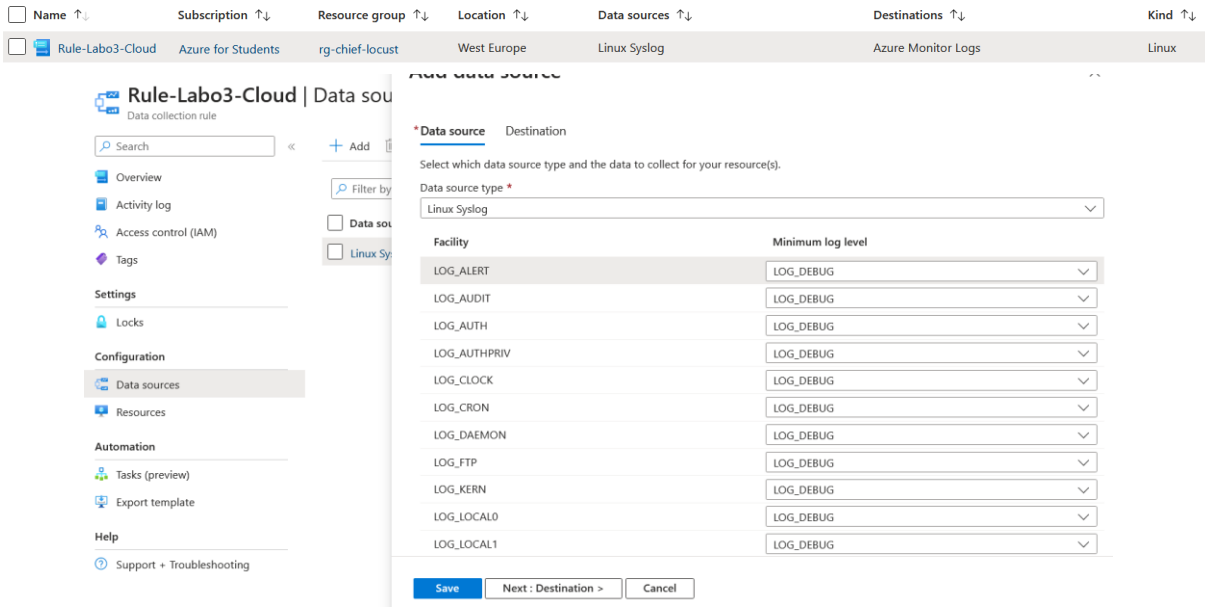
Labo Cloud – Azure Sentinel

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

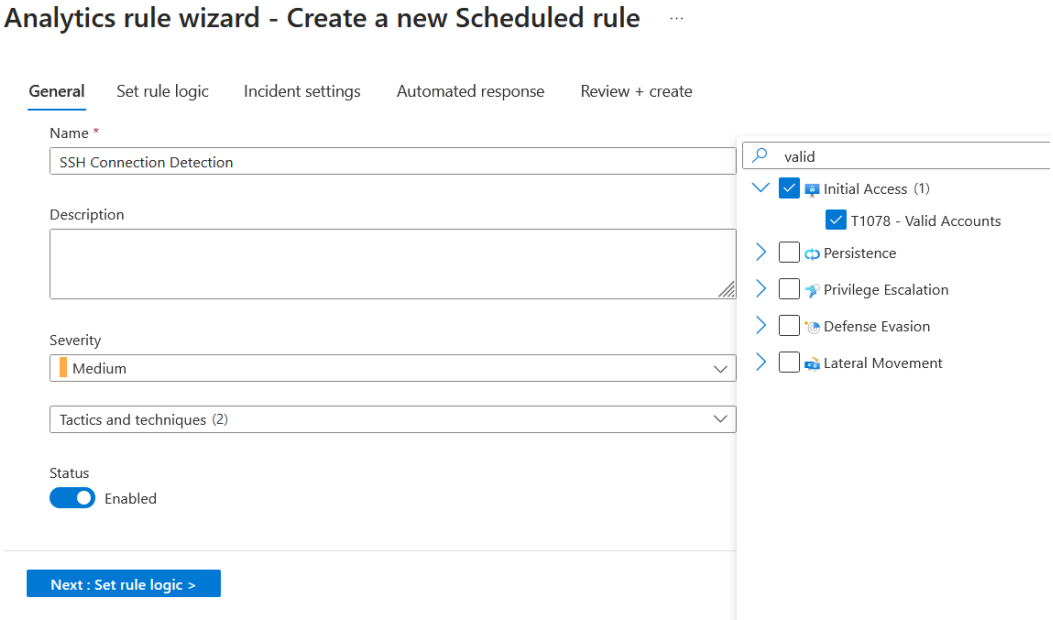
Activate Sentinel, create necessary data collection rules so that you can create a threat detection rule for one of the steps of your attack flow. Detection rule templates can be used as a basis for your own detection rule.

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.

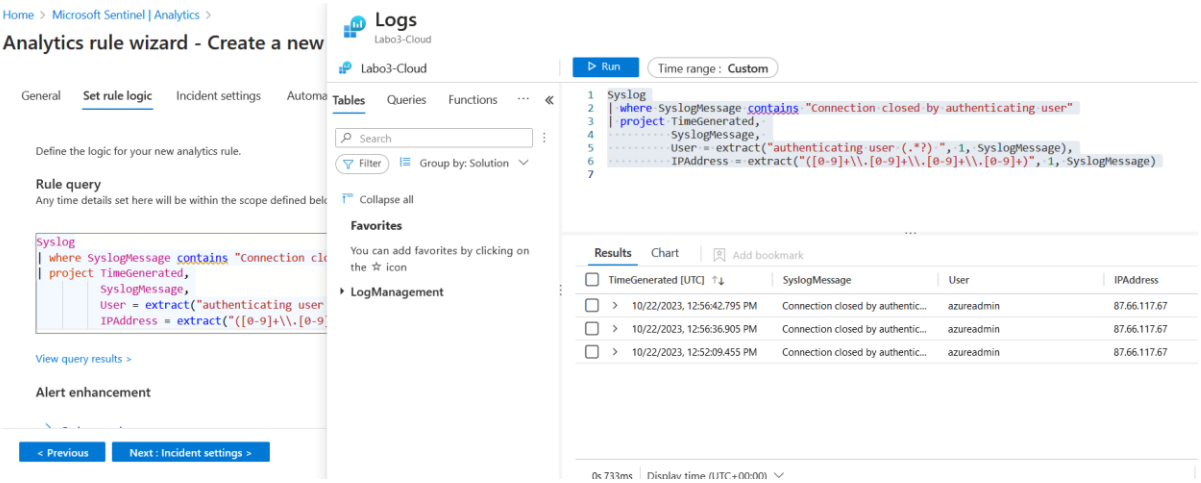
- Configuration de l'importation des logs SYSLOG de la VM vers « Azure Sentinel »



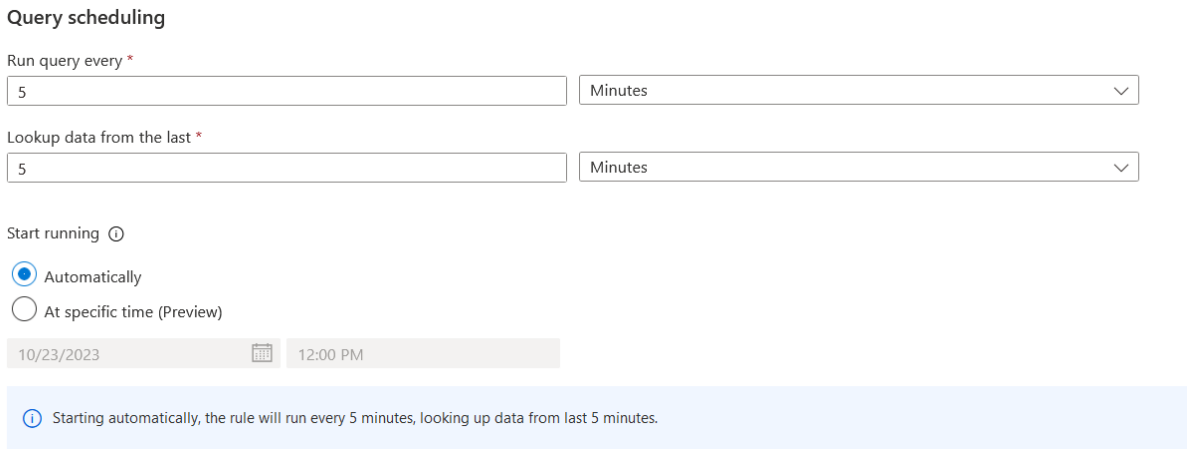
- Création de la règle d'Incident dans « Azure Sentinel »



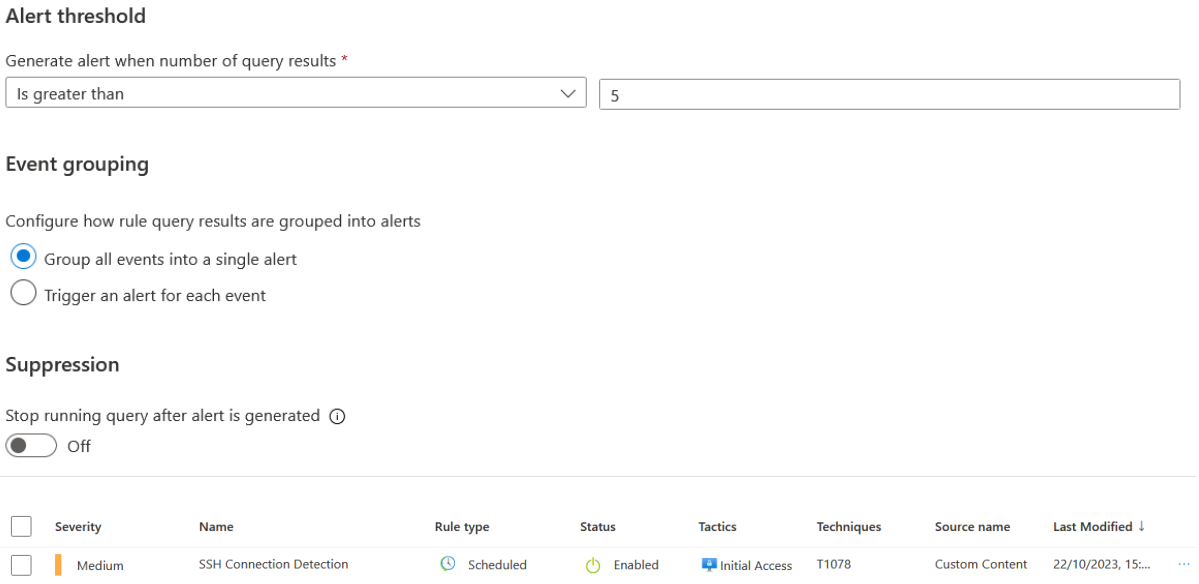
- Requête utilisé pour analyser uniquement les connexions SSH infructueuses



- On exécute la règle toutes les 5 minutes



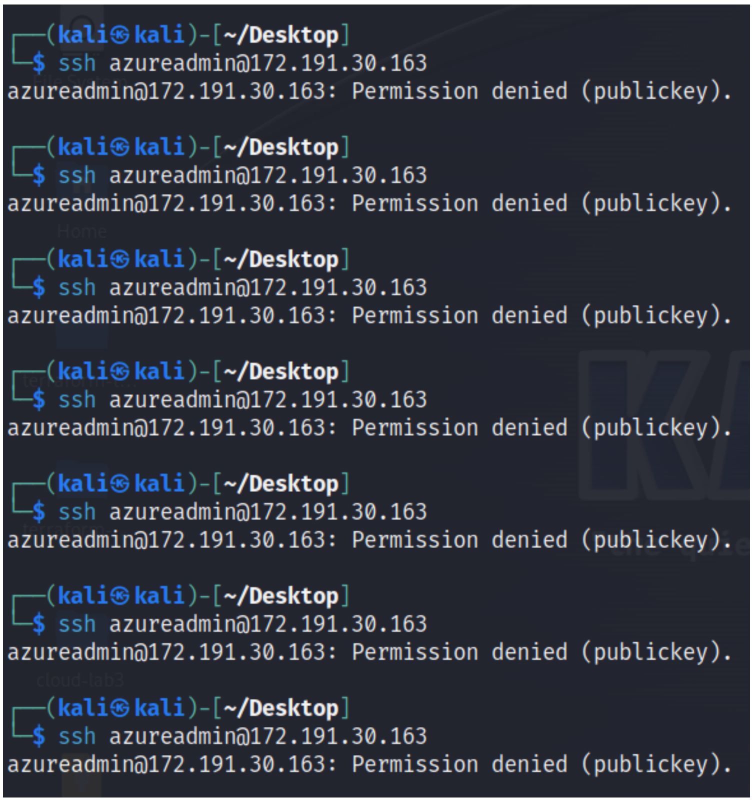
- Et on vérifie si le nombre d'évent est plus grand de 5



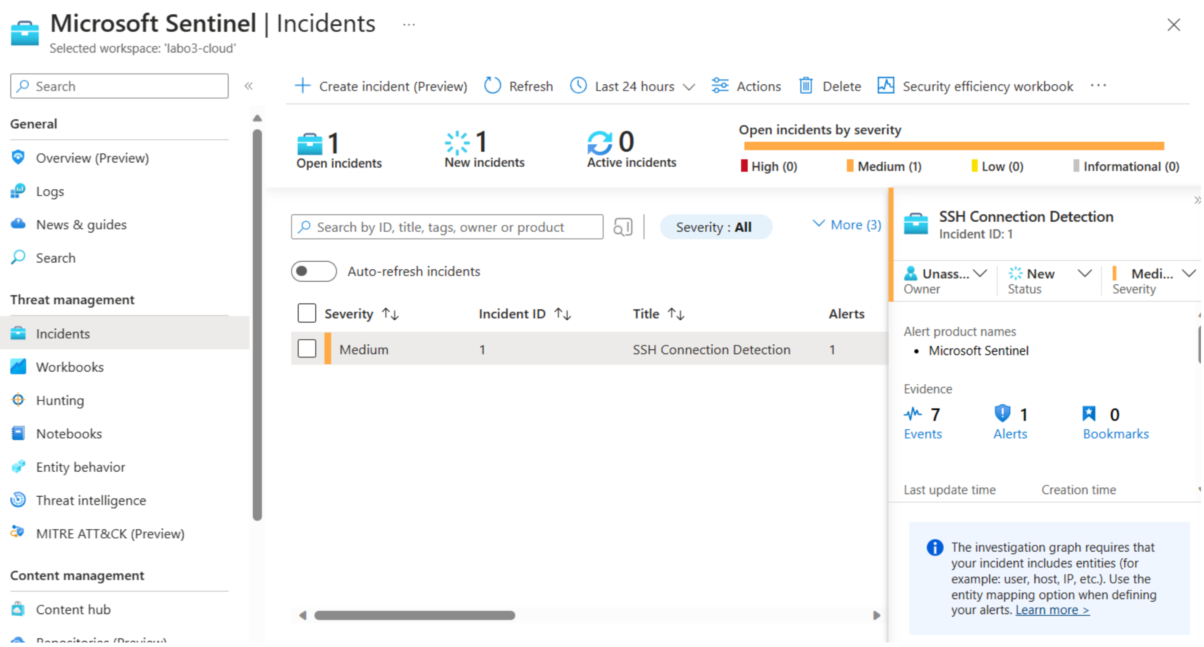
Carry out one of the steps of the attack that you described in the attack flow. You can assume that the previous steps were successful.

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)



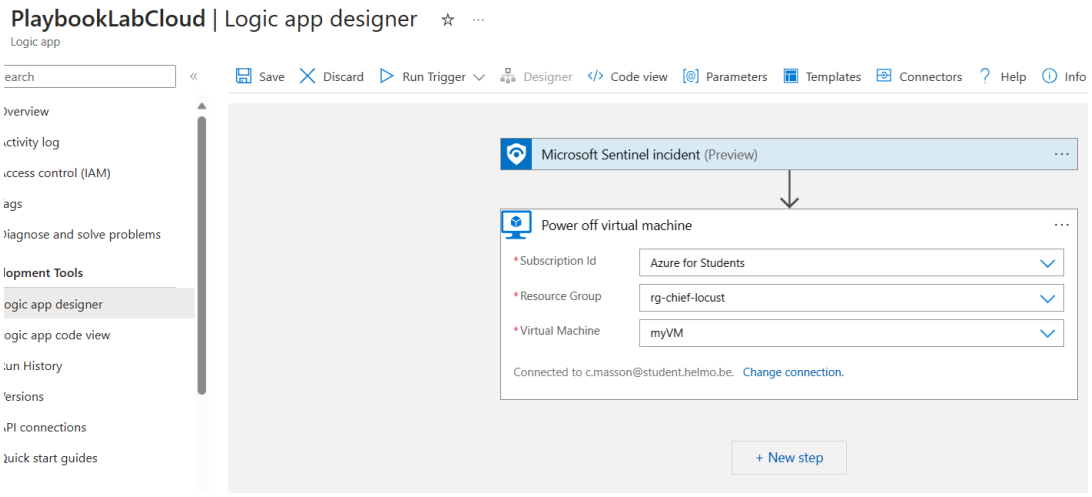
- Après quelques minutes on constate bien que Azure Sentinel a 1 « Incidents », concernant notre attaque, cet accident à 7 events car c'est le nombre de messages de log généré par Syslog pour les connexions infructueuses.

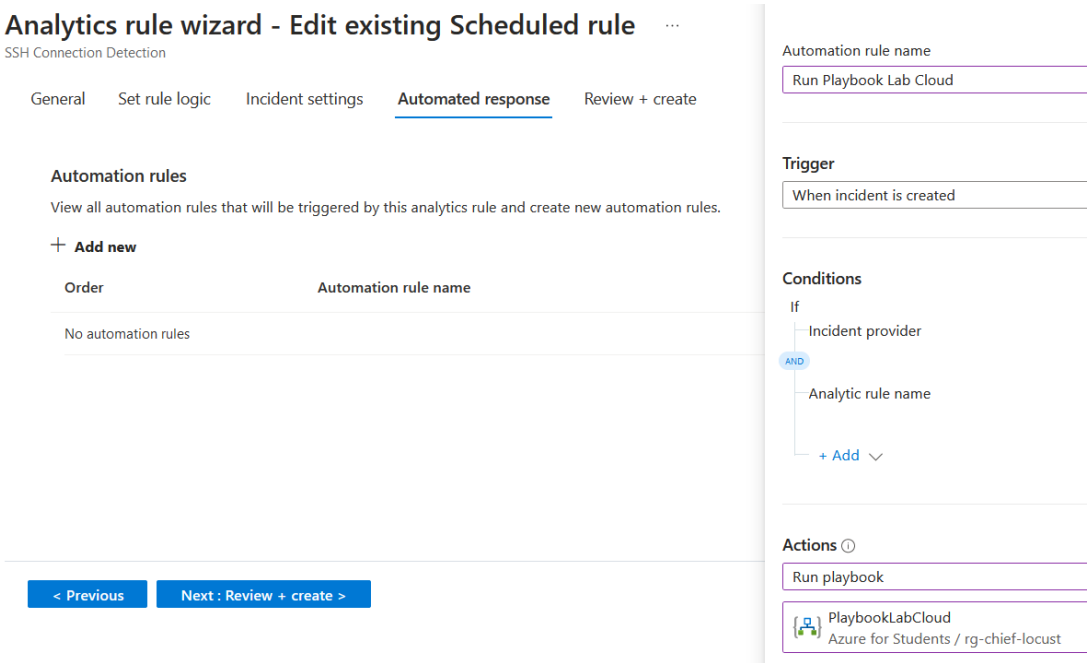


Automate the response to the alert triggered in the previous step using Sentinel playbooks and automation rules. Explain why and how your remediation works, include links to screenshots hosted on GitHub that show the remediation configuration and execution. If you use scripts to perform the remediation (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 crée et que la machine virtuelle se stoppe.