Alert Triage With Elastic

Introduction

This lab simulates an investigation involving suspicious activity detected in a client's infrastructure. As the on-call SOC analyst, the goal is to use Kibana dashboards and Windows/Sysmon logs to confirm whether the activity is malicious and to reconstruct the attacker's actions step by step. The scenario includes web exploitation attempts, account manipulation, and command execution across the host, requiring correlation between different log sources to fully understand the attack chain.

Objectives

- Access and configure the Kibana environment to retrieve relevant log data.
- Identify malicious web activity, including POST requests and suspicious user agents.
- Detect exploitation patterns through URL path queries and timestamp filtering.
- Trace Windows Security and Sysmon events related to account creation and privilege escalation.
- Reconstruct attacker behaviour by analysing executed commands and host-level activity.
- Document all findings clearly to support incident triage and response.

By:Fábio Vieira

Provided: TryHackMe

Scenario Briefing

Your team is responsible for managing several small businesses' servers, applications, and network infrastructure. Suspicious activity in your client, SomeCorp's infrastructure, has triggered multiple alerts. As the on-call SOC analyst, use the provided logs, dashboards, and tools to investigate the activity, determine if it is malicious, and reconstruct the attack sequence.

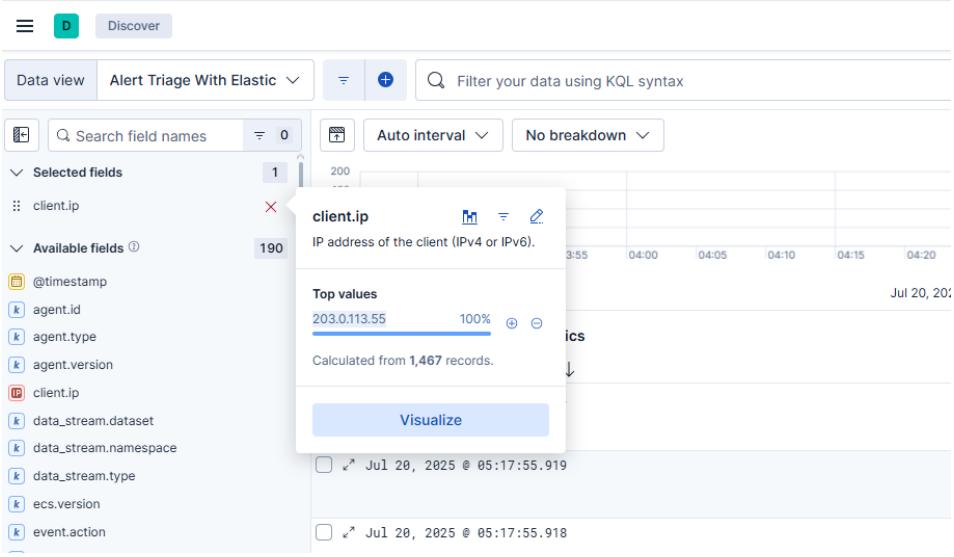
Time	Name	Severity	Status	Verdict	Assignee	Actions
Jul 20th 2025 at 04:38	Web Requests Indicating File Upload	High	Awaiting action	None	None	
Jul 20th 2025 at 04:45	GET Requests to ASPX File with Query Parameters	High	Awaiting action	None	None	
Jul 20th 2025 at 05:11	Administrator Access Outside of Business Hours	High	Awaiting action	None	None	
Jul 20th 2025 at 05:13	New User Account Created	Critical	Awaiting action	None	None	
Jul 20th 2025 at 05:13	Unusual Command-Line Behavior: Privilege Changes	Critical	Awaiting action	None	None	

You log in to the SOC dashboard provided above and see many alerts to triage. But first, you must build out your environment on the Kibana interface. Let's start by accessing the Kibana dashboard and choosing the correct filters.

How many logs are available for analysis within the entire time range?

Documents (1,467)

What is the field value for the client.ip in the weblogs index?



Investigating Web Attacks

How many POST requests did the IP address 203.0.113.55 make to proxyLogon.ecp?

By adding **@timestamp/client.ip/user.agent /http.response.status_code/url.path** and the filter **_index:weblogs and client.ip:203.0.113.55 and http.request.method:POST** we get to the conclusion that was 3 POST requests to proxyLogon.ecp.

Which user.agent paired with the IP address 203.0.113.55 made the POST requests?

Using the same table as in the previous question, we obtained **python-requests/2.25.1**.

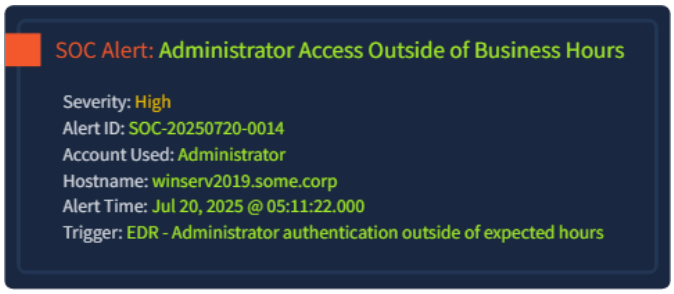
How many logs contain the cmd= query parameter in the url.path field?

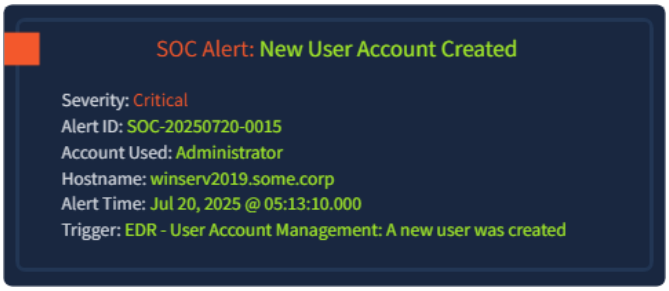
With the query **url.path : cmd** we obtain the result '**20**'.

Which command was run utilizing errorEE.aspx on Jul 20, 2025 @ 04:45:50.000?

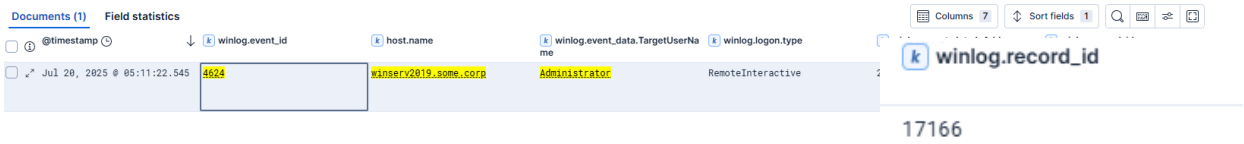
With the query **@timestamp : "2025-07-20T04:45:50.000Z"** we see that the executed command was **hostname.**

Uncovering Account Activity

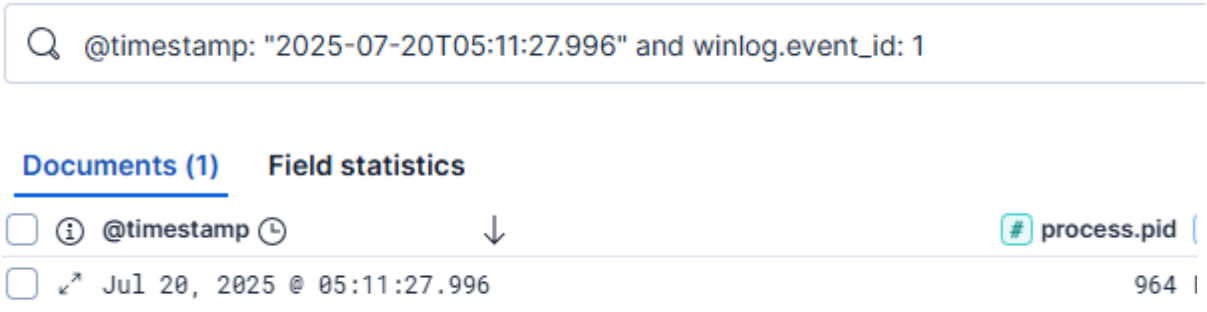




What is the winlog.record_id of the Administrator 4624 logon event?



What is the process.pid of the Sysmon 1 event that occ 2025 @ 05:11:27.996?



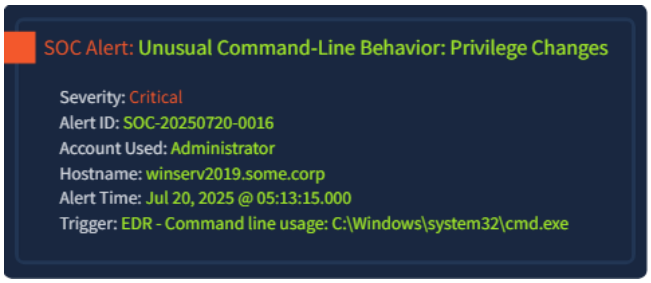
What is the winlog.event_id for the new user account being created?

4720.

What is the name of the new user account?

Using the filter **winlog.event_id: 4720**, we can see in the message that the username is **svc_backup.**

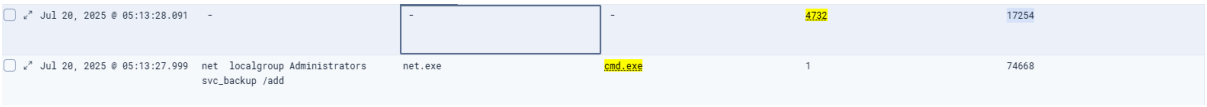
Exposing Command Execution



What command does the attacker use to add the new account to the "Remote Desktop Users" group?

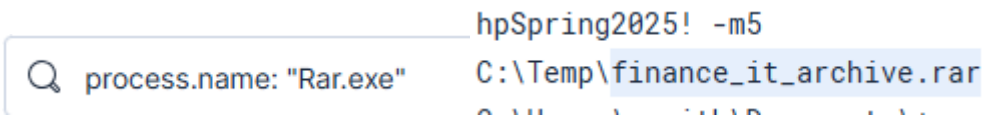
With the filter **@timestamp >= "2025-07-20T05:13:15" and process.parent.name:cmd.exe and user.name:Administrator**, we conclude that the command executed was **“net localgroup Administrators svc_backup /add”.**

What is the winlog.record_id of the 4732 Security event when the attacker adds the user to the Administrator group?



What PowerShell command did the attacker run on Jul 20, 2025 @ 05:16:14.628?

What is the name of the archive that the attacker creates using the Rar.exe executable?



Conclusion

Through log analysis in Kibana, we confirmed that the attacker performed targeted POST requests, executed commands via web exploitation endpoints, created a new user account, and escalated its privileges using Windows command-line activity. Correlation of event IDs, timestamps, and process metadata allowed the full attack sequence to be rebuilt. The investigation shows clear evidence of malicious activity, demonstrating how a SOC analyst can pivot across different log sources to identify compromise and understand the attacker's actions.