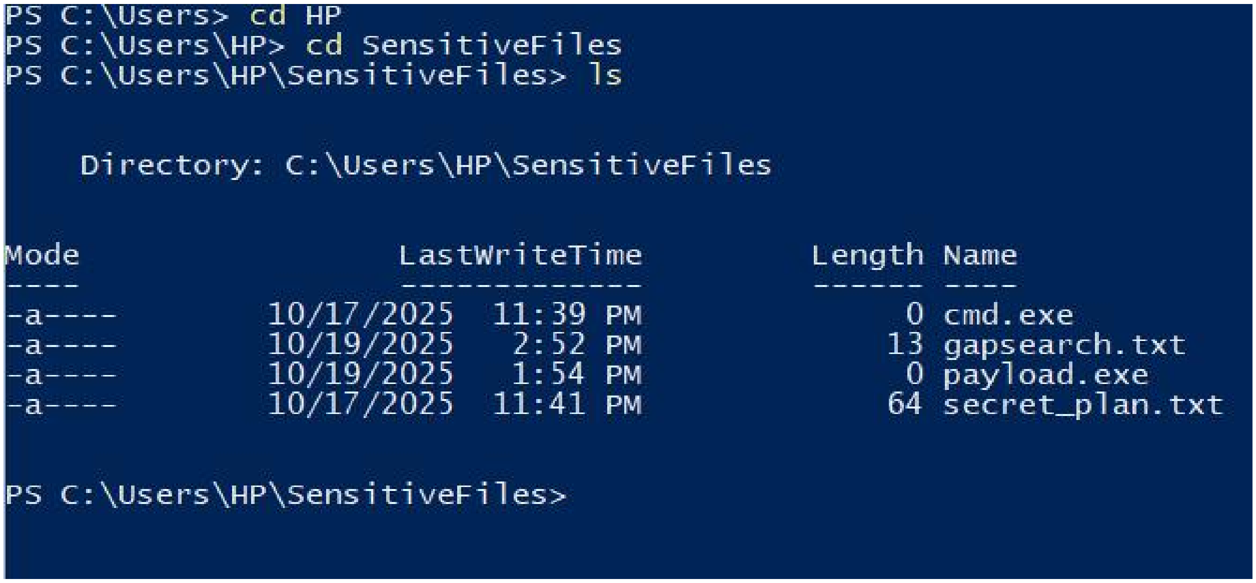
NAME: Adeyemi Akande

REGNO: INT/2024/EH/3800

COURSE:INT403 LAB 3

This lab report summarises my investigation and findings. The exercises were executed on the assigned Windows agent (CrownFitSMe, 192.168.100.146) and supporting lab hosts. Ninety percent of the evidence collected consists of screenshots capturing process creation, scheduled tasks, and file artifacts, ensuring a verifiable timeline. Logs and alerts from the Wazuh manager complement the visual records

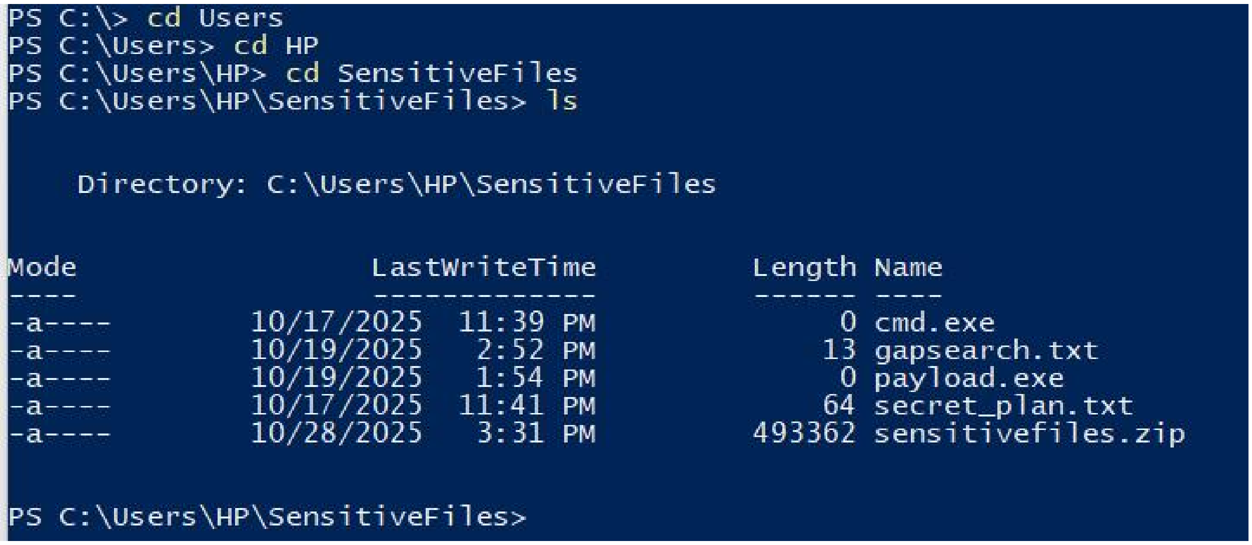


```
PS C:\Users> cd HP
PS C:\Users\HP> cd SensitiveFiles
PS C:\Users\HP\SensitiveFiles> ls


    Directory: C:\Users\HP\SensitiveFiles


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       10/17/2025  11:39 PM              0 cmd.exe
-a----       10/19/2025   2:52 PM             13 gapsearch.txt
-a----       10/19/2025   1:54 PM              0 payload.exe
-a----       10/17/2025  11:41 PM             64 secret_plan.txt


PS C:\Users\HP\SensitiveFiles>
```



```
PS C:\> cd Users
PS C:\Users> cd HP
PS C:\Users\HP> cd SensitiveFiles
PS C:\Users\HP\SensitiveFiles> ls


    Directory: C:\Users\HP\SensitiveFiles


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/17/2025  11:39 PM              0 cmd.exe
-a----        10/19/2025   2:52 PM             13 gapsearch.txt
-a----        10/19/2025   1:54 PM              0 payload.exe
-a----        10/17/2025  11:41 PM             64 secret_plan.txt
-a----        10/28/2025   3:31 PM         493362 sensitivefiles.zip


PS C:\Users\HP\SensitiveFiles>
```

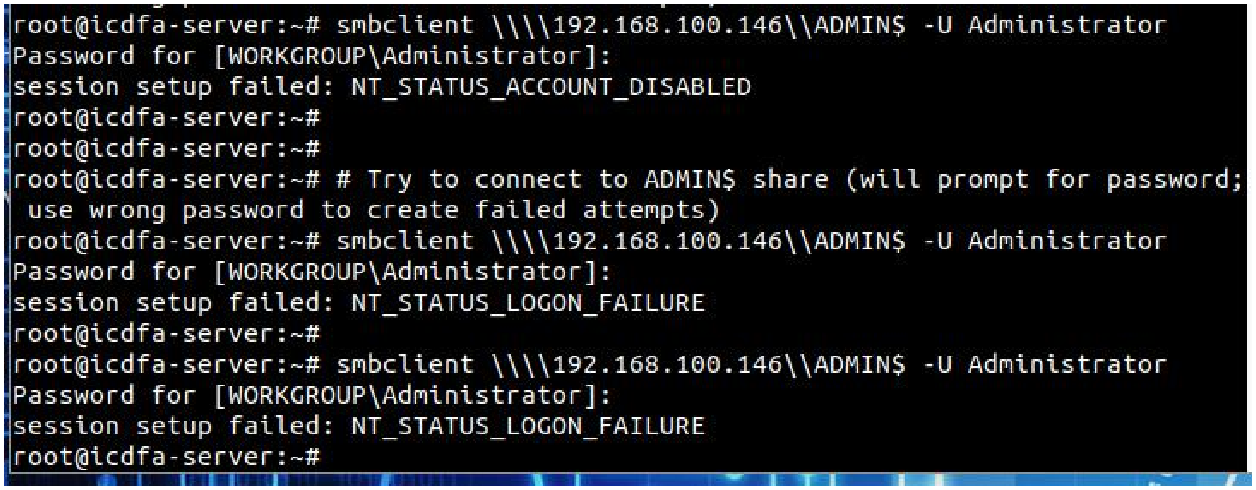
Simulate Lateral Movement (from your Linux/Web Server VM toward CrownFistMe)

I ran this command for easy access to windows:

sudo apt update && sudo apt install -y smbclient

i simulated login into windows agent using

smbclient \\\\192.168.100.146\\ADMIN$ -U Administrator

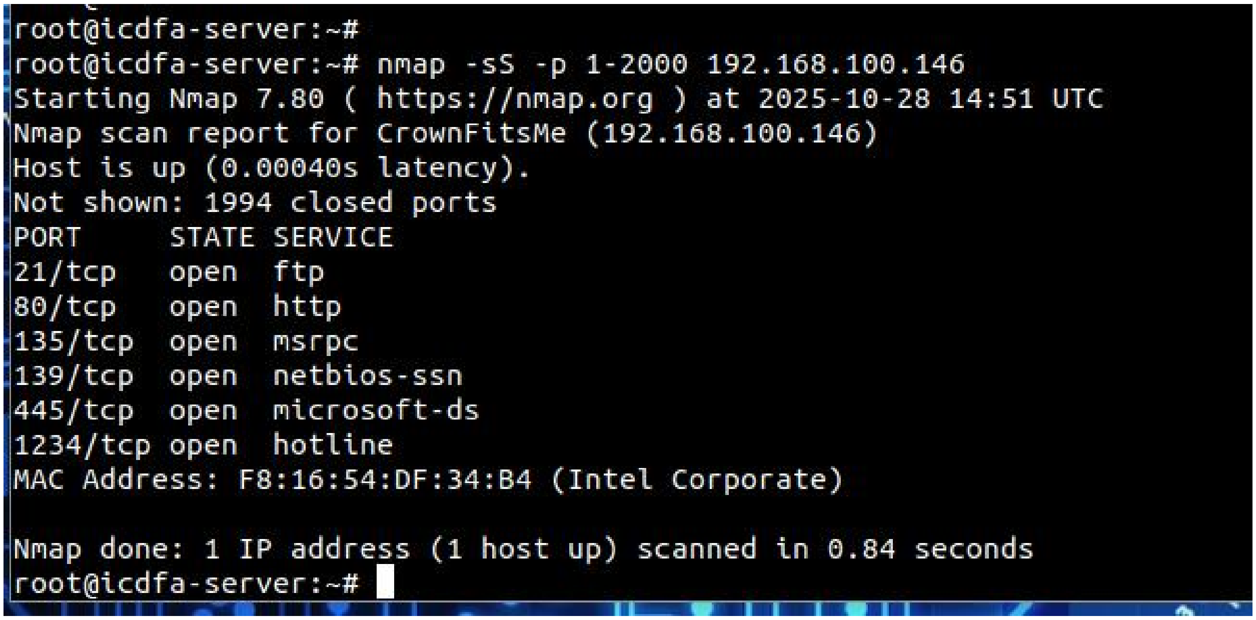


```
root@icdfa-server:~# smbclient \\\\192.168.100.146\\ADMIN$ -U Administrator
Password for [WORKGROUP\Administrator]:
session setup failed: NT_STATUS_ACCOUNT_DISABLED
root@icdfa-server:~#
root@icdfa-server:~#
root@icdfa-server:~# # Try to connect to ADMIN$ share (will prompt for password;
 use wrong password to create failed attempts)
root@icdfa-server:~# smbclient \\\\192.168.100.146\\ADMIN$ -U Administrator
Password for [WORKGROUP\Administrator]:
session setup failed: NT_STATUS_LOGON_FAILURE
root@icdfa-server:~#
root@icdfa-server:~# smbclient \\\\192.168.100.146\\ADMIN$ -U Administrator
Password for [WORKGROUP\Administrator]:
session setup failed: NT_STATUS_LOGON_FAILURE
root@icdfa-server:~#
```

I also Simulated Reconnaissance & Weaponization on using this command:

Please note that 192.168.100.146 is my windows agent 1p.

Suspicious operation: carrying out nmap scan on windows agent

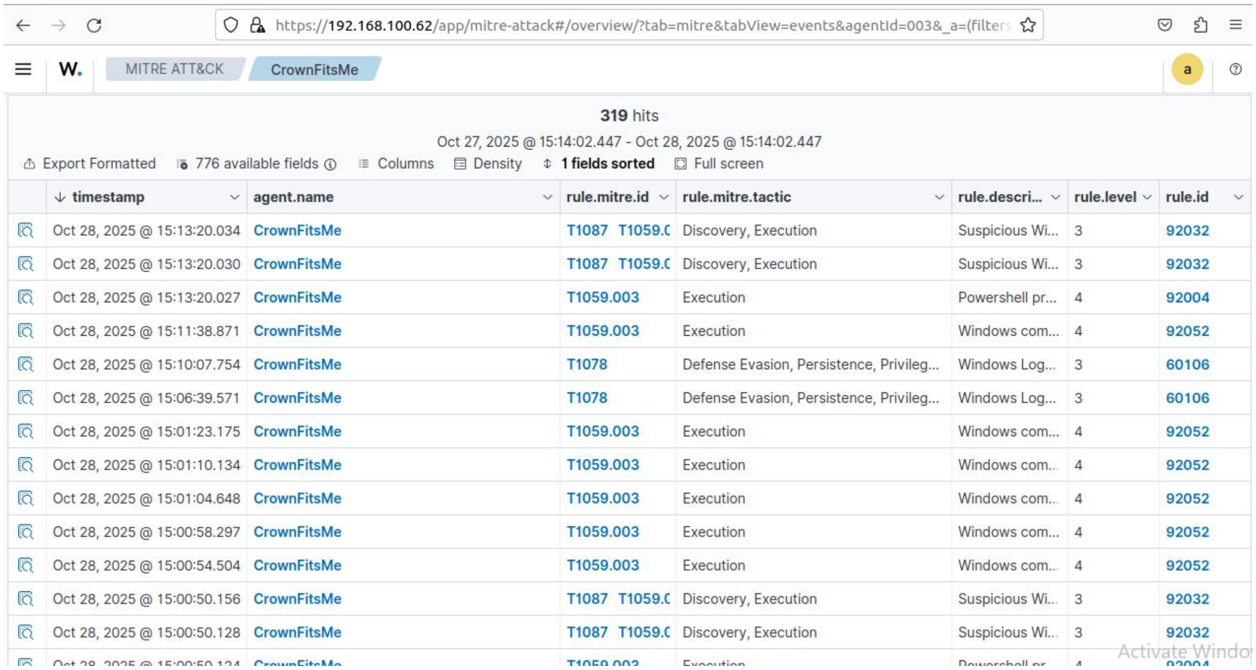


```
root@icdfa-server:~#
root@icdfa-server:~# nmap -sS -p 1-2000 192.168.100.146
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-28 14:51 UTC
Nmap scan report for CrownFitsMe (192.168.100.146)
Host is up (0.00040s latency).
Not shown: 1994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1234/tcp open  hotline
MAC Address: F8:16:54:DF:34:B4 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
root@icdfa-server:~# 
```

Hunting & Wazuh Dashboard Queries (use these in the Wazuh Dashboard search bar)

As it can be seen all the simulated mitre attack are captured in the wazuh dashboard



https://192.168.100.62/app/mitre-attack#/overview/?tab=mitre&tabView=events&agentId=003&_a=(filters

319 hits

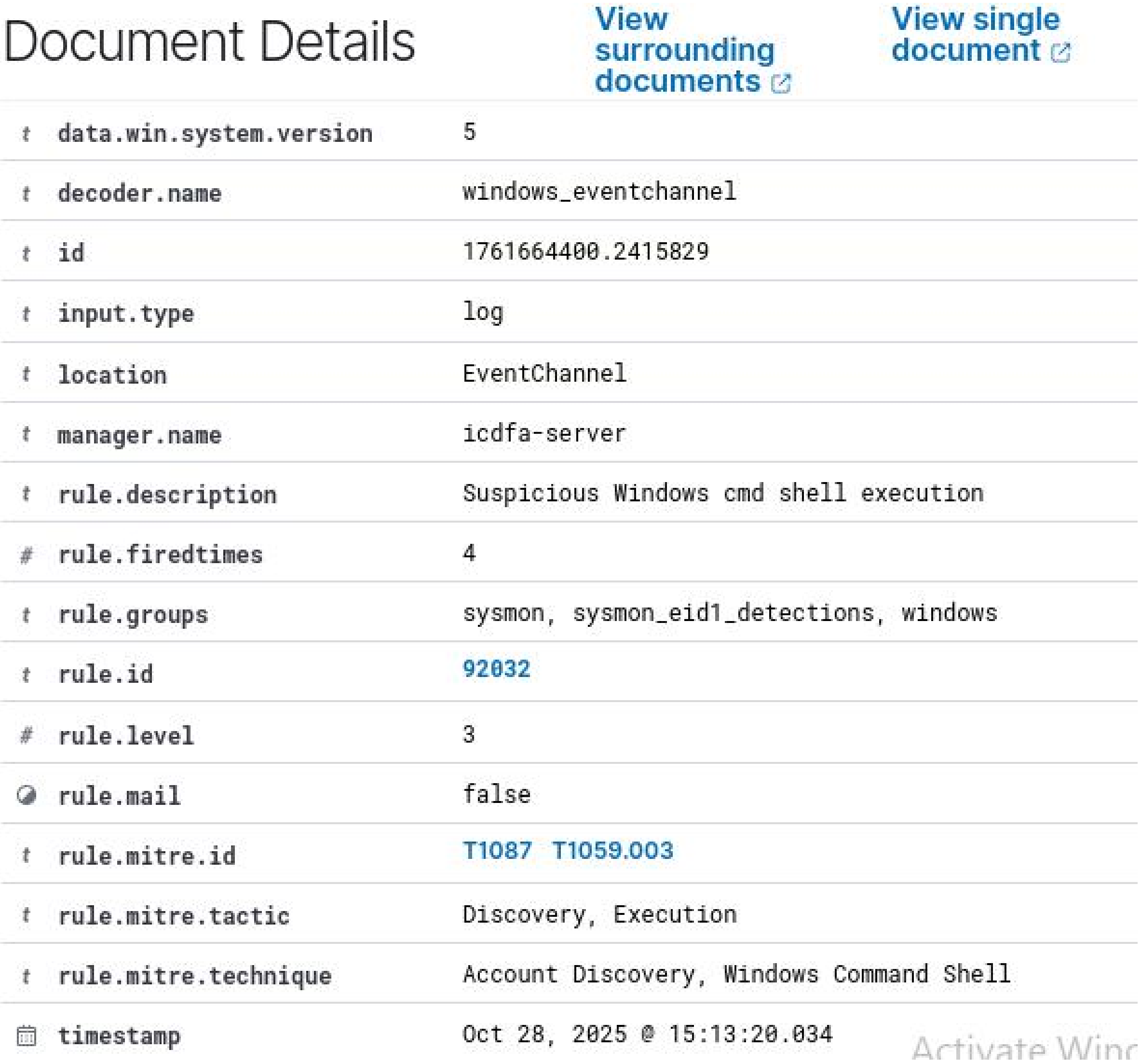
Oct 27, 2025 @ 15:14:02.447 - Oct 28, 2025 @ 15:14:02.447

776 available fields

1 fields sorted

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.descri...	rule.level	rule.id
Oct 28, 2025 @ 15:13:20.034	CrownFitsMe	T1087 T1059.(	Discovery, Execution	Suspicious Wi...	3	92032
Oct 28, 2025 @ 15:13:20.030	CrownFitsMe	T1087 T1059.(	Discovery, Execution	Suspicious Wi...	3	92032
Oct 28, 2025 @ 15:13:20.027	CrownFitsMe	T1059.003	Execution	Powershell pr...	4	92004
Oct 28, 2025 @ 15:11:38.871	CrownFitsMe	T1059.003	Execution	Windows com...	4	92052
Oct 28, 2025 @ 15:10:07.754	CrownFitsMe	T1078	Defense Evasion, Persistence, Privileg...	Windows Log...	3	60106
Oct 28, 2025 @ 15:06:39.571	CrownFitsMe	T1078	Defense Evasion, Persistence, Privileg...	Windows Log...	3	60106
Oct 28, 2025 @ 15:01:23.175	CrownFitsMe	T1059.003	Execution	Windows com...	4	92052
Oct 28, 2025 @ 15:01:10.134	CrownFitsMe	T1059.003	Execution	Windows com...	4	92052
Oct 28, 2025 @ 15:01:04.648	CrownFitsMe	T1059.003	Execution	Windows com...	4	92052
Oct 28, 2025 @ 15:00:58.297	CrownFitsMe	T1059.003	Execution	Windows com...	4	92052
Oct 28, 2025 @ 15:00:54.504	CrownFitsMe	T1059.003	Execution	Windows com...	4	92052
Oct 28, 2025 @ 15:00:50.156	CrownFitsMe	T1087 T1059.(	Discovery, Execution	Suspicious Wi...	3	92032
Oct 28, 2025 @ 15:00:50.128	CrownFitsMe	T1087 T1059.(	Discovery, Execution	Suspicious Wi...	3	92032
Oct 28, 2025 @ 15:00:50.124	CrownFitsMe	T1059.003	Execution	Powershell pr...	4	92004

The sysmon i installed played great role in capturing all the events

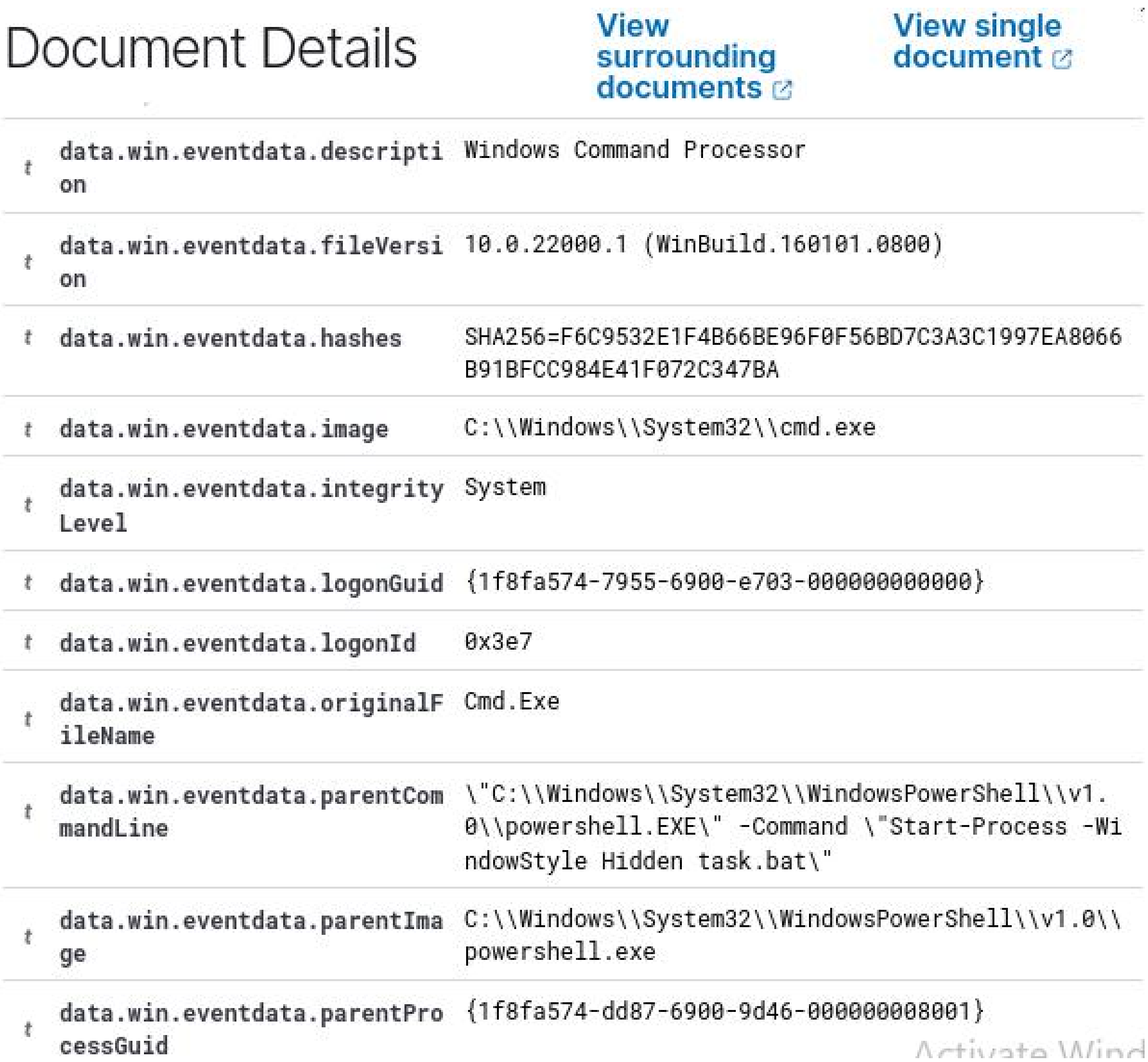


Document Details

View surrounding documents ↗

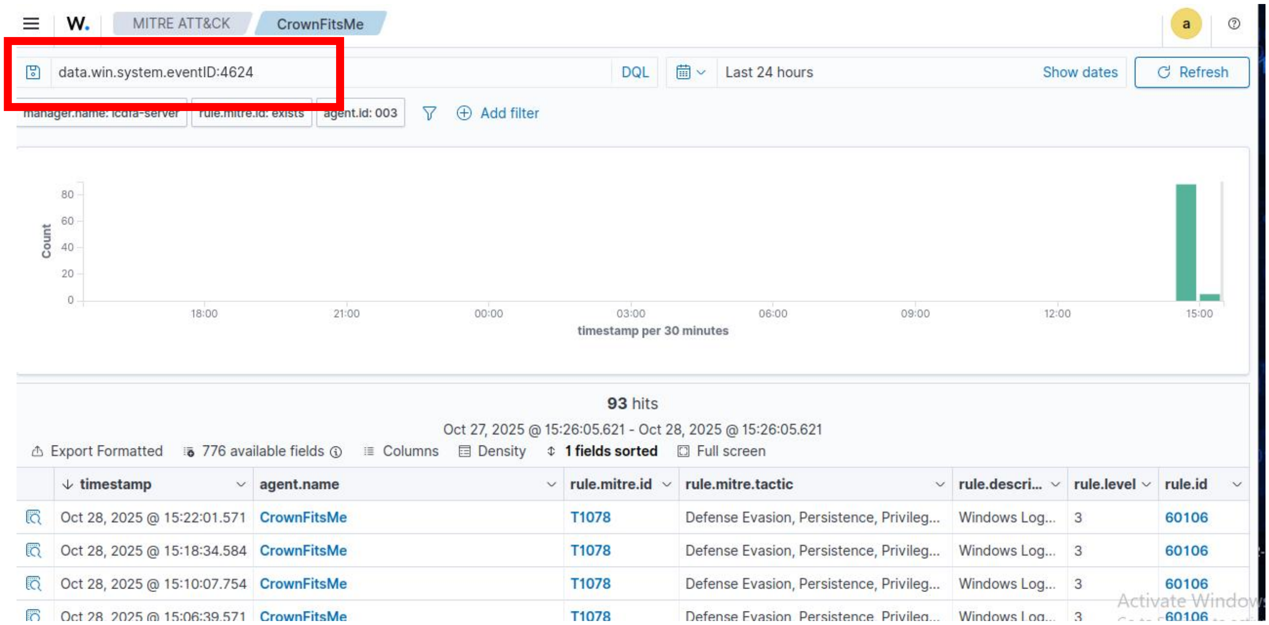
View single document ↗

t	data.win.system.version	5
t	decoder.name	windows_eventchannel
t	id	1761664400.2415829
t	input.type	log
t	location	EventChannel
t	manager.name	icdfa-server
t	rule.description	Suspicious Windows cmd shell execution
#	rule.firedtimes	4
t	rule.groups	sysmon, sysmon_eid1_detections, windows
t	rule.id	92032
#	rule.level	3
◐	rule.mail	false
t	rule.mitre.id	T1087 T1059.003
t	rule.mitre.tactic	Discovery, Execution
t	rule.mitre.technique	Account Discovery, Windows Command Shell
📅	timestamp	Oct 28, 2025 @ 15:13:20.034



t	data.win.eventdata.description	Windows Command Processor
t	data.win.eventdata.fileVersion	10.0.22000.1 (WinBuild.160101.0800)
t	data.win.eventdata.hashes	SHA256=F6C9532E1F4B66BE96F0F56BD7C3A3C1997EA8066B91BFCC984E41F072C347BA
t	data.win.eventdata.image	C:\\Windows\\System32\\cmd.exe
t	data.win.eventdata.integrityLevel	System
t	data.win.eventdata.logonGuid	{1f8fa574-7955-6900-e703-000000000000}
t	data.win.eventdata.logonId	0x3e7
t	data.win.eventdata.originalFileName	Cmd.Exe
t	data.win.eventdata.parentCommandLine	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.EXE\" -Command \"Start-Process -WindowStyle Hidden task.bat\"
t	data.win.eventdata.parentImage	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
t	data.win.eventdata.parentProcessGuid	{1f8fa574-dd87-6900-9d46-000000008001}

Defence evasion captured by wazuh using wazuh filter



```
data.win.system.eventID:4624
```

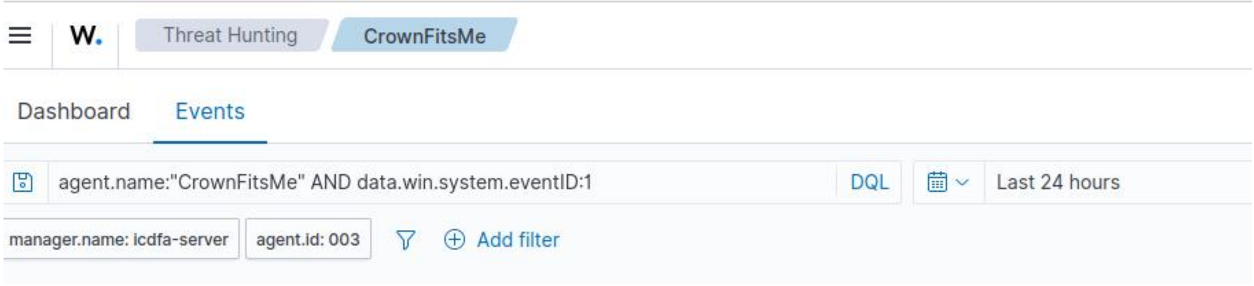
manager.name: icdfa-server | rule.mitre.id: exists | agent.id: 003

93 hits

Oct 27, 2025 @ 15:26:05.621 - Oct 28, 2025 @ 15:26:05.621

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.descri...	rule.level	rule.id
Oct 28, 2025 @ 15:22:01.571	CrownFitsMe	T1078	Defense Evasion, Persistence, Privileg...	Windows Log...	3	60106
Oct 28, 2025 @ 15:18:34.584	CrownFitsMe	T1078	Defense Evasion, Persistence, Privileg...	Windows Log...	3	60106
Oct 28, 2025 @ 15:10:07.754	CrownFitsMe	T1078	Defense Evasion, Persistence, Privileg...	Windows Log...	3	60106
Oct 28, 2025 @ 15:06:39.571	CrownFitsMe	T1078	Defense Evasion, Persistence, Privileg...	Windows Log...	3	60106

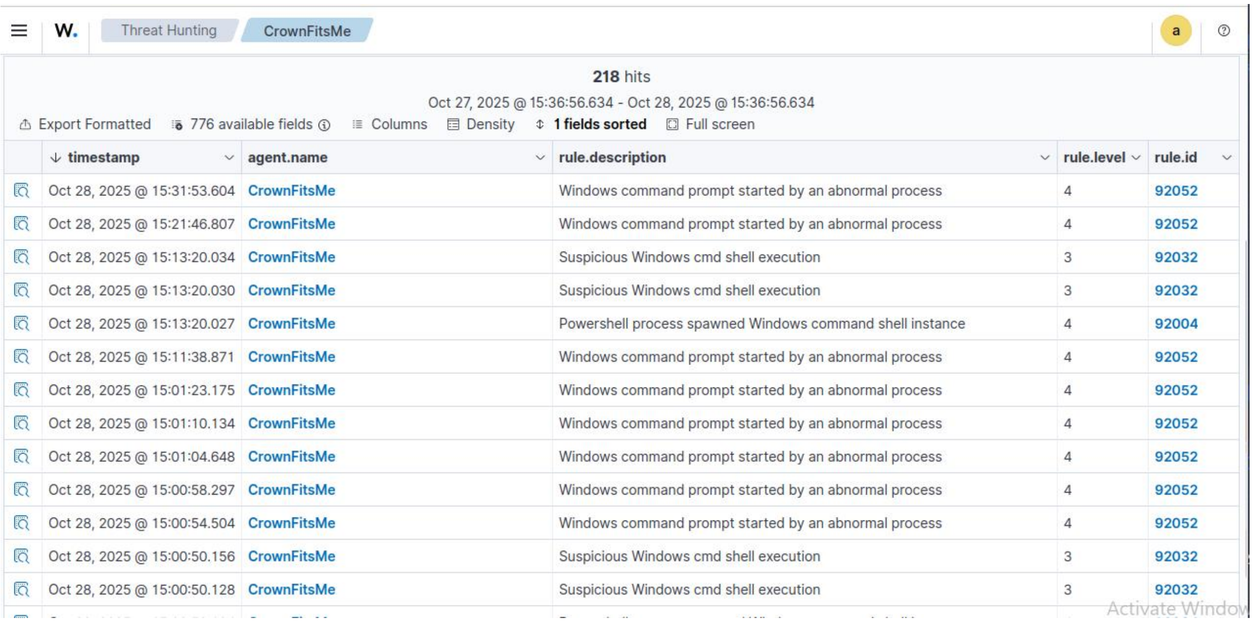
This wazuh filter was able to capture the following



```
agent.name:"CrownFitsMe" AND data.win.system.eventID:1
```

manager.name: icdfa-server | agent.id: 003

It catured 218 suspicious execution as seen below

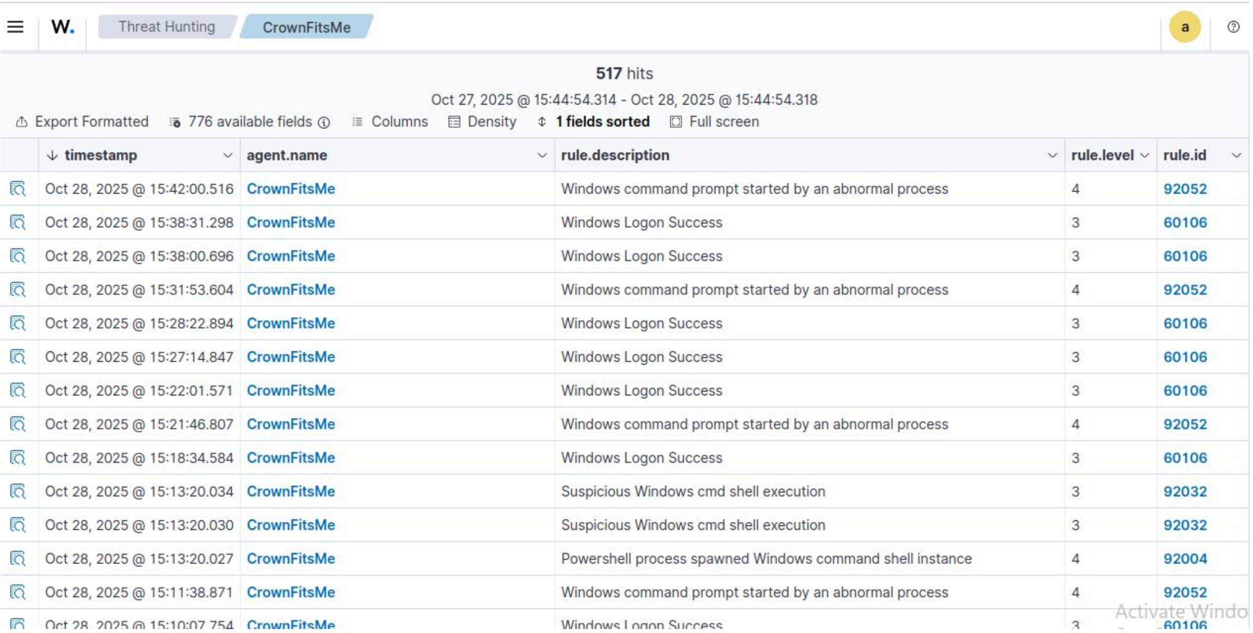


218 hits

Oct 27, 2025 @ 15:36:56.634 - Oct 28, 2025 @ 15:36:56.634

timestamp	agent.name	rule.description	rule.level	rule.id
Oct 28, 2025 @ 15:31:53.604	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:21:46.807	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:13:20.034	CrownFitsMe	Suspicious Windows cmd shell execution	3	92032
Oct 28, 2025 @ 15:13:20.030	CrownFitsMe	Suspicious Windows cmd shell execution	3	92032
Oct 28, 2025 @ 15:13:20.027	CrownFitsMe	Powershell process spawned Windows command shell instance	4	92004
Oct 28, 2025 @ 15:11:38.871	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:01:23.175	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:01:10.134	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:01:04.648	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:00:58.297	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:00:54.504	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:00:50.156	CrownFitsMe	Suspicious Windows cmd shell execution	3	92032
Oct 28, 2025 @ 15:00:50.128	CrownFitsMe	Suspicious Windows cmd shell execution	3	92032

Threat hunting events captured on wazuh



517 hits

Oct 27, 2025 @ 15:44:54.314 - Oct 28, 2025 @ 15:44:54.318

timestamp	agent.name	rule.description	rule.level	rule.id
Oct 28, 2025 @ 15:42:00.516	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:38:31.298	CrownFitsMe	Windows Logon Success	3	60106
Oct 28, 2025 @ 15:38:00.696	CrownFitsMe	Windows Logon Success	3	60106
Oct 28, 2025 @ 15:31:53.604	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:28:22.894	CrownFitsMe	Windows Logon Success	3	60106
Oct 28, 2025 @ 15:27:14.847	CrownFitsMe	Windows Logon Success	3	60106
Oct 28, 2025 @ 15:22:01.571	CrownFitsMe	Windows Logon Success	3	60106
Oct 28, 2025 @ 15:21:46.807	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:18:34.584	CrownFitsMe	Windows Logon Success	3	60106
Oct 28, 2025 @ 15:13:20.034	CrownFitsMe	Suspicious Windows cmd shell execution	3	92032
Oct 28, 2025 @ 15:13:20.030	CrownFitsMe	Suspicious Windows cmd shell execution	3	92032
Oct 28, 2025 @ 15:13:20.027	CrownFitsMe	Powershell process spawned Windows command shell instance	4	92004
Oct 28, 2025 @ 15:11:38.871	CrownFitsMe	Windows command prompt started by an abnormal process	4	92052
Oct 28, 2025 @ 15:10:07.754	CrownFitsMe	Windows Logon Success	3	60106