**CYB102 Milestone 2 (🔗** [**Instructions Page**](https://courses.codepath.org/courses/cyb102/unit/9#!milestones)**)**

**Team Members (Required)**

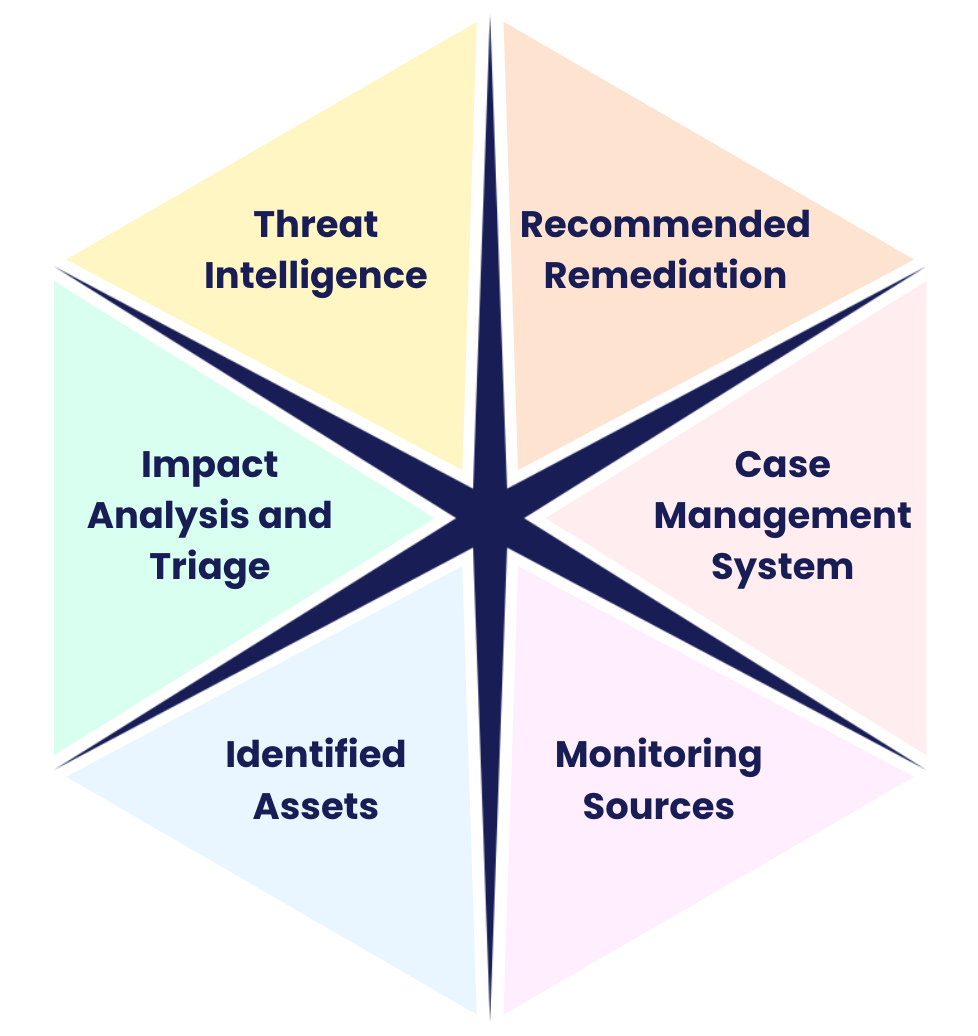
**Reminder**: Make sure to provide **edit access** for this Milestone document to **everyone on your team!**

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

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

**Answer each of the *key aspect* questions (Required)**

***Instructions:*** *For each of the key aspects below, include a few sentences explaining how your project is demonstrating that aspect. Please include at least one specific example.*

**

*For a full definition of each of the key aspects, please*

*view the Data Dig Project page on the Course Portal.*

| **Monitoring Sources** | |
| --- | --- |
| How it relates to our project: | In our project, monitoring sources are critical for identifying potential security incidents involving AWS S3 buckets. By leveraging AWS CloudTrail logs, we can track API activity in real-time, helping to detect unauthorized or suspicious actions, such as attempts to list objects or access sensitive bucket data. These logs are crucial in understanding who accessed the resources, when, and from where, thus enabling us to conduct effective threat analysis. |
| Example(s): | AWS CloudTrail Logs: Capturing detailed information about API calls made to S3, including ListObjects and HeadBucket operations. These logs provide insights into activities such as suspicious requests from unfamiliar IP addresses or repeated unauthorized access attempts |

| **Identified Assets** | |
| --- | --- |
| How it relates to our project: | The key asset identified in our project is the AWS S3 bucket microsoft-devtest. This bucket is critical as it contains essential data for development and testing processes. Protecting this asset is paramount to ensure the integrity and confidentiality of our project's data. |
| Example(s): | **AWS S3 Honeypot Bucket: microsoft-devtest**  **Purpose:** Acts as a decoy to lure attackers and detect unauthorized access attempts.  **Contents:** Contains no real sensitive data but mimics the structure of a genuine bucket.  **Monitoring:** Closely monitored using CloudTrail and other logging services to capture all interactions. |

| **Impact Analysis and Triage** | |
| --- | --- |
| How it relates to our project: | Analyzing the interactions with the honeypot bucket allows us to identify and understand the tactics, techniques, and procedures (TTPs) used by potential attackers. Through the analysis of CloudTrail logs using splunk, we discovered multiple unauthorized access attempts to the microsoft-devtest honey bucket. These attempts provide insight into possible threats targeting our infrastructure and help us assess the potential risk to our actual assets. |
| Example(s): | * Repeated HeadBucket and ListObjects API calls from anonymous users * Access attempts from IP addresses known for malicious activities * Unusual patterns in access times and frequencies indicating automated scanning |

| **Threat Intelligence** | |
| --- | --- |
| How it relates to our project: | By deploying the honeypot bucket and analyzing the gathered data, we enhance our threat intelligence capabilities. The information collected helps us identify malicious actors, understand common attack vectors, and stay updated on emerging threats. This intelligence is critical for refining our security measures and protecting actual assets. |
| Example(s): | **Malicious IP Addresses Identified:**  Several IP addresses attempting to access the bucket are listed in threat intelligence databases as sources of malicious activity.  Example: IP 3.94.59.56 is associated with previous scanning and intrusion attempts.  **Known Attack Patterns:**  Repeated HeadBucket and ListObjects API calls are indicative of automated scanning tools used by attackers to discover misconfigured or publicly accessible buckets.  **Geolocation of Threats:**  Access attempts originating from mainly the United states countries where we have no business operations, suggesting potential external threats. |

| **Recommended Remediation** | |
| --- | --- |
| How it relates to our project: | Based on the insights gained from monitoring the honeypot, we can recommend strategies to enhance the security of our actual assets. Implementing these recommendations helps prevent unauthorized access and strengthens our overall security posture. |
| Example(s): | **Implement Broader Detection Rules:**  Use patterns observed from the honey bucket interactions to develop and refine detection rules across our network.  For instance, if certain API call sequences are indicative of reconnaissance attempts, we can set up alerts for similar activities on genuine buckets.  **Enhance Security Policies:**  Review and tighten access policies for all S3 buckets to ensure they are not publicly accessible unless necessary.  **Conduct Simulated Tests:**  Use the honeypot data to inform red team exercises and simulate attacks on our infrastructure to test and improve our incident response strategies. |

| **Case Management System** (and screenshots) | |
| --- | --- |
| How it relates to our project: | Our case management system, Catalyst, was essential for documenting and tracking the incidents detected through the honeypot. By logging each event in Catalyst, we maintain a comprehensive record that aids in analysis, reporting, and compliance. It also facilitates collaboration among team members during the investigation and remediation processes. |
| Example(s): | **Incident Overview:**  Incident ID: #26750: INC-20241115-0001  Status: Open  Timeline: 2024-11-15 11:35:08 to 01:38:40  Severity: Medium  Traffic Light Protocol (TLP): Amber  **Description:**  Multiple unauthorized API calls (HeadBucket, ListObjects) were detected targeting the microsoft-devtest S3 honeypot bucket. These attempts originated from anonymous principals and suspicious IP addresses not associated with our organization.    **IP Address Classification:**  **Clean IPs:** 54.175.203.19, 3.94.59.56, 177.131.167.145, 92.240.207.254,  93.100.136.232  **Malicious IPs:** 64.15.129.102, 212.83.184.15, 212.83.184.16  **Analysis Notes:**  Identified repeated **HeadBucket** and **ListObjects** API calls from IPs including: 3.94.59.56, 54.175.203.19, 177.131.167.145  IPs are not within our operational range; some are flagged in threat databases.  Access attempts made by **ANONYMOUS\_PRINCIPA**L, indicating unauthorized/unauthenticated access.    **Evidence Gathering:**  **Attached Logs and Documents:**  **CloudTrail Logs:** Showing unauthorized API calls.    **Screenshots:** CloudTrail events highlighting suspicious activities.  **Repeated Attempts & IPs**    **Anonymous Principal**    **API Calls**    **Threat Intelligence Reports:** Correlating IP addresses with known malicious activities.  **64.15.129.102**    **212.83.184.15:**    **212.83.184.16**      **Risk Assessment:**  **Data Exposure:** No critical data or customer information was exposed, as the honeypot is intentionally isolated and contains no real data.  **Threat Level:** Medium, due to the presence of malicious IP addresses making unauthorized attempts.  **External Threat Indicators:** IPs outside the organization's approved network range suggest external threat actors.    **Key Actions Taken:**  **Maintained Honeypot Accessibility:**    Continued to allow access to the honeypot to monitor attacker behavior without tipping them off.  **Enhanced Logging Implementation:**  Configured CloudTrail to capture more detailed logs for in-depth analysis.  **Documentation of Unauthorized Access:**  All unauthorized attempts were recorded in Catalyst for tracking and future reference.  **Threat Intelligence Correlation:**  Cross-referenced IP addresses with threat intelligence databases to assess risk levels.  **Exposure Assessment:**  Confirmed that no critical data was exposed due to the nature of the honeypot.  **Lessons Learned & Behavioral Insights:**  Attackers are likely using automated tools, evidenced by repeated API calls and similar access patterns.  Threat actors are showing interest in exploring S3 buckets using HeadBucket and ListObjects as initial access attempts.  **Future Recommendations:**  **Deploy Additional Honey Buckets:**  Set up more honeypot buckets with varied configurations to observe different attacker strategies.  **Implement Advanced Detection Rules:**  Use AWS Security Hub or GuardDuty to flag these patterns across all resources for early detection. |

**Presentation Prep (Required)**

| **Presentation Plan:**  What is your plan for the presentation? Please include a roadmap, flowchart, diagram, or outline.  Things to consider:   * ~~What will you talk about, and in what order?~~ * ~~Who will be talking at what times?~~ * What visual-aids will you use? |
| --- |
| **Introduction** (Presenter: Team Lead)   * Overview of the project and objectives. * Importance of honeypots in cybersecurity strategy.   **Data Chosen for Data Dig**   * Name * Link to data source   **Monitoring Sources**   * Use of AWS CloudTrail for real-time monitoring. * Types of data collected from the honeypot.   **Threat Intelligence Gathered**   * Analysis of unauthorized access attempts. * Identification of malicious IPs and attack patterns. * Screenshots   **Case Management with Catalyst**   * How Catalyst was used to document and manage the incident.   **Impact on Security Posture**   * Insights gained from the honeypot data.   **Recommended Remediation**   * Strategies for improving security based on findings. * Action plan for implementation.   **Conclusion** |

**Draft of Visual Aids (Required)**

| **Visual Aids Draft:**  Please include a draft of your visual aids for the presentation. This may include slides, screen recordings, GIFs showing demos, or more!  Note: If you link to Google Docs/Slides/etc, be sure your document is set to *“Anyone with the link can view”*! |
| --- |
| https://docs.google.com/presentation/d/1MYBJ1RBJSI8GvbHlLt6iosVyJme4CZBbZrhC7Au-QEs/edit?usp=sharing |

**Stretch Feature: One-Pager (Optional)**

| **One-Pager Draft:**  Please include a draft of a one-page handout, or “one-pager”, you can give your audience prior, during, or after the presentation. One-pagers can be used both to provide extra context and summarize key information.  Note: If you link to Google Docs/Slides/etc, be sure your document is set to *“Anyone with the link can view”*! |
| --- |
| https://docs.google.com/document/d/116Z2lWesvZOFGw0CMFLnDxipWQoVPXknKEgJ6n0\_YkI/edit?usp=sharing |

**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**

* ~~Answer each of the key aspect questions:~~
  + ~~Monitoring Sources~~
  + ~~Identified Assets~~
  + ~~Impact Analysis and Triage~~
  + ~~Threat Intelligence~~
  + ~~Recommended Remediation~~
  + ~~Case Management System~~
* ~~Your presentation plan: A roadmap, outline, or diagram~~
* A draft of your visual aids (slides, screen recordings, etc)

**Stretch Feature**

* ~~Submit a draft for a one-pager summarizing your project for the audience~~

***💡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.***