CYB102 Project 5

(🔗 Instructions Page)

👤 Student Name: Didier Joseph DESMANGLES

✉️ Student Email: djdesmangles@gmail.com

Reflection (Required)

🤔 **Reflection Question #1:** If I had to **explain "what is SIEM" in 3 emojis,** they would be… (Feel free to put other comments about your experience in this unit here, too!)

🛡️ ➡️ 📊 **SIEM** (Security Information and Event Management)
🛡️ **(Shield)**: Represents the security aspect of SIEM, which focuses on defending systems from cyber threats.
➡️ **(Arrow)**: continuous flow of data being monitored and analyzed in real-time.
📊 **(Chart)**: Symbolizes the data analysis and reporting of security events, which is crucial for identifying and responding to threats.

🧠**Reflection Question #2:** What field do you think is most important for logs to have?

The **timestamp** is the more important field. Timestamp is the field that helps understand the flow of events or the sequence of actions and correlating logs across different systems.

📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

All my pals from Team 17. I have to be prepared to be able to support them

CTF Challenges (Required)

Use the answer boxes below to document any CTF challenges you completed. If you don't complete a particular challenge, leave it blank.

Part 1 - Searching the Netflix Data (1pt each)

index=main source=Netflix

👥 **Challenge 1:** How many TV shows on Netflix are in the Docuseries genre?

Solution:

1. **170**
2. index=main host="Netflix" type="TV Show" listed_in="Docuseries" | stats count

👥 **Challenge 2:** How many movies on Netflix have a rating of TV-PG?

Solution:

1. **1080**
2. index=main host="Netflix" type="Movie" rating="TV-PG" | stats count

👥 **Challenge 3:** How many movies on Netflix were released in the year 2020?

Solution:

1. **1034**
2. index=main host="Netflix" type="Movie" release_year="2020" | stats count

👥 **Challenge 4:** What is the longest duration by season on Netflix, and what is its TV rating?

Solution:

1. **Longest TV Show = 17, rating = TV-14, title = Grey's Anatomy**
2. index=main host="Netflix" type="TV Show"
   | rex field=duration "(?<season_duration>\d+)"
   | stats max(season_duration) as longest_duration by rating, title
   | sort - longest_duration
   | head 1
   | table longest_duration, rating, title

👥 **Challenge 5:** How many movies on Netflix are listed as action and are rated PG-13?

Solution:

1. **46**
2. index=main host="Netflix" type="Movie" listed_in="Action & Adventure" rating="PG-13" | stats count

👥 **Challenge 6:** How many movies and TV shows on Netflix have their country of origin as Turkey?

Solution:

1. **210**
2. index=main host="Netflix" (type="Movie" OR type="TV Show") country="Turkey"
   | stats count as Total

👥 **Challenge 7:** Which release year had the most movies rated G? (Not TV-G)

Solution:

1. **Release_year = 2009, Count = 8**

2.
   ```
   index=main host="Netflix" type="Movie" rating="G"
   | stats count by release_year | sort - count
   | head 1
   | table release_year, count
   ```

👥 **Challenge 8:** What two TV-Y7 rated shows were released in 2019 and were added to Netflix on November 22, 2019?

Solution:

1. **“The Dragon Prince”, “Trolls: The Beat Goes On!”**

2.
   ```
   index=main host="Netflix" type="TV Show" rating="TV-Y7" release_year=2019
   date_added="November 22, 2019"
   | stats values(title) as Titles
   ```

👥 **Challenge 9:** Which year had the most movies from the United States?

Solution:

1. **Release_year = 2017, Count = 568**

2.
   ```
   index=main host="Netflix" type="Movie" country="United States"
   | stats count by release_year
   | sort - count
   | head 1
   | table release_year, count
   ```

👥 **Challenge 10:** What is the oldest TV show by Release Year on Netflix?

Solution:

1. **Release_year=1925, Title=”Pioneers: First Women Filmmakers*”**

2.
   ```
   index=main host="Netflix" type="TV Show"
   | sort release_year
   | head 1
   | table title, release_year
   ```

Part 2 - Investigating the Malware (2pts each)

For Part 2 we are investigating an attacker who got into our systems that happened at PathCode Inc.

For these logs use index=pathcode

> 👥 **Challenge 11:** What was the IP address that uploaded the malware (MD5 hash: 3AADBF7E527FC1A050E1C97FEA1CBA4D)
>
> **Solution:**
>
> 1. **192.168.1.10**
> 2. index="pathcode" host="uploadedhashes" "File Hash"="3AADBF7E527FC1A050E1C97FEA1CBA4D"
>    ```
>    | dedup IP
>    | table _time,  IP, “User Agent”, Filename
>    ```

> 👥 **Challenge 12:** What usernames did that IP address try to login to the system as? Which one did they upload a file as?
>
> **Solution:**
>
> 1. **What usernames did that IP address try to login to the system as ?**
>
>   Aburk, Pi, Admin
>
>    ```
>    index="pathcode" host="webserver02" Event="Login Attempt" IP="192.168.1.10"
>    | dedup Username
>    | table _time, IP, "User Agent", Username
>    ```
> 2. **Which one did they upload a file as?**
>
>   2023-06-24-04 15:29:00 JMann
>
>   2023-06-24-04 15:21:00   Aburk
>
>    ```
>    index="pathcode" host="webserver02" Event="File Upload"
>    | dedup Username
>    | table _time, IP, “User Agent”,Username, Event
>    ```

> 👥 **Challenge 13:** What was the User Agent String of the attacker when they successfully uploaded a file?
>
> **Solution :**
>
> 1. **Opera/75.0.3969.218**
>
>    ```
>    index="pathcode" (host="BluecoatProxy01" OR host="failedlogins64" OR host="uploadedhashes" OR host="webserver02") Event="File Uploaded" IP="192.168.1.10" "File Hash"="3AADBF7E527FC1A050E1C97FEA1CBA4D"
>    | dedup IP
>    | table _time, IP, Filename, "User Agent"
>    ```

👥 **Challenge 14:** Did any other users also upload a file around that time? If so, who and what was their IP address?

Solution:

1. **2023-06-04 15:21:00 ABurk : 192.168.1.10,**
   2023-06-04 15:29:00 Jmann: 192.168.1.7

2.
   ```
   index="pathcode" (host="BluecoatProxy01" OR host="failedlogins64" OR
   host="uploadedhashes" OR host="webserver02") (Event="File Upload" OR Event="File
   Uploaded") Username="*"
   | dedup Timestamp
   | table Timestamp, IP, Username
   ```

👥 **Challenge 15:** Looking at the uploaded hashes, what were the files called that the two users uploaded? Which one seems like it was malicious?

Solution:

1. **Looking at the uploaded hashes, what were the files called that the two users uploaded?**
   2023-06-04 15:29:00, 192.168.1.7, Jmann, **proposal.pdf** ,
   2023-06-04 15:21:00, 192.168.1.10, ABurke, **EvilScript.exe**

2. **Which one seems like it was malicious?**
   EvilScript.exe

   ```
   index="pathcode" host="webserver02" Event="File Upload"
   | table Timestamp, IP, Username
   | Join IP
       [search index="pathcode" host="uploadedhashes"
       | table IP, Filename]
   | dedup IP
   | table Timestamp, IP, Username, Filename
   ```

Submission Checklist

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

Reflection

- ~~Reflection Question #1 answered above~~
- ~~Reflection Question #2 answered above~~

CTF Challenges (10pts needed for full credit, 17pts needed for extra credit)

Part 1 - 1pt each

- ~~Challenge #1: How many TV shows on Netflix are in the Docuseries genre?~~
- ~~Challenge #2: How many movies on Netflix have a rating of TV-PG?~~
- ~~Challenge #3: How many movies on Netflix were released in the year 2020?~~
- ~~Challenge #4: What is the longest duration by season on Netflix, and what is its TV rating?~~
- ~~Challenge #5: How many movies on Netflix are listed as action and are rated PG-13?~~
- ~~Challenge #6: How many movies and TV shows on Netflix have their country of origin as Turkey?~~
- ~~Challenge #7: Which release year had the most movies rated G? (Not TV-G)~~
- ~~Challenge #8: What two TV-Y7 rated shows were released in 2019 and were added to Netflix on November 22, 2019?~~
- ~~Challenge #9: Which year had the most movies from the United States?~~
- ~~Challenge #10: What is the oldest TV show by Release Year on Netflix?~~

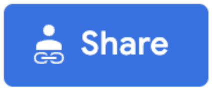
Part 2 - 2pts each

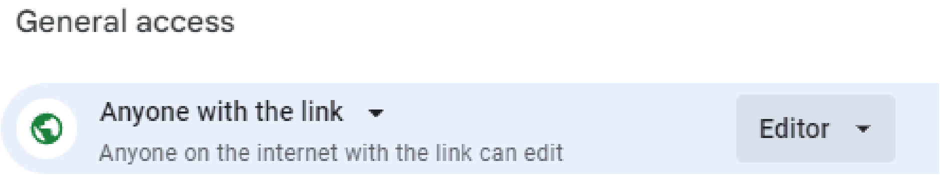
- ~~Challenge #11: What was the IP address that uploaded the malware (MD5 hash: 3AADBF7E527FC1A050E1C97FEA1CBA4D)~~
- ~~Challenge #12: What usernames did that IP address try to login to the system as? Which one did they upload a file as?~~
- ~~Challenge #13: What was the User Agent String of the attacker when they successfully uploaded a file?~~
- ~~Challenge #14: Did any other users also upload a file around that time? If so, who and what was their IP address?~~
- ~~Challenge #15: Looking at the uploaded hashes, what were the files called that the two users uploaded? Which one seems like it was malicious?~~

💡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.



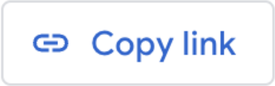

General access

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.