** column and created items will appear as the last item in the table.

You see the following sub-tabs on this page:

- Rule Name Filters
- Classification
- Consolidation
- Dispatch
- Playbooks
    - Advanced Script Playbooks
    - Workflow Playbooks
    - Import
- Scheduled Playbooks
- Automation Bits
- Triggers
- Tasks

Rule Name Filters

The **Rule Name Filters** page is updated automatically as SOAR gets new rule name filters and currently it is not possible to create a rule name filters manually. Rule Name Filters list is in ascending order of **Rule Name**.

You can edit the rule name filter configurations by clicking on the "**Edit**" buttons in the list of configurations.

By clicking **+ Create Alert Source Rule Name** button you can create a new alert source rule name filter. A typical **Alert Source Rule Name Editor** screen fields are:

Parameter	Description
Rule Name	Display name of the rule.
Alert Source	Type of the alert source. Select an alert source from the pulldown list of created alert sources.
Ignore Mode	Select from the list [Create alerts", "Ignore base events", "Ignore for all alerts sources", "Ignore for all alert sources of this type", "Ignore for this alert source"].
Pattern Matcher	[checkbox].

You can only change the **Ignore Mode** and **add / delete Scope Item Extraction** information while you are editing.

The following are the possible ignore modes:

Parameter	**Description**
Create alerts	For all alert sources and alert source types, always creates incidents when an alert having this rule name is received.
Ignore base events	It does not create incidents for base events.
Ignore for all alert sources	It does not create incidents for this rule name, for all alert sources defined on the system.
Ignore for all alert sources of this type	It does not create a incident when an alert having this rule name is received, only for the alert sources of the type shown in the “**Alert Source Type**” field. It creates incidents for the alert sources of other types.
Ignore for this alert source	It does not create a incident when an alert having this rule name is received, only for the alert source shown in the **“Alert Source”** field. It creates incidents for the other alert sources.

Scope Item Extraction Section

Parameter	Description
Field Name	Name of the field.
Select Source	Select from the list [“Base Event”, “Correlated”].
Select Category	Select from the list [“Computer Name”, “Email Address”, “File”, “File Name”, “Hash”, “Host”, “Keyword”, “MAC Address”, “Network Address”, “Process”, “Rule name”, “Unknown”, “URL”, “Username”].
Select A Role	Select from the list [“Impact”, “Offender”, “Related”].
Add	[Button]

You cannot edit an existing **Scope Item Extraction**.

You can delete an existing **Scope Item Extraction** by clicking **Delete** button under the **Actions** column.

You can edit an existing alert source rule name definition by clicking the **Edit** button under the **Actions** column.

You cannot rename or delete an existing alert source rule name filter.

Classification

Classification list is processed from top to bottom and only the first match is executed. You can edit the rank of a classification rule via the **Rank** column and created items will appear as the last item in the table.

By clicking **Create Classification Rule** button you can create a new classification.

You can create a classification with no condition, which will execute on all incidents. You cannot create a classification without any action.

Matching Mode: (All condition, Any condition)

Create Conditions:

- **Type**: See Table: Condition Types
- **Parameters**: Appropriate value for the type. Select from the list or enter a value.

Create Actions:

- **Action**: (Add incident label, Change severity of incident)
- **Parameters**: Appropriate value for the type. Select from the list or enter a value.

Table: Condition Types

Type	Description
Address contains	An address value which will be searched in the IP address of alert sources. You can use the “*” character as the wildcard. Assume that this value is .*.*.22, then the condition will be met when an incident is created for all the alert sources having IP addresses that end with “22”.
Address doesn’t contain	Condition will be met when the value typed here is not a part of alert source IP addresses.
Address is in subnet	A subnet value which will be searched in the subnet address of alert sources. You can use the __*__ character as the wildcard.
Address is not in subnet	Condition will be met when the value typed here is not a part of alert source subnet addresses.
Address matches regex	Condition will be met when the IP address of the alert source is matched to the regular expression specified here.

Address doesn’t match regex	Condition will be met when the IP address of the alert source does not match the regular expression specified here.
Alert is manual	Condition will be met when the alert is created manually.
Alert is not manual	Condition will be met when the alert is not created manually.
Alert parameter matches key value pair	Pair can be given as key=value. Condition will be met when the parameter (key) is equal to the value specified here for any alert parameters.
Alert parameter doesn’t match key value pair	Condition will be met when the parameter (key) is not equal to the value specified here for any alert parameters.
Alert source is	Condition will be met when the alert source of the related incident is the one selected here.
Alert source is not	Condition will be met when the alert source of the related incident is not the one selected here.
Alert source rule name is any of	Condition will be met when the rule name of incident’s alert source is any of the selected values here. You can select multiple rule names in the “Parameters” combo box.
Alert source rule name is not any of	Condition will be met when the rule name of incident’s alert source is not any of the selected values here. You can select multiple rule names in the “Parameters” combo box.
Alert source rule name is in list	Condition will be met when the alert source rule name of the related incident is in the list selected here.
Alert source rule name is not in list	Condition will be met when the alert source rule name of the related incident is not in the list selected here.
Alert source rule name matches regex	Condition will be met when the alert source rule name is matched to the regular expression specified here.
Alert source rule name doesn’t match regex	Condition will be met when the alert source rule name is not matched to the regular expression specified here.

Alert time is between (day of week)	Condition will be met when the creation time of an alert is between the dates and times selected here.
Alert time is not between (day of week)	Condition will be met when the creation time of an alert is not between the dates and times selected here.
Alert time is between (time of day)	Condition will be met when the creation time of an alert is between the times of each day selected here.
Alert time is not between (time of day)	Condition will be met when the creation time of an alert is not between the times of each day selected here.
Assignee is	Condition will be met when the assignee of the related incident is the one selected here.
Assignee is not	Condition will be met when the assignee of the related incident is not the one selected here.
Assignee is set	Condition will be met when the assignee of the related incident is set.
Assignee is not set	Condition will be met when the assignee of the related incident is not set.
Assignee is a member of group	Condition will be met when the assignee of the related incident is a member of the group selected here.
Assignee is not a member of group	Condition will be met when the assignee of the related incident is not a member of the group selected here.
Classification contains	Condition will be met when the classification typed here is in classification list.
Classification doesn’t contain	Condition will be met when the classification typed here is not in classification list.
Scope item category is	Condition will be met when the scope item category of the related incident is the one selected here.
Scope item category is not	Condition will be met when the scope item category of the related incident is not the one selected here.
Scope item role is	Condition will be met when the scope item role of the related incident is the one selected here.

Scope item role is not	Condition will be met when the scope item role of the related incident is the one selected here.
Scope item value equals	Condition will be met when the scope item value of the related incident is equal to the value expressed here.
Scope item value doesn’t equal	Condition will be met when the scope item value of the related incident is not equal to the value expressed here.
Scope item value is in list	Condition will be met when the scope item value of the related incident is in the list selected here.
Scope item value is not in list	Condition will be met when the scope item value of the related incident is not in the list selected here.
Severity is	Condition will be met when the severity of the related incident is the one selected here.
Severity is not	Condition will be met when the severity of the related incident is not the one selected here.
Status is	Condition will be met when the status of the related incident is the one selected here.
Status is not:	Condition will be met when the status of the related incident is not the one selected here.

You can edit an existing classification by clicking the “Edit” button under the “Actions” column.

You can delete an existing classification by clicking the “Delete” button under the “Actions” column.

You cannot edit an existing condition or action. You have to delete the condition or action and create a new one.

Consolidation

Consolidation rules are processed from top to bottom and only the first match is executed. Any alerts that matches the same consolidation rule will be gathered in to the same incident until that incident status is **Close**. In that instance a new incident will be created and alerts will be consolidated in to this incident.

You can enable/disable a consolidation rule by clicking the **Enable/Disable** buttons.

By clicking **Create Consolidation Filter** button, you can create a new consolidation.

Timespan: Value in minutes, hours, weeks or days

Since Last Alert: Timespan will be calculated from the last alerts creation time.

Since First Alert: Timespan will be calculated from the first alerts creation time.

Until First Response: Consolidation will stop when the incident is responded by an analyst. When this checkbox is selected SOAR will track the response status of the incident and timespan and stop the consolidation at whichever comes first.

Create Conditions:

- **Type**: Type of the consolidation. Select from the list.
  - Alert source is
  - Alert source rule name is any of
  - Alert source rule name is in list
  - Alert source rule name matches regex
  - Scope item category is
  - Scope item role is
  - Scope item value does not equal
  - Scope item value equals
  - Scope item value is in list
  - Scope item value is not in list
- Parameters: It varies depending on selected type.

Dispatch

You can create dispatch rules for incidents using the **Dispatch** sub-tab. Dispatch rules define the actions to be taken for the incidents having the specified conditions. Dispatch rules will be processed from top to bottom and only the first match is executed.

Here, you can see the rank of the rule (to see the order of dispatch actions to be applied to the incidents), conditions of the dispatch rule, dispatch actions, and the user and date of last edits performed on the rule.

You can always edit the previously created dispatch rules by clicking on the “**Edit**” buttons in the list. To remove a dispatch rule from the system, click on the “**Delete**” button.

You can edit the rank of a dispatch rule via the **Rank** column and created items will appear as the last item in the table.

If you do not want to remove the rule permanently, you can disable it using the “**Disable**” button in the list.

To create a dispatch rule, click on the **Create Dispatch Rule** button.

In this editor you define the conditions and actions that will form the rule.

First you need to specify whether all or any of the conditions you define will be taken into consideration. For this, select **All Conditions** or **Any Condition** in the **Matching Mode** combo box. If you choose **All Conditions**, then ALL of the conditions you define for this rule must be met so that SOAR can perform the dispatch action. The other option (**Any Condition**) means that it will be enough to perform the dispatch action when at least a single condition is met.

To create conditions for the rule, click on the **Create** button within the **Conditions** box. Select the condition type from the **Type** combo box and provide the value for the selected condition type in the **Parameters** field. For example, you may want SOAR to perform a dispatch action when the alert source rule name is any of the values you provided in the **Parameters** field.

Click on the **Save** button within the **Conditions** box to add your condition. You can add as many conditions as you want.

To create incident dispatch actions for the rule, click on the **Create** button within the **Actions** box. Select the action from the **Action** combo box and provide the value for the selected action in the **Parameters** field. The following are the available actions:

- **Add a incident label**: When selected, **Parameters** field toggles to a combo box listing the incident labels defined in the system. You can choose a label from the list, so that when the incident meeting the above conditions is created, it will be labeled as the one selected here.
- **Assign to a user or group**: When selected, **Parameters** field toggles to a combo box listing the users/groups defined in the system. You can choose a user or group from the list, so that when the incident meeting the above conditions is created, it will be assigned to the user or group selected here.
- **Change severity of incident**: When selected, **Parameters** field toggles to a combo box listing the incident severities defined in the system. You can choose a severity from the list, so that when the incident meeting the above conditions is created, the incidents initial severity will be changed to the one selected here.

Click on the **Save** button within the **Actions** box to add your rule action. You can add as many actions as you want.

You cannot edit a previously created conditions or actions. You have to delete and create a new condition and action.

Playbooks

Playbooks tab is the main workflow definition page for SOAR. Playbooks are processed from top to bottom and all of the playbooks with matching conditions will be executed.

While designing the playbooks, users should be aware of the conditions they give and whether multiple playbooks are expected to run or not. Since seperate playbooks running on the same incident are not aware of each other, they should be independently designed. Users should be careful so that one playbook should not interfere with another if they are supposed to work on the same incident. If the process does not require it SOAR suggest that an incident should only match to one playbook.

You can always edit the previously created playbooks by clicking on the **Edit** buttons in the list of playbooks. To remove a playbook from the system, click on the **Delete** button. Rank defines the execution priority of the playbook, i.e., smaller the rank, higher the priority.

On this page, you can create three types of playbooks: **advanced**, **workflow** and **scheduled**.

The advanced and scheduled playbooks creation lets you write your own playbook scripts. Scheduled Playbooks are listed in a seperate page (in **Scheduled Playbooks** tab).

The following section explains each type:

Creating Advanced (Script) Playbook

In order to create a new advanced (script) playbook click on the **Create Advanced Playbook** button.

You should specify the playbook attributes as explained below.

Value	**Description**
Name	Display name of the playbook.
Matching Mode	**“All Conditions”** means playbook will be executed if all the conditions are true. **“Any Conditions**” means playbook will be executed if any of the conditions is true.
Rollback Mode	Set if the action will be permanent or will be rolled back after a period of time.
Incident auto-close	From the combo box, you can select in which conditions the playbook will close the incidents.
Conditions	Use the **“Create**” button to add a condition to this playbook. You can define multiple conditions. Please see the : **Table: Condition Types**.

In the black console area, you can type any command lines using Python programming language to define your script playbook.

You can immediately test your playbook using the **Test** button at the bottom of this editor. Select a defined alert source from the combo box, type a value into the **Value to Block** field to test your script, and press the **Test** button. Your test results will be shown on the same editor as a console. **Value to block** can be anything depending on your script, such as IP or email address.

Creating Workflow Playbook

Workflows run automatically and follows the visual process definition.

While creating a workflow playbook, you can add elements from the right side of the page.

These items are:

- Automation Bits
- Actions
- Enrichments
- Tasks
- Utilities
- Properties

Each element must be connected to another except the last item.

After selecting the item, you have to enter appropriate and valid values depending on the element.

The match conditions of the workflow playbook are defined in the **Start** element of the playbook.

Workflow playbooks are run automatically when:

- **a new incident is created**: Incidents are created by the Alert Rule Name Filter configuration.
- **a new alert is received**: Alerts are added to the incidents by the Consolidation rules.
- **rules of the incident is updated**: Some alert sources update an existing alert e.g QRadar Offences and these can trigger an execution.

Element Usage

Automation Bit Usage

Automation Bits are custom code created by the users to execute custom business logic. A detailed explanation for Automation Bit's can be found in Automation Bit section of this guide. While using Bits scope will be supplied from the **Start from here** element if **Scope Filter** variable is not used.

Actions Usage

There are two kinds of Actions in SOAR. One is from SOAR itself and these actions will act on incidents to change it appropriately e.g Status, Severity.

Second is the action capabilities coming from integrations. There are different capabilities depending on the target device and all of them takes some input regarding their role in the workflow. Action elements are named as <Integration Name> - <Capability Name> e.g

Active Directory - Lock User

Title: Visible name of the element in the visual editor.

Continue on Error: In some cases an action on a device can return an error e.g network problems. In such cases SOAR will stop the execution of the workflow entirely. If this option is selected SOAR will continue execution even if the action is failed.

Rollback Mode: SOAR can undo the action after a set time if needed. In many devices there are limits to how many items can be blocked and most of these artifacts usefulness drops over time. Rollback future gives the SOAR users a way to control their actions and the health of the target device.

Scope Filter: This part's name can be changed from capability to capability but in essence filter will define which scope items from the alert will be included in the execution.

Some actions also have other fields and these are populated from data that resides on the target device. Like tag's, group names.

Actions are asyncronous. Therefore when a workflow processes an action element it queues this action and after successful queueing of this action workflow will resume processing the next element. This means in an ideal SOAR, processing actions will not create a performance issue for the workflow execution. There however some edge cases that when SOAR is under heavy load or an unexpected error is present, actions might be queued but different elements are executed before these actions are finished.

Enrichment

Enrichments are data gathering capabilities that will assist in incident response procedures and decision making. Enrichments have several standard properties.

Title: Visible name of the element in the visual editor.

Continue on Error: In some cases an enricment on a device can return an error e.g network problems. In such cases SOAR will stop the execution of the workflow entirely. If this option is selected SOAR will continue execution even if the enrichment is failed.

Integration: On which integration this capability will be executed.

Scope Filter: This part's name can be changed from capability to capability but in essence filter will define which scope items from the alert will be included in the execution.

Do not use cache: Enrichments use a dynamic cache of previous enrichments and by default these are defined in the integration itself. This option will force the execution to not look into the cache and execute on the target device directly.

Enrichments are synchronous. When executed they will start immediately and hold the workflow execution on this state until a result is returned. It's important to note that not every enrichment works as fast as we expect and in some cases rate limits might apply affecting the execution time of the overall workflow. Some enrichments execute and then wait for the process to be completed in the target device. These are also called asynchronous for their update part but for workflow execution they are treated as synchronous as well and will stop the execution until the response is returned.

Tasks

Tasks are elements that does not have an automatic component and are dependent to human interaction to complete. Tasks therefore will hold the execution at that stage until it's completed by an analyst. Task properties are dependant on the configuration of the task itself so one or more of these properties might not appear.

Title: Visible name of the element in the visual editor.

Scope Filter: This part's name can be changed from task to task but in essence filter will define which scope items from the alert will be included in the execution. Filter's can occur more than once and they are restricted to the Scope Item Type defined for them. So a **Network Address** type filter only works on **Network Address** type scope items.

Timeout Span: When the task is due will be defined by this property. Task will be timed out when it's due and execution will continue. If left empty this value will be taken from the Configuration Parameter **WorkflowTimeout** as a global value.

Analyst Decision is the logic element and will give the analyst a true/false component.

Title: Visible name of the element in the visual editor.

Description: Description of the decision.

Timeout Span: When the task is due will be defined by this property. Task will be timed out when it’s due and execution will continue. If left empty this value will be taken from the Configuration Parameter **WorkflowTimeout** as a global value.

Send Additional Email for Approval: When this is checked SOAR will send an additional email for out of SOAR interaction to the selected Analyst.

Analyst: Recipient of the approval Email.

Utilities

There are three types of utility elements: **Notification**, **Decision** and **User Decision**.

Notification: This element supports sending different notifications to different users.

Notifications can be sent from different channels and currently on-screen, SMS, Email and Windows type messages are supported. Notifications use free-form Subject and a pre-defined template for the message itself.

Decision: Decision are standard logic element of the workflow. For a given predicate group in the property section SOAR will look into the alert and workflow scope and if it matches it’ll return true. Alert scope is defined at the **Start from here** and workflow scope is the enrichment data that’s specific to the workflow execution gathered until this point.

User Decision: User decisions are true/false type checkpoints and they are sent to a recipient to gather input from them. Difference from the **Task Decision** is that this element can send the decision message to a variety of recipients. It can send it to a free-text e-mail address, to an SOAR user or it can take the recipient from the incident scope.

User decision takes a template to form the message and expects the recipient to reply with an **APPROVE** or **DENY**. You can create more than one template to send different data and messages to the relevant recipients. SOAR comes with **User Decision Notification Email Template** as a built-in template in the **Customization Library**.

You can also define scope restricted parameters and they will be filled on the fly. Please note that using a scope restricted parameter in e-mail subject will only show the first item in the parameter. Rest will be appended to the body of the message.

Decision should be in the body of the reply message.

Connector Types

Every element in workflow has a pre-defined connector type. There can be one, two or three output connector.

Single connector: All actions and most other types of elements fall into this category and after the element executes workflow continue to the next element.

Double connector: Elements that contain a timeout falls into this category. First connector will lead to a successful completion of the element within the given time, these are named **then** and second connector will lead to timeout.

Triple connector: User and Analyst Decision falls into this category. First two connectors will lead to true and false respectively in a successful execution and third connector will lead to timeout.

After completing the creation of workflow playbook, you can save it by clicking the **“Save”** button.

Creating Scheduled Playbooks

To create a new scheduled playbook click on the **“Create Scheduled Playbook”** button.

You should specify the playbook attributes as explained below.

Value	**Description**
Name	Display name of the scheduled playbook.
Trigger Frequency	
Custom Frequency Cron	

In the black console area, you can type any command lines using Python programming language to define a complex process. .

You can immediately test your playbook using the **“Test”** button at the bottom of this editor. Select a defined alert source from the combo box, type a value into the **“Value to Block”** field to test your script, and press the **Test** button. Your test results will be shown on the same editor as a console. **“Value to block”** can be anything depending on your script, such as IP or email address.

The options for **Trigger Frequency** are:

Every minute

Every 5 minutes

Every 10 minutes

Every 30 minutes

Every hour

Every 2 hours

Every 3 hours

Custom cron value

In the black console area, you can type any command lines using a programming language, e.g., JavaScript, to define a complex process. Please refer to **SOAR Developer's Guide.**

You may select either one of the predefined values as Trigger Frequency or define your own frequency using crontab-like syntax.

Automation Bits

Automation Bits are custom code created by the users to execute custom business logic. ArcSight SOAR supports Python as programming language.

Name: Visible name of the element in the visual editor.

Description: Description of the Automation Bit.

Input Parameters: Starting parameters of the Automation Bit. These can be **Date**, **String** or **Scope Filter** and named here to be used in the Automation Bit. **Date** will result in current time. **String** will create a parameter input field in workflow playbooks. **Scope Filter** will create a filter field in workflow playbooks.

Automation Bit's are **syncronous** and will hold the workflow executions until they are done. This capability if used in unexpected ways might create longer than usual workflow execution times and delays.

Triggers

Triggers are mini playbooks that are triggered by several events. These events are created by human interaction or passage of time where SLA is concerned. Triggers will evaluate the changes in the incidents and if it matches to a trigger execution will start. Trigger evaluations will be from **top to bottom** and all triggers that matches the conditions will run. Only Event Type condition can be used in trigger **Start Condition** and the rest of the evaluations will be done in the workflow itself via **Decision** elements.

Events can't be matched to two different **Event Type** so **AND** operator is not supported.

In order to create a new trigger click on the **"Create Trigger"** button. The following Trigger Playbook Editor shows up:

Tasks

Tasks are a way to define manual processes for incident response and SOAR handles the automatic and manual elements together in the workflow. Analyst Task will create a task that is going to be handled by the SOC Analysts inside the SOAR Incident Management.

Analyst Tasks are defined here and the resulting task can be then used in the workflow as a standard element. Task definition has below components.

Name: Visible name of the element in the visual editor.

Description: Description of the Task to be shown to the analyst.

Task Scope: Task scope is enabled here and these items will be filtered and shown to the analyst and expected to be completed by him/her.

Scope Item Categories: Input scope item types are selected here. This area supports multiselection.

Task Output:Task output is enabled here.

Scope Item Category: Expected scope item type is selected here. Scope item’s created by the analyst will have this type. This area is single selection.

Task Merge: If in an incident has more than one alert or a consolidation is ongoing it’s possible that the workflow will run more than once and there will be tasks recurring for the analyst to complete. **Task Merge** gathers tasks occurring from the same workflow and shows them as one task to the analyst reducing their load. **Timeout Span** will be merged as well and SOAR will update the merged tasks **Due Time** as the most current one.

Using Task Output or Analyst Decision will disable **Task Merge** capability of SOAR for that elements. **Task Scope** is limited to handle **200** scope items. A task containing more than 200 will be divided into more than one task.

Incident Management Service Desk

Managing Incidents

Incidents menu of the SOAR User Interface allows you to:

- see the list of incidents created by the system,
- see the context, scope items, events and other details of the incident,

- edit incident information such as its label, status and priority,
- edit assignees and watchers of an incident, add related incidents, comments, and attach files, add enrichments and perform actions,
- create manual incidents
- create reports

When you click on the Incidents menu, the following page shows up:

On the top left of page, you see the list of incidents; all the other parts of the page provides information about the incident selected in the list. These information include the description, scope and progress of the incident, the team working on the incident, and activities performed on the incident as a timeline.

Below sections detail these parts of the page.

Layouts

There are two different layouts in SOAR named **Tier 1** and **Tier 2**.

Tier 1 is default layout in which Incident Context and Scope Items take the central focus.

Tier 2 layout is recommended for higher tier analysts who wants to handle deeper details of the incidents. In this layout **Scope Items** and **Base Event** views take the central focus.

Incident List and Navigation

On the left scrollable panel, you can see the page-by-page list of incidents created by the system according to your SOAR configuration. In this list, incident’s number, severity, headline description, the avatar of the user to whom it is assigned, and count of the days that passed since the incident was created are displayed.

You can refresh the incident list anytime by clicking on the **“Refresh”** button located on top of the incident list. To navigate between the pages, you can use the navigation area, either by selecting a specific page from the combo box or using the left and right arrowed buttons.

You can also enter into multiple edit mode by using the **“Multiple Edit Mode button”**, and hide or show the incident list by using the **“Hide”** and **“Show”** buttons located on top of the incident list. For the multiple edit mode explanations, please see the **Multiple Edit Mode section** below.

Sorting Incidents

You can sort the incident list using the **“sorting”** button located on top of the incident list. When you click on this button, you will be shown the options as below:

You can sort the incidents by their creation, last update, severity, respond and resolution times.

Searching and Filtering Incidents

At the bottom of the incidents list, there is a search functionality with a text field and a combo box.

You can type any word into the text field (labeled as **Search**); when you click on the **“search”** button, the incident list will bring the incidents which have the search term in their headlines or descriptions.

There are also some predefined default filters for you. When you click on the **combo box** button next to the search button, you can see a list of default filters; just click on a desired filter and get the list of related incidents:

- Incidents assigned to me
- Incidents I’m watching
- Open incidents

You may notice the **New Search** item in the list (shown after you click on the combo box). You can create your own search using this option. When you select it, Incident Search Editor shows up.

As you can see, you can select the types, statuses, severities, assignees and labels (one or more for each) and you can enter a search term into the **Text Search** (which will look for this text in the description and headline of incidents). If you want to save this search and reuse it in the future, you can do this by selecting the **Save Search** checkbox and giving it a name in the **Search Name** field. After you close the editor by using the **Close** button, you can see your newly created search added to the default searches stated above.

In the Incident Search Editor, you can just retrieve the related incidents at that moment by using the **Search** button and you can clear your selections in the editor by using the **Clear Search** button.

Incident Details

When you select an incident in the incident list on the left panel, its details will be shown on the right panel. This panel consists of the following information:

- **Incident Details** where you can see the rule name, description, custom parameters, alerts, status, severity and labels of the incident.
- **Scope Item** where you can see the extracted artifacts of the incident. Clicking on an item will show it's extended details and Properties. An analyst with right permissions can add a new scope item from this panel via **Add New Scope Item** button. You can also download File Type scope item's directly from the details.
- **Task** where you can see the current task assigned from the playbook.
- **Events** where you can see the events that creates the incident in detail and a graph of incoming events. A binocular in each event will show the extended detail of that specific event.
- **Featured Enrichment** where you can see the information about the enrichment plugin used for the incident.
- **Activity** where you can see each activity performed on the incident along with the user who performed the activities. You can also add, edit or delete comments, or attach files using the editor at the bottom of the **"Activity"** area. You can also filter based on task types and order by ascending or descending.
- **Approval Requests** where the defined actions are approved or denied.(*)
- **Team** which shows the assignee, source and watchers of the incident.
- **Progress** which shows the count of days/hours that passed since the creation of and last update on the incident. You can also track the SLA status of Response and Resolution here.
- **Related** which allows you to add other incidents that you want to relate to this incident. You can relate incidents using the **Add** button on this area and specifying the related incident number and relation type (which could be **DUPLICATE, RELATED** and **DEPENDSON)** in the dialog that pops up.

* : If a SMTP integration is used without credentials then it can't be used as incoming email processor and for approvals.

Editing Incidents

On the right panel of the **Incidents** page, you see the details of the selected incident in the list. Here, you can edit an incident using the **Edit** button located on top right of the page.

You can edit all fields of an incident shown in this dialog.

Multiple Edit Mode

As stated in the Incident List and Navigation section, you can also enter into multiple edit mode by using the **Multiple Edit Mode** button and edit some fields for multiple incidents at the same time. When you click on that button, the incident list toggles to a view where you can select multiple incidents (using the checkboxes shown in front of each incident); you can select incidents not only shown in the current incident list but also the ones listed in other pages using the navigation button described in Incident List and Navigation section. Please see the following example page:

Here you can change the severities, statuses, labels and assignees for the selected incidents at once using the **Update All Selected Tickets”** button. You can also discard your changes using the **Discard** button. And, using the **Run Playbooks Again** button you can execute the playbooks predefined on your system on the selected incidents.

As you can notice, when you click on the **Multiple Edit Mode** button once, the button’s background becomes blue, which means the page enters to the multiple edit mode as explained in the paragraph before the above image. If you click on this button twice, the button’s background becomes yellow, which means all the incidents in the current navigated incident list page are selected. When you click on this button thrice, all the incidents in the incident list will be selected to be edited. To disable the multiple edit mode, just click on this button four times.

Please note the “Approximately…” phrase when you select all the incidents in your incident list (by pressing the **Multiple Edit Mode** button thrice). This is because the incident count may change just after the moment you select all the incidents and during this time some of the incidents may be updated.

Adding Enrichments to Incidents

For some incidents you may need more detail. SOAR provides an enrichment feature for this purpose. You can use the desired plugin for the incident using the **Enrich** button located at the top right corner of the **Incidents** page.

When you press the **Enrich** button, the **Launch Enrichment Plugin** dialog appears as shown below:

Enrichment plugins are grouped according to the information they provide. So, you need to first select a group from the **Group Name** area. Then, according to your group selection, related plugins appear under the **Enrichment Plugin** area. When you select an enrichment plugin from this area, its capabilities are listed under the **Capability** area. Each capability requires different information in this editor.

The following is the plugin dialog for Micro Focus ArcSight enrichment plugin as an example:

Please see the **Enrichments chapter** and **Capabilities chapter** for the full details of each enrichment and their capabilities.

Performing Actions on Incidents

You can trigger an action on an incident at anytime using the **Action** button located at the top right corner of the Incidents page. These actions, such as sending a notification to a related person or blocking an IP address, may vary according to the incident’s special condition.

When you click on the **Action** button, select a integration with which the defined action will be triggered.

Each capability requires a different information in this editor. In the above example, you specify the username from the incident’s scope. Please see **Integration Guides** for the action capabilities.

When you click on the **Create Action** button, the action will fall into the **Approval Requests** field of the **Incidents** page, if any integration approval is configured. The action will be performed once it is approved. If no integration approval is configured, then action will be performed automatically.

Exclusion list control is performed before **Approval** request.

Closing Incidents

You can close an incident using the **Close** button at the top right corner of the page.

Here you need to select the status which will be assigned to the incident after it is closed. You can also type an explanatory comment explaining the closing reason. Click on the **Save and Close** button to close the incident.

Please note that you cannot close an incident unless all the actions to be performed are approved.

Creating Manual Incidents

SOAR receives alerts in two ways:

Automatically from the alert sources, such as ArcSight ESM

Manually, i.e., people call or send emails to an operator to inform about their incidents.

For the latter case, the operator will need to create an incident manually using the **“New Incident”** button at the top right of SOAR interface.

The following list describes the fields:

Parameter	**Description**
Type	Rule name for the type of manual incident type that you will select in the **“Incident Type”** field. You can also use this field to create a new rule if it is not already defined in the **Rule Names**. When you start typing the rule name, this field lists you the defined rules in this combo box matching the entered characters; if the phrase you entered is not a match, just click on the **“Create New Rule”** in the combo box list to create one.
Subject	Subject for this new manual incident which will be the headline of the incident to be created.
Incident Type -DEPRECATED-	Incident type to be selected from this combo box which are predefined on your SOAR system.
Custom Fields -DEPRECATED-	You can provide values for the custom fields which are defined on your system for the selected incident type.
Description	Description for the manual incident to be created.
Time	Time and date of the manual incident which you can select from the calendar in this field.
Severity	Severity of this manual incident, defined on your system, which you can select from this combo box.
Add Scope Item	You can add a scope for this manual incident by selecting the scope category and role, and entering the scope value.
Upload	You can attach a file (original email, a scanned document explaining the alert, etc.) to this manual incident using the **“Choose File**” button in this field.

When **Save** button is clicked, SOAR will create a new incident and display it.

Dashboard and Reports

ArcSight SOAR supports two different options for reporting. First is the Internal Reports supported out of the box. Second type of reports is the External Reports. These reports are created from templates by SOAR and can be edited or created from scratch by users.

Dashboard

Refer to Users' Guide for ArcSight Fusion.

Out of the Box Reports

A user requires Manage Reports and View Reports permissions to access Reports. The following is the list out-of-the-box reports:

- Analyst Performance Report
- Analyst Task Summary
- Closed Incidents Report
- Detailed Incident Report
- Incident Summary Report
- Integration History report
- Integration Summary Report
- Monthly SOC Summary
- Open Incidents Report
- Scope Item Reoccurrence
- SLA Summary
- SOC Current Status Report
- SOC Summary Report
- Threat Summary Report

Analyst Performance Report

Analyst Performance Report presents the user with KPI’s about the selected analyst in the given timeframe.

Analyst Task Summary

Analyst Task Summary Report presents list of taken action for each analyst per incident.

Closed Incidents Report

This report lists the closed incidents in a given timeframe.

Detailed Incident Report

This report can be called directly from the incident itself or in the reports pane.

Incident SummaryReport

Incident Summary Report presents the following data: Total Incidents Count, Total Analyst Count, Total Urgent SLA Breaches, Response SLA ratio, Resolution SLA ratio, Incident status timeline per close types as legend, Incident severity timeline per severies as legend, Open close incident ratio in pie chart, Top ten closure reason in bar chart, Open and close incident per analyst in seperate bar charts and Urgent Incidents lists.

Integration History Report

Integration History Report and it’s detailed counterpart presents the user with a report about all integrations or a selected integration.

Integration Summary Report

Integrations Summary Report presents the customer with a summary information about alert sources and device integrations that exists on SOAR in the given timeframe.

Monthly SOC Summary

Monthly SOC Summary Report presents incident summary for selected month in details of severity, classification, taken action, closed or open incident count and daily distribution of closed action with false positive tag. It also gives you logged in analyst information in month and incident distribution per alert source.

Open Incidents Report

This report lists the open incidents in a given timeframe.

Scope Item Reoccurence Report

Scope Item Reoccurrence Report presents top 10 reoccuring count of scope items those types are IP Address, Username, Email Address, File Name, Hostname, URL and Computer Name.

SLA Summary Report

SLA Summary Report presents Analyst, Rule, Severity and Classification based SLA distribution in detail of response and resolution.

SOC Current Status Report

SOC Current Status Report presents the following data: Open and close incident count, analyst count, urgent incident count, Analyst assigned workload in bar chart per analyst in details of severities as legend, Incident chart per incident severity with open-close detail as legend, Response and resolution SLAin pie chart with miss and met ratio, Queued activity chart and open incident assignment in pie chart.

SOC Summary Report

SOC Summary Report presents following data, total count of incident, total hours saved by SOAR, total count of analyst, total counf of SLA breaches and met ratio for response and resolution, open and closed incidents by time, response SLA and resolution SLA miss and met count in pie chart, incident classification, analyst work load per user in bar chart, incident counts analyst distribution with users as legend.

Threat Summary Report

This report generates a summary of threats in a given timeframe.

External Reports

A user requires Manage Report Templates and View Report Templates permissions to access External Reports.

You can use **Configuration** -> **Report Templates** section to import new templates and change current ones in your environment. After import operation is successful new report templates are available under Reports. To create a new report with this new template you should choose **Create Report Profile** -> **Report Origin** and change it to **External Reports**. **Report Type** drop down will list the available templates for creating a new report.

Every template has different variables that can be used in report profile and SOAR will show these for selection in the creation.

New report templates can be created using JasperSoft Studio v6.8.0 Community Edition which is free to use and resulting .jrxml files can be imported into SOAR.

Abbreviations

- A -

ACL : Access Control List

AD : Active Directory

API : Application Programming Interface

ATAR : Automated Threat Analysis and Response

- C -

CCP : Central Credential Provider

CEF : Common Event Format

CIB : Cluster Information Base

CSOC : Cyber Security Operations Center

CSV : Comma Separated Values

- D -

DLP : Data Leak Prevention

DoS : Denial of Service

- E -

ESB : Erisim Saglayicilar Birligi

ESM : Enterprise Security Manager

- F -

FTP : File Transfer Protocol

- I -

iSCSI : internet Small Computer System Interface

- J -

JSON : JavaScript Object Notation

- L -

LDAP : Lightweight Directory Access Protocol

- N -

NIC : Network Interface Controller

- O -

OVA : Open Virtual Application

- R -

RBL : Remote Blackhole List

REST : Representational State Transfer

- S -

SCSI : Small Computer System Interface

SEPM : Symantec Endpoint Protection Manager

SFTP : Secure FTP Server

SIEM : Security Information and Event Management

SLA : Service Level Agreement

SMS : Short Message Service

SMTP : Simple Mail Transfer Protocol

SOAP : Simple Object Access Protocol

SOAR : Security Orchestration Automation and Response

SOC : Security Operations Center

SORBS : Spam and Open Relay Blocking System

SQL : Structured Query Language

SSH : Secure Shell

SSL : Secure Socket Layer

- T -

TCP : Transmission Control Protocol

TI : Threat Intelligence

- U -

UI : User Interface

URL : Uniform Resource Locator

USOM : Ulusal Siber Olaylara Müdahale Merkezi

USTA : Ulusal Siber Tehdit Agi

- V -

VM : Virtual Machine

- W -

WinRM : Windows Remote Management

WMI : Windows Management Instrumentation

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on ArcSight SOAR User's Guide (ArcSight SOAR 3.0.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!