CYB102 Milestone 1

(🔗 Instructions Page)

Team Members (Required)

Reminder: Make sure to provide **edit access** for this Milestone document to **everyone on your team!**

👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🐹Favorite Animal:	Alexander Nguyen He/Him alexanderhonguyen19@gmail.com Hummingbird	👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🍦Favorite Flavor:	Bratt Morejon He/Him bratmorejon@gmail.com Coffee
👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🎡Favorite Park:		👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🎮Favorite Game:	
👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: ☕Favorite Drink:	Amit Gupta He/Him amitgupta44347@gmail.com Coffee		

What are pronouns /
Why are they included here?

Select one (or more) open-source Datasets to analyze (Required)

Data Set Chosen: The data set we have chosen to analyze for The Data Dig is…

Name: **CIC-IDS2017**	CICIDS2017
Primary Link:	The CICIDS2017 Dataset
Other Resource:	http://205.174.165.80/CICDataset/CIC-IDS-2017/Dataset/CIC-IDS-2017/CSVs/

Other Resource: http://205.174.165.80/CICDataset/CIC-IDS-2017/Dataset/CIC-IDS-2017/PCAPs/

Data Set Description: Where does the data come from? Who generated it? What kind of devices / technologies does it target? What format is the data in?

- It came from the CIC(Canadian Institute of Cybersecurity).
- It was also generated by the CIC to address the lack of test and reliable data, for Intrusion detection systems. Aiming towards real-life background traffic and using 25 users based on the protocols HTTP, HTTPS, FTP, SSH, and email protocols.
- There were a wide range of operating systems tested.
    - This included:
        - Ubuntu servers and Web servers(victims)
        - Windows OS(Win 7 PRO, Win 8.1, Win Vista, Wins 10), victims.
        - MAC computer(victim).
        - Kali and Win(attackers)
- The data was formatted in .csv files for future reference, listing the IPs, timestamps, destination ports, source, etc.

Hypothesis: What are 3 things you expect to find when you analyze the data?
Tip: You won't lose points if these hypotheses turn out to be wrong! Make educated guesses!

Finding #1: The traffic volume of the DDoS attacks may be much more disastrous with more than one machine, besides that one Kali attacker.

Finding #2: The NAT should not be exclusively used for firewalls. But to other implementations with routers or other devices.

Finding #3: Regarding the older models of OS like the Win Vista. There should always be recent updates and disable unnecessary services being runned.

Select an incident-response playbook to follow (Required)

Playbook Chosen: The playbook we have decided to follow for The Data Dig is...

Name: CERT Societe Generale Playbooks

Primary Link: CERT Societe Generale Playbooks

Other Resource: Incident Response Consortium Playbooks

Other Resource: GuardSight Playbook Battle Cards

Playbook Description: Who wrote this playbook? Who is the target audience? Does it make any specific assumptions about the data set? If so, do those match your data, or will you have to adapt the playbook?

This playbook was written by CERT Societe Generale. The target audience includes response teams, SOC analysts, and cybersecurity professionals. Since, the dataset includes network-based traffic attacks it might contain IOCs like IP addresses, packet captures, logs, etc. Yes, these assumptions match our dataset but we might need to adapt for the specific attack types with the dataset.

Tools we Plan to Use: Based on your dataset and playbook, what blue-team tools from this course will you use to analyze the incident? (MINIMUM of 2)

Tool #1:	Wireshark(To analyze the network traffic and figure out the packets being send)
Tool #2:	Splunk(To analyze and visualize the data)
Tool #3:	VirusTotal & AbuseIPDB (To scan IPs)
Tool #4:	Auditd(Checking the logs for any file changes)
Tool #5:	

Project Plan (Required)

Project Plan: Draft a plan for completing your project on time. Who is doing what? When is the next step due? How will you get from here to your goal?

Data Preparation and Tool Setup:

- Dataset cleaning and organizing; configuring tools
- Due Date: Nov 15, 2024

Initial Analysis and Visualizations:

- Analyze data and create visualizations

- Due Date: Nov 19, 2024

Playbook application and documentation:

- Implement playbook steps and document findings
- Due Date: Nov 25, 2024

Final Report and Presentation:

- Gather findings and prepare the presentation.
- Due Date: Nov 28, 2024

Stretch Feature: Custom Playbook (Optional)

If you have chosen to write or modify a playbook, document it here.

Tip: To link your drafts, we recommend using Google Drive files. **Be sure any linked files are set to *"Anyone with the link can View"*!** If the grading team cannot open your file, you **will not get credit** for this stretch feature.

Original Playbook: The original playbook we started with / used as inspiration:

Our Playbook: Our modified playbook for The Data Dig: (Can be a WIP, but clear differences should be visible from the Original Playbook)

Description of Changes:

Milestone Workbook (Optional)

Please use this space to brainstorm, draft, share resources, and otherwise plan out your project!

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Required Features

- ☑ ~~Select one (or more) open-source Datasets to analyze~~
    - ☑ ~~Data Set Chosen (Name & Link)~~
    - ☑ ~~Data Set Description~~
    - ☑ ~~3 Hypotheses Made~~
- ☑ ~~Select an incident-response playbook to follow~~
    - ☑ ~~Playbook Chosen (Name & Link)~~
    - ☑ ~~Playbook Description~~
    - ☑ ~~2+ Tools Identified~~
- ☑ ~~Draft a Project Plan to track your progress~~

Stretch Feature

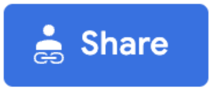
- ☐ Customize a playbook to fit your dataset / scenario
    - ☐ Original/Inspiration Playbook LInk
    - ☐ Custom Playbook Link
    - ☐ Description of Changes

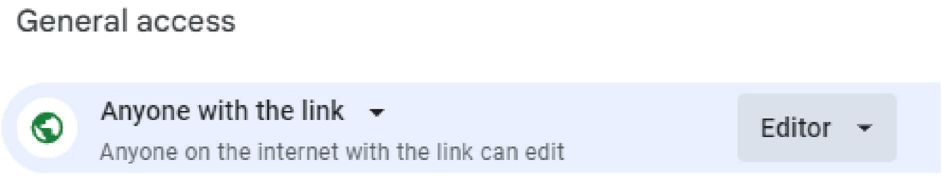
💡***Tip: You can see specific grading information, including points breakdown, by going to*** 🔗 ***the grading page on the course portal.***

Submit your work!

Step 0: **Decide** which group member will submit! **Only one person should submit the milestone** each unit – So make sure everyone's names/emails are on this document!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.



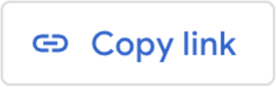

General access

Anyone with the link

Anyone on the internet with the link can edit

Editor

Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.