Description: This project aims to showcase how an attacker uses C2 commands to delete shadow files as part of a ransomware attack. It also covers how a SOC analyst can detect this attack and prevent it by writing a new rule. Additionally, in this project, the new rule will be tested to demonstrate its effectiveness and explain why an attacker would attempt to delete shadow files.

Software and tools I use: Vmware Workstation Pro, Windows 11(victim), Sliver Command (Offensive tool), LimaCharlie.

Project: First, I will start from the attacker's point of view by demonstrating how to delete shadow files from a victim's computer. To initiate the attack, I will use C2 commands to access the victim's terminal. I will not show the entire C2 command process because I have already covered it in the 'C2 Payloads Detection' project. I will begin by typing 'shell' into my Sliver C2 shell.

```
[server] sliver (BROAD_REPLICATION) > shell
? This action is bad OPSEC, are you an adult? Yes
[*] Wait approximately 10 seconds after exit, and press <enter> to continue
[*] Opening shell tunnel (EOF to exit) ...
[*] Started remote shell with pid 6692
PS C:\Windows\system32> ■
```

I will have access to the victim's Windows terminal. To delete shadow files, I will type 'vssadmin delete shadows /all'. When the attacker encrypts the victim's files, they delete all the shadow files so that the victim cannot recover their files. As a result, the victim has only one option, which is to pay the ransom.

```
PS C:\Windows\system32> vssadmin delete shadows /all vssadmin delete shadows /all vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool (C) Copyright 2001-2013 Microsoft Corp.

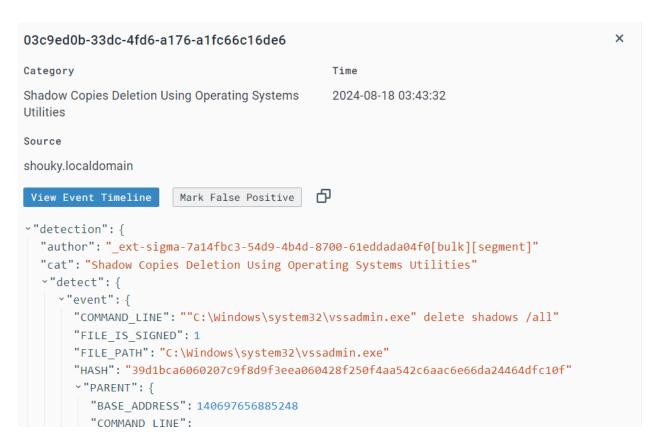
No items found that satisfy the query.
PS C:\Windows\system32>
```

I will go to LimaCharlie's detection tab to check for any signs of shadow file deletion.

```
You're up-to-date!

2024-08-18 03:43:32 Shadow Copies Deletion Using Operating Systems Utilities shouky.localdomain {"event":{"COMMAND_LINE":"\"C:\\Windows\\system32\\vssadmin.e}
2024-08-18 03:18:52 Non Interactive PowerShell Process Spawned shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248,"COMMAND_LINE":"C:\\Windows\\Syste
2024-08-18 03:18:52 HackTool - Sliver C2 Implant Activity Pattern shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248,"COMMAND_LINE":"C:\\Windows\\Syste
2024-08-18 03:10:17 LSASS access shouky.localdomain {"event":{"BASE_ADDRESS":140695338156032, "COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-08-18 02:54:38 LSASS access shouky.localdomain {"event":{"EventS":[{"event":{"BASE_ADDRESS":140695338156032, "COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-08-18 02:11:58 Non Interactive PowerShell Process Spawned shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248, "COMMAND_LINE":"C:\\Windows\\System32\\\lsass
2024-08-18 02:11:58 Non Interactive PowerShell Process Spawned shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248, "COMMAND_LINE":"C:\\Windows\\System32\\\lsass
2024-08-18 02:11:58 Non Interactive PowerShell Process Spawned shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248, "COMMAND_LINE":"C:\\Windows\\System32\\\lsass
2024-08-18 02:11:58 Non Interactive PowerShell Process Spawned shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248, "COMMAND_LINE":"C:\\Windows\\System32\\\lsass
```

I can see the 'shadow Copies Deletion' at the top. That SOC analyst will see when the attacker deleted shadow files. To stop that from happening anymore, I have to create a rule. I will click 'shadow Copies Deletion'.



I will click 'View Event Timeline' and then click 'Build D&R Rule'.

```
IE":"C:\\Windows\\syste*
                        Event Routing
                                                                                                          67 区
":"\"C:\\Program Files
COMMAND_LINE":"\"C:\\Us
                      ~"event": {
IE":"C:\\Windows\\syste
                         "COMMAND_LINE": ""C:\Windows\system32\vssadmin.exe" delete shadows /all"
NE":"C:\\Windows\\syst
                         "FILE_IS_SIGNED": 1
OMMAND_LINE":"\"C:\\Us
                        "FILE_PATH": "C:\Windows\system32\vssadmin.exe"
ap.fastly.net {"CNAME"
                         "HASH": "39d1bca6060207c9f8d9f3eea060428f250f4aa542c6aac6e66da24464dfc10f"
ft.com CNAME: cdp-f-t
                        ~"PARENT": {
 {"DNS_TYPE":1,"DOMAIN
                           "BASE ADDRESS": 140697656885248
o.tlu.dl.delivery.mp.mi
                           "COMMAND LINE":
system32\svchost.exe -
                           "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoExit -Command [Console]::Ou
IE":"C:\\Windows\\Syste
                           tputEncoding=[Text.UTF8Encoding]::UTF8"
                           "FILE_IS_SIGNED": 1
E":"C:\\Windows\\syste
_ADDRESS":"192.168.177
                           "FILE_PATH": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
                           "HASH": "c50057756cdb25d481cf2502abcef124f864c27618c5057468bfc6b82b2c4edd"
                           "MEMORY_USAGE": 65650688
OMMAND_LINE":"\"C:\\Us
                           "PARENT ATOM": "3007854989e024327045d1b466c15f7a"
                           "PARENT PROCESS ID": 2172
:":"\"C:\\Program Files
                           "PROCESS ID": 6692
IE":"C:\\Windows\\Syste
                           "THIS ATOM": "3f1bbf720a7841c0094f975966c1681d"
IE":"C:\\Windows\\syste
                           "THREADS": 16
                           "TIMESTAMP": 1723951132572
ssadmin.exe Command:
                           "USER_NAME": "shouky\comed"
c.exe Command: C:\Win
chost.exe Command: C:
                         "PARENT_PROCESS_ID": 6692
dfc10f Path: C:\Windc
                         "PROCESS_ID": 3852
dfc10f Path: C:\Windc }
```

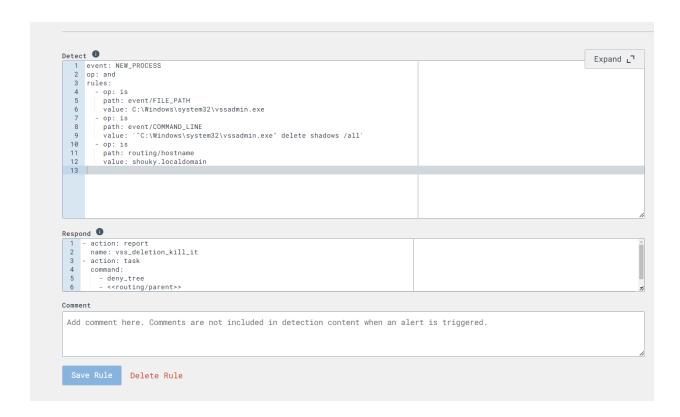
In the Respond section, I will type:

- action: report

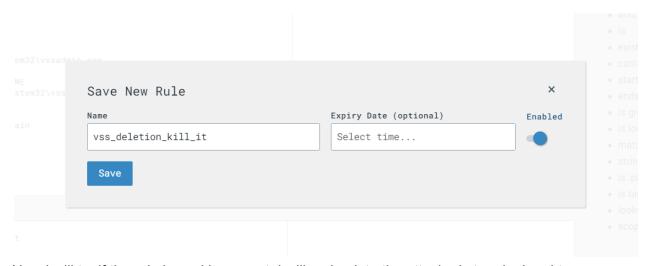
name: vss_deletion_kill_it

action: taskcommand:deny_tree

- <<routing/parent>>



The "action: report" section to send a detection report to the "Detections" tab. The "action: task" section to kill the parent process with the deny tree for 'vssadmin delete shadows /all' command. I will save the rule as 'vss_deletion_kill_it'.



Now I will try if the rule is working or not. I will go back to the attacker's terminal and type 'vssadmin delete shadows /all'.

```
PS C:\Windows\system32> vssadmin delete shadows /all vssadmin delete shadows /all vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool (C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.
PS C:\Windows\system32> vssadmin delete shadows /all vssadmin delete shadows /all vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool (C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.
PS C:\Windows\system32>
```

To fully test the rule's functionality, I will type 'whoami'.

```
PS C:\Windows\system32> whoami
Shell exited

[server] sliver (BROAD_REPLICATION) >
```

The system shell failed to return from the 'whoami' command because the parent process was terminated because of the rule I created. That is one of the rules for stopping the deletion of shadow files.