Lab Guide

True Vulnerability Management:

Take Control and Improve Your Security Posture

Jonathan Walker & David Bell

Default Login / Password: Knowledge17

admin / Knowledge17

itil / Knowledge17

employee / Knowledge17

Lab Sponsored by Microsoft Azure



This
Page
Intentionally
Left
Blank

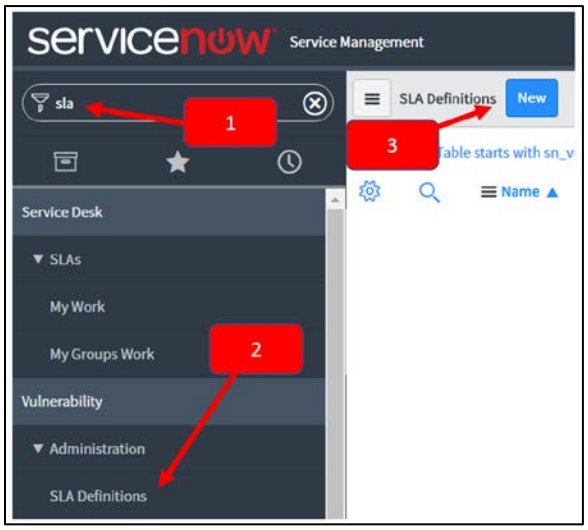
Lab Goal

Move to **DEFINED** on vulnerability management maturity model. Define your success criteria! The purpose of this lab is to quantify your organization's success criteria by creating Service Level Agreements (SLAs) for specific types of vulnerabilities and to reduce the noise from the overwhelming amount of vulnerabilities.

Lab 1.0
Define Success

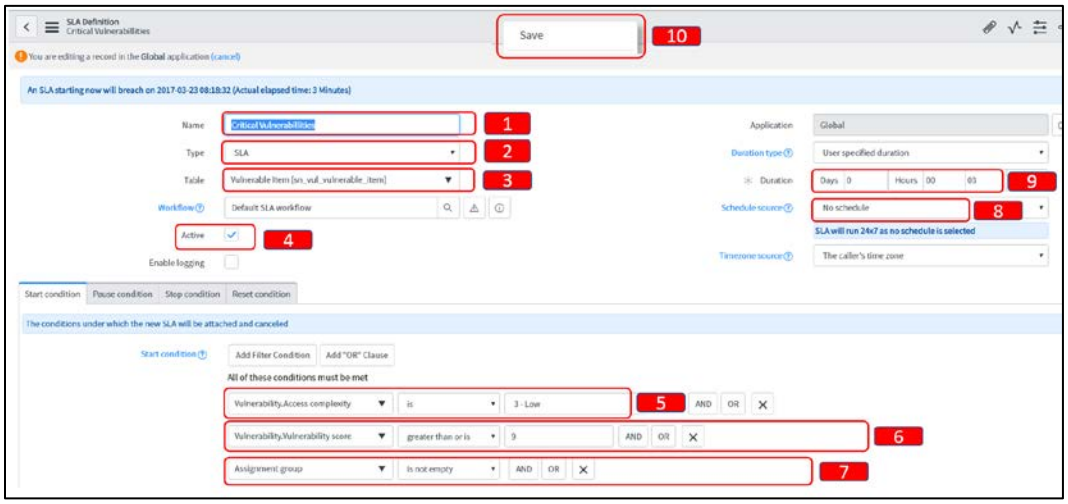
Create the SLAs

1. Navigate to **Vulnerability > SLA Definitions.**

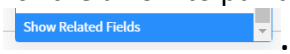


   a. Filter navigation by typing **sla**
   b. Click **SLA Definitions**
   c. Click **New**

2. Enter the **SLA details** for the first SLA.

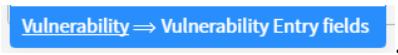


a. Name: **Critical Vulnerabilities**
b. Type: **SLA**
c. Table: **Vulnerable Item [sn_vul_vulnerable_item]**
d. Active: **Check for "true"**
e. Add a filter condition: **Assignment group – is not empty**
**********(click "AND" to add another filter condition)**
f. Add a filter condition: Click the arrow to pull down the 

option. Scroll to the bottom and click 

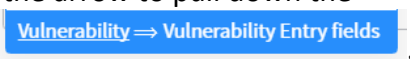
.
Click into 

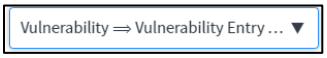
and type **vulnerability** 

and choose 

. Click into 

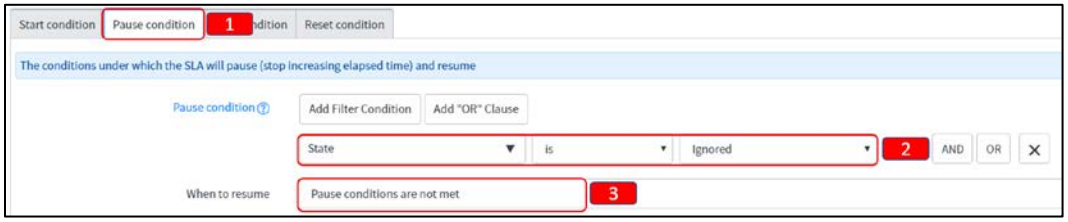
and choose **vulnerability score" - is greater than – 9**.
g. Add a filter condition: Click the arrow to pull down the 

option and type **vulnerability**. Choose 

. Click into 

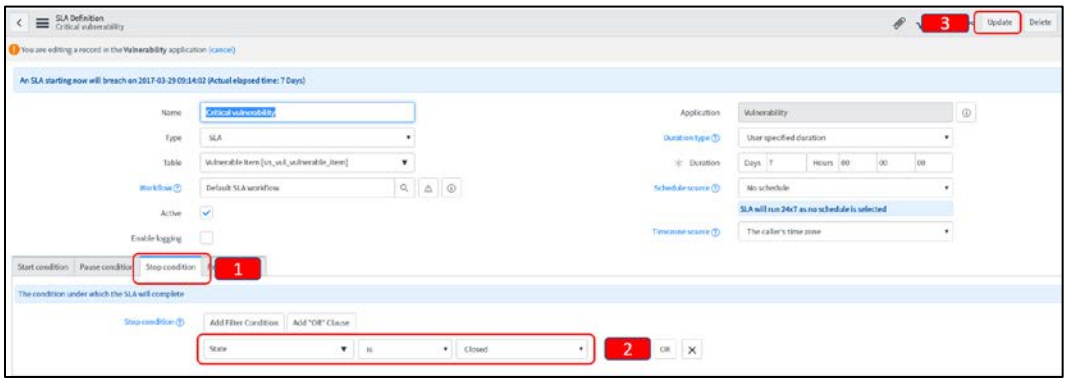
and choose **Access complexity - is – low**.
h. Schedule source: **No schedule**
i. Duration: **7 days**
j. Right-click gray banner at the top and choose **Save**.

3. Set a **Pause** condition.



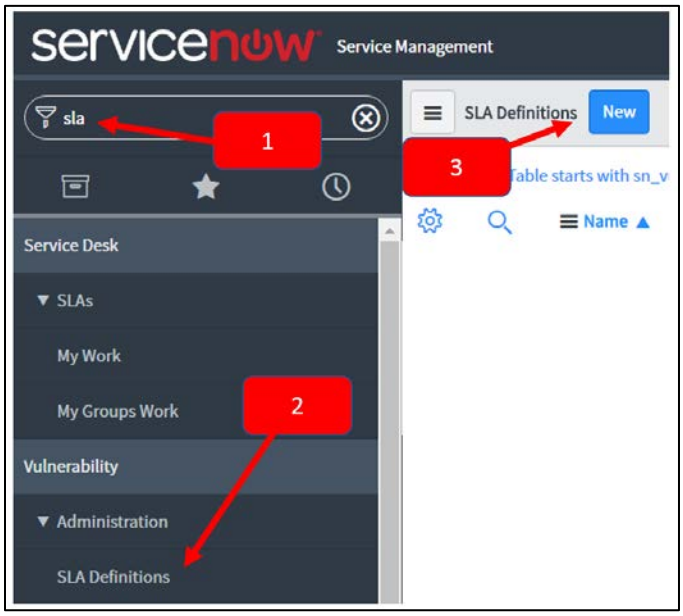
   a. Click the **Pause condition** tab.
   b. Add a filter condition: **State - is – ignored**.
   c. Pull down and set When to resume to **Pause conditions are not met**.

4. Set a **Stop** condition.



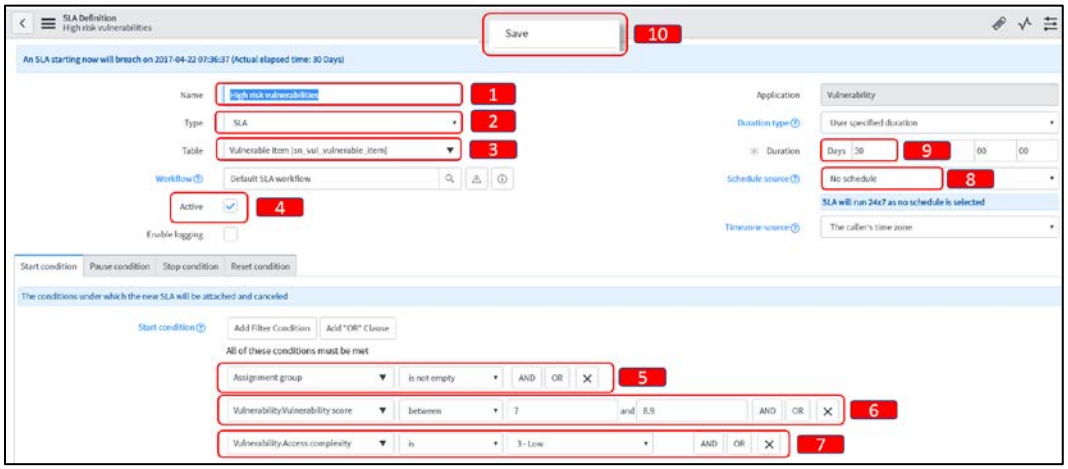
   a. Click the **Stop condition** tab.
   b. Add a filter condition: **State - is – Closed**.
   c. Click **Update**.

5. Create the 2nd SLA (Navigate to Vulnerability > SLA Definitions):



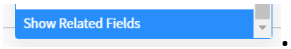
a. Filter navigation by typing **sla**.
b. Click **SLA Definitions**.
c. Click **New.**

6. Enter the SLA details for the 2nd SLA.



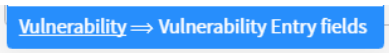
a. Name: **High Risk Vulnerabilities**
b. Type: **SLA**

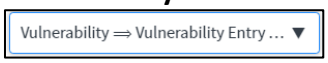
c. Table: **Vulnerable Item [sn_vul_vulnerable_item]**
d. Active: **Check "true"**
e. Add a filter condition: **Assignment group – is not empty**
**********(**click **AND** to add another filter condition).
f. Add a filter condition: Click the arrow to pull down the 

option and scroll to the bottom. Click 

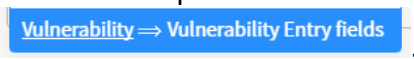
. Click into 

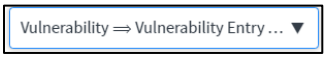
and type **vulnerability** 

and choose 

. Click into 

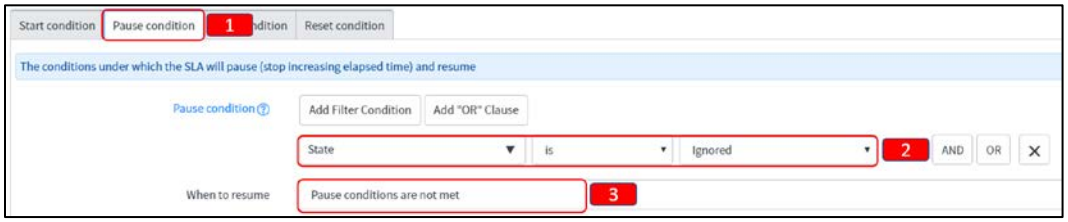
and choose **vulnerability score - between – 7 and 8.9**.
g. Add a filter condition: Click the arrow to pull down the 

option and type **vulnerability**. Choose 

. Click into 

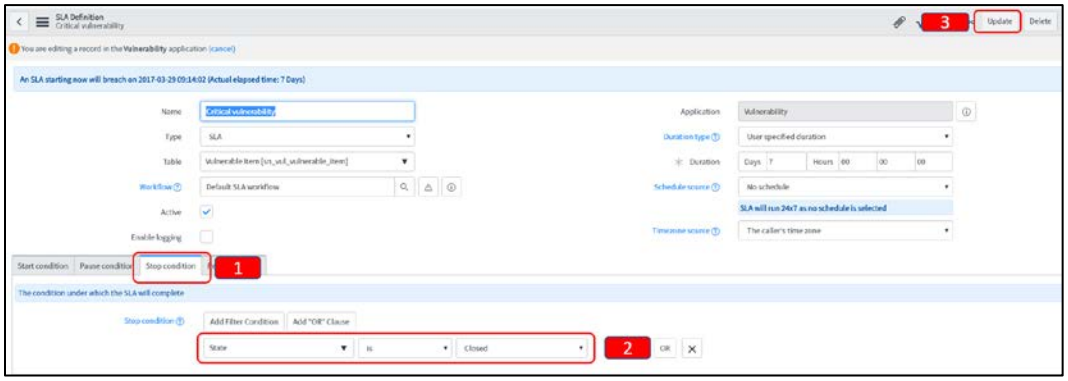
and choose **Access complexity - is – low**.
h. Schedule source: **No schedule**.
i. Duration: **7 days**.
j. Right-click gray banner at the top and choose **Save**.

7. Set a **Pause** condition.



a. Click the **Pause condition** tab.
b. Add a filter condition: **State - is – ignored**.
c. When to resume: Pull down and set to **Pause conditions are not met**.

8. Set a **Stop** condition.



a. Click the **Stop condition** tab**.**
b. Add a filter condition: **State - is – Closed.**
c. Click **Update** to save and close.

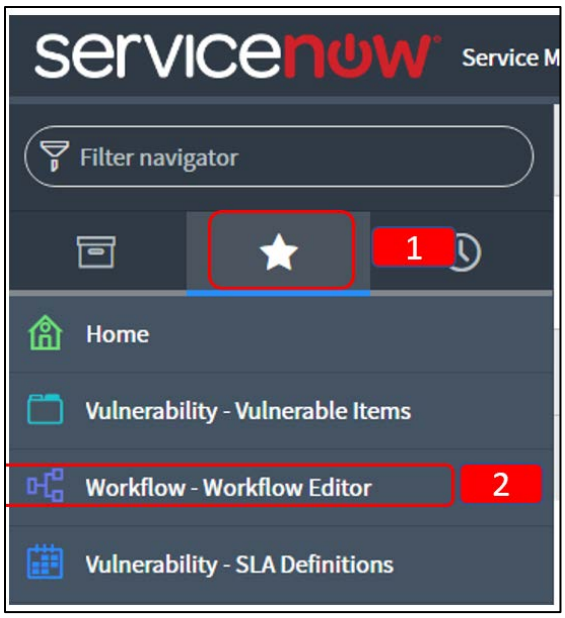
Lab Goal

Move to **DEFINED** on vulnerability management maturity model. Once success criteria have been established, an automated response to these vulnerabilities should be created. The purpose of this lab is to create automated workflows to replace manual vulnerability response tasks.

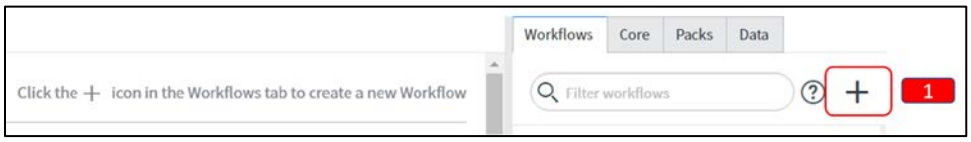
Lab 2.0
Automate the Response Process

Create the Workflows

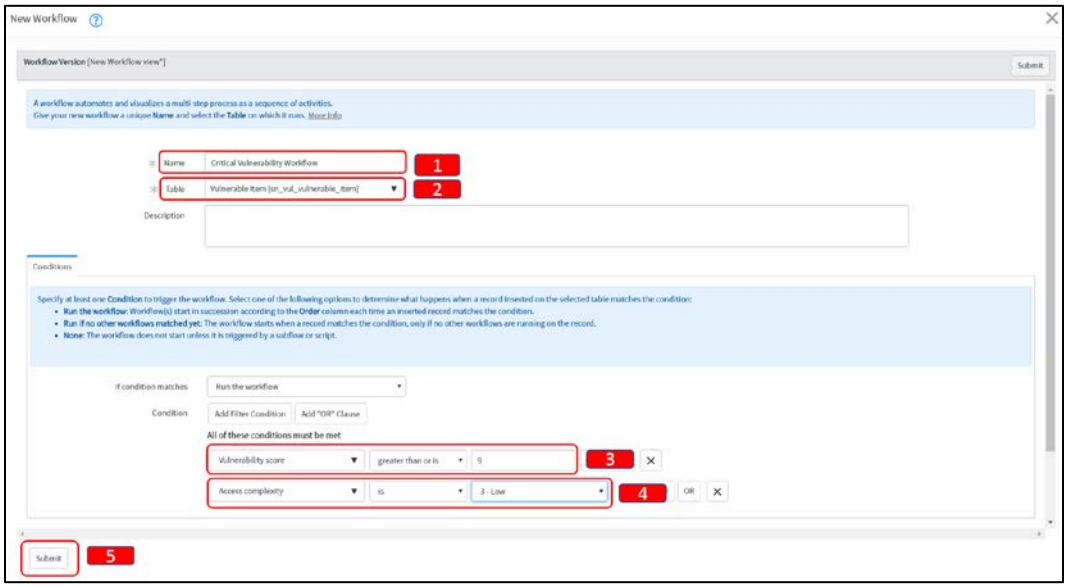
1. Navigate to **Favorites > Workflow-Workflow Editor**.



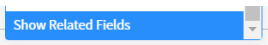
2. Click the **+** button to create a new workflow for Critical Vulnerabilities.

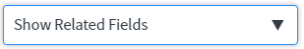


3. Enter the run conditions for the workflow.

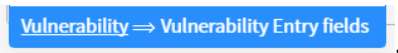


a. Name: **Critical Vulnerability Workflow**.
b. Table: **Vulnerable Item [sn_vul_vulnerable_item]**.
c. Add a filter condition: Lick the arrow to pull down the 

option and scroll to the bottom. Click 

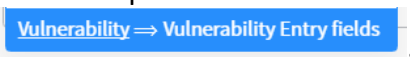
. Click into 

and type **vulnerability** 

and choose 

. Click into 

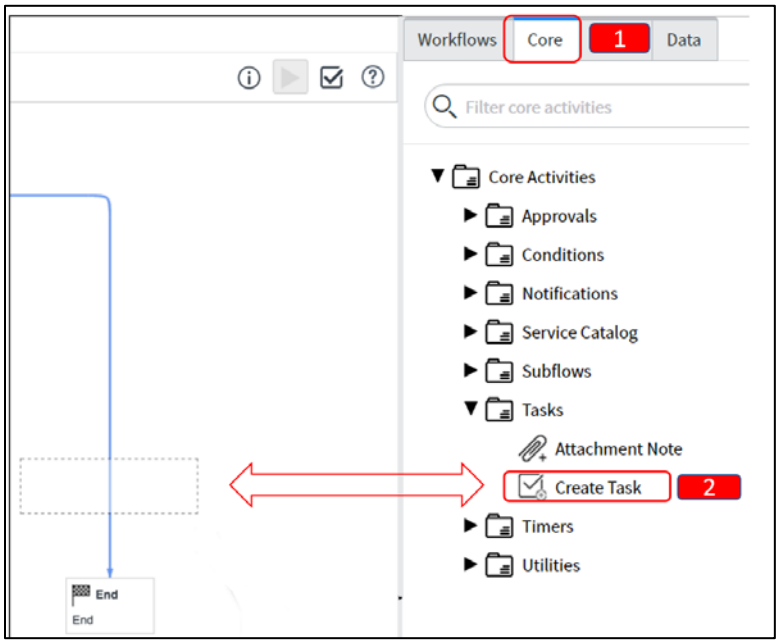
and choose **vulnerability score – greater than or is – 9**.
d. Add a filter condition: Click the arrow to pull down the 

option and type **vulnerability** and choose 

. Click into 

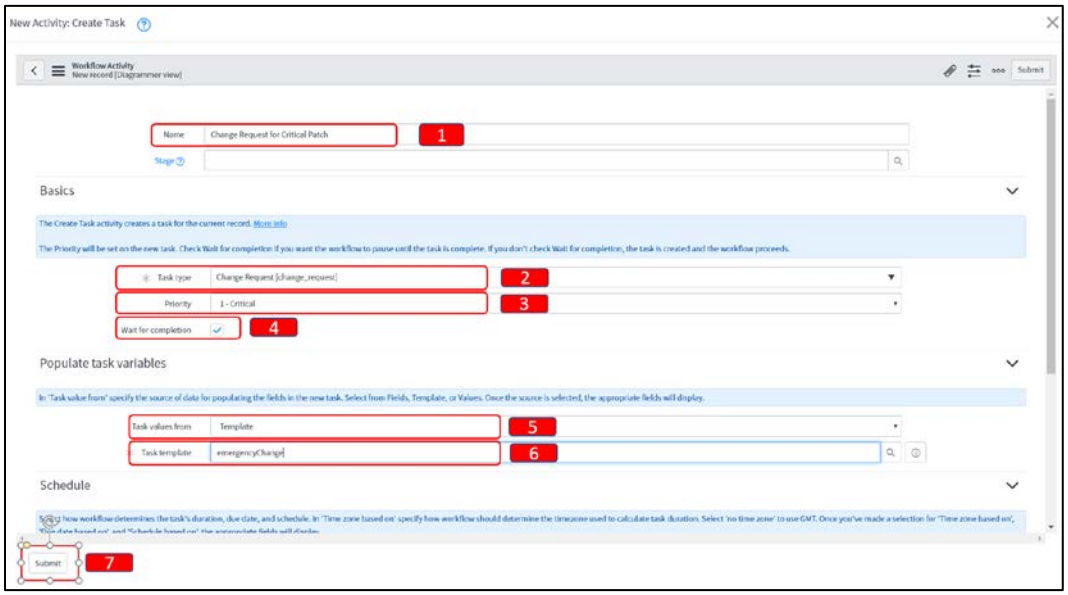
and choose **Access complexity" - is – low**.
e. Click **Submit**.

4. Create a **Task** activity.



a. Click the **Core** button in the top-right of the workflow builder.
b. Click/hold **Create Task** and drag and drop it to the left into the workflow canvas.

5. Configure the **Create Task** workflow activity.

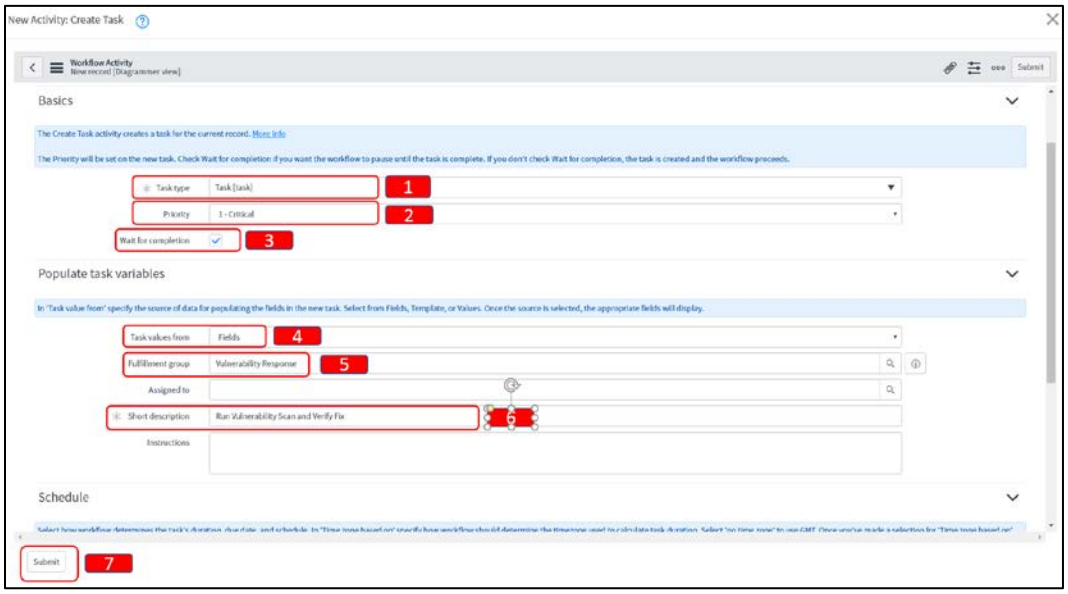


   a. Name: **Change Request for Patch (Critical Vulnerability)**
   b. Task type: **Change Request [change_request]**
   c. Priority: **Critical**
   d. Wait for completion: Check box for **true**.
   e. Task values from **Template**.
   f. Task template: **CriticalVulnerabilityEmergencyChange**.
   g. Click **Submit**.

6. Add a second **Create Task** activity to the workflow:

   a. Ensure the **Core** tab is selected.
   b. Navigate to the **Core Activities > Tasks** folder.
   c. Click and drag **Create Task** onto the workflow canvas after the first **Create Task** activity, ensuring that the connecting line turns **blue**.

7. Configure the **Create Task** workflow activity.

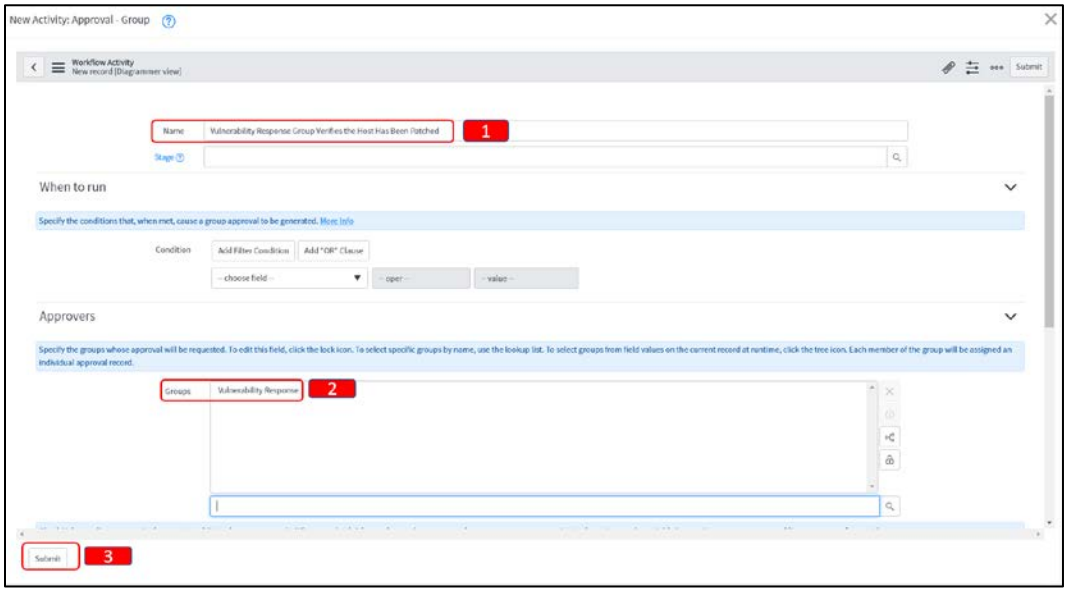


a. Task type: **Task [task]**.
b. Priority: **Critical**.
c. Wait for completion: Check for **true**.
d. Task values from: **Fields**.
e. Fulfillment group: **Vulnerability Response**.
f. Short description: **Run Vulnerability Scan and Verify Fix**.
g. Click **Submit**.

8. Create an **Approval – Group** workflow activity.

   - Ensure the **Core** tab is selected.
   - Navigate to the **Core Activities > Approvals** folder.
   - Click and drag **Approval - Group** onto the workflow canvas after the previous **Create Task** activity, ensuring that the connecting line turns blue.

9. Configure the **Approval - Group** workflow activity.



   a. Name: **Vulnerability Response Group Verifies the Host Has Been Patched**.
   b. Groups: **Vulnerability Response**.
   c. Click **Submit**.

10. Create a **workflow** activity:

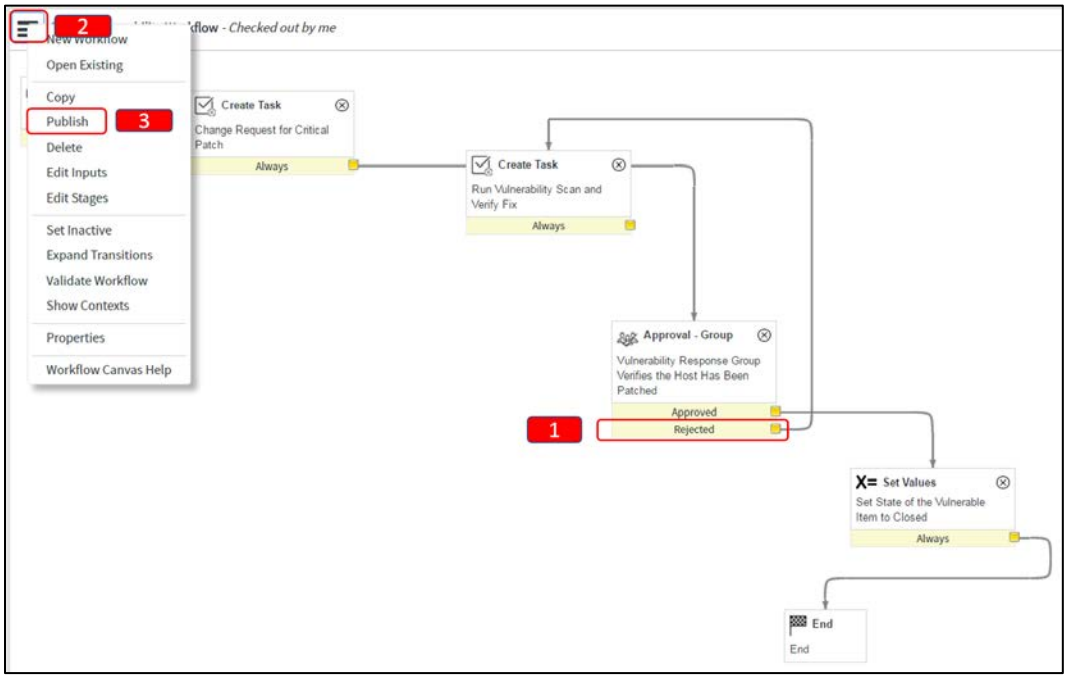
    - Ensure the **Core** tab is selected.
    - Navigate to the **Core Activities > Utilities** folder.
    - Click and drag **Set Values** onto the workflow canvas after the previous **Approval – Group** activity, ensuring that the connecting line turns **blue**.

11. Configure the **Set value** workflow activity.



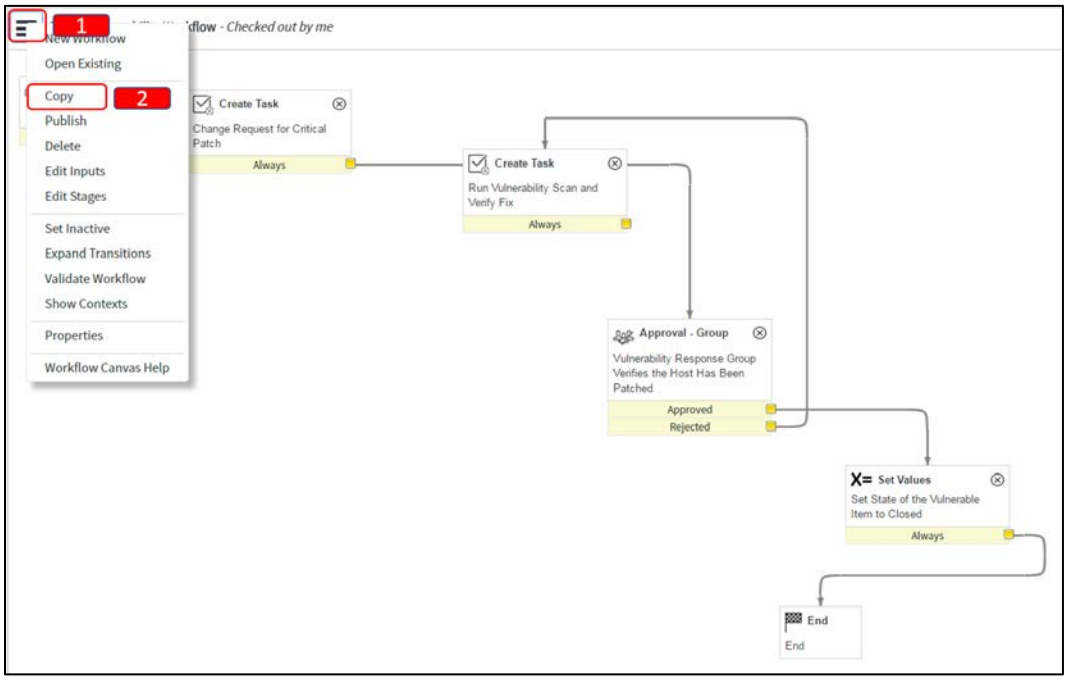
a. Name: **Set State of the Vulnerable Item to Closed**.
b. Set these values: **State – Closed**.
c. Click **Submit**.

12. Finish workflow and publish.



a. Connect the **rejected** approval response up to the previous **Create Task**.
b. Click the **hamburger"**
c. Click **Publish**.

13. Create a second workflow for High Risk Vulnerabilities.

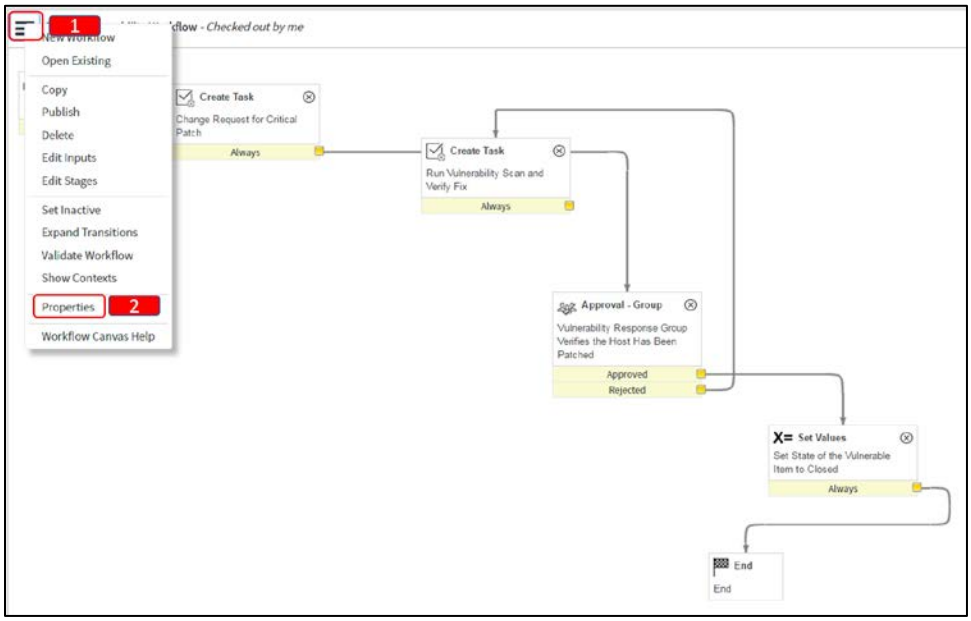


a. Right-click the **hamburger**.
b. Click **Copy** to copy the workflow you just created.

14. Name the workflow for **High Risk Vulnerability Workflow**.

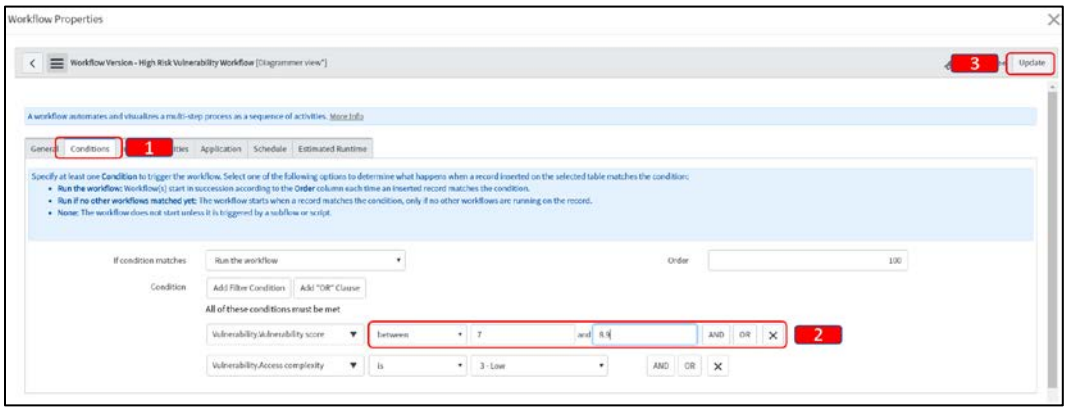


15. Access the workflow properties.



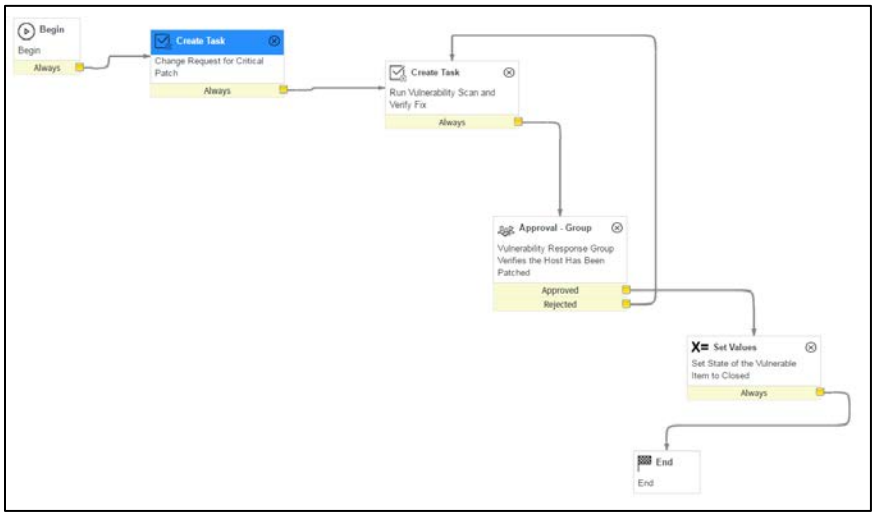
a. Right-click on the **hamburger**.
b. Click **Properties**.

16. Access the workflow properties.

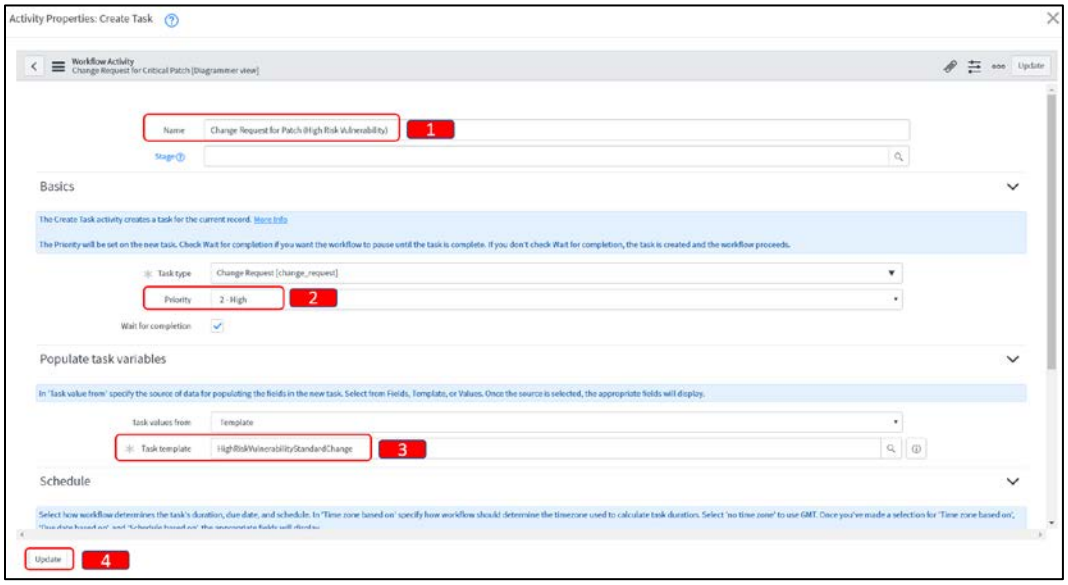


a. Click the **Conditions** tab.
b. Change the **Vulnerability Score** filter condition to **between – 7 and 8.9**.
c. Click **Submit**.

17. Double-click the first **Create Task** in blue to edit the properties.

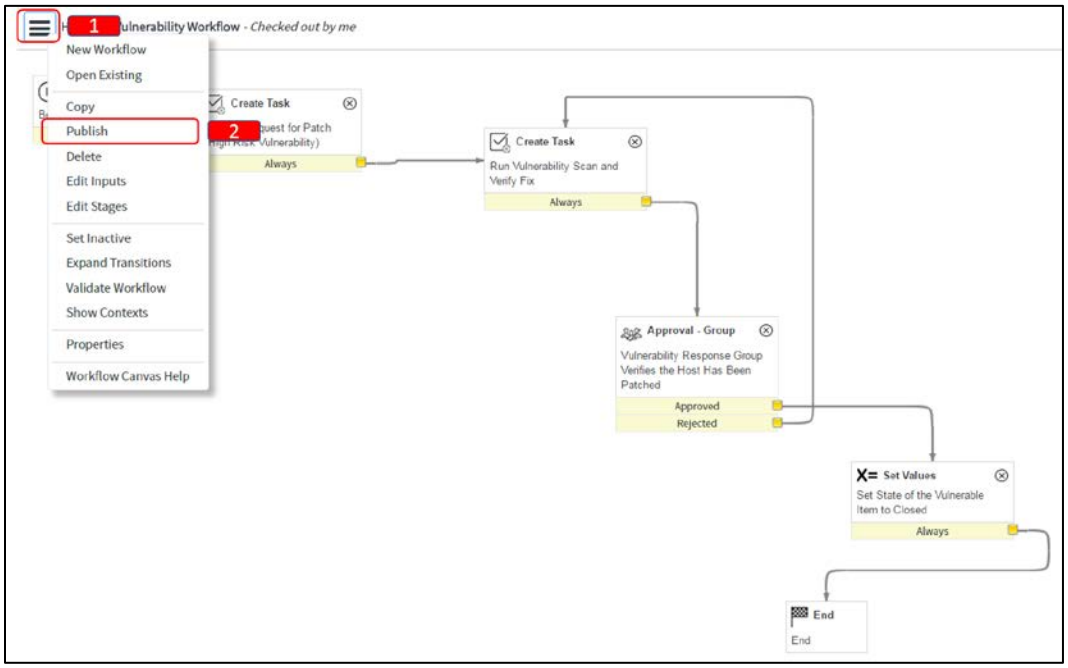


18. Edit the properties.



a. Name: **Change Request for Patch (High Risk Vulnerability)**.
b. Priority: **High**.
c. Task template: **HighRiskVulnerabilityStandardChange**.

19. Finish workflow and publish.



a. Click the **hamburger**.
b. Click **Publish**.

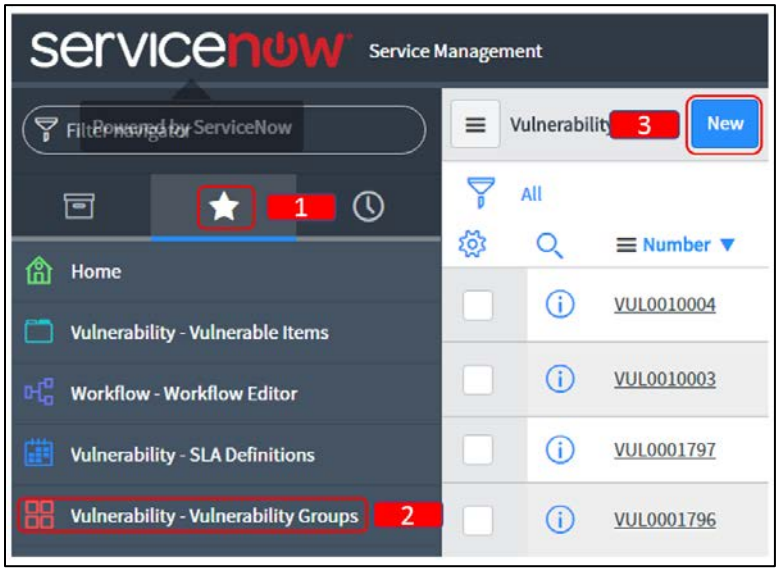
Lab Goal

Move to **QUANTITAINTIVELY MANAGED** on vulnerability management maturity model. Vulnerabilities can be grouped in bulk to assign ownership, ignore, close, accept risk, create exceptions etc. Creating vulnerability groups based on any number of different conditions or criteria is one way to accomplish this. The purpose of this lab is to create three Vulnerability Groups and manage vulnerabilities in bulk.

Lab 3.0
Manage Vulnerabilities in bulk

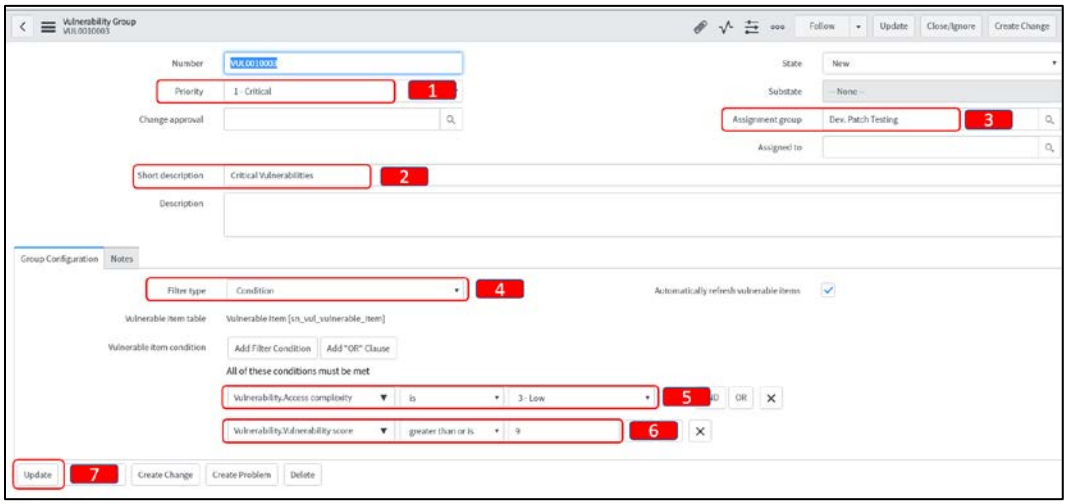
Create the Vulnerability Groups

1. Navigate to **Favorites > Vulnerability – Vulnerability Groups**.

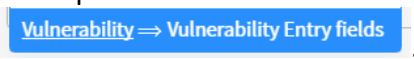


   a. Click **Favorites** tab.
   b. Click **Vulnerability – Vulnerability Groups**.
   c. Click **New**.

2. Enter the conditions for the **Vulnerability Group**.



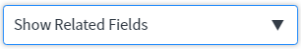
a. Priority: **Critical**.
b. Short description: **Critical Vulnerabilities**.
c. Assignment group: **Dev. Patch Testing**.
d. Filter type: **Condition**.
e. Add a filter condition: Click the arrow to pull down the 

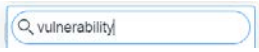
option and type **vulnerability** and choose 

. Click into 

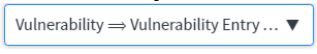
and choose **Access complexity - is – low**.
f. Add a filter condition: Click the arrow to pull down the 

option and scroll to the bottom. Click 

. Click 

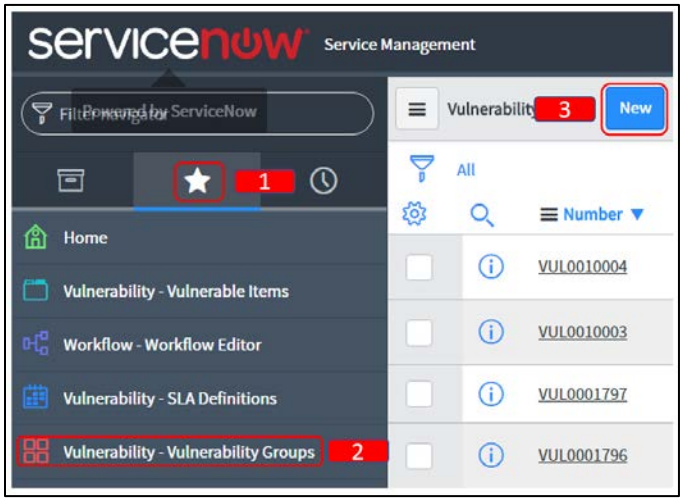
and type **vulnerability** 

and choose 

. Click 

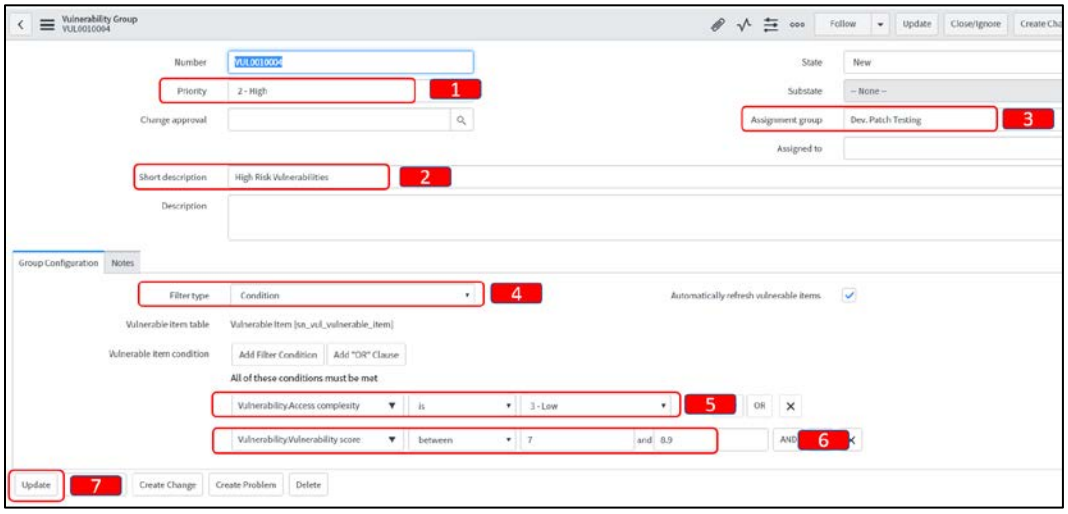
and choose **vulnerability score – greater than or is – 9**.
g. Click **Submit**.

3. To create the 2nd vulnerability group, navigate to **Favorites > Vulnerability – Vulnerability Groups**.

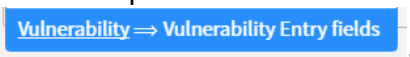


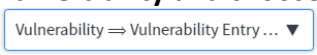
a. Click **Favorites** tab.
b. Click **Vulnerability – Vulnerability Groups**.
c. Click **New.**

4. Enter the conditions for the **Vulnerability Group**.

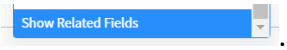


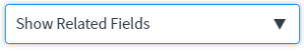
a. Priority: **High.**
b. Short description: **High Risk Vulnerabilities**.
c. Assignment group: **Dev. Patch Testing**.
d. Filter type: **Condition**.
e. Add a filter condition: Click the arrow to pull down the 

option and type **vulnerability** and choose 

. Click 

and choose **Access complexity - is – low**.
f. Add a filter condition: Click the arrow to pull down the 

option. Scroll to the bottom and click 

. Click 

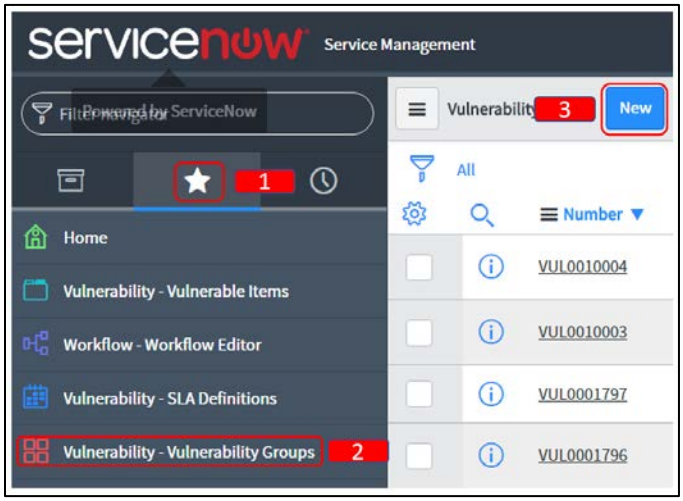
and type **vulnerability** 

and choose 

. Click 

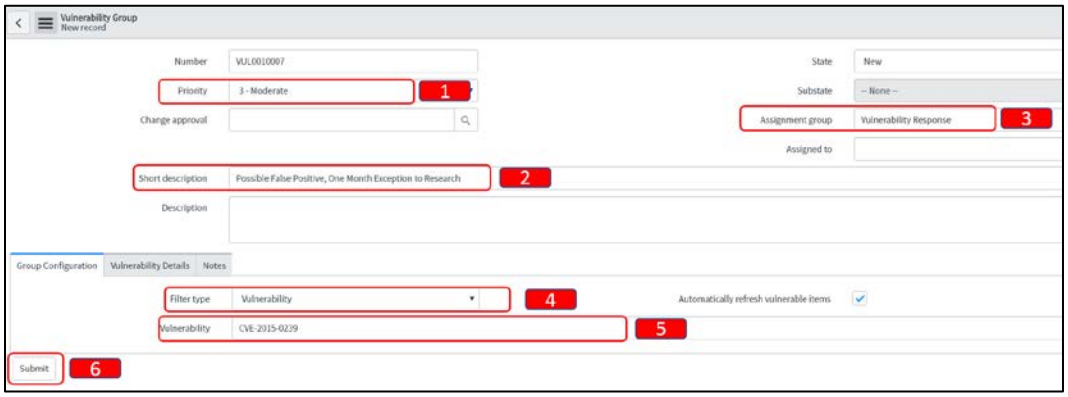
and choose **vulnerability score – between – 7 and 8.9**.
g. Click **Submit**.

5. To create the 3rd vulnerability group, navigate to **Favorites > Vulnerability – Vulnerability Groups**.



a. Click **Favorites** tab.
b. Click **Vulnerability – Vulnerability Groups**.
c. Click **New**.

6. Enter the conditions for the **Vulnerability Group**.



a. Priority: **Moderate**.
b. Short description: **Possible False Positive, One Month Exception to Research**.
c. Assignment group: **Vulnerability Response**.
d. Filter type: **Vulnerability**.
e. Vulnerability: **CVE-2015-0239**.
f. Click **Submit**.

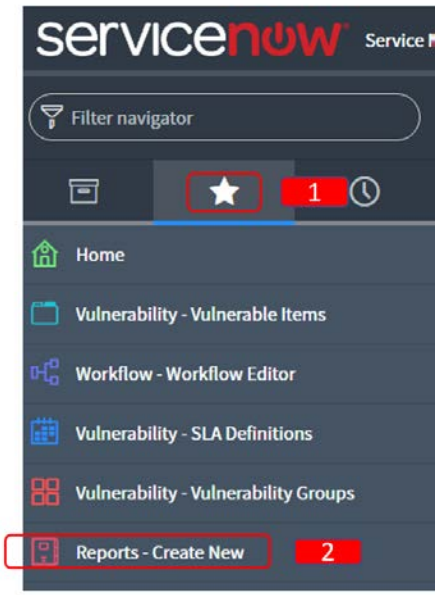
Lab Goal

Move to **OPTIMIZED** on vulnerability management maturity model. Any data point within service now can be used to report on the vulnerability management process. The purpose of this lab is to create reports and dashboards for visibility into the vulnerability management process.

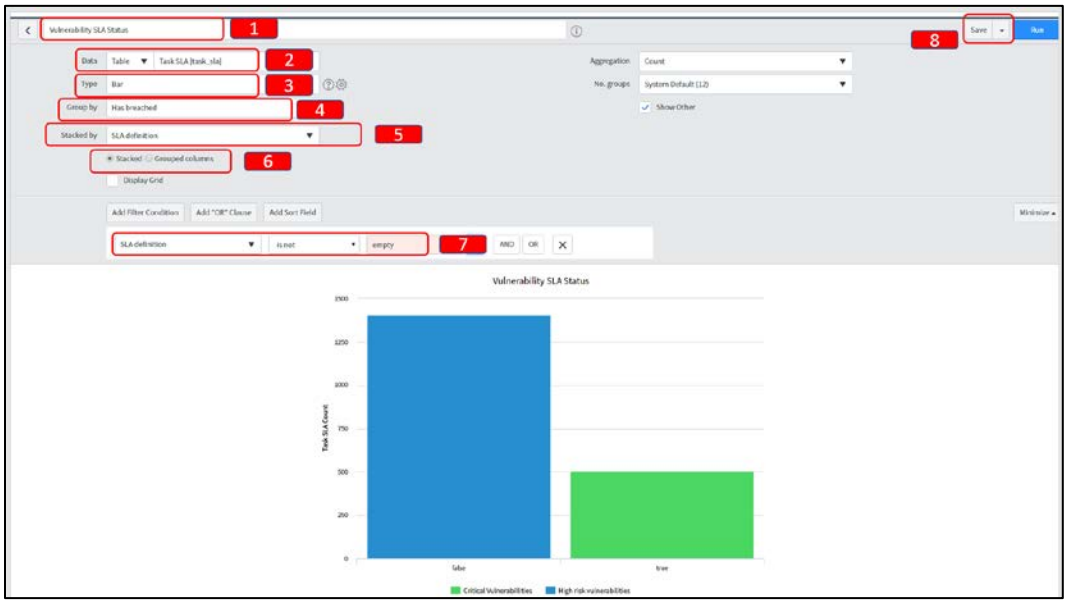
Lab 3.0 Complete Visibility Leads to Process Improvement

Create the Vulnerability Groups

1. Navigate to **Favorites > Reports – Create New**.

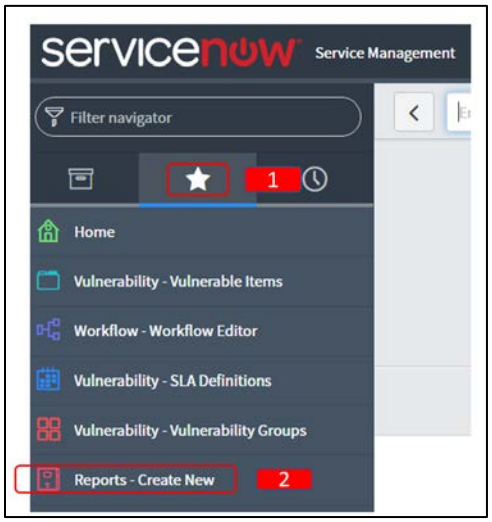


2. Enter the conditions for the **Report**.

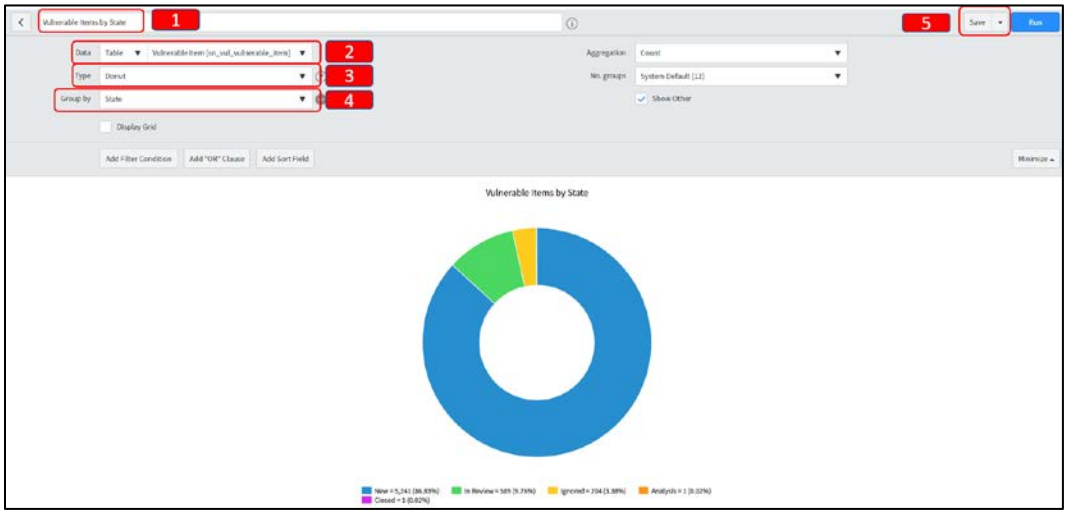


a. Name: **Vulnerability SLA Status**.
b. Data: **Table – Task sla [task_sla]**.
c. Type: **Bar**.
d. Group by: **Has breached**.
e. Stacked by: **SLA definition**.
f. Choose: **Stacked**.
g. Add Filter Condition: **SLA definition – is not – empty**.
h. Click **Save**.

3. Navigate to **Favorites > Reports – Create New**.

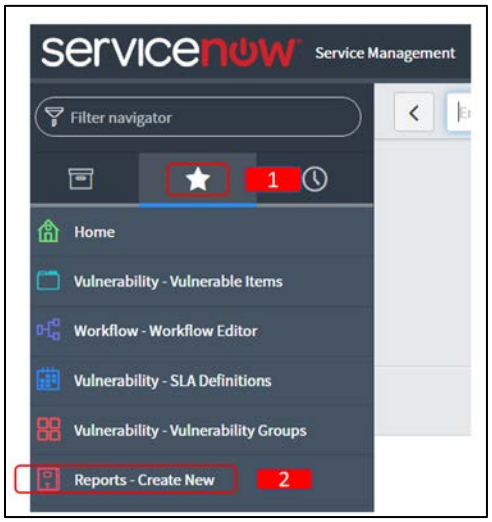


4. Enter the conditions for the **Report**.



a. Name: **Vulnerable Items by State**.
b. Data: **Vulnerable Item – [sn_vul_vulnerable_item]**.
c. Type: **Donut**.
d. Group by: **State.**
e. Click **Save**.

5. Navigate to **Favorites > Reports – Create New**.



6. Enter the conditions for the **Report**.



a. Name: **Current Open Exceptions**.
b. Data: **Vulnerable State Change Approval – [sn_vul_change_approval]**.
c. Type: **List**.
d. Group by: **None**.
e. Click **Save**.

Lab Goal

Move to **QUANTITAINTIVELY MANAGED** on vulnerability management maturity model. After you define SLAs, create vulnerability workflows, and create pertinent reports, you can explore what this looks like and how the platform can transform the vulnerability management maturity level of an organization.

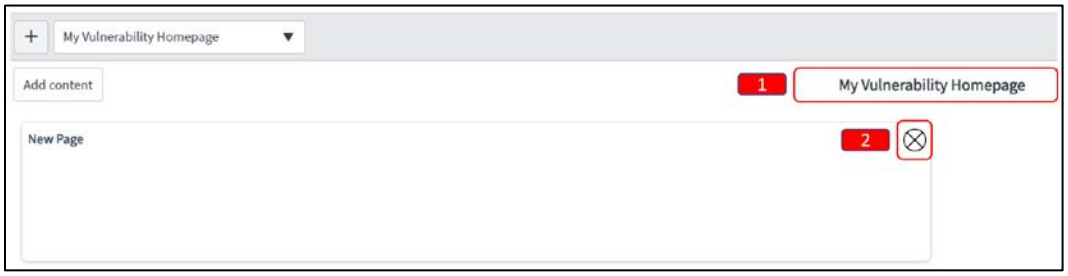
Lab 3.0
The Whole Picture

Create a Vulnerability Homepage

1. Navigate to **Favorites > Reports – Create New**.

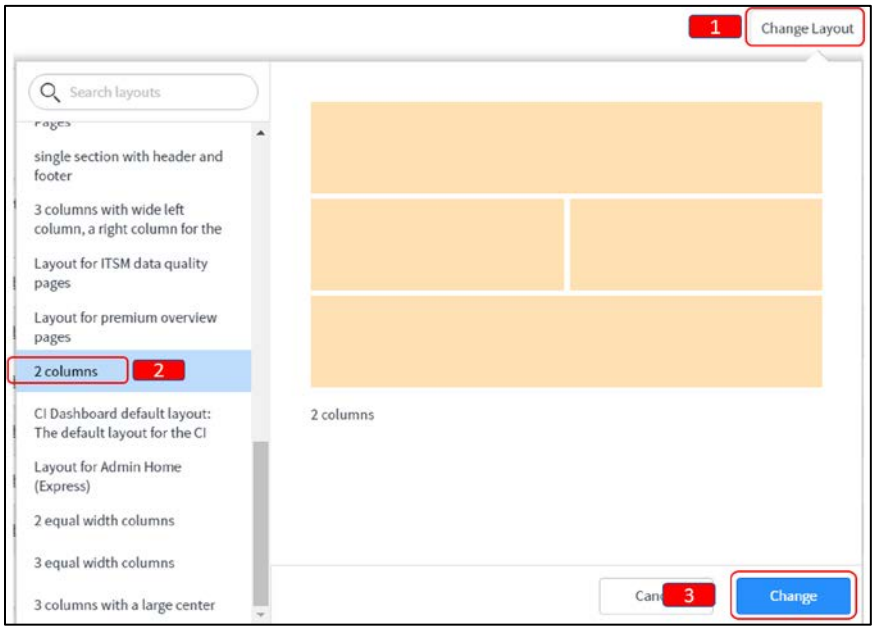


2. Change the name of the **homepage**.



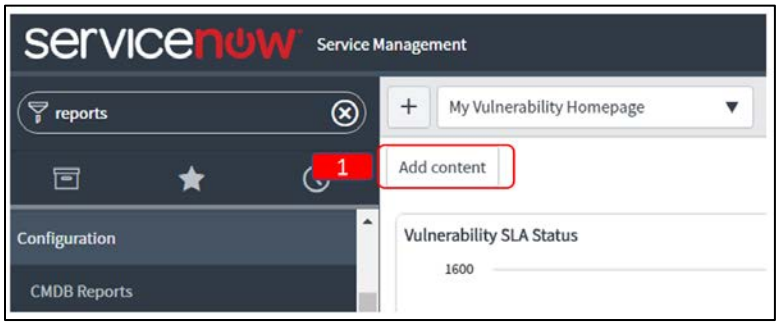
   a. Click **My Homepage1** in the middle of the screen and change to **My Vulnerability Homepage**.
   b. Hover over the top right of the **New Page Widget** to reveal the **X** and click to remove.

3. Change the layout and click **change layout**.



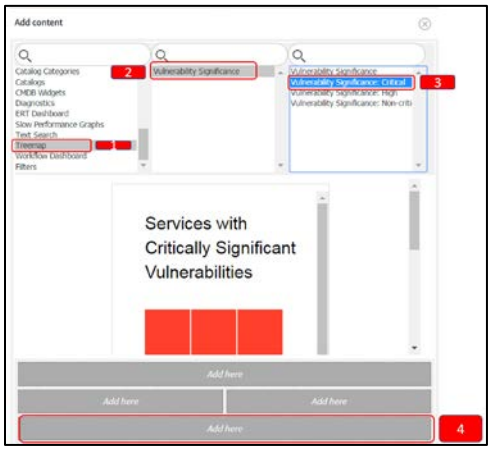
a. Click **Change Layout**.
b. Scroll to the bottom of the list and choose **2 columns**.
c. Click **Change**.

4. Add Content.



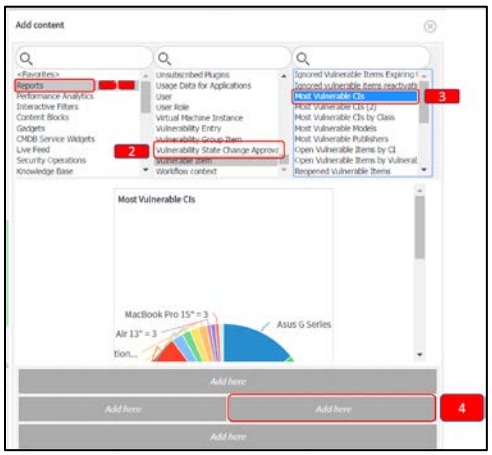
a. Click **Add content**.

5. Add reports to homepage.



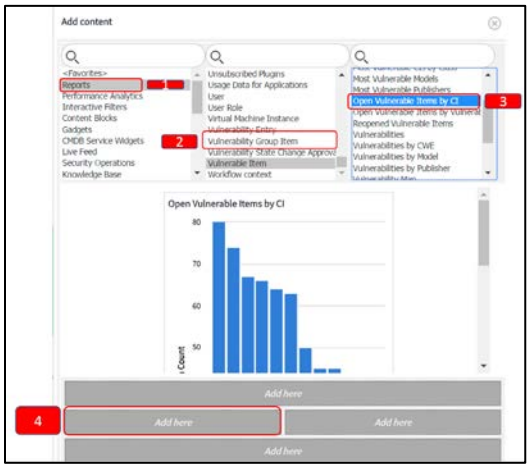
a. Click **Treemap**.
b. Click **Vulnerability Significance**.
c. Click **Vulnerability Significance: Critical**.
d. Click **Add here**.

6. Add (additional) reports to homepage.



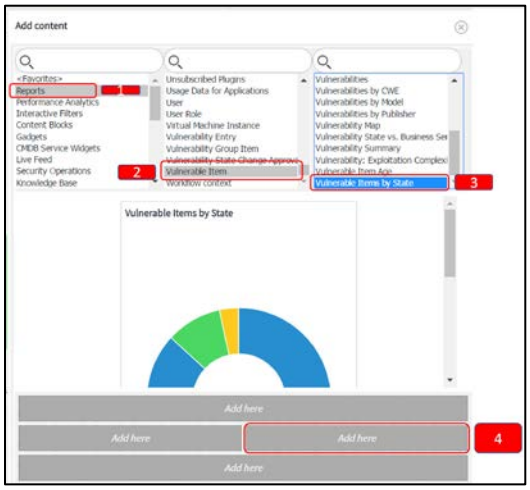
a. Click **Reports**.
b. Click **Vulnerable Item**.
c. Click **Most Vulnerable Cis**.
d. Click **Add here**.

7. Add (additional) reports to homepage.



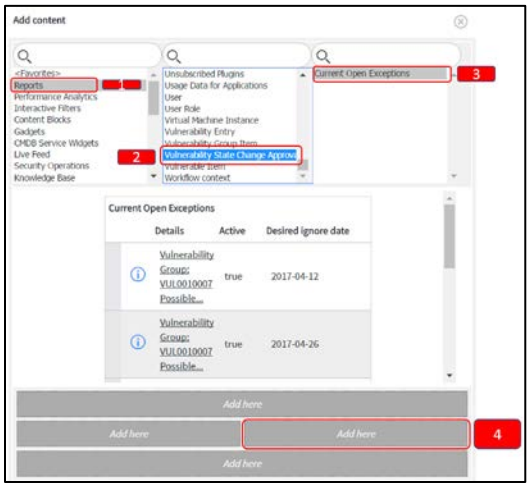
a. Click **Reports**.
b. Click **Vulnerable Item**.
c. Click **Open Vulnerable Items by CI**.
d. Click **Add here**.

8. Add (additional) reports to homepage.



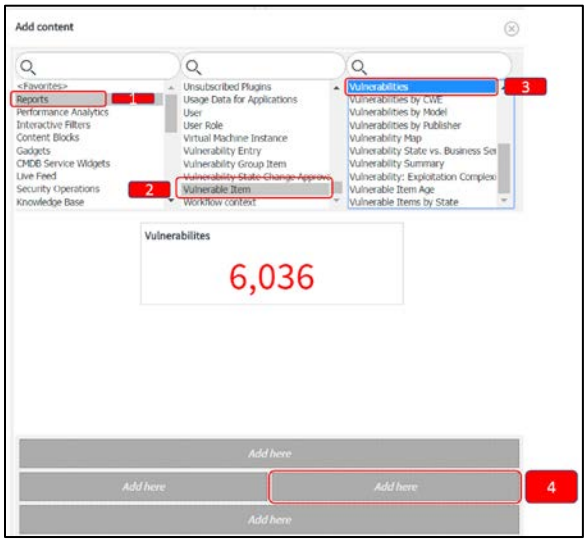
a. Click **Reports**.
b. Click **Vulnerable Item**.
c. Click **Vulnerable Items by State**.
d. Click **Add here**.

9. Add (additional) reports to homepage.



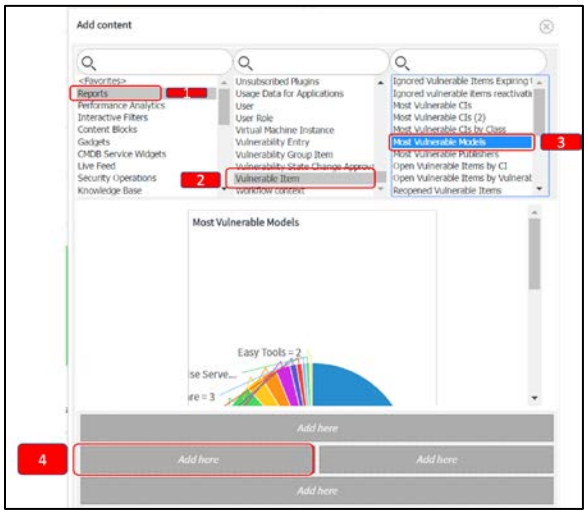
a. Click **Reports**.
b. Click **Vulnerability State Change Approval**.
c. Click **Current Open Exceptions**.
d. Click **Add here**.

10. Add (additional) reports to homepage.



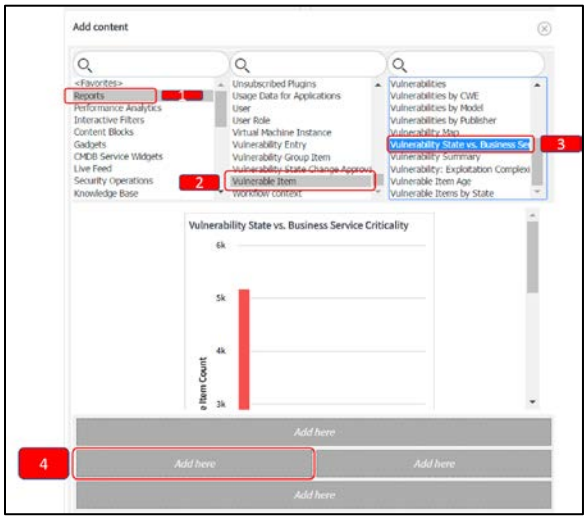
a. Click **Reports**.
b. Click **Vulnerable Item**.
c. Click **Vulnerable Items by State**.
d. Click **Add here**.

11. Add (additional) reports to homepage.



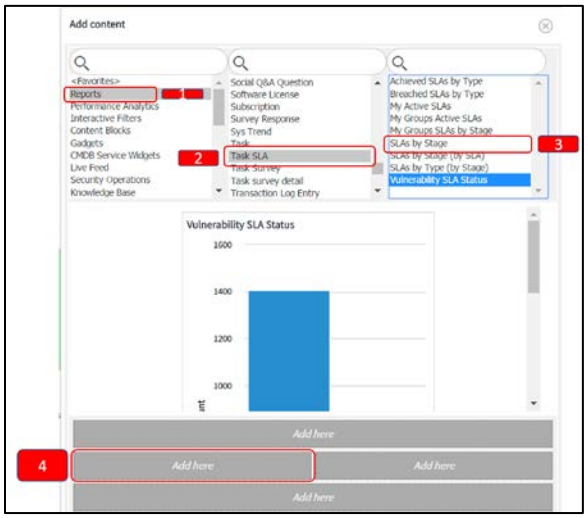
a. Click **Reports**.
b. Click **Vulnerable Item.**
c. Click **Most Vulnerable Models.**
d. Click **Add here**.

12. Add (additional) reports to homepage.



a. Click **Reports.**
b. Click **Vulnerable Item.**
c. Click **Vulnerability State vs. Business Service Criticality.**
d. Click **Add here**.

13. Add (additional) reports to homepage.



a. Click **Reports**.
b. Click **Task**.
c. Click **SLAs by Stage**.
d. Click **Add here**.