Lab Guide

Enterprise Security Response

Creating Automated Workflows for Security Playbooks

Sean Barrett, Robert Held, Jerry Hu

Default Login / Password: Knowledge17

admin / Knowledge17

itil / Knowledge17

employee / Knowledge17

Lab Sponsored by Amazon Web Services



This
Page
Intentionally
Left
Blank

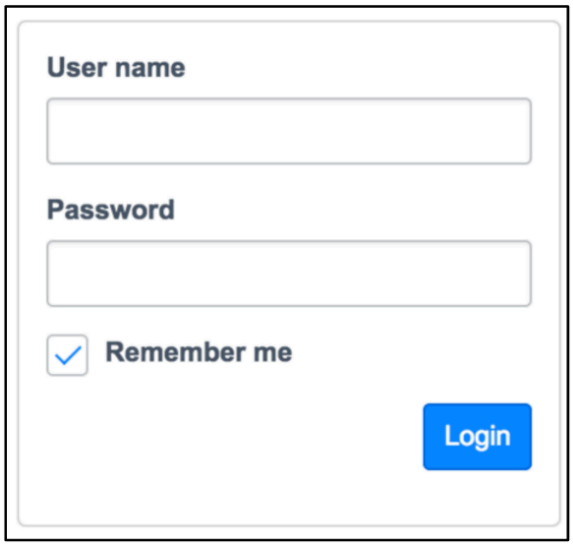
Lab Goal

This lab explains the steps required to access your instance.

Lab 1
Access Your Instance

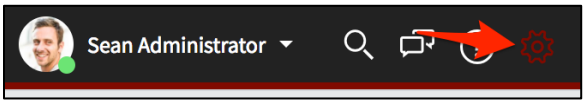
Log On to Your Lab Instance

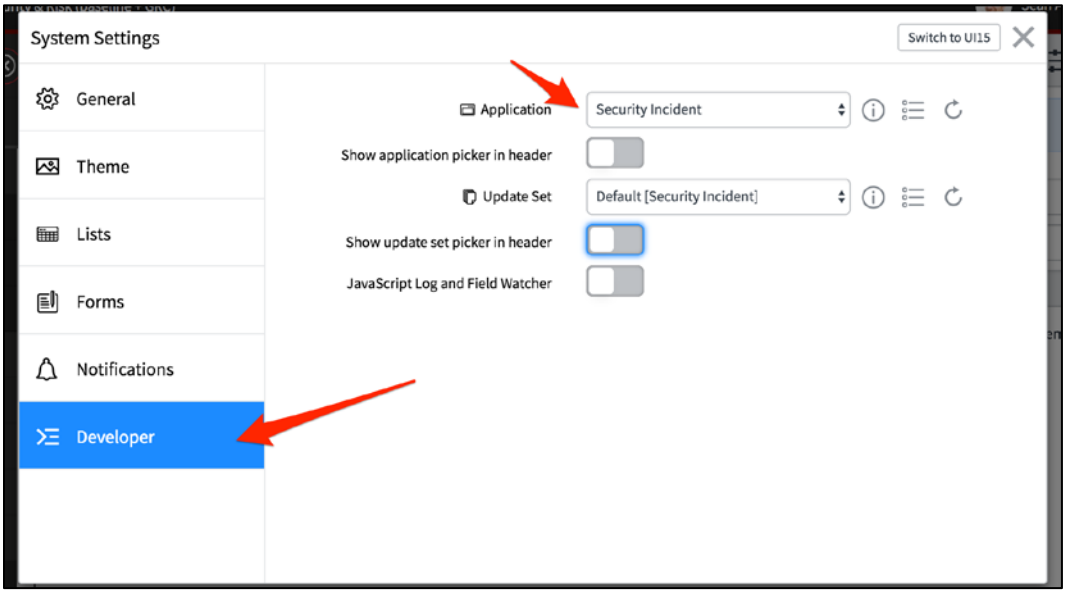
1. Navigate to the unique instance URL provided to you.



2. Log on with provided credentials.
3. Change Application Scope to **Security Incident**.
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 Security Incident -> Exit**.





Lab Goal

This lab explains the steps required to set up your lab instance.

Lab 1.1
Lab Configuration

Plugin Confirmation

1. Navigate to **System Definitions>Plugins**.
2. Confirm that the following plugins have been enabled:

   Security Incident Response
   Vulnerability Response
   Security Support Orchestration

Lab Goal

Lab 2
Understand the Workflow Interface

This lab introduces the Workflow Editor and the Workflow Engine. It defines the role of Workflow in the Platform and tours the individual pieces of **Workflow**.

About ServiceNow Workflow

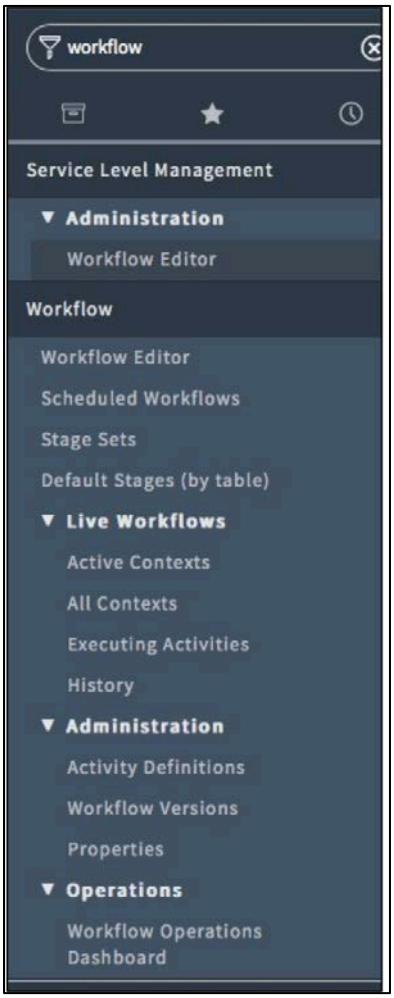
ServiceNow Workflow has two main components:

- **Workflow Editor** is the part of ServiceNow UI that process owners and designers use to design workflows that automate business processes. The Workflow Editor always opens in an adjacent browser tab. The main work area is referred as the canvas.
- **Workflow Engine** is part of the Glide Script Engine and is invoked with insert, update, delete or cancel of a Glide record. Because of this, each workflow can be configured to run based on conditions. This is similar to how Business Rules determine when to run.

Log On to Your Lab Instance

1. Log on with provided credentials.

2. Enter **workflow** in the Application Navigator Type filter text field to open the **Workflow** Application.

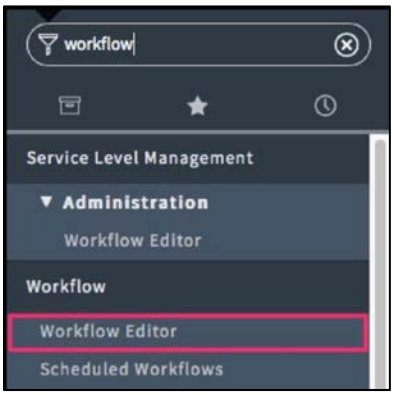


The Workflow application contains these functions:

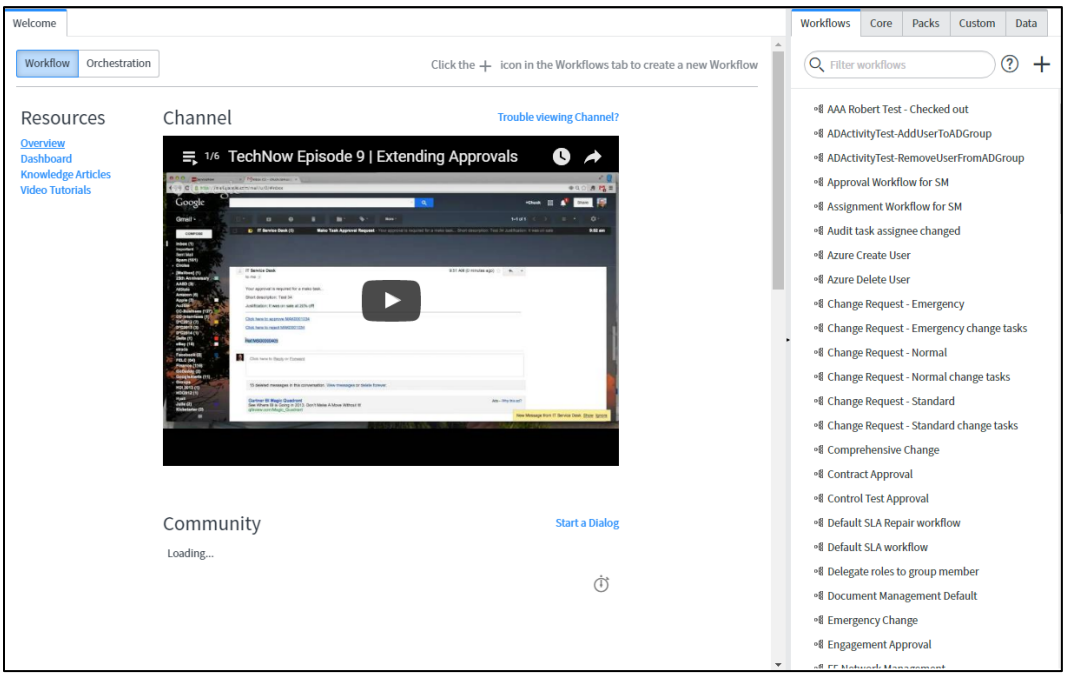
- The Workflow Editor for creating and editing workflows
- Monitoring, running, and reviewing workflows
- Administering the Workflow Engine
- Workflow Operations Dashboard

3. Select the **Workflow Editor**.

   Note: In subsequent labs, these navigation steps are abbreviated to: **Workflow > Workflow Editor.**

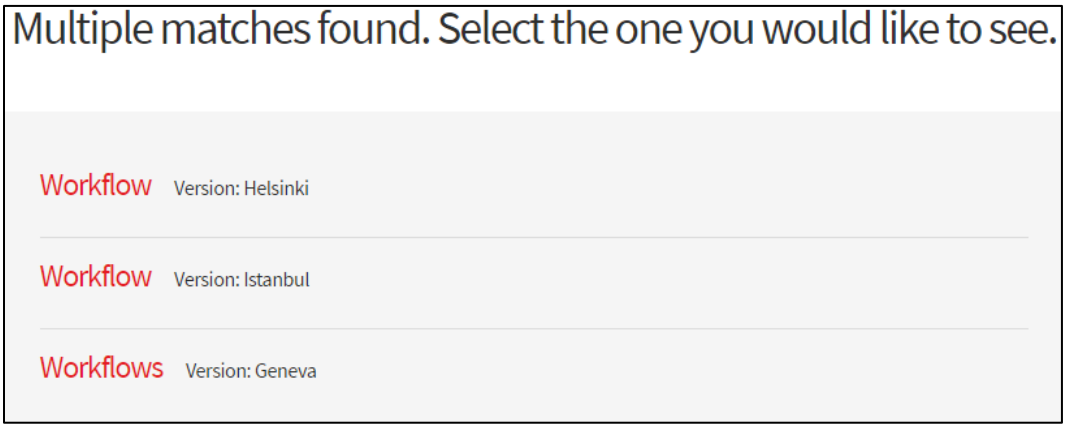


4. The browser loads the Workflow Editor in an adjacent browser. **Workflow Editor** is also the canvas. The screen should look like the example.

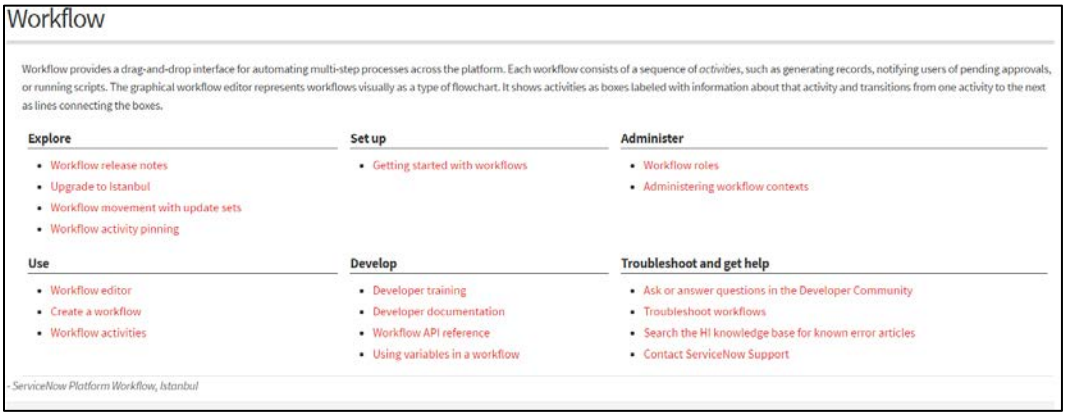


5. The center of the workflow palatte contains a regularly updated series of video talks and tutorials related to workflow development. At your leisure, please spend some time watching those informative videos!

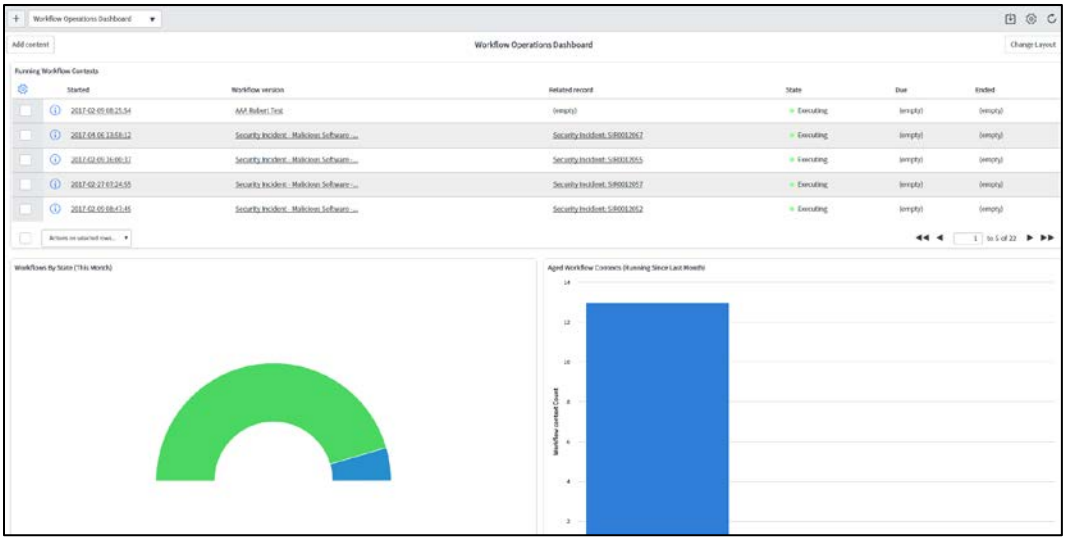
6. Select the **Overview** link on the left. This opens a new tab. Help resources in ServiceNow are broken down by version. On this new tab, select the Istanbul version of the **Workflow** overview.



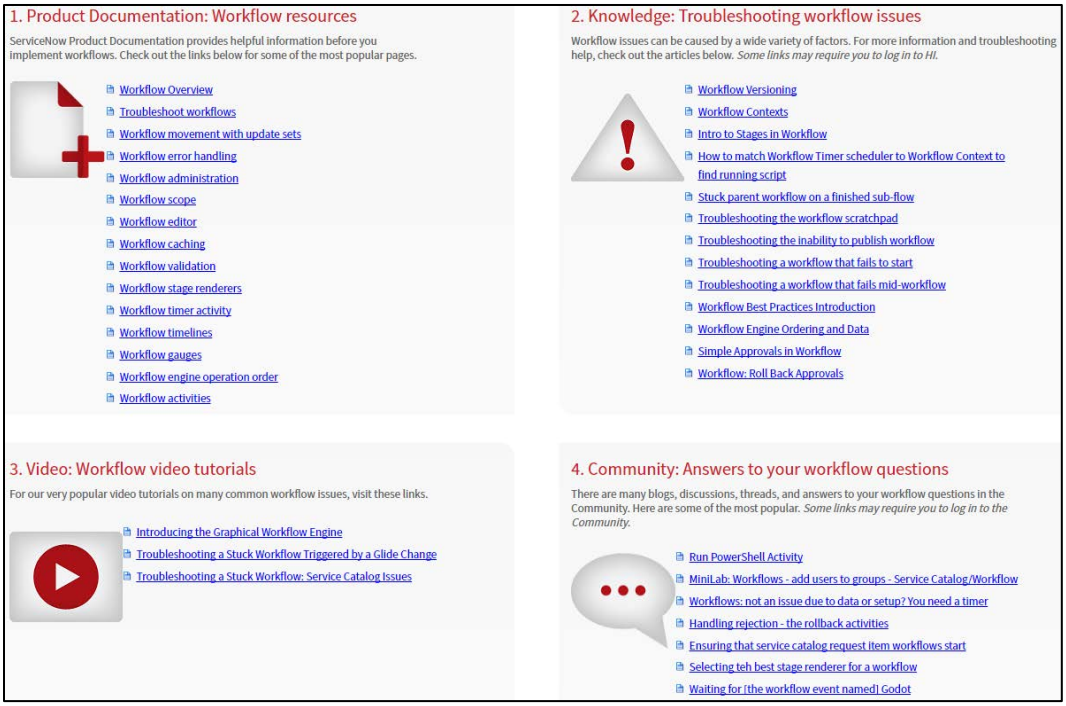
7. The next screen provides many options for getting started with workflow development. We recommend that in the future you review all the links in this section to expand your understanding of workflows. For now, close this tab.



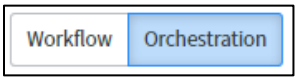
8. From the main workflow editor tab, select the **Dashboard** option. This launches a new tab that gives insight into what workflows are currently in progress, what has recently run, and how long workflows have been running. This is useful in troubleshooting workflows and identifying long running workflows that may need some attention. After review, close this tab.



9. Next, click into the **Knowledge Articles** section. ServiceNow has robust product documentation, knowledge articles, video tutorials, and an active developer community to assist you with workflow development. Outside this class it is recommended that you spend some time reviewing these resources in detail. For now, close this tab.



10. Those resources were related to the workflow management of ServiceNow. In the top-left corner of the pallet, click the **Orchestration** section of the editor.

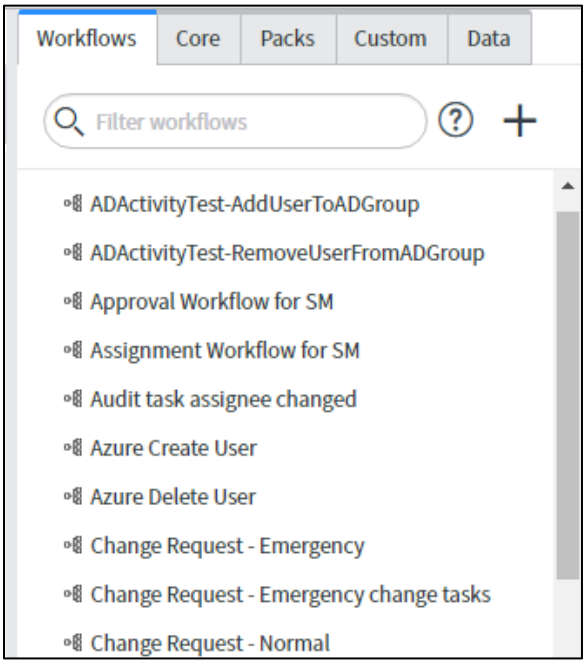


11. An identical set of resources are available to assist you in Orchestration activities. Orchestration is an important part of workflow creation, allowing you to take actions on other systems based on workflow activities. A few examples of orchestration include:

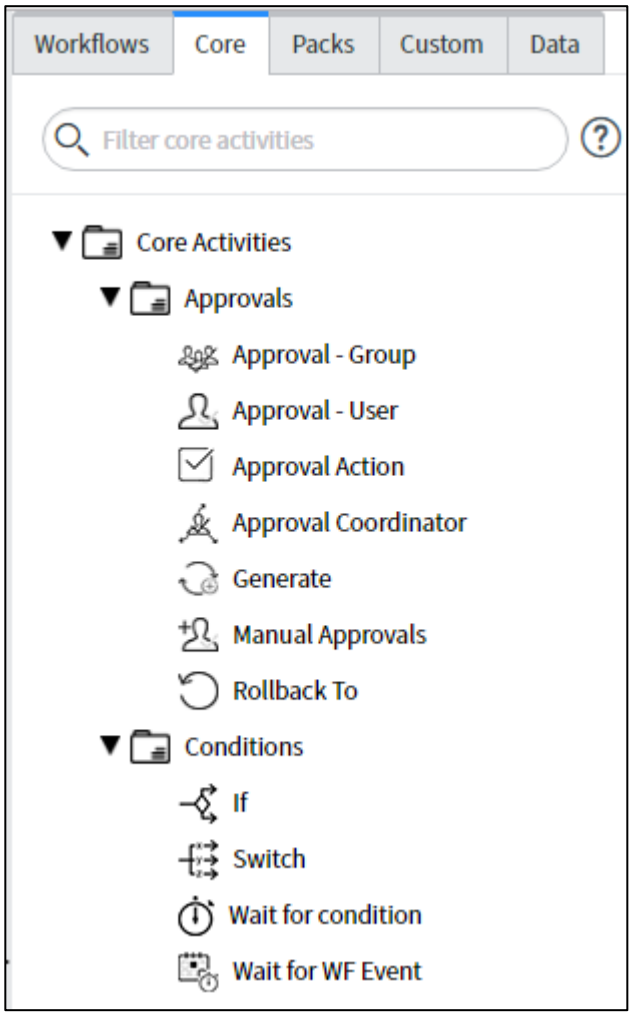
- Blocking a port on a firewall
- Running a WMI query to gather information from an endpoint
- Querying Microsoft Exchange for phishing email information
- Disabling a user account in Active Directory

- Provisioning a new cloud asset
- Interaction with Palo Alto Wildfire (You'll do this in a later lab!)

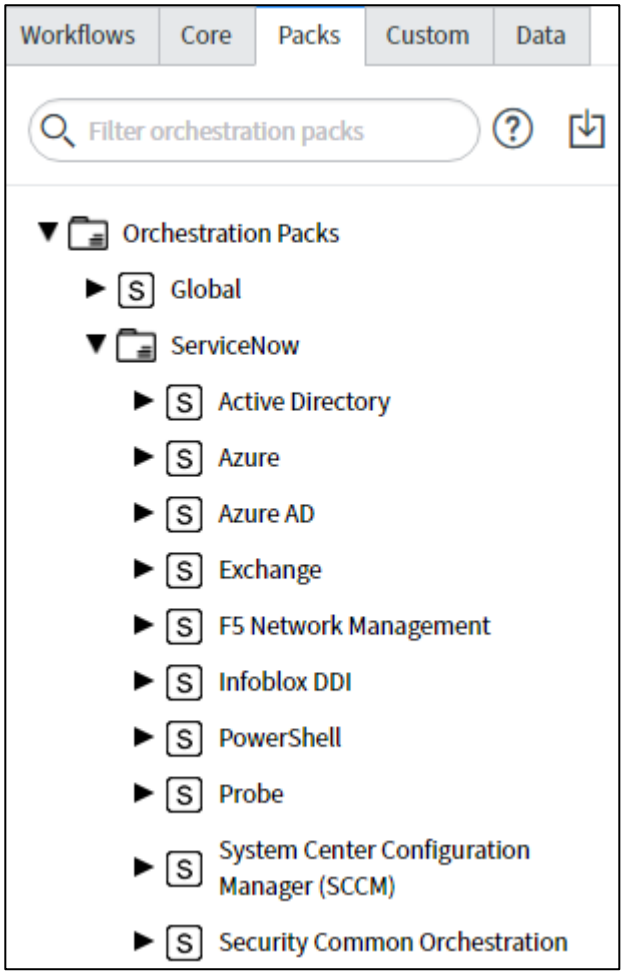
12. Look at the right pane. The **Workflows** tab contains the current workflows defined in ServiceNow. The list also shows any workflows that have been checked out to users by displaying a **– checked out** following the workflow name. Open a workflow. Scroll down (or use the filter) to the workflow **Security Incident Response - Create IoC Lookup Request for IoC Changes.** This opens the workflow in the center pane. You will not review the workflow at this point, but you need an open workflow to examine the next few tabs.



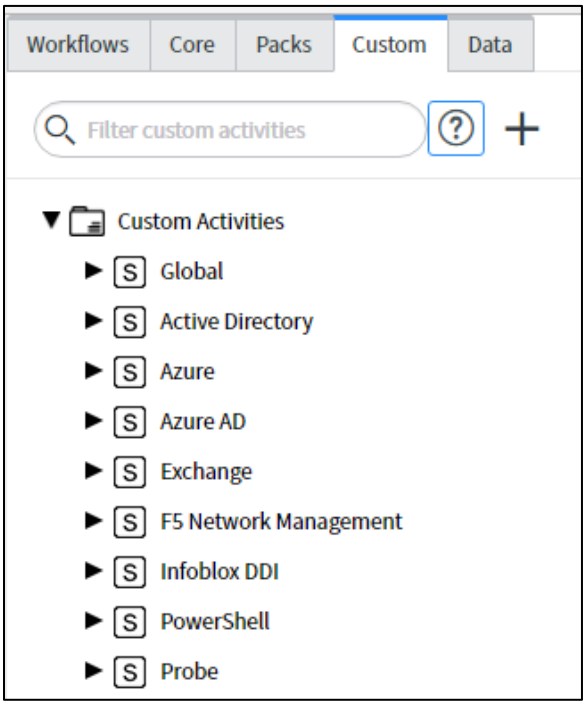
13. Look at the **Core** tab. This contains a number of built-in activities you can use to build your workflows. A review of some of these activities is done in Lab 3.



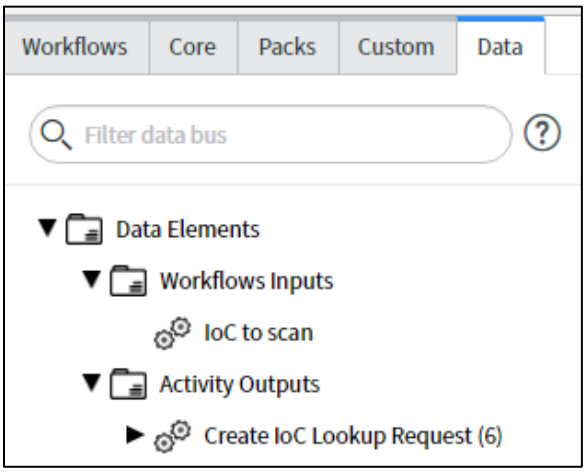
14. Next, move over to the Packs tab. The Packs tab of the Workflow Editor contains any activity packs downloaded from the ServiceNow Store and any activity packs that you create. These are prebuilt activities that you can use in your workflows.



15. Look at the **Custom** tab. This tab contains additional activities as part of the orchestration plugin of ServiceNow. Note that if Orchestration is not enabled in your instance, the Custom tab is not present.



16. Look at the **Data** tab. This tab displays all the input and output elements for the workflow and its activities. This can be helpful to understand how you pass variables and data from one activity to the next.



Lab Goal

Lab 3
Walk Thru Security Workflow Examples

This lab walks through examples of **Security Operation Workflows**, which allows faster response to security incidents and vulnerabilities.

Security Operation Workflow Examples

This lab explores how the solution works in the following activities:

- **Logging data in a workflow**
- **Parallel and Serial Work**
- **Updating NIST process states**
- **Task Based Decision Making**
- **Simple code example to check values**
- **Custom activities**

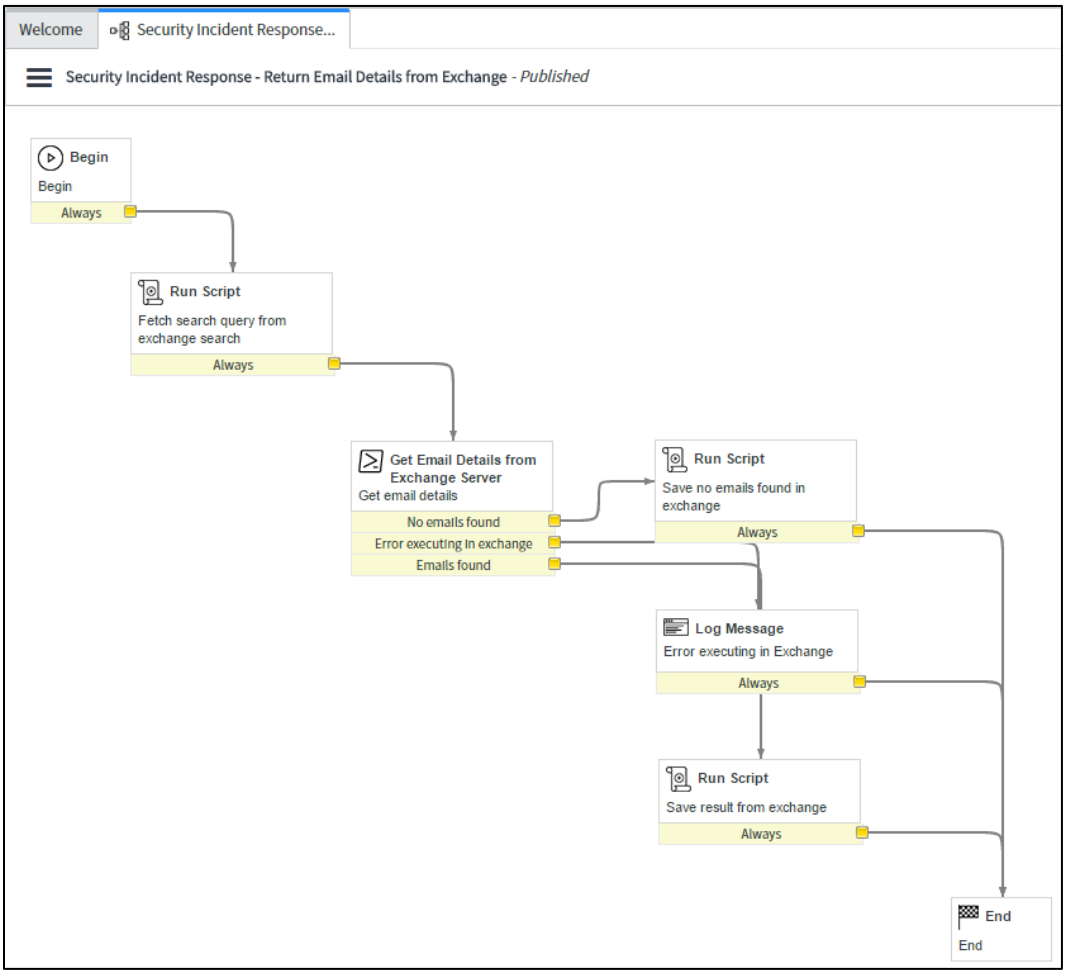
Log On to Your Lab Instance

1. Log on with provided credentials.

2. Enter **workflow** in the Application Navigator Type filter text field to open the **Workflow** Application.

Log Data in a Workflow

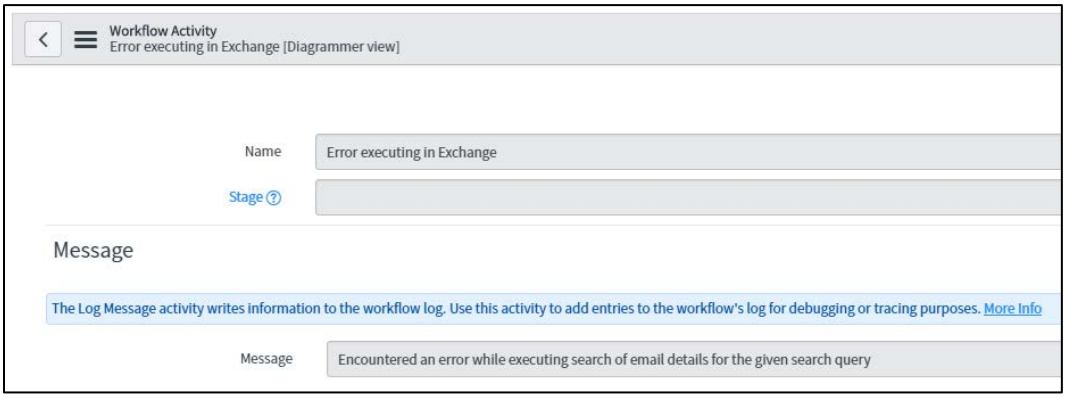
1. In the **Workflows** tab on the right pane scroll to and click **Security Incident Response - Return Email Details from Exchange** to open the workflow in the center pane.



2. Double click the **Error executing in Exchange** activity in the workflow.



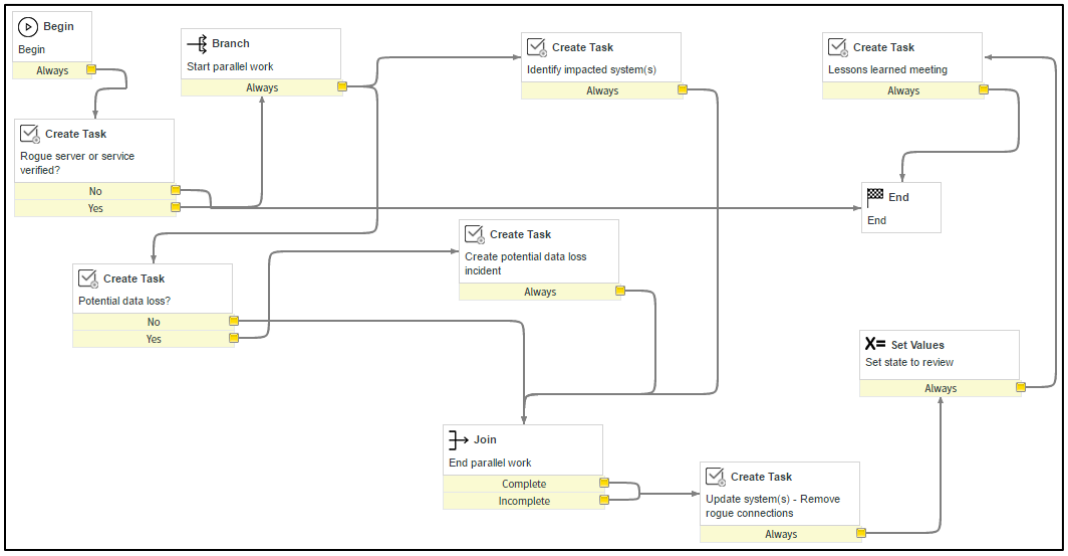
3. Similar to the importance of logging status, state, and error messages in traditional code writing, these activities are critical to troubleshooting and debugging workflows. This is a simple activity used to write data to the workflow log. The example below uses a simple hardcoded string as a log message. Javascript may also be used to include values from the workflow activities. Additional information on log messages can be found here - Log Message.



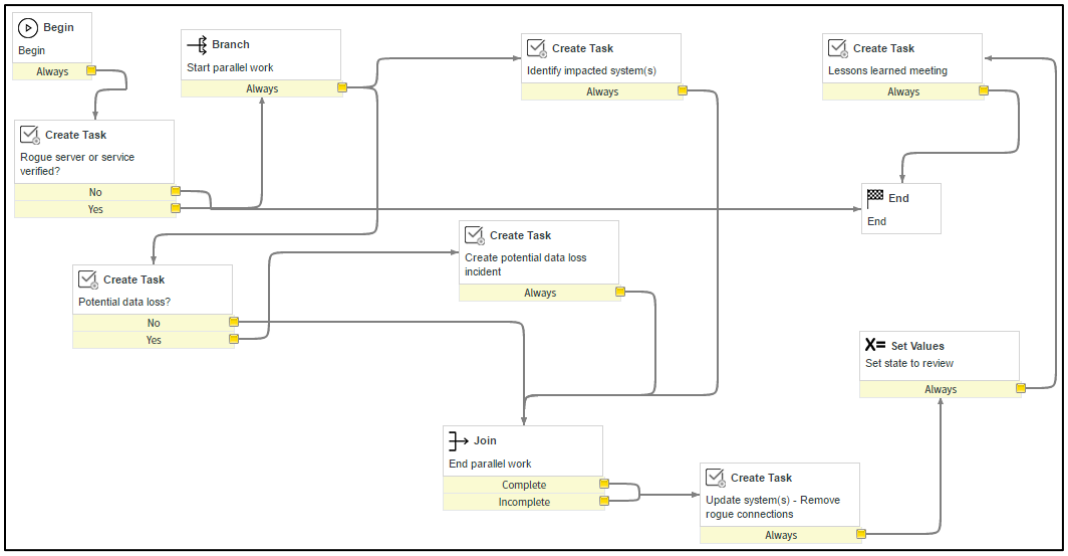
4. Close the activity and the workflow.

Parallel and Serial Work

1. Next, explore how to group activites in a workflow. In the right pane, click the workflow **Security Incident - Rogue Server or Service – Template**.



2. Notice in this workflow that some tasks are happening in a serial fashion, one after another. Often times you need several activities running in parallel. This is done with the activities **Branch** and **Join.** All activities that immediately follow the branch activity can run simultaniously. The Join activity merges those workstreams back to a serial workflow. These are simple activities that require no configuration. Additional information on this activity can be found at Branch and Join.



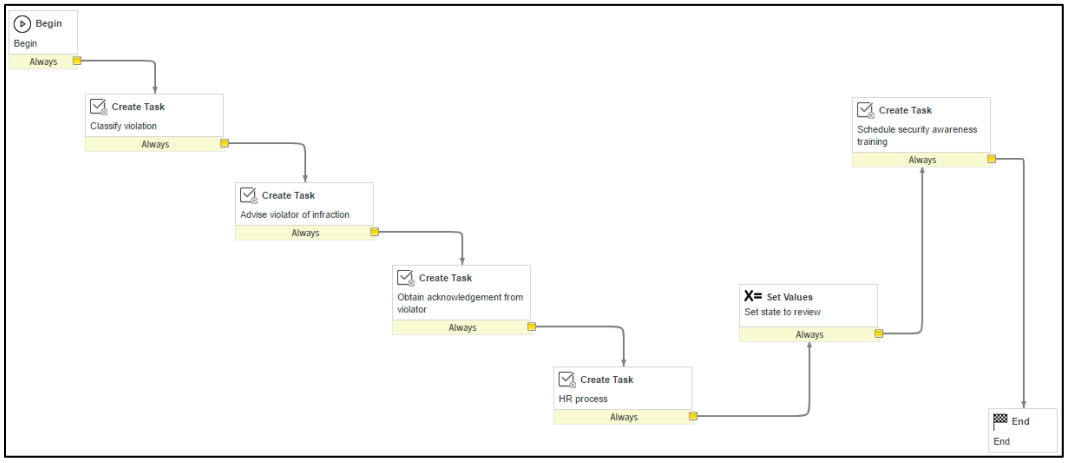
3. Close the workflow.

Update NIST process states

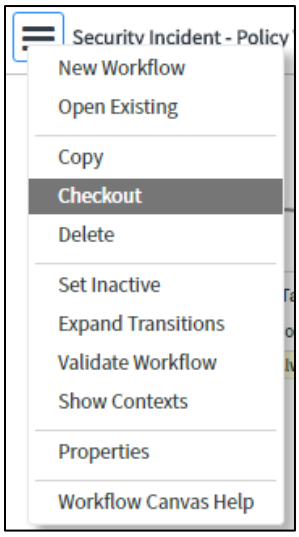
1. The Security Incident workflow includes a mapping to industry standards such as **NIST**. The **NIST 800-61** is the default security incident remediation tracking mechanism in ServiceNow Security Operations. While moving through the workflow, update the state of the Security Incident with the proper state information. Below is an example of how the NIST stages are represented in a Security Incident.



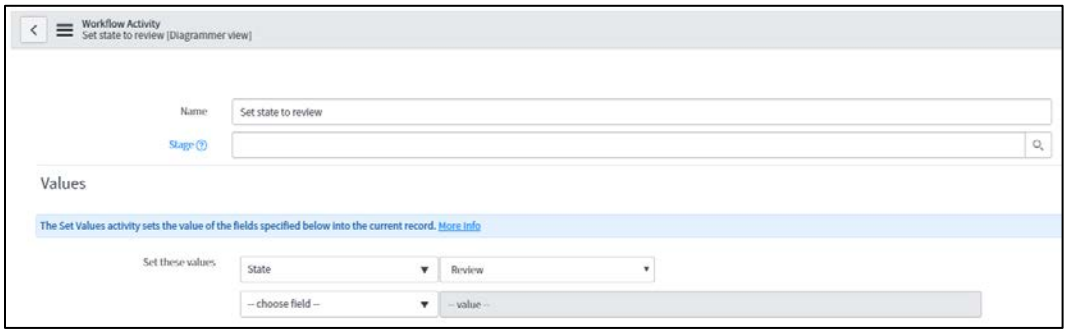
2. Explore some methods for updating the state of a Security Incident. In the **Workflows** tab on the right pane of the workflow editor, click **Security Incident - Policy Violation – Template.**



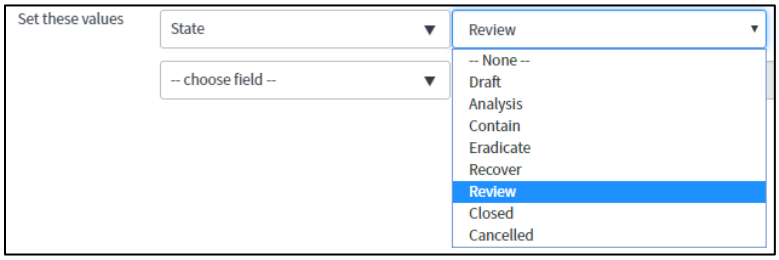
3. In this example, you check the workflow. In the top-left of the workflow, click the ☰ icon, then select **Checkout**.



4. Open the activity **Set state to review**.



5. In this activity, you set the value of **State** to **Review.** Click the drop-down liston the available values.

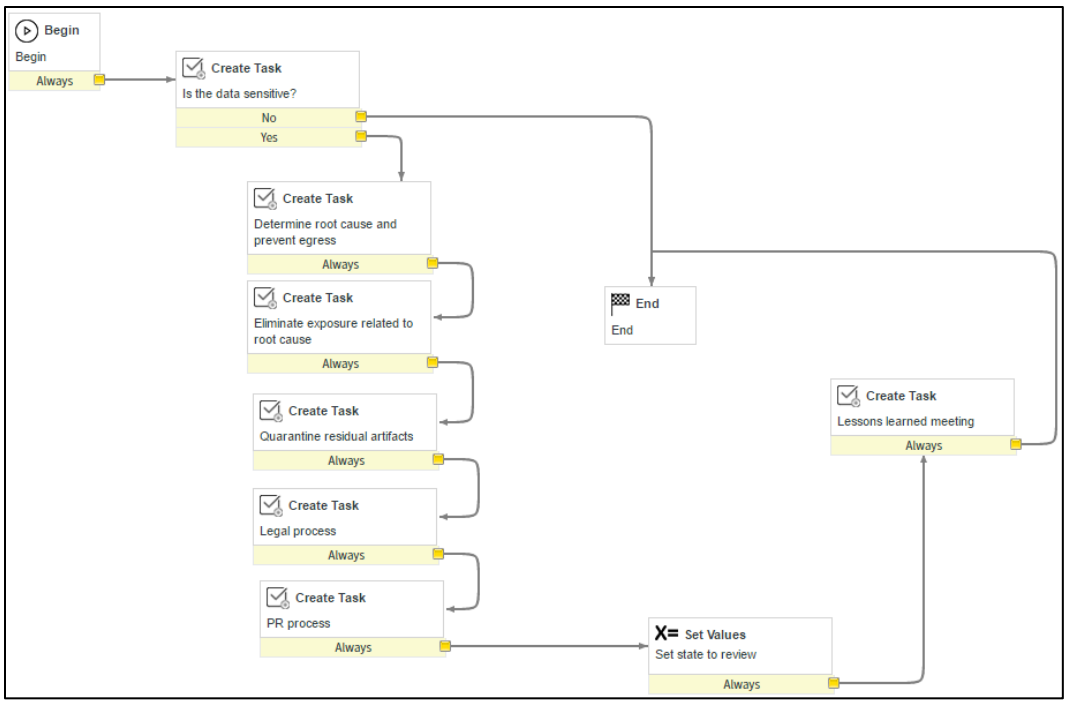


6. Note that these values correspond to the NIST states in this doc above, with the addition of **Cancelled**. Close the activity and workflow. Additional information on the **Set Values** activity can be found here – Set Values.

7. You also can update the state of the workflow using JavaScript. The statement **State = Review** in any advanced activity also changes the **State** value.

Task-Based Decision Making

1. In the right pane of **Workflows** tab, click **Security Incident - Confidential Data Exposure – Template** workflow. This workflow begins with a simple decision: is the data that was exposed confidential. If **No**, you can end the incident; if **Yes**, there is work to do.

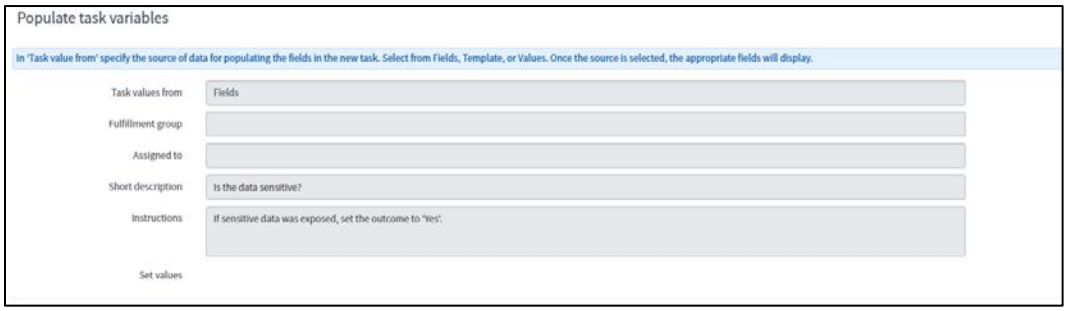


2. Open the activity **Create Task – Is the data sensitive**. Now, look at the options presented in the Basics section.



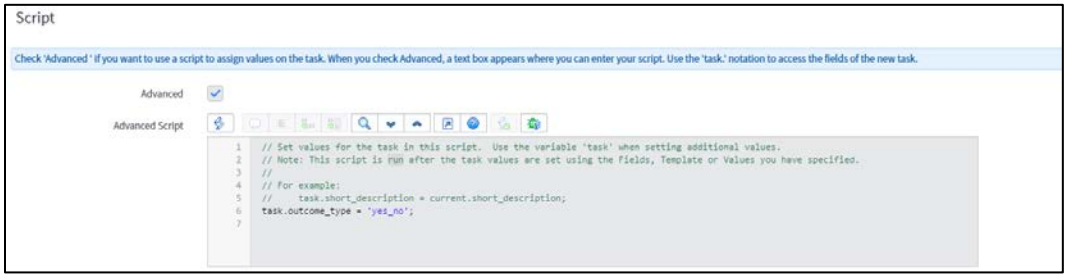
3. We defined a name for the activity, “Is the data sensitive?” and assigned a task type of **Security Incident Response Task**. This task type has additional features such as recording data to the Security Incident Post Incident Review. Wait for this activity to complete before moving on in the workflow as this is a critical decision point.

4. Look at the **Populate Task Variables** section of the activity.

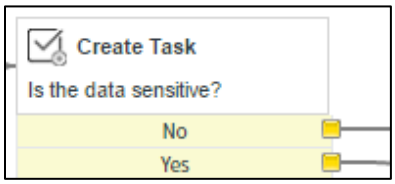


5. You can assign a target group here if required, though in most cases roles-based routing is used. A short description and instructions to the assignee is always important!

6. Scroll to Script defined section to see what the result of this workflow should be. Several options exist, but in this case, use a simple yes/no result.



7. This allows you to map **Yes** and **No** from the activity to other activities.

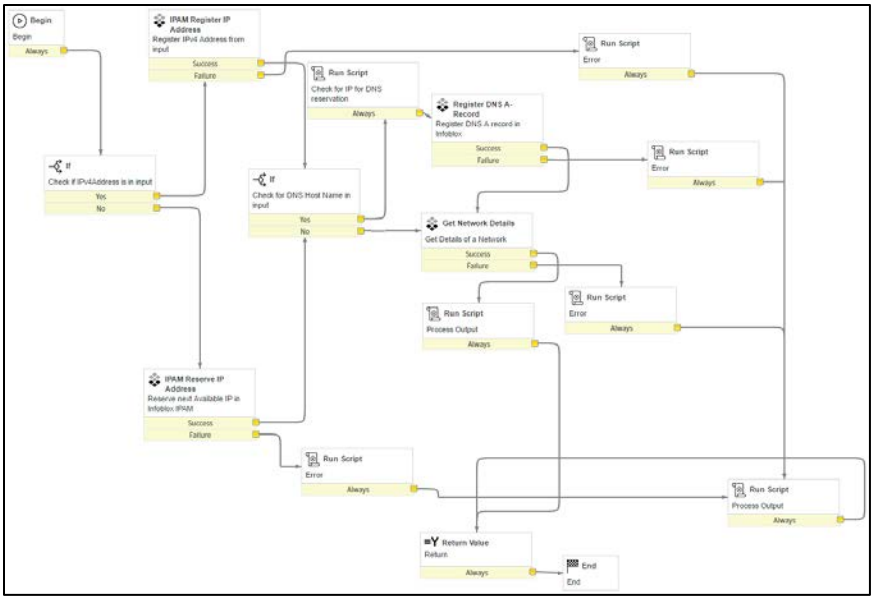


8. Close the activity and workflow.

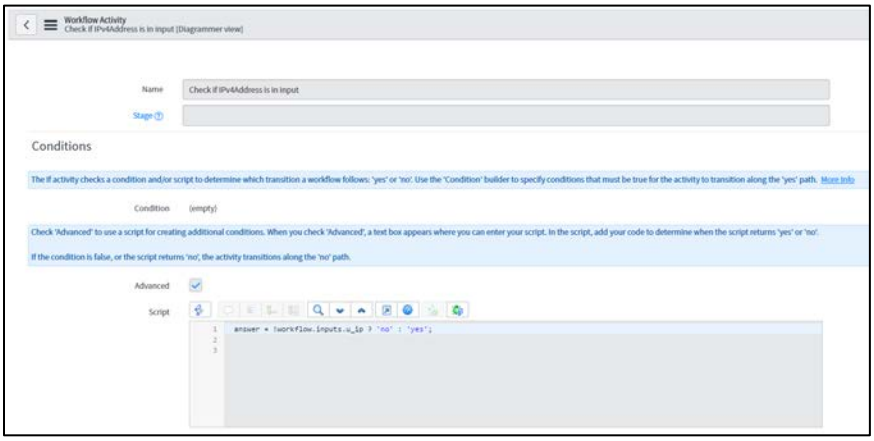
Simple Code Example to Check Values

1. Look at how to use simple code in the workflows to make decisions. In this example, you want to see if the workflow receives an IPv4 Address.

2. In the Workflows tab click workflow Infobox Reserve/ Register IP in IPAM.



3. Open the activity by double-clicking **if – Check if IPv4Address is in input**.

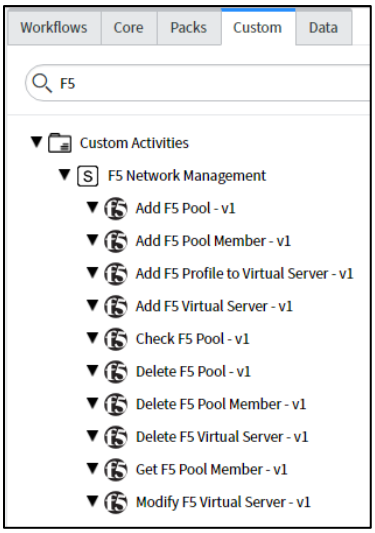


4. Notice that JavaScript checks to see if the value is missing. It returns a **no** value if true, else it returns a **yes** value. While this is a simple example, more complex JavaScript logic can be used in these decisions. You can also query other data from the ServiceNow platform to assist in these dicisions.

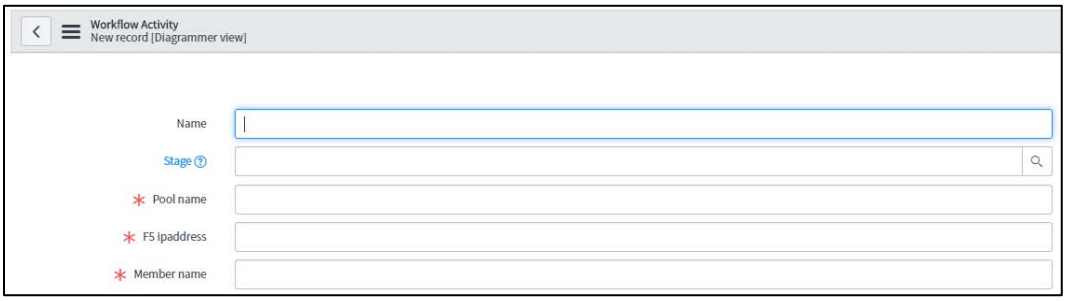
5. More information on the **if** activity can be found here - if.

Custom Activities

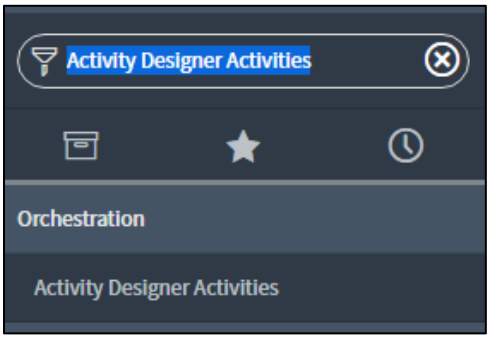
1. Custom Activities allows you to create reusable components, which can be incorporated into workflows. Look at one. On the right pane of the workflow editor, click the **Custom** tab and enter **F5** in the search box.



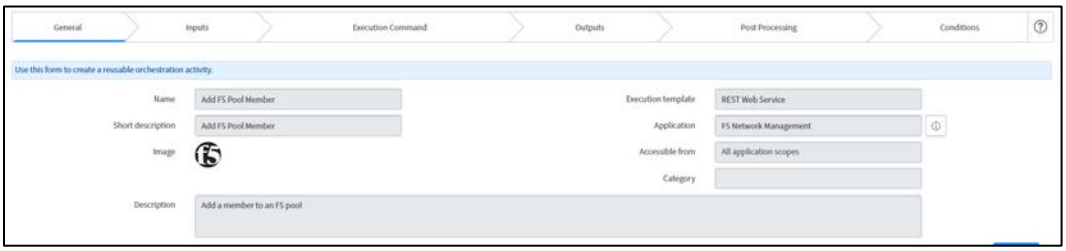
2. Click the **Add F5 Pool Member – v1**. This opens the properties for adding this activity to the pallet, allowing you to specify the pool name, the IP for the F5, and the member name to be added. Look into what is behind this activity:



3. In the main ServiceNow interface, search for **Activity Designer Activities**.



4. Click **Activity Designer Activities** to open a list of all the available activities. In the **Name** filter, enter the activity name **Add F5 Pool Member**. Then left-click the result and bring up the activity designer interface.



5. Note from the General tab:

   The **Execution template** indicates that this activity is part of a **REST Web Service**.

   The **Application** is defined under is **F5 Network Management**. You can create Applications for integrations with the platform. This allows you to have several activities in the custom section of the workflow editor grouped under the application.

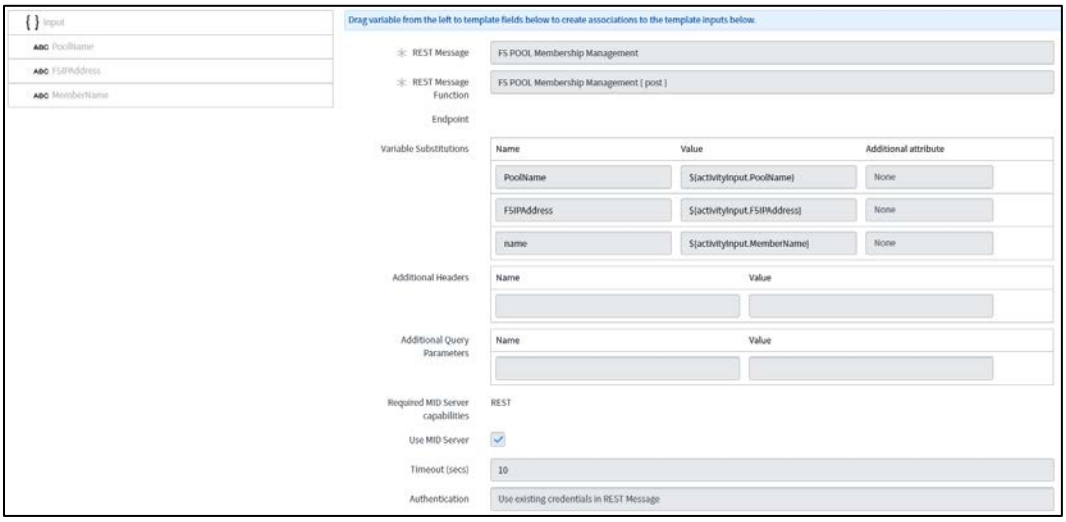
   Accessibility allows you to define where in the platform can this activity be used.

6. Click to the **Inputs** tab.



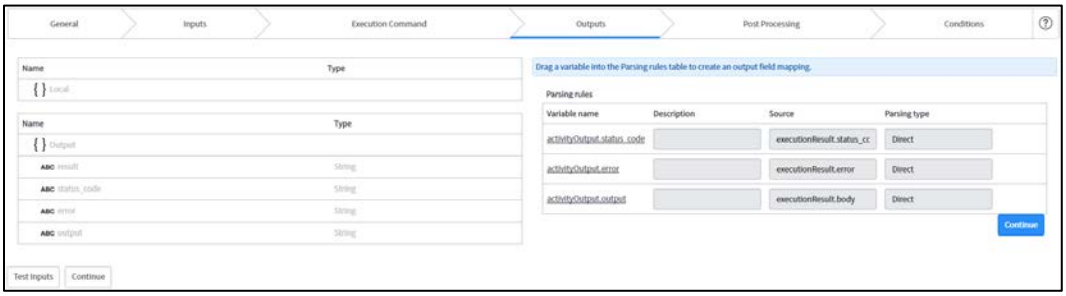
7. Here you define what is required to initiate this activity. The defined fields can be either mandatory or optional.

8. Click the **Execution Command** tab.



9. Execution command allows you to map the input data into the REST message fields. You can also set properties required for the Mid Server here if required by the activity as well as authentication options.

10. Look at the **Outputs** tab**.**



11. This allows you to map the values received from the REST request and map them back to the activity output.

12. Click the **Post Processing** tab.



13. In post processing, you can use script to perform additional functions. In this example, you generate an output status variable for the activity based on the HTTP return code.

14. Click the **Conditions** tab. Here you use the status variable to generate an ouput status condition for the activity.



15. Close the activity designer.

Lab Goal

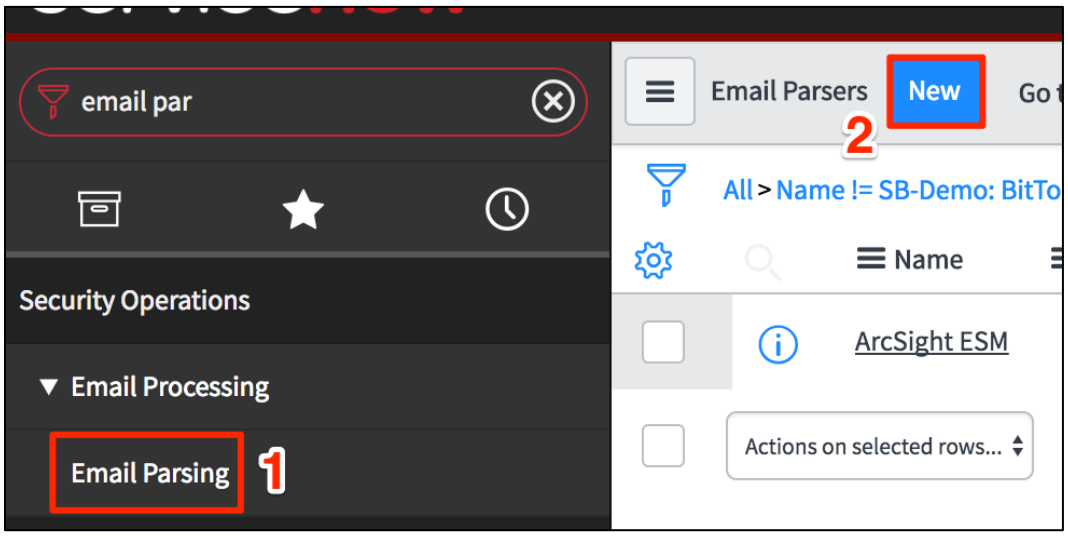
Lab 4
Configure Security Operation Email Parser

This lab includes all the steps needed to configure a security operation Email Parser.

Email Parser creates records from your email alert and parses details in to designated fields on your record. This information can then be used to run IoC lookups, trigger workflows, etc.

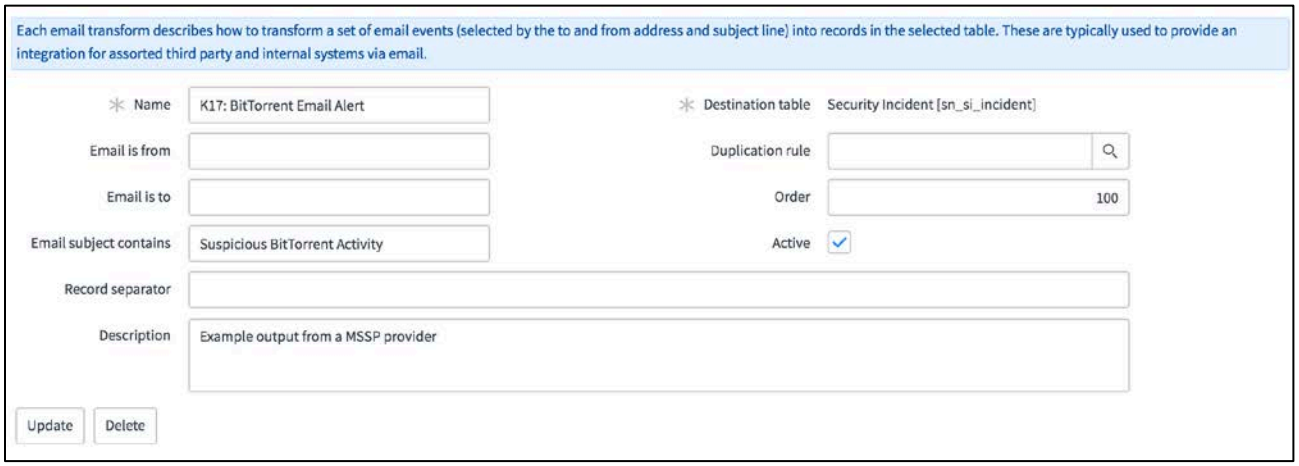
Log On to Your Lab Instance

1. Log on with provided credentials.
2. In the left navigator, go to **Security Operations > Email Parsing > New**.



3. Here you define what the email parser is being used for, and how. Fill in the following fields from the image below:

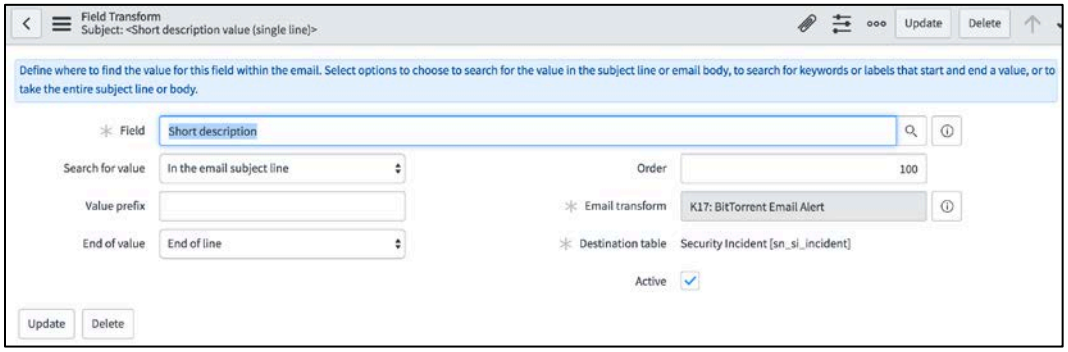
   Name: **K17: BitTorrent Email Alert**
   Email Subject contains: **Suspicious BitTorrent Activity**
   Description: **Example output from a MSSP provider**
   Destination table: **Security Incident [sn_si_incident]**



4. Click the  in the top-left corner -> **Save**.

5. Now define what attributes from the email get parsed, and where those values are placed on the created record. Click **New** in the **Field Transforms** related list and complete the following from the image below:

   Field: **Short Description**
   Search for value: **In the email subject line**
   End of value: **End of line**
   Order: **100**
   Please take a moment to visit our doc site and review the definitions to these fields so you understand how it actually parses the email (doc link).



6. Create more: Before updating the field transform just created, click the  in the top left and click **Save**. This keeps you on the record and allow you to insert modifications and new records with ease. Change some of the values:

   Field: **Source IP**
   Search for value: **At the start of a line in the email body**
   Value prefix: **IP:**
   End of value: **End of line**
   Order: **200**

7. **DO NOT SUBMIT!** Click the  and choose **Insert and Stay**. This submits the new record without overwriting the initial one. You now have 2 field transforms. Create few additional ones (for a total of **5**):

   Field: **Malware Hash**
   Search for value: **At the start of a line in the email body**
   Value prefix: **Malware Hash:**
   End of value: **End of line**
   Order: **300**

8. Remember to **Insert and Stay**, not submit or update!

9. **THEN:**

   Field: **Attack network**
   Search for value: **At the start of a line in the email body**
   Value prefix: **Zone:**
   End of value: **End of line**
   Order: **400**

10. Remember to **Insert and Stay**, not submit or update!

11. **THEN:**

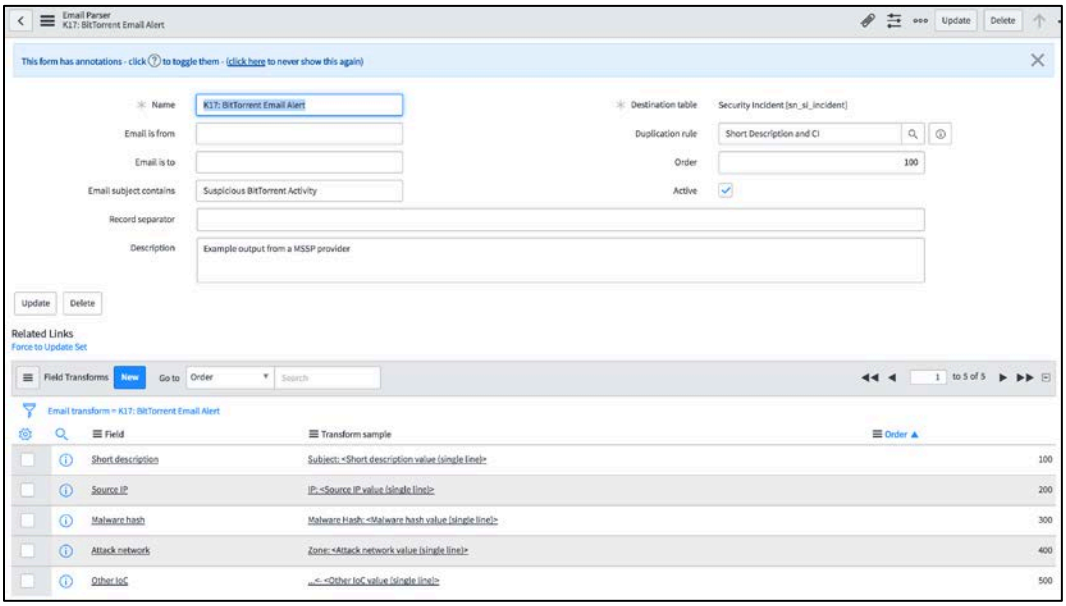
    Field: **Other IoC**
    Search for value: **Anywhere in the email body**
    Value prefix: **<-**
    End of value: **End of line**
    Order: **500**

12. Just **Insert** this time because it is the last field transform.

13. Last, identify a **Duplication** rule. A duplication rule dictates how the system handles a duplicate inbound email. First a pattern is defined, then an action is chosen. In this simple case, you already created one that looks for the same description and CI, then adds it as a child incident to the initially created incident. In the Duplicate rule field, choose **Short Description** and **CI**. For more information on duplication rules, please review our documentation.

Lab Success Verification

1. Your Email Parser should look like the example.



Lab Goal

Lab 5
Build Security Operation Workflow

This lab includes the steps needed to build a real-world example of **Security Operation Workflow**.

Security Operation Workflow Use Case

A customer's MSSP monitors the network for anything suspicious. Upon receiving an alert, the MSSP immediately sends and email alert to the customer about a BitTorrent activity. The customer leverages the ServiceNow Security Operations solution to consume the alert, automatically create a security incident, enrich the incident with data for determining course of action and prioritization, and leverage workflow to respond in a timely manner. This lab explains how to design the workflow.

Log On to Your Lab Instance

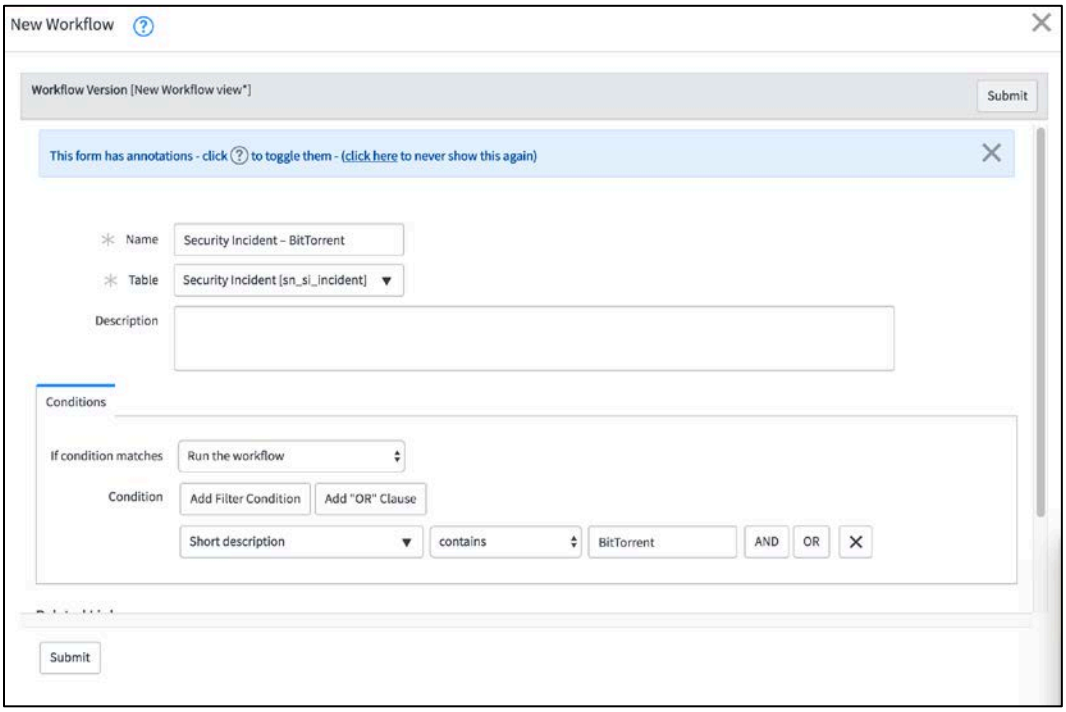
1. Verify you are still logged in as System Administrator. Also, confirm that you are still in the **Security Incident** application scope (refer to the beginning of this entire lab).

2. In the left navigator, navigate to **Workflow** -> **Workflow Editor** -> and click the  at the top right of the screen.

3. Populate the following fields:

   Name: Security Incident – BitTorrent
   Table: Security Incident [sn_si_incident]
   Conditions:
   --choose field-- : Short description
   Change 'starts with' to 'contains'
   Type: **BitTorrent**

4. Click **Submit**.



5. You now have an empty workflow canvas to work with and build a workflow to manage the use case.

6. Drag the 

to the bottom right corner of the canvas. This gives you more room to work.

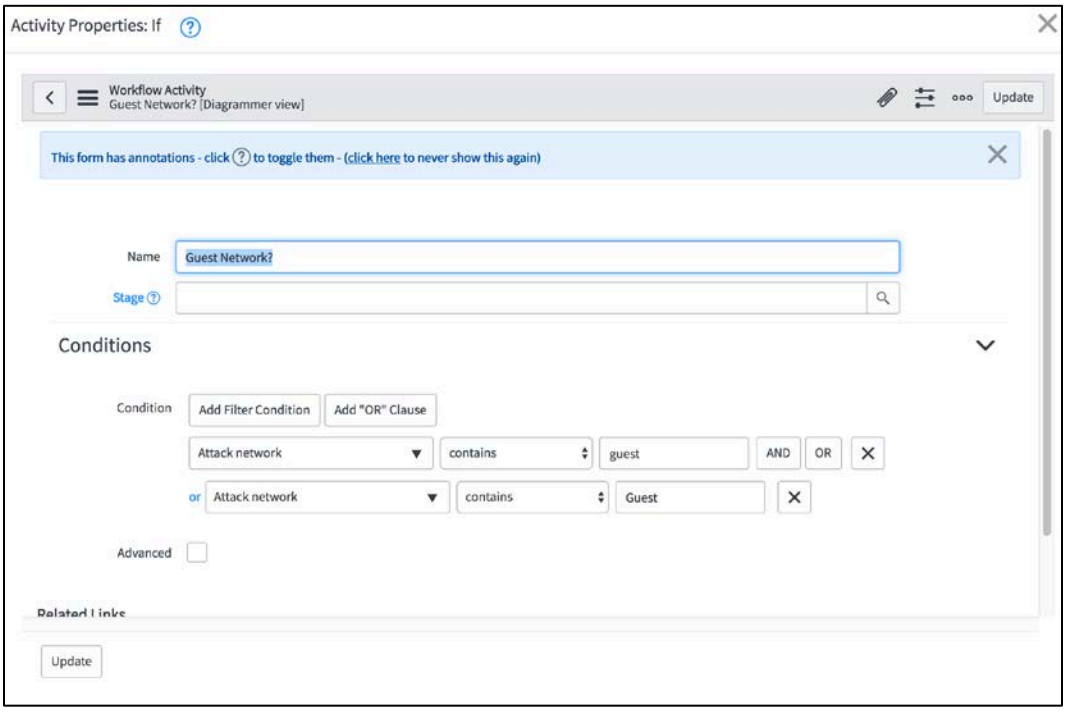
7. Click the line so that it turns blue, then press the **Delete** key to remove the line. You redraw this after creating all the workflow activities.

Now, assume a customer might have 2 ways they respond to a BitTorrent incident – one option if it's a known host (an employee), and another if it's a guest that has joined the guest Wi-Fi network. ServiceNow's workflow can handle that. Start by creating an "If" activity to check which Wi-Fi network the intruder has joined.

1. On the right pane, click the **Core** tab and search for **If** (grouped under Conditions). An If condition evaluates whether a certain value is true or not. Drag it onto the canvas to the right of the 

activity and release.

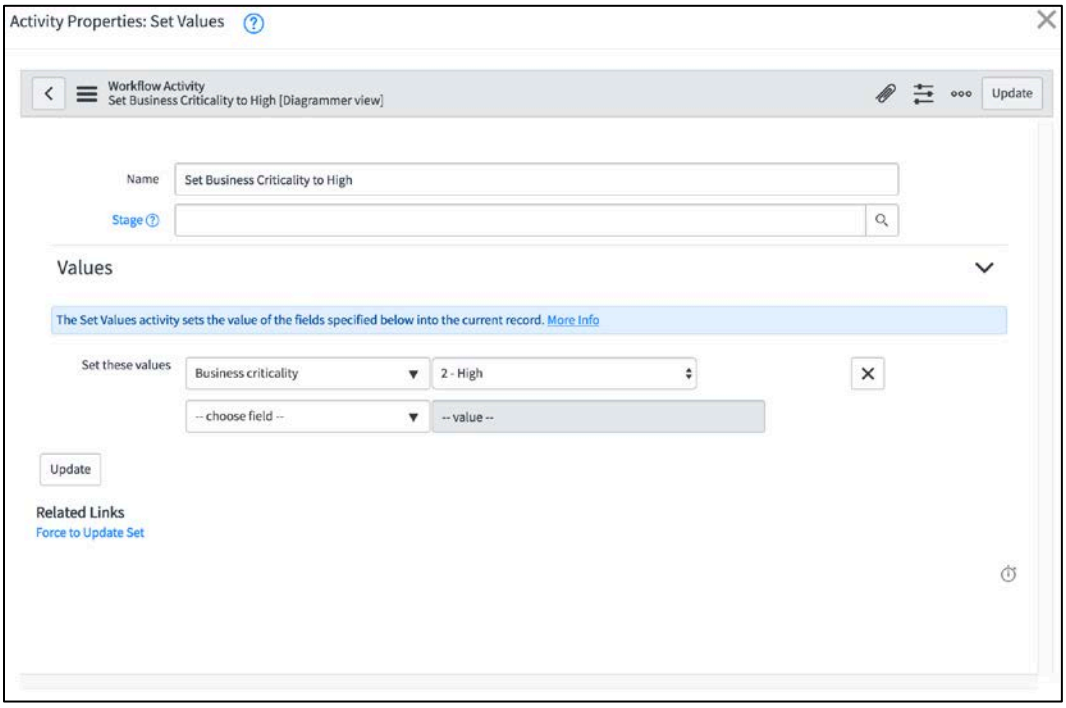
2. Compete the form according to the example:



3. Click **Submit**.

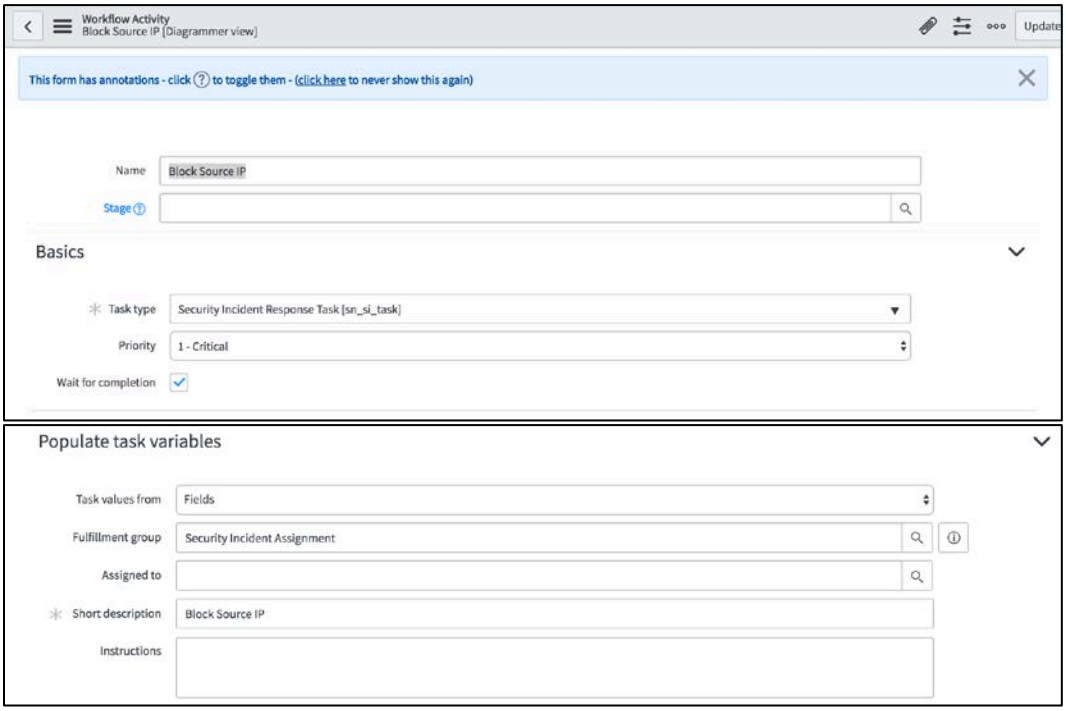
4. Assuming yes, the intruder is on a guest network, be sure to raise the business criticality on the incident to **high** so that it is better prioritized. On the right pane, search for **Set Values**. A Set Value activity does exactly what it says – sets a value of the choice on the security incident. Drag it to the right of the last activity and release.

5. Complete the form according to the example:



6. Click **Submit**.

7. Since this is an anonymous intruder, there is no sense in letting him/her hang out on the network any longer. Leverage the powerful integration to Palo Alto's firewall to have the analyst drop the intruder from the network and block him from joining again.
   Note: this is conceptual; this lab is not integrated to a live PAN environment. On the right pane, search for **Create Task** (under Tasks). Drag to the right of the previous activity, and complete just the values from the example:



8. Set the status of the incident to recover, now that you successfully automated the blocking of an IP on the network. You can start to relax again (or can we?). Drag a **Set Value** activity to the right of the previous activity and set the **State** to **Recover** (do you remember how you did this earlier?).

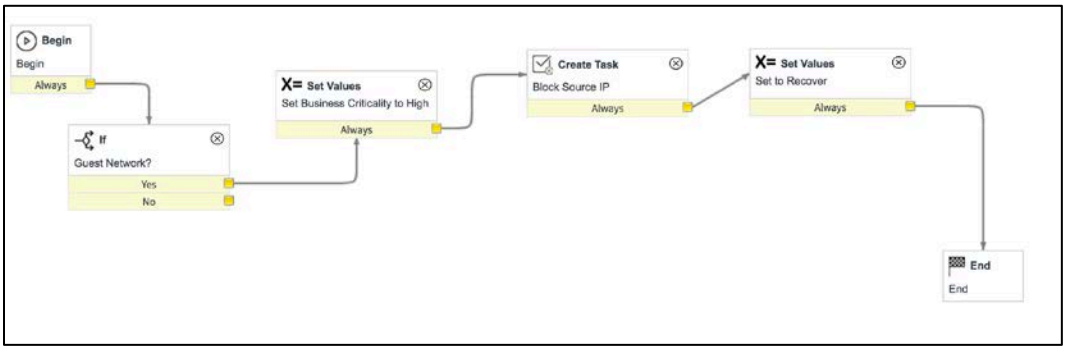
9. Now connect the dots for the path of the workflow! Starting at **Begin**:

10. Click the and hold, then drag the line to the next **If** activity.

11. On the **If** activity click the next to the **Yes**, hold, then drag to the next **Set Values** activity.

12. Do the same for the remaining activities in that path all the way to **End**.

13. So far, the workflow should look something like the example:



What happens if the intruder is known – an employee!!! This section explains how to automate the process within the same workflow for handling that use case.

14. Look at the first activity – the If: Guest Network. Begin building out what happens if the answer is No. Start with setting some values. You can set more than one value on the record with a single activity. Drag a Set Value activity just below the If condition you started with.

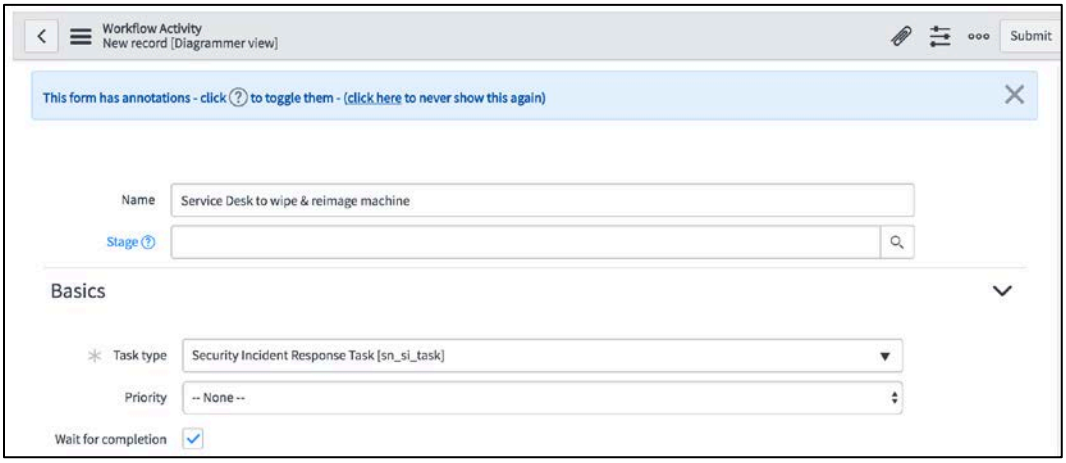
15. Set values for both Business criticality to Critical (since this is an insider threat), and

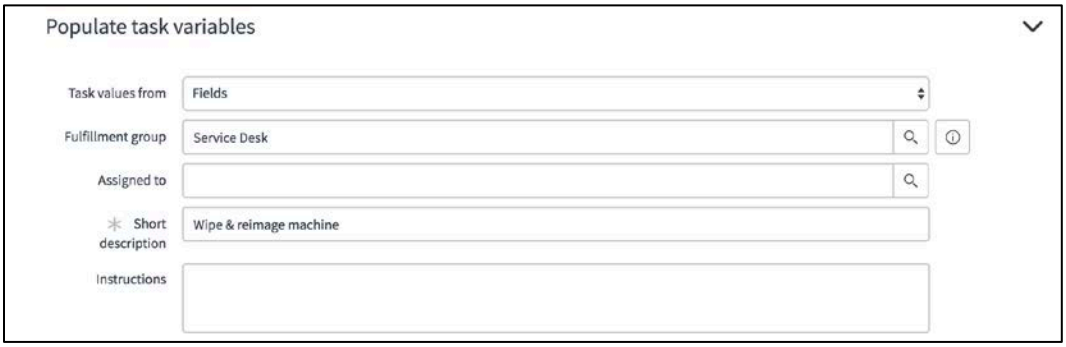
16. Set State to Eradicate.

17. Click Submit.

A huge advantage of ServiceNow is the platform – working from a single system of record. Often, security teams need to involve other groups (e.g., IT, HR) in their investigation/response process. If those other groups are also managing work in ServiceNow (as they should!), then it becomes super simple to engage them programmatically from workflow. In this next step, you give instruction to the IT service desk to assist.

1. Drag a Create Task activity to the right of the previous one, and set the fields based on the following example:





Note: You assigned the fulfillment group to Service Desk. This typically requires a security analyst to enter another system, send an email to another group, or pick up the phone and request help – all of which leave no accountability, traceability, or visibility—terrible! ServiceNow automates the work to be routed to the right group. This can be traced and have SLAs attached to it. Simple.

2. Create one more **Set Value** to set the **State** to **Recover**.

Time to wrap this workflow up! Connect the dot for this path of the workflow.

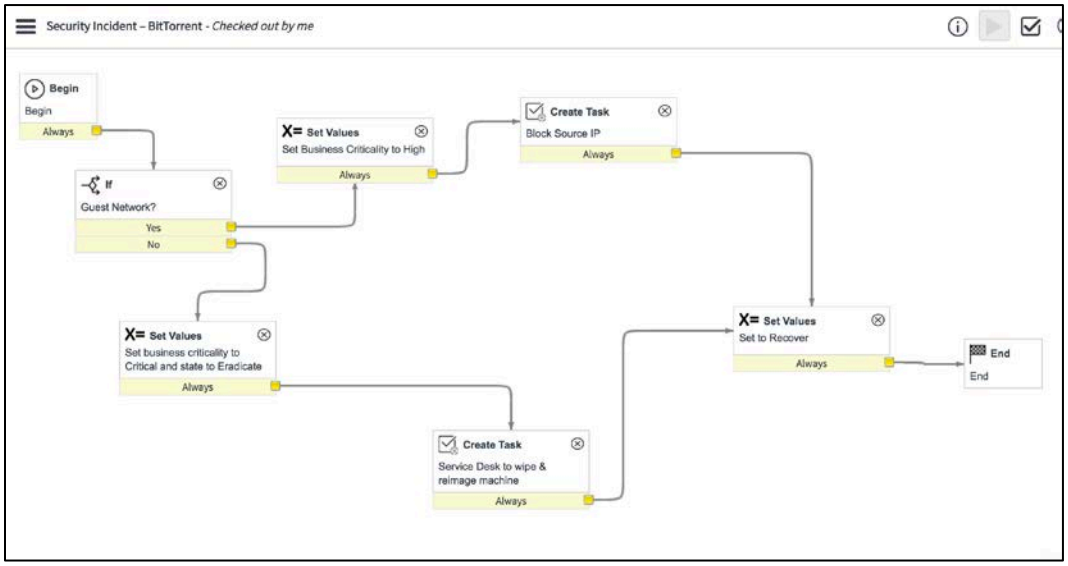
1. Starting at the **If Guest Network**: Click and hold the next to the **No** path, then drag it to the **Set Values** activity.

2. Click and hold the from the **Set Values** activity to the **Task** you created.

3. Continue until you connect to **End**, but make sure to connect your **Service Desk Task** to the existing **Set Value for Recover**. When workflow paths converge to the same path, it is appropriate to share activities.

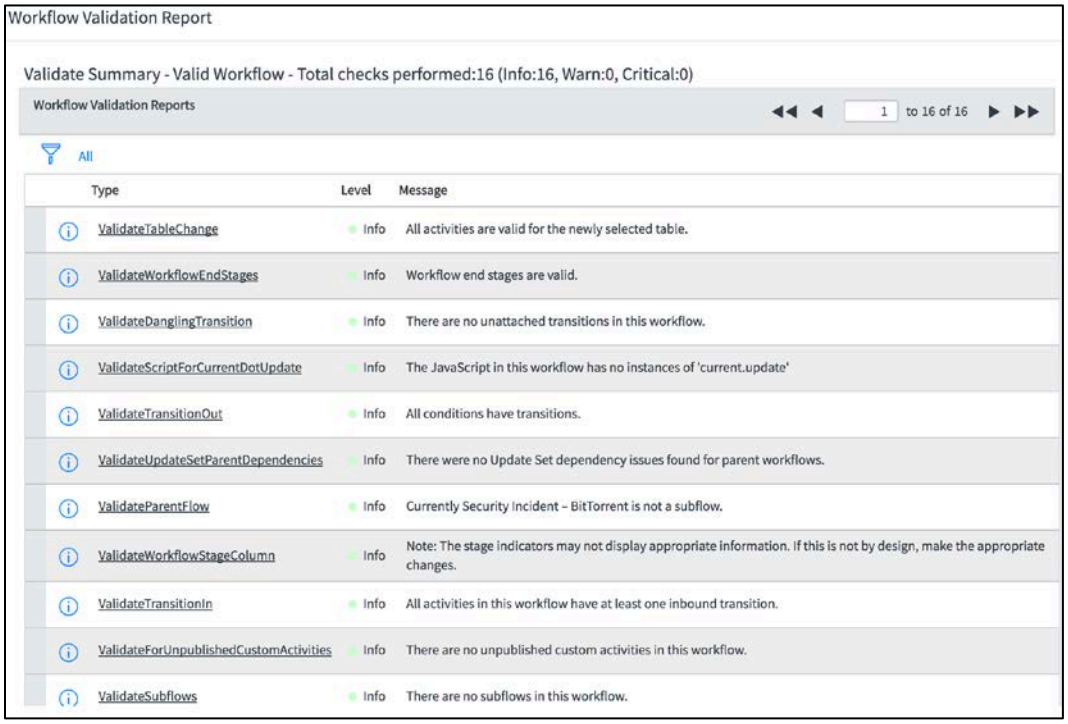
Lab Success Verification

1. Your final workflow should look like the example:



2. If all looks good, Validate and Publish the workflow for immediate use!

3. Click the ☰ at the top-left corner of the canvas. Choose **Validate Workflow**. This goes through a process to check for critical flaws that would leave a workflow inoperable. You want to see all green, like the example.



4. Click the ☰ and **Publish**. This officially activates the workflow and you can expect it to run as defined when creating the workflow initially.

Lab Goal

This lab includes all the steps needed to test and demonstrate the **Email Parser** and **Security Operation Workflow** built in the previous lab.

Lab 6 Test/Demo What You Built

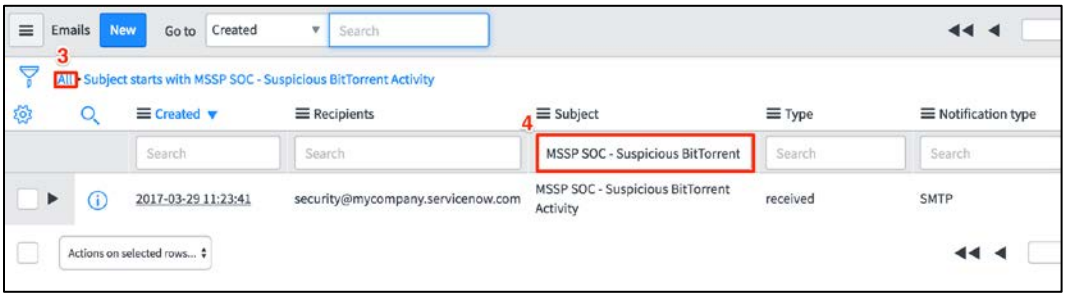
Log On to Your Lab Instance

1. Verify you are still logged in as System Administrator.
2. Also validate the receiving inbox for all security related alerts. For your convenience, we created some relevant bookmarks. Find these by clicking the ★ on the left navigator. Choose **Security Inbox Properties**.
3. In the top of the properties page is message box advising that you are about to edit a record that is in a different application scope. That is OK. Click to edit the record (see example).



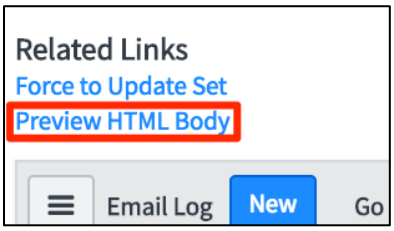
4. In the first property titled **Inbox for Security Operations tools** verify that **security@mycompany.servicenow.com** is the value. If not, replace the existing with this.
5. Go to the bookmarks again and choose **Email Log**.
6. Be sure to click the **All** in the breadcrumb to remove any filters.
7. Then search on the **Subject** column for **MSSP SOC – Suspicious BitTorrent Activity**.

8. Click **Enter**.

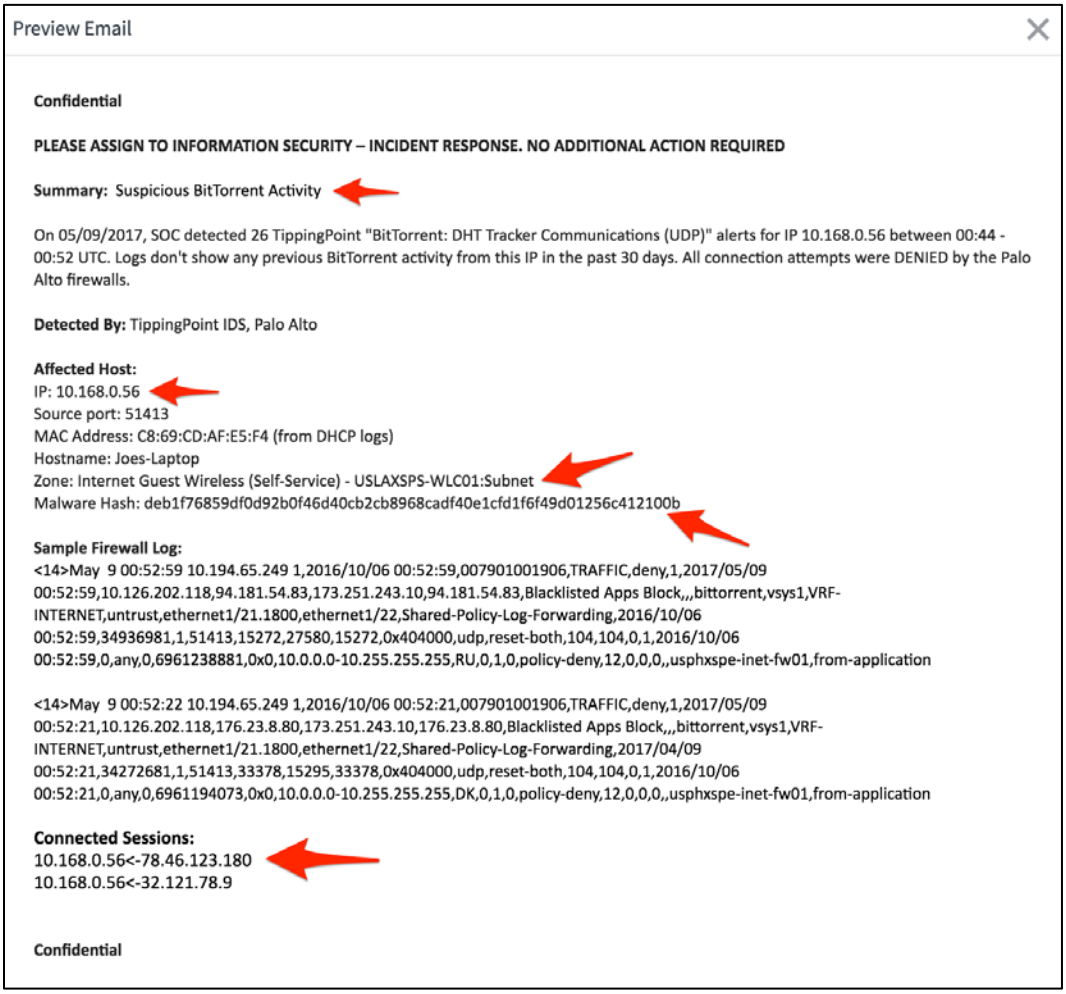


9. Click the ⓘ next to the one email record to view the details of this record. This is a raw version of an email that has been received by the system. For today, reprocess this email to validate the email parser created earlier does what it is designed to do – consume the email and parse out the details you want!

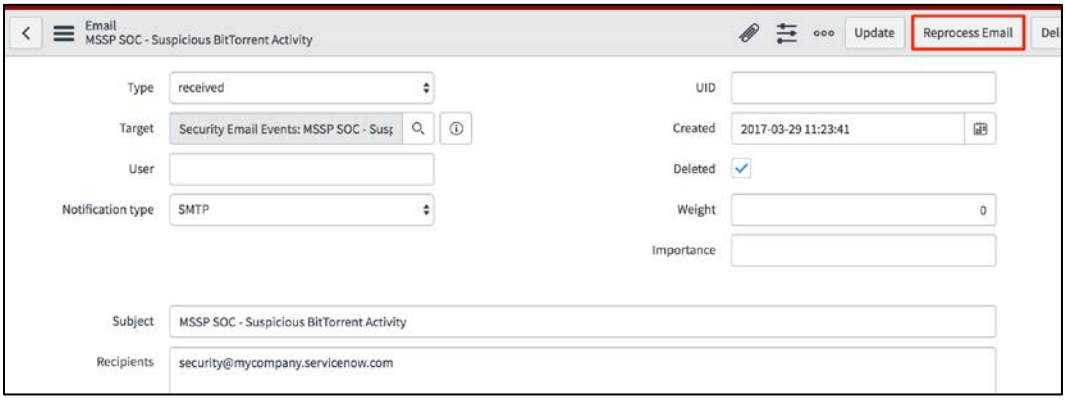
10. Preview before processing the email. Click the **Preview HTML Body** link under the Related Links section (towards the bottom of the record).



11. Note the details about **Summary, IP, Zone, Malware Hash,** and **Connected Sessions**. These are the things you told the email parser to look for, remember?

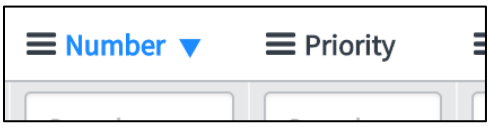


12. Now you can process this. Click the **Reprocess Email** button in the top right of the pane. This also creates the new security incident.



13. In the left navigator, type **Show Open Incidents** to move to a list of existing Security Incidents.

14. Reverse order by the Number column by clicking the header until the blue arrow is pointing down (see example).



The newly created security incident should be sitting at the top, verifying that the email parser successfully consumed the email alert and created the incident. Click the ⓘ next to the record to view the details of the incident. Also notice the result of the parsing, any workflows that have been triggered (including the one created), as well as any threat intelligence used to enrich the incident (also managed by workflow).

1. Note the following that was successfully parsed in from the email:

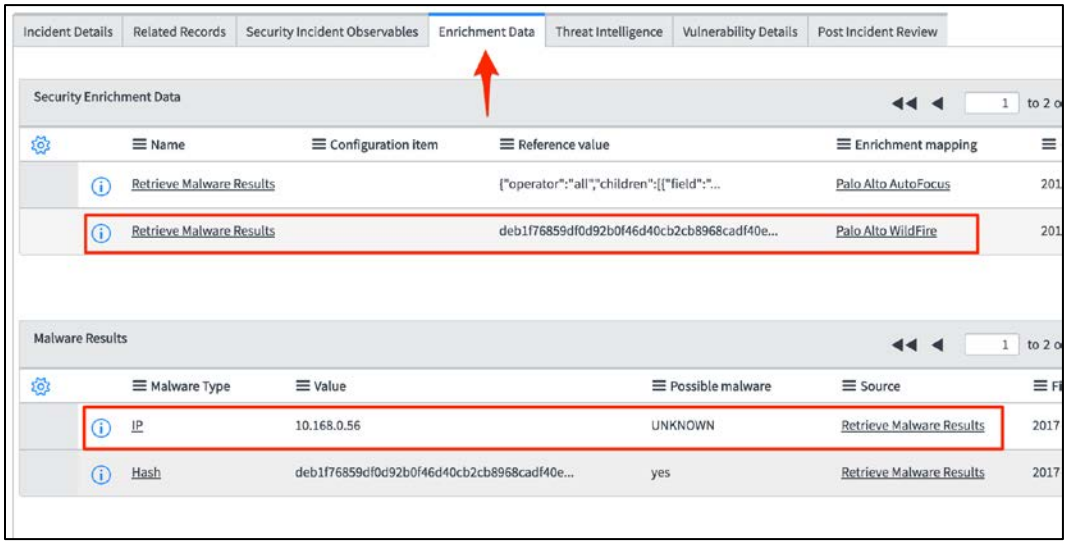
   Short description
   Under the **Security Incident Observables** tab:
   - Source IP
   - Malware hash
   - Other IoC
   - Attack network

   Awesome? Yes.

2. See how this incident was enriched. Under the **Enrichment Data** tab, find the following:

   Palo Alto Wildfire integration was run via workflow. We scanned the Malware Hash (parsed from the email alert) and retrieved results, and even attached a nicely formatted PDF report to the incident. Scroll to the top of the record and click the PDF attachment to review.

   There were also malware results for the IP you parsed.



3. After retrieving all that great information about this threat, you can see how Threat Intelligence was leveraged to compare the data against known indicators of compromise. Click the **Threat Intelligence** tab and note the following:

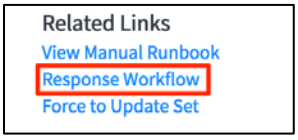
   There were **Associated Observables** discovered from the connected session we parsed. Because ServiceNow is able to catalog IoC information through integrations to public threat feeds and third-party threat tools (like Wildfire), this observable was cross referenced with known IoC – in this case, **TorrentLocker**.

4. Drill into the **TorrentLocker** record under **Associated Indicators**. Note the description and related information across the bottom of the record. Powerful.

5. Click **back** on the browser to return to the security incident.

   - How did workflow come in to play?

1. In the **Related Links** area, click on **Response Workflow**. A new window pops up with 3 workflows running across the top, including the **Security Incident – BitTorrent**, one you created. Review this one first.

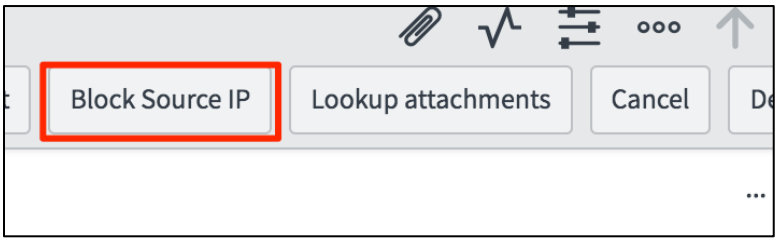


2. Some of the workflow activities are blue, meaning these have completed. The green one shows where you are at currently in the process. In this case, it successfully identified the intruder as being anonymous and on the guest network. This you know because of the activity looking for **guest** in the description of the **Attack network** field. You set the incident State and are now ready to block the source IP (as stated in the create task activity).

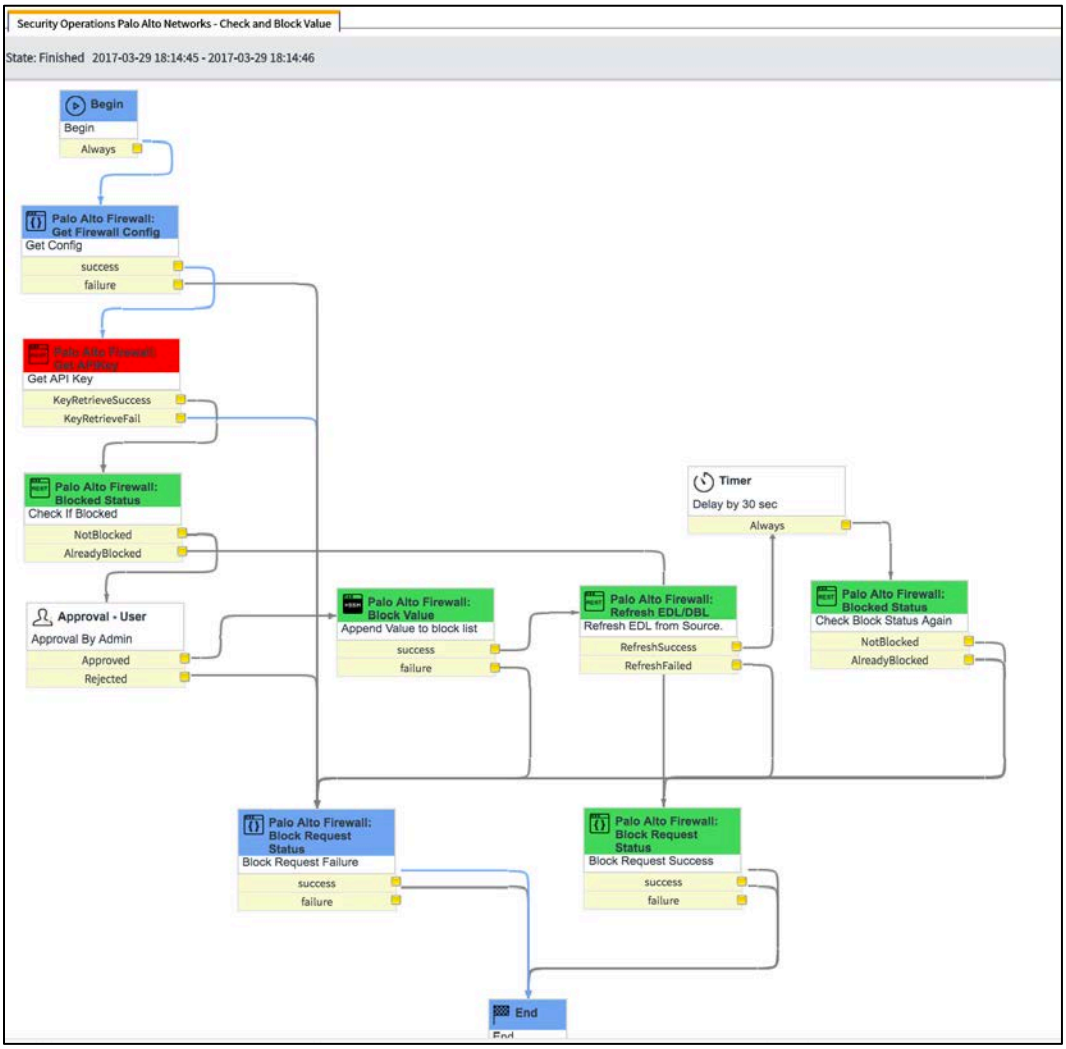
3. Return to the browser tab with the incident, and notice a **Response Task** was created in the related lists at the bottom of the record.



4. On the top right of the incident record, you should see a button to **Block Source IP**. This leverages an included orchestration workflow to block a source (e.g., IP, URL) in Palo Alto's firewall. Keep in mind you are not actually connected to PAN during the lab, but please do click the button and see how it populates the **block value** and kicks off the workflow. Click **Show Block Request Workflow** (see following examples).







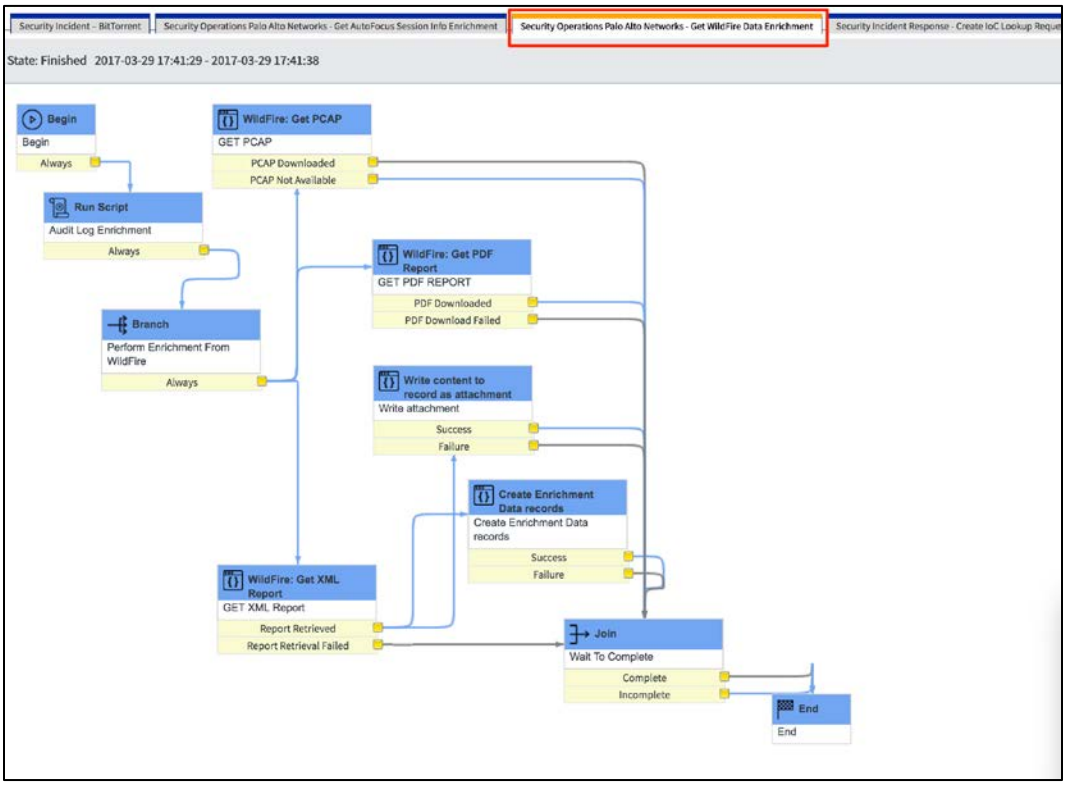
5. Return to the browser tab with the security incident. Close out the task. Double-click the white space under the Outcome column of the Response Task.

   Outcome type: Yes/No
   Outcome: **Yes**

6. Click the ✓ icon to confirm.

7. Verify the workflow has completed. Click the **Response Workflow** under **Related Links** and see that the workflow has turned blue down the path it took. Neat!

8. Also feel free to browse the other workflows that are running, like the **Get Wildfire Data Enrichment**. All using workflow to manage work in and out of ServiceNow, and bidirectional integrations to other systems!



Lab Success Verification

1. All workflow should be complete.