Lab Guide

Accelerating Security Incident Response, Including Threat Intelligence

Joseph Wheeler & Erich Dobroth

Default Login / Password: Knowledge17

admin / Knowledge17

itil / Knowledge17

employee / Knowledge17

Lab Sponsored by Amazon Web Services



This
Page
Intentionally
Left
Blank

Lab Overview

Lab Introduction

This lab introduces the new Security Incident Response application. You use a different persona in each lab subsection to see how Security Incident Response can streamline your process, time to resolution, and post assessment review.

Because you use multiple personas, all your passwords on your instance are set to Knowledge17.

But first, meet our players!

Lab Personas – (Login ID Is in the Parenthesis)

- **Security Manager (si_manager)** – This is the department head or administrator of the Security Incident application. They oversee making sure all work contains the proper information, routes correctly, and that the incident moves to a closed state when ready.
- **Security Commander (si_commander)** – This persona is primarily responsible for the incoming incident and gathering all the post incident information into the Security Incident.
- **IT Technician (si_user)** – This persona is someone who may be on your security team or in your IT organization. They are responsible for completing a task that is auto-assigned to them. They complete the task through a variety of steps, and once the task is complete they notify the Security Manager that they are done.
- **Human Resources (hr_user)** – This persona shows you how to involve another department in your security process, while keeping them siloed out into their own task and workflow.

Lab Goal

This lab uses the login of the Security Technician. A security issue has arisen from one of the monitoring tools. This event generated an alert in ServiceNow and a Security Incident has been opened by the system. This persona overviews the incident, making sure that everything in the incident is correct, and progresses it through the workflow.

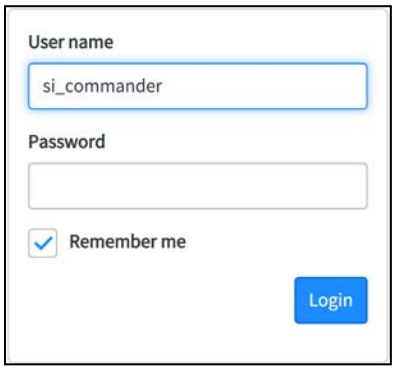
Lab 1.0
New Security Incident Received

ALERT! A New Security Incident Has Arisen!

1. You have received a notification from your ServiceNow instance! It is time to jump into action and start taking care of business!

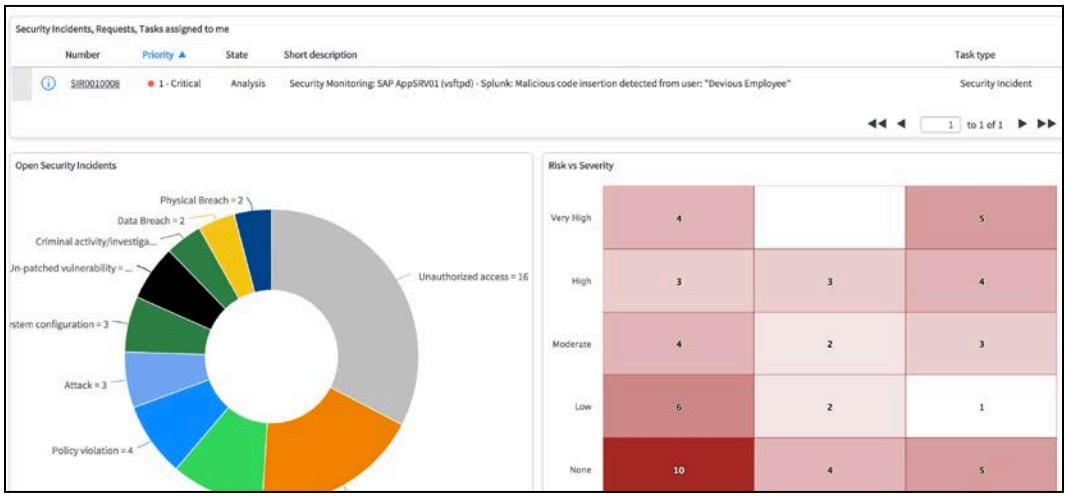
2. Navigate to the unique instance URL provided to you.

3. Log in to your instance as the Security Technician. The user id is **si_commander** and password is **Knowledge17**.

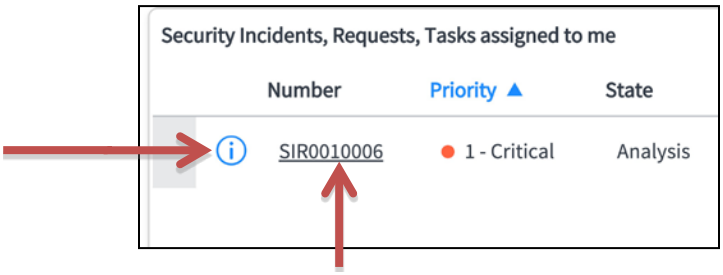


Get to Your Work from Your Dashboard

1. Welcome to your Security Incident dashboard! Here is an example of a dashboard containing reports available to you, most important is the top section, which is the work assigned to you.



2. Go into this new incident. Click the blue **i** icon or the **Incident Number**. (Your incident number may be different than the one in the image)



3. You are now in the Security Incident assigned to you.

4. Along the top, you can see what stage the incident is in, based on the NIST standard process that ServiceNow has included in the platform for you.



5. In the Analysis stage, you can overview the incident to see what is going on and that all the information in it is ready to move it forward to remediation.

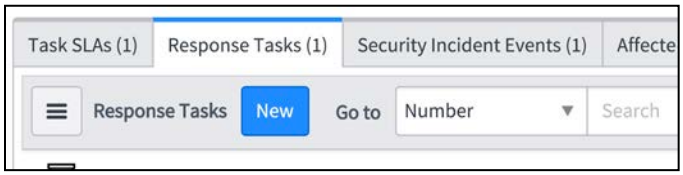
Security Incident Overview

This section touches on the important pieces of the incident that were generated in the system.

1. The focus on the right side is the assigned criteria. Using ServiceNow means you get all the functionality of that single platform, including the robust assignment engine. **Assignment group** and **Assigned to** are set via the workflow running for this incident, and by using the On-Call Rotation functionality (which can be enabled via a plugin). You were assigned this task based on your availability, which could consider things such as skill level, your current workload, and whether you are on shift or on call.

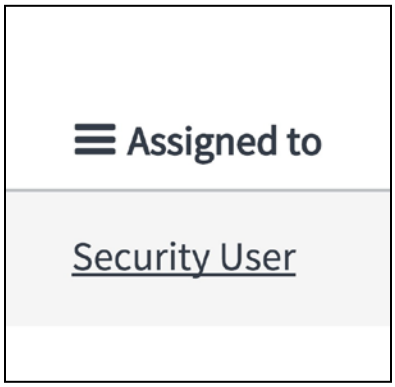


2. Next read the **Short Description** to find out what happened.
   - Find the field **Short Description**.
   - This description should read **Security Monitoring: SAP AppSRV01 (vsftpd) - Splunk: Malicious code insertion detected from user: "Devious Employee**."
3. UH OH! Someone internal has inserted some code into the system. Luckily the monitoring tool knows who the user was! Get the malicious code contained or eradicated first, and then have HR have a conversation with that user!
4. Scroll to the bottom to see the related list of records in the system. Make sure you select **Response Tasks** tab by clicking on it.



5. A task appears that was automatically generated in the system for someone to scan and remove the malicious code.

6. Look at the task; it is assigned to **Security User**.

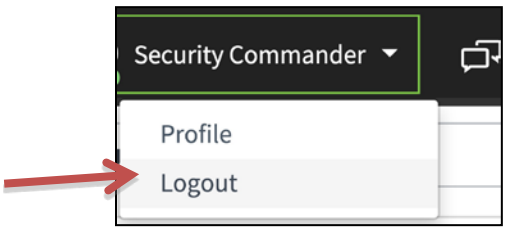


7. To see the details of the task, hover over the **I** icon in the list. Here you see that the system has already assigned it to a group and is ready to be worked on! Log out and work this task as the Security User.

8. To log out, in the upper-right corner find your name, image, and a **white** drop-down arrow.



9. Click the white **arrow**. A drop-down list appears. Select the **Logout** option.



Lab Goal

In this section of the lab, you log in as the IT Technician. The purpose is to find the task assigned to you, work the task, and then upon completion let the Security Manager know you are done.

Lab 1.1
Work a Security Task

IT Department! You Have a Task Assigned to You That Requires Immediate Attention!

1. Log in to your instance as the IT Technician. The user id is **si_user** and password is **Knowledge17**.



Fix the Wrongdoing!

Welcome Security User. Here you see the same dashboard that the previous persona encountered on login. However, the top report shows only work available to you. Within ServiceNow, you can build dynamic reporting that will identify who has logged in. Based on information in their user account, groups they are part of, or roles they are granted for access levels, these reports only display information they can access.

1. Get to work on the task!

2. Click the ⓘ icon to access the Security Response Task.

3. You are directed to the task assigned to you.
4. You will now see a new process workflow along the top.



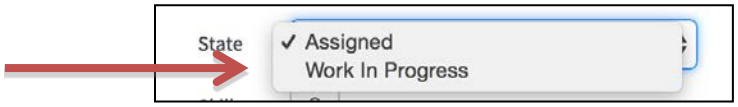
5. ServiceNow allows you to have different processes for your different tasks that need to be completed in order to resolve issues like this Security Incident.

Accept the Task Assigned

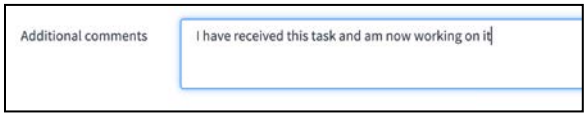
1. Change the state to work in progress by clicking the **state** field on the right side of the form.



2. **Work In Progress** appears; select that option.



3. Scroll to the **Additional Comments** field and add the comment **I have received this task and am now working on it**.



4. Scroll to the top of the page and click the **Update** button.



5. You may be redirected back to the Security Dashboard. If this happens, click the blue  icon again to return to the task.

Work the Task

1. The task is to scan and remove the malware. Because you are an expert, you know that this could be potentially impactful to the business if you cause this system to go offline. First make sure that no one is already working on this system.

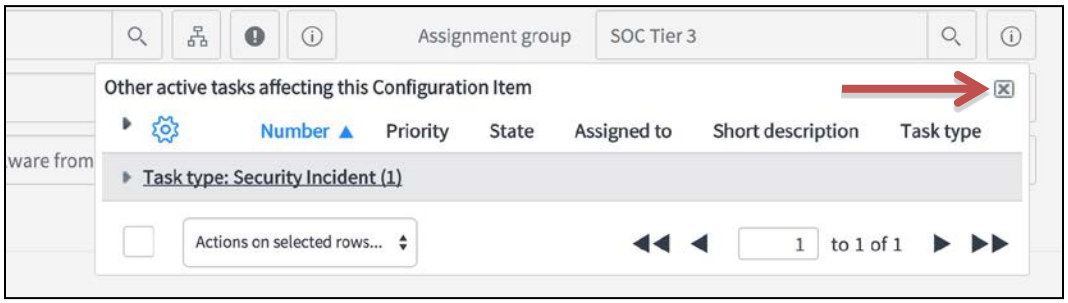
2. Click the icon next to affected CI that looks like a black **exclamation point**.



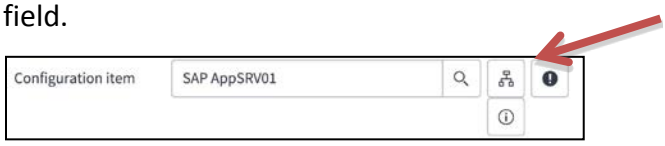
3. This brings up a list of any other tasks that are open against this specific CI. This list is role-based as well, so if you do not want certain types of tasks to appear to this user, you could hide them. Alternatively, click the black **arrow** to expand the list of related issues.



4. Since there are other issues, close this dialog by clicking on the **X** in the upper-right corner.



5. Now check to see what the potential impact will be on the infrastructure if you need to take this system off-line for remediation. Do this by clicking on the **flow chart** icon next to the CI field.



6. You move to the **Business Service Map** (also referred to in this guide as the **BSM**).

7. Here you can see all the systems that use the SAP App Server in the infrastructure. This is a powerful way to see the potential impact of making any changes to a piece of equipment.

8. You can see the device you entered the map on, a pulsating gray halo.



9. Click on **SAP AppSRV01** to see it now has a blue ring around it.



10. Zoom in and out of the map by using your mouse **scroll** up and down, or by clicking the **plus** and **minus** signs in the upper-left corner.



11. Click on the **Details** button in the upper-right corner.

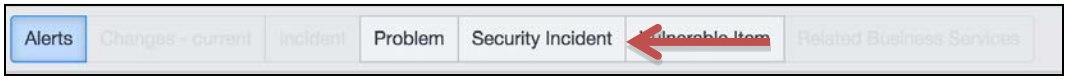


12. The details section of the Business Service Map appears.

13. First to note are the available buttons that appear. Some are grayed out.



14. These are **Map Indicators** and are fully customizable by you. Click the one for **Security Incident**.

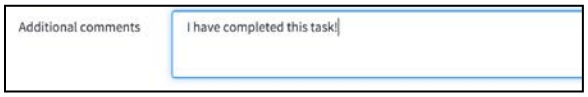


15. You can see all the other security incidents that have been opened against this CI in its history. You can click on the blue ⓘ to open any of these records from the map. This makes the **BSM** extremely versatile and valuable.

16. You have review the possible impact and decide to move forward due to the criticality of this issue. Close the BSM by closing the tab in the browser.

17. You return to the Security Incident Task.

18. For lab purposes, assume that the work is done. In the **Additional Comments** section type **I have completed this task!**



19. Go to the field labeled **Case**. Highlight and copy the number in this field. (This number may be different in your instance)



20. Click the **Close Complete** button on the top right of the form.

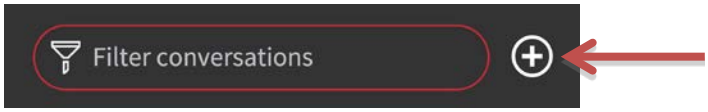


21. You completed the main goal; however, due to the criticality of this issue you need to inform the manager that this is done so you can get him involved.

22. Click on the **Chat** icon in the upper-right corner next to your user name.



23. Welcome to ServiceNow collaborate. Click the **plus** icon to initiate a new chat.



24. In the **To** field, type **Security Manager.** The auto-suggest starts to give you some options. Select the first one by clicking it.



25. Click in the **Message** field. Type **I have completed my task, you can now take it from here, Sir** and paste the number you copied in **step 23** into the message and send the message.

26. Great work! Now the Manager can take it from here! Log out of this persona!

Lab Goal

In this lab, you are the Security Incident Manager. The goal is to:

- Receive a new chat from one of your employees
- Go into the incident and overview that it is in the right stage
- See a new task for HR is in the system and get it assigned

Lab 1.2 Verify Work and Get a New Task Assigned

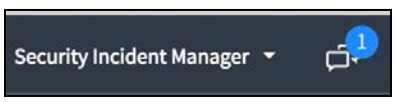
Manager! You Have Received a Notification That a New Collaboration Chat Has Appeared in Your Queue

1. Log in to your instance as the Security Technician. The user id is **si_manager** and password is **Knowledge17**.

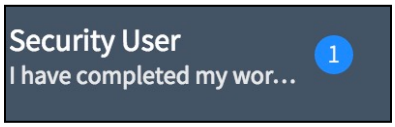


Check Your New Chats!

1. Welcome Manager! You have new chats. You can see this by the number in the chat icon in the upper-right corner. Click the **chat** icon to see your items.



2. The chat panel should auto open. You can now click on the new chat.



3. The new chat shows your employee's update and because they pasted in the number of the Security Incident, ServiceNow can recognize this and make it a clickable link. Click the blue **SIR** box in the chat to go to the Security Incident.



Get HR involved!

1. You came to the Security Incident as the Manager. Collapse any open items so you see the incident. First click the **X** on the chat window.



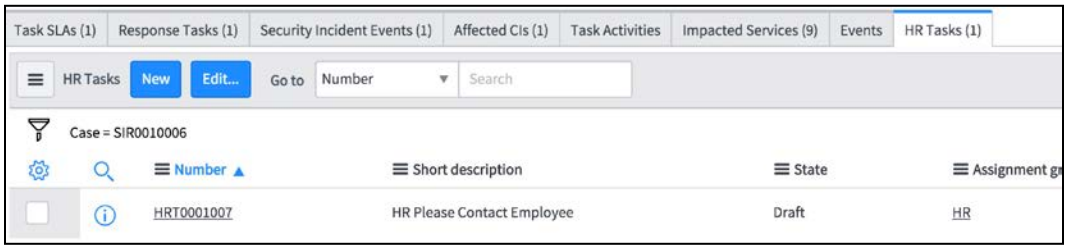
2. Next collapse the Collaborate panel by clicking the **collapse** icon on the bottom right.



3. According to the **short description** of the incident, it appears the monitoring tool has identified that the Security issue was caused by code insertion from user **Devious Employee**.

4. You have a process for this: all incidents caused by users get HR intervention!

5. Scroll to the bottom and see if an HR task is open. This one appears to be in a draft state!



6. This is a good thing; you want to make sure that the task is ready to send to HR. Click into it by clicking the blue ⓘ.

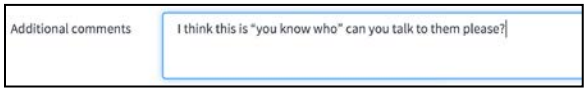
Get Some Teamwork Going!

1. Now you are in an HR task. Notice at the top that it is in a **Draft** state!

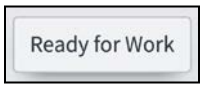


2. ServiceNow allows you to create individual tasks, in different states, that way if you need to review it before if goes out and automatically assigns, you can!

3. Everything looks A-OK in here, so in the additional comments add a note that says **I think this is "you know who" can you talk to them please?**



4. Click the **Ready for Work** button in the upper-right corner.



5. The workflow has now moved to the **Assigned** state and is assigned to the **Human Resources** persona. If you need to make sure this is the correct person, you can always hover over the icon next to the name to see a snapshot of the individual.



6. Great work, Manager! You can now log out.

Lab Goal

Lab 1.3 Verify Work and Get a New Task Assigned

In this lab, you are the HR persona responsible for handling the intercompany snafu. The goal is to:

- Log in and see your unique HR dashboard
- See a critical task assigned to you and to handle it
- Close out your work so Security can move on!

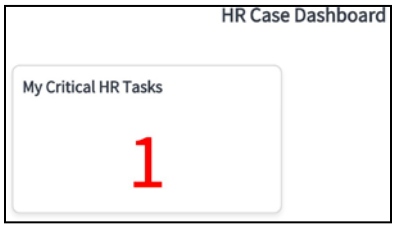
Good Morning and Welcome to ServiceNow Human Resources! Log in and See What We Have for Today

1. Log in to your instance as the Human Resources worker. The user id is **hr_user** and password is **Knowledge17**.



Welcome to HR, That's a Wonderful Color You Chose for Your Theme!

1. Welcome Human Resources persona! Man, you have really slacked on some of those SLAs! Regardless, you have a CRITICAL task assigned to you. Click the **red number** to see what is going on.



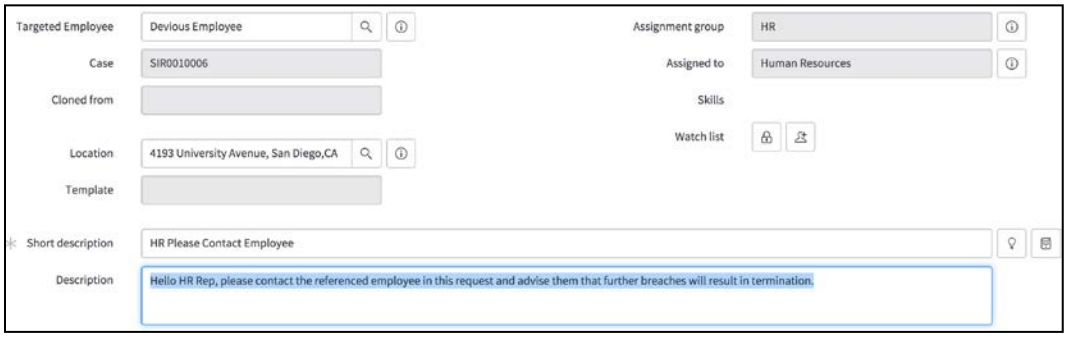
2. You are in the task to help the Security Team. First note that you can see what the Security Incident number is, but you have no access.



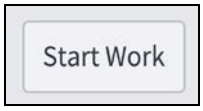
3. That's expected. ServiceNow has placed NEW security behind this application that allows other departments to get involved, but limit what they can actually see!

4. Review some of the other information on this form:

   Targeted Employee: **Devious Employee**
   Short description: **HR Please Contact Employee**
   Description: **Hello HR Rep, please contact the referenced employee in this request and advise them that further breaches will result in termination.**



5. Looks good; accept this work. Click the **Start Work** button in the upper-left corner to accept the work.



6. You need to talk to this individual. Hover over the  icon next to the **Targeted Employee** field to see who this is.



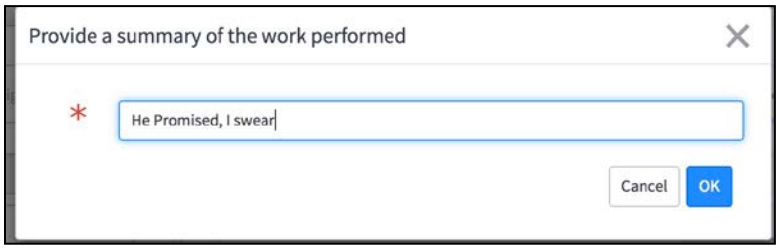
7. Update the task and Security can take it from there! Add the additional comment **I have spoken to this person, and it won't happen again.**



8. Click the **Close Complete** button to close the task.



9. You need to provide a work note before moving forward. Type anything into the box and Click the **OK** button.



10. Log out now.

Lab Goal

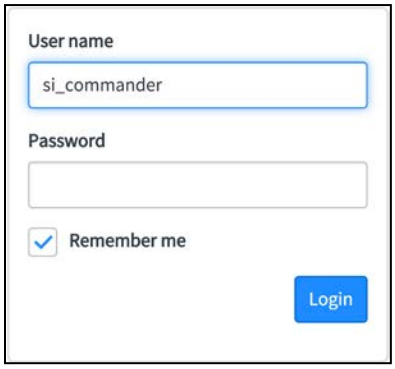
In this lab, you return as the Security Commander to assess how things went.

Lab 1.5 Complete Your Assessments

All Is Well; Time to Assess How You All Did

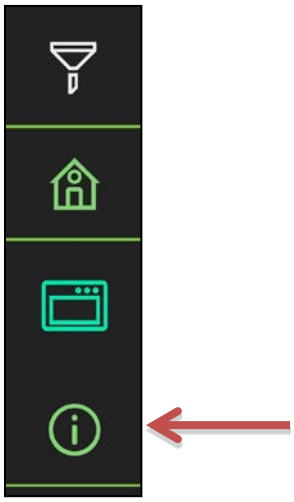
1. You received a notification from the ServiceNow instance that HR is finished. You need to assess the findings.

2. Log in to your instance as the Security Technician. The user id is **si_tech** and password is **Knowledge17**.

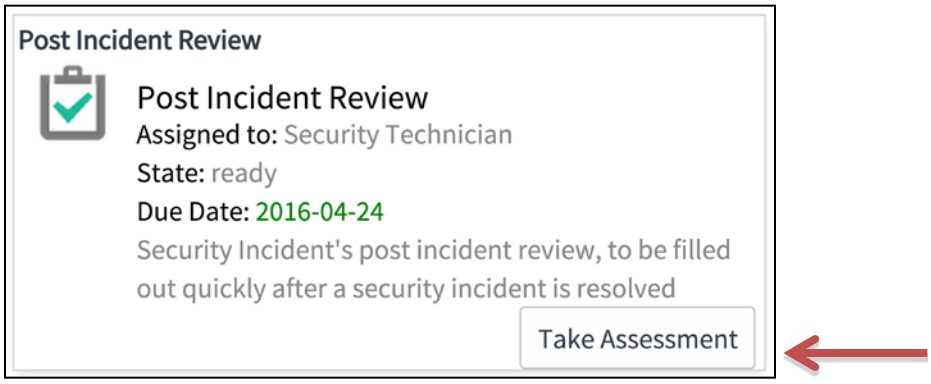


Welcome Back, Commander! You Have a New Assessment

1. On the left navigation bar, you see a series of icons. Click the one at the bottom for your new assessments.



2. This displays any assessments you have pending in the system. Note a due date. ServiceNow can be configured to remind you when you are getting close to that date if need be! Click the **Take Assessment** button and fill out the following form!



3. Once the assesment is complete, log out.

Lab Goal

In this lab, you finish the process as the Security Incident Manager. The purpose of this section is to review the incident, format the Post Incident Review (PIR), and close the incident out.

Lab 1.6
Review and Close Out

All Work Is Complete and Ready for Your Review

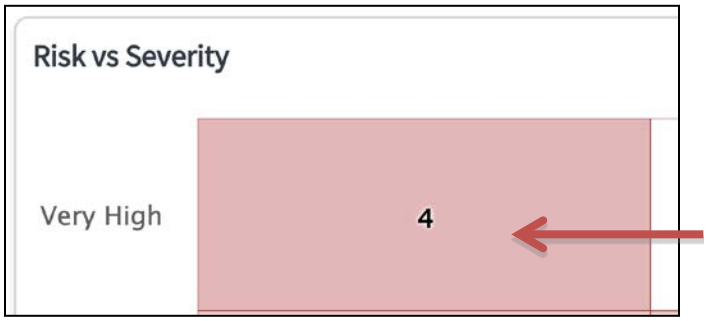
1. Log in to your instance as the Security Incident Manager. The user id is **si_manager** and password is **Knowledge17**.



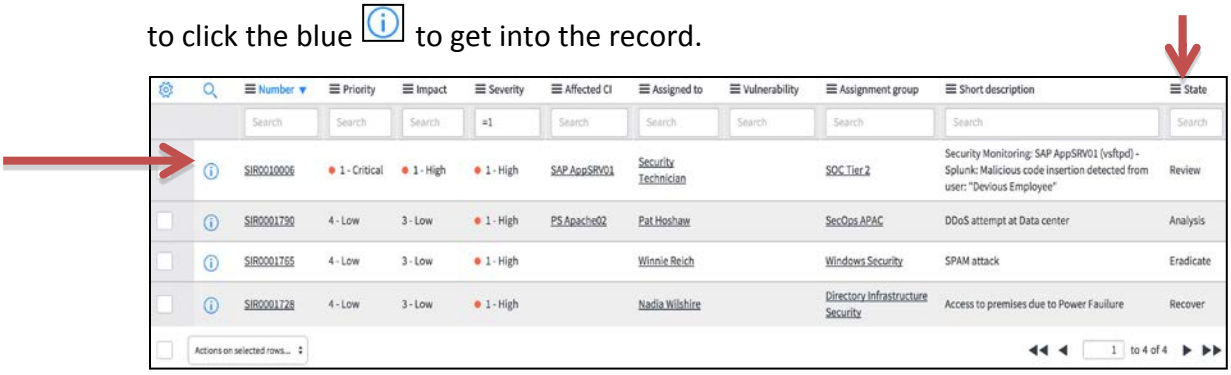
Welcome Back, Manager!

All work is complete. Review and close the incident.

1. Back on the dashboard, click on the upper-right section of the heat map report.



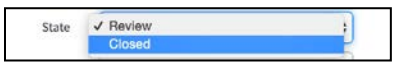
2. A list of incidents for this metric opens. Go into the one that is in the review state. Remember to click the blue ⓘ to get into the record.



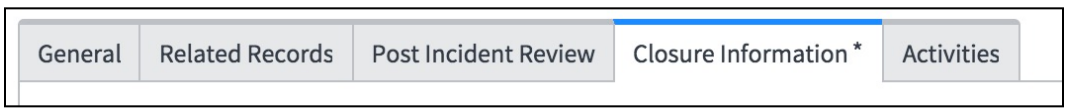
3. On the incident, first click the **Format Post Incident Report** button in the upper-right. This makes sure all the work is brought into the report.



4. Next set the incident to closed by **setting** the state field to **closed**.



5. Note that the **Closure Information** tab has an *.



6. Click this tab.

7. There are mandatory fields that need to be set before the incident can be closed. Set the **Close Code** to any value in the drop-down list and add any comments to the **Close Notes**.

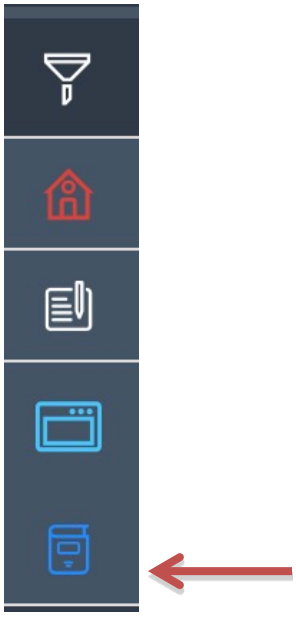


8. **Click** the **Update** button on the top of the form.



Look at the Post Incident Review

1. On your left navigation bar, click the last icon.



2. You move to a list with the incident just completed.



3. Click the blue ⓘ for the incident to see the final version of the incident review.
4. Once in the incident, click the tab for **Post Incident Review**.



5. Scroll to see how ServiceNow automatically generates all the activity that has happened in the incident, in a nice time-lined manner. You also see how the response form and the assessment is included as well.

Great Work, Security Team! Your job is done … for now!