

Labo Cloud – Azure Sentinel

Now, we will configure Azure Sentinel SIEM to detect threats on our infrastructure.

Activate Sentinel, create necessary data collection rules so that you can create a threat detection rule for one of the steps of your attack flow. Detection rule templates can be used as a basis for your own detection rule.

If you do this in the Azure console, provide GitHub links to console screenshots of the data collection and threat detection rules configuration. If you prefer using Terraform, provide links to the corresponding Terraform configuration.

- Configuration de l'importation des logs SYSLOG de la VM vers « Azure Sentinel »

The screenshot shows the 'Add data source' configuration page in the Azure Sentinel console. The 'Data source' tab is selected, and 'Linux Syslog' is chosen as the data source type. A table lists various facilities (LOG_ALERT, LOG_AUDIT, LOG_AUTH, LOG_AUTHPRIV, LOG_CLOCK, LOG_CRON, LOG_DAEMON, LOG_FTP, LOG_KERN, LOG_LOCAL0, LOG_LOCAL1) and their corresponding minimum log levels (all set to LOG_DEBUG). The 'Save' button is visible at the bottom.

- Création de la règle d'Incident dans « Azure Sentinel »

Analytics rule wizard - Create a new Scheduled rule ...

The screenshot shows the 'Create a new Scheduled rule' wizard in the Azure Sentinel console. The 'General' tab is selected, showing fields for Name, Description, Severity, Tactics and techniques, and Status. The 'Name' field is filled with 'SSH Connection Detection'. The 'Severity' is set to 'Medium'. The 'Tactics and techniques' dropdown shows '(2)'. The 'Status' is 'Enabled'. The 'Next: Set rule logic >' button is visible at the bottom.

- Requête utilisé pour analyser uniquement les connexions SSH infructueuses

Home > Microsoft Sentinel | Analytics >

Analytics rule wizard - Create a new

General **Set rule logic** Incident settings Automation

Define the logic for your new analytics rule.

Rule query
Any time details set here will be within the scope defined below.

```
Syslog
| where SyslogMessage contains "Connection closed by authenticating user"
| project TimeGenerated,
      SyslogMessage,
      User = extract("authenticating user (.*?)", 1, SyslogMessage),
      IPAddress = extract("[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+", 1, SyslogMessage)
```

View query results >

Alert enhancement

< Previous Next: Incident settings >

Logs
Labo3-Cloud

Run Time range: Custom

```
1 Syslog
2 | where SyslogMessage contains "Connection closed by authenticating user"
3 | project TimeGenerated,
4   SyslogMessage,
5   User = extract("authenticating user (.*?)", 1, SyslogMessage),
6   IPAddress = extract("[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+", 1, SyslogMessage)
```

Results Chart Add bookmark

TimeGenerated [UTC]	SyslogMessage	User	IPAddress
> 10/22/2023, 12:56:42.795 PM	Connection closed by authentic...	azureadmin	87.66.117.67
> 10/22/2023, 12:56:36.905 PM	Connection closed by authentic...	azureadmin	87.66.117.67
> 10/22/2023, 12:52:09.455 PM	Connection closed by authentic...	azureadmin	87.66.117.67

0s 733ms | Display time (UTC+00:00) ▾

- On exécute la règle toutes les 5 minutes

Query scheduling

Run query every *

5 Minutes

Lookup data from the last *

5 Minutes

Start running ⓘ

☒ Automatically

☐ At specific time (Preview)

10/23/2023 12:00 PM

Starting automatically, the rule will run every 5 minutes, looking up data from last 5 minutes.

- Et on vérifie si le nombre d'événement est plus grand de 5

Alert threshold

Generate alert when number of query results *

Is greater than 5

Event grouping

Configure how rule query results are grouped into alerts

- ☒ Group all events into a single alert
- ☐ Trigger an alert for each event

Suppression

Stop running query after alert is generated ⓘ

☐ Off

<input type="checkbox"/> Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last Modified ↓
<input type="checkbox"/> Medium	SSH Connection Detection	Scheduled	Enabled	Initial Access	T1078	Custom Content	22/10/2023, 15:...

Carry out one of the steps of the attack that you described in the attack flow. You can assume that the previous steps were successful.

Explain how you carry the attack and show that Sentinel detects the threat.

- Pour simuler l'attaque, il suffit d'effectuer plusieurs tentatives de connexion SSH infructueuse (7 dans notre exemple)

```
(kali㉿kali)-[~/Desktop]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali㉿kali)-[~/Desktop]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali㉿kali)-[~/Desktop]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali㉿kali)-[~/Desktop]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali㉿kali)-[~/Desktop]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali㉿kali)-[~/Desktop]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali㉿kali)-[~/Desktop]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).
```

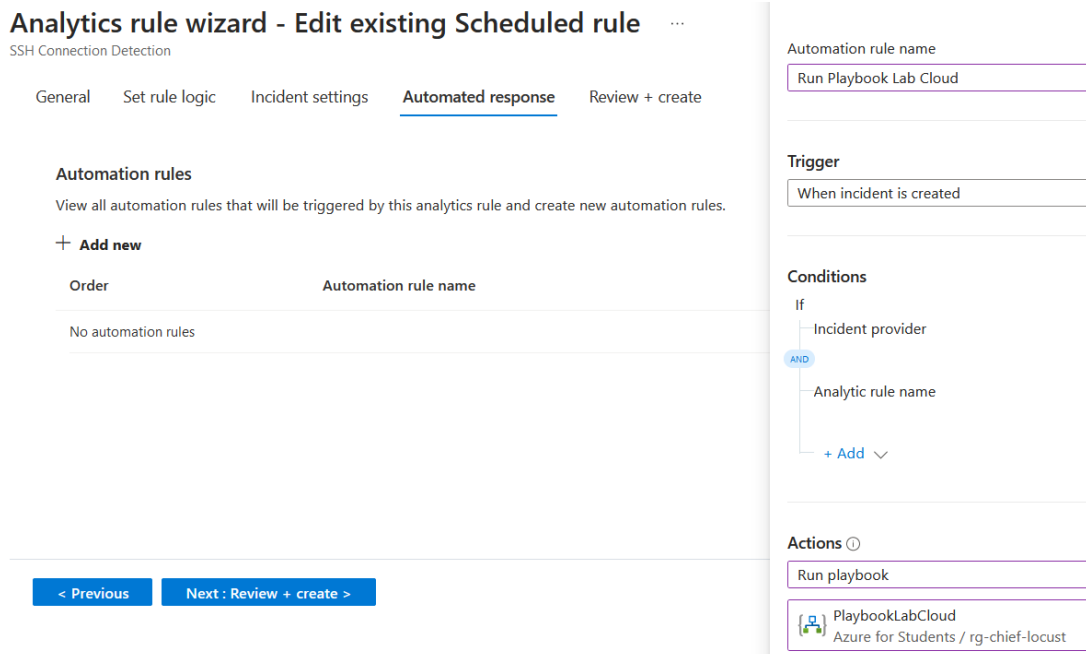
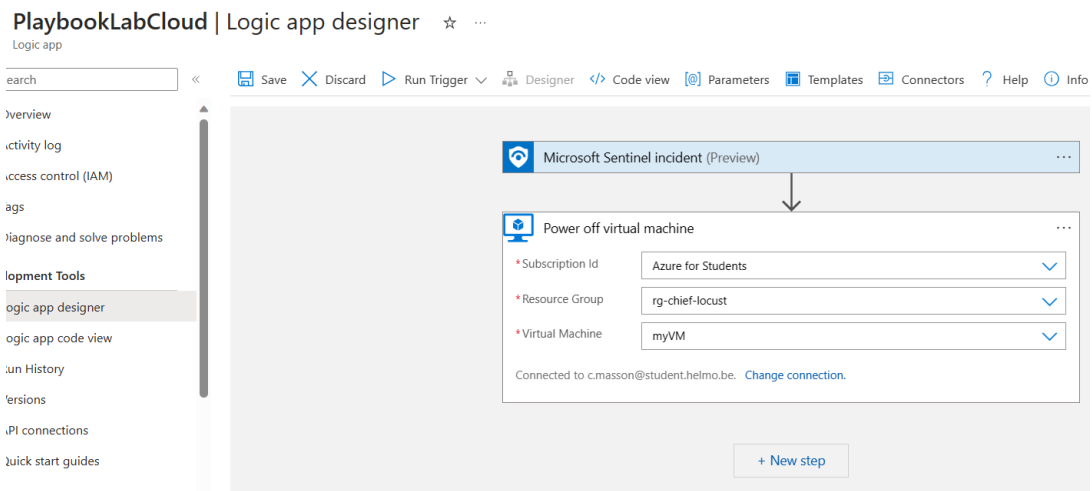
- Après quelques minutes on constate bien que Azure Sentinel a 1 « Incidents », concernant notre attaque, cet accident à 7 events car c'est le nombre de messages de log généré par Syslog pour les connexions infructueuses.

The screenshot shows the Microsoft Sentinel 'Incidents' page. The left sidebar contains navigation options like 'Overview (Preview)', 'Logs', 'Threat management', and 'Content management'. The main area displays incident statistics: 1 Open incident, 1 New incident, and 0 Active incidents. A bar chart shows 'Open incidents by severity' with 0 High, 1 Medium, 0 Low, and 0 Informational incidents. Below this, a table lists incidents. The first incident is 'SSH Connection Detection' (Incident ID: 1) with a severity of Medium and 1 alert. A detailed view of this incident is shown on the right, indicating 7 Events, 1 Alerts, and 0 Bookmarks. A note at the bottom states: 'The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the entity mapping option when defining your alerts. [Learn more >](#)'

Automate the response to the alert triggered in the previous step using Sentinel playbooks and automation rules. Explain why and how your remediation works, include links to screenshots hosted on GitHub that show the remediation configuration and execution. If you use scripts to perform the remediation (for example Azure client commands, Terraform config, ...), add those to your GitHub repository and include a link.

The remediation action depends on the threat detected, examples would be: shutdown/quarantine/destroy a virtual machine, enable DDoS/portknocking protection (fail2ban), etc.

- J'ai créé un Playbook, que j'ai relié à notre « Incident », dans la configuration j'ai fait en sorte que la machine virtuelle se stoppe quand l'Incident est détecté.



- En reproduisant l'attaque précédente, on constate qu'un nouveau « Incident » est créé et que la machine virtuelle se stoppe.

```
(kali@kali)-[~/Desktop/cloud-lab3]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali@kali)-[~/Desktop/cloud-lab3]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali@kali)-[~/Desktop/cloud-lab3]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali@kali)-[~/Desktop/cloud-lab3]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali@kali)-[~/Desktop/cloud-lab3]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali@kali)-[~/Desktop/cloud-lab3]
$ ssh azureadmin@172.191.30.163
azureadmin@172.191.30.163: Permission denied (publickey).

(kali@kali)-[~/Desktop/cloud-lab3]
$ ssh azureadmin@172.191.30.163
ssh: connect to host 172.191.30.163 port 22: Connection refused
```

2
Open incidents

2
New incidents

0
Active incidents

Open incidents by severity

High (0)

Medium (2)

Severity : All

Status : 2 selected

More (2)

☒ Auto-refresh incidents

<input type="checkbox"/> Severity ↑↓	Incident ID ↑↓	Title ↑↓	Alerts	Product names	Created time
<input type="checkbox"/> Medium	2	SSH Connection De...	1	Microsoft Sentinel	10/22/23, 03:
<input type="checkbox"/> Medium	1	SSH Connection De...	1	Microsoft Sentinel	10/22/23, 03:

Connect
 Start
 Restart
 Stop
 Capture
 Delete
 Refresh
 Open in mobile
 Feedback
 CLI / PS

Essentials

Resource group (move) : [rg-chief-locust](#)

Status : Stopped

Location : East US

Subscription (move) : [Azure for Students](#)

Subscription ID : 91dc98b1-a425-4df8-860a-444066b71f66

Operating system : Linux

Size : Standard DS1 v2 (1 vcpu, 3.5 GiB memc

Public IP address : [172.191.30.163](#)

Virtual network/subnet : [myVnet/mySubnet](#)

DNS name : [Not configured](#)

Health state : -