CYB102 Milestone 2

(🔗 Instructions Page)

Team Members (Required)

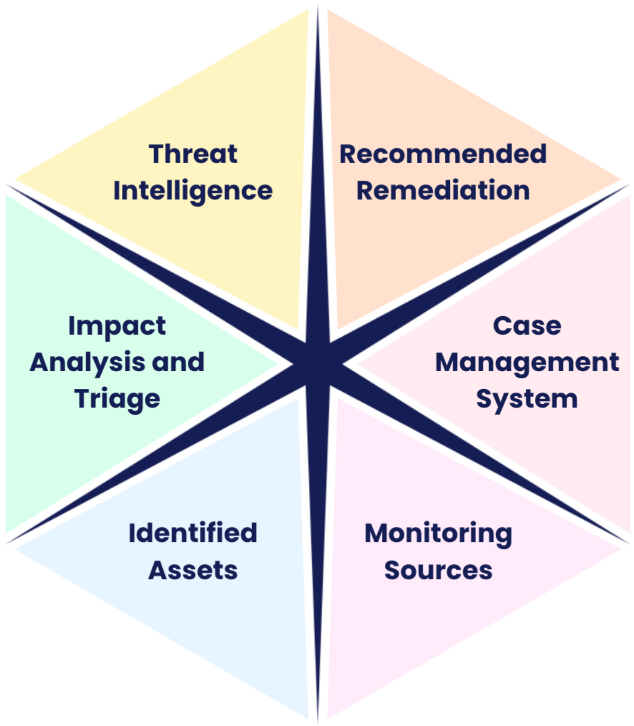
Reminder: Make sure to provide **edit access** for this Milestone document to **everyone on your team!**

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

What are pronouns / Why are they included here?

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:

When monitoring the sources from the CICIDS2017, the objective would be to look for the network logs and check when the firewalls have observed and filtered traffic. With that being said, we can identify the unauthorized access attempts and the preventable malware attacks from an IPS/IDS. Following it up is application logs with web-based attacks and analyzing the user behavior. And the addition of endpoint logs that can help looking for any vulnerabilities in the operating system.

Example(s):

Countless of attacks, but focusing on Thursday, July 6, 2017. There's been 3 types of web attacks: Brute Force, XSS, Sql Injection. There was the Kali machine as the attacker and a web server as ubuntu. And the NAT process on the Firewall denying the attacks.

Identified Assets

How it relates to our project:

Identifying the assets that were involved in the incident is key when attempting a response plan. This dataset provides an easily identifiable list of the network information and the hosts' operating system information. Therefore, when looking at an incident in this dataset performing an identification of assets is straightforward and involves a simple look at the incident log.

Example(s):

For instance, in the July 4th, 2017 incident that involved attack patterns, Brute Force, FTP-Patator, SSH-Patator, there were 2 hosts involved: a Kali attacker and a Ubuntu web server.

Impact Analysis and Triage

How it relates to our project:

When inspecting a dataset such as CICIDS2017, one evaluates the severity of an incident by analyzing factors such as the attack pattern and their target, reaching a calculated impact which correlates to the response efforts employed. Triaging is also part of this analysation by determining the full scope of the impact of the attack. A combination of these two will allow for a more focused response to the incident.

Example(s):

Looking at the dataset, a potential analysis could be prioritizing DDoS attacks as they have the highest impact potential due to the service disruption they cause. Triaging is then performed by determining how many systems are affected by the incident by perhaps following the network packet flow.

Threat Intelligence

How it relates to our project:

By analyzing and utilizing a dataset such as CICIDS2017, IDS/IPS systems can be trained upon with realistic traffic and a diverse set of attack types to provide a better threat recognition. A greater detection and response rate to evolving threats causes more effective automation, reliable systems, and an overall secure infrastructure.

Example(s):

Taking an overview of the dataset, a plethora of different patterns are explored which include well-known attacks such as SQL Injection or Cross-Site Scripting, to more simple ones such as port scanning.

Recommended Remediation

How it relates to our project:

Performing all of these key aspects in analysing the CICIDS2017 dataset provide valuable insights into what remediation actions should be taken depending on the incident. Taking into account the frequency and ease of these incidents should be a key factor in the remediation actions that should be recommended. For instance, if a certain incident occurs a lot compared to others, there should be measures in place to help mitigate that in the future as there is a clear hole in the security against it.

Example(s):

For instance, in the dataset on July 5th, 2017, there are 4 instances of a DoS attack, followed by a DDoS on July 7th, 2017. Analysing these incidents should highlight that the remediation actions that should take place are those that address this clear flaw in the availability of the network. A potential remediation action could be improving the IPS used in the network.

.

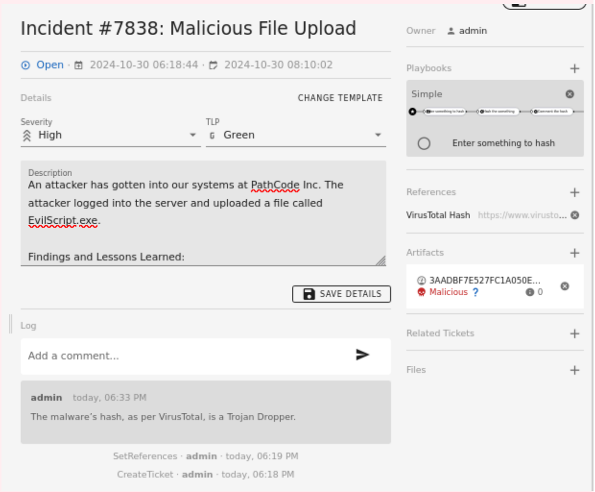
Case Management System (and screenshots)

How it relates to our project:

A case management system is key to properly document the efforts taken to tackle the incidents that occurred in the dataset. These systems could log and track these separate incidents into a clear and usable user interface to efficiently provide an overview of the incident response status over the specific incident.

Example(s):

Catalyst could be used as shown here to track an incident investigation and provide useful information that can be used in the incident response process. This will utilise all of the other key aspects to provide a good overview and detailed results of the investigation of this incident.



Incident #7838: Malicious File Upload

Open · 2024-10-30 06:18:44 · 2024-10-30 08:10:02

Owner: admin

Severity: High

TLP: Green

Description
An attacker has gotten into our systems at PathCode Inc. The attacker logged into the server and uploaded a file called EvilScript.exe.

Findings and Lessons Learned:

Playbooks: Simple

Enter something to hash

References: VirusTotal Hash https://www.virusto...

Artifacts: 3AADBF7E527FC1A050E... Malicious ? 0

Log

admin today, 06:33 PM
The malware's hash, as per VirusTotal, is a Trojan Dropper.

SetReferences · admin · today, 06:19 PM

CreateTicket · admin · today, 06:18 PM

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?~~

Outline

1. Introduction
   a. Presenter:
   b. Content: Introduce the team, introduce the CICIDS2017 dataset, provide an overview of the analysis that will be performed and what will be talked about.
   c. Visual Aid: Slides
2. Chosen Incident Identification
   a. Presenter:
   b. Content: Explain the details of the chosen incident, present the tools used for the investigation, present the results of said investigation
   c. Visual Aid: Slides, Demo, Screenshots
3. Assessment of Incident
   a. Presenter:
   b. Content: Perform impact analysis & triage, relate the findings to a popular attack of the same type, provide recommendations for remediation
   c. Visual Aid: Slides, Demo, Screenshots
4. Conclusion
   a. Presenter:
   b. Content: Recap all of the information gathered through the investigation, provide the lessons learned along the way, and conclude the presentation
   c. Visual Aid: Slides

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/1cTZ-5RVt9fk82BZbnVO8tTvpNDgtB5_dUZzzI93sBvo/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"*!

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

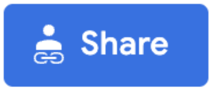
- ☐ Submit a draft for a one-pager summarizing your project for the audience

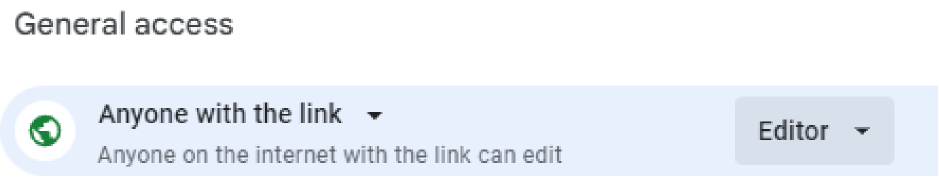
💡***Tip: You can see specific grading information, including points breakdown, by going to 🔗 the grading page on the course portal.***

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.



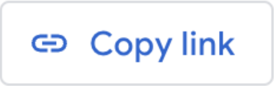

General access

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.