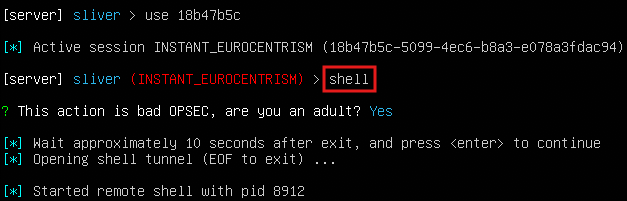
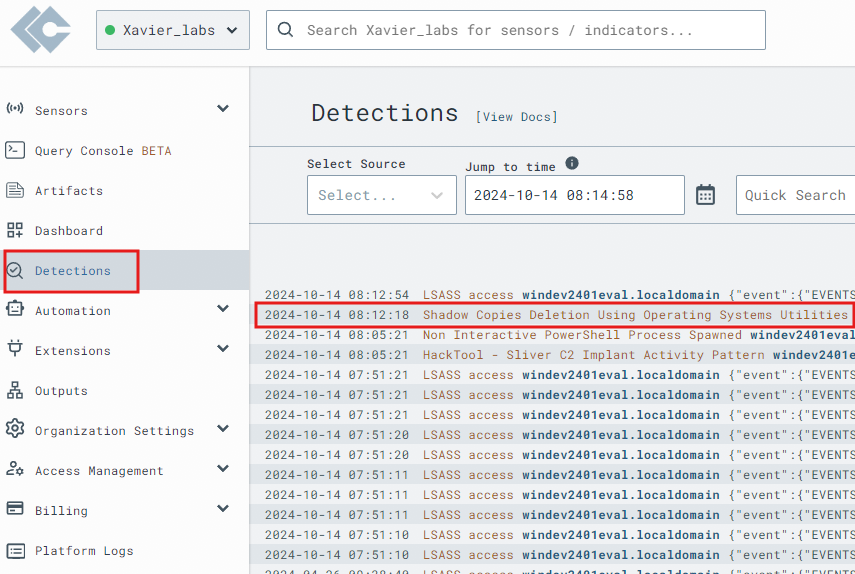
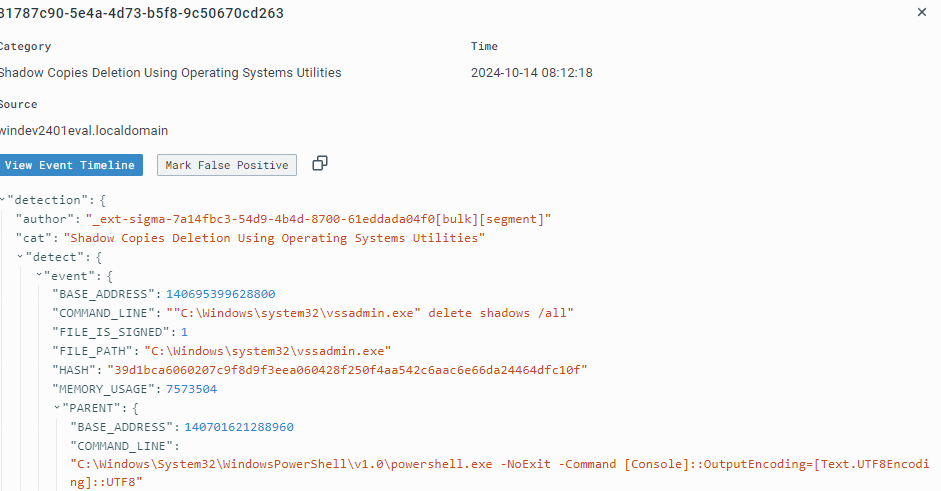
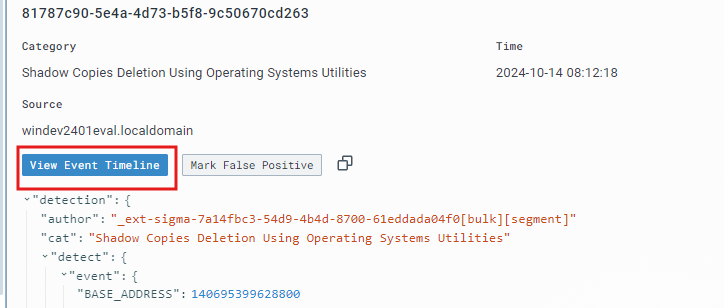
1. Follow The steps in part 2 to get here.
   1. If you have issues reestablishing your HTTP listener, reboot your ubuntu
2. In the ubuntu, type the command “Shell”
   1. When prompted with “are you an adult?” type y
   2. 
3. In the new system shell, type in this command “vssadmin delete shadows /all”
   1. Output is not important, as there may or may not be any telemetry. Just want to see if the signal pick up anything
4. Type in “whoami” to guarantee you still have an active directory
   1. 
5. You should get this when you sign in limacharlie under detections
   1. 
6. Click to expand the detection
   1. 
   2. Under references, it is full of references that can help you understand why that specific detection exist
      1. 
7. Click on event timelines after expanding detections
   1. 
8. After entering, click on this icon to start crafting a rule
   1. 
9. From the template, we can begin crafting our response action when this action is done again
   1. Type this in in the response section:

- action: report

name: vss\_deletion\_kill\_it

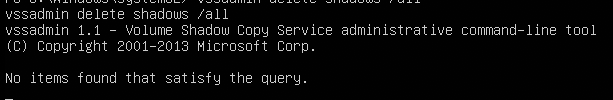
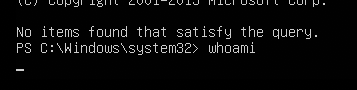
- action: task

command:

- deny\_tree

- <<routing/parent>>

* + 1. Action: report basically just send out a report under detection
    2. Action:task is what is responsible for denying attacks

1. Save the rule under “vss\_deletion\_kill\_it”
2. Now go back to linux and try “vssadmin delete shadows /all” again
3. This should be your output
   1. 
4. Now, to test if our D&R rule terminated our parent process. Type “whoami”. The result should be it hanging, you might need to take a bit for the process to work.
   1. 
      1. This is effective because in a real ransomware scenario,the parent process would likely be the ransomware payload or lateral movement tool
5. Terminate it with ctrl +D now on the nowdead system
6. Download and execute Florian’s [ransomware simulator](https://github.com/NextronSystems/ransomware-simulator) and see how it holds up against your new D&R rule.
   1. One tweak you’d certainly want to consider is using more intelligent ways of matching on the command line instead of matching on a literal string of “vssadmin delete shadows /all”. One weakness of the rule the way its written is that adding a simple space somewhere breaks our detection. You can try adding operator instead like below
      1. - op: is

path: event/FILE\_PATH

value: C:\Windows\system32\vssadmin.exe

- op: contains

path: event/COMMAND\_LINE

value: 'delete'

- op: contains

path: event/COMMAND\_LINE

value: 'shadows'

- op: contains

path: event/COMMAND\_LINE

* + 1. value: '/all'