

CYB102 Project 5

([🔗 Instructions Page](#))

👤 Student Name: Amirhossein Ghafouri Nejad

✉ Student Email: Amiredroit66@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 is like a smart tool that helps you search through logs, spot problems, and understand what's going on in a system. At first, it was a little confusing, but once I got used to it, solving each challenge actually felt fun and satisfying.

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

Timestamps , they help you know when things happened. Without them, it's hard to tell the order of events or figure out what went wrong.

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

Shoutouts to online resources for helping to complete this project.


CTF Challenges (Required)

Use the answer boxes below to document any CTF challenges you completed.

- For each challenge, document both:
 1. The challenge answer
 2. The search command used to find the answer
- 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. Search: index=main host=Netflix "Docuseries" "TV Show"
2. 798

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


Solution:

1. Search: index=main host=Netflix type="Movie" rating="TV-PG"
2. 1080

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

Solution:

1. index=main host=Netflix type="Movie" release_year=2020
2. 1034

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

Solution:

1. index=main host=Netflix type="TV Show" | sort -duration | table title, duration, rating
2. 17 Seasons, TV-14

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

Solution:

1. index=main host=Netflix type="Movie" rating="PG-13" genre="Action & Adventure"
2. 296

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

Solution:

1. index=main host=Netflix country="Turkey"
2. 10

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

Solution:

1. index=main host=Netflix type="Movie" rating="G" | stats count by release_year | sort -count
2. 2009 and 1977 (8 movies each)

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

Solution:

1. index=main host=Netflix rating="TV-Y7" release_year=2019 date_added="November 22, 2019" | table title, rating, release_year, date_added
2. Trolls: The Beat Goes On! and The Dragon Prince

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

Solution:

1. index=main host=Netflix type="TV Show" country="United States" | stats count by release_year | sort -count
2. 2020 (318 TV Shows)

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


Solution:

1. index=main host=Netflix type="TV Show" | sort release_year | table title, release_year
2. Pioneers: First Women Filmmakers (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. "3AADBF7E527FC1A050E1C97FEA1CBA4D"
2. 192.168.1.10

 **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. host=failedlogins64 "192.168.1.10" and host=uploadedhashes "192.168.1.10"
2. The attacker tried to log in as ABurke and uploaded the file using that account.

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


Solution:

1. host=uploadedhashes "192.168.1.10"
2. Opera/75.0.3969.218

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

Solution:


1. host=uploadedhashes
2. Another user from IP 192.168.1.3 uploaded "FamilyPhoto.jpg" just before the malware upload..

 **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. host=uploadedhashes
2. 192.168.1.10 uploaded: EvilScript.exe
3. 192.168.1.3 uploaded: FamilyPhoto.jpg
4. EvilScript.exe is clearly the malicious one.

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-14 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: 3AADB7E527FC1A050E1C97FEA1CBA4D)?
- ☒ 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!