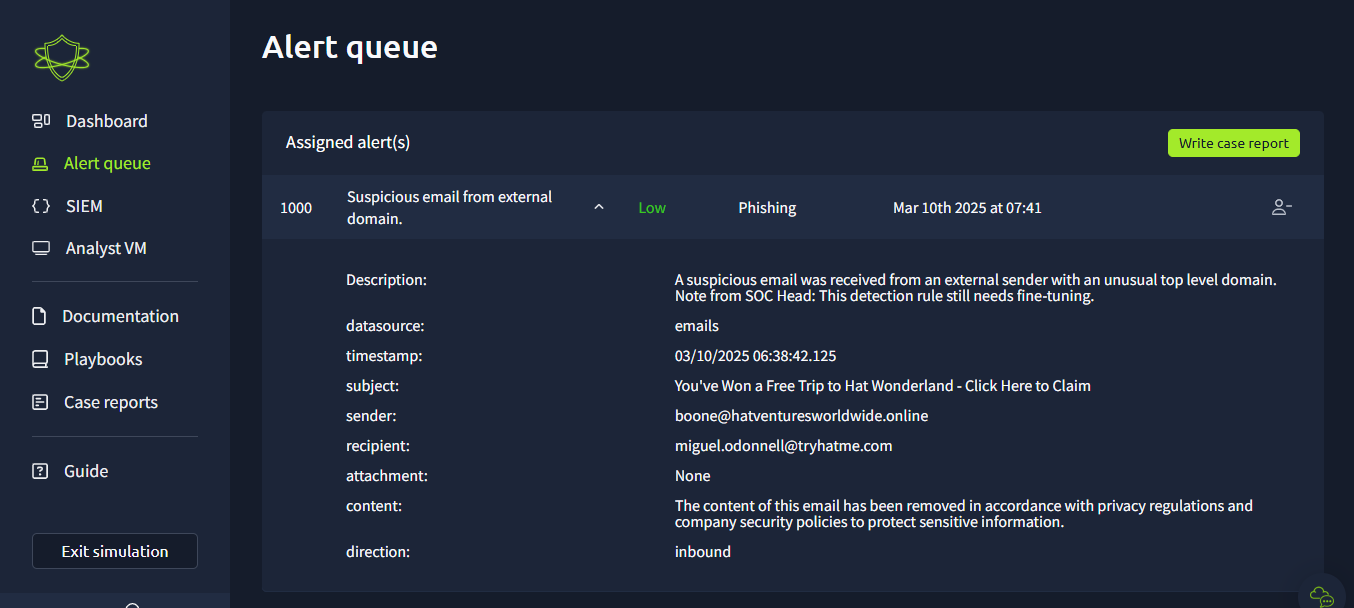
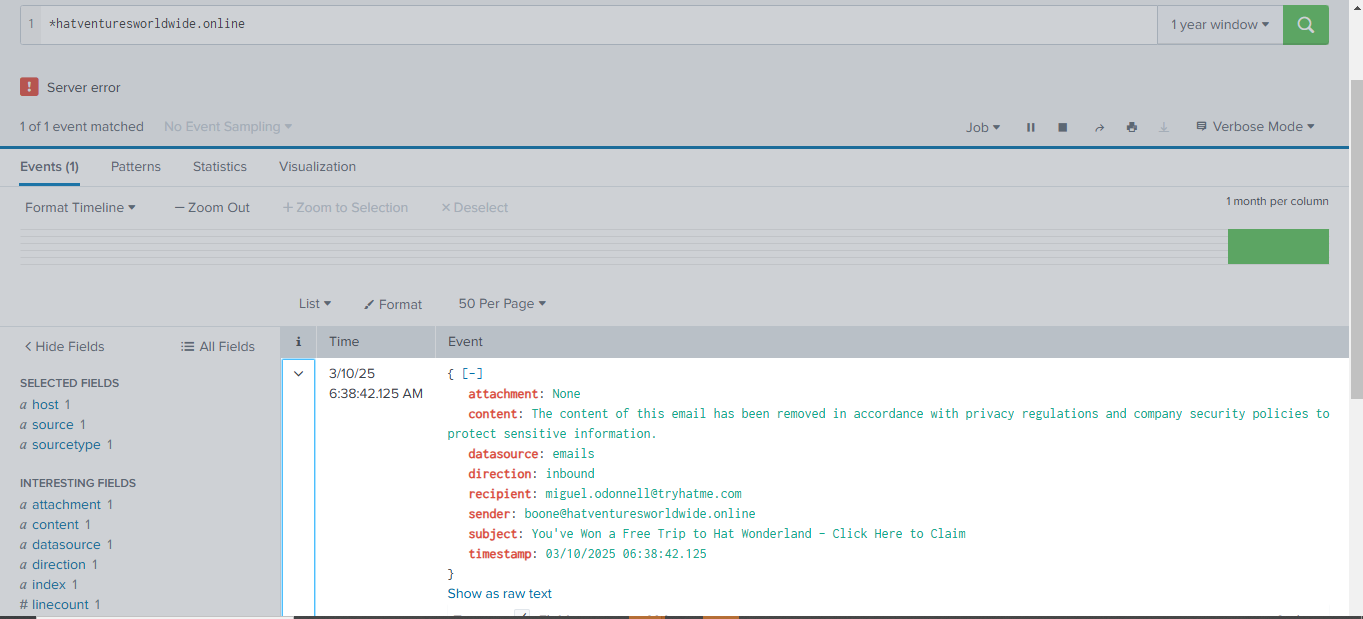
**Real Time SOC analysis on TryHackme**

This exercise was done in SOC Simulator scenarios on <https://tryhackme.com> . The focus of this exercise is a real day activity on the dashboard with the objective of finding a True Positive phishing alert.

**Alert 1000; Suspicious email from an external domain**

****

Took ownership of this alert by assigning myself to this alert. On investigating the alert, no attachment was added to the mail so no files to be analyzed. However, the mail is from an external sender. [boone@hatventuresworldwide.online](mailto:boone@hatventuresworldwide.online) So, we check the threat intelligence of this domain to know if the domain is trusted. To do this, we use the SIEM tool on the platform (Splunk)

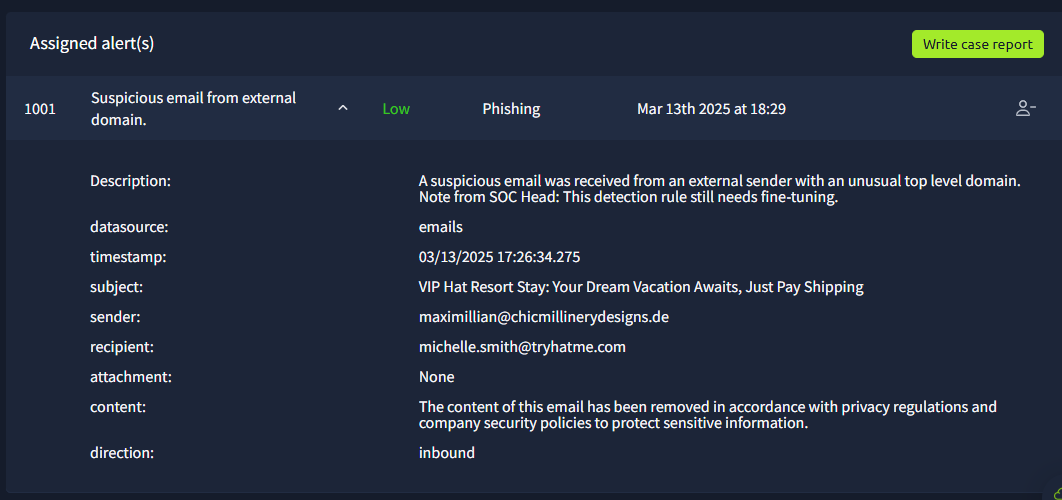
On Splunk, changed the time frame to a 1-year window and the search if there are events recorded about this domain. On checking the events, no attachment and it appears to be the same email we are analyzing. Next, we use online sandbox like virustotal.com 

From the online sandbox (Virustotal.com) we can see that the domain is marked as a non-malicious domain.

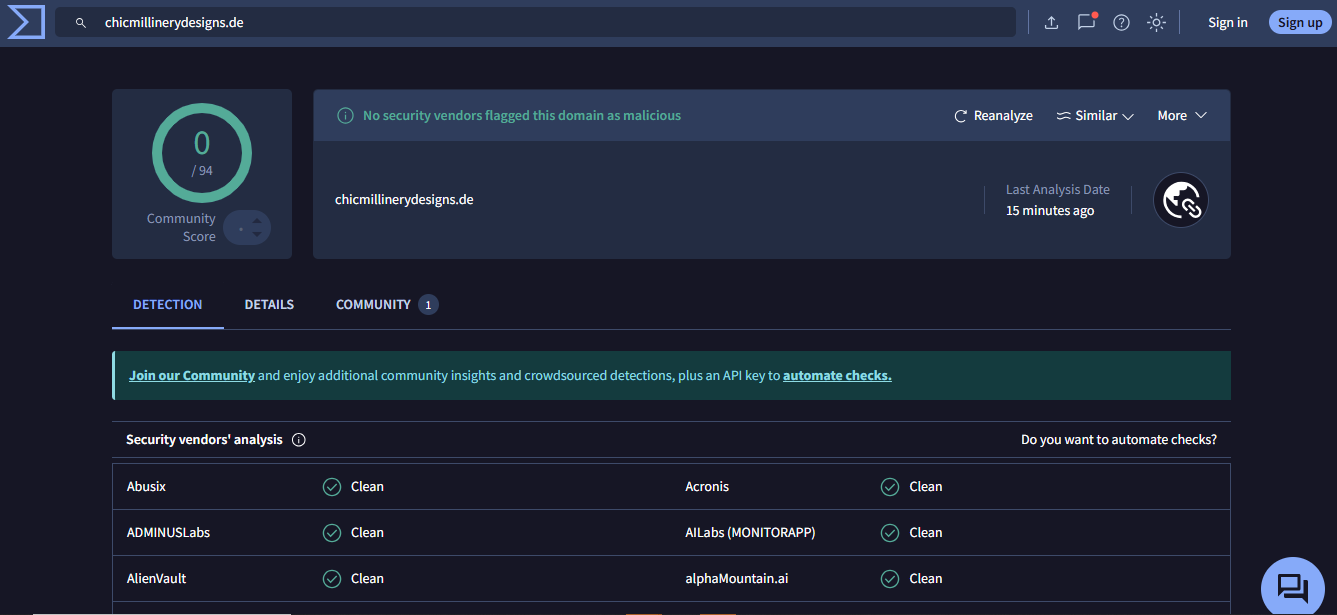
***This incident classification***– False Positive

***Closure rationale*** – The domain is not flagged by an online sandbox.

**Alert 1001; Suspicious email from an external domain**

****

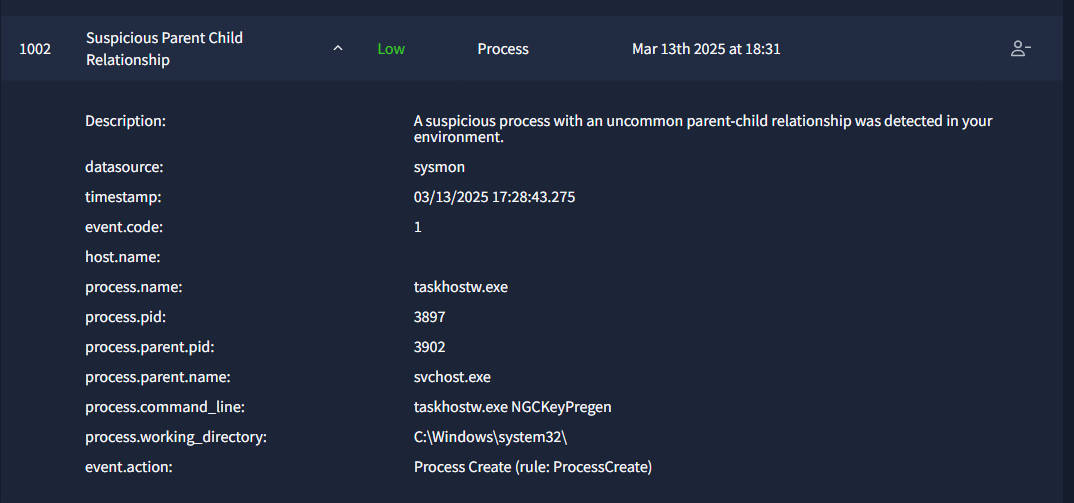
Similar to the first alert, no attachment in the mail, so I checked the online sandbox just like the first alert. From all indications, the domain is marked as non-malicious.



***Incident classification*** – False Positive

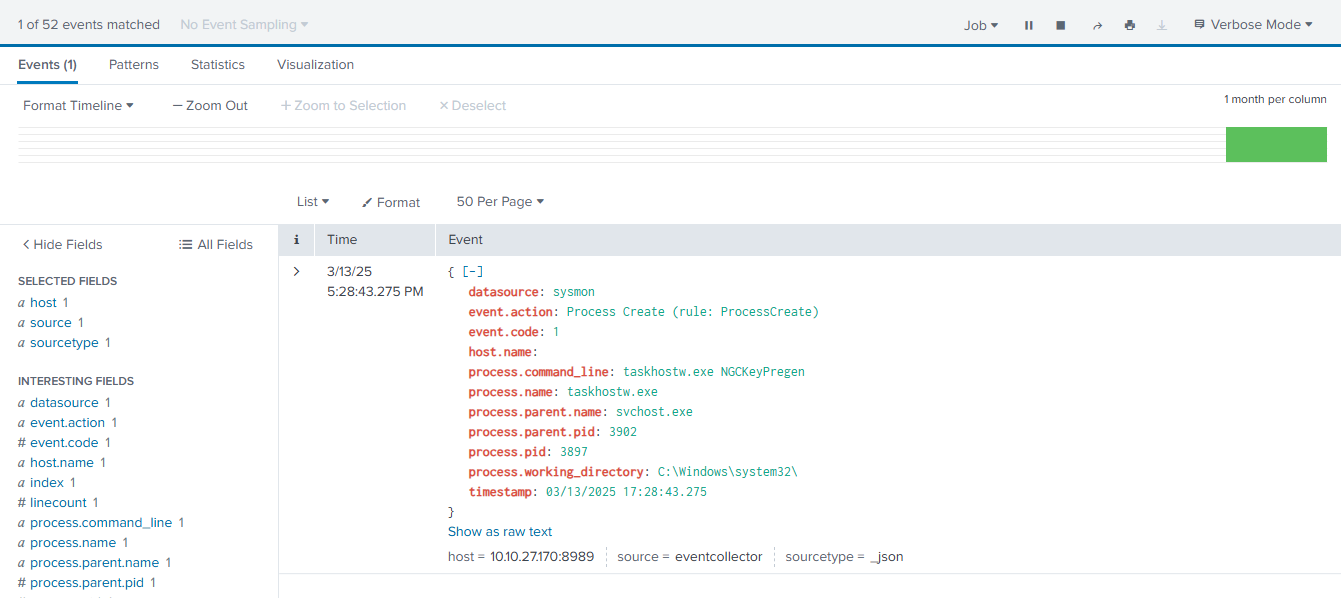
***Closure rationale*** – The mail sender domain is not malicious.

**Alert 1002; A suspicious process with an uncommon parent-child relationship was detected in your environment.**

****

Parent-child process relationships in security is when a parent process is a process pretending to be a system process spawned by a non-system process. From this alert, we see the process id, process name, parent name, parent pid, the command line , working directory and the event action. From the command line and the working directory, I discovered the process is a process to crack a software on a windows system32.

First, I took ownership of the alert, then moved over to Splunk to investigate the process to find out if this is common or not common.



On Splunk, search all available events and then streamline the search with the Process ID (3897), including a table with the process. Name, process. parent,working directory

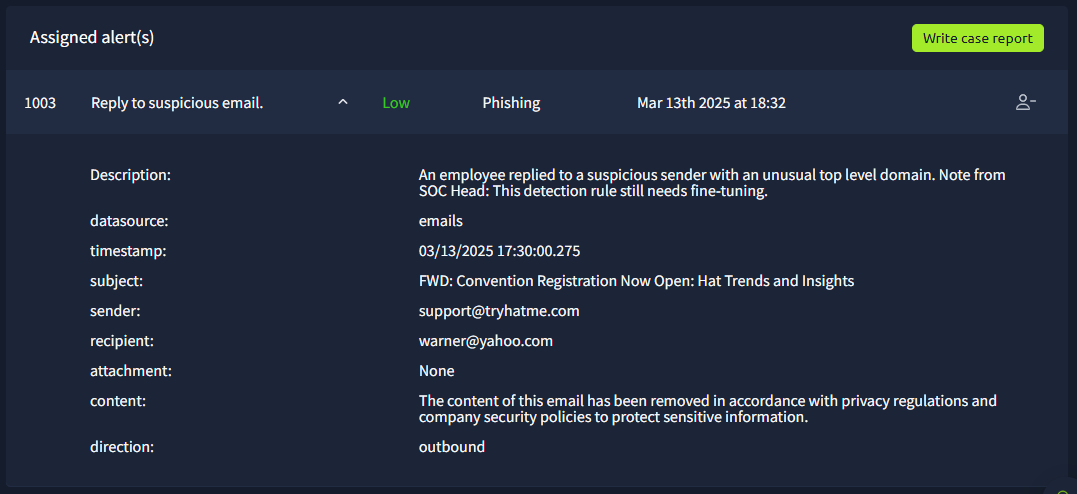
From the search, there is a total of one event which is the same as the alert received.

Looking at this, the working directory is in the main system containing all of the original system executable. The process Parent name is the service host and the task host is the process responsible for the task scheduler service. This appears to be a normal process.

***Incident classification*** – False Positive

***Closure rationale*** – After the investigation, the relationship between the mentioned process is normal.

**Alert 1003; Reply to Suspicious email**

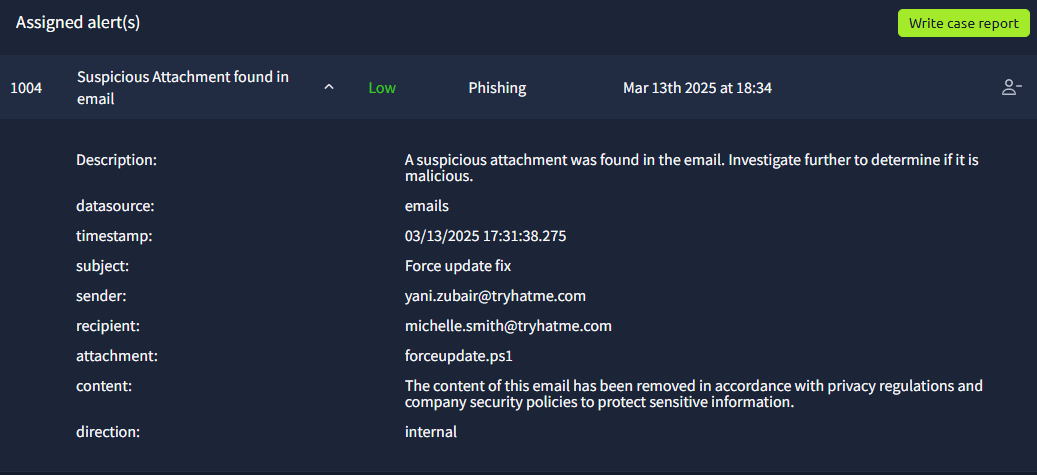
****

From the alert, it is an outbound message to someone with a yahoo email. This alert would be straight forward, no attachment and yahoo is a trusted domain.

***Incident classification*** – False Positive

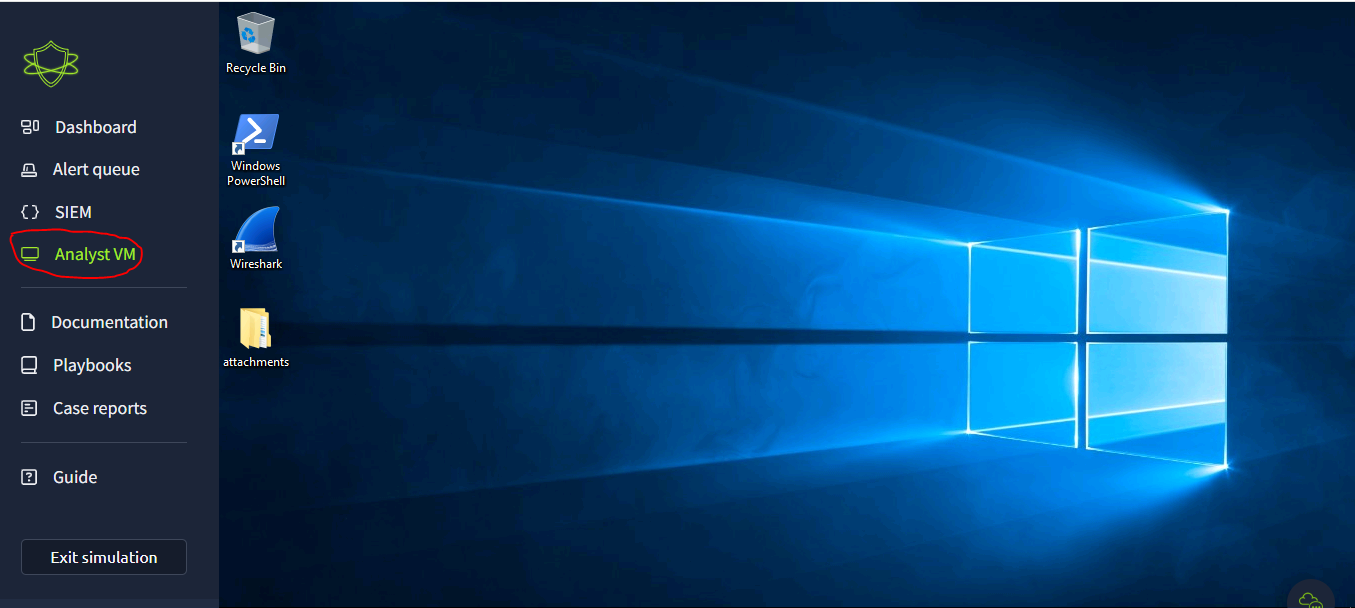
***Closure rationale*** – Both the sender and the receiver domains are not malicious and have no attachment.

**Alert 1004; Suspicious attachment found in email.**

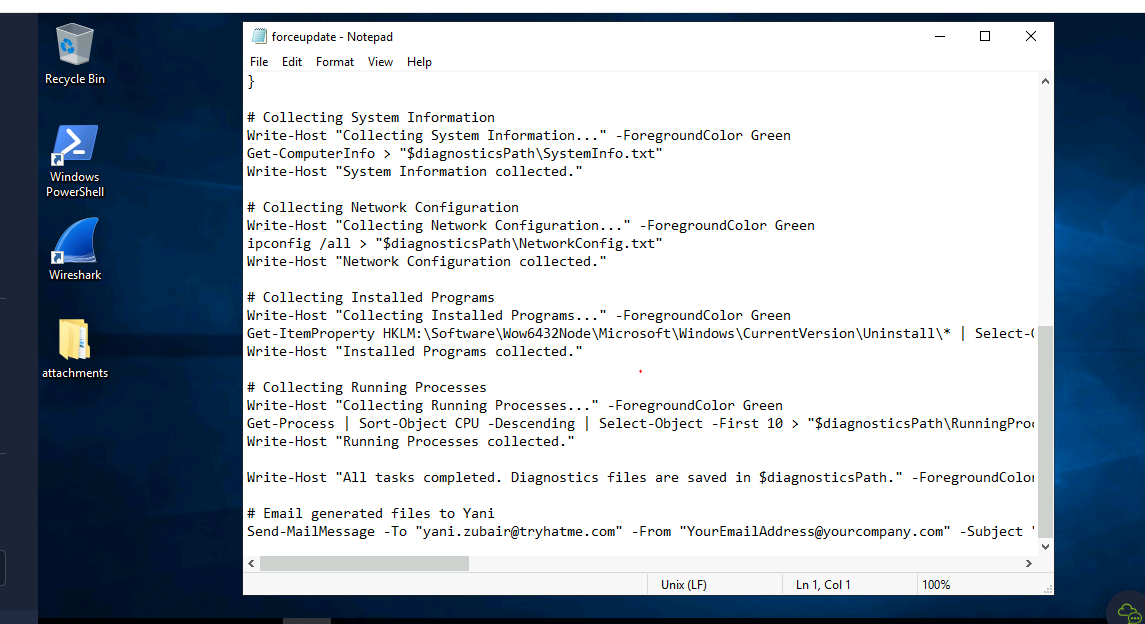
****

This alert indicates a mail with a file attachment between two people in the same organization. The extension of this attachment is a partial script. Judging from the attachment name it is a force update.

To check this alert we do not have to analyze the domain because this is an internal mail, but the attachment needs to be analyzed. To do this, I used the analyst virtual machine (Analyst VM)



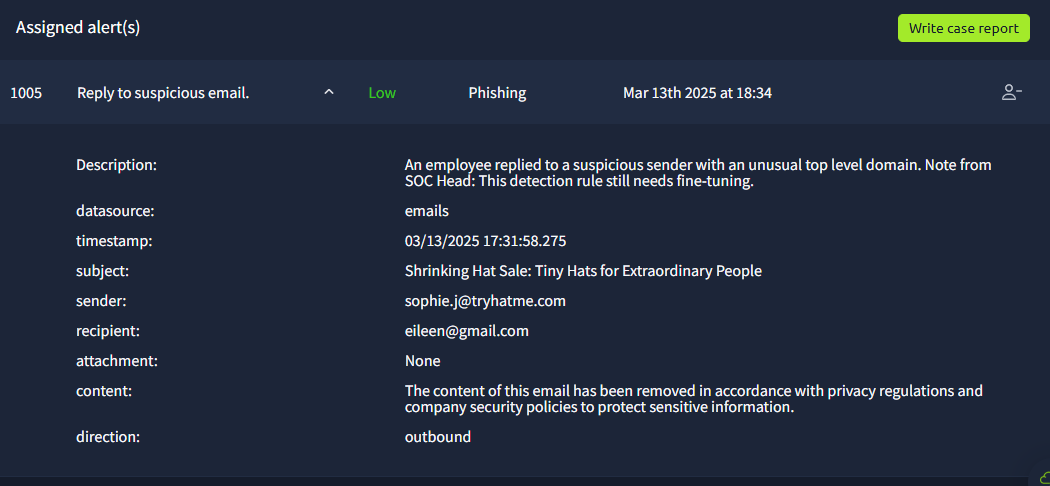
I checked the attachments; there we see the forceupdate file. Then open the file with notepad

The script on the notepad shows that the script is running system diagnostics, collecting information on the system as well as on the network. From all indications, this seems to be a normal script.

***Incident classification*** – False Positive

***Closure rationale*** – The script looks normal after the analysis.

**Alert 1005; Reply to suspicious email.**

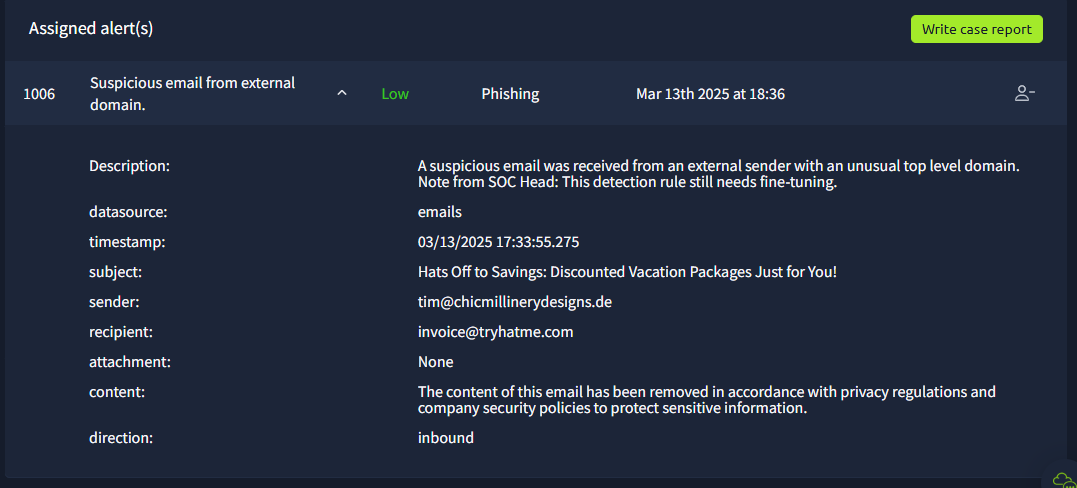
****

This alert is like **Alert 1003**. It is an outbound message to someone with a gmail account and no attachments.

***Incident classification*** – False Positive

***Closure rationale*** – Both the sender and the receiver domains are not malicious and have no attachment.

**Alert 1006; Suspicious email from an external domain**

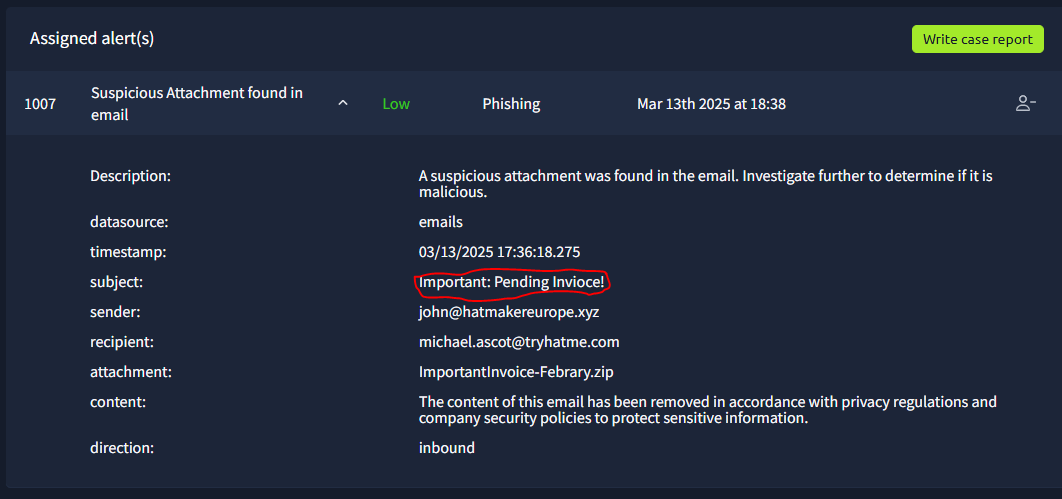
****

This domain was the same domain on the **Alert 1001** and from the analysis, this domain is a non-malicious domain and no attachment in the mail.

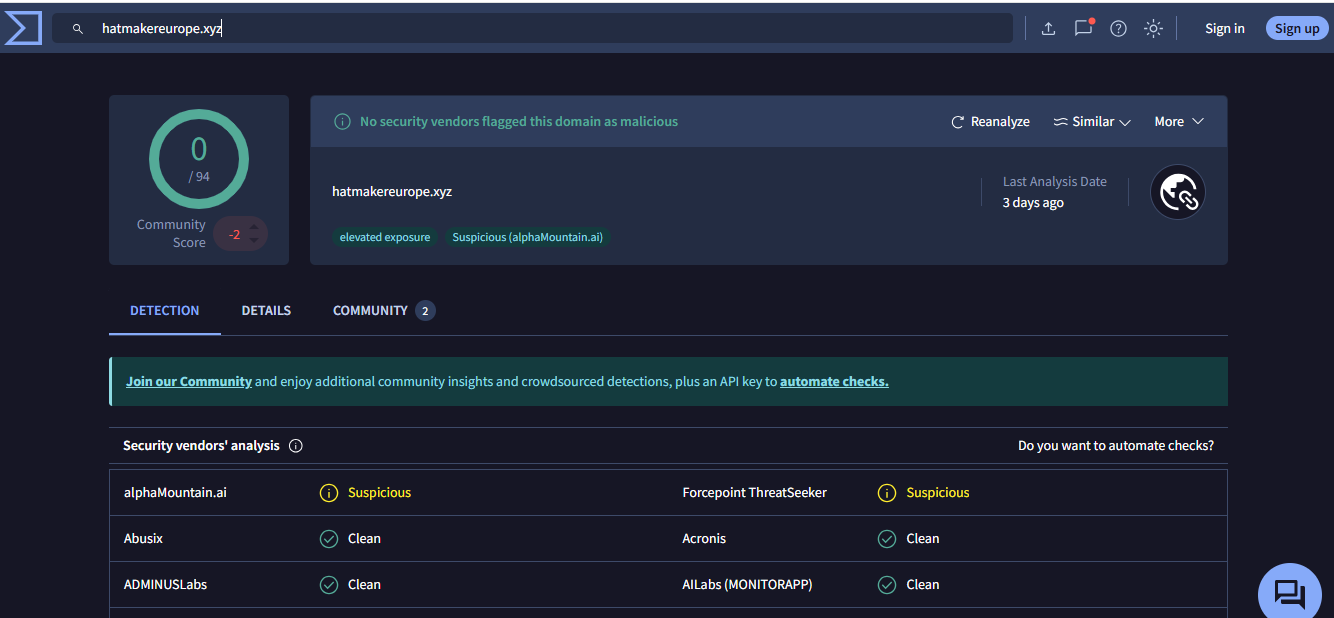
***Incident classification*** – False Positive

***Closure rationale*** – Previously analyzed domain and found to be non-malicious.

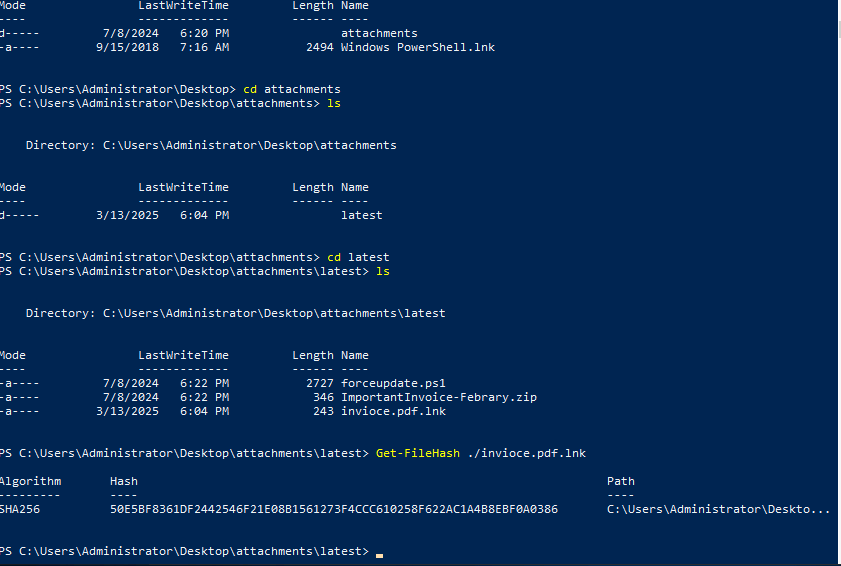
**Alert 1007; Suspicious attachment found in email.**

****

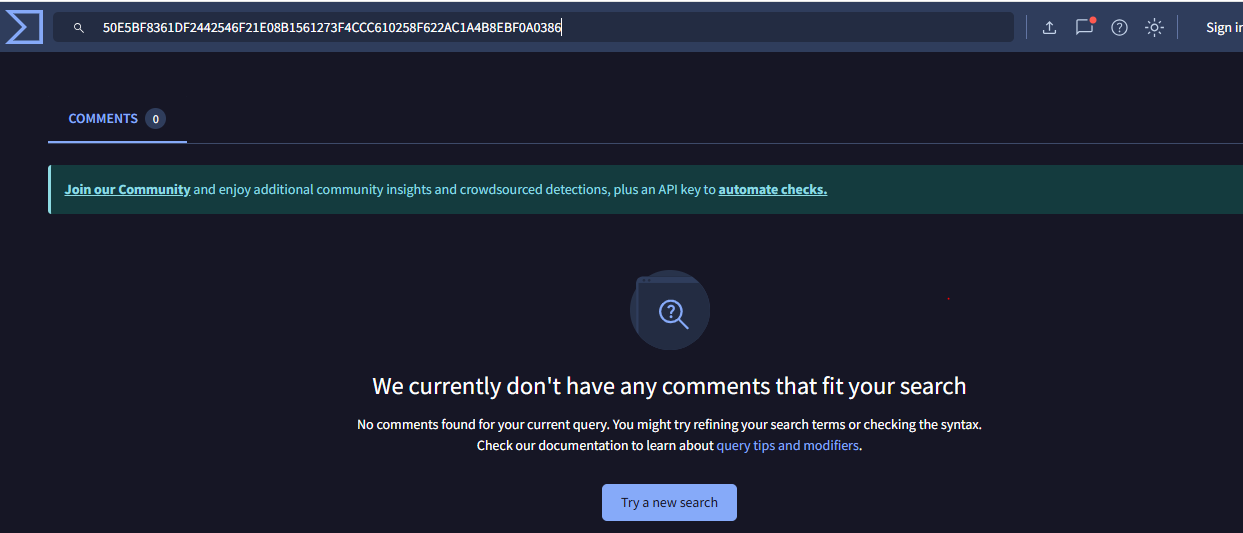
The email was sent from a domain hatmarkereurope.xyz with an attachment, importantinvoice.zip. First, I checked the domain on an online sandbox.



The domain was marked as non-malicious however, some vendors marked it as a bit suspicious. Moving on to analyze the attachment: for this I used the virtual machine. After unzipping the file, I see it is a PDF file, so I need to analyze this file. For this, I will use Powershell to acquire the hash. Use the adequate command lines to see what is in the important invoice.

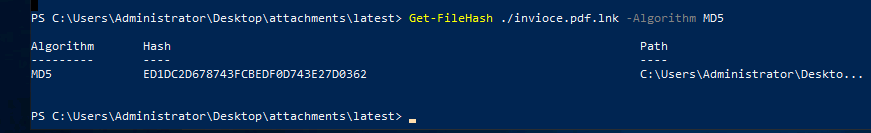


The hash is SHA256. Copied this on check on online sandbox – virustotal.



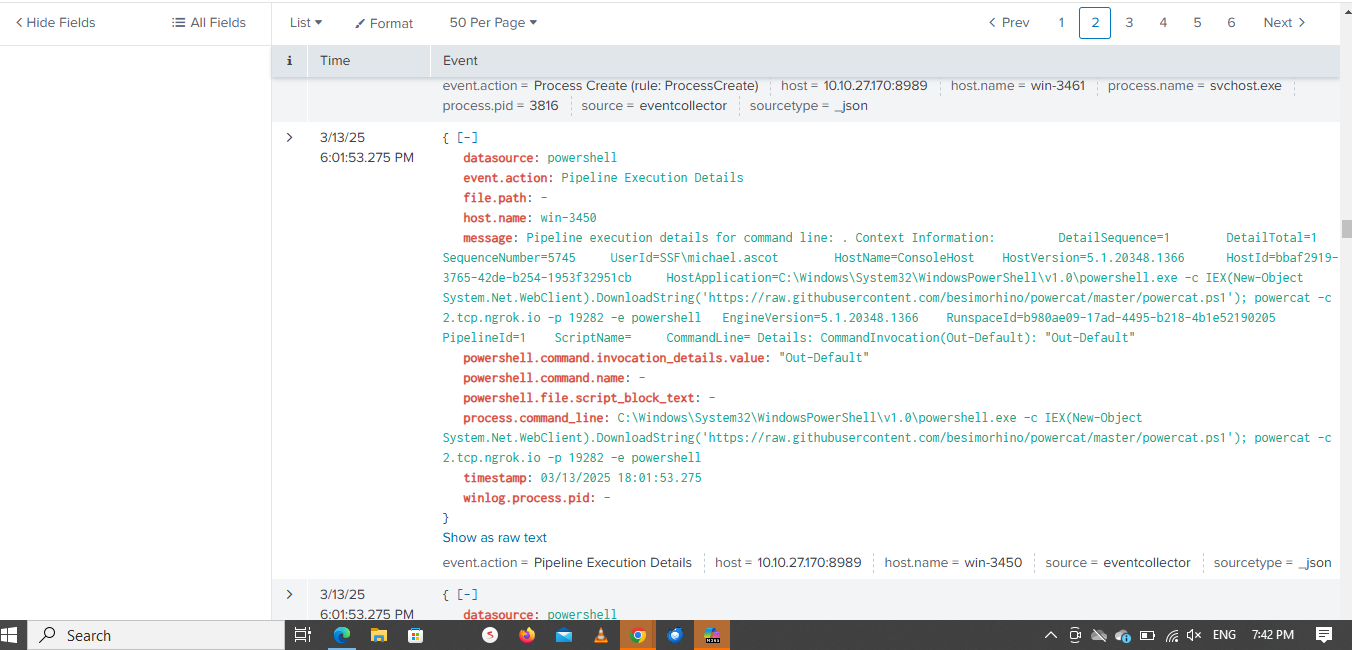
No data was found on virustotal.

Tried selecting algorithm MD5 hash. Copied this and checked on virustotal



No data was found as well.

This file still seems suspicious, because the naming of the file raises concerns and additionally it is from an external source. So, for further analysis, I used Splunk to check activities that have happened since the time the file was received.



From the analysis I see a Powershell execution and it is connected to the invoice. Upon investigation, there is a partial executable right to download an object from this URL. It is a git repository to receive power cat which is a privilege escalation.

***Incident classification*** – True Positive

***Closure rationale*** – Using the timestamp of the received invoice attachment. A powershell command was executed to download a privilege escalation powershell script, powercat.ps1 and connected to a C2 server.

**Final step** – Escalate the alert.

Tools used

* Virtual Machine
* SIEM Tool (Splunk)
* Online sandbox - Virus Total
* BASH script.