**CYB102 Milestone 1 (🔗** [**Instructions Page**](https://courses.codepath.org/courses/cyb102/unit/8#!milestones)**)**

**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: | Elisha Jeanbaptiste  elishajean84@gmail.com | 👤 Student Name:  💬 Student Pronouns:  ✉️ Student Email:  🍦Favorite Flavor: | Ikechukwu Anyanwu  Ike.anyanwu02@gmail.com |
| --- | --- | --- | --- |
| 👤 Student Name:  💬 Student Pronouns:  ✉️ Student Email:  🎡Favorite Park: | Alejandro Cuevas  [cuevasalejandro20051@gmail.com](mailto:cuevasalejandro20051@gmail.com) | 👤 Student Name: 💬 Student Pronouns:  ✉️ Student Email:  🎮Favorite Game: | Fares Amamou  famam001@fiu.edu |
| 👤 Student Name: 💬 Student Pronouns:  ✉️ Student Email:  ☕Favorite Drink: | Kwadwo Fening Okai  feningokai@gmail.com |  |  |

[*What are pronouns /   
Why are they included here?*](http://pronouns.org)

**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:** | AWS S3 Honey Bucket Logs |
| **Primary Link:** | https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/aws/discovery/aws\_s3\_honeybucketlogs.zip |
| Other Resource: |  |
| Other Resource: |  |

| **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? |
| --- |
| This dataset represents adversaries trying to scan , discover and access open S3 honeybucket based on known hostname patterns. In this case honeybucket microsoft-devtest.s3.amazonaws.com. It is a csv file. Ashwin Patil generated the data. |

| **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:** | Multiple login attempts |
| **Finding #2:** | Frequently changing IP addresses |
| **Finding #3:** | Types of user agents used to access information |

**Select an incident-response playbook to follow (Required)**

| **Playbook Chosen:** The playbook we have decided to follow for The Data Dig is… | |
| --- | --- |
| **Name:** | AWS Incident Response Runbook |
| **Primary Link:** | https://github.com/aws-samples/aws-incident-response-playbooks |
| Other Resource: |  |
| Other Resource: |  |

| **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? |
| --- |
| Chamandeep Singh wrote the playbook. The target audience are customers using AWS products and who are looking to improve their incident response capability. |

| **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:** | Splunk |
| **Tool #2:** | Catalyst |
| Tool #3: | VirusTotal |
| Tool #4: | AbuseIPDB |
| 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? |
| --- |
| ( Elisha Jeanbaptiste and Alejandro Cuevas)  Gather evidence  Conduct post-incident activities, including post-mortem and feedback processes  (Ikechukwu Anyanwu, Kwadwo Fening Okai, and Fares Amamou)  Contain and then eradicate the incident  Recover from the incident  To achieve our goal on time, we will utilize the tools that we have learned in the past along with our combined intellects to complete the project.  Week 1:  Gather evidence  Contain and then eradicate the incident  Due: 11/11/2024  Week 2:  Recover from the incident  Conduct post-incident activities, including post-mortem and feedback processes  Due: 11/18/2024  Week 3:  Make presentation |

**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***](https://courses.codepath.org/courses/cyb102/pages/grading) ***on the course portal.***