

Day 2
Advent of Cyber 2024
SIEM

Knowing the actual difference between false positives and true positives is challenging for SOC, but certain softwares can enhance it, still we need to make sure of some other activities.


- If an organisation doesn't have a change request process in place.
- The performed activity was outside the scope of the change request or was different from that of the approved change request.
- The activity triggered an alert, such as copying files to a certain location, uploading a file to some website, or a failed login to a system.
- An insider threat performed an activity they are not authorised to perform, whether intentionally or unintentionally.
- A user performed a malicious activity via social engineering from a threat actor.

We are going to use the concept of correlation using the Elastic SIEM on day 2 of the challenge. What is correlation?

Correlation requires a lot of hypothesis creation and ensuring that the evidence supports that hypothesis. A hypothesis can be something like the user downloaded malware from a spoofed domain. The evidence to support this can be proxy logs that support the hypothesis that a website was visited, the website used a spoofed domain name, and a certain file was downloaded from that website. Now, let's say, we want to identify whether the malware executed through some vulnerability in an application or a user intentionally executed the malware. To see that, we might look at the parent process of the malware and the command line parameters used to execute the said malware. If the parent process is Windows Explorer, we can assume the user executed the malware intentionally (or they might have been tricked into executing it via social engineering), but if the parent process is a web browser or a word processor, we can assume that the malware was not intentionally executed, but it was executed because of a vulnerability in the said application.

Logging into SIEM (Elastic siem here lol)

https://10-10-34-199.p.thmlabs.com/login?next=%2F



Welcome to Elastic

Username

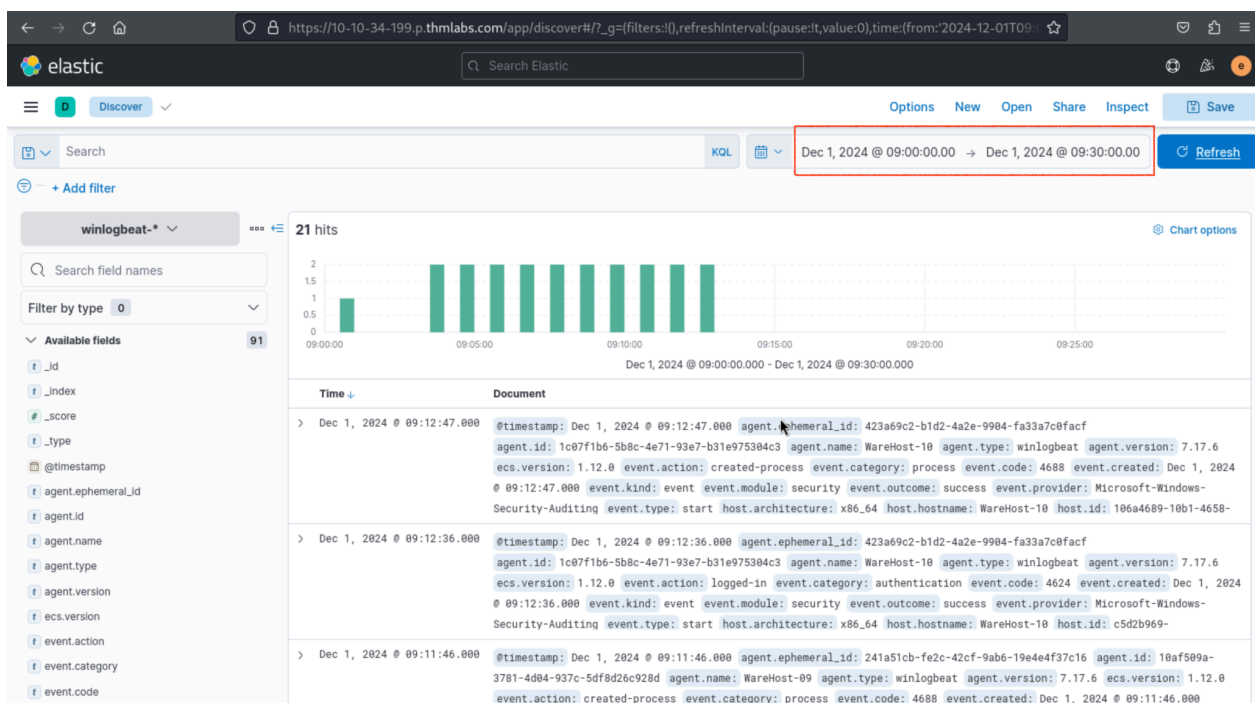
elastic

Password

••••••••

Log in

Start time and end time (Dec 1: 9.00 to 9.30)

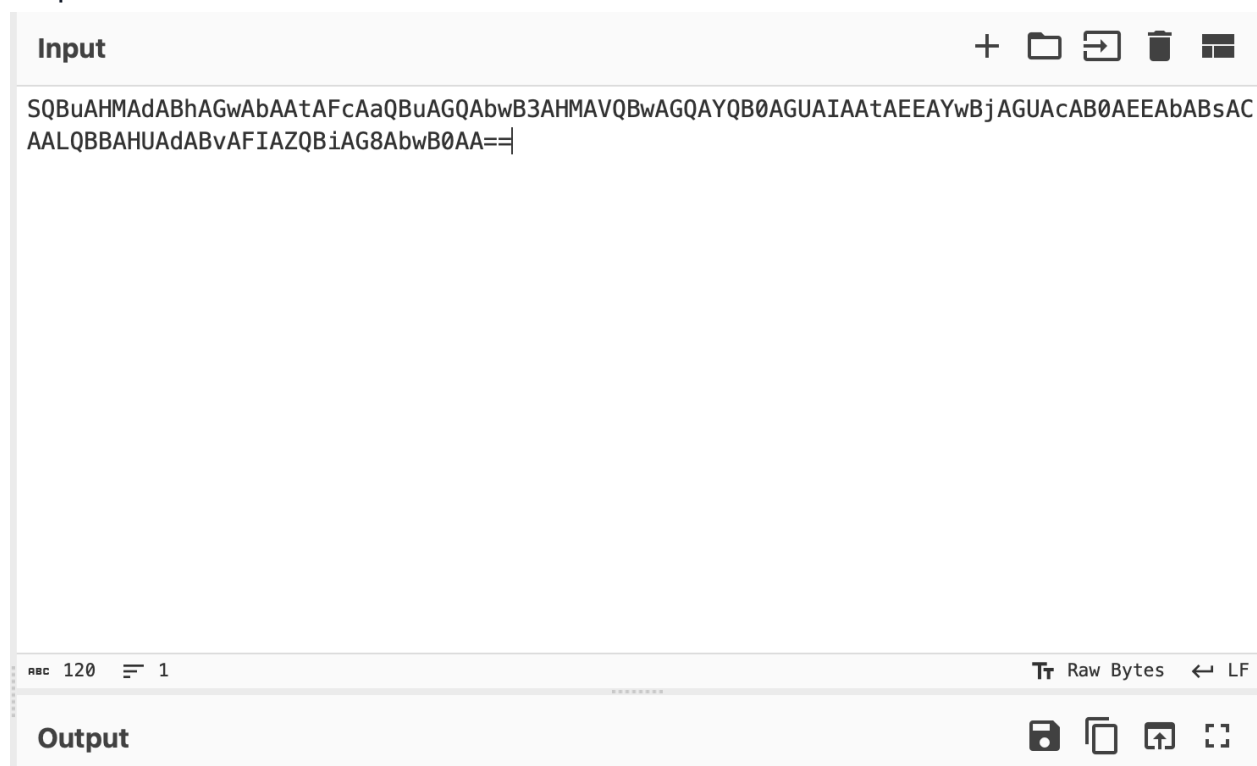


Adding these 5 columns for seeing it better and giving attention to detail.

Investigate it further with process and authentication using + or - on the column and it seems to be a brute force attack. Especially on Dec 1.

So we investigated further on the powershell command and it seems to have a base 64 value which can be decoded on cyberchef and we did it successfully.

Output is secret



It seems like Glitch is a good boy helping to improve defence, but now suspicion is on tragedy because we don't know who is the culprit, mayor or glitch? Confusion begins but we will try to find more evidence to knock the case out.

Hint for this exercise.

Filtering is the key, make sure you include and exclude right columns and IP (I mean IP it is one of the clues).

Enjoy the task that is the second hint. (Task will become easier).