CYB102 Project 5

(🔗 Instructions Page)

👤 Student Name: Alexander Nguyen

✉️ Student Email: alexanderhonguyen19@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!)
>
> 🧐🔎🪵

> 🧠**Reflection Question #2:** What field do you think is most important for logs to have?
>
> I think the simple "source=<this/path/file>" and it all depends on what you're looking at for the field.
> The event "time=*" is important too to realize if there was an instance of logins that was simultaneous.
> I also came to the conclusion that show_id field to be exponentially helpful. Giving a unique identification to each event and eliminating confusion for duplicates.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!
>
> Omkar helped me out on how to proceed in azure labs with the rdp.
> Although I didn't set it up yet, it was helpful.

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. host=AlexPC447 source=*netflix_titles.csv type="TV Show" listed_in=Docuseries
2. | stats count by country
3. | sort -count
4. 85

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

Solution:

1. host=AlexPC447 source=*netflix_titles.csv type="Movie" rating="TV-PG"
2. | stats count by country
3. | sort -count
4. **540**

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" type="Movie" release_year="2020"
2. **517**

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" type="TV Show"| rare limit=20 duration
2. source="/root/tmp_splunk/netflix_titles.csv" type="TV Show" duration="17 seasons" rating="TV-14"
3. Duration: "17 seasons" Rating: ”TV-14”

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" type="Movie" rating="PG-13" listed_in="Action*"

2. **56**

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" type="Movie" OR type="TV Show" country="Turkey" show_id=*
2. **73**

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" type="Movie" rating="G" | top limit=20 release_year
2. 2

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" type="TV show" release_year="2019" date_added="November 22, 2019" rating="TV-Y7"
2. The Dragon Prince, Trolls: The Beat Goes On!

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" sourcetype="csv" type="Movie" release_year="*" country="United States"| top limit=20 release_year
2. 2019

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

Solution:

1. source="/root/tmp_splunk/netflix_titles.csv" sourcetype="csv" type="TV show"| rare limit=20 release_year
2. Pioneers: First Women Filmmakers*, released in 1925

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. source="uploadedhashes.csv" host="longpc" "File Hash"=3AADBF7E527FC1A050E1C97FEA1CBA4D
2. 192.168.1.10
3.

👥 **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. source="webserver02.csv" host="longpc" sourcetype="csv" IP="192.168.1.10"
2. Admin, Pi, ABurke
3. ABurke

👥 **Challenge 13:** What was the User Agent String of the attacker when they successfully uploaded a file?

Solution:

1. source="webserver02.csv" host="longpc" sourcetype="csv" Event="File Upload" IP="192.168.1.10" "User Agent"="Firefox/89.0"
2.

> 👥 **Challenge 14:** Did any other users also upload a file around that time? If so, who and what was their IP address?
>
> **Solution:**
> 1. source="webserver02.csv" host="longpc" sourcetype="csv" Event="File Upload"
> 2. It was Jmann, around 15:29. ABurke uploaded around 15:21
> 3. Jmann's IP address: 192.168.1.7

> 👥 **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. source="uploadedhashes.csv" host="longpc" IP="192.168.1.10" OR IP="192.168.1.7"
> 2. proposal.pdf, EvilScript.exe
> 3. EvilScript.exe

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?~~

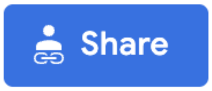
Part 2 - 2pts each

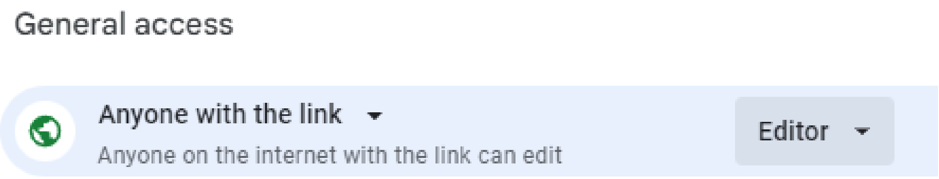
- ☑ ~~Challenge #11: What was the IP address that uploaded the malware (MD5 hash: 3AADBF7E527FC1A050E1C97FEA1CBA4D)~~
- ☑ ~~Challenge #12: What usernames did that IP address try to login to the system as? Which one did they upload a file as?~~
- ☑ ~~Challenge #13: What was the User Agent String of the 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.



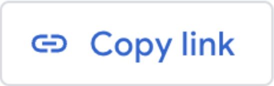

General access

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.