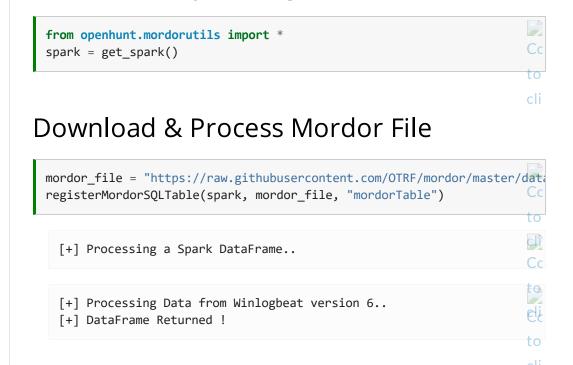


Analytics

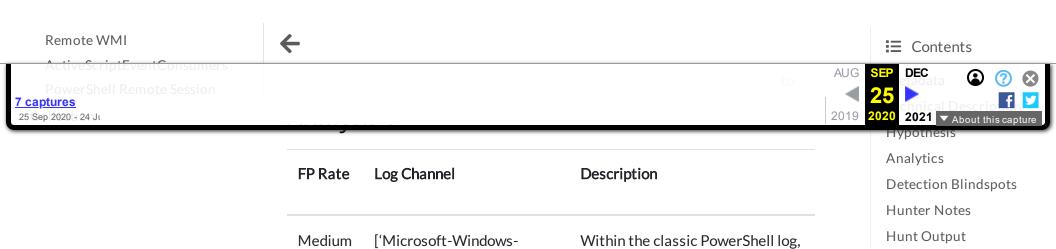
Extraction

Initialize Analytics Engine



PowerShell/Operational',

'PowerShell']



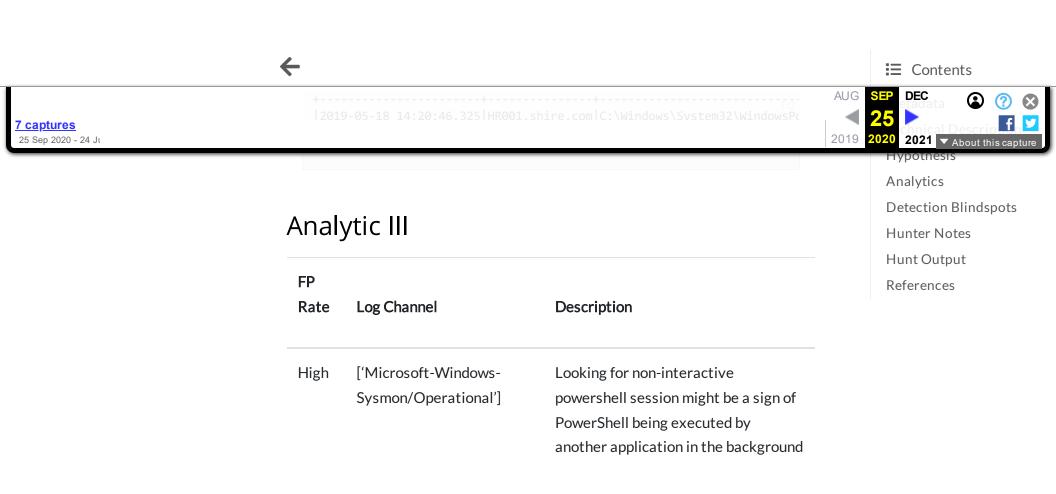
event ID 400 indicates when a

new PowerShell host process has

References

Analytic II

FP Rate	Log Channel	Description
High	['Security']	Looking for non-interactive powershell session might be a sign of PowerShell being executed by another application in the background



```
|@timestamp | computer_name | Image | Cc | 2019-05-18 14:20:46.353 | HR001.shire.com | C:\Windows\System32\Windows\Ci.
```

Analytic IV

FP Rate	Log Channel	Description
Medium	['Microsoft-Windows- Sysmon/Operational']	Monitor for processes loading PowerShell DLL system.management.automation



Analytic VI

FP Rate	Log Channel	Description	
Medium	['Microsoft-Windows- Sysmon/Operational']	The "PowerShell Named Pipe IP event will indicate the name of the PowerShell AppDomain that started. Sign of PowerShell execution	
df = spar	k.sql(Otimestamp`, computer_name,	message	Cc
FROM mordorTable WHERE channel = "Microsoft-Windows-PowerShell/Operational" AND event_id = 53504			cli
) df.show(1	0,False)		

|computer_name |message

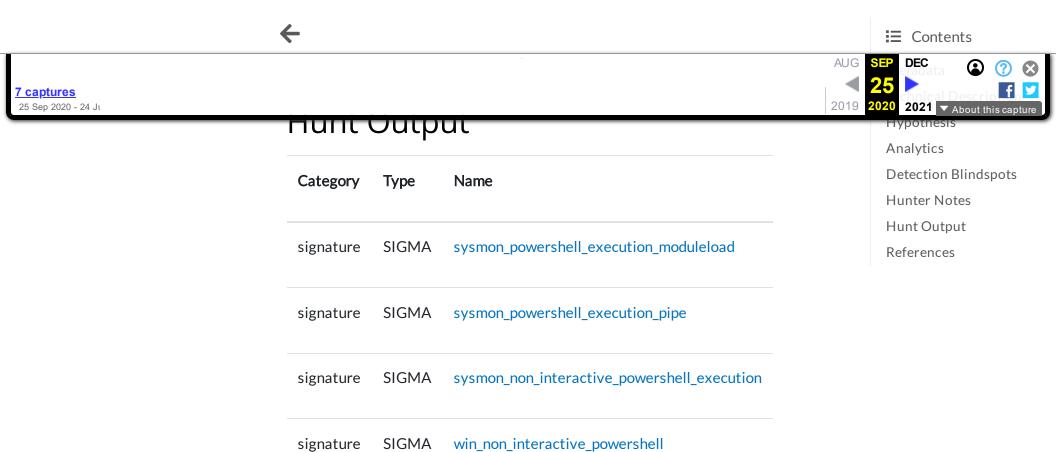
|2019-05-18 14:20:49.47|HR001.shire.com|Windows PowerShell has started

Detection Blindspots

Hunter Notes

|@timestamp

- Explore the data produced in your environment with the analytics above and document what normal looks like from a PowerShell perspective.
- If execution of PowerShell happens all the time in your environment, I
 suggest to categorize the data you collect by business unit to build profiles
 and be able to filter out potential noise.



References

- https://github.com/darkoperator/Presentations/blob/master/PSConfEU%202019%20Tracking%20PowerShell
- https://posts.specterops.io/abusing-powershell-desired-state-configurationfor-lateral-movement-ca42ddbe6f06

<< WMI Win32_Process Class and Create Method for Remote Execution Service Creation >>

By Roberto Rodriguez @Cyb3rWard0g © Copyright 2020.