Lab Guide

Proving Compliance of Security Controls

Syra Arif & David Perodin

Default Login / Password: Knowledge17

admin / Knowledge17

itil / Knowledge17

employee / Knowledge17

Lab Sponsored by Microsoft Azure



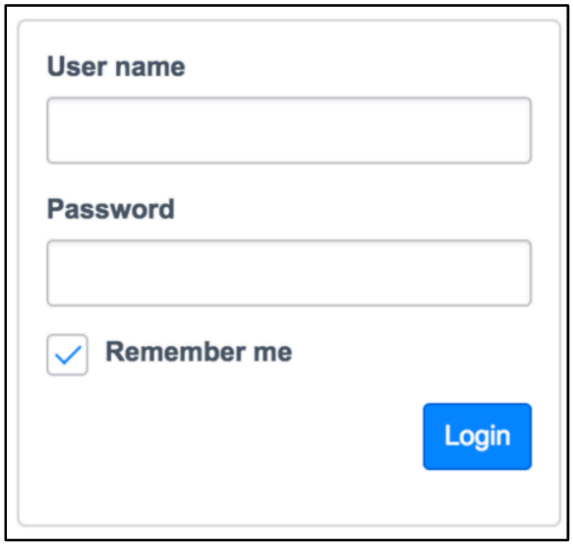
This
Page
Intentionally
Left
Blank

Lab Goal

Many organizations struggle to manage the unrelenting onslaught of disruptive cyber-attacks, increasing B2B accountability, security audits (for HIPAA, PCI, ISO 27002, etc.), mounting regulatory oversight, and the relentless tidal wave of event noise. This has resulted in CISO spending countless nights grasping for an efficient response to the intensifying challenge. The need for a proven good practice for managing the entire lifecycle of a security control has become paramount. ServiceNow enables an integrated end to end process for managing risk and security in the enterprise. In this session, learn about a united solution; bringing the power of Security Operations and Governance, Risk, and Compliance. We will cover the lifecycle of a security control; from policy, to implementation, from continuous monitoring to failure remediation.

Getting Started – Log on to Your Lab Instance

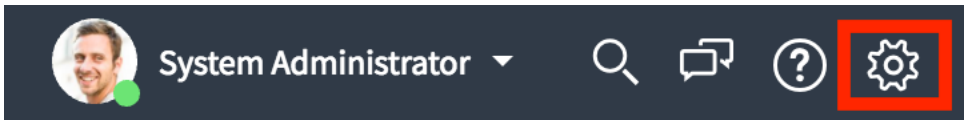
1. Navigate to the unique instance URL provided to you.



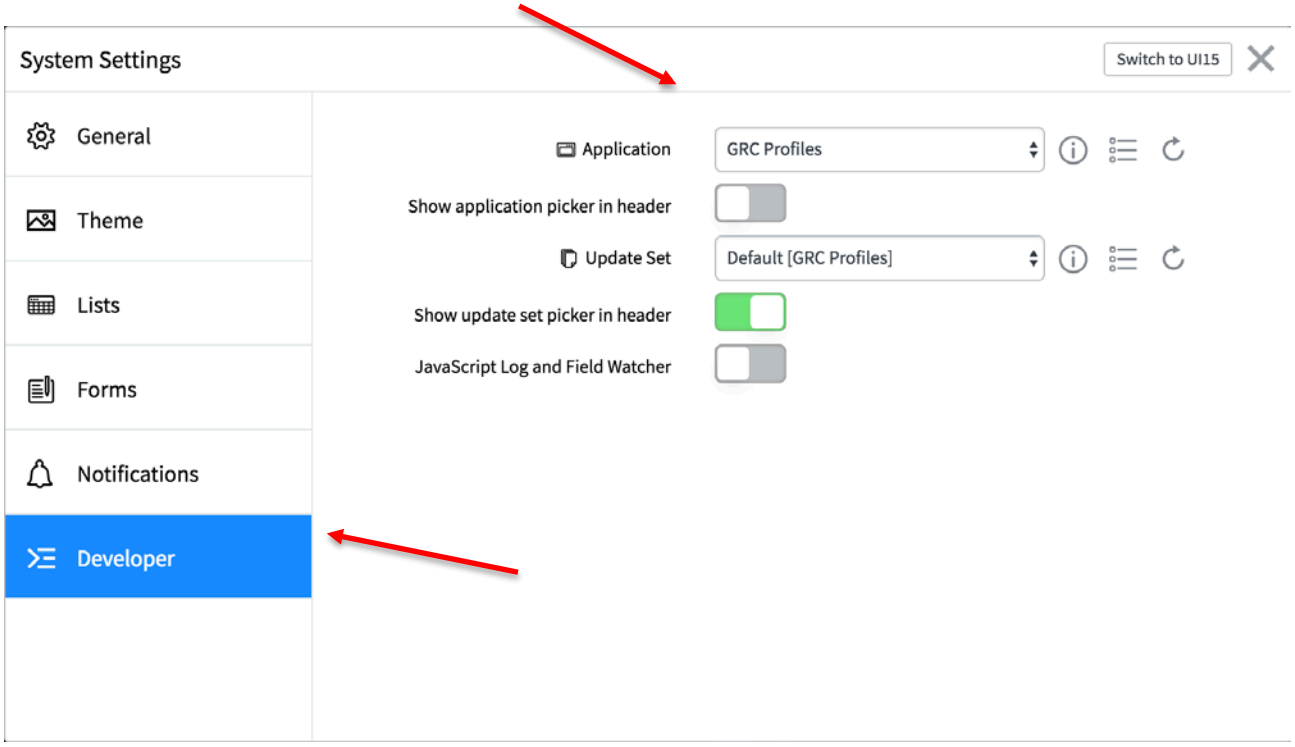
2. Log on with provided credentials on title page of this lab guide.

3. Change Application Scope to **GRC Profiles**.

4. Click the gear icon in the top right of your instance (to the right of your logged in user name).



5. Click **Developer -> Change Application to GRC Profiles -> Exit**.



Great! You are done with this part of the lab!

Proceed to the next section when ready.

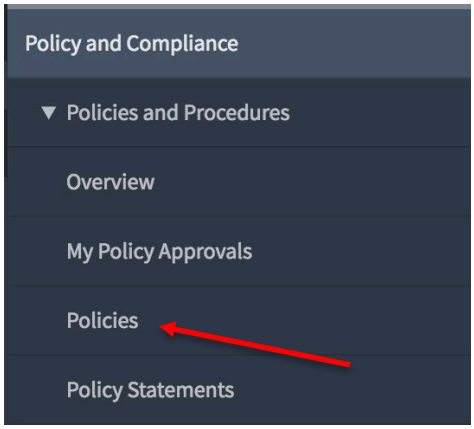
Lab Goal

This lab explains the processes of creating a policy, associating policy statements with policies, creating and testing controls, and reviewing indicators. This setup is critical to reviewing any non-compliant controls in the Policy Overview dashboard.

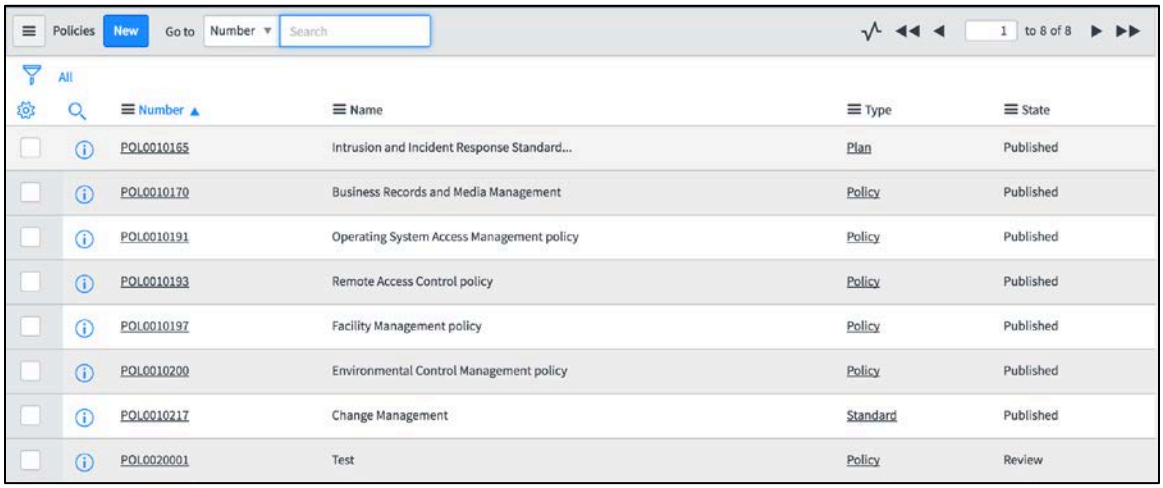
1. Type **Policies** into the Filter navigator box to locate the Policies and Compliance application.



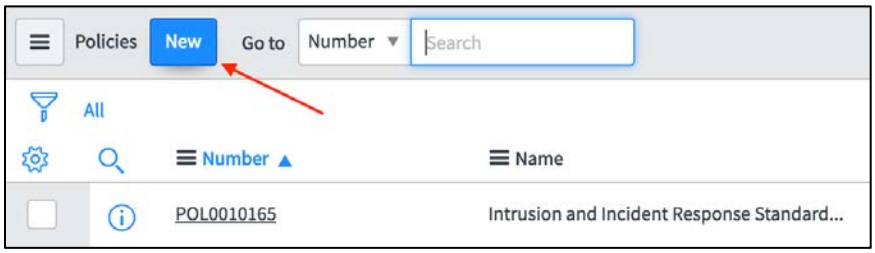
2. Select the Policies module under the Policies and Procedures application.



3. The Policies list appears.

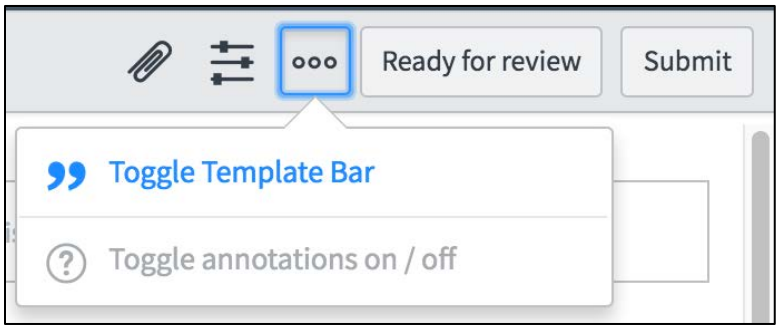


4. Click the **New** button to create a new policy.



5. Click on the  icon in the top right-hand corner and select 'Toggle Template Bar'.

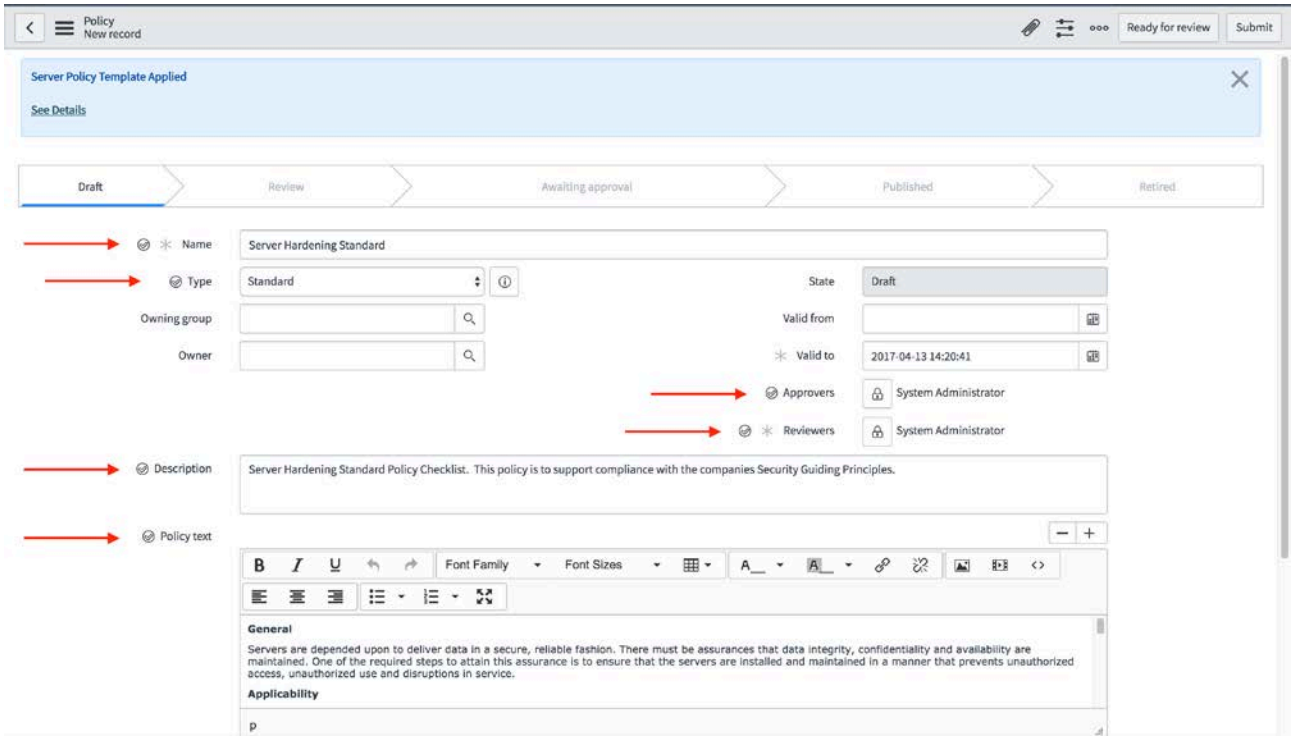
Note: To make this process easier, there is a **Server Policy** template that can be used to fill in the fields.



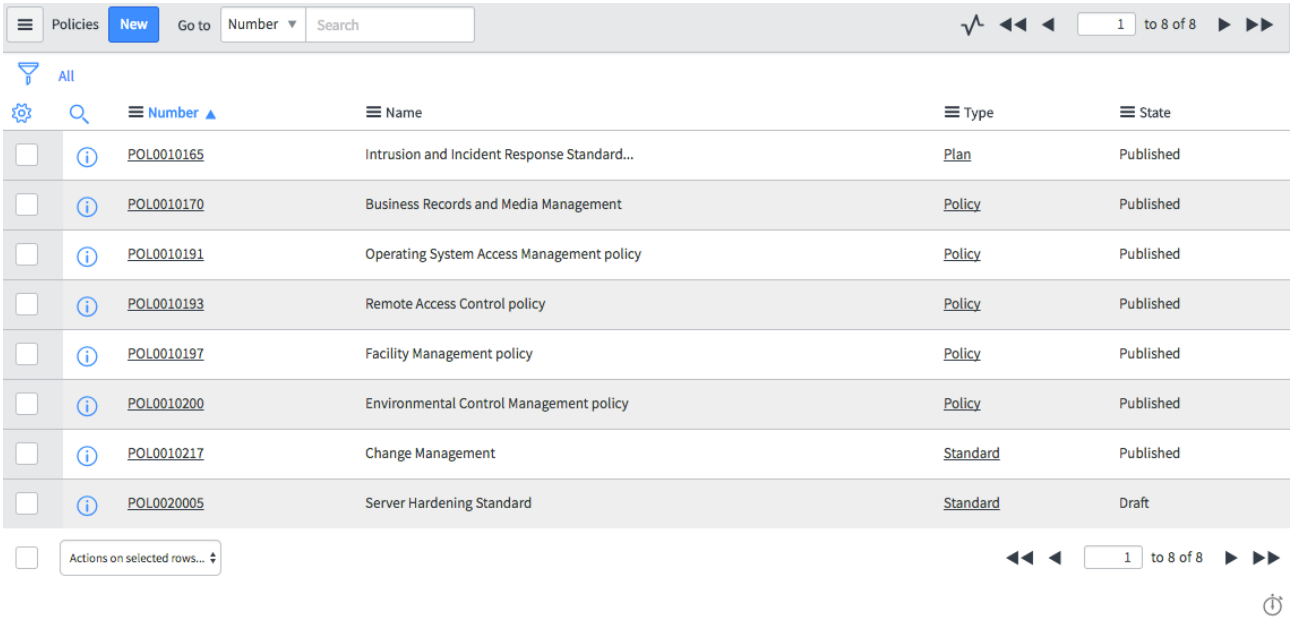
Scroll to the bottom of the new record and select the template.



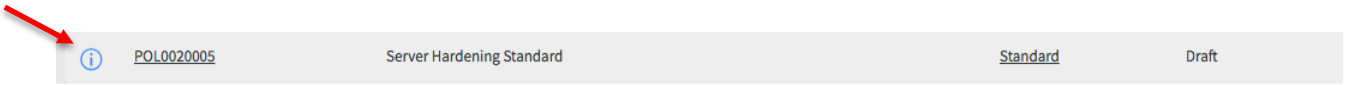
6. The fields will be populated with the necessary data.



7. Click **Submit** to create the new policy record and you will be returned to the list view of all policies.

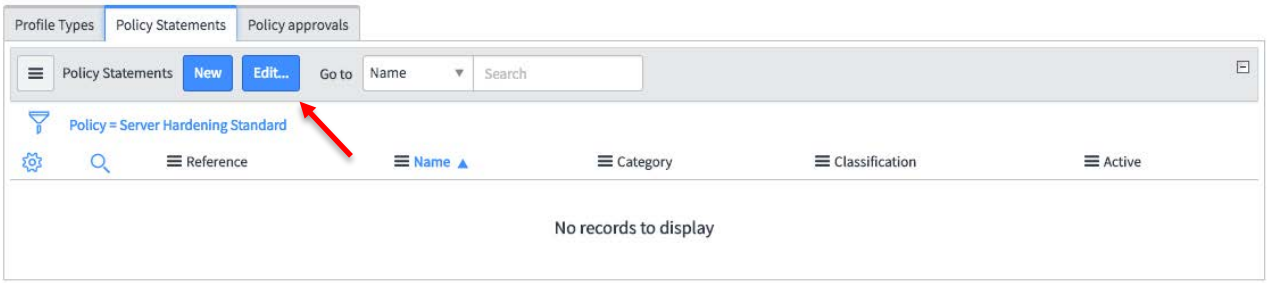


8. Open the policy just created (Server Hardening Standard) by clicking on the **POL** number, or the information icon .

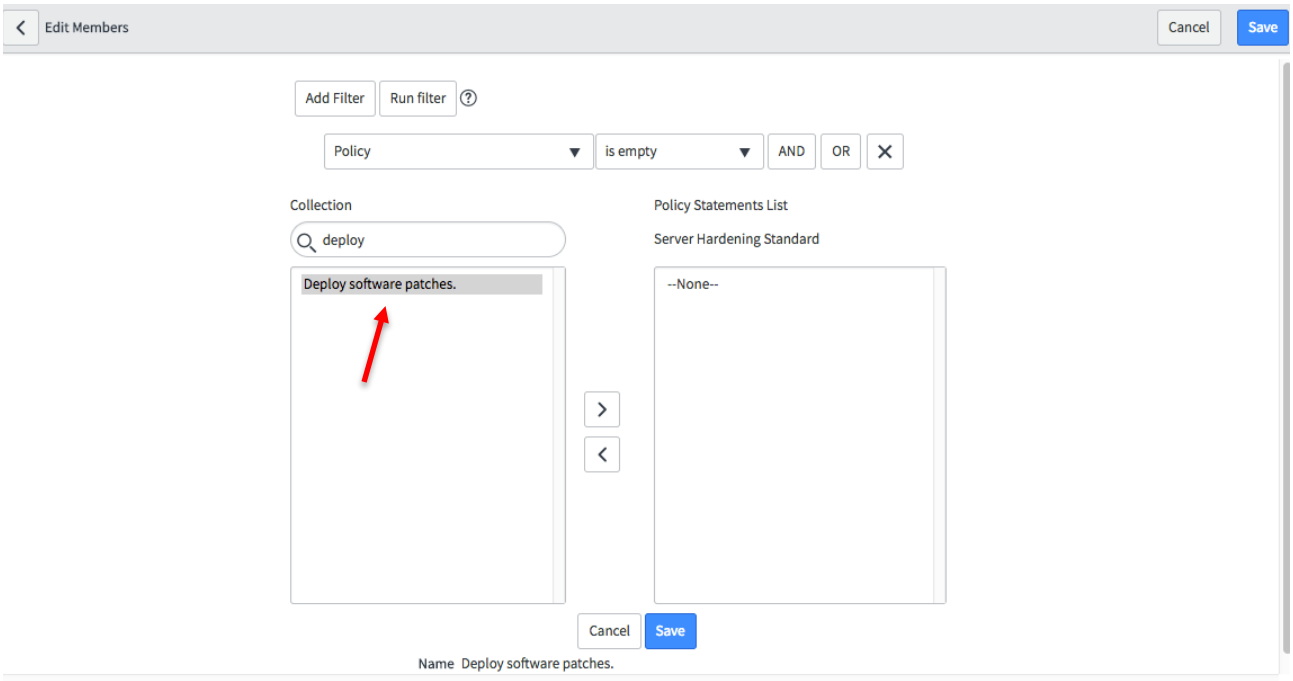


The next step demonstrates the process of creating a *policy statement* that will be tied to the previously created *policy.*

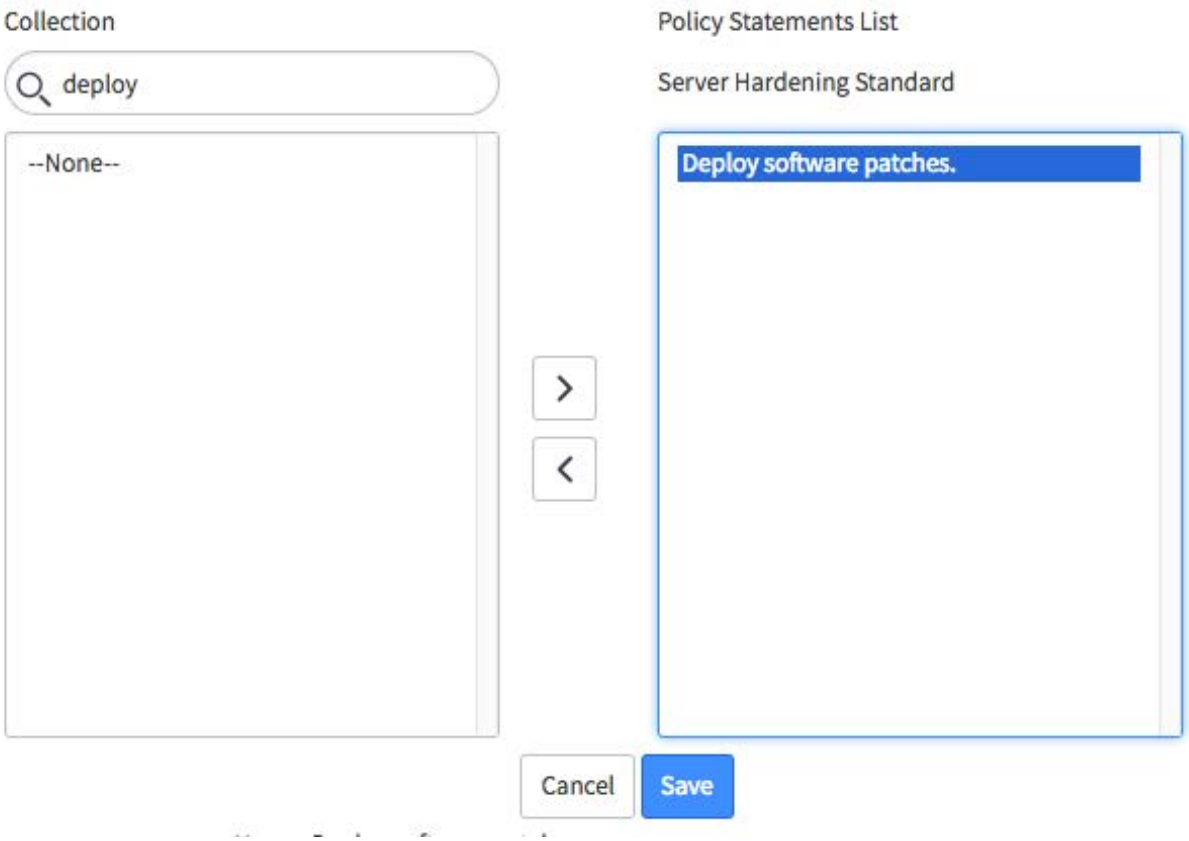
9. Scroll to the bottom of the Policy record and select the Policy Statements tab. Click **Edit**.



10. In the Collection field, type deploy. Double-click on the returned result, Deploy Software Patches. The Policy Statement will move from the left to the right column.

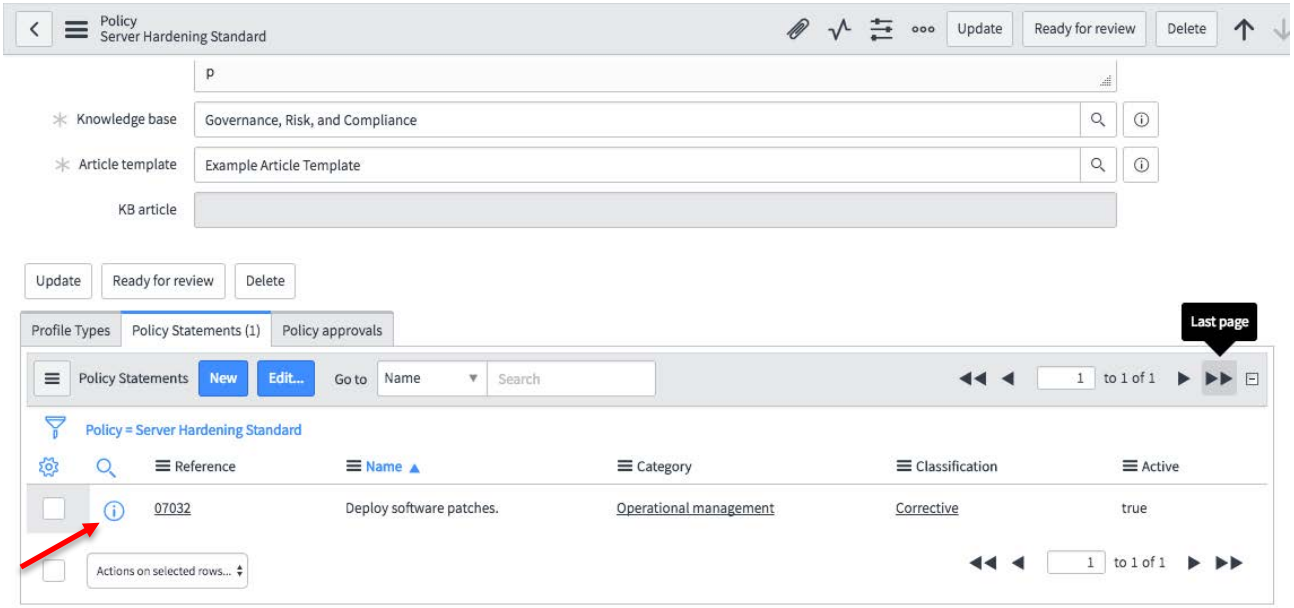


11. Click **Save** in either the upper-right hand corner or below the columns.



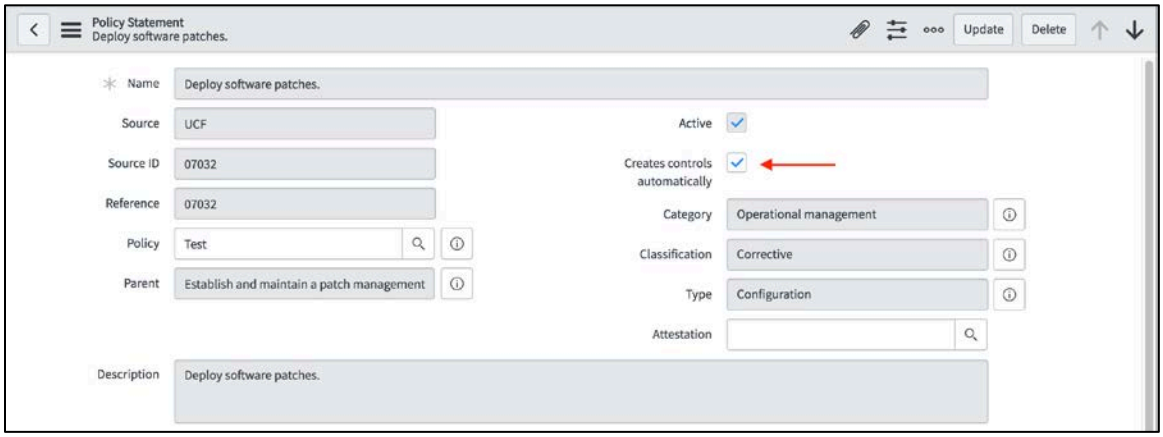
12. You will see the Policy Statement associated with the Policy.

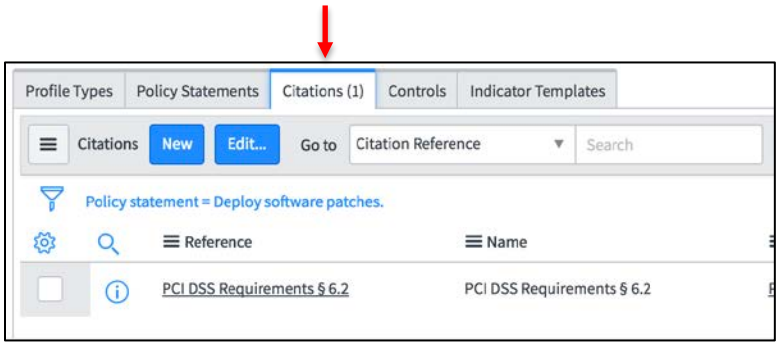
13. Select **Deploy software patches** by either clicking on the information icon ⓘ or the reference number associated to it.



14. The next screen displays the record.

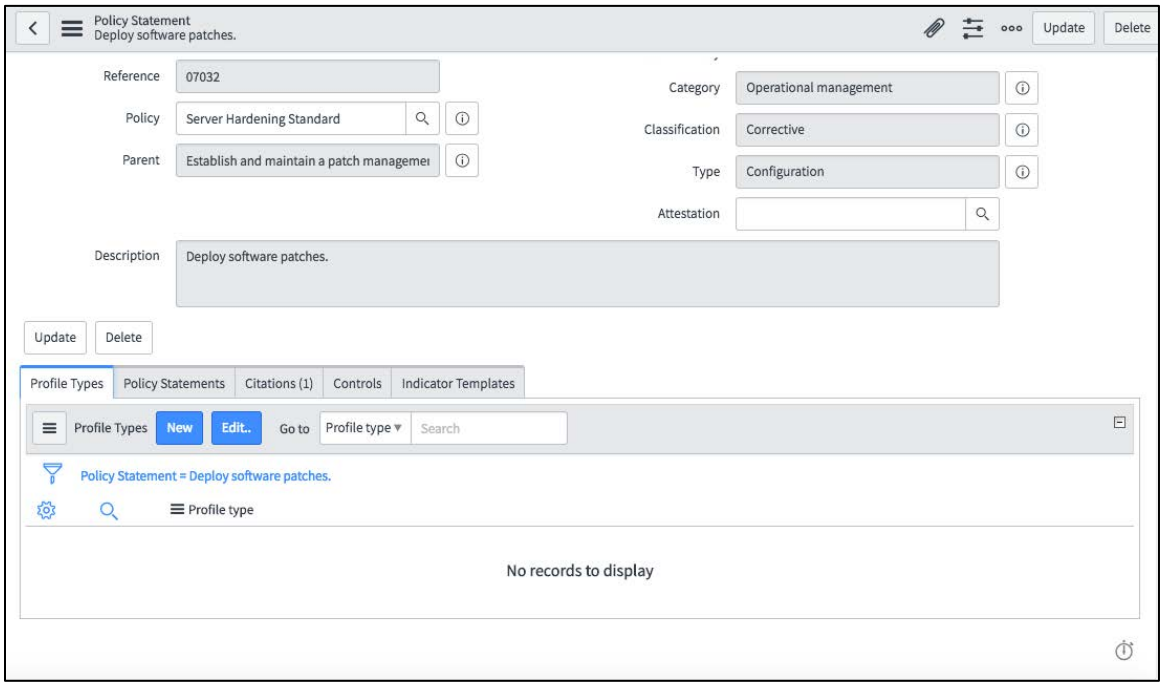
15. Place a checkmark in the **Creates controls automatically** box. Scroll to the bottom of the record and note the **Citations** tab with the imported PCI DSS Requirement.





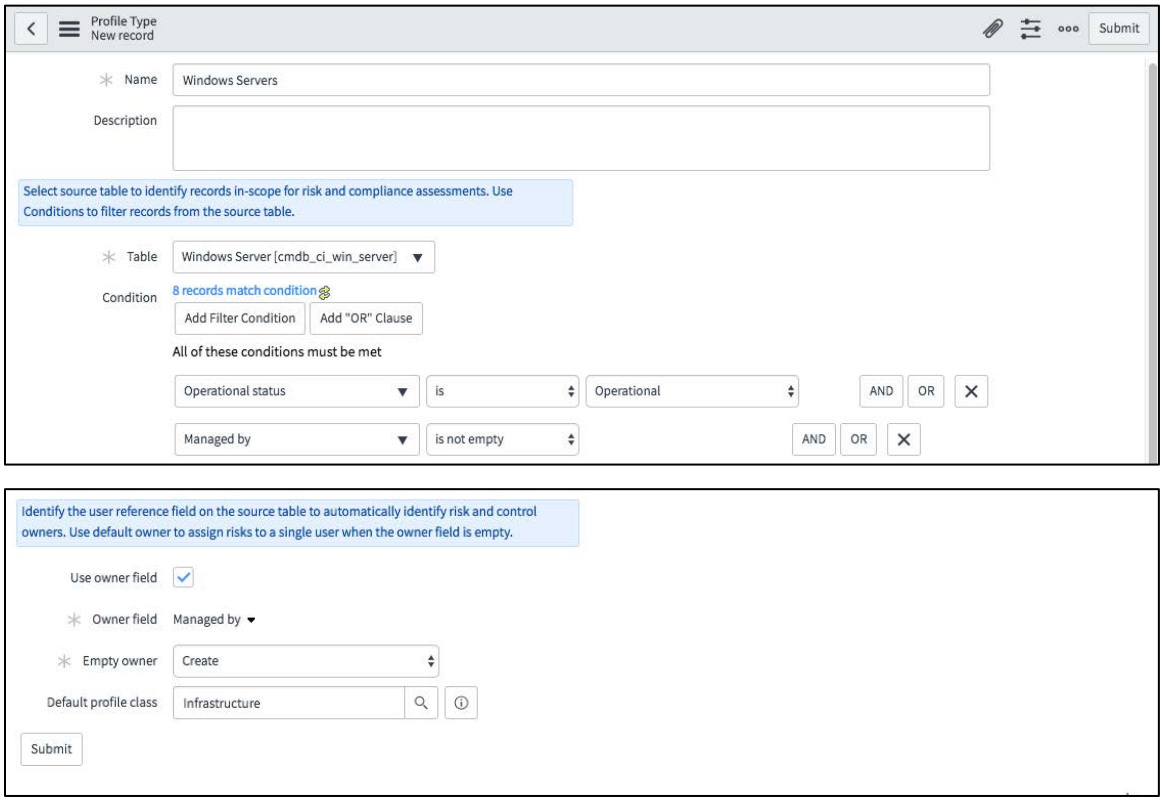
Task 2

1. Navigate to the profile types tab. Select **New**.

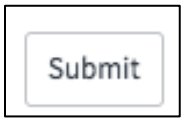


2. Fill in and select the following information on the Profile Type record:

   Name: **Windows Servers**
   Table: **Windows Server [cmdb_ci_win_server]** *note that 8 records match the condition
   Condition: **Operational Status is Operational**
   Owner field: **Managed by**
   Default profile class: **Infrastructure**

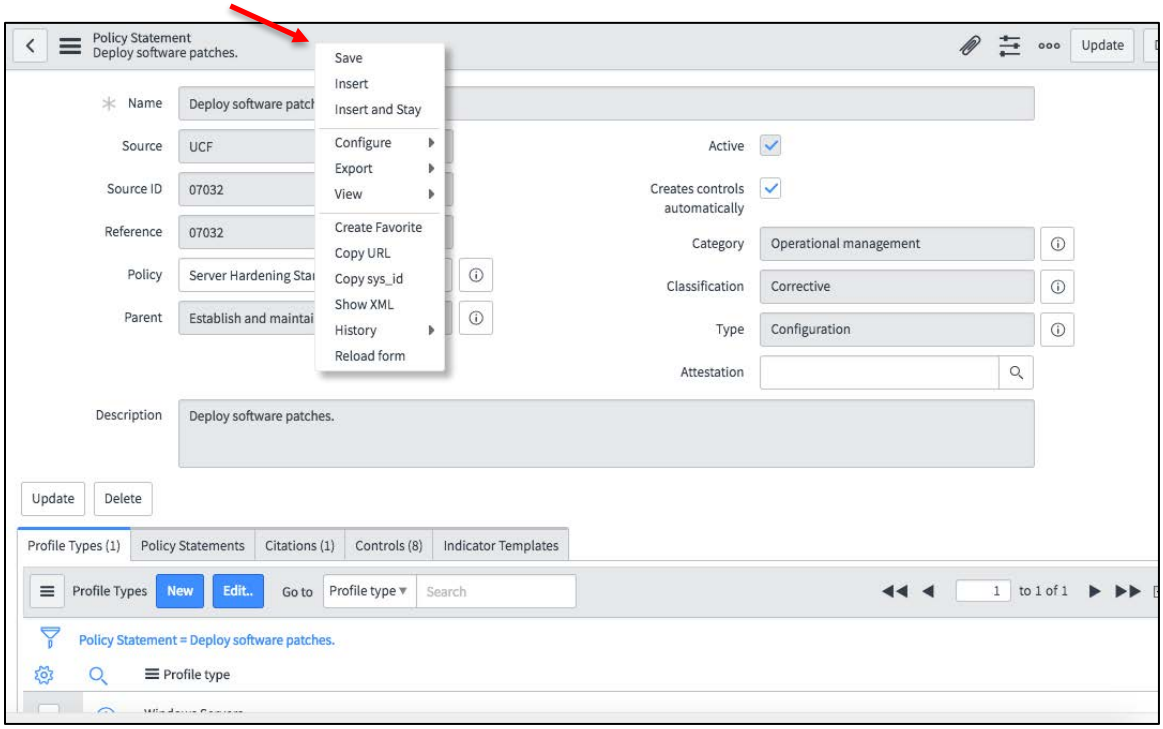


3. Click **Submit**.

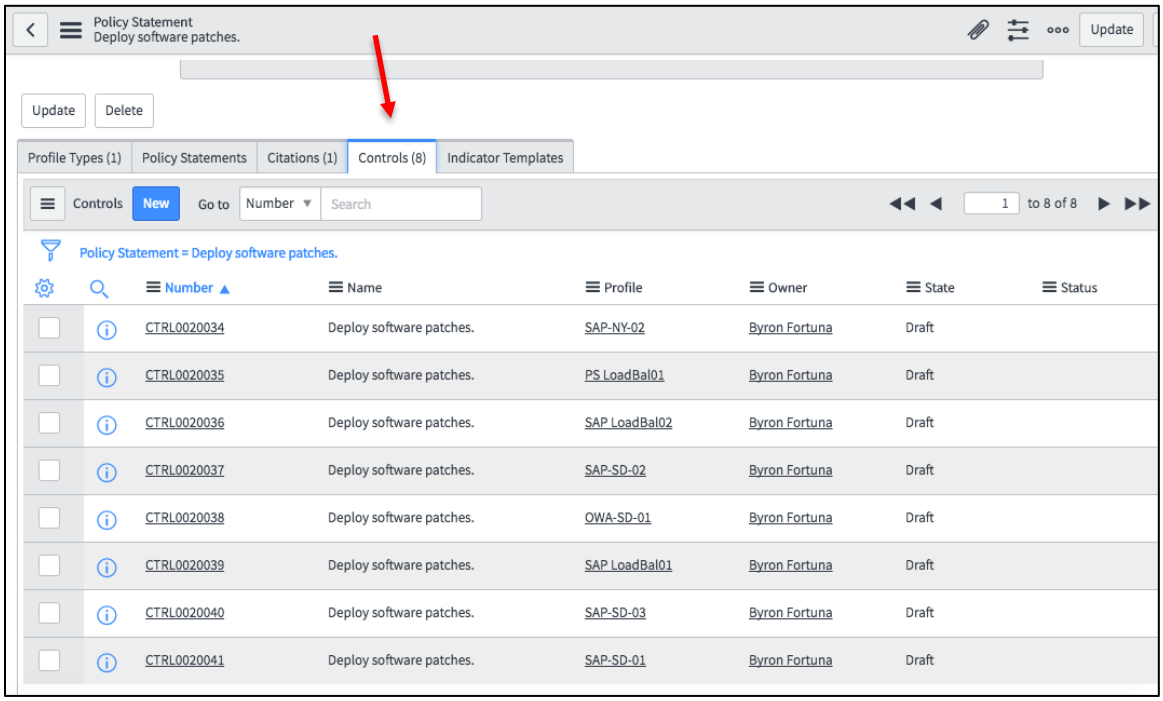


Note: There will be a message stating *"Items are currently generating for this content, Click here to see progress."* Saving or reloading the form will make this disappear.

4. The Profile Type **Windows Server** is now associated to the Policy Statement. Navigate to the top. Right-click and select **Reload form**.

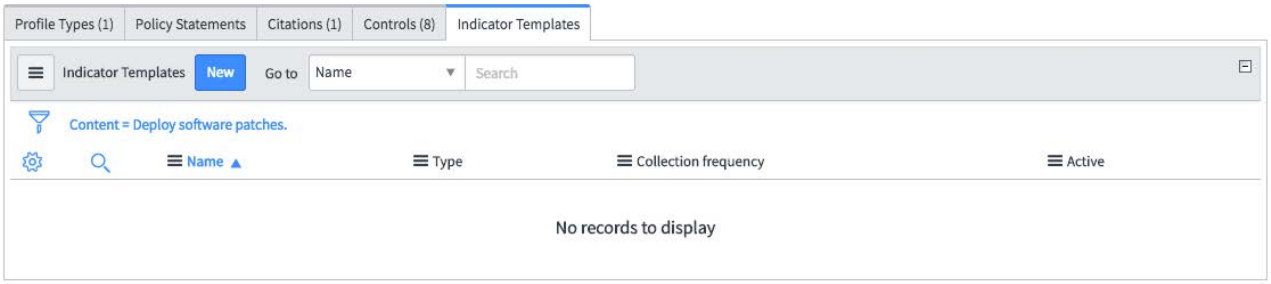


5. There are 8 controls associated with the policy statement.

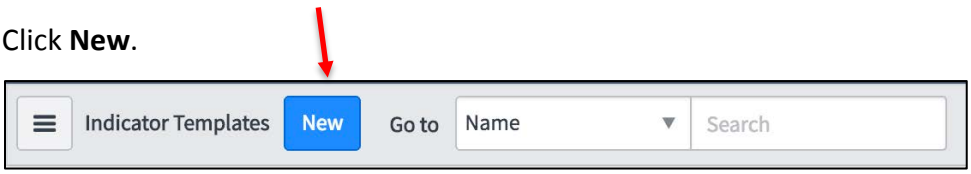


Task 3

1. Navigate to **Indicator Templates** tab.



2. Click **New**.

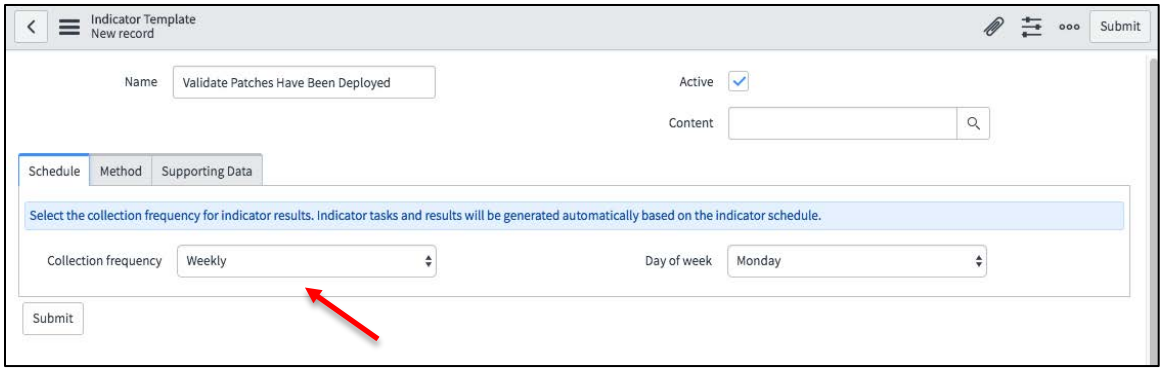


3. Fill out the following information:

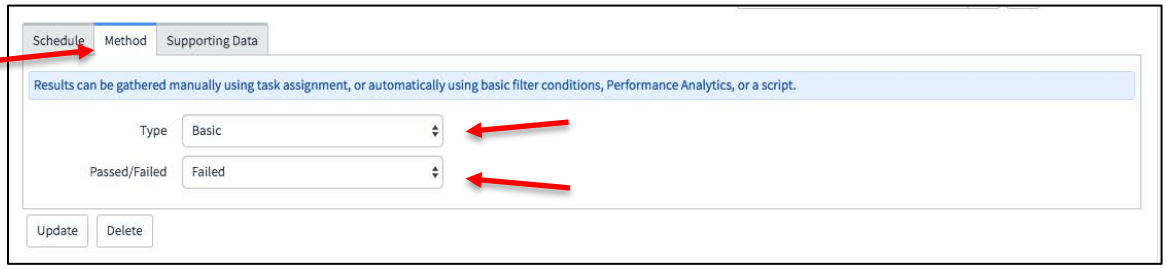
   Name: **Validate Patches Have Been Deployed**



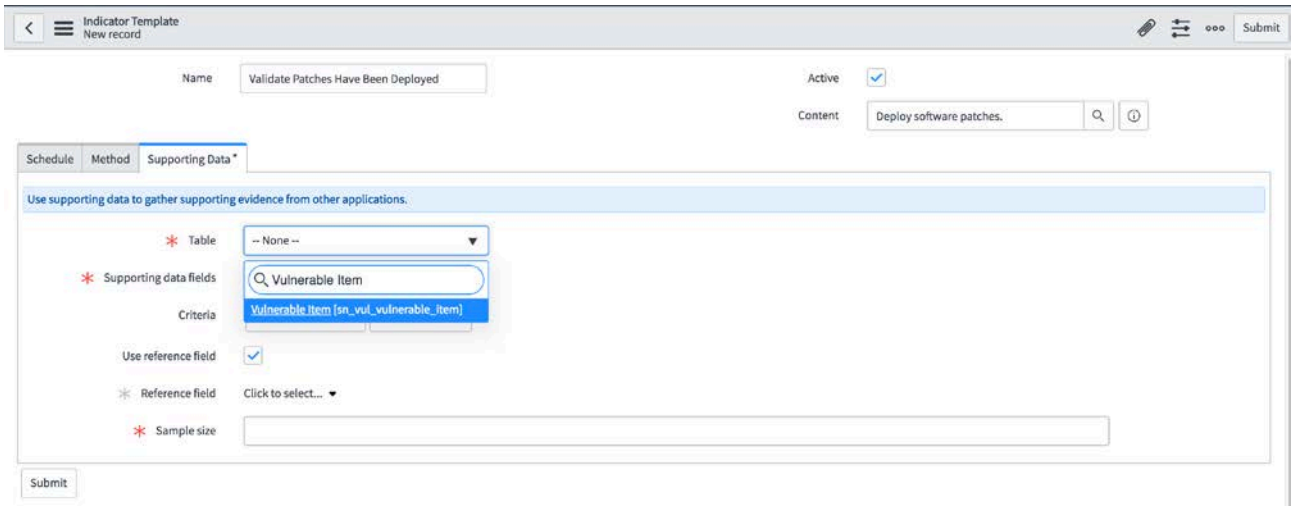
4. On the schedule tab, set Collection frequency to **Weekly** and Day of week to **Monday**



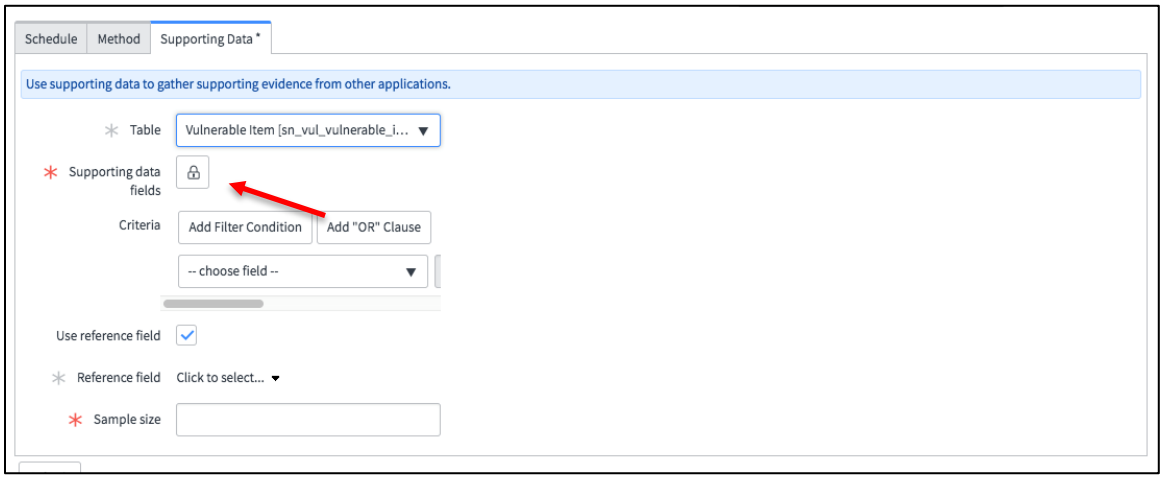
5. On the Method tab, set Type to **Basic** and Passed/Failed to **Failed**.



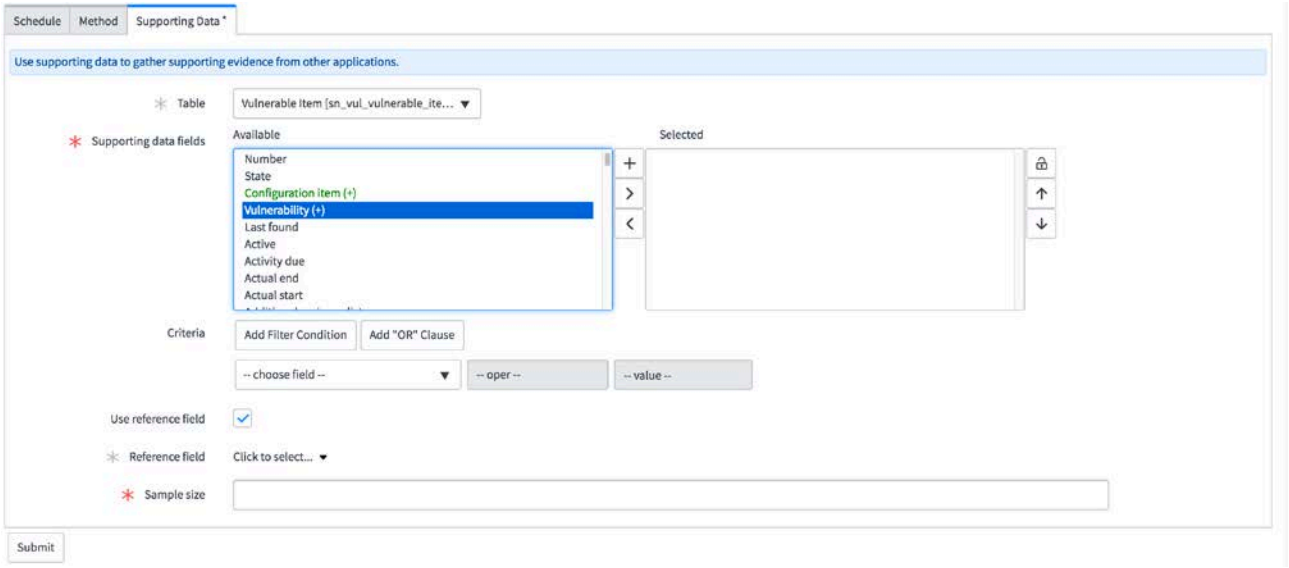
6. On the Supporting Data tab, select the drop-down menu arrow next to **Table**. Select the **Vulnerable Item** [sn_vul_vulnerable_item] table.



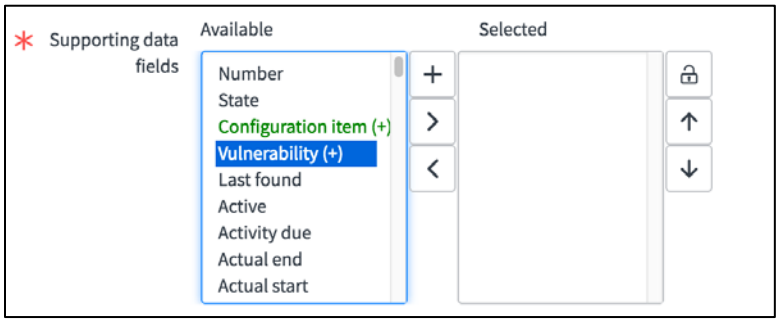
7. Next to **Supporting data fields**, press the **lock** icon.



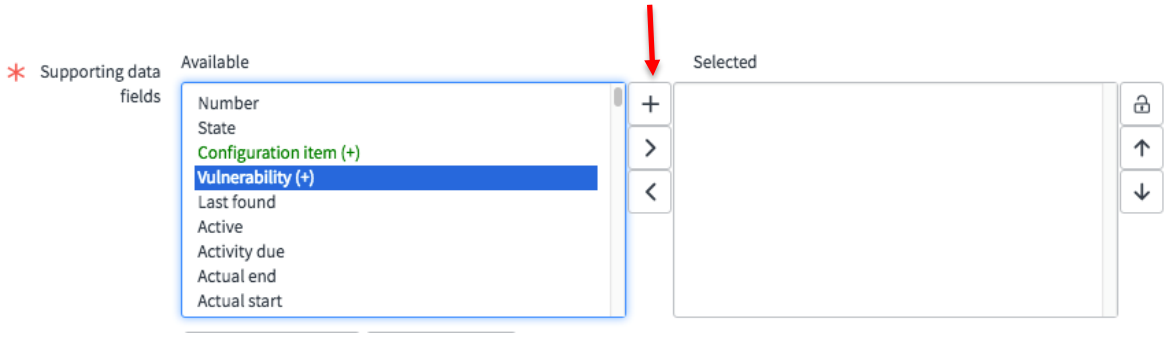
8. The data field selector expands.



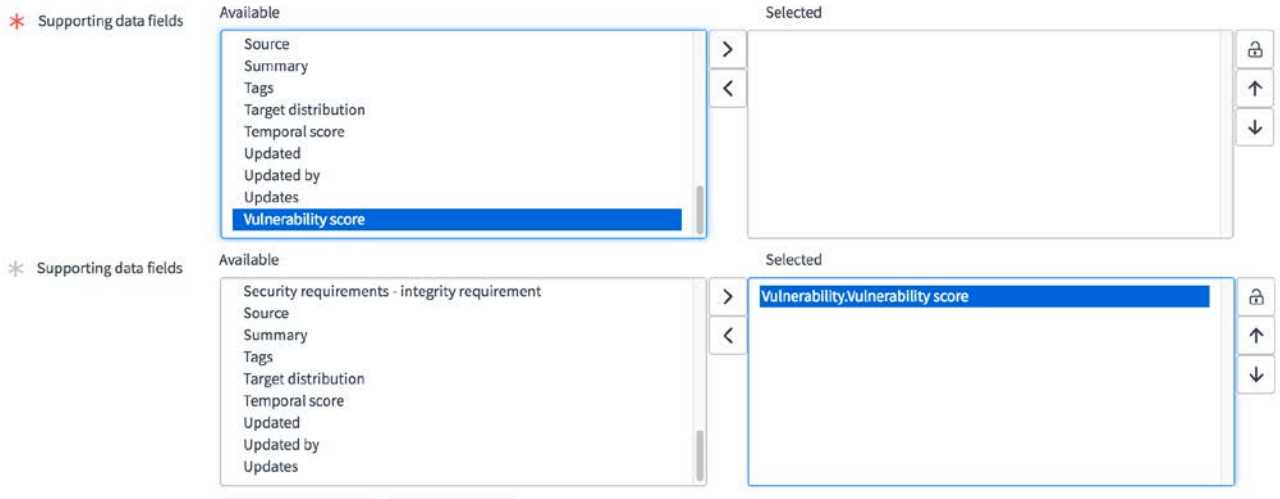
9. Click **Vulnerability(+)** once.



10. Press the **+** button to the right of the data field selector.

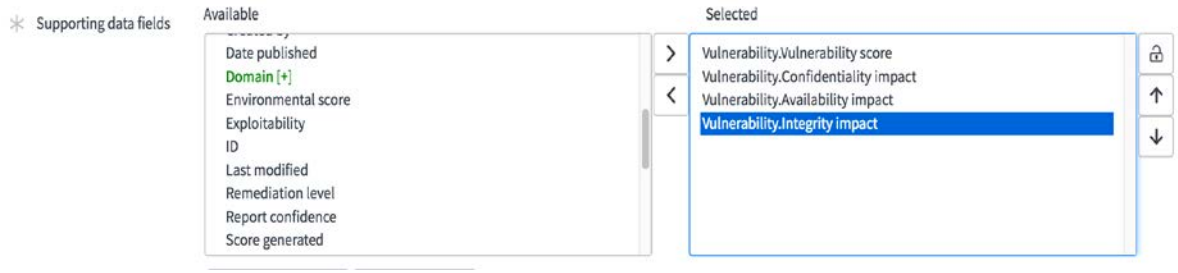


11. Scroll to the bottom of the expanded list and select **Vulnerability.Vulnerability score**. Press the **>** button to bring it to the Selected box on the right.

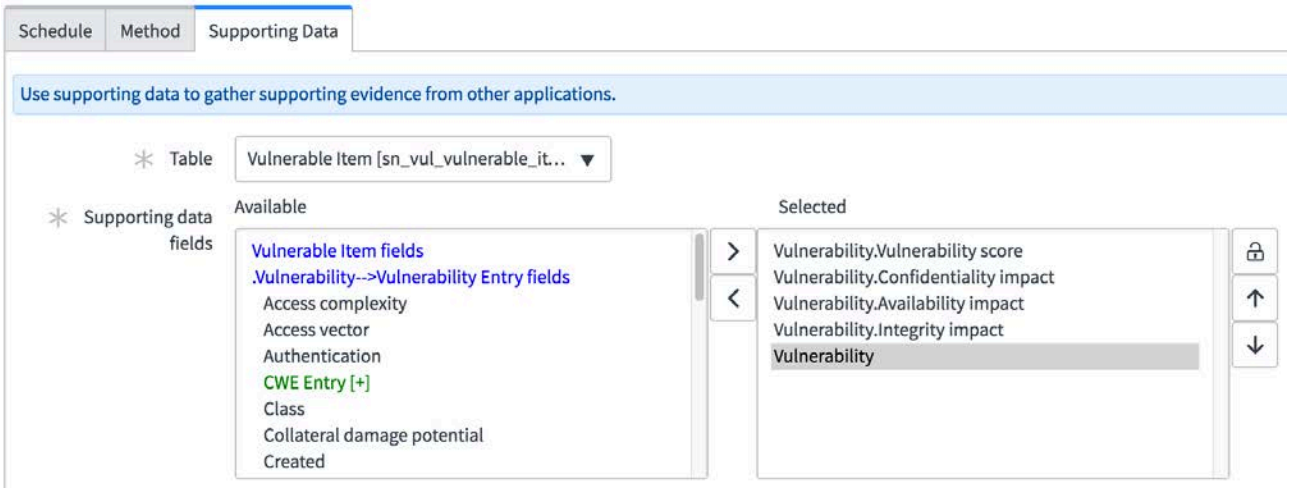


12. Add the following fields by clicking and pressing **>** to add to the Selected box on the right:

Vulnerability.Confidentiality impact
Vulnerability.Availability impact
Vulnerability.Integrity impact

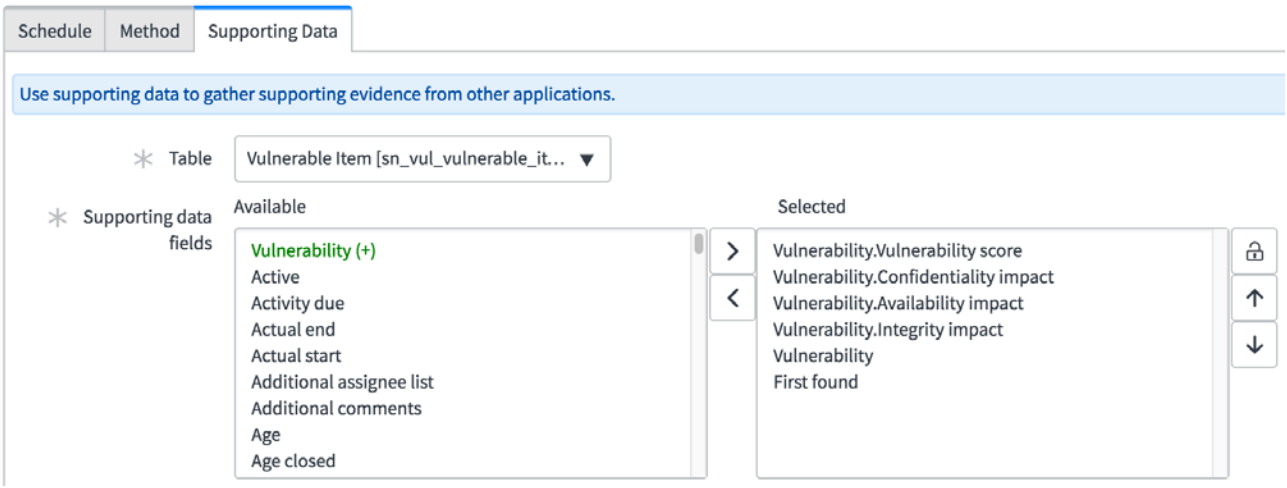


13. In the left **Available** box of the data field selector, scroll to the top of the list and click **Vulnerable Item fields**.

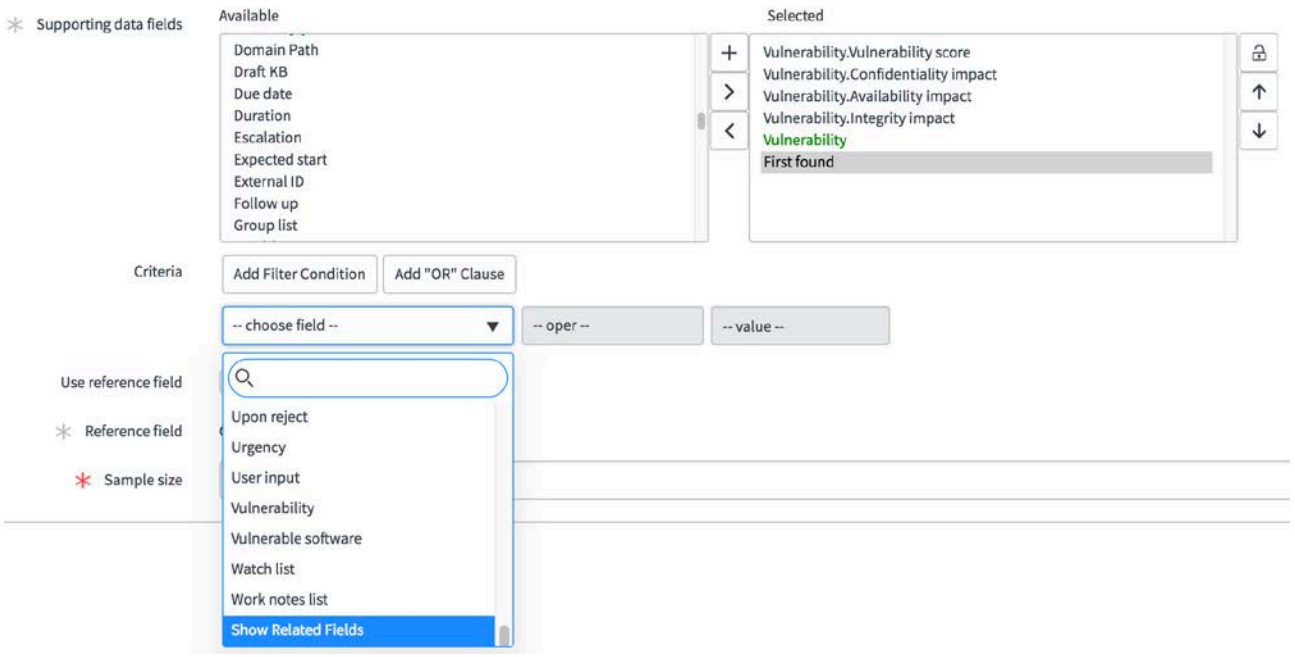


14. Add the following data fields, following the same process to click and press **>** to add to the selected box:

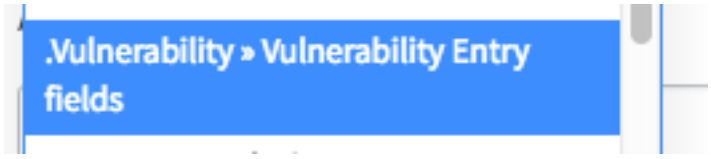
    Vulnerability [+]
    First found



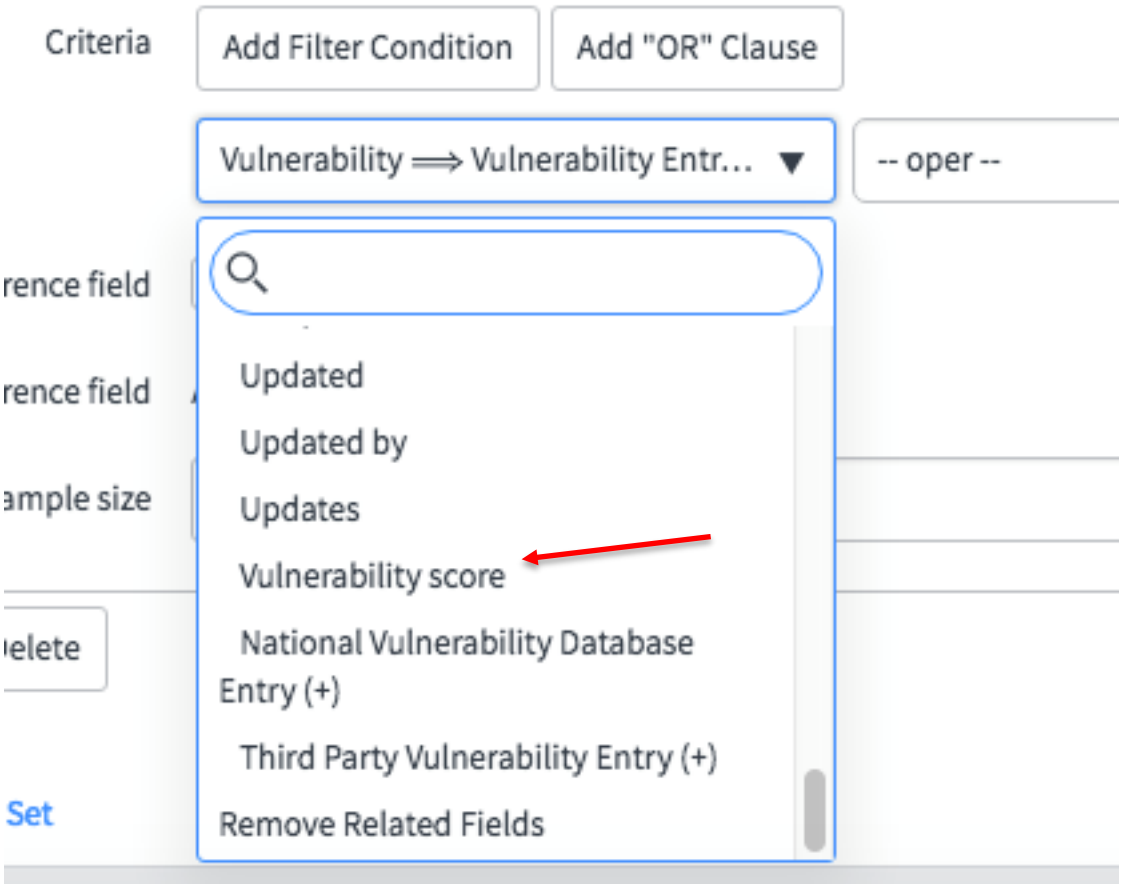
15. In the Criteria section, click on '**choose field**' and scroll to the bottom of the list to select '**Show Related Fields**'.



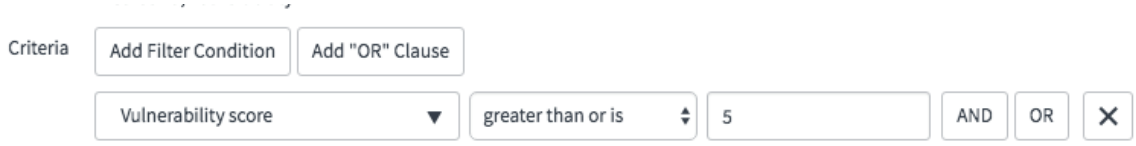
16. In the same menu, select **Vulnerability → Vulnerability Entry fields**.



17. In the same menu, next select **Vulnerability Score**.



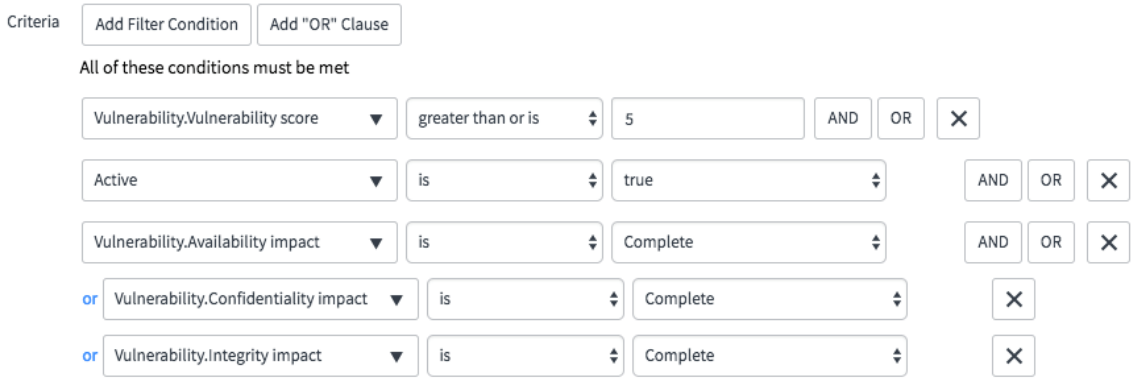
18. Complete the logic configuration by using the drop down menus to select '**Vulnerability Score' 'greater than or is' 5**.



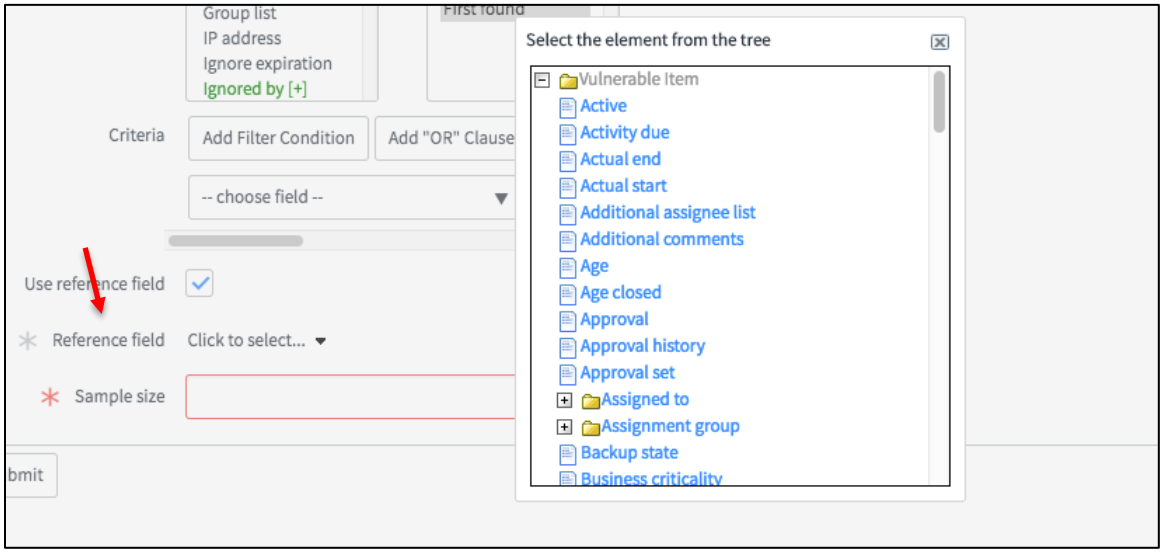
19. Press the **AND** button to add the next line of logic.



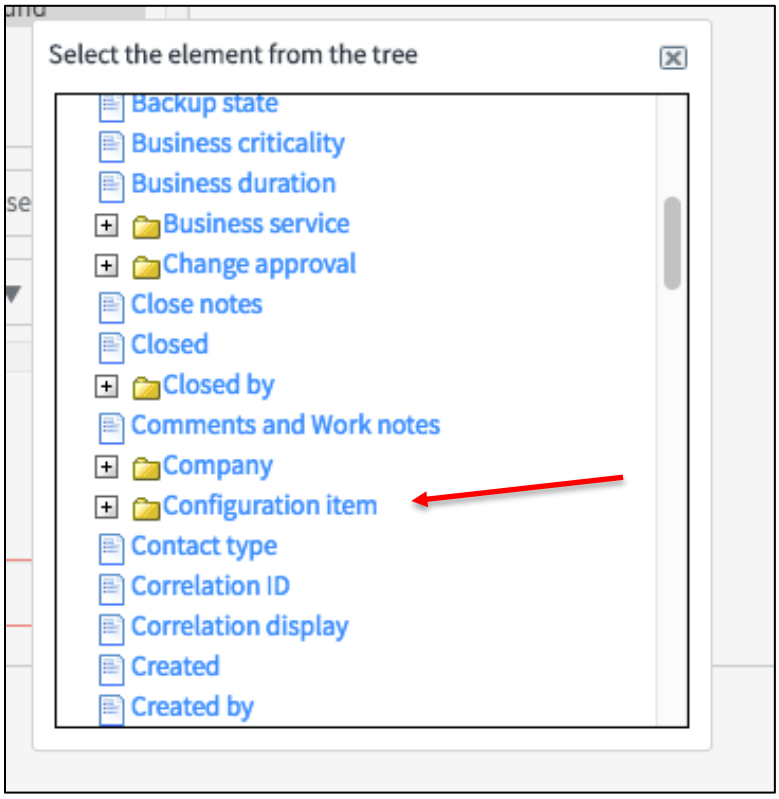
20. Build the following logic by selecting 'choose field' and the AND, OR buttons to continue building out the logic below. Note that for **Vulnerability.Confidentiality Impact** and **Vulnerability.Integrity Impact** the logic is '**OR**'. (**Reminder**: The Confidentiality Impact and the Integrity Impact fields are under 'vulnerability entry fields'.)



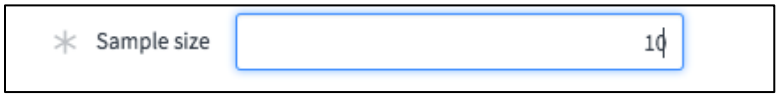
21. Scroll to Reference field and press the **down** arrow.



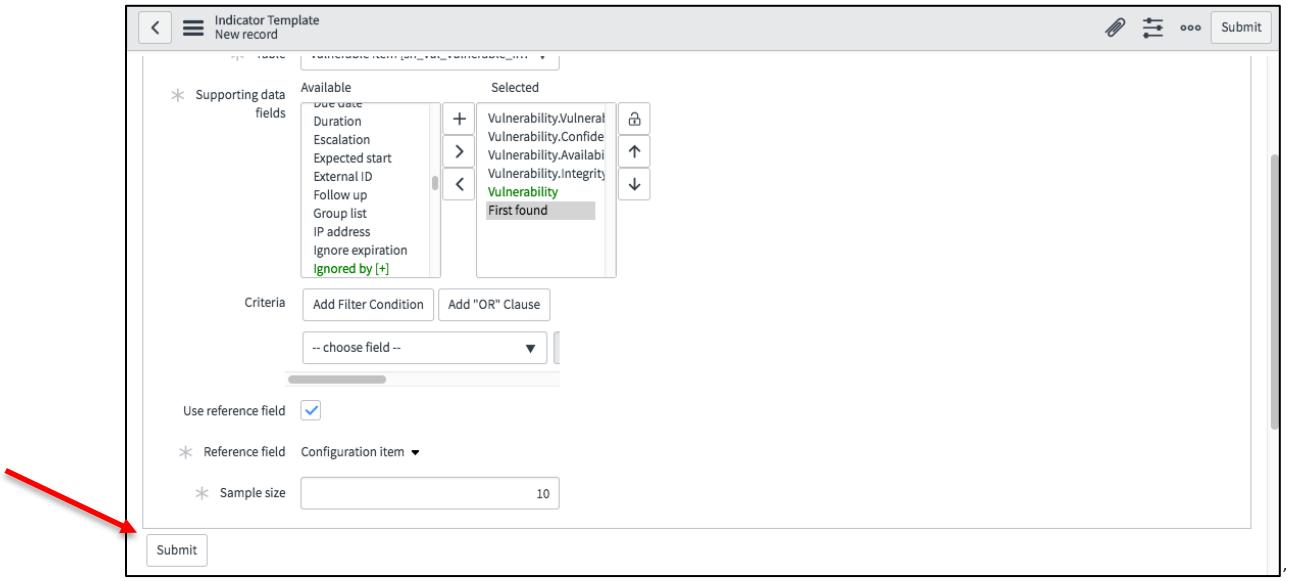
22. Select **Configuration Item**.



23. In the Sample size field, enter **10**.

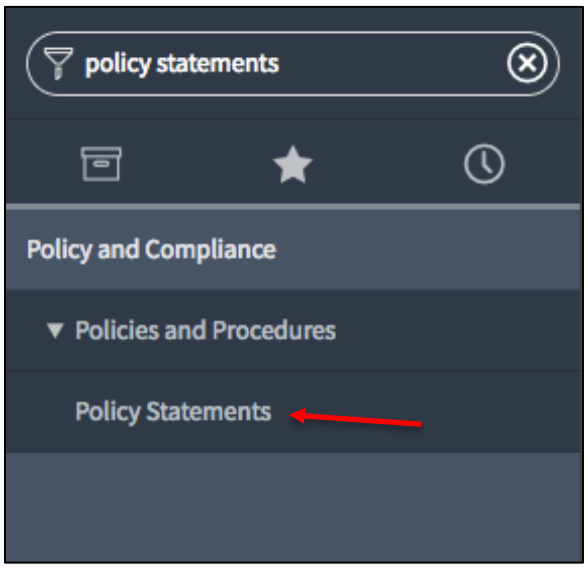


24. Click **Submit** in the upper-right corner or bottom-left corner of the screen.



Task 4

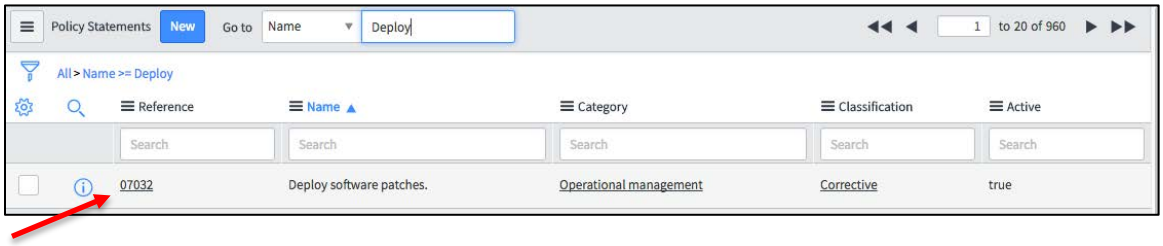
1. In the filter navigator, type **policy statements**. Select **Policy Statements** under Policy and Compliance.



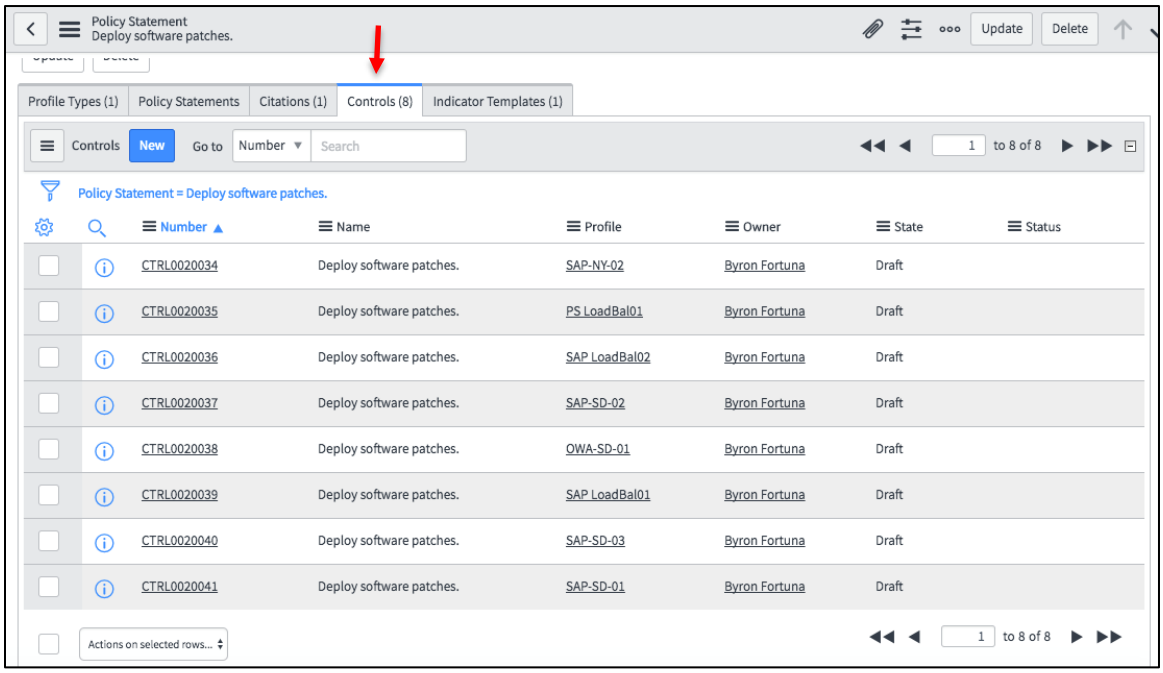
2. In the top bar, type **Deploy** in the field next to 'Go to' = Name and hit Enter or Return on your keyboard.



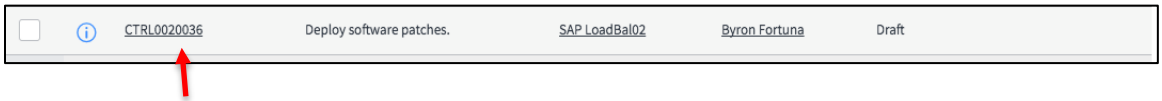
3. Select **Deploy Software Patches** by clicking on the reference number.



4. Scroll to and click the **Controls** tab.



5. Select the control for Profile SAP LoadBal02 by clicking on **the CTRL reference field.**



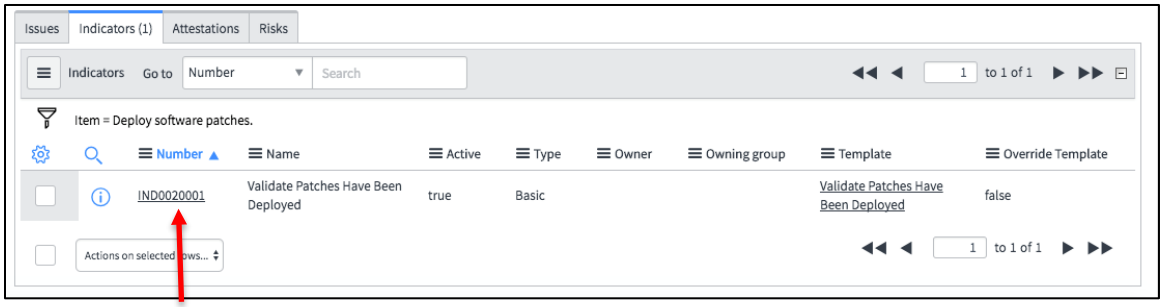
6. Scroll down to the Indicators tab and select **Add**.



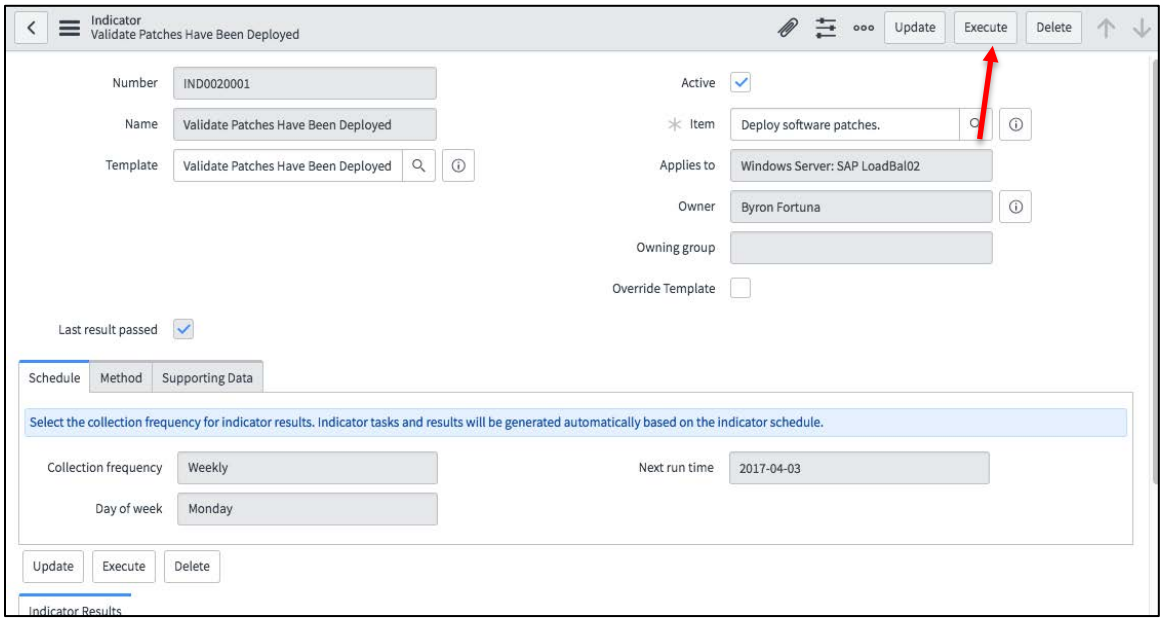
7. Select **Validate Patches Have Been Deployed** and press **Create Indicators**.



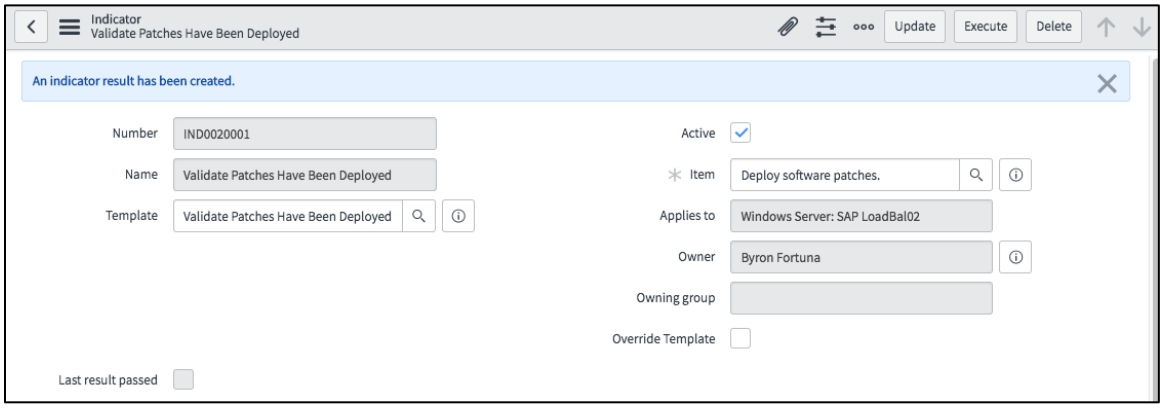
8. The indicator has now been added to the control. Click Number **IND field** to open the indicator.



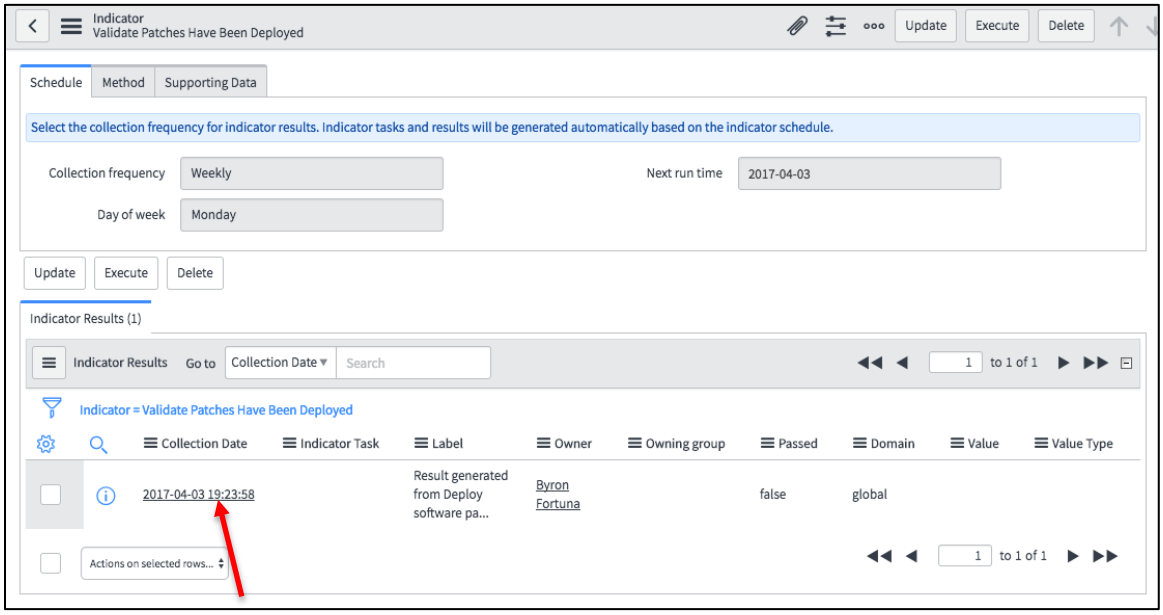
9. Press the **Execute** button in the top-right corner.



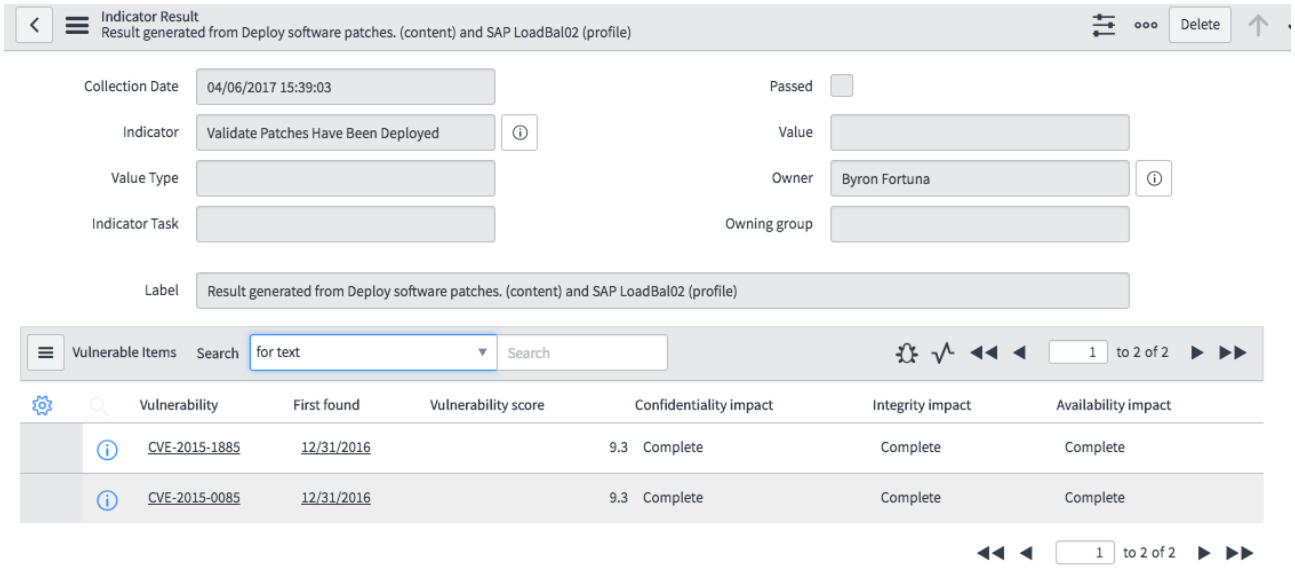
10. The indicator result is created.



11. Scroll to the bottom of the record to view results. Click **Collection Date** timestamp to view results.

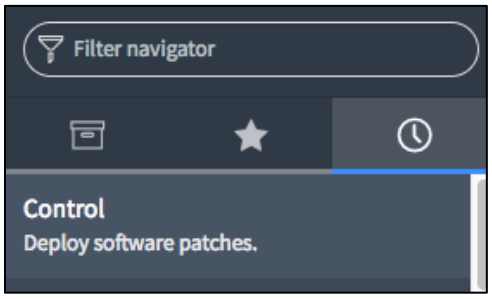


12. The Indicator Result record will return evidence that the indicator is failing. This evidence is in the form of found vulnerabilities per the predefined criteria.

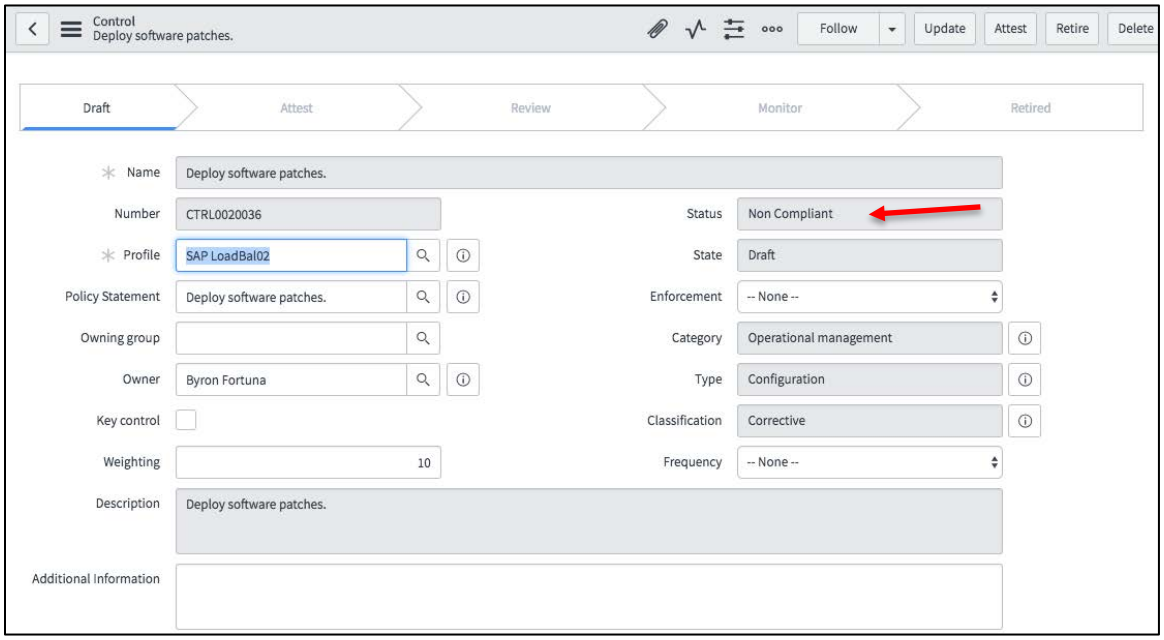


Task 5

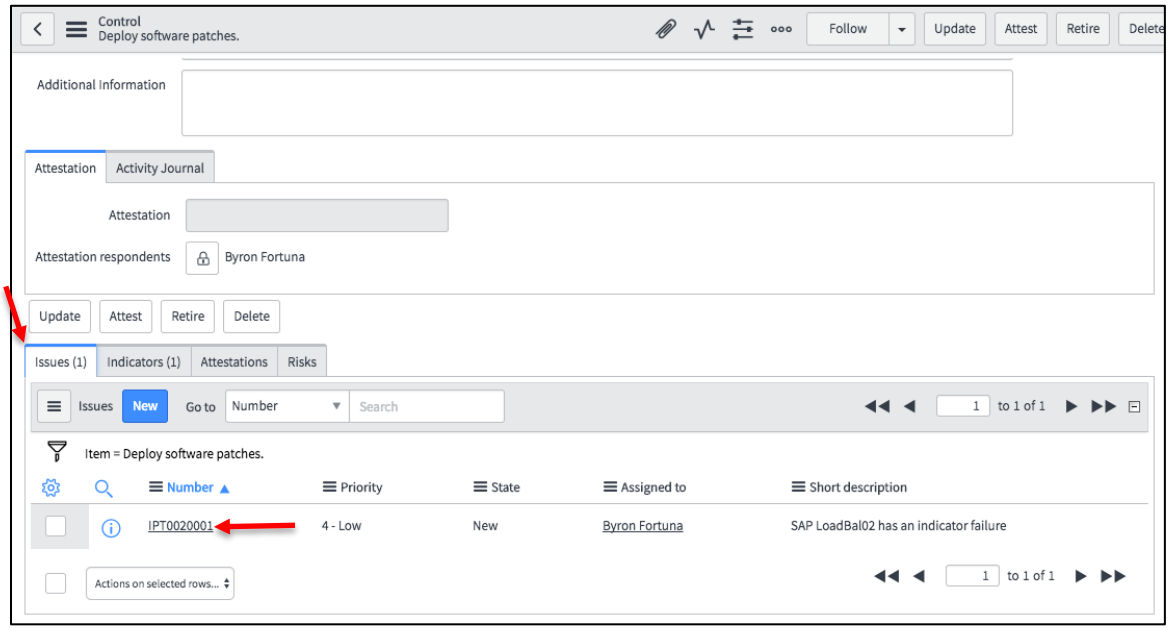
1. Return to the Control **Deploy Software Patches** by using the history in the filter navigator.



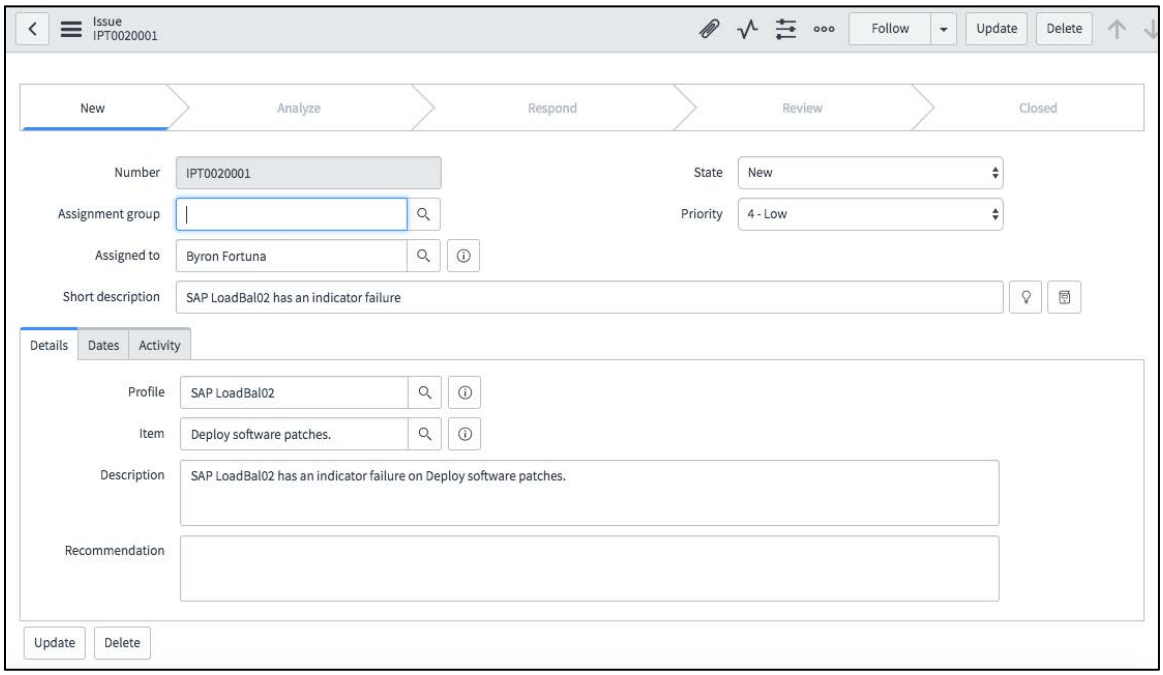
2. Note the control status is set to **Non Compliant**.



3. Scroll to the **Issues** tab. An issue is created as a result of a failed control.



4. Click into the issue by selecting the Number **IPT field.**

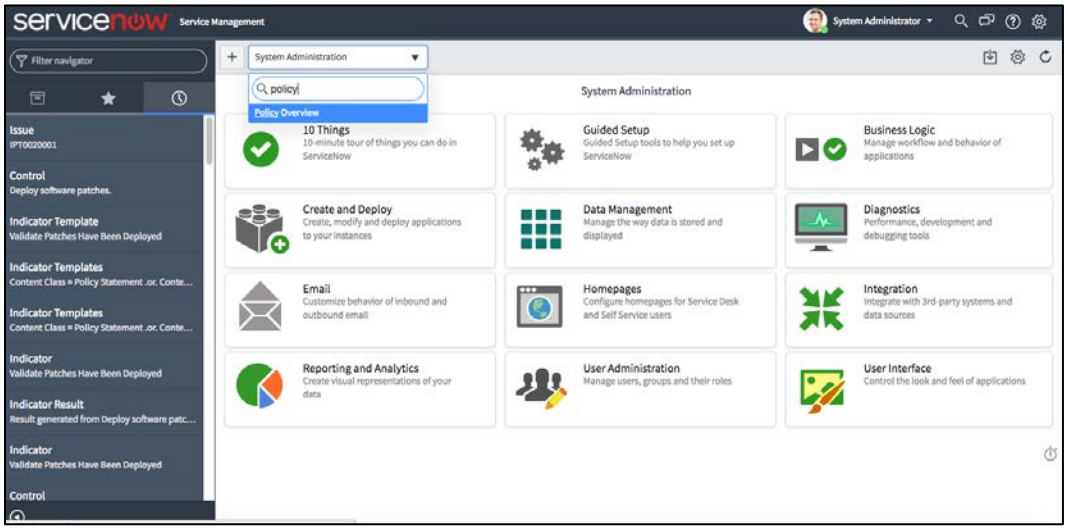


Task 6

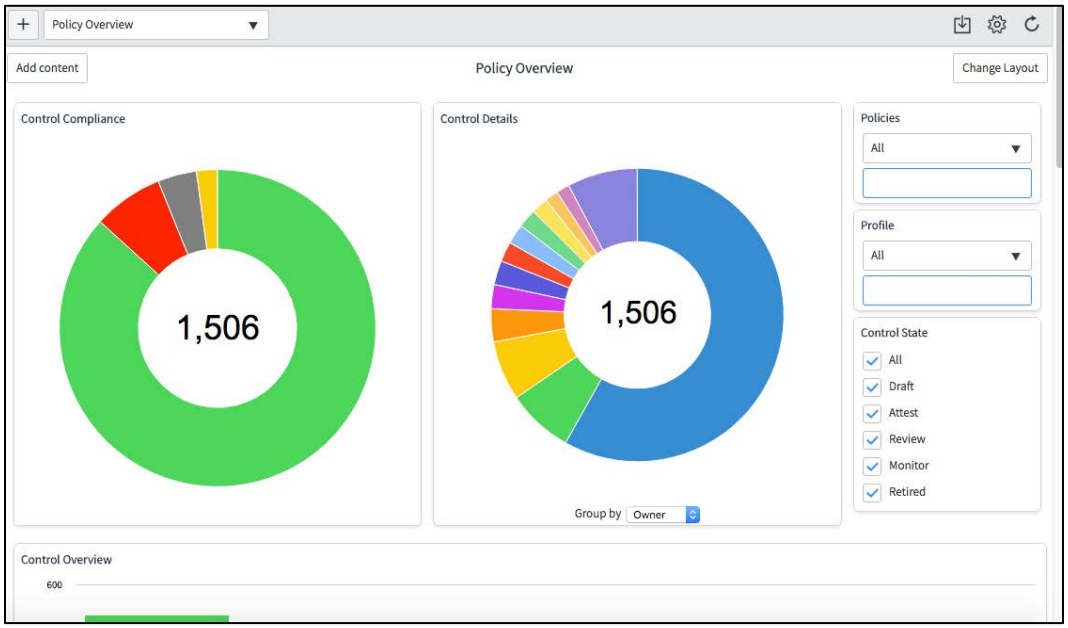
1. Click on the ServiceNow logo in the top-left corner to return to the home screen.



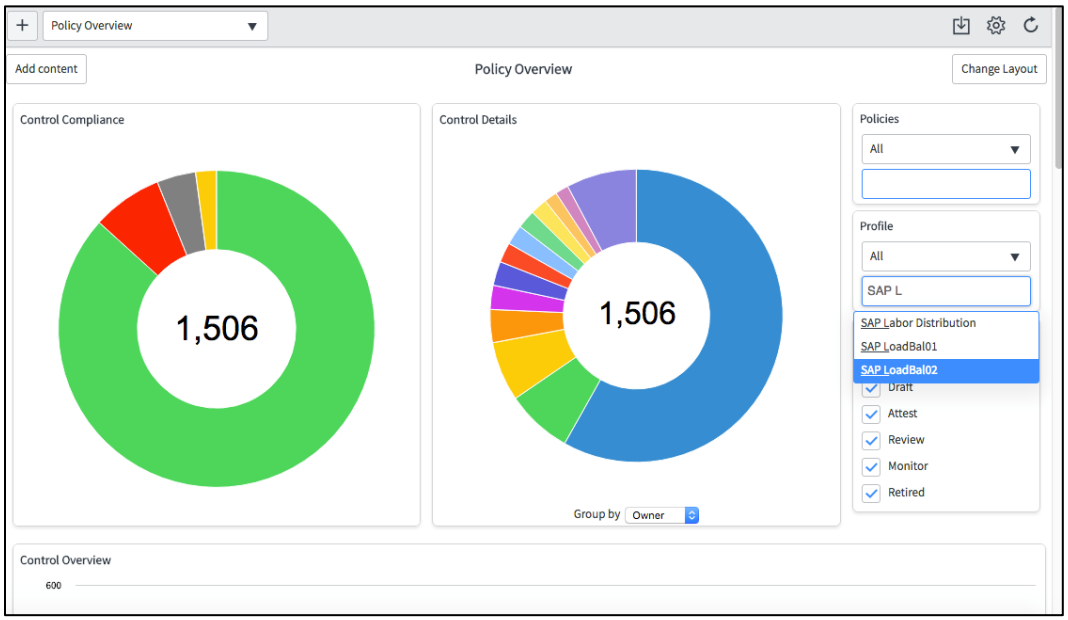
2. In the dashboard navigator, click the arrow and type **Policy Overview**.



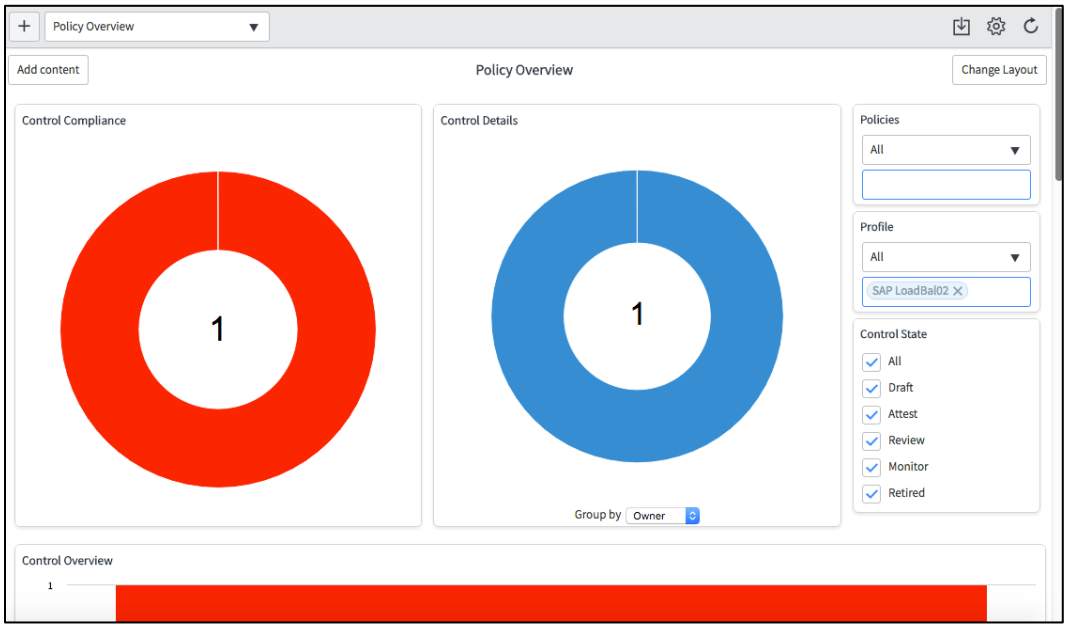
3. You are now viewing the Policy Overview dashboard.



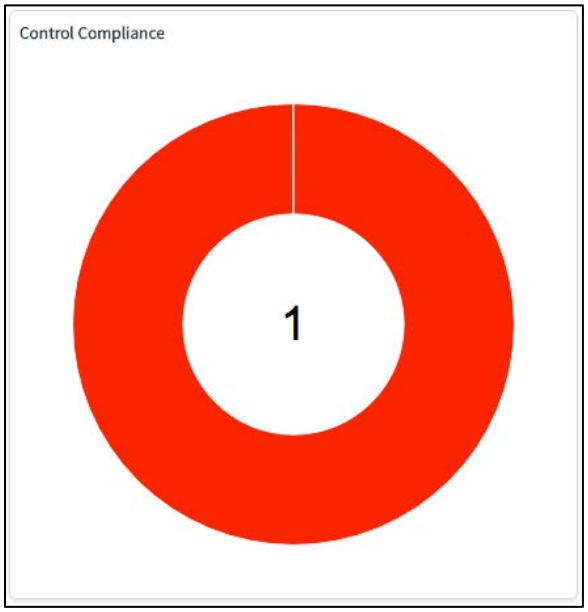
4. On the right side, under Profile type **SAP LoadBal02** and select it.



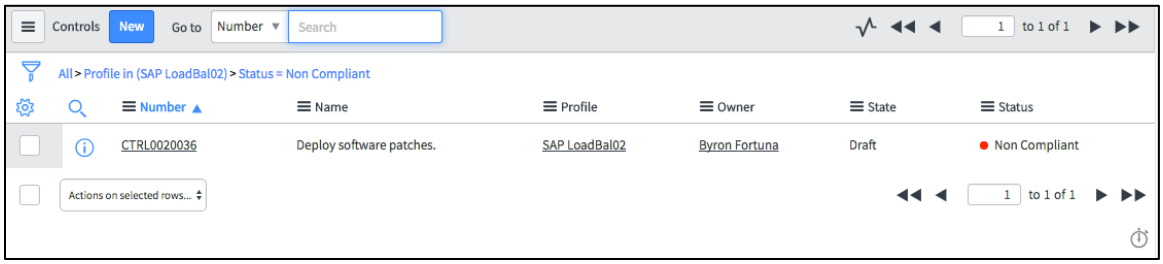
5. The dashboard updates to show **SAP LoadBal02** control posture.



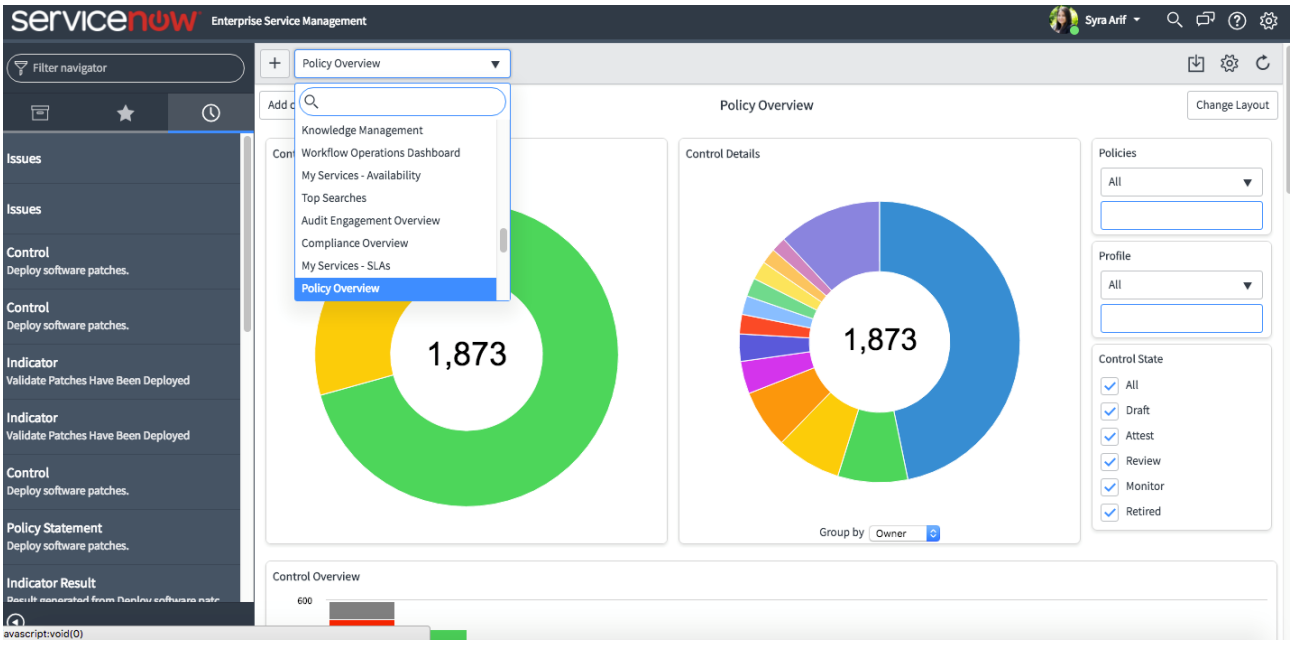
6. Click the red wheel in the Control Compliance dashboard on the left.



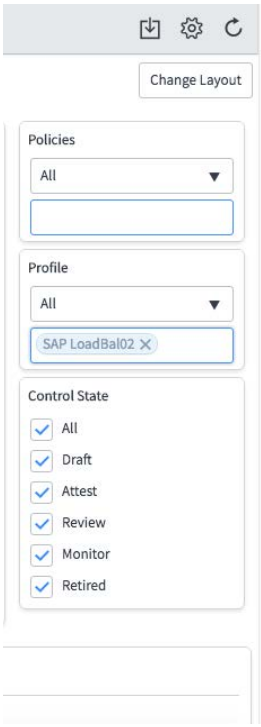
7. You are redirected to a list view of non-compliant controls.



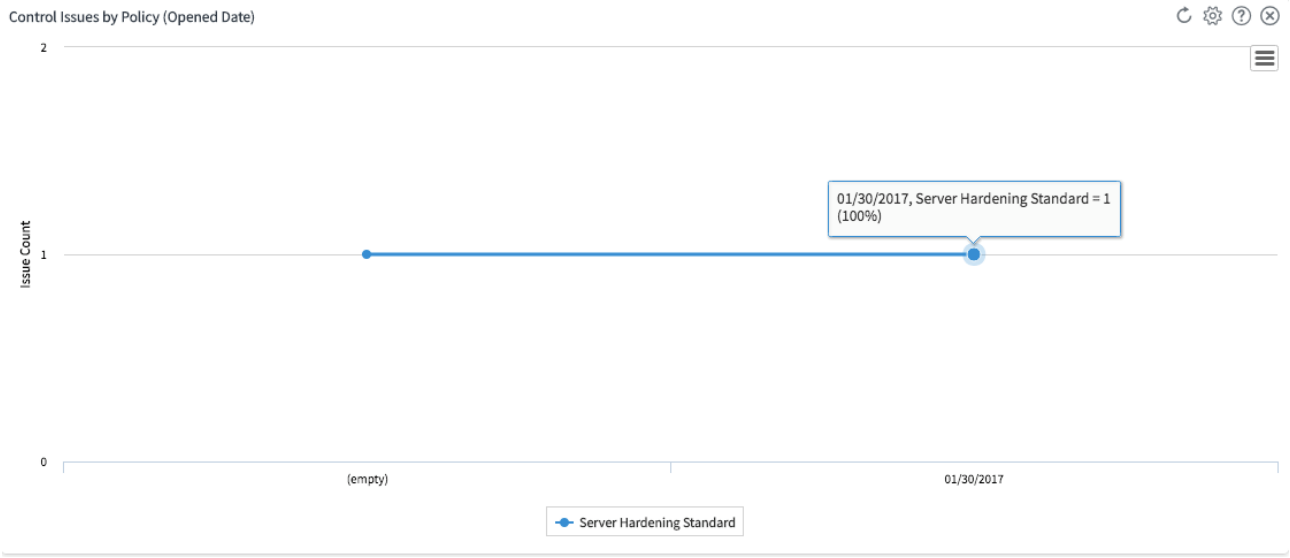
8. Return to the Policy Overview dashboard by clicking on the ServiceNow Logo in the top left-hand corner and selecting Policy Overview from the dashboard picker.



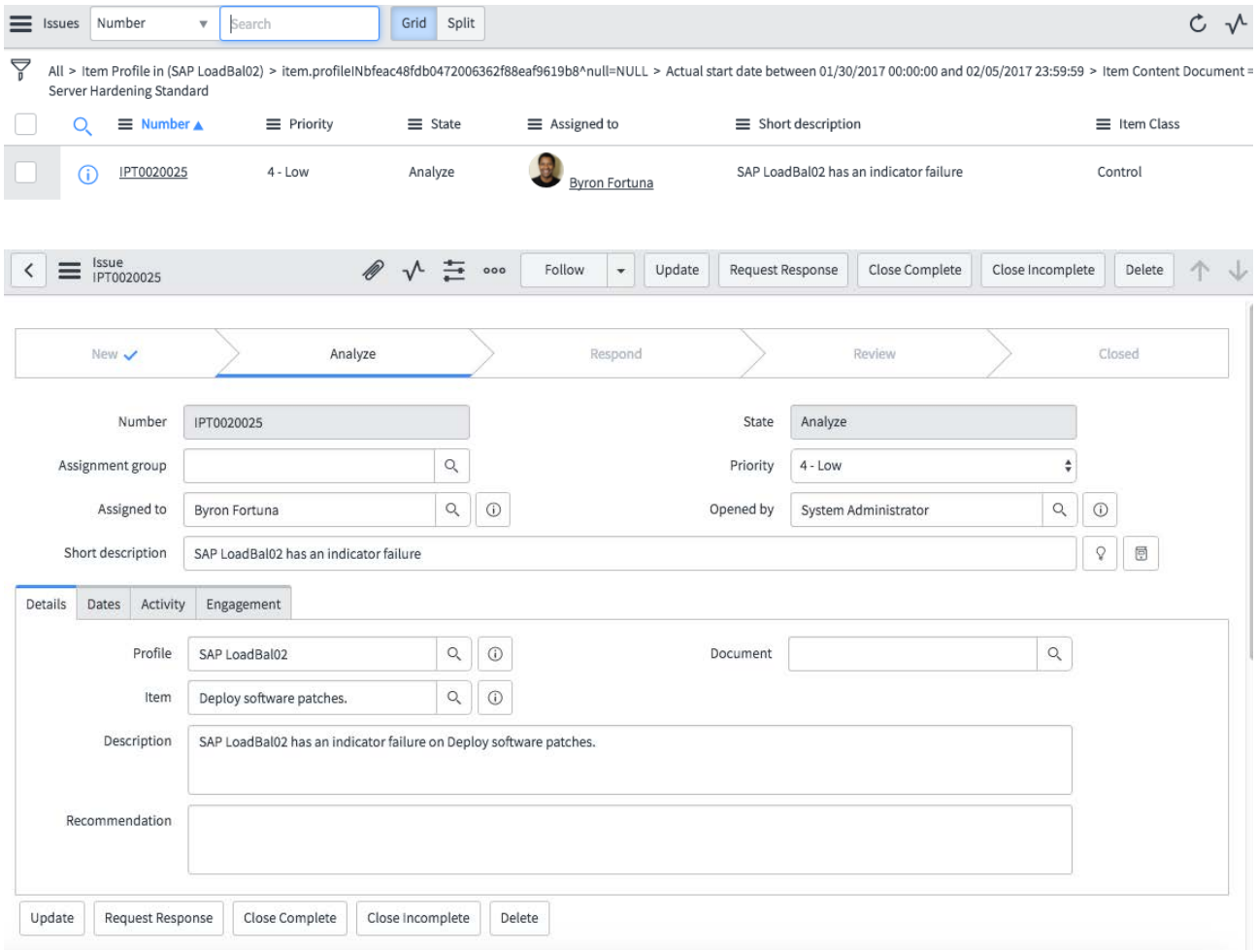
9. On the right side of the dashboard, type ‘SAP LoadBal02’ under Profile. The dashboard will automatically update with reports related to this SAP profile.



10. Scroll to the bottom of the dashboard to view the Control Issues by Policy dashboard. You can drill into the issue by clicking on the data point.



11. Next, drill into the Control Issue to view the full issues lifecycle related to this SAP profile.



You have reached the end of the lab.