CYB102 Project 6

(🔗 Instructions Page)

👤 Student Name: [ ]
✉️ Student Email: [ ]

Reflection (Required)

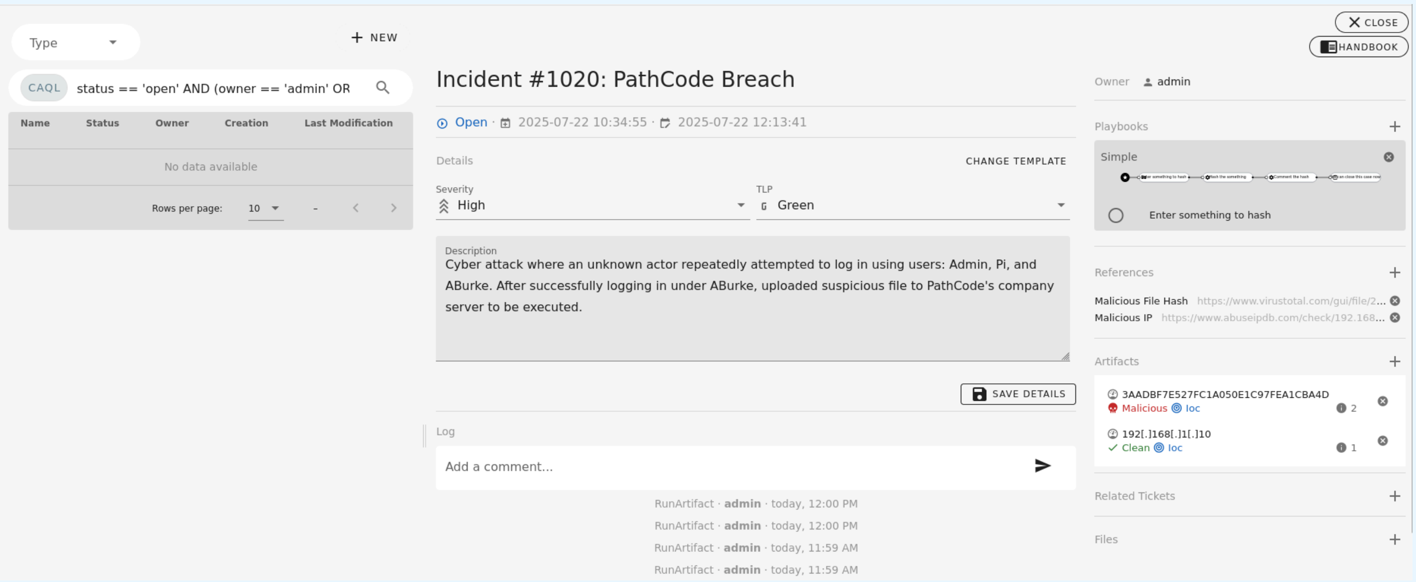
> 🤔 **Reflection Question #1:** If I had to **explain "what is a cyber breach" in 3 emojis,** they would be…
> (Feel free to put other comments about your experience in this unit here, too!)
>
> 📁🤺💻
> Putting together an Incident Report is more straightforward than I anticipated.

> 🧠**Reflection Question #2:** Which step of the incident response process do you think is most important?
>
> I would argue that incident identification/detection is the most important IR process. Not being able to see signs of a possible incident is alarming enough, but it will lead to a high number of incidents occurring which defeats the purpose of having protection against attacks. Additionally, it is important to be able to distinguish between real attacks and false positives. Otherwise, the CSIRT may become overwhelmed and unable to fulfill its duties if incidents cannot be detected effectively.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!
>
> Shoutout to the slack homework bot for the reminder!

Required Challenges (Required)

> **Item #1:** A screenshot of your Splunk Malware case in Catalyst:



Type

+ NEW

CAQL status == 'open' AND (owner == 'admin' OR

Name	Status	Owner	Creation	Last Modification
No data available				

Rows per page: 10 -

Incident #1020: PathCode Breach

Open · 2025-07-22 10:34:55 · 2025-07-22 12:13:41

Details

CHANGE TEMPLATE

Severity: High

TLP: Green

Description
Cyber attack where an unknown actor repeatedly attempted to log in using users: Admin, Pi, and ABurke. After successfully logging in under ABurke, uploaded suspicious file to PathCode's company server to be executed.

SAVE DETAILS

Log

Add a comment...

```
RunArtifact · admin · today, 12:00 PM
RunArtifact · admin · today, 12:00 PM
RunArtifact · admin · today, 11:59 AM
RunArtifact · admin · today, 11:59 AM
```

CLOSE

HANDBOOK

Owner: admin

Playbooks +

Simple

Enter something to hash → Hash the something → Comment the hash → You can close this case now

○ Enter something to hash

References +

Malicious File Hash https://www.virustotal.com/gui/file/2...

Malicious IP https://www.abuseipdb.com/check/192.168...

Artifacts +

3AADBF7E527FC1A050E1C97FEA1CBA4D
Malicious Ioc 2

192[.]168[.]1[.]10
✓ Clean Ioc 1

Related Tickets +

Files +

Item #2: At least one artifact and notes from an external source:

1. **Indicator Type: Malware Hash**

   Indicator Value: 3AADBF7E527FC1A050E1C97FEA1CBA4D (MD5)

   Source: VirusTotal

   - **46/63 security vendors flagged this file as malicious**
   - **Size: 7.95 MB**
   - **Executable performs: copying a document to a specific directory, unzipping a document to a specific directory, deleting the original document and zipped file, and running a Python script.**

Item #3: A brief write-up of your findings and Lessons Learned:

An attacker logged into the company's server under user ABurke to upload and execute a malicious file.

The attacker obtained the credentials of a user to gain access to the server before uploading a malicious executable.

The documentation of user events like login attempts, file uploads, file hashes, and tracking of IP addresses proved to be useful in building the incident report efficiently. Logging tools proved to be invaluable in reconstructing the attack to see which users may have been compromised and what these users did.

Server access must be removed from the compromised user. The affected server should be isolated until further notice.

> **Obtaining login credentials gives server access to anyone, and file uploads may not be restricted enough.**
>
> **- Monitor suspicious login patterns.**
>
> **- Enforce multi-factor authentication (MFA).**
>
> **- IP validation.**
>
> **- Restrict file uploads.**

Stretch Challenge (Optional)

> **Bonus Task #1:** Catalyst Investigation - Use Catalyst to manage the incident and fill out the case with the Artifacts, Tasks, and TTPs that you researched:
>
> **[Insert Screenshot Here]**

> **Bonus Task #2:** NIST or Sans Framework Analysis - Write a report that outlines the steps of either the NIST or SANS framework and how it could have prevented the breach:
>
> **TODO**

Submission Checklist

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

Required Challenges

- ☑ ~~Item #1~~
- ☑ ~~Item #2~~
- ☑ ~~Item #3~~

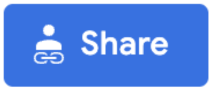
Stretch Challenge

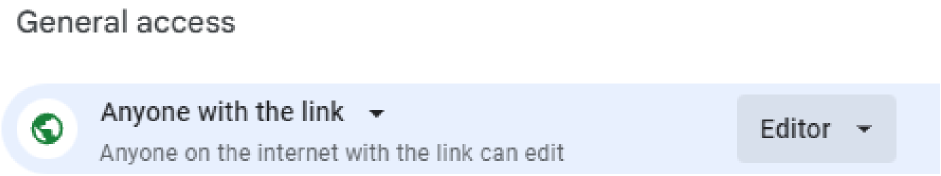
- □ Bonus Task #1
- □ Bonus Task #2

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

Submit your work!

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





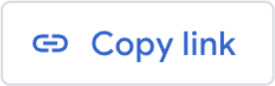
General access

Anyone with the link

Anyone on the internet with the link can edit

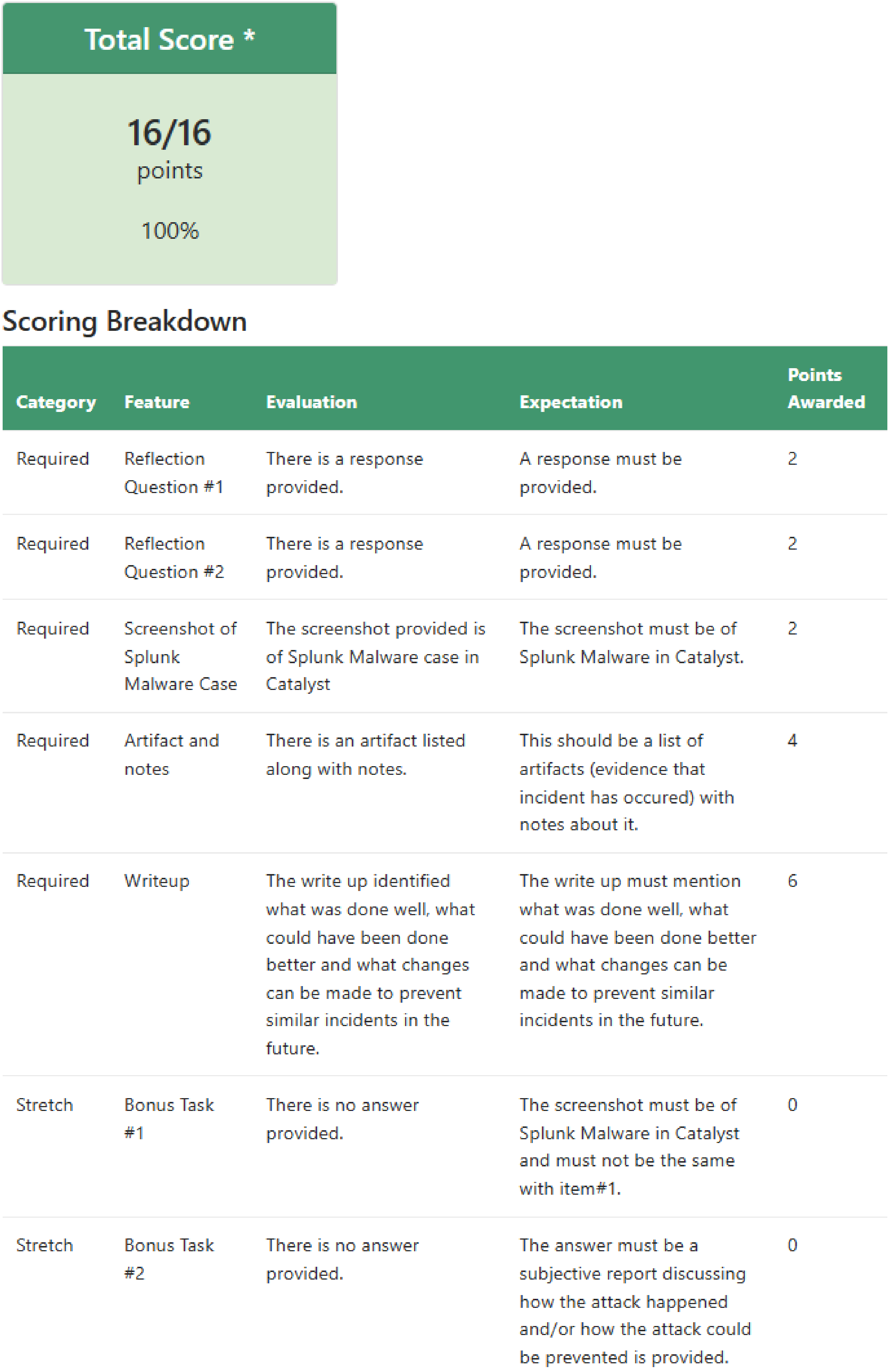
Editor

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



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

Grading



Total Score *

16/16
points

100%

Scoring Breakdown

Category	Feature	Evaluation	Expectation	Points Awarded
Required	Reflection Question #1	There is a response provided.	A response must be provided.	2
Required	Reflection Question #2	There is a response provided.	A response must be provided.	2
Required	Screenshot of Splunk Malware Case	The screenshot provided is of Splunk Malware case in Catalyst	The screenshot must be of Splunk Malware in Catalyst.	2
Required	Artifact and notes	There is an artifact listed along with notes.	This should be a list of artifacts (evidence that incident has occured) with notes about it.	4
Required	Writeup	The write up identified what was done well, what could have been done better and what changes can be made to prevent similar incidents in the future.	The write up must mention what was done well, what could have been done better and what changes can be made to prevent similar incidents in the future.	6
Stretch	Bonus Task #1	There is no answer provided.	The screenshot must be of Splunk Malware in Catalyst and must not be the same with item#1.	0
Stretch	Bonus Task #2	There is no answer provided.	The answer must be a subjective report discussing how the attack happened and/or how the attack could be prevented is provided.	0