Name:Ramya Ajay

Roll No:CBE.N.P2CYS22004 SIGMA

Task-2: What is Sigma?

- Sigma is an open-source generic signature language developed by Florian Roth & Thomas Patzke to describe log events in a structured format. This allows for quick sharing of detection methods by security analysts.

Sigma Use Cases

- To make detection methods and signatures shareable alongside IOCs and Yara rules.
- To write SIEM searches that avoid vendor lock-in.
- To share signatures with threat intelligence communities.
- To write custom detection rules for malicious behaviour based on specific conditions.

Sigma Development Process

- Sigma Rule Format: Generic structured log descriptions written in YAML.
- Sigma Converter: A set of python scripts that will process the rules on the backend and perform custom field matching based on specified SIEM query language.
- Machine Query: Resulting search query to filter out alerts during investigations. The query will be based on the specified SIEM.

Task-3: Sigma Rule Syntax

Sigma Syntax

```
title: WMI Event Subscription
```

- **Title** - Names the rule based on what it is supposed to detect. This should be short and clear.

- **ID** - A globally unique identifier mainly used by the developers of Sigma to maintain the order of identification for the rules submitted to the public repository, found in UUID format.

- **Status** - Describes the stage in which the rule maturity is at while in use. There are five declared statuses that you can use:

- Stable: The rule may be used in production environments and dashboards.

- Test: Trials are being done to the rule and could require fine-tuning.

- Experimental: The rule is very generic and is being tested. It could lead to false results, be noisy, and identify interesting events.
- Deprecated: The rule has been replaced and would no longer yield accurate results. Therelated field is used to create associations between the current rule and one that has been deprecated.
- Unsupported: The rule is not usable in its current state (unique correlation log, homemade fields).
- **Description:** Provides more context about the rule and its intended purpose. With the rule, you can be as verbose as possible on the malicious activity you intend to detect.

a) Which status level could lead to false results or be noisy, but could also identify interesting events?

- experimental

b) The rule detection comprises two main elements: __ and condition expressions.

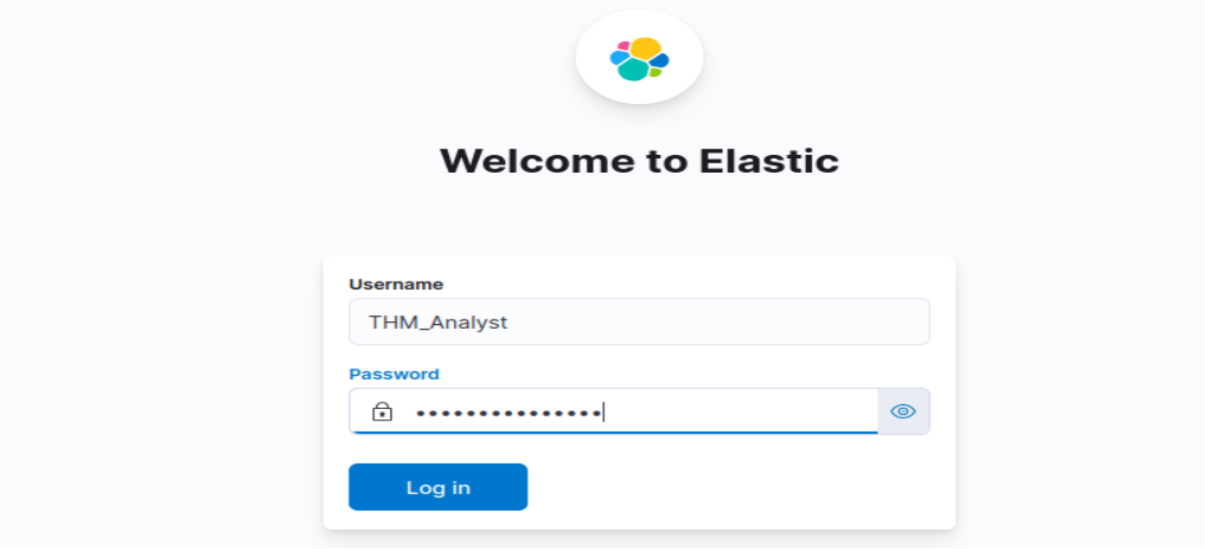
- search identifiers

c) What two data structures are used for the search identifiers?

- lists and maps

Task-4: Rule Writing & Conversion

- First we deploy the machine and go to the elastic server and log into the server with the given credentials



Welcome to Elastic

Username

THM_Analyst

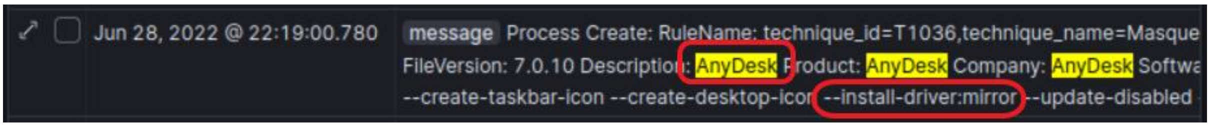
Password

•••••••••••••••

a) What command line tool is used to convert Sigma rules?

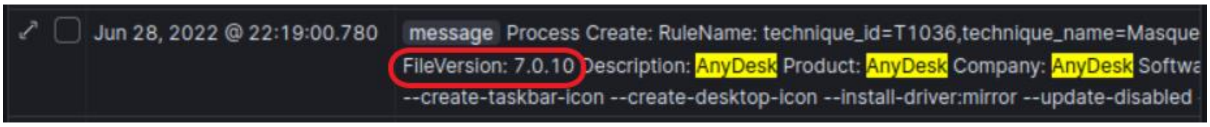
- sigmac

b) At what time was the AnyDesk installation event created? [MMM DD, YYYY @ HH:MM:SS]



```
Jun 28, 2022 @ 22:19:00.780   message Process Create: RuleName: technique_id=T1036,technique_name=Masque
                              FileVersion: 7.0.10 Description: AnyDesk Product: AnyDesk Company: AnyDesk Softwa
                              --create-taskbar-icon --create-desktop-icon --install-driver:mirror --update-disabled
```

c) What version of AnyDesk was installed?



```
Jun 28, 2022 @ 22:19:00.780   message Process Create: RuleName: technique_id=T1036,technique_name=Masque
                              FileVersion: 7.0.10 Description: AnyDesk Product: AnyDesk Company: AnyDesk Softwa
                              --create-taskbar-icon --create-desktop-icon --install-driver:mirror --update-disabled
```

Practical Scenario (Task 6)

Your organisation, Aurora, has recently been experiencing unusual activities on some of the machines on the network. Amongst these activities, the IT Manager noted that an unknown entity created some scheduled tasks on one of the machines and that a ransomware activity was also recorded.

The SOC Manager has approached you to find ways of identifying these activities from the logs collected on the environment. It would be best if you used Sigma rules to set your detection parameters and perform search queries through the Kibana dashboard.

To complete the task, you will require two Sigma rules processed into ElasticSearch to query for the scheduled task and the ransomware events. Below are tips to construct a good rule for the task:

- For the Scheduled Task, understand that it is a process creation event.
- The rule's detection variables should contain image and commandline arguments.
- You may choose to exclude SYSTEM accounts from the query.
- For the ransomware activity, you'll look for a created file ending with .txt.
- The file creation process would be run via cmd.exe.
- Change the default time window on Kibana from the default last 30 days to last 1 year (or ensure it encompasses 2022).

The query of above task will be:

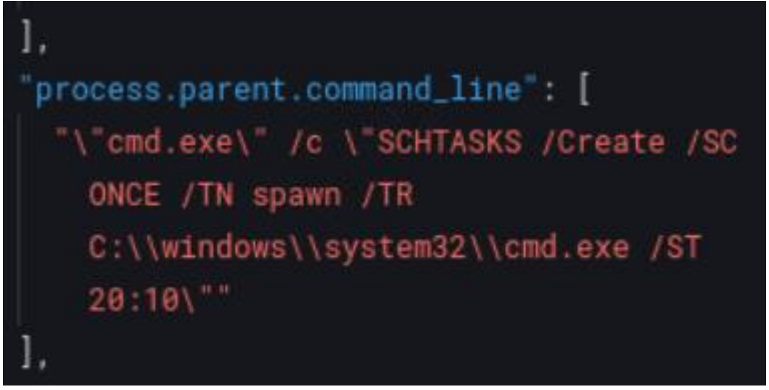
```
    (process.executable.text:"\schtasks.exe" AND process.command_line.text:
"*schtasks*" AND process.command_line.text: *Create*)
```

To detect the creation of the scheduled task, what detection value would be appropriate for the Sigma rule?

```
schtasks.exe
```

What was the name of the scheduled task created?

```
spawn
```

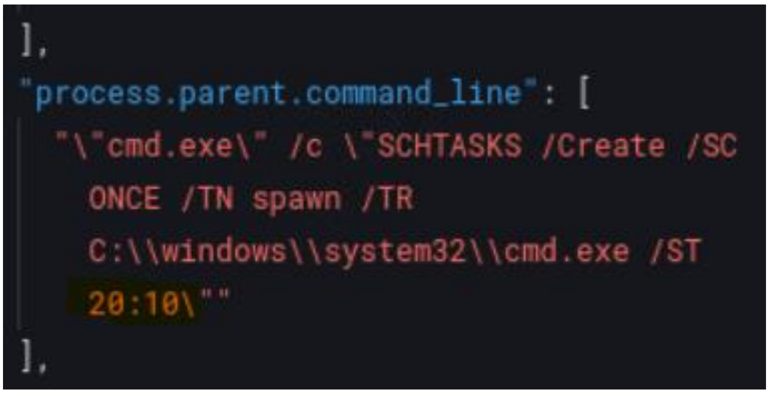


```
],
"process.parent.command_line": [
  "\"cmd.exe\" /c \"SCHTASKS /Create /SC
    ONCE /TN spawn /TR
    C:\\windows\\system32\\cmd.exe /ST
    20:10\""
],
```

In the above command, it will create task called spawn. Thus, the name of the scheduled task is `spawn`

What time is this task meant to run?

```
20:10
```



```
],
"process.parent.command_line": [
  "\"cmd.exe\" /c \"SCHTASKS /Create /SC
    ONCE /TN spawn /TR
    C:\\windows\\system32\\cmd.exe /ST
    20:10\""
],
```

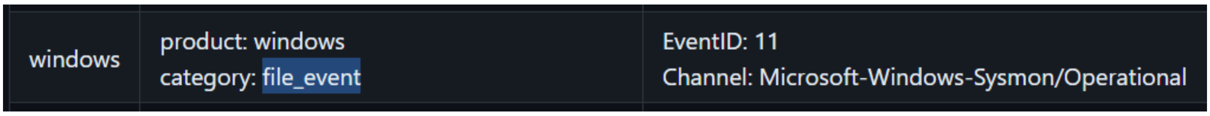
Time is also mentioned there when the task is created.

To detect ransomware activity, what logsource category would be appropriate for the Sigma rule?

```
file_event
```

- To detect this logsource category, we need to refer the Sigma taxonomy.
- https://github.com/SigmaHQ/sigma-specification/blob/main/Taxonomy_specification.md

- Look for Event_ID : 11



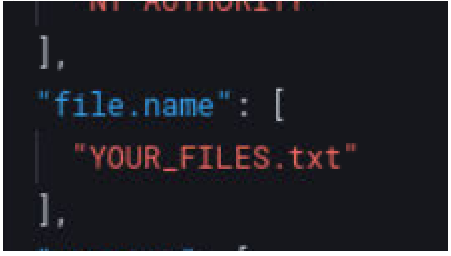
windows	product: windows category: file_event	EventID: 11 Channel: Microsoft-Windows-Sysmon/Operational

What is the name of the created file?

```
YOUR_FILES.TXT
```

Query :

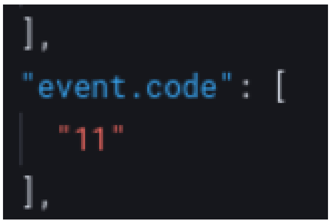
```
(process.executable.text:"\cmd.exe" AND file.path.text:*.txt)
```



```
  NT AUTHORITY
],
"file.name": [
  "YOUR_FILES.txt"
],
```

What was the event code associated with the activity?

```
11
```

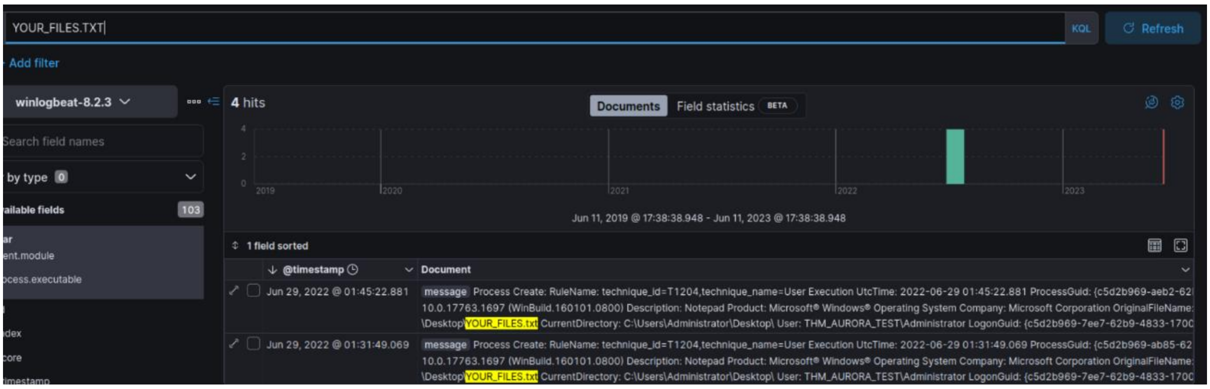


```
],
"event.code": [
  "11"
],
```

What were the contents of the created ransomware file?

```
echo T1486 - Purelocker Ransom Note
```

- We know already that created ransomware file is `YOUR_FILES.txt`
- Let's search that in kibana search

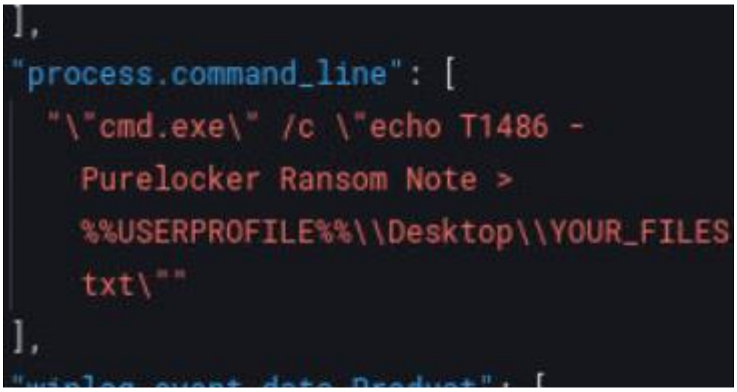


YOUR_FILES.TXT

Jun 11, 2019 @ 17:38:38.948 - Jun 11, 2023 @ 17:38:38.948

```
Jun 29, 2022 @ 01:45:22.881  message Process Create: RuleName: technique_id=T1204,technique_name=User Execution UtcTime: 2022-06-29 01:45:22.881 ProcessGuid: {c5d2b969-aeb2-62
                             10.0.17763.1697 (WinBuild.160101.0800) Description: Notepad Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName:
                             \Desktop\YOUR_FILES.txt CurrentDirectory: C:\Users\Administrator\Desktop\ User: THM_AURORA_TEST\Administrator LogonGuid: {c5d2b969-7ee7-62b9-4833-1700
Jun 29, 2022 @ 01:31:49.069  message Process Create: RuleName: technique_id=T1204,technique_name=User Execution UtcTime: 2022-06-29 01:31:49.069 ProcessGuid: {c5d2b969-ab85-62
                             10.0.17763.1697 (WinBuild.160101.0800) Description: Notepad Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName:
                             \Desktop\YOUR_FILES.txt CurrentDirectory: C:\Users\Administrator\Desktop\ User: THM_AURORA_TEST\Administrator LogonGuid: {c5d2b969-7ee7-62b9-4833-1700
```

- We got 4 hits.
- First file that entered is the one which consists of contents. Inspecting the last hit will display us the contents of the ransomware file.



```
],
"process.command_line": [
  "\"cmd.exe\" /c \"echo T1486 -
    Purelocker Ransom Note >
    %%USERPROFILE%%\\Desktop\\YOUR_FILES
    txt\""
],
"winlog.event_data.Product": [
```