RELEASE NOTES 6.0.0

VERSION 1.0

FEBRUARY 2020

Copyright

Trademark

Table of Contents

Release Notes v6.0.0

The Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) 6.0.0 release marks an important milestone in our efforts to make orchestrated and automated incident response more and more aligned towards the industry requirements and evolving cybersecurity landscape.

FortiSOAR™ 6.0.0 balances multiple new features additions with equally important feature improvements. Some notable new additions are the introduction of FortiSOAR Recommendation Engine as an analyst aid for informed investigations, ability to execute connector actions dynamically without the need to write playbooks and a rich OOB expression library for simplified playbook development experience amongst many others. Key feature enhancements have been in allowing visual monitoring of playbook executions, improved data ingestion experience, filterable manual inputs and enhancements in HA and Multi-tenant models amongst other important improvements.

FortiSOAR™ 6.0.0 introduces "Record Field Value Prediction" based on the criteria you have defined, and "Record Similarity" that displays records that are similar to the record on which you are working, providing analysts with the complete picture and making it easier for analysts to make informed decisions. It also provides you the ability to run connector actions directly in the detail view of a record and investigate the alert without the need of writing a playbook.

The overall user interface has been revamped making it more intuitive and adaptable to your security needs. It also focuses on enhancing MSSP support by allowing the master to make changes to the tenants' model metadata remotely, and also enhances the Data Ingestion Wizard to allow for fetching of data for each configuration of your connector and adding support for multiple queries for pulling data based on your requirement

Browser Compatibility

FortiSOAR™ 6.0.0 User Interface has been tested on the following browsers:

- Chrome version 79.0.3945.117
- Firefox version 72.0.1
- Internet Explorer version 11.592.18362.0

New Features List

- Important enhancements in Distributed Multi-Tenancy Model, to allow Master node a better control over tenant data and modules remotely by adding support for the following:

  - Introduced the ability that allows the master to make changes to the tenants' model metadata (MMD) and push those changes on the tenant node if the tenant has allowed the master to make changes to its MMD. Similarly, if tenants make any changes to their mmd, those changes will also reflect on the master.
  - Introduced the ability to push picklists from the master node to the selected tenant nodes. Pushing picklists replaces all the picklists that are present in the selected tenant node(s) with the picklists from the master node.
  - Introduced the ability to push modules from the master node to the selected tenant nodes. Pushing modules replicates the module structure of the master on the selected tenant node(s), making onboarding new tenants from the master node effective.
- Strengthening and further simplifying data ingestion experience by changing the following:
  - Added support for fetching data for each configuration of your connector, i.e., if you have two configurations present in your connector, then you can configure unique ingestion for each configuration.
  - Added support for fetching additional sample data to enrich the data mapping.
  - Enhanced the usability of the data ingestion wizard.
  - Added a **Data Ingestion** tab on the `Connectors` page that monitors your data ingestion and provides information on which connectors are configured for using the Data Ingestion Wizard, as well as other information such as what is the status of a configuration, what is the schedule for ingestion, when data was last pulled using that configuration, etc.
  - Added support for configuring bulk ingestion of data during data ingestion, to improve performance.
- Introduced the FortiSOAR™ Recommendation Engine that enables you to do the following:
  - Finding similar alerts, incidents, campaigns, etc. FortiSOAR™ displays records that are similar to the record on which you are working. For example, FortiSOAR™ will display alerts that contain similar filehashes, source IP, domains, etc. based on the similarity criteria you have defined, giving the SOC analysts the complete picture of the event and makes it easier for the analyst to take remedial action.
  - Predicting field values i.e., FortiSOAR™ predicts values of fields of your choice within a record from the values of fields of existing records based on the criteria you have defined, making it easier for analysts to make informed decisions.
- Simplified the playbook building experience by introducing a rich expression library enabling you to build playbooks without any programming knowledge. FortiSOAR™ 6.0.0 introduces an "Expression" section in "Dynamic Values" to help you build playbooks based on your requirements and without programming knowledge.
- Introduced "Password Vault" which integrates FortiSOAR™ with external vaults such as "Thycotic Secret Server" and "CyberArk" that are used by organizations to securely store their sensitive data and credentials. Integration with external vaults also enables users to periodically change system credentials in their central vaults and automatically

having the configurations fetch those passwords using the vault. Once you have configured your external vault using Password Vault, users can then use the credentials stored in the vault to configure connectors in FortiSOAR™.

- Empowered investigations and incident status monitoring by visually showing playbook execution progress from the incident's vantage point; especially useful for viewing the parallel execution paths in playbooks.
- Empowered dynamic investigations by allowing the execution of connector actions dynamically, thereby eliminating the need to write playbooks for ad-hoc requirements. You can run the connector actions directly in the detail view of a record and investigate the alert without the need of writing a playbook. You can also consume the saved output for past connector actions as an input to another connector action within the record for further investigation.
- Overall branding changes with respect to re-branding the product from CyOPs™ to FortiSOAR™, including changes to the login screen, about section, navigation, initial configuration wizard, and documentation changes.
- Enhanced the Time To X widget as follows:
    - Added support to display MTTR values as a Bar Chart, both horizontal and vertical. Earlier this widget could only be displayed using the "Card View".
    - Added support to display categories within the MTTR view. For example, displaying the time to resolve alerts of different levels of severity by a specific user.
- Enhanced the **Detail** view of records such as "Alerts" as follows:
    - Added support for adding tags to records, playbooks, etc. Also added support for searching records based on tags, making tags very useful in searching and filtering.
    - Included a **Playbooks** tab in the detail view, which displays the playbooks that have been executed on that record in the flowchart format, as is displayed in the playbook designer. This makes it easier for users to view the flow of playbooks, especially useful for viewing the parallel execution paths in playbooks.
- Added support for triggering playbooks conditionally based on tag additions, changes, or updates.
- Introduced the ability to auto-align playbook steps vertically or horizontally in the playbook designer. Use these buttons to make your playbook look neat and organized, which is especially useful for very large playbooks where playbook readability might be an issue.
- Introduced the ability to create or upsert records in bulk using the **Bulk** option in the `for each` loop in the "Create Record" and "Update Record" steps.
- Enhanced the **Global Search** in FortiSOAR™ to allow searching for playbooks and rules based on tags, names, and descriptions.
- Introduced the **Matches Pattern** and **Does Not Match Pattern** operators that allow you to use basic pattern matching in conditional statements using the percentage (`%`) or underscore (`_`) wildcards.

- Introduced the JSON field type, which can be used for fields such as `Source Data` that commonly store data in the JSON format. Using JSON as a field type for such fields allows playbooks to get to the JSON data directly, without having to use a JSON parse step.
- Added support for advanced date operations and nested conditions for the **Visible (by condition)** and **Required (by condition)** fields in the Module Editor.
- Added a **Configure Picklist Option Visibility** checkbox in the Module Editor using which can filter a picklist field based on specified criteria.
- Upgraded the FortiSOAR™ technology stack to enhance product security and robustness.
- FortiSOAR™ 6.0.0 includes the following versions of the built-in connectors:
    - Utilities connector version 3.0.0
    - Database connector version 2.1.1
    - IMAP connector version 3.5.0
    - SMTP connector version 2.3.1
    - SOAP connector version 2.2.1
    - SSH connector version 2.1.1
    - Report Engine connector version 1.0.3
    - Code Snippet connector version 1.2.2
    - BPMN version 1.0.1
    - System Monitoring version 1.2.0
      Important: FortiSOAR™ has refactored the output of some operations of some built-in connectors such as the "Email: Extracts email's metadata from email file" operation of the Utilities connector. Due to refactoring, there have been some changes to the output of the Utilities and IMAP connector which are not backward compatible. For more information on FortiSOAR™ Built-in connectors, see the "FortiSOAR™ Built-in connectors" article present on the support site. You must log onto the support site to view this information.
- Removed the Quick Add functionality from FortiSOAR™.

Bugs Addressed

Following is a list of some of the important bugs addressed in **FortiSOAR™ release 6.0.0**:

- **Bug #45135**: Fixed the issue that variables entered in the "No Trigger" step did not have access to input parameters.
- **Bug #46385**: Fixed the issue that the generated report was not getting displayed in the context of the record and users had to navigate to **Reports** > **History** page view the report. Now, the link to the generated report will be present in the comment of the record of the module on which the report creation was triggered.
- **Bug #55822**: Fixed the issue of the Single Sign On (SSO) failing due to a certificate issue.

- **Bug #60026**: Fixed the issue that child playbooks could not be searched in the executed playbook logs.
- **Bug #65936**: Fixed the issue of allowing Python reserved keywords such as “items”, “files”, “input”, etc to be used as variable names in playbooks. Now, FortiSOAR™ ensures that users cannot use the reserved keywords as variable names.
- **Bug #66893**: Fixed the issue of searching fields and filtering not supported in the “Create Record” step and “Update Record” step.
- **Bug #68171**: Fixed the issue of fetching all picklists (even those not used) while loading a simple grid in a report, which in turn lead to a performance impact in FortiSOAR™. Now, the performance of reporting in FortiSOAR™ has been improved since only required column values will be fetched while loading a simple grid.
- **Bug #68526**: Fixed the issue of not allowing the filtering of playbook execution logs on time range. Now, filtering execution logs based on a time range is supported, which makes it easier to navigate to the desired log.
- **Bug #68533**: Fixed the issue that while importing or exporting playbooks, their associated macros were not imported or exported.
- **Bug #69808**: Fixed the issue that bulk insert, update, upsert would cause bloating of execution history and a slowdown of the UI since even though you could specify only the fields that you wanted to update or insert in the input, the output would always contain the complete array of objects with all their attributes. Therefore, when these steps are used in a playbook to update a large number of records, the response time increases since complete objects require to be serialized. To fix these issues, FortiSOAR™ has added support for `__selectFields` in the response of Bulk APIs.
- **Bug #70169**: Fixed the issue that if you change the name of a step, then this breaks the steps that uses the output of the step whose name has been changed.
- **Bug #74627**: Fixed issues associated with the Manual Input step such as not being able to view the record for which the decision is pending, or on whom the decision is pending, filtering of decisions based on items pending on *Me*, or pending on *My Team*, etc. Now, the Manual Input step has been enhanced to address all these issues and improve usability.
- **Bug #75149**: Fixed the issue that while building a prompt, you could only specify *Custom* fields as the “Input Type” in case of a Manual Input step. Now, while building a prompt you can specify either *Record* fields or *Custom* fields as the “Input Type” in case of a Manual Input step.
- **Bug #76111**: Fixed the issue that there was no option to limit records in the Top #n Charts. Now, FortiSOAR™ provides you with the ability to limit records shown in bar graphs.
- **Bug #75491**: Fixed the issue of loading all reports on the report view screen. Now, only the current report will load on the report view screen, which improves the performance of reporting in FortiSOAR™.
- **Bug #75492**: Fixed the issues of rendering and performance of reporting in FortiSOAR™ by deprecating the “Grid” and “Tabs” widgets from reports. Instead of the “Grid” widget, use the “Simple Grid” widget in reports. The “Simple Grid” widget is

lightweight and contains report-specific implementation to improve the performance of reporting in FortiSOAR™.

Known Issues and Workarounds

For a list of known issues and workarounds, see the Known Issues and Workarounds article present on the Fortinet Support Site. You must log onto the support site to view information.

Technical support contact information

Contact the FortiSOAR™ support team for any technical issues or customer service requests.

Email: support@cybersponse.com