**Nwachukwu Edumanichukwu**

**CYBR 440 - Incident Detection and Response  
Module 9 Lab – Incident Tracking**

In this ninth lab, we will learn how to use automated incident tracking systems to document what happens during an incident. Depending on the incident, incident responders often have to produce a written report meant for external entities such as executives, legal, and third parties while utilizing automated tools to help with the more technical aspects of incident tracking. We will use two popular open-source tools for incident tracking in this lab. The first is an eGRC tool used for compliance but has incident tracking functionality as an integrated compliance tool. The second is an incident tracking and response platform explicitly built for incident responders. This second platform integrates much of the threat intelligence and malware analysis capability to make research and tracking seamless.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

Accessing the Lab

This lab is hosted in the university IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. It would be best if you used the native Horizon client when possible as it provides better performance. The web client can be accessed at <https://workspace.bellevue.edu>. Make sure you log in to this interface with your Bellevue student ID and password.

After accessing workspace.bellevue.edu and selecting the IS Lab desktop, open a browser and navigate to <https://10.98.100.11>. The first time you access this site, you will see a warning in the browser. Make sure to click advanced and then Proceed to 10.98.100.11 (Unsafe). Next, you should see the following remote access page.

Graphical user interface, application, Word

Description automatically generated

After accessing Bellevue Bank and Trust’s Remote Management Portal, login in using the following information:

* Username: analyst# - Where # is the number provided to you by your instructor
* Password: An@lyst#!! - Where # is the number provided to you by your instructor

After logging in, you should see the following page:

Graphical user interface, application

Description automatically generated

You should have three available connections, RDP Kali #, RDP Workstation#, and SSH Kali #. These are the three analyst tools you will use throughout this course.

You will be using the Windows 10 RDP Workstation# connection for this lab. Therefore, it would be best to open each new RDP or SSH connection in a new tab.

Part 1 - Incident Tracking with Eramba eGRC

In this first lab, we will use Eramba, an eGRC tool, to track an incident from start to finish. You will be using the Bellevue Bank and Trust case study for this lab.

1. After accessing your analyst Windows 10 desktop, open a browser and navigate to <https://eramba.bbtrust.com>. You can also click the shortcut link on your analyst desktop. Log in using the username analyst# and password An@lyst#!!, where # is your analyst number.

Graphical user interface, application

Description automatically generated

1. After logging in, hover over the second to the bottom icon on the left side of the screen, labeled Security Options, and then click Security Incidents.

Graphical user interface, application

Description automatically generated

1. At the top of the screen, click Actions, and then + Add.

Graphical user interface, application

Description automatically generated

1. On the first tab of this screen, fill out the following information based on the information on your case study.
   1. Title - Your choice
   2. Type - Incident
   3. Description - A good description of the incident
   4. Tags - Phishing, Ransomware
   5. Open Date - The date the incident started (see the case study), September 16th, 2021.
   6. Automatically Close Incident - Leave disabled
   7. Close Date - Leave blank for now
   8. Status - Ongoing
2. On the Risk Profile tab, fill in the following information
   1. Related Risk Assets - Select Widespread Ransomware Attack Against Multiple Systems
   2. Related Third-Party Risks - Leave Blank
   3. Related Business Risks - Leave Blank
3. On the Incident Stakeholder tab, fill in the following information
   1. Owner - Select Bruce Edwards
   2. Reporter - Type the name Jordan Brands
   3. Victim - List the names of the victims
      1. Charles Sullivan
      2. Sarah Kopsa
      3. Michelle Michelson
4. On the Incident Profil, fill in the following information
   1. Affected Compensating Controls - Select Backups, Malware Cleanup/Reimage
   2. Affected Assets - As the users are already linked to assets, this field should already be filled in with the affected assets. If not, select the following assets:
      1. VDI15A22
      2. lincolnbackoffice15
      3. l55cm2
      4. cio1
      5. mgr257
      6. bankshare01
      7. Bank Share 01 Data
   3. Affected Third-Parties - Leave Blank.
5. Click Save at the bottom of the Add Item (Security Incident) page. You should see a new incident appear on the Security Incident page with Ongoing and Lifecycle Incomplete status.
6. On the Security Incident page, click on the arrow pointing down next to the number 7 in the stages column and then click show. You will see the seven stages of incident response.

Text

Description automatically generated

1. Click on the hamburger menu next to the Preparation stage and click Comments and Attachments. Type in the comment box what you think the CSIRT team in this case study did to be ready for this incident. They have a reasonably mature team, so there should be plenty of description. While we don’t have this available, a written playbook for phishing and ransomware could be attached here. Click Add Comment, and then Close when you finish.

Graphical user interface, application, Teams

Description automatically generated

1. Click on the hamburger menu next to Preparation and click Edit. Change the Status to completed and then click Save.

Graphical user interface

Description automatically generated with low confidence

1. Click the hamburger menu next to the Detection stage and click Comments & Attachments. Add a description of how the incident was detected. Make sure you include plenty of detail. Click Add Comment and then Save.
2. Click the hamburger menu next to the Detection stage, click Edit, change the Status to Complete, and then click Save.
3. Click the hamburger menu next to the Analysis stage and click Comments & Attachments. Add a description of the analysis completed to determine an incident/attack was taking place. Make sure you include plenty of detail. Click Add Comment and then Save.
4. Click the hamburger menu next to the Analysis stage, click Edit, change the Status to Complete, and then click Save.
5. Click the hamburger menu next to the Containment stage and click Comments & Attachments. Add a description of what the CSIRT team did to contain the incident. Make sure you include plenty of detail. Click Add Comment and then Save.
6. Click the hamburger menu next to the Containment stage, click Edit, change the Status to Complete, and then click Save.
7. Click the hamburger menu next to the Eradication stage and click Comments & Attachments. Add a description of what the CSIRT team did to eradicate the ransomware. Make sure you include plenty of detail. Click Add Comment and then Save.
8. Click the hamburger menu next to the Eradicate stage, click Edit, change the Status to Complete, and then click Save.
9. Click the hamburger menu next to the Recovery stage and click Comments & Attachments. Add a description of what the CSIRT team did to recover from the incident. Make sure you include plenty of detail. Click Add Comment and then Save.
10. Click the hamburger menu next to the Recover stage, click Edit, change the Status to Complete, and then click Save.
11. Click the hamburger menu next to the Post-Incident Activity stage and click Comments & Attachments. Add a description of what the CSIRT team and the organization can do better to prevent and respond to a similar incident in the future. Make sure you include plenty of detail. Click Add Comment and then Save.
12. Click the hamburger menu next to the Post-Incident Activity stage, click Edit, change the Status to Complete, and then click Save.
13. Click on the Security Incident tab at the very top of the page, next to Stages to return to the Security Incidents page.

Graphical user interface, text, application, email

Description automatically generated

1. Click on the hamburger menu next to your security incident and click edit. On the General Page, scroll down to the Closure Date on the General Tab and select a closure date of September 21st, 2021. Change the Status to closed. Click Save.

**Take a screenshot of your closed case and paste it belowGraphical user interface, text, application

Description automatically generated**

**Type in the name/title you gave your case below**

**BBTrust Ransomware Attack**

Part 2 - Incident Tracking with TheHive IR Platform

In this second part of the lab, we will use a platform that has been purpose-built for incident responders. Using MISP and Cortex, TheHive allows you to add malicious files and potential indicators of compromise and will automatically go to services like threat intelligence services, virus total, any.run, AbuseIPDB to check for malicious indicators.

1. Open Chrome and navigate to <https://thehive.bbtrust.com> or click the shortcut on your analyst desktop for TheHive. Log in using the name [analyst#@bbtrust.com](mailto:analyst#@bbtrust.com) and the password An@lyst#!!.

Graphical user interface, application

Description automatically generated

1. At the top of the screen, click + New Case.



1. On the Create a new case page, fill in the following information:
   1. Title - A unique title for your case based on the case study
   2. Date - The date the incident began, 16 September, 2021
   3. Severity - High
   4. TLP - Amber
   5. PAP - Amber
   6. Tags - Phishing, Ransomware
   7. Description - A good description of the event based on the case study
   8. Click + Create Case
2. Now that the case is created, we can begin adding tasks. First, click on the Tasks tab. Then click on the Add Task. For the Task group and Task title, add the following values and be sure to click the green checkmark on the right after adding the values:
   1. Task group: Preparation, Task title: Prepare for phishing and ransomware, write playbook and deploy controls.
   2. Task group: Detection, Task title: Monitor controls and take reports to detect incidents.
   3. Task group: Analysis, Task title: Add observables to security incident tracking and perform analysis.
   4. Task group: Containment, Task title: Keep malware from spreading, add observables to anti-malware and firewalls.
   5. Task group: Eradication, Task title: Remove malware by imaging systems, remove malware with other tools.
   6. Task group: Recovery, Task title: Restore encrypted files from backup.
   7. Task group: Post-Incident Activity: Conduct after-action meeting, write incident and after-action report. Conduct continuous improvement activities.

Note: It is a good idea to align your task groups with the top-level stages of an incident response framework.

1. Go through each task on the tasks page and change the Assignee for each task to your Analyst #. Ex. Analyst One if you are analyst1.
2. Start with the Preparation task, hit play. This action will open the task for you to include information. Click the + Add new tasklog button and type a description for the preparation you believe was done for the incident in the case study. Click Add log.



1. Go back to the Tasks tab and click the close button (gray circle with a checkmark where the play button used to be.)



1. Next, go to the Detection task and click the start (play) icon. Click + Add a new task log. Add a detailed description of how the incident in the case study was detected and click Add log. Return to the Tasks tab and close this task.
2. For the analysis group task, click start. Then, instead of adding a new task log, click the observables tab at the top of the case.
3. Click + Add Observable. You will repeat this process four times, one for each observable type, domain names (fqdn), hashes, IP addresses, and email addresses. Fill out the following information for each new observable type.
   1. Type (fqdn, hash, mail, or IP address).
   2. In the Value field, put each observable of the correct type on each line, one per line.
   3. Keep the One observable per line checked.
   4. TLP Amber
   5. Is IOC: True
   6. Tags: Ransomware, Phishing
   7. Description: Provide a good description of the IOCs, i.e., where they came from, who reported them, etc.

Graphical user interface, text, application, email

Description automatically generated

A note on copying and pasting: You can copy and paste from your own computer into your analyst computer to make things easier (especially with the hashes). Copy the text you want to paste into the remote workstation. Then click on the remote analyst workstation and press CTRL+SHIFT+ALT. This action will bring up the following dialog.

Graphical user interface, text, application, email

Description automatically generated

Paste the text into this box and then close it by pressing CTRL+SHIFT+ALT again. You can now paste this text into a Window on the analyst workstation.

1. At this point, we will use the integration with Cortex to automatically fetch threat intelligence and other information from web services like AbuseIPDB, OTX, and Virus Total. Note that there are over 100 different integrations with platforms like Threat Grid, DomainTools, Any.Run, Cuckoo, and other IR tools. Due to the throttling limit on Virus Total, make sure that you are only running three or fewer analyzers at a time. Start by selecting three observables that have not been analyzed by selecting the checkmark next to the observable.

Graphical user interface, application

Description automatically generated

1. Next, locate the drop-down button that says X selected observables, press it, then press Run analyzers on the menu that appears. The analyzer dialog will give you one, two, or three options. Click all the available options, then click Run selected analyzers. After running the analyzers, inspect the observables for which the analyzers were run and ensure you have all the results and no errors. If you receive errors, try rerunning the analyzers. VirusTotal is rate limited because it uses the free API, so running too many analyses at once can cause failures. Also, note that there are no analyzers configured for email addresses, so you will not be able to run

Graphical user interface, text, application, chat or text message

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated with medium confidence

1. After all of the observables have been successfully analyzed, ensure that you spend a few minutes clicking on the color-coded results from VirusTotal, OTX, and AbuseIPB when more than 0 records are shown. The information provided will be in JSON, but there is often great information. Make sure you take notes of the results.
2. Return to the Tasks tab. Click on the highlighted text for the Analysis task title and then click + Add New task log. Describe what you found with the analysis. Include information in the case study, then click Add log. Return to the Tasks tab and close the Analysis task.
3. Now, go to the Containment task and click the start (play) icon. Click + Add a new task log. Add a detailed description of how the incident in the case study was contained and click Add log. Return to the Tasks tab and close this task.
4. Repeat these actions with the Eradication task and click the start (play) icon. Click + Add a new task log. Add a detailed description of how the incident in the case study was eradicated and click Add log. Return to the Tasks tab and close this task.
5. Repeat these actions with the Recovery task and click the start (play) icon. Click + Add a new task log. Add a detailed description of how the incident in the case study was recovered and click Add log. Return to the Tasks tab and close this task.
6. Repeat these actions with the Post-Incident Activity task and click the start (play) icon. Click + Add a new task log. Add a detailed description of what could be improved to better prevent and respond to an incident of this nature in the future and click Add log. Return to the Tasks tab and close this task.
7. Though we will often add TTPs and other information as part of incident tracking, we will not do so in this case as we covered the critical core functionality. When you are ready, click the Close button at the top of the case. Mark the status as True Positive, mark the Impact as Yes, then provide an executive summary of the case in the Summary textbox. Click Close case.

A picture containing chart

Description automatically generated

Graphical user interface, text, application

Description automatically generated

1. To return to view the case after closing it, as you will need to copy and paste some information into this lab, return to the main TheHive page by clicking the TheHive in the upper left-hand corner of the page. First, clear all filters by clicking the Red X next to the listed filters, then click the title of the case you worked. Next, answer the following questions and provide the following screenshots.

**Paste a screenshot of the closed tasks from the Tasks tab in the incident case you created.**

**Paste a screenshot of the Observables tab, the first page that shows short color-coded summary reports. Make sure the screenshot shows an OTX, AIPDB, or VT with > 0 results.**

**What benefits do you see over using TheHive, which is built specifically for incident responders, rather than other tools like Eramba or IT service ticketing systems?**