Qualys SaaS Detection and Response (SaaSDR)

Release Notes

Version 1.6.0

April 12, 2022

Here's what's new in SaaS Detection and Response 1.6.0!

Fixing Security Misconfigurations on Office 365 Tenants

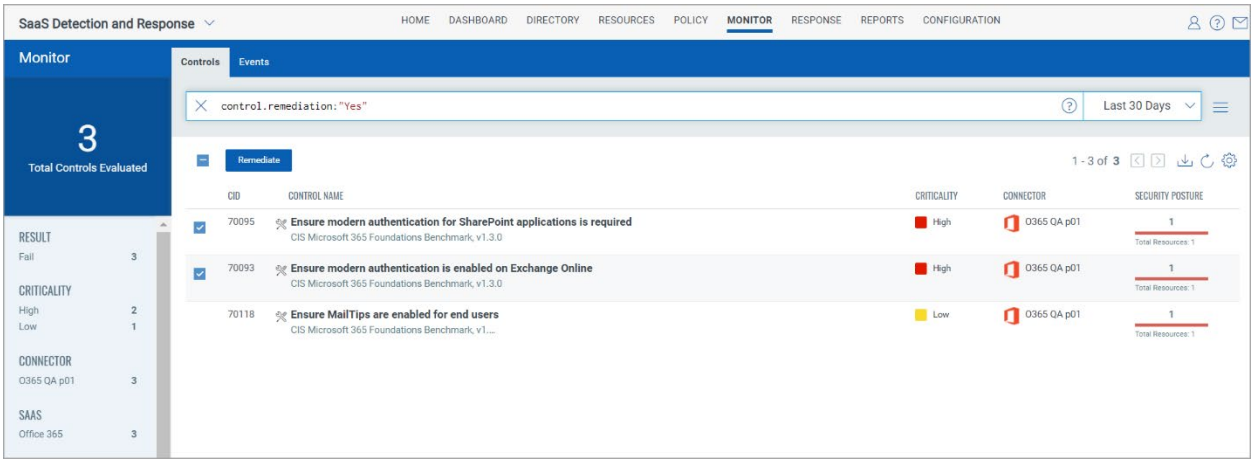
The compliance assessment marks specific controls (checks) as failed if corresponding configurations are not hardened enough. To fix such misconfigurations, Office 365 administrators need to log in to the Office 365 admin center.
With this release, Qualys introduces a new auto-remediation feature in SaaSDR that allows you to fix the misconfigurations right from the SaaSDR UI without having to separately log in to the Admin Center of Office 365.
Note: You can only fix tenant-level misconfigurations without logging into the Office 365 admin center.

To filter the tenant-level misconfiguration, use the **control.remediation: "Yes"** search token. It filters and displays only those failing controls and thus is remediable.
The connector through which the remediation is performed must have the following privileges and roles:

- Enable the following App Permissions:
    - Exchange Administrator
    - SharePoint administrator
- Grant the following User Roles/Permissions:
    - Teams Administrator
    - Privileged Role Administrator

To remediate a control, go to the **Monitor** > **Controls** tab, select the control(s) you want to remediate, and click **Remediate**.

Note: Only the controls with an  icon are remediable. Use the **control.remediation: "Yes"** search token to filter the remediable controls.



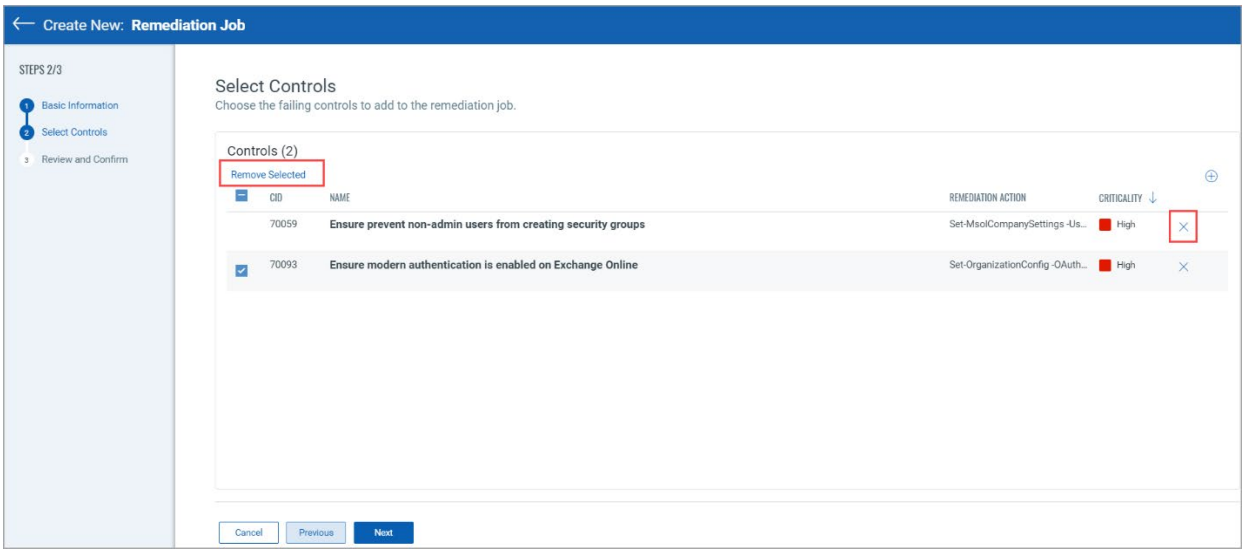
Creating a Remediation Job

Once you click **Remediate**, you can create a remediation job.

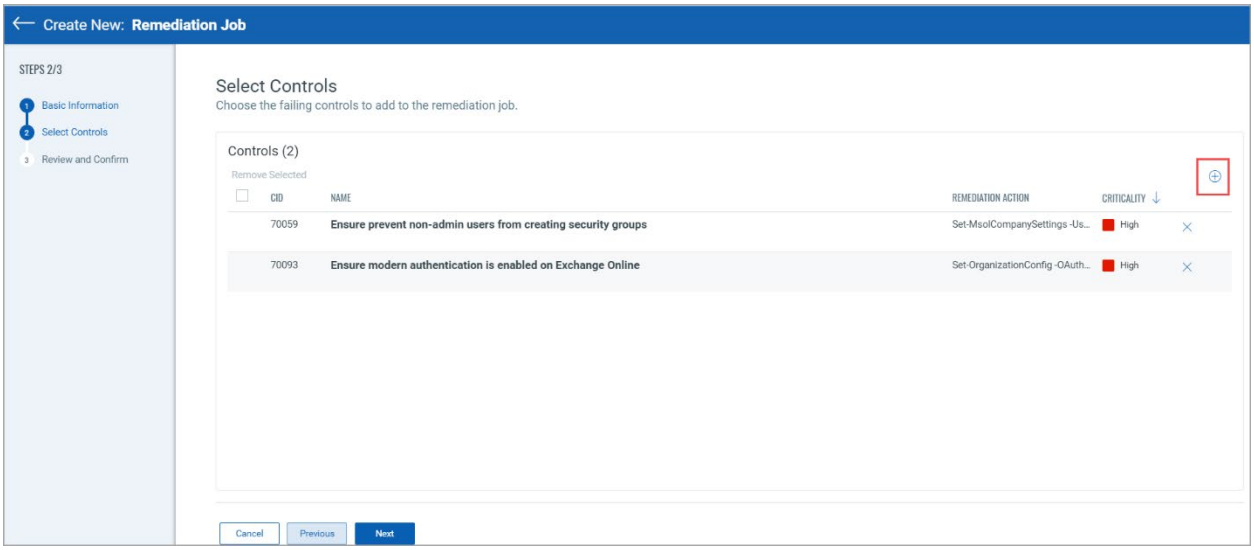
1. On the Basic Information window, enter the **Name** and **Description** and click Next. The SaaS and the Connector fields are auto-populated.
2. On the Select Controls window, click **Next** if all the details appear correctly.
   Or,

Optional: You can choose to remove controls or add new controls.

Remove controls: Select one or more controls available in the list and click **Remove Selected** or use the Remove control icon to remove control.

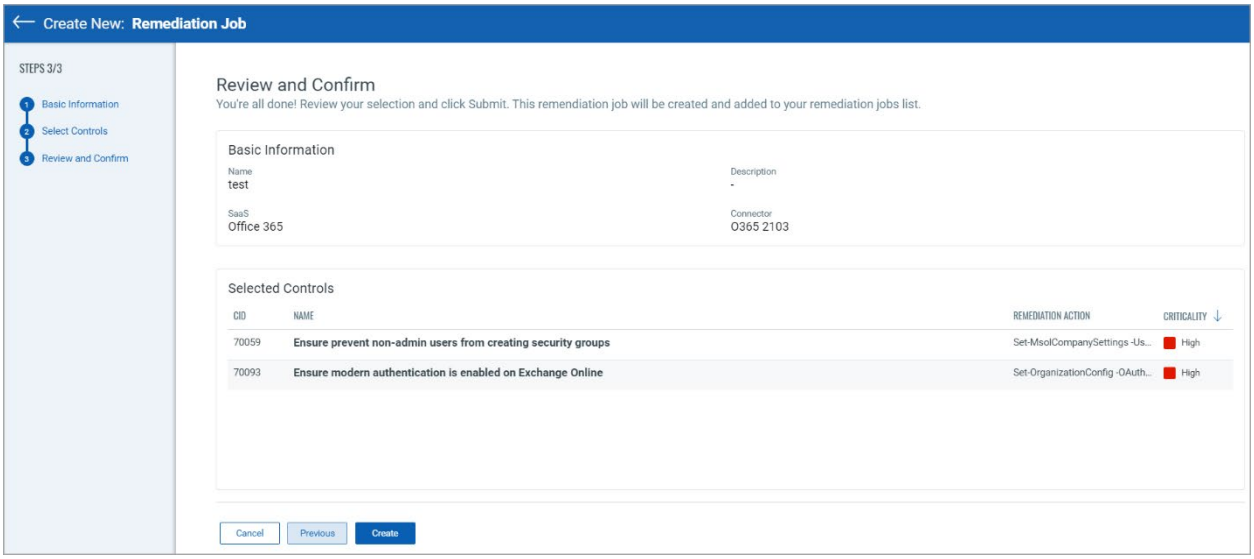


Add controls: You can also add controls when creating the remediation job using the **Add Controls** icon as highlighted below:



3. Review the controls and click **Next**.

4. On the Review and Confirm window, confirm the details and click **Create**.

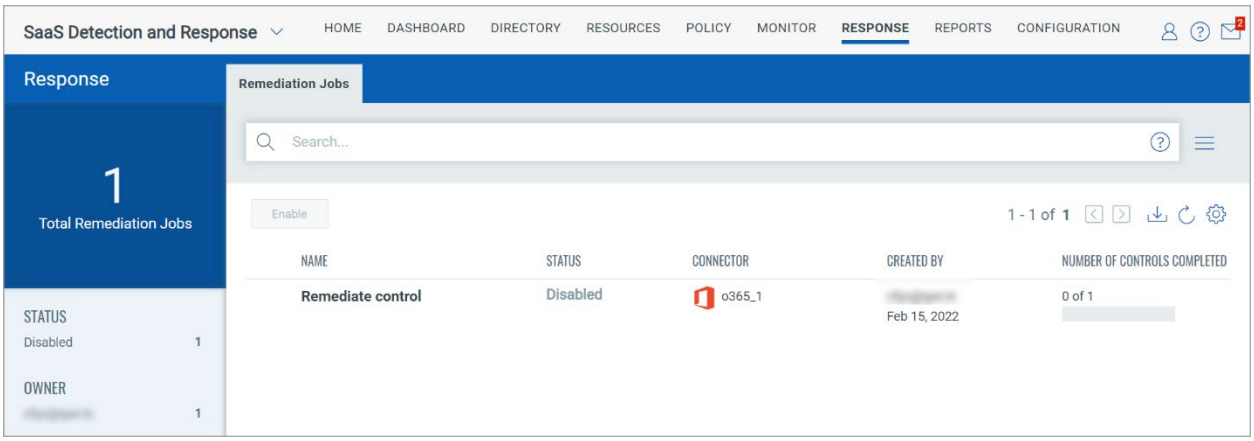


Once you initiate the remediation, the compliance scan automatically reflects the latest compliance posture. The status of the controls changes based on the scan results once the remediation is successful.

View Status of the Controls

To check the status of the controls, go to the **Monitor** > **Controls** tab.

In the **Response** tab, you can view the status of different response activities and export the details if required.
In the **Remediation Jobs** sub-tab, you can check the remediation jobs used to fix the misconfigurations on your SaaS tenants.



Note: The remediation job needs to be explicitly enabled to get it started.

New Home Page

The SaaSDR 1.6 release comes with a modified **Home** page.
On the Home page, the three sub-tabs give you in-depth knowledge of the supported features.

Build Inventory

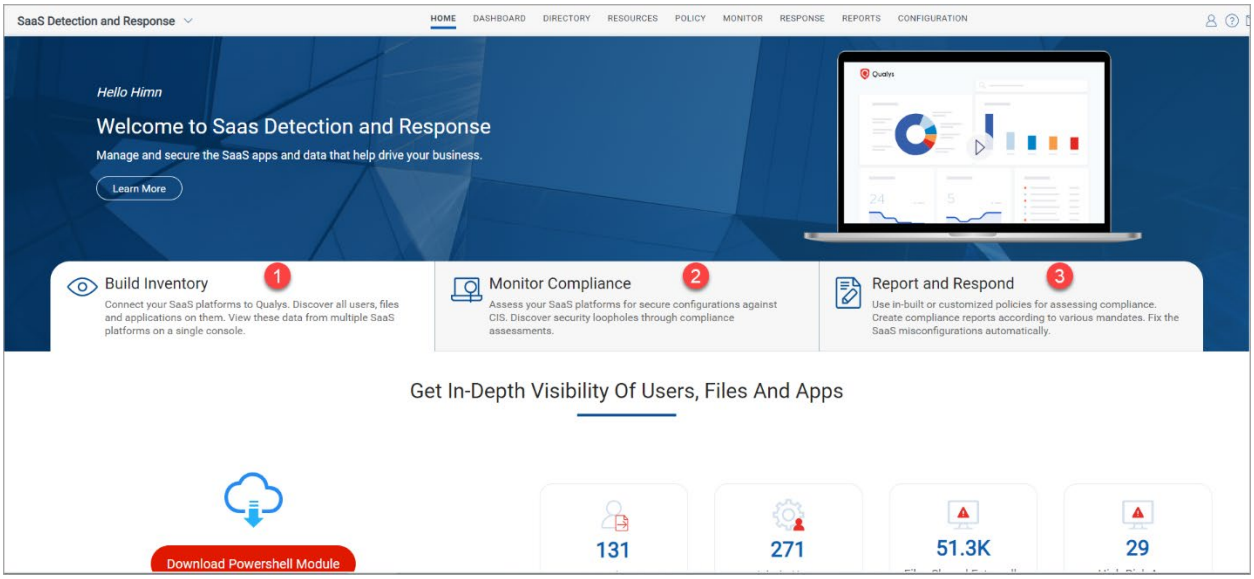
View all the Users and User Groups in your organization. Also, view all your resources, like files and folders, third-party applications, and meetings identified from the scanned SaaS applications.

Monitor Compliance

Enable and run the CIS Microsoft 365 Foundations Benchmark v1.3 policy for your connectors. View the policy controls to monitor your compliance posture.

Report and Respond

Perform different actions on the existing reports. Fix the security misconfigurations in SaaS to enhance their security posture.

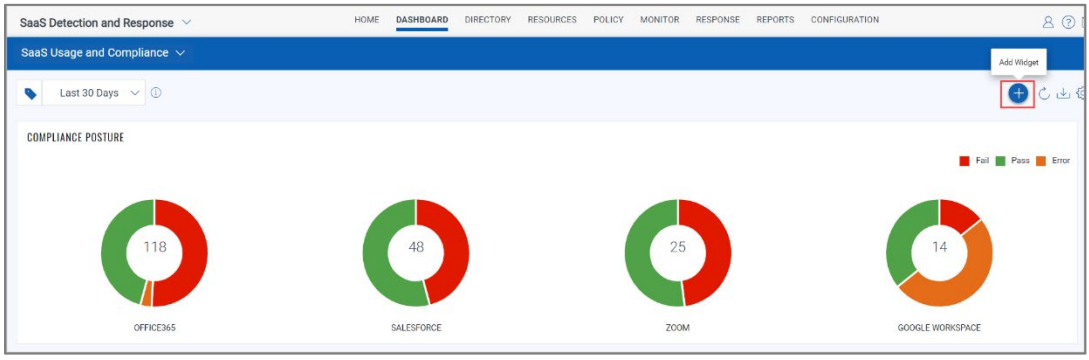


Unified Dashboard (UD) Support for SaaSDR

Dashboards help you visualize your resources such as assets, users, and applications, see your threat exposure, vulnerabilities, misconfigurations, and highlight essential findings in a summarized manner. We have integrated Unified Dashboard (UD) with SaaS Detection and Response (SaaSDR).

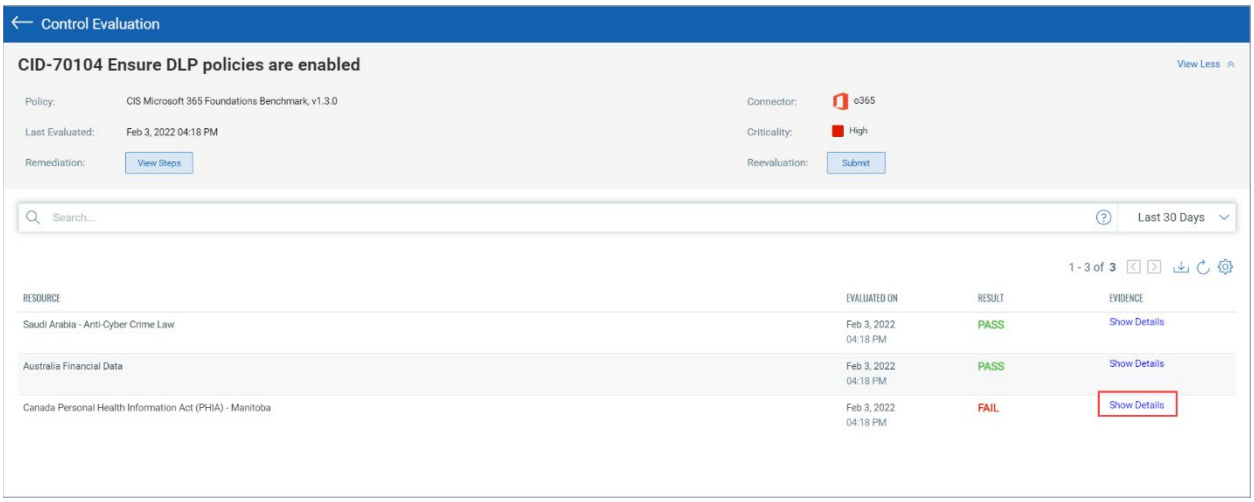
UD brings information from all Qualys applications into a single place for visualization. UD provides a robust new dashboarding framework and a platform service used by all other products to enhance the existing dashboard capabilities. You can use the default dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your vulnerability posture view.

Click the **Add Widget** icon on the Dashboard page to access the **Add Widget to Dashboard (SaaSDR)** screen to add more widgets.

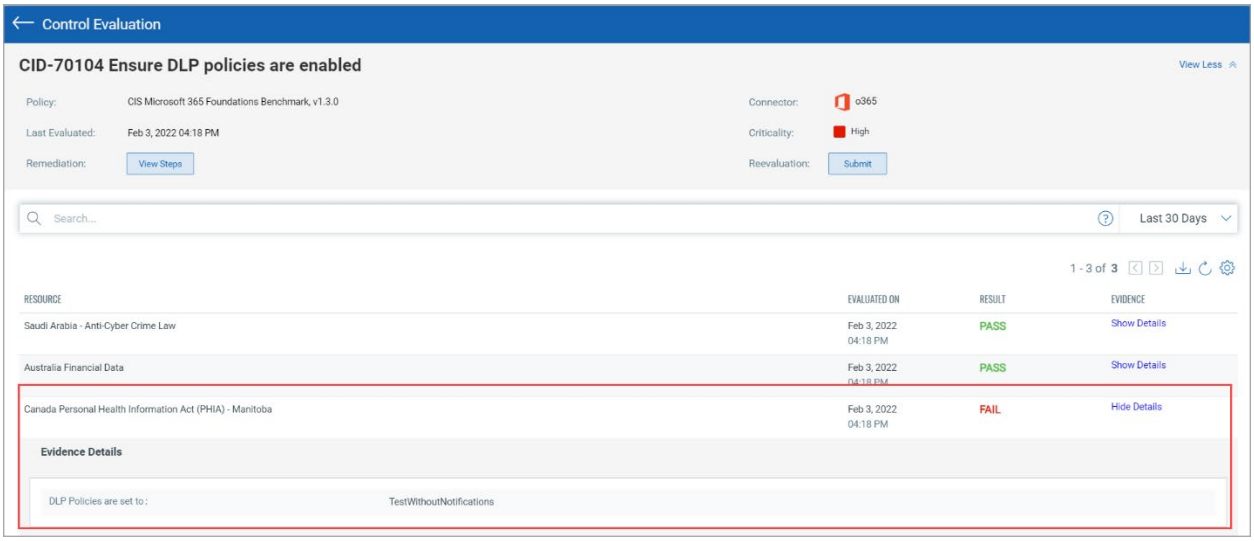


Control Evaluation and Evidence at Resource Level

You can now view the control evaluation and evidence details at the resource level instead of the policy level. Go to **Monitor** > **Controls** and click the Security Posture of the control for which you want to view the evaluation and evidence details.
Under the Evidence column, click **Show Details** to view the evaluation details.

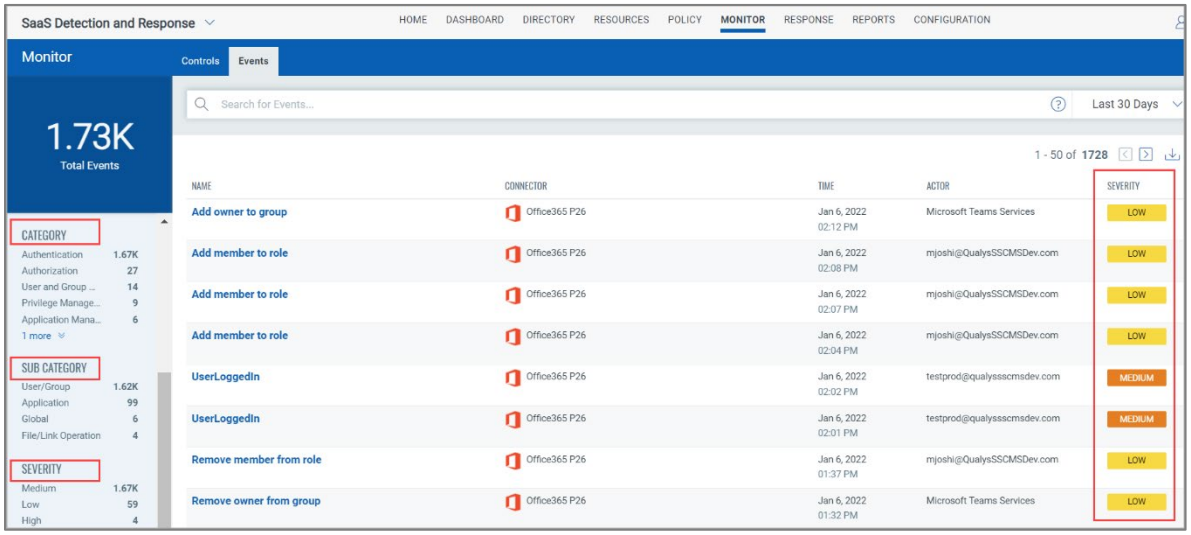


You can view the evaluation details with Pass/Fail reasons.

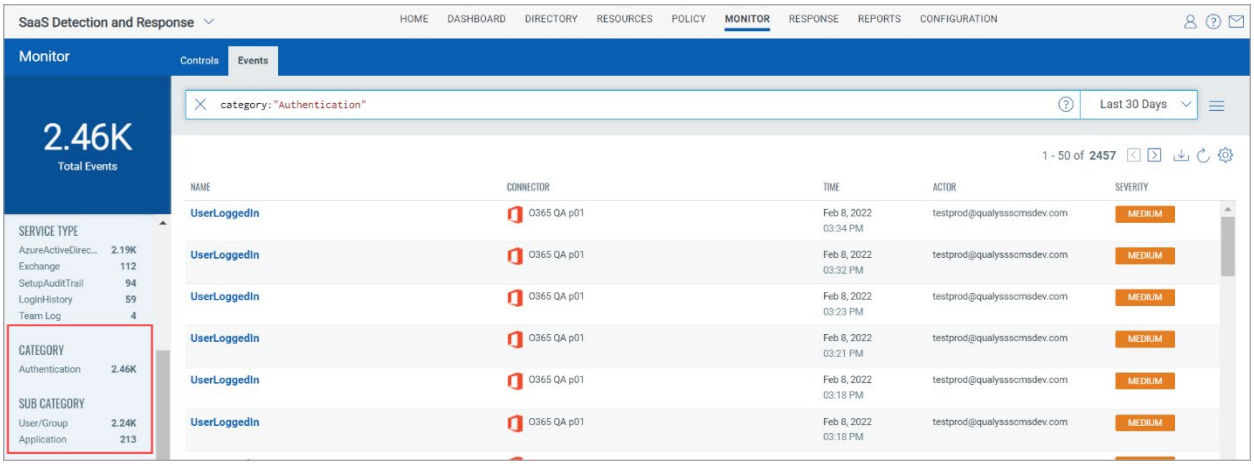


Improvised View of Events Data

You can view all types of connectors' events under the **Severity** column introduced with this release under the Monitor > Events sub-tab.
The **IP** and **Result** columns are now removed from the grid but not from metadata. You can still view the IP and Results in the metadata details.
New filters are also added for **Category**, **Sub-category,** and **Severity**.



We have assigned a few categories and some specific sub-categories against each category to enable a better search and to ease the filtration.
For example, if you pick Authentication from Category options, User/Group and Application appear in the Sub-Category column.

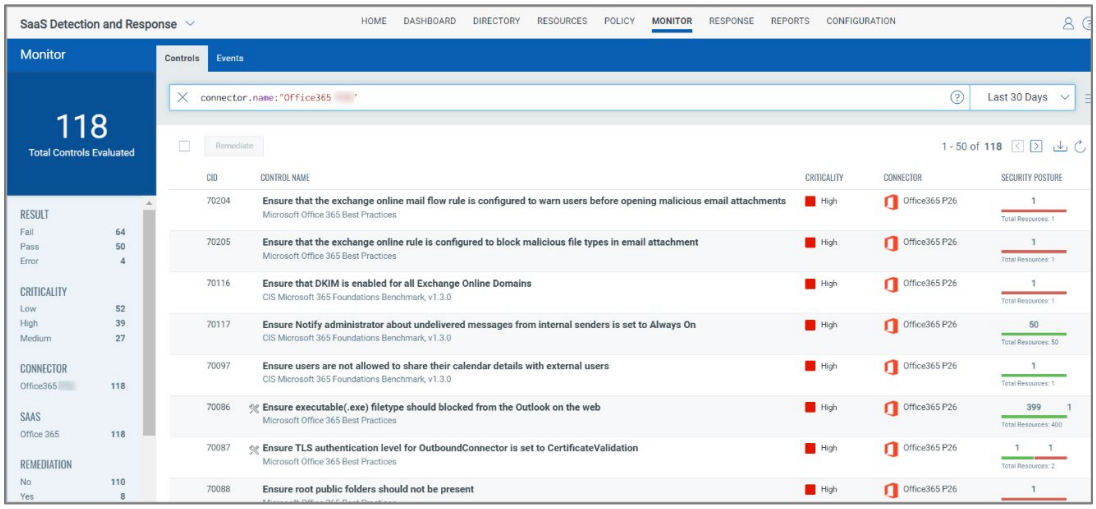


The categorization parameters are set individually for each connector type based on the requirements and specifications of the apps.

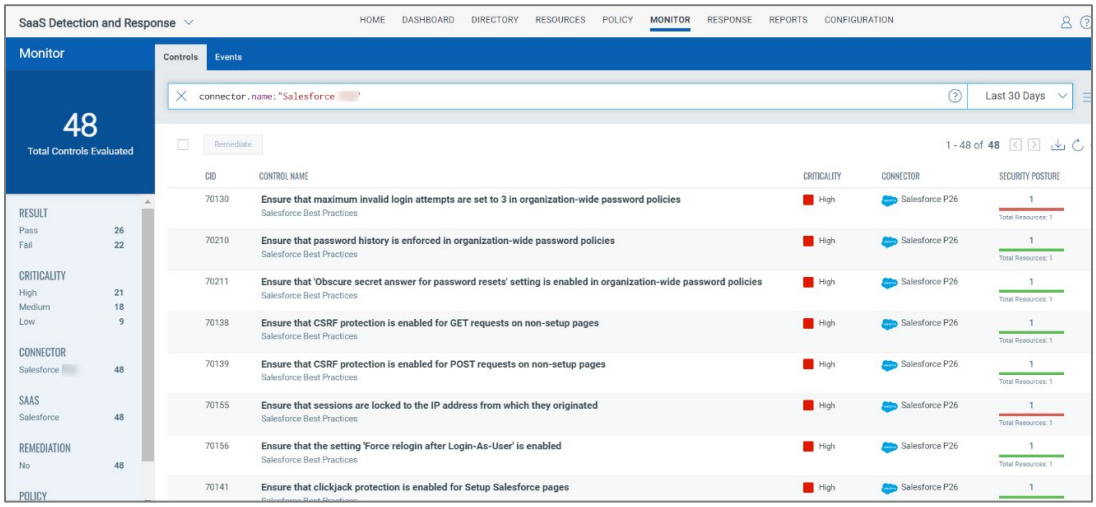
Content Updates

Following are some updates for this release:

Office 365 Controls - New controls are added to assess the compliance against the lateral attacks originating from ADFS setups. These controls help assess your organizational preparedness for preventing lateral movement of Solar Winds Attacks originating from the ADFS setup.
To view the list of the controls, go to the **Monitor** > **Controls** tab.
To refine your search, select the required connector from the **Connector** filter.



Salesforce Controls – SaaSDR is now publishing out-of-the-box controls as suggested in Salesforce Security Guide 2021 edition. New controls are added to the Control Library based on the Salesforce Security Guide 2021 edition. However, you can view the evaluations under the **Monitor** > **Controls** tab.



Salesforce Events - SaaSDR monitors all the events generated by Salesforce.
All the events, including configuration changes, privilege escalations, failed logins, data exposure, apps with high exposure, and so on, are monitored in SaaSDR and listed under the **Monitor** > **Events** tab.