

# **CHAPITRE 3 :      *Implémentation d'un SIEM sur Azure***

Dans ce chapitre nous allons mettre en place une preuve de concept de détection et de réponse aux menaces basée sur Microsoft Sentinel.

Nous allons donc en premier lieu mettre en place l'environnement qui regroupe Microsoft Sentinel et deux outils pour la collecte de données à savoir Azure Monitor (Log Analytic) et Microsoft Defender for Cloud. Dans un deuxième temps nous allons invoquer un incident pour voir comment les solutions Microsoft collaborent entre elles pour détecter celles-ci.

## **3.1 Mise en place de l'environnement**

La mise en place du lab sera subdivisé en trois parties

### **3.1.1 Déploiement azure Monitor**

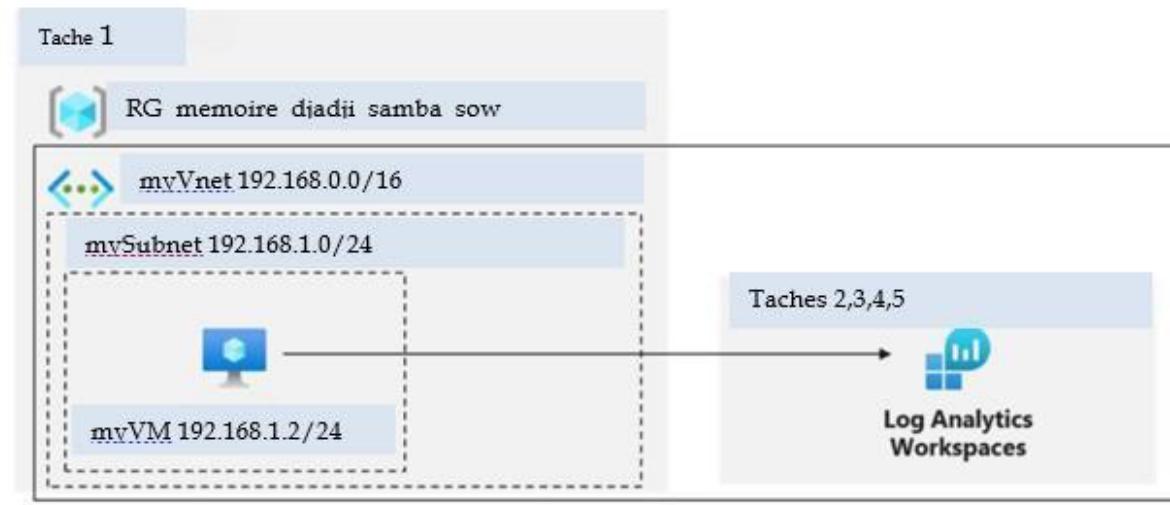


Figure 21: Déploiement Azure Monitor (Log Analytics Workspaces [18]

Avec Azure Monitor, nous allons créer une preuve de concept de surveillance des performances de la machine virtuelle. Pour cela nous devons atteindre les objectifs suivants :

- ✓ Configurer une machine virtuelle de sorte que la télémétrie et les journaux puissent être collectés.
- ✓ Afficher les données de télémétrie et les journaux qui peuvent être collectés.
- ✓ Montrer comment les données peuvent être utilisées et interrogées.

### **3.1.1.1 Tâche 1 : Déployer une machine virtuelle Azure**

Avant de pouvoir déployer des ressources sur Azure il faut un compte doté du rôle Propriétaire ou Contributeur dans l'abonnement Azure. Dans notre environnement nous avons utilisé un compte azuré pour étudiant.

- ❖ Pour déployer une machine virtuelle azure nous devons nous connecter au portail Azure <https://portal.azure.com/>. Comme illustré par la figure suivante

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

domoda402@outlook.fr  
DEFAULT DIRECTORY

## Services Azure

- Créer une ressource
- Microsoft Sentinel
- Abonnements
- Journal d'activité
- Microsoft Defender pour...  
Déployer un modèle...
- Gestion des coûts +...
- Machines virtuelles
- Espaces de travail Log...
- Autres services

## Ressources

Récent Favori

Nom	Type	Dernier affichage
Azure for Students	Abonnement	il y a 13 heures
Change-Incident-Severity	Application logique	il y a 14 heures
RG_memoire_djadji_samba_sow	Groupe de ressources	il y a 14 heures
myVM	Machine virtuelle	il y a 18 heures
monanalyseurdelog	Espace de travail Log Analytics	il y a 20 heures

Tout afficher

**Figure 22: Portail Azure**

Une fois sur cette interface nous avons plusieurs façons de créer une machine virtuelle : soit via une interface graphique, soit en utilisant Azure CLI (PowerShell).

- ❖ Nous ouvrons le Cloud Shell en cliquant sur la première icône en haut à droite du portail Azure. Une fenêtre va s'ouvrir nous invitant à sélectionner PowerShell et créer un stockage.
  - ❖ Dans la session PowerShell du volet Cloud Shell, nous exécutons la commande suivante pour créer un groupe de ressources qui va contenir notre ressource (machine virtuelle) portant le nom **RG\_memoire\_djadji\_samba\_sow** :

```
PowerShell | ⌂ ? ⌂ {} ⌂
PS /home/lil> New-AzResourceGroup -Name RG_memoire_djadji_samba_sow -Location 'EastUS'

ResourceGroupName : RG_memoire_djadji_samba_sow
Location         : eastus
ProvisioningState : Succeeded
Tags             :
ResourceId       : /subscriptions/fa6f13be-9623-4e6d-8525-dc32ee9e28c2/resourceGroups/RG_memoire_djadji_samba_sow

PS /home/lil> █
```

**Figure 23:** Cration d'un Groupe de ressource avec PowerShell

- ❖ Toujours dans le même Cloud Shell, exécutons ce qui suit pour créer une machine virtuelle Azure.

```
PowerShell v | ⚡ ? ⚡ 🔍 ⚡ {} 🔍
PS /home/lil> New-AzVm -ResourceGroupName "RG_memoire_djadji_samba_sow" -Name "myVM" -Location 'EastUS' -VirtualNetworkName "myVnet" -SubnetName "mySubnet" -SecurityGroupName "myNetworkSecurityGroup" -PublicIpAddressName "myPublicIpAddress" -PublicIpSku Standard -OpenPorts 80,3389 -Size Standard_DS1_v2

cmdlet New-AzVM at command pipeline position 1
Supply values for the following parameters:
Credential
User: djadji
Password for user djadji: *****

ResourceGroupName : RG_memoire_djadji_samba_sow
Id             : /subscriptions/fa6f13be-9623-4e6d-8525-dc32ee9e28c2/resourceGroups/RG_memoire_djadji_samba_sow/providers/Microsoft.Compute/virtualMachines/myVM
VmId          : 7efcd0a5-4a43-4d85-8a5e-81bb43b8ef37
Name           : myVM
Type           : Microsoft.Compute/virtualMachines
Location       : eastus
Tags           : {}
HardwareProfile: {VmSize}
NetworkProfile: {NetworkInterfaces}
OSProfile      : {ComputerName, AdminUsername, WindowsConfiguration, Secrets, AllowExtensionOperations, RequireGuestProvisionSignal}
ProvisioningState: Succeeded
StorageProfile : {ImageReference, OsDisk, DataDisks}
FullyQualifiedDomainName: myvm-ec2cc0.EastUS.cloudapp.azure.com
TimeCreated     : 1/8/2023 9:30:33 PM
```

**Figure 24:** Cration d'une machine virtuelle avec PowerShell

- ❖ Vérifions que la machine virtuelle nommée **myVM** a été créée et que son **ProvisioningState** est **Succeeded**.

```
PowerShell | ⌂ ? ⌂ {} ⌂
PS /home/lil> Get-AzVM -Name 'myVM' -ResourceGroupName 'RG_memoire_djadji_samba_sow' | Format-Table
ResourceGroupName          Name Location        VmSize OsType   NIC ProvisioningState
-----                   --      --           --       --      --      --      --
RG_memoire_djadji_samba_sow myVM  eastus  Standard_DS1_v2 Windows myVM      Succeeded
PS /home/lil> █
```

**Figure 25:** Vérification du provisionnement des ressources

### 3.1.1.2 Tâche 2 : Créer un espace de travail Log Analytics

Dans cette tâche, nous allons créer un espace de travail Log Analytics.

- ❖ Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, cherchons Espaces de travail Log Analytics.

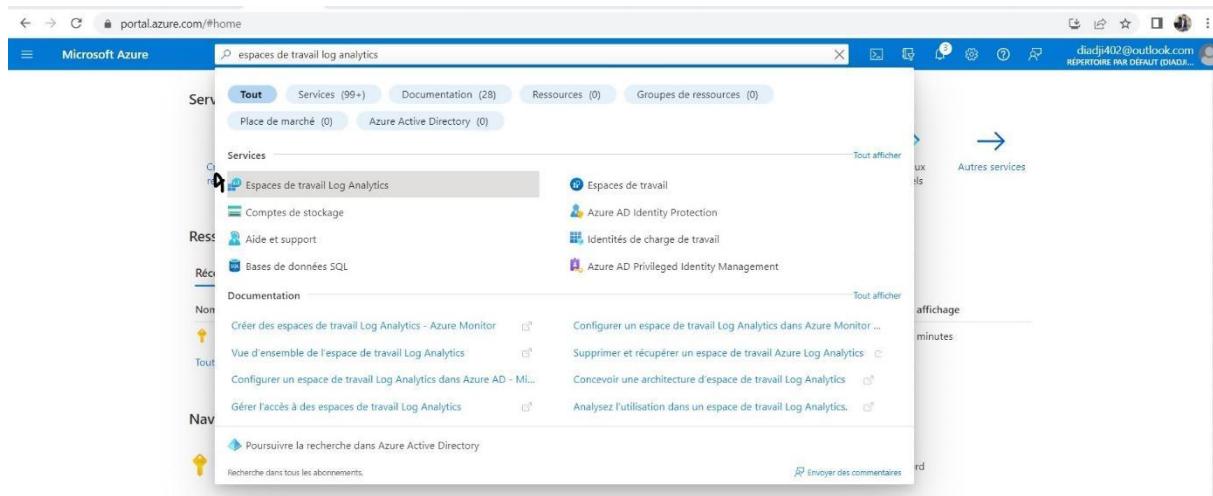


Figure 26: recherche de log Analytics sur le portail azure

- ❖ Dans le panneau Espaces de travail Log Analytics, cliquons sur le bouton + Créer.

Figure 27: création d'un espace de travail Log Analytics

- ❖ Nous spécifions les paramètres suivants : l'abonnement, le groupe de ressources, le nom de l'espace de travail ainsi que la région ou la ressource est déployer. Puis sur vérifier + créer

Figure 28: configuration des fonctions de base de log Analytics

Une fois la création effectuer nous devons activer l'extension de machine virtuelle Log Analytic

### 3.1.1.3 Tâche 3 : Activer l'extension de machine virtuelle Log Analytics

Dans cette tâche, nous allons activer l'extension de machine virtuelle Log Analytics. Cette extension installe l'agent Log Analytics sur les machines virtuelles Windows et Linux. Cet agent collecte les données de la machine virtuelle et les transfère vers l'espace de travail Log Analytics que nous désignons. Une fois l'agent installé, il sera automatiquement mis à niveau, ce qui nous permettra de toujours disposer des dernières fonctionnalités et correctifs.

- ❖ Dans le panneau Espace de travail Log Analytics, dans la page Vue d'ensemble, dans la section Connecter une source de données, on choisit l'entrée Machines virtuelles Azure puis on sélectionne la machine **myVM** que nous avons déployée dans la première tâche et notons qu'elle est répertoriée ici comme **Non connectée**. Il faudra veiller à ce que la machine soit en cours d'exécution pour que l'agent soit correctement installé.g

The screenshot shows the Azure Log Analytics workspace interface. On the left, there's a sidebar with 'Sources de données de l'espace de travail' (Data sources of the workspace) containing 'Machines virtuelles' (selected), 'Journaux de comptes de stockage', and 'System Center'. The main area has a search bar and an 'Actualiser' (Update) button. A filter bar at the top includes 'Filtrer par nom...' (Filter by name...), '8 sélectionné' (8 selected), '2 sélectio...', 'Azure for Students', 'rg\_memoire\_djadj... (selected)', 'East US', and 'Emplacement' (Location). Below these filters is a table with columns: Nom (Name), Connexion Log Analyti..., Système d'exploitati..., Abonnement, Groupe de ressources, and Emplacement. The 'myVM' row is highlighted with a blue border and shows the status as 'Non connecté' (Not connected), operating system as 'Windows', and resource group as 'RG\_memoire\_djadj...'. The table also lists other rows with similar columns.

Figure 29: Activer l'extension de machine virtuelle Log Analytics

- ❖ Maintenant reste plus qu'à connecter la machine en cliquant sur **se connecter**

Accueil > Espaces de travail Log Analytics > monanalyseurdelog | Machines virtuelles >

The screenshot shows the details for the 'myVM' machine. At the top, it says 'myVM ... Machine virtuelle'. Below that are three buttons: 'Se connecter' (selected and circled in blue), 'Déconnecter', and 'Actualiser'. A 'Connexion...' button is also present. The 'État' (State) section shows 'Connexion en cours' (Connection in progress). The 'Nom de l'espace de travail' (Workspace name) is listed as 'monanalyseurdelog'. In the 'Message' section, it says 'Connexion de la machine virtuelle à Log Analytics. Vérifiez ultérieurement l'évolution de l'état.' (Connection of the virtual machine to Log Analytics. Check the state evolution later.)

Figure 30: connecter la machine virtuelle à log Analytics

- ❖ Attendons que la machine virtuelle se connecte à l'espace de travail Log Analytics. Autrement dit jusqu'à ce que l'état affiché dans le panneau myVM passe de **Connexion à cet espace de travail** comme illustré ci-dessous.

Figure 31: vérification de l'état de la connexion du VM à Log Analytics

### 3.1.1.4 Tâche 4 : Collecter des données d'événement et de performances de machine virtuelle

Dans cette tâche, nous allons configurer la collection du journal système Windows et plusieurs compteurs de performance courants. Nous examinerons également d'autres sources disponibles.

- ❖ Toujours dans l'espace de travail Log Analytics, dans la section Paramètres, nous cliquons sur Gestion des agents hérités. Dans le panneau Configuration des agents, passons en revue les paramètres configurables, notamment les journaux des événements Windows, les compteurs de performance Windows, les compteurs de performance Linux, les journaux IIS et Syslog. Sur l'option Journaux des événements Windows, nous cliquons sur + Ajouter le journal des événements Windows, dans la liste des types de journaux des événements, nous sélectionnons Système. Il faudra aussi décocher la case Informations en laissant les cases à cocher Erreur et Avertissement activées. C'est ainsi qu'on ajoute des journaux d'événements à l'espace de travail. D'autres choix incluent, par exemple, les événements matériels ou le service de gestion de clés.

Figure 32: configuration d'un collecteur d'événement Windows liées aux systèmes

- ❖ Sur l'option Compteurs de performance Windows, nous cliquons sur + Ajouter un compteur de performance, et nous ajoutons les compteurs suivants avec un intervalle d'échantillonnage de collecte de 60 secondes :
  - ✓ Mémoire (\*)\Mo de mémoire disponible
  - ✓ Processus (\*)\% Temps processeur
  - ✓ Suivi des événements pour Windows\Utilisation totale de la mémoire --- pool non paginé
  - ✓ Suivi des événements pour Windows\Utilisation totale de la mémoire --- pool paginé

The screenshot shows the 'monanalyseurdelog | Gestion des anciens agents' page in the Azure Log Analytics workspace. On the left, a sidebar lists various navigation options like 'Paramètres', 'Verrou', 'Gestion des agents', 'Gestion des anciens agents', and 'Tables'. The main area is titled 'Compteurs de performances Windows' and displays a table of configured performance counters:

Nom du compteur de performances	Taux d'échantillonnage
Event Tracing for Windows(*),Total Memory Usage --- No...	60
Event Tracing for Windows(*),Total Memory Usage --- Pag...	60
Memory(*)\Available Memory Mbytes	60
Process(*)\% Processor Time	60

A yellow warning box at the top right states: 'Les agents Log Analytics ne seront pas pris en charge à compter du 31 août 2024. Prévoyez de migrer vers l'agent Azure Monitor avant cette date. Si vous avez déjà installé l'agent Azure Monitor, veillez à créer et associer [règles de collecte de données](#) aux agents.'

Figure 33: configuration de quelques compteurs de performances Windows

### 3.1.1.5 Tâche 5 : Afficher et interroger les données collectées

Dans cette tâche, nous allons effectuer une recherche dans les journaux de notre collecte de données.

- ❖ Dans l'espace de travail Log Analytics, dans la section Général, cliquons sur Journaux. Si nécessaire, dans le volet Requêtes, dans la colonne Toutes les requêtes, nous choisissons parmi les requêtes prédéfinies pour afficher les données concernant Utilisation de la mémoire et du processeur.

The screenshot shows the 'monanalyseurdelog | Journaux' page in the Azure Log Analytics workspace. The left sidebar includes 'Général', 'Journaux', and 'Solutions'. The main area displays a list of pre-defined query requests under the 'Requêtes' tab:

- VIRTUAL MACHINES**
  - What data is being collected? (Exécuter)
  - Virtual Machine available memory (Exécuter)
  - Chart CPU usage trends (Exécuter)
  - Virtual Machine free disk space (Exécuter)

Figure 34: requêtes pour l'interrogation des données

La requête s'ouvrira automatiquement dans un nouvel onglet de requête montrant le résultat obtenu. A noter que Log Analytics utilise le langage de requête Kusto. Nous pouvons personnaliser les requêtes existantes ou créer les nôtres. Nous avons également la possibilité d'afficher les données dans

différents formats et créer une règle d'alerte basée sur les résultats de la requête. Étant donné que cette machine virtuelle vient d'être créée, il y a peu de données qui s'affichent sur le graphique.

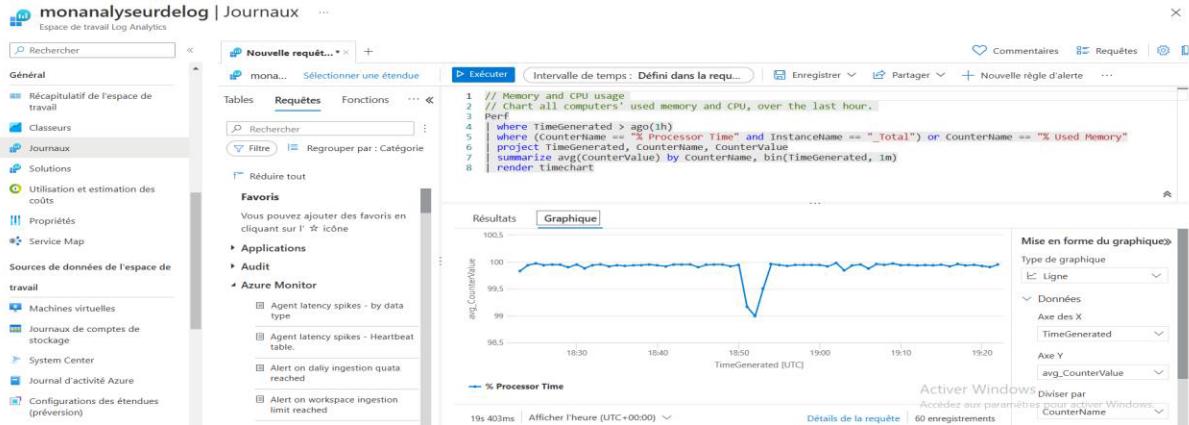


Figure 35: Résultat des requêtes sur le CPU et la Mémoire

Ce qui termine la mise en place d'Azure Monitor.

### 3.1.2 Déploiement de Microsoft defender pour le cloud

Toujours dans l'optique de mettre en place une infrastructure sécurisée, cet outil nous permet de créer une preuve de concept de Microsoft Defender pour environnement basé sur le cloud. Pour cela, nous souhaitons :

- ✓ Configurer Microsoft Defender pour Cloud pour surveiller une machine virtuelle.
- ✓ Consulter les recommandations de Microsoft Defender for Cloud pour la machine virtuelle.
- ✓ Implémenter des recommandations pour la configuration des invités et l'accès juste à temps aux machines virtuelles.

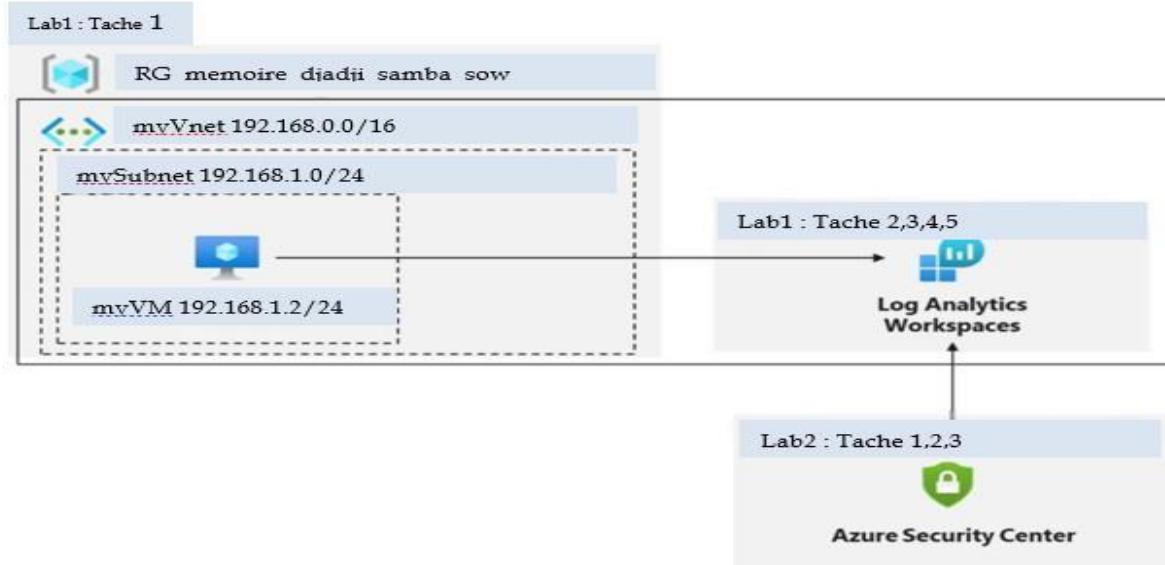


Figure 36: Déploiement de Microsoft Defender pour le Cloud [19]

### 3.1.2.1 Tâche 1 : Configurer Microsoft Defender pour le Cloud

Dans cette tâche, nous allons intégrer et configurer Microsoft Defender pour Cloud.

- ❖ Dans le portail Azure, dans la zone de texte Rechercher des ressources, nous cherchons Microsoft Defender for Cloud

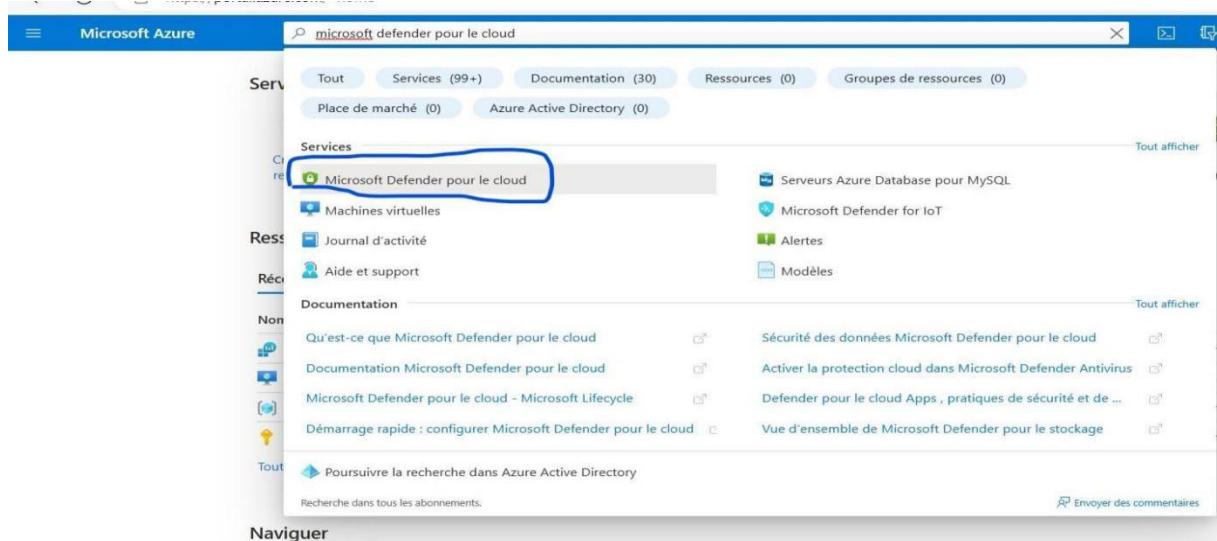


Figure 37: recherche de Microsoft Defender sur le portail azure

- ❖ Sur Microsoft Defender pour Cloud, dans le panneau Mise en route, il faudra Mettre à niveau puis Installer les agents.

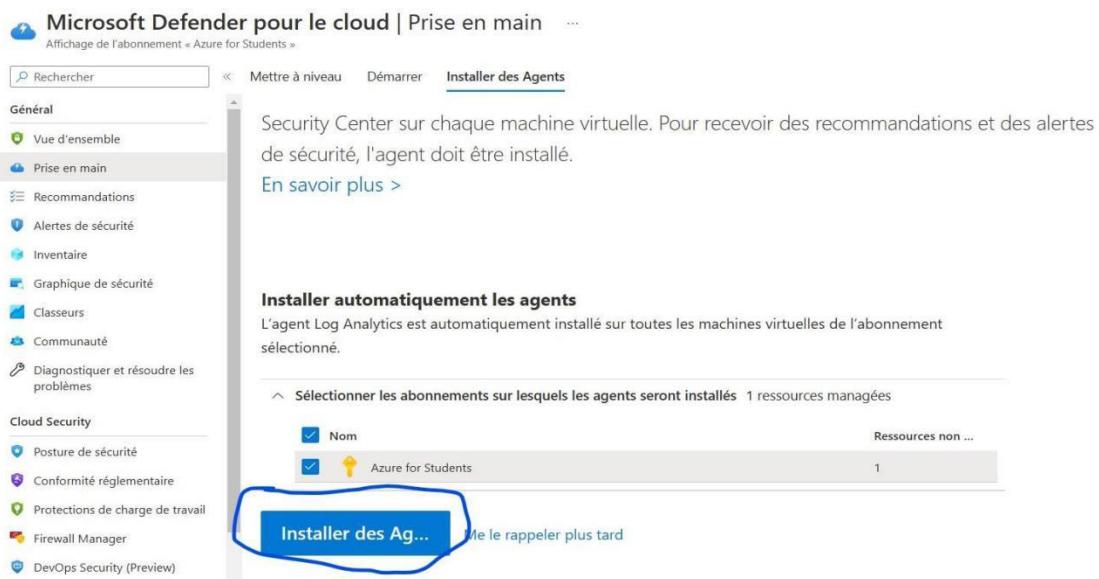


Figure 38: Mise à jour et installation de l'agent

- ❖ Puis Sur Microsoft Defender pour Cloud, dans Paramètres d'environnement, nous choisissons l'abonnement approprié.

Figure 39: choix de l'abonnement approprier

- ❖ Une autre fenêtre apparaît nous incitant à Activer tous les plans Microsoft Defender pour Cloud, comme vous pouvez le voir ci-dessous.

Microsoft Defender pour	Plan / Tarification	Quantité de ressources	Configuration	Statut
Defender CSPM	Free (preview) Details >	N/A	Full Modifier la configuration	<span style="color: green;">Activé</span> Désactivé
Serveurs	Plan 2 (15 \$/Serveur/mois) Changer de plan >	1 serveurs	Partial Modifier la configuration	<span style="color: green;">Activé</span> Désactivé
App Service	15 \$/Instance/mois Details >	0 instances	Full Modifier la configuration	<span style="color: green;">Activé</span> Désactivé
Bases de données	Sélectionné : 4/4 Sélectionner des types > Protégé : instances 0/0		Full Modifier la configuration	<span style="color: green;">Activé</span> Désactivé
Stockage	0.02 \$/10 000 transactions Details >	1 comptes de stockage	Full Modifier la configuration	<span style="color: green;">Activé</span> Désactivé
Conteneurs	7 \$/Mémoire à tores magnétiques de n Details > 0 registres de conteneurs; 0 coeurs kubi		Full Modifier la configuration	<span style="color: green;">Activé</span> Désactivé

Figure 40: Activation des plans Microsoft defender

- ❖ Dans les paramètres, Approvisionnement automatique, il faudra s'assurer que l'approvisionnement automatique est défini sur Activé pour le premier élément Agent Log Analytics pour les machines virtuelles Azure.

Component	Description	Defender plans	Configuration	État
Agent Log Analytics pour les machines virtuelles Azure/Agent Azure Monitor pour les machines virtuelles Azur (préversion)	Collecte les configurations et journaux d'événements liés à la sécurité à partir de l'ordinateur et stocke les données dans votre espace de travail Log Analytics pour analyse. <a href="#">En savoir plus</a>		-	Activé
Évaluation des vulnérabilités pour les machines	Active l'évaluation des vulnérabilités sur vos machines Azure et hybrides. <a href="#">En savoir plus</a>		-	Désactivé
Agent Configuration Invité (préversion)	Vérifie que les machines exécutées dans Azure et les machines connectées Arc présentent pas d'erreurs de sécurité. Des paramètres tels que la configuration du système d'exploitation, les configurations d'applications et les paramètres d'environnement sont tous validés. Pour en savoir plus, consultez <a href="#">Comprendre Configuration Invité d'Azure Policy</a> .		-	Désactivé
Agentless scanning for machines (preview)	Scans your machines for installed software and vulnerabilities without relying on agents or impacting machine performance. <a href="#">Learn more</a>		Modifier la configuration	Activé

Figure 41: vérifier si l'approvisionnement est active sur log Analytics

- ❖ Revenons à Microsoft Defender pour Cloud, dans Paramètres d'environnement, sur l'entrée représentant l'espace de travail Log Analytics nous Sélectionnons Collecte de données dans Microsoft Defender pour Cloud, sur Panneau Paramètres. On choisit Tous les événements puis on enregistre.

Stocker des données brutes supplémentaires - Événements de sécurité Windows

Pour vous aider à auditer, étudier et analyser les menaces, vous pouvez collecter des événements bruts, des journaux et des données de sécurité supplémentaires et les enregistrer dans votre espace de travail Log Analytics.

Sélectionnez le niveau de données à stocker pour cet espace de travail. Les frais s'appliquent à tous les paramètres autres que « Aucun ».

**Tous les événements**  
Tous les événements de sécurité Windows et AppLocker.

**Commun**  
Ensemble standard d'événements à des fins d'audit.

**Minimal**  
Petit ensemble d'événements susceptibles d'indiquer des menaces potentielles. En activant cette option, vous ne pourrez pas obtenir une trace d'audit complète.

**Aucun**  
Aucun événement de sécurité ou AppLocker.

Figure 42: Collecte de données de tous les événements

### 3.1.2.2 Tâche 2 : Examiner la recommandation Microsoft Defender for Cloud

Dans cette tâche, nous allons passer en revue les recommandations de Microsoft Defender for Cloud.

- ❖ Dans Microsoft Defender pour Cloud, Vue d'ensemble, Ressources évaluées, dans le panneau Inventaire, sélectionnons l'entrée **myVM** correspondant à notre machine virtuelle.

The screenshot shows the Microsoft Azure portal's inventory page for a virtual machine named 'myVM'. The left sidebar is collapsed, and the main area shows a summary of resources: 6 total resources, 4 non-compliant resources, 0 unmonitored resources, and 0 unregistered subscriptions. Below this is a detailed list of resources, including 'myVM' which is highlighted with a blue circle. The list includes columns for Name, Type, Subscription, Status, and Recommendation status. At the bottom right, there is a link to 'Activer Windows'.

Figure 43: inventaire de la machine virtuelle myVM

- ❖ Dans le panneau Intégrité des ressources, sous l'onglet Recommandations, passons en revue la liste des recommandations pour myVM. On s'aperçoit qu'il y a pas mal de recommandations qui sont remontées par exemple l'accès aux machines virtuelles Just in time.

The screenshot shows the 'Resource Health' blade for the virtual machine 'myVM'. The 'Recommendations' tab is active, showing a list of 10 recommendations. The columns are Gravité (Severity), Description, and État (Status). Most recommendations are marked as 'Saines' (Safe) or 'Non saines' (Not safe). The descriptions include Endpoint Protection, migration to new Azure Resource Manager resources, configuration for regular system updates, and enabling Guest Configuration extension and Windows Defender Exploit Guard. At the bottom right, there is a link to 'Activer Windows'.

Figure 44: Les recommandations liées à la machine virtuelle myVM

### 3.1.2.3 Tâche 3 : Implémenter la recommandation Microsoft Defender for Cloud pour activer l'accès aux machines virtuelles Just in time

Dans cette tâche, nous allons implémenter la recommandation Microsoft Defender for Cloud pour activer l'accès juste à temps aux machines virtuelles sur la machine virtuelle.

- ❖ Dans le portail Azure, revenons à Microsoft Defender pour Cloud, dans le panneau Protection contre la charge de travail, dans la section Protection avancée, nous cliquons sur la vignette Accès juste à temps aux machines virtuelles et, dans le panneau Accès juste à temps aux machines virtuelles, nous cliquons sur Essayer d'accéder juste à temps aux machines virtuelles. Il peut arriver que les machines virtuelles ne soient pas répertoriées, dans ce cas il faut accéder au panneau Machine virtuelle et cliquer sur Configuration, puis sur l'option Activer les machines virtuelles juste-à-temps sous l'accès de la machine virtuelle juste-à-temps. Répéter ainsi l'étape ci-dessus pour revenir à Microsoft Defender for Cloud et actualiser la page, la machine virtuelle apparaîtra.

The screenshot shows the Microsoft Defender for Cloud interface in the Azure portal. The main navigation bar includes tabs for Microsoft Defender, myVM - Microsoft AI, Accès aux machines virtuelles, A2500-AzureSecurity, Comment utiliser l'accès JIT, azure defender jit, and How to configure JIT. The current view is 'Prise en main > Microsoft Defender pour le cloud'. The left sidebar has sections for Général (General), Cloud Security (Posture de sécurité, Conformité réglementaire, Protections de charge de travail), and Administration. The main content area displays 'Alertes de sécurité' (Security alerts) with a chart showing 0 high severity, 0 medium severity, and 0 low severity alerts. Below this is the 'Protection avancée' (Advanced Protection) section, which includes 'Accès JIT à la machine virtuelle' (1 Non protégé), 'Contrôle d'application adaptatif' (Aucun Non protégé), 'Analyse de l'image de conteneur' (Aucun Non protégé), 'Renforcement réseau adaptatif' (Aucun Non protégé), 'Protection des vulnérabilités SQL' (AUCUN Non protégé), 'Arc-enabled SQL Servers' (Aucun Non protégé), 'Monitoring de l'intégrité du fichier' (Aucun Non protégé), 'Carte réseau' (Aucun Non protégé), and 'Sécurité IoT' (Activé Windows). The bottom status bar shows the date (09/01/2023), time (23:08), and weather (23°C Temps dégagé).

Figure 45: Implémenter JIT sur myVM

- ❖ Sur l'accès à la machine virtuelle juste à temps, sélectionnons **Non configuré**, puis cliquons sur l'entrée myVM. Il faudra peut-être attendre quelques minutes avant que l'entrée myVM ne soit disponible. Et puis nous Sélectionnons Activer JIT sur une machine virtuelle.

The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#view/Microsoft\\_Azure\\_Security\\_R3/JITNetworkAccessBlade](https://portal.azure.com/#view/Microsoft_Azure_Security_R3/JITNetworkAccessBlade). The page title is "Accès JIT à la machine virtuelle". It includes sections for "Qu'est-ce que l'accès JIT à la machine virtuelle?", "Machines virtuelles", and a table listing a single VM named "myVM". The table has columns for Machine virtuelle, Groupe de ressources, Nom de l'abonnement, Gravité, Motif, and a status message. A blue button at the bottom right of the table row for "myVM" is circled in red.

Figure 46: Activation de l'accès JIT sur myVM

- ❖ Dans le panneau Configuration de l'accès à la machine virtuelle JIT, à l'extrême droite de la ligne faisant référence au port 22, nous cliquons sur le bouton de sélection puis sur Supprimer.

The screenshot shows the "Configuration de l'accès JIT à la MV" page for the VM "myVM". It lists four ports: 22, 3389, 5985, and 5986. Each entry includes a "Supprimer" (Delete) button at the end of the row. The "Supprimer" button for port 22 is circled in red.

Port	Protocole	Adresses IP sources autorisées	Plage d'adresses IP	Plage de temps (heures)	
22 (Recommandé)	Tous	Par demande	N/A	3 hours	<span style="color: red; border: 1px solid red; border-radius: 50%; padding: 2px;">Supprimer</span>
3389 (Recommandé)	Tous	Par demande	N/A	3 hours	...
5985 (Recommandé)	Tous	Par demande	N/A	3 hours	...
5986 (Recommandé)	Tous	Par demande	N/A	3 hours	...

Figure 47: configuration de l'accès JIT sur myVM

- ❖ Pour finir on enregistre la configuration de l'accès à la machine virtuelle JIT. Nous avons aussi la possibilité de configurer l'accès sur les autres ports dépendamment de nos besoins en sécurité d'accès.

Accès JIT à la machine virtuelle > myVM - Microsoft Azure > Accès aux machines virtuelles > AZ500-AzureSecurityTechno > Comment utiliser l'accès à ... > How to configure JIT in azure > +

Microsoft Azure | Rechercher dans les ressources, services et documents (G+) | domoda402@outlook.fr | DEFAULT DIRECTORY (DOMODA...)

Accès JIT à la machine virtuelle > ...

La semaine dernière

Qu'est-ce que l'accès JIT à la machine virtuelle ?

Comment cela fonctionne-t-il ?

Sur demande d'un utilisateur, Defender pour le cloud décide d'accorder ou non l'accès sur la base d'Azure RBAC. Si une demande est approuvée, Defender pour le cloud configure automatiquement les NSG de manière à autoriser le trafic entrant vers ces ports, pendant la durée demandée. Ensuite, il restaure les NSG à leur état précédent.

En savoir plus sur l'utilisation de l'accès JIT à la machine virtuelle >

Machines virtuelles

Configuré Non configuré Non pris en charge

Machines virtuelles pour lesquelles le contrôle d'accès JIT est déjà en place. Les données présentées datent de la semaine dernière.

1 Machines virtuelles

Demander l'accès

Rechercher pour filtrer les éléments...

Machine virtuelle	Approuvé	Dernier accès	Détails de la connexion	Dernier utilisateur
myVM	0 Requêtes	N/A	(highlighted with a blue circle)	N/A

Figure 48: Détails de la connexion

Nous avons intégré Microsoft Defender for Cloud et implémenté des recommandations de machines virtuelles.

### 3.1.3 Déploiement de Microsoft Sentinel

Après la mise place d'Azure Monitor et de Microsoft Defender for cloud, nous en arrivons à l'objectif final qui est la création d'une preuve de concept de détection et de réponse aux menaces basée sur Microsoft Sentinel. Pour cela, nous allons :

- ✓ Commencer à collecter des données à partir d'Azure Activity et de Microsoft Defender pour le Cloud.
- ✓ Ajouter des alertes intégrées et personnalisées
- ✓ Découvrir comment les Playbooks peuvent être utilisés pour automatiser une réponse à un incident.

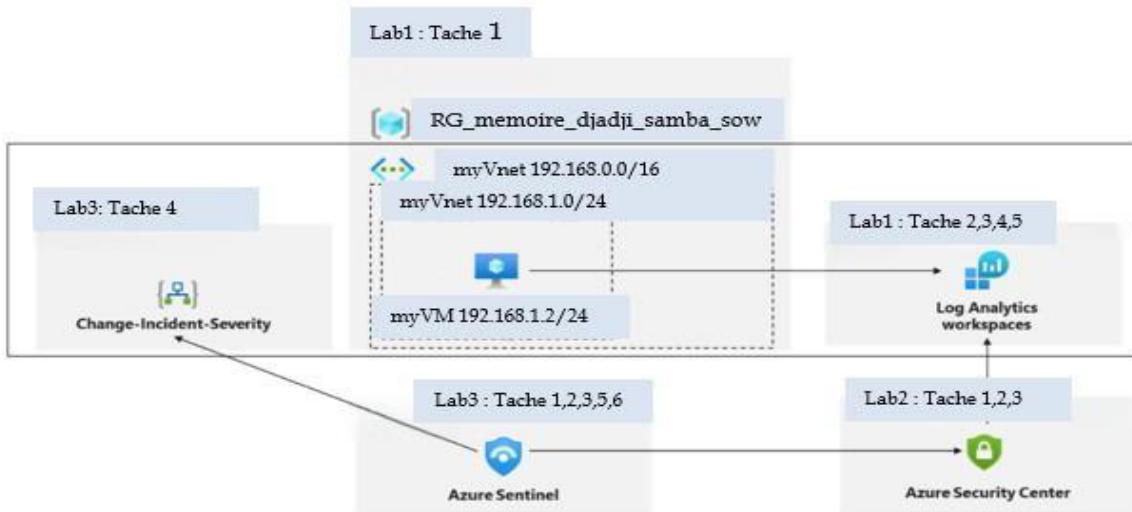


Figure 49: Déploiement de Microsoft Sentinel [20]

### 3.1.3.1 Tâche 1 : Intégrer Azure Sentinel

Dans cette tâche, nous allons intégrer Microsoft Sentinel et connecter l'espace de travail Log Analytics.

- ❖ Il s'agit de notre première tentative d'action Microsoft Sentinel dans le tableau de bord Azure, effectuons les étapes suivantes : Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, tapons Microsoft Sentinel, sélectionnons Microsoft Sentinel dans la vue Services et appuyons sur la touche Entrée.

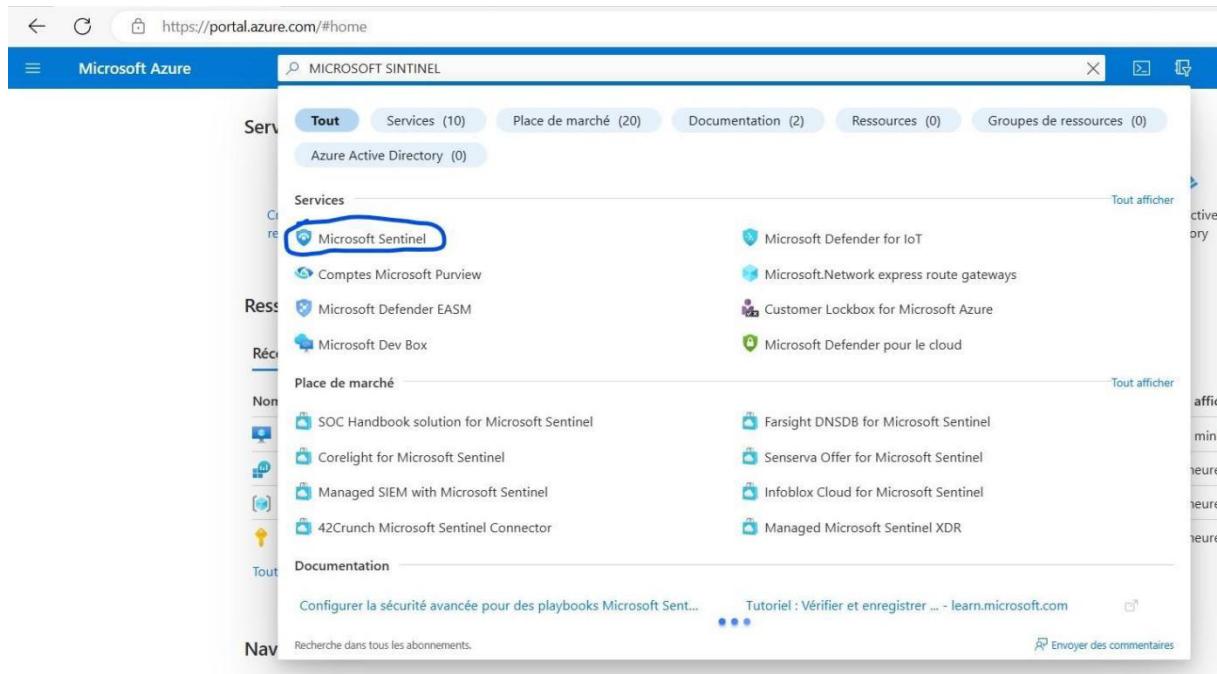


Figure 50: Recherche de Microsoft Sentinel sur le portail azure

- ❖ Dans le panneau Microsoft Sentinel, nous cliquons sur le bouton + Créer.

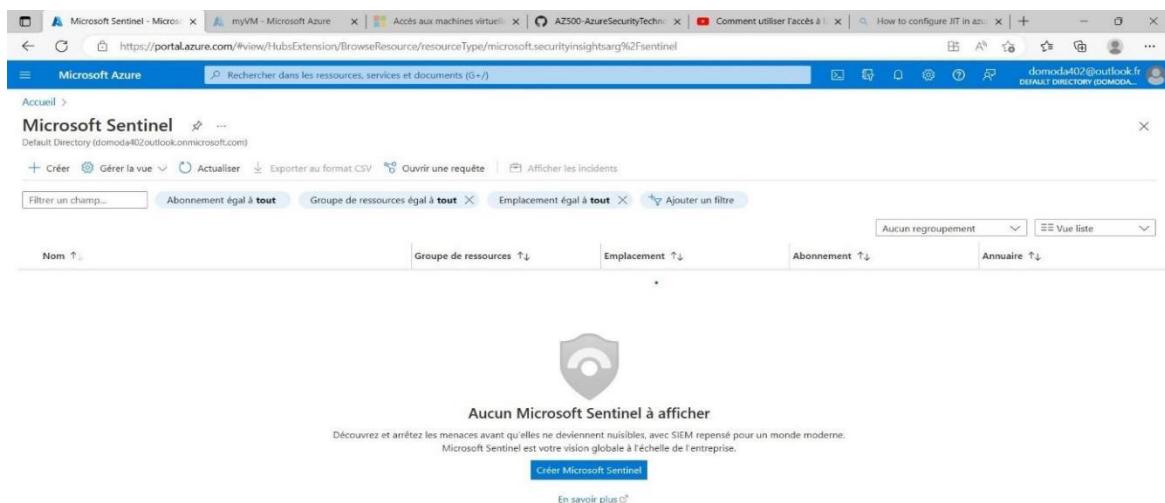


Figure 51: Le panneau de Microsoft Sentinel

- ❖ Dans le panneau Ajouter Microsoft Sentinel à un espace de travail, nous sélectionnons l'espace de travail Log Analytics que nous avons créé dans le laboratoire Azure Monitor, puis cliquons sur Ajouter.

Emplacement	Espace de travail	ResourceGroup	Abonnement	Annuaire
eastus	monanalyseurdeblog	rg_memoire_djadjii_samba_sow	Azure for Students	Default Directory

Figure 52: Ajout d'un espace de travail à Microsoft Sentinel

Il est à noter que Microsoft Sentinel a des exigences très spécifiques pour les espaces de travail. Par exemple, les espaces de travail créés par Microsoft Defender for Cloud ne peuvent pas être utilisés.

### 3.1.3.2 Tâche 2 : configurer Microsoft Sentinel pour utiliser le connecteur de données Azure Activity

Dans cette tâche, nous allons configurer Sentinel pour utiliser le connecteur de données Azure Activity.

- ❖ Sur Microsoft Sentinel, Connecteur de données, passons en revue la liste des connecteurs disponibles, sélectionnons l'entrée représentant le connecteur d'activité, nous vérifions sa description et son état, puis nous cliquons sur Ouvrir la page du connecteur.

Figure 53: Ajout d'un connecteur d'activité

- ❖ Dans l'onglet Configurer les journaux d'activité Azure pour les diffuser vers l'espace de travail Log Analytics spécifié (page Affecter une stratégie), cliquons sur le bouton Points de suspension de l'étendue (...). Dans la page Étendue, choisissons notre abonnement Azure dans la liste déroulante des abonnements, puis cliquons sur le bouton Sélectionner en bas de la page.

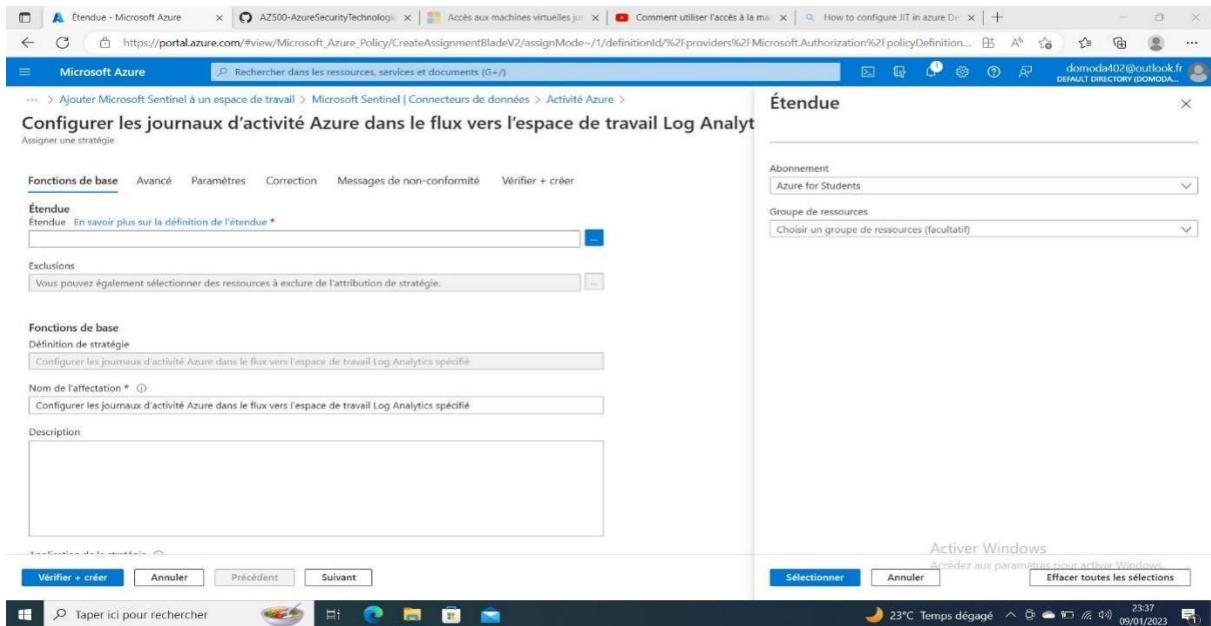


Figure 54: Configurer les journaux d'activité Azure dans le flux vers l'espace de travail Log Analytics

- ❖ Sur le bouton Suivant en bas de l'onglet Notions de base pour passer à l'onglet Paramètres. Sous l'onglet Paramètres, sur le bouton ellipse (...) de l'espace de travail Primary Log Analytics (...). Dans la page Espace de travail Log Analytics principal, assurons-nous que notre abonnement Azure est sélectionné et utilisons la liste déroulante Espaces de travail pour sélectionner l'espace de travail Log Analytics que nous utilisons pour Sentinel. Puis le bouton Sélectionner en bas de la page.

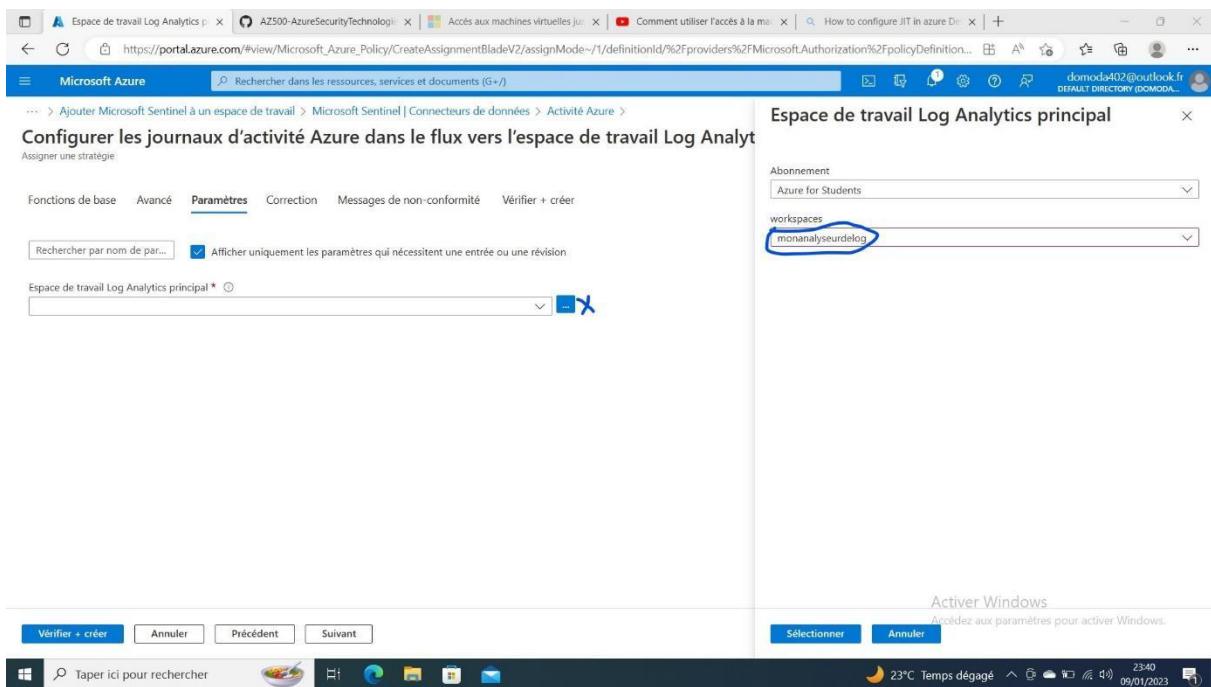


Figure 55: ajout de l'espace de travail principale

- ❖ Sur l'onglet Correction, nous cochons la case Crée une tâche de correction. Cela activerait la liste déroulante « Configurer les journaux d'activité Azure pour diffuser vers l'espace de travail Log Analytics spécifié » dans la liste déroulante Stratégie pour corriger. Dans la liste

déroulante Emplacement de l'identité attribuée au système, nous sélectionnons la région (dans notre cas États-Unis de l'Est) que nous avons utilisée précédemment pour votre espace de travail Log Analytics.

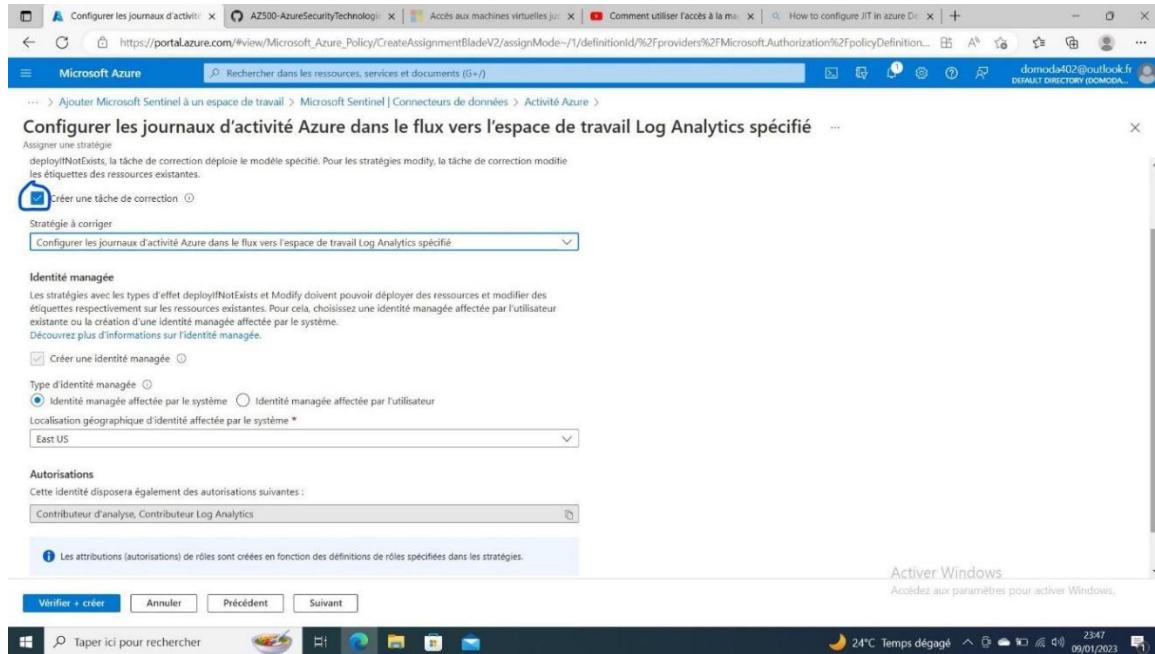


Figure 56: Activation de la gestion d'une tâche correction

- ❖ Sur l'onglet Message de non-conformité, nous pouvons entrer un message de non-conformité si nous le souhaitons (facultatif), enfin sur le bouton +créer. Sur la page activité azure on peut s'apercevoir l'affichage de quelques données collectées.

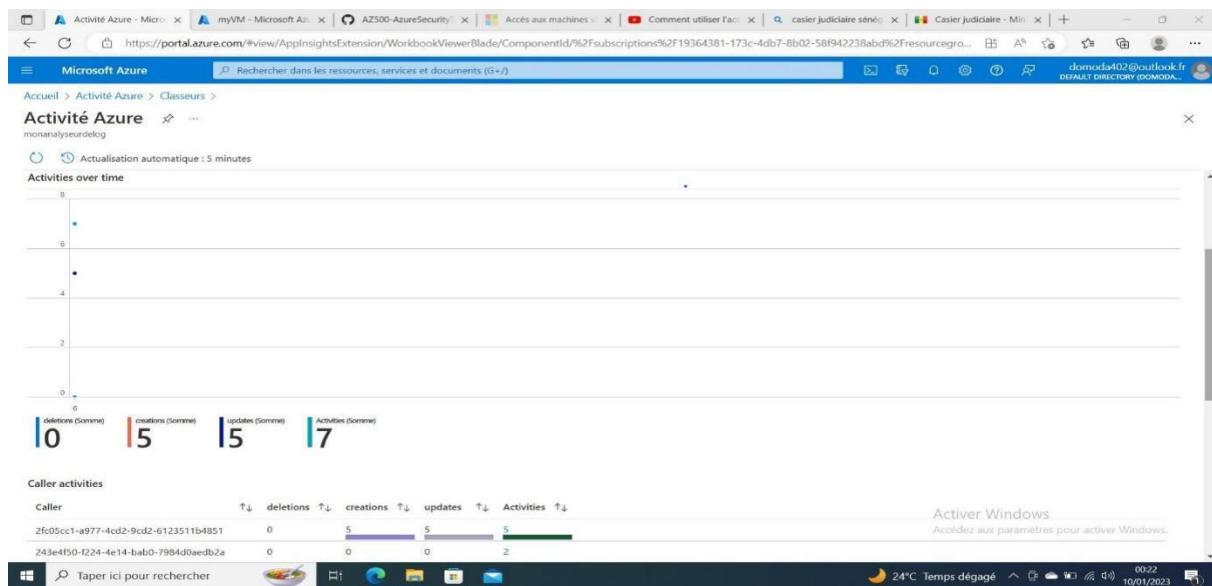


Figure 57: l'affichage de quelques données collectées

### 3.1.3.3 Tâche 3 : Créer une règle qui utilise le connecteur de données Azure Activity

Dans cette tâche, nous allons examiner et créer une règle qui utilise le connecteur de données Azure Activity.

- Sur Microsoft Sentinel, Analyse, dans la liste des modèles de règles, choisissons **Nombre suspect de création ou de déploiement de ressource** associée à la source de données Azure Activity. Ensuite, dans le volet affichant les propriétés du modèle de règle, on clique sur Créer une règle. Cette règle a une gravité moyenne.

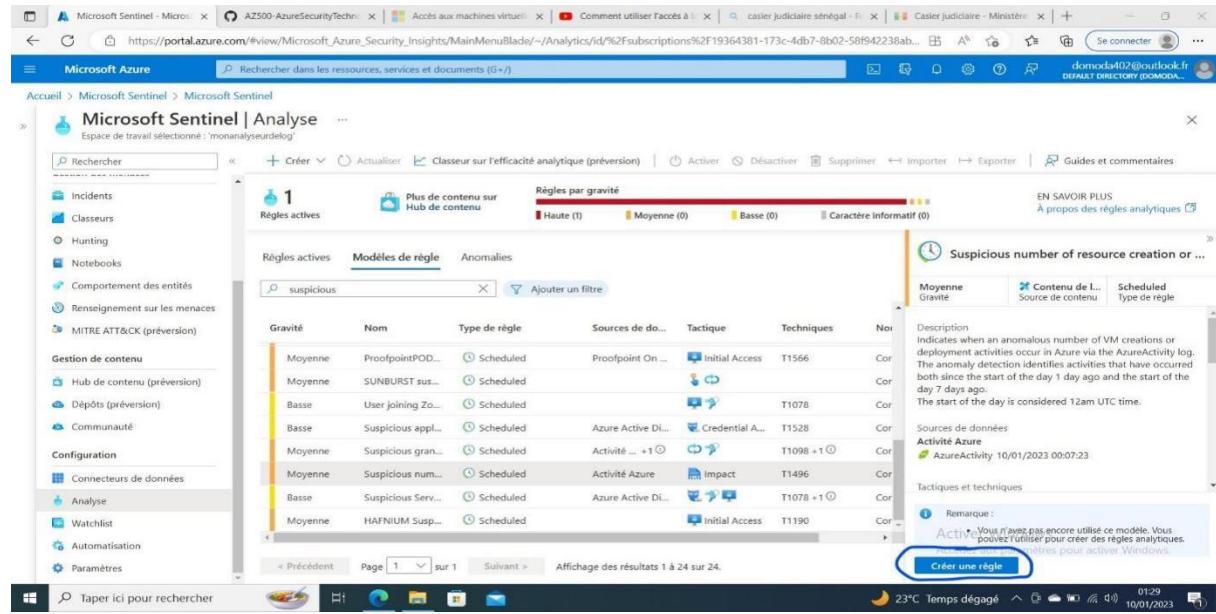


Figure 58: création d'une règle utilisant Azure Activity

- Sous l'onglet Général de l'Assistant Règle analytique - Créons une règle à partir du panneau Modèle, puis acceptons les paramètres par défaut et cliquons sur Suivant : Définir la logique de règle.

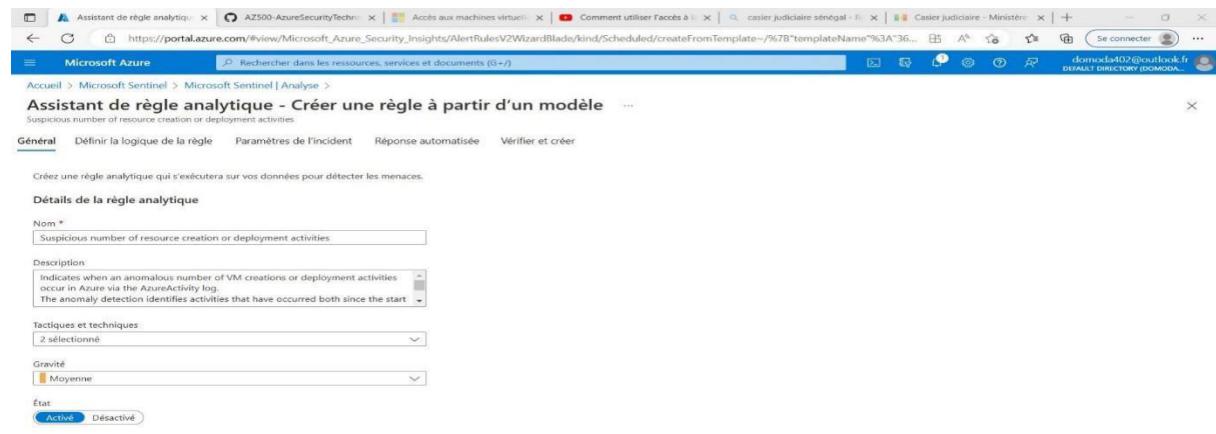


Figure 59: Définir la logique de règle

- ❖ Sous l'onglet Définir la logique de la règle de l'Assistant Règle analytique - Créons une règle à partir du panneau Modèle, puis acceptons les paramètres par défaut et cliquons sur Suivant : Paramètres d'incident.

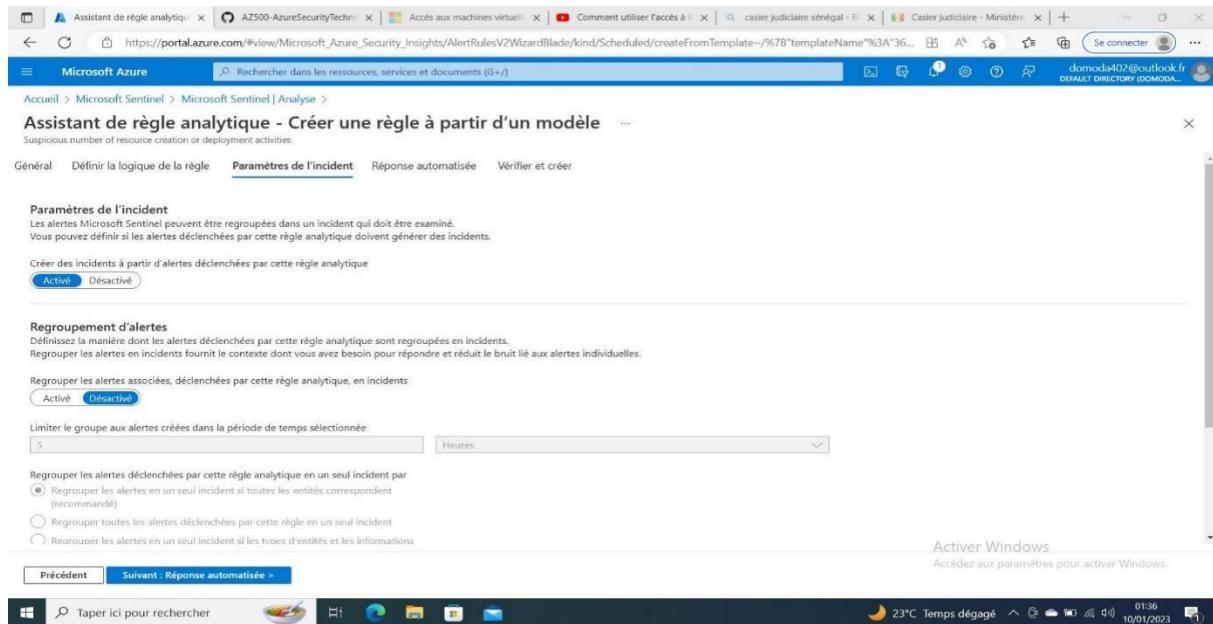


Figure 60: configuration du paramètre d'incident

- ❖ Sous l'onglet Paramètres d'incident de l'Assistant Règle analytique - Créons une règle à partir du panneau Modèle, puis acceptons les paramètres par défaut et cliquons sur Suivant : de réponse automatisée. C'est ici que nous pouvons ajouter un playbook, implémenté en tant qu'application logique, à une règle pour automatiser la correction d'un problème. Après création nous avons une règle active.

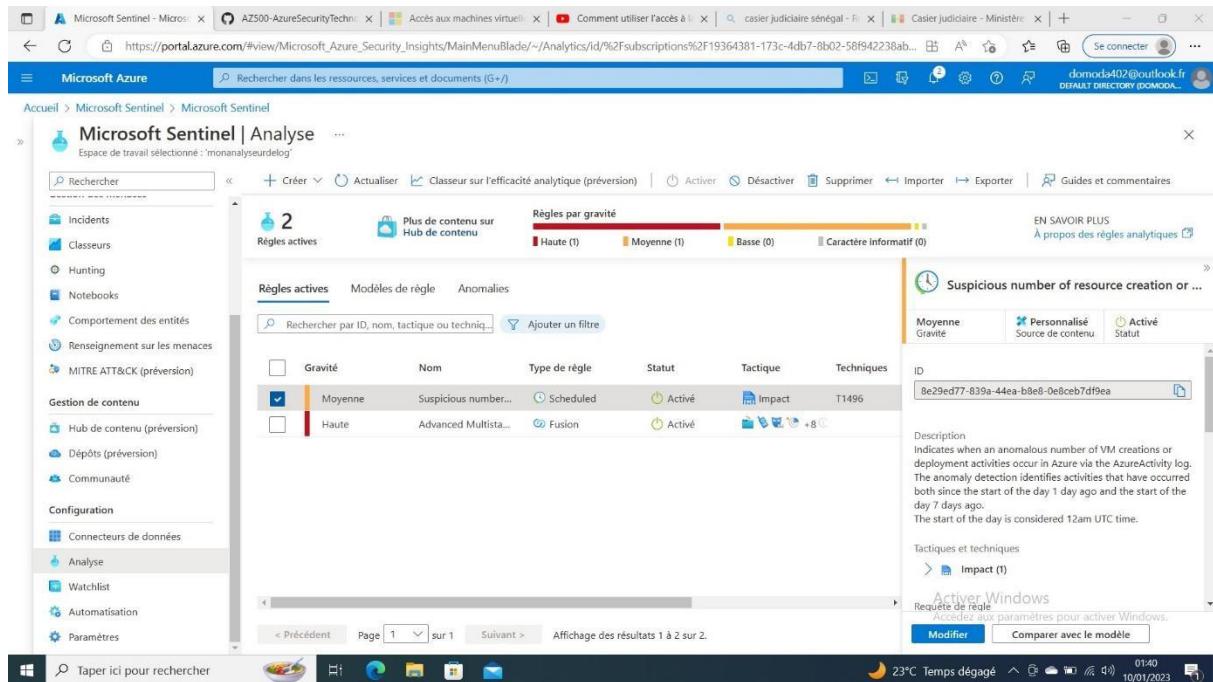


Figure 61: visualisation de la règle créée

### 3.1.3.4 Tâche 4 : Créer un playbook

Dans cette tâche, nous allons créer un playbook. Un playbook de sécurité est un ensemble de tâches qui peuvent être appelées par Microsoft Sentinel en réponse à une alerte.

- ❖ Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, tapons Déployer un modèle personnalisé et appuyons sur la touche Entrée.

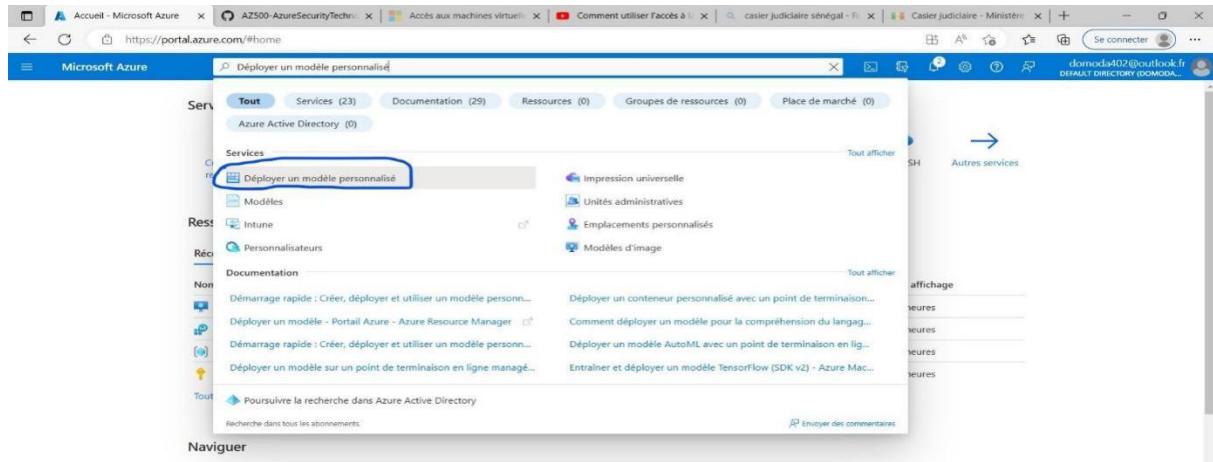


Figure 62: recherche de Déployer un modèle personnalisé sur le portail azure

- ❖ Dans le panneau Déploiement personnalisé, cliquons sur l'option Créez votre propre modèle dans l'éditeur.

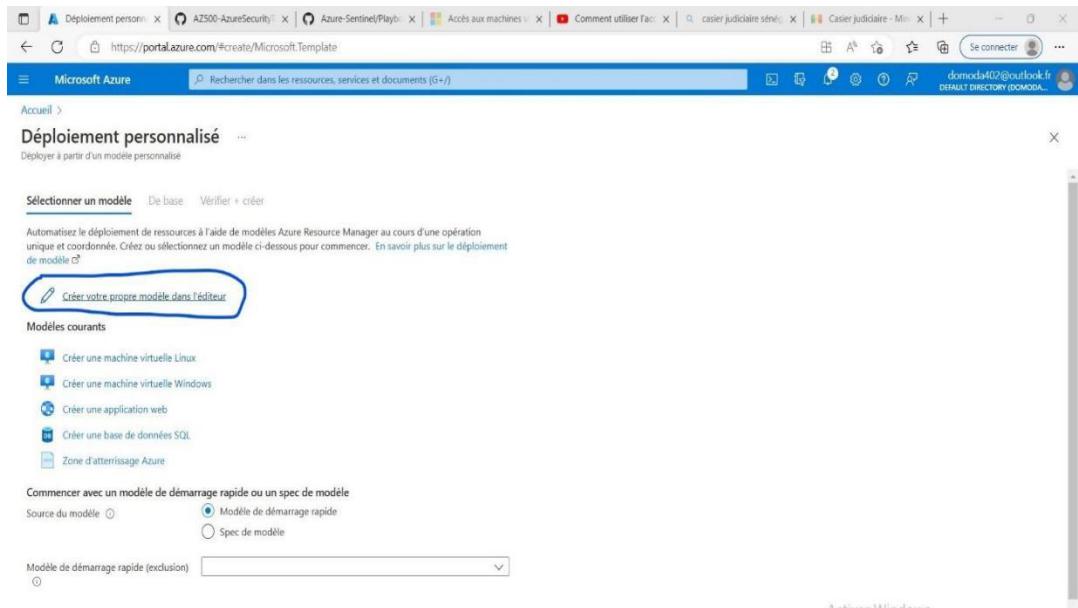


Figure 63: création d'un modèle personnalisé

- ❖ Dans le panneau Modifier le modèle, cliquons sur Charger le fichier, puis recherchons le fichier stocké sur notre machine en local pour l'ouvrir. Dans le panneau Modifier le modèle, cliquons sur Enregistrer. Selon différents scénarios y a des Playbooks correspondants et disponible sur la page GitHub de Microsoft Azure <https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks>. [21]

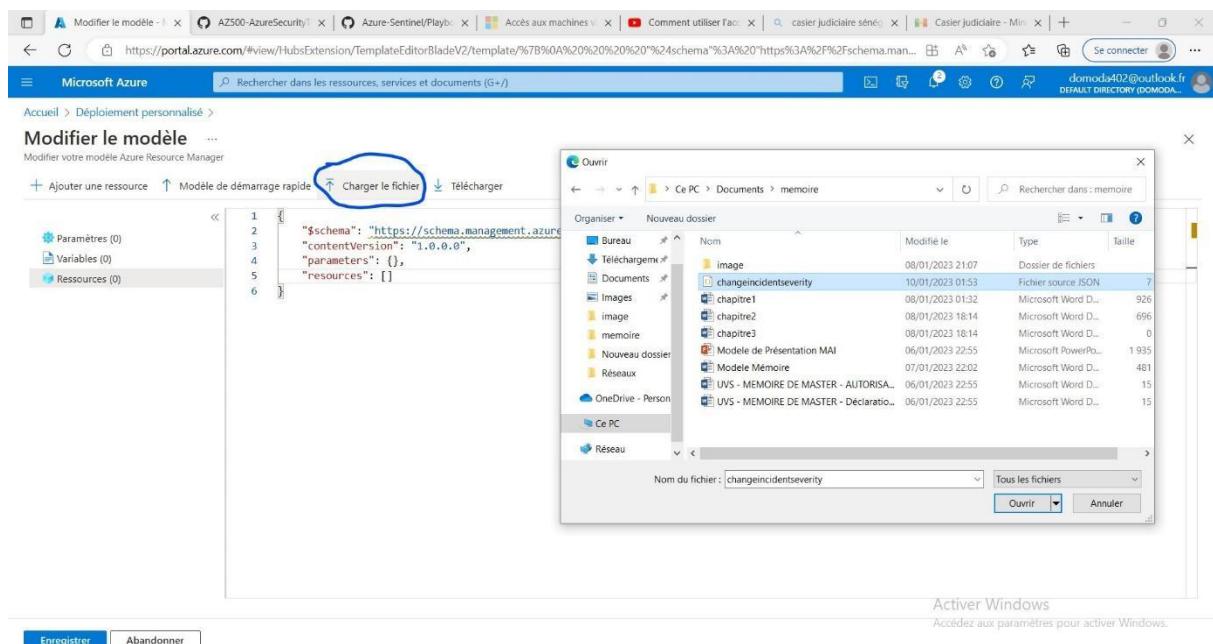


Figure 64: L'ajout de notre Playbooks

- ❖ Maintenant On valide Sur Vérifier + créer, puis sur Créer.

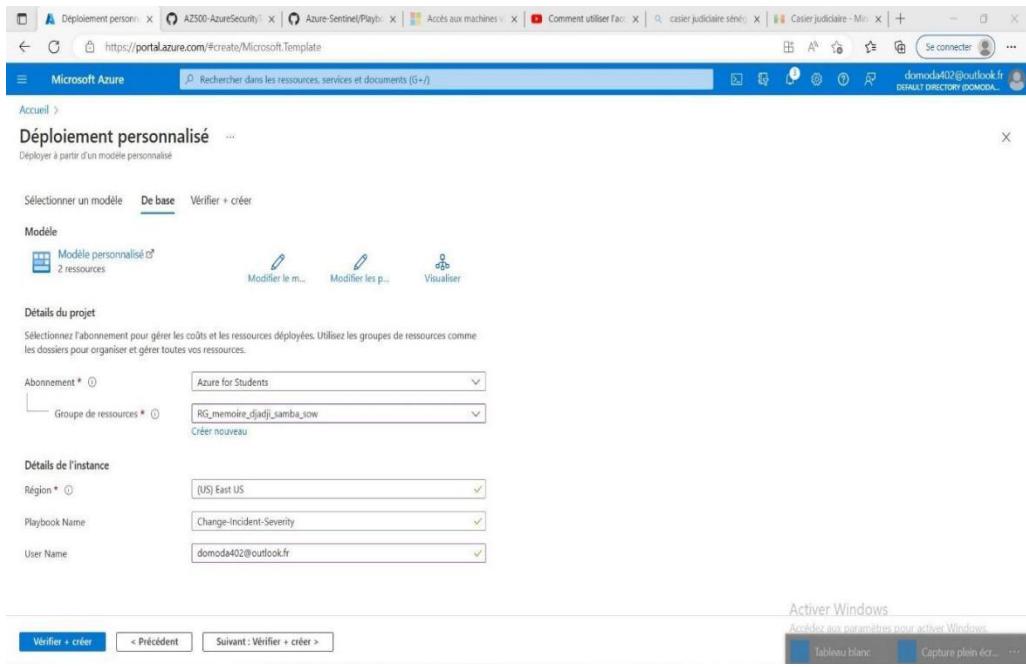


Figure 65: finalisation de la création

- ❖ A la fin du déploiement, dans le panneau Groupes de ressources, dans la liste des groupes de ressources RG\_memoire\_djadji\_samba\_sow, dans la liste des ressources, choisissons l'entrée représentant l'application logique Change-Incident-Severity nouvellement créée

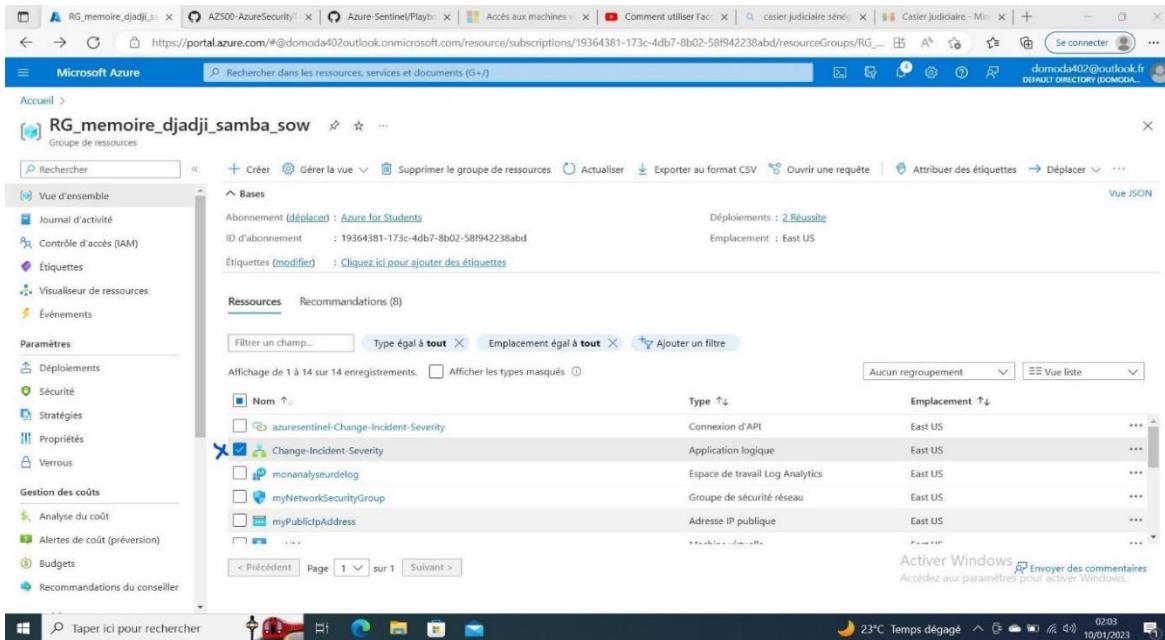


Figure 66: la logique Change-Incident-Severity

- ❖ Dans le panneau Concepteur d'applications logiques, chacune des quatre connexions affiche un avertissement. Cela signifie que chacun doit être revu et configuré. Cliquons sur Ajouter nouveau, vérifions que l'entrée de la liste déroulante Locataire contient notre nom de locataire Azure AD, puis cliquons sur Connexion. Nous allons répéter l'étape précédente pour les trois autres étapes de connexion en s'assurant qu'aucun avertissement ne s'affiche sur aucune des étapes. Pour finir, enregistrons nos modifications.

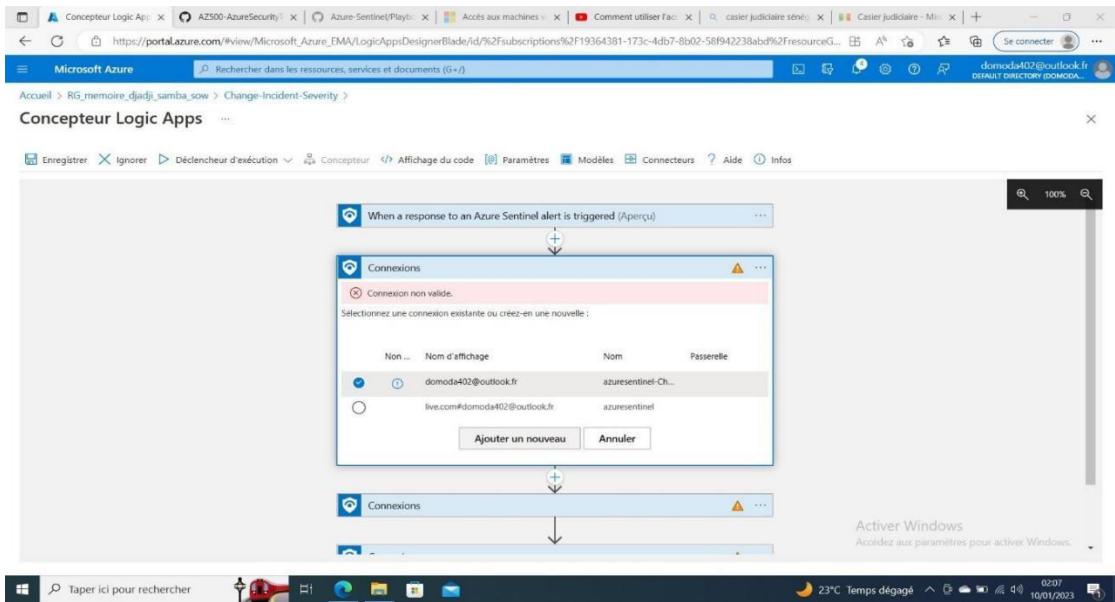


Figure 67: configuration des quatre connexions

### 3.1.3.5 Tâche 5 : Créer une alerte personnalisée et configurer un playbook en tant que réponse automatisée

- ❖ Sur Microsoft Sentinel, Analyse, sur Règle de requête planifiée, Créons une règle en spécifiant les paramètres suivants : nom du playbooks **djadji playbooks**, les autres paramètres sont par défaut.

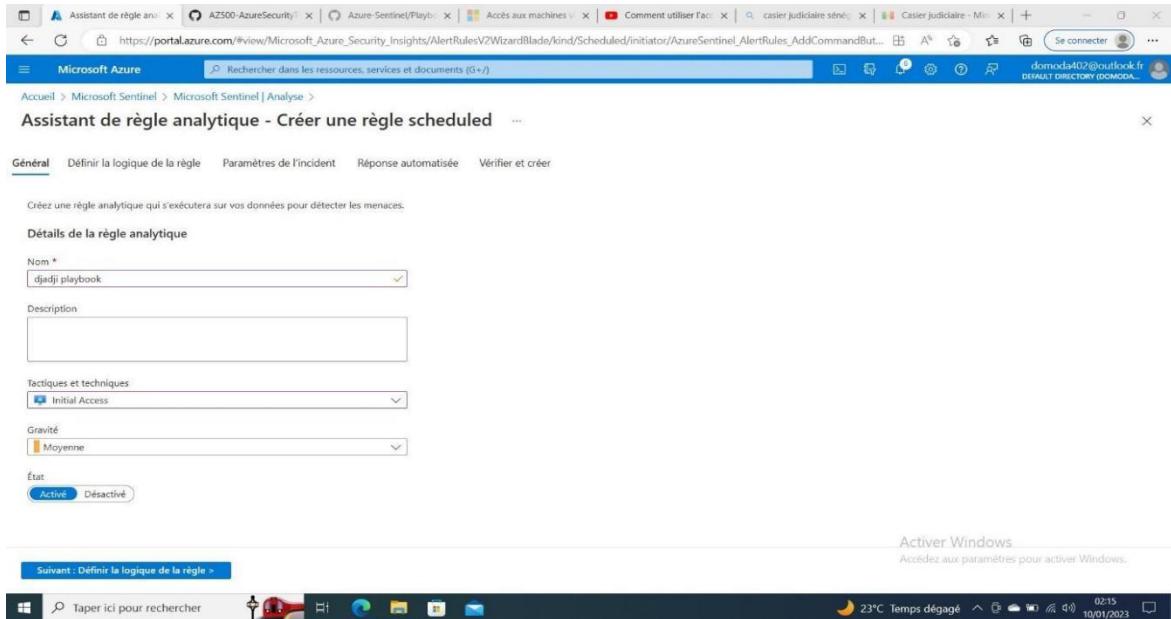


Figure 68: création d'une règle Scheduled

- ❖ Sous l'onglet Définir la logique de la règle de l'Assistant Règle analytique, dans la zone de texte Requête de règle, mettons la requête de règle suivante. Cette règle identifie la suppression des stratégies d'accès aux machines virtuelles juste-à-temps.

```
AzureActivity|where ResourceProviderValue =~ "Microsoft.Security" |where OperationNameValue =~ "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"
```

Définissez la logique de votre nouvelle règle analytique.

**Requête de règle**

Les détails de l'heure définis ici seront inclus dans l'étendue définie ci-dessous dans les champs de planification de la requête.

```
AzureActivity
| where ResourceProviderValue == "Microsoft.security"
| where OperationNameValue == "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"
```

Afficher les résultats de la requête >

**Enrichissement de l'alerte**

- ✓ Mappage d'entités
- ✓ Détails personnalisés
- ✓ Détails de l'alerte

**Planification de la requête**

Simulation des résultats

Ce graphique montre les résultats des 50 dernières évaluations de la règle analytique définie. Cliquez sur un point du graphique pour afficher les événements bruts pour ce point dans le temps.

Tester avec les données actuelles

Alertes par jour

Seuil

31 déc. 2023 3 janv. 5 janv. 7 janv. 9 janv.

Activer Windows

Accédez aux paramètres pour activer Windows.

Précédent Suivant : Paramètres de l'incident >

Figure 69: Cette règle identifie la suppression des stratégies d'accès aux machines JIT

- ❖ Pour les autres onglets, on laisse les paramètres par défaut et on valide pour créer la règle. Nous avons maintenant une nouvelle règle active appelée **djadji Playbook**. Si un événement identifié par la logique se produit, il en résulte une alerte de gravité moyenne, qui générera un incident correspondant.

Microsoft Sentinel | Analyse

Espace de travail sélectionné : monanalyseurdelog

Rechercher

Créer Actualiser Classeur sur l'efficacité analytique (prévision) Activer Désactiver Supprimer Importer Exporter Guides et commentaires EN SAVOIR PLUS À propos des règles analytiques

3 Règles actives

Plus de contenu sur Hub de contenu

Règles par gravité

Haute (1) Moyenne (2) Basse (0) Caractère informatif (0)

Règles actives Modèles de règle Anomalies

Rechercher par ID, nom, tactique ou technique Ajouter un filtre

Gravité	Nom	Type de règle	Statut	Tactique	Techniques
Moyenne	djadji playbook	Scheduled	Activé	Initial Access	
Moyenne	Suspicious number...	Scheduled	Activé	Impact	T1496
Haute	Advanced Multist...	Fusion	Activé		+ 8

djadji playbook

Moyenne Gravité Personnalisé Source de contenu Activé

ID: 04fb32b1-6f85-464b-b20e-d5518c58dee4

Description

Tactiques et techniques Initial Access (0)

Requête de règle

```
AzureActivity
| where ResourceProviderValue == "Microsoft.security"
| where OperationNameValue == "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"
```

Modifier Ouvrir dans l'historique Ouvrir dans l'historique 02:26 10/01/2023

Figure 70: visualisation de la règle active appelée djadji Playbook

### 3.2 Tâche 6 : Invoquer un incident et passer en revue les actions associées

- ❖ Sur Microsoft Defender pour Cloud, Panneau Protection contre les charges de travail, cliquons sur la section Accès juste à temps aux machines virtuelles sous Protection avancée. Sur le côté droit de la ligne référençant la machine virtuelle myVM, cliquons sur le bouton de points de suspension, puis sur Supprimer.

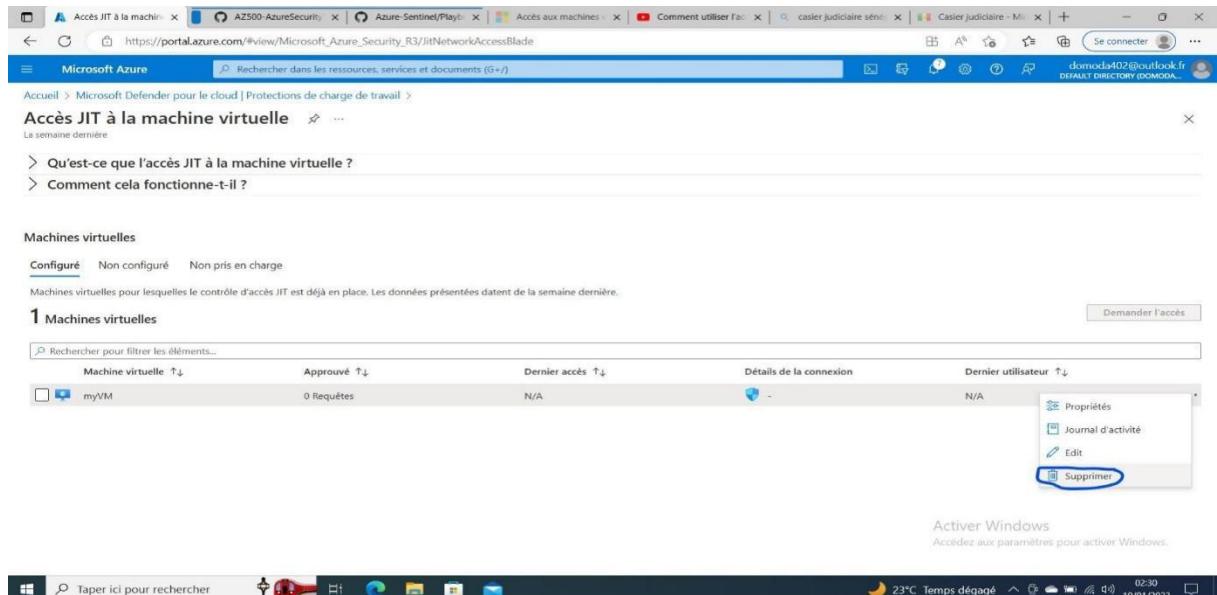


Figure 71: Invoquer un incident sur myVM

- ❖ Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, tapons Journal d'activité et appuyons sur la touche Entrée.

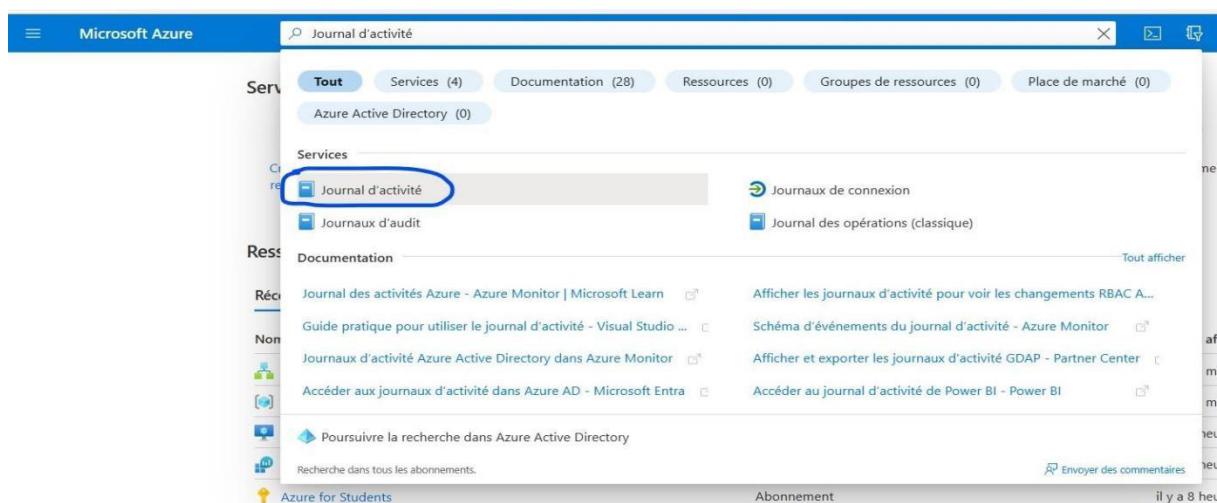


Figure 72: recherche de journal d'activité sur le portail azure

- ❖ En accédant au panneau Journal d'activité, nous pouvons noter une entrée **Supprimer les stratégies d'accès réseau JIT** qui apparaît

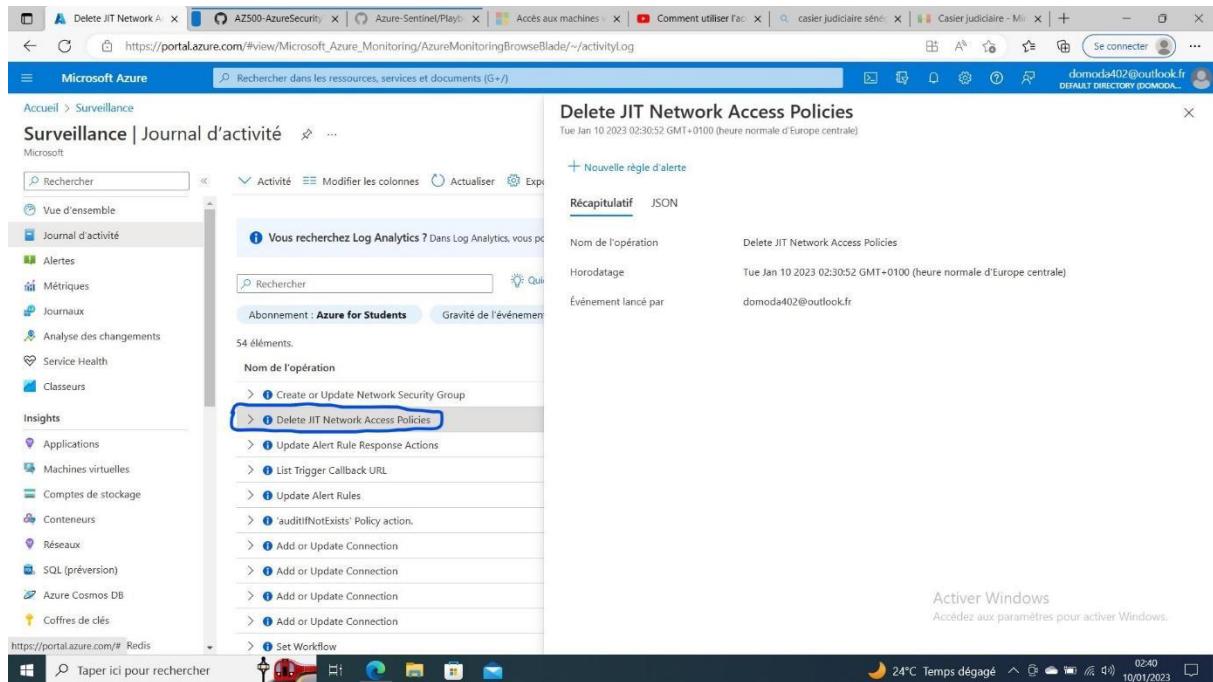


Figure 73: apparition de entrée Supprimer les stratégies d'accès réseau JIT

- ❖ Sur Microsoft Sentinel Vue d'ensemble, passons en revue le tableau de bord et vérifions qu'il affiche une alerte correspondant à la suppression de la stratégie d'accès aux machines virtuelles juste-à-temps. Nous pouvons apercevoir ci-dessous qu'une alerte à belle et bien été détectée.

Figure 74: une alerte correspondant à la suppression de la stratégie d'accès aux machines virtuelles JIT

Nous avons créé un espace de travail Microsoft Sentinel, l'avons connecté aux journaux d'activité Azure, créé un playbook et des alertes personnalisées déclenchées en réponse à la suppression des stratégies d'accès aux machines virtuelles juste-à-temps, et vérifié que la configuration est valide. Maintenant pour aller plus loin votre équipe SOC à travers les informations fournies par Sentinel va pousser l'investigation.