**CYB102 Project 5 (🔗** [**Instructions Page**](https://courses.codepath.org/courses/cyb102-dev/unit/1#!projects)**)**

👤 Student Name: Nickodemus Konde

✉️ Student Email:Ntkonde88@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 timestamps are the most important. Without knowing when an event happened, it’s almost impossible to connect logs or spot attack timelines. Time helps you line up events, detect anomalies, and track what the attacker did step by step. |

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

**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. index=main host=Netflix type="TV Show" 2. | where like(listed\_in, "%Docuseries%") 3. | stats count 4. 790 |

| **👥 Challenge 2:** How many movies on Netflix have a rating of TV-PG? |
| --- |
| **Solution:**   1. index=main host=Netflix type=Movie rating="TV-PG" 2. | stats count 3. 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. | stats count 3. 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" 2. | rex field=duration "(?<num>\d+)\s+(?<unit>\w+)" 3. | search unit="Season" OR unit="Seasons" 4. | eval seasons=tonumber(num) 5. | sort - seasons 6. | head 1 7. | table title rating duration seasons 8. Grey’s Anatomy, TV-14, 17 Seasons, 17 |

| **👥 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" 2. | where like(listed\_in, "%Action & Adventure%") 3. | stats count 4. 296 |

| **👥 Challenge 6:** How many movies and TV shows on Netflix have their country of origin as Turkey? |
| --- |
| **Solution:**   1. index=main host=Netflix 2. | where like(country, "%Turkey%") 3. | stats count by type 4. | addcoltotals label=Total 5. Movie - 166 6. TV Show - 60 |

| **👥 Challenge 7:** Which release year had the most movies rated G? (Not TV-G) |
| --- |
| **Solution:**   1. index=main host=Netflix type=Movie rating=G 2. | stats count by release\_year 3. | sort - count 4. | head 1 5. Release Year - 2009 , Count - 8 |

| **👥 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 type="TV Show" rating="TV-Y7" release\_year=2019 "date\_added"="November 22, 2019" 2. | table title release\_year date\_added 3. Trolls: The Beat Goes On! - 2019 - November 22, 2019 4. The Dragon Prince - 2019 - November 22, 2019 5. Trolls: The Beat Goes On! - 2019 - November 22, 2019 6. The Dragon Prince - 2019 - November 22, 2019 |

| **👥 Challenge 9:** Which year had the most movies from the United States? |
| --- |
| **Solution:**   1. index=main host=Netflix type="Movie" 2. | where like(country, "%United States%") 3. | stats count by release\_year 4. | sort - count 5. | head 1 6. Release\_year- 2017 7. Count - 720 |

| **👥 Challenge 10:** What is the oldest TV show by Release Year on Netflix? |
| --- |
| **Solution:**   1. index=main host=Netflix type="TV Show" 2. | eventstats min(release\_year) as oldest 3. | where release\_year=oldest 4. | table title release\_year 5. Pioneers: First Women Filmmakers\* - 1925 6. 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. index=pathcode sourcetype=csv host=uploadedhashes 2. | regex \_raw="(?i)3AADBF7E527FC1A050E1C97FEA1CBA4D" 3. | rex field=\_raw "(?<attacker\_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" 4. | rex field=\_raw "(?<filename>[A-Za-z0-9\_\-\.]+\.exe)" 5. | table \_time attacker\_ip filename md5 6. | sort - \_time 7. \_time attacker\_ip filename 8. 2023-06-04 17:59:00 192.168.1.10 EvilScript.exe 9. 2023-06-04 17:59:00 192.168.1.10 EvilScript.exe 10. 2023-06-04 17:59:00 uploadedhashes csv |

| **👥 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. index=pathcode (sourcetype=failedlogins64 OR host=failedlogins64) 2. | regex \_raw="192\.168\.1\.10" 3. | rex field=\_raw "(?<user>\w+)" 4. | stats values(user) AS attempted\_users 5. **Attempted Users - 6** 6. index=pathcode sourcetype=csv host=uploadedhashes 7. | regex \_raw="192\.168\.1\.10" 8. | rex field=\_raw "(?<user>\w+)" 9. | stats values(user) as uploading\_user values(filename) as files 10. **Uploading\_user - 6** |

| **👥 Challenge 13:** What was the User Agent String of the attacker when they successfully uploaded a file? |
| --- |
| **Solution:**   1. index=pathcode (host=uploadedhashes OR host=webserver02 OR host=BluecoatProxy01 OR sourcetype=csv) 2. | regex \_raw="192\.168\.1\.10" 3. | rex field=\_raw "(?i)(?<user\_agent>(?:Opera|Firefox|Chrome|Safari|curl|Wget|python-requests|Mozilla)[^,;\r\n]+)" 4. | table \_time user\_agent \_raw 5. | dedup user\_agent 7. \_time - 2023-06-04 17:20:00 user\_agent - Firefox/89.0 6/4/2023 8. \_raw - 17:20,192.168.1.10,ABurke,216.58.192.206,http://google.com,GET,Firefox/89.0,200,512,2048,Search Engines,ALLOW, 9. \_time - 2023-06-04 15:50:00 user\_agent - Safari/13.1.1 6/4/2023 10. \_raw   15:50,192.168.1.10,ABurke,69.171.250.35,http://www.microsoft-updateserver.cf,GET,Safari/13.1.1,200,768,3072,Software,ALLOW,ALLOW   1. \_time - 2023-06-04 17:59:00 user\_agent - Opera/75.0.3969.218 2. \_raw   6/4/2023 17:59,192.168.1.10,File Uploaded,Opera/75.0.3969.218,200,EvilScript.exe,3AADBF7E527FC1A050E1C97FEA1CBA4D |

| **👥 Challenge 14:** Did any other users also upload a file around that time? If so, who and what was their IP address? |
| --- |
| **Solution:**   1. index=pathcode sourcetype=csv host=uploadedhashes 2. | where \_time>=strptime("2023-06-04 17:54:00","%Y-%m-%d %H:%M:%S") 3. AND \_time<=strptime("2023-06-04 18:04:00","%Y-%m-%d %H:%M:%S") 4. | rex field=\_raw "(?<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" 5. | rex field=\_raw "(?<filename>[A-Za-z0-9\_\-]+\.(?:exe|css|html|js|txt|csv))" 6. | rex field=\_raw "(?i)(?:user(?:name)?[:=]\s\*(?<user>[\w\.\-@]+))" 7. | rex field=\_raw "(?i)(?<user\_agent>(?:Opera|Firefox|Chrome|Safari|curl|Wget|python-requests|Mozilla)[^,;\r\n]+)" 8. | table \_time ip user filename user\_agent 9. | sort \_time 10. \_time ip user filename user\_agent 11. 2023-06-04 17:59:00 192.168.1.10 EvilScript.exe Opera/75.0.3969.218 12. 2023-06-04 17:59:00 192.168.1.10 EvilScript.exe Opera/75.0.3969.218 |

| **👥 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. index=pathcode sourcetype=csv host=uploadedhashes 2. | rex field=\_raw "(?<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" 3. | rex field=\_raw "(?<filename>[A-Za-z0-9\_\-]+\.(?:exe|css|html|js|txt|csv))" 4. | rex field=\_raw "(?<md5>[A-Fa-f0-9]{32})" 5. | stats values(filename) as filenames values(md5) as md5s by ip 6. | eval malicious=if(mvfind(filenames,"EvilScript.exe")>=0,"yes","no") 7. | table ip filenames md5s malicious 8. | sort ip 9. ip filenames md5s malicious 10. 192.168.1.3 A68DE2C044417E8D5B1D16948F7B4871 no 11. 192.168.1.4 Homepage.html 2D3F8B8E8DCB501C020C3857C6E2A1E4 no 12. 192.168.1.6 EBD61D1B938F1B47B4E3BD57758B1405 no 13. 192.168.1.7 2453EAF1B75CF1B2DF2513B3E1FFDDF1 no 14. 192.168.1.8 Style.css 75441F0A76544B5983E31DFA1C0D8EA2 no 15. 192.168.1.9 D9A8C67E4716C46B8B28F54D06B5471C no 16. 192.168.1.10 EvilScript.exe 3AADBF7E527FC1A050E1C97FEA1CBA4D yes 17. 192.168.1.11 4E8F8C3FAB57D23E5D48BF3B01AABD6A no 18. 192.168.1.12 README.txt 8BF6356FBE76C7E1DA9A9CDA9B582EFD no 19. 192.168.1.13 5DB8467B1C10F83719A7115B2D223F82 no |

**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***](https://courses.codepath.org/courses/cyb102/pages/grading) ***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.      Step 2: **Copy** the link to this document.    Step 3: **Submit** the link on the portal. |
| --- |