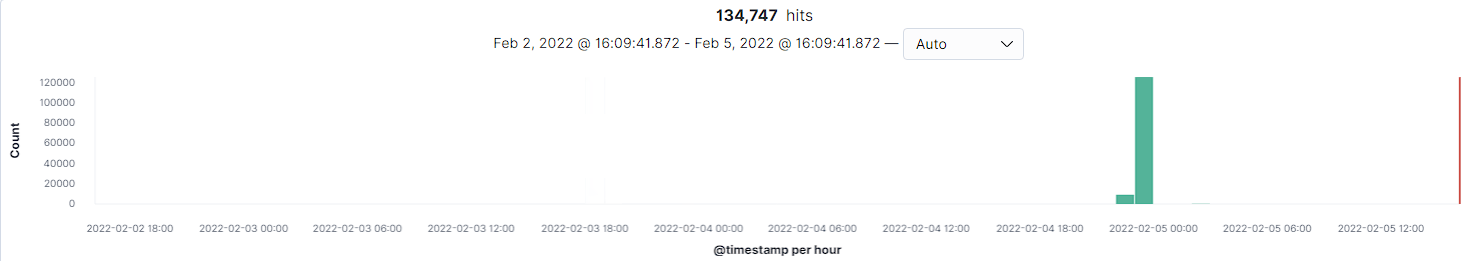
Project 2: Day 2

After creating your dashboard and becoming familiar with the search syntax, use these tools to answer the questions below:

1. Identify the offensive traffic.
   * Identify the traffic between your machine and the web machine:
     + When did the interaction occur?

It started at 10 PM on February 5, 2022 (9,018 hits) and peaked at 11 PM (125,435 hits).





* + - What responses did the victim send back?

The http.response.status\_code(s) sent back were: 200, 207, 301, 401, and 404.

Chart, bubble chart

Description automatically generated

* + - What data is concerning from the Blue Team perspective?

1. Find the request for the hidden directory.
   * In your attack, you found a secret folder. Let's look at that interaction between these two machines.
     + How many requests were made to this directory? At what time and from which IP address(es)?

There were 16,004 requests to the directory starting at 11 PM on February 4, 2022 from the IP address 192.168.1.90.

Graphical user interface, text

Description automatically generated

* + - Which files were requested? What information did they contain?

The files that were requested were from a query for GET /company\_folders/secret\_folder. The requests failed until 11:07 PM on February 4, 2022. The information that was contained in here was a hash and a guide on how to login and which username to use.

Graphical user interface, text, application, email

Description automatically generated

* + - What kind of alarm would you set to detect this behavior in the future?
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

1. Identify the brute force attack.
   * After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:

Graphical user interface, text, application, email

Description automatically generated

* + - Can you identify packets specifically from Hydra?

You can search for it by utilizing “user\_agent.original : \* Hydra”

* + - How many requests were made in the brute-force attack?

16,004

Graphical user interface, application

Description automatically generated

* + - How many requests had the attacker made before discovering the correct password in this one?  
        
      16,003. The only correct one had the status as “OK” and the http.response.status\_phrase as “moved permanently”

Graphical user interface, text, email

Description automatically generated

* + - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

1. Find the WebDav connection.
   * Use your dashboard to answer the following questions:
     + How many requests were made to this directory?

194 requests.

Graphical user interface, text, application, email

Description automatically generated

* + - Which file(s) were requested?

The two files that were requested:  
/webdav/rev\_shell.php  
/webdav/passwd.dav

* + - What kind of alarm would you set to detect such access in the future?
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

1. Identify the reverse shell and meterpreter traffic.
   * To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
     + Can you identify traffic from the meterpreter session?

You can find the time when the rev\_shell.php was added by using:  
query: \*PUT\*



* + - What kinds of alarms would you set to detect this behavior in the future?
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.