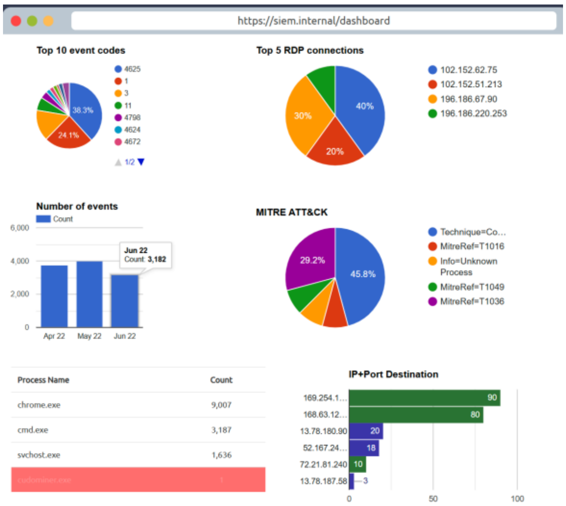
SIEM Alert Analysis – Potential Crypto Miner Activity

Q1 – Which process caused the alert?

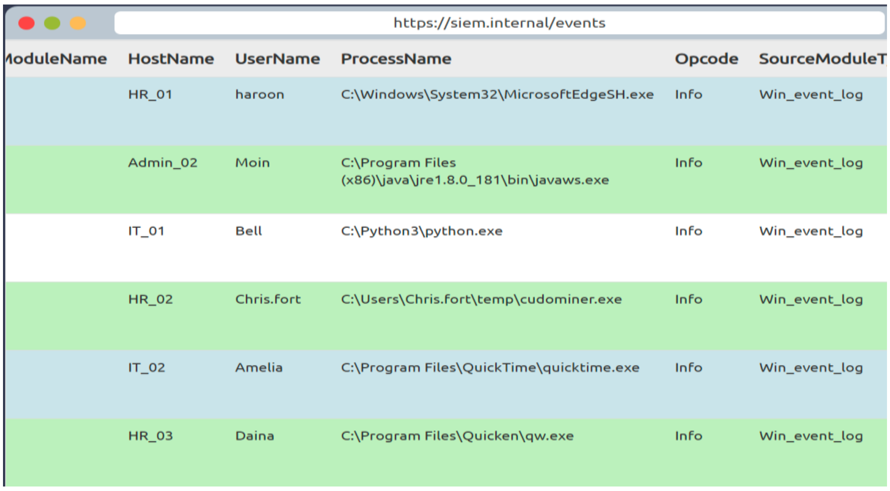


Process Name	Count
chrome.exe	9,007
cmd.exe	3,187
svchost.exe	1,636
cudominer.exe	1

Explanation:

By examining the SIEM dashboard, I checked the section displaying Process Name and Count to identify which process triggered the alert. The suspicious process cudominer.exe appeared highlighted in red with a single event count, indicating potential cryptocurrency mining activity.

Q2 – Find the event that caused the alert. Which user was responsible for the process execution?



https://siem.internal/events

ModuleName	HostName	UserName	ProcessName	Opcode	SourceModuleT
	HR_01	haroon	C:\Windows\System32\MicrosoftEdgeSH.exe	Info	Win_event_log
	Admin_02	Moin	C:\Program Files (x86)\java\jre1.8.0_181\bin\javaws.exe	Info	Win_event_log
	IT_01	Bell	C:\Python3\python.exe	Info	Win_event_log
	HR_02	Chris.fort	C:\Users\Chris.fort\temp\cudominer.exe	Info	Win_event_log
	IT_02	Amelia	C:\Program Files\QuickTime\quicktime.exe	Info	Win_event_log
	HR_03	Daina	C:\Program Files\Quicken\qw.exe	Info	Win_event_log

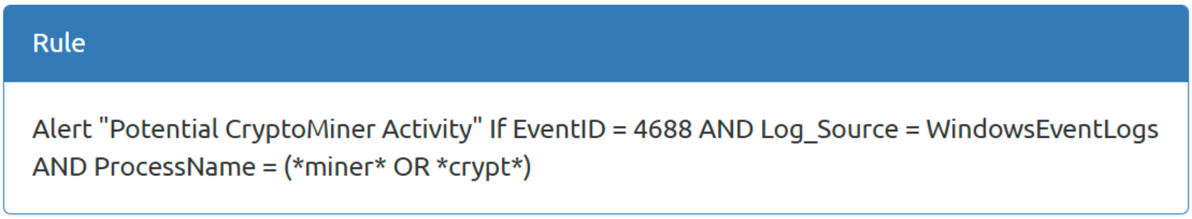
Explanation:
After identifying cudominer.exe as the suspicious process, I reviewed the event logs to determine which user executed it.
The log analysis showed that Chris.fort was responsible for running the process.

Q3 – What is the hostname of the suspect user?

Answer: HR_02

Q4 – Examine the rule and the suspicious process; which term matched the rule that caused the alert?

Explanation:
The detection rule named “Potential CryptoMiner Activity” triggers when process creation events (Event ID 4688) contain keywords such as miner or crypt.
In this case, the suspicious process cudominer.exe matched the term “miner”, which activated the alert.



Rule

```
Alert "Potential CryptoMiner Activity" If EventID = 4688 AND Log_Source = WindowsEventLogs
AND ProcessName = (*miner* OR *crypt*)
```

Post-Incident Actions

After validating the alert as True-Positive, the following containment and remediation steps should be executed:

Isolate the affected host (HR_02) to prevent lateral movement or continued resource abuse.

Collect forensic evidence, including memory capture, process list, and active network connections.

Terminate and remove the malicious process (cudominer.exe) and inspect for persistence methods such as scheduled tasks or registry keys.

Reimage or clean the compromised machine if integrity cannot be guaranteed.

Update SIEM detection rules to enhance identification of mining software variants.

Notify and train the user (Chris.fort) about unauthorized software installations to prevent recurrence.