

Téléchargez votre application *Whova*

Connectez-vous à votre profil en entrant l'adresse courriel utilisée lors de votre inscription.

Whova vous permet de :

Vous mettre présent dans la formation suivie

Recevoir votre **badge de certification!**



ITSec

SOMMET DE
LA SÉCURITÉ
INFORMATIQUE

PRÉSENTÉ PAR DEVOLUTIONS ET SHERWEB








**JOURNÉE DE
FORMATION**

Microsoft Sentinel, votre allié sécurité

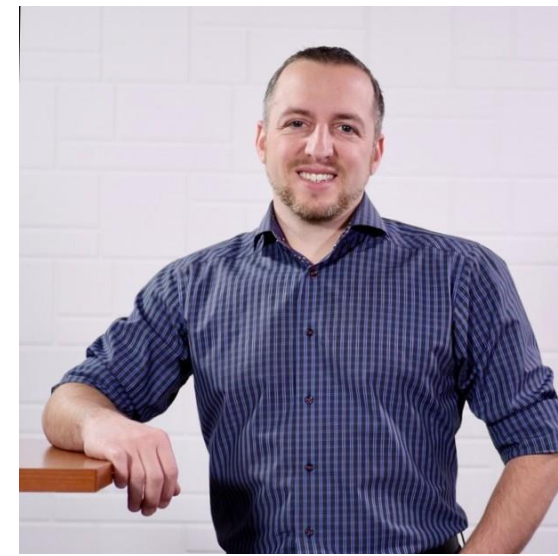
Workshop complet pour
une maîtrise rapide






À propos de Patrick Pilotte



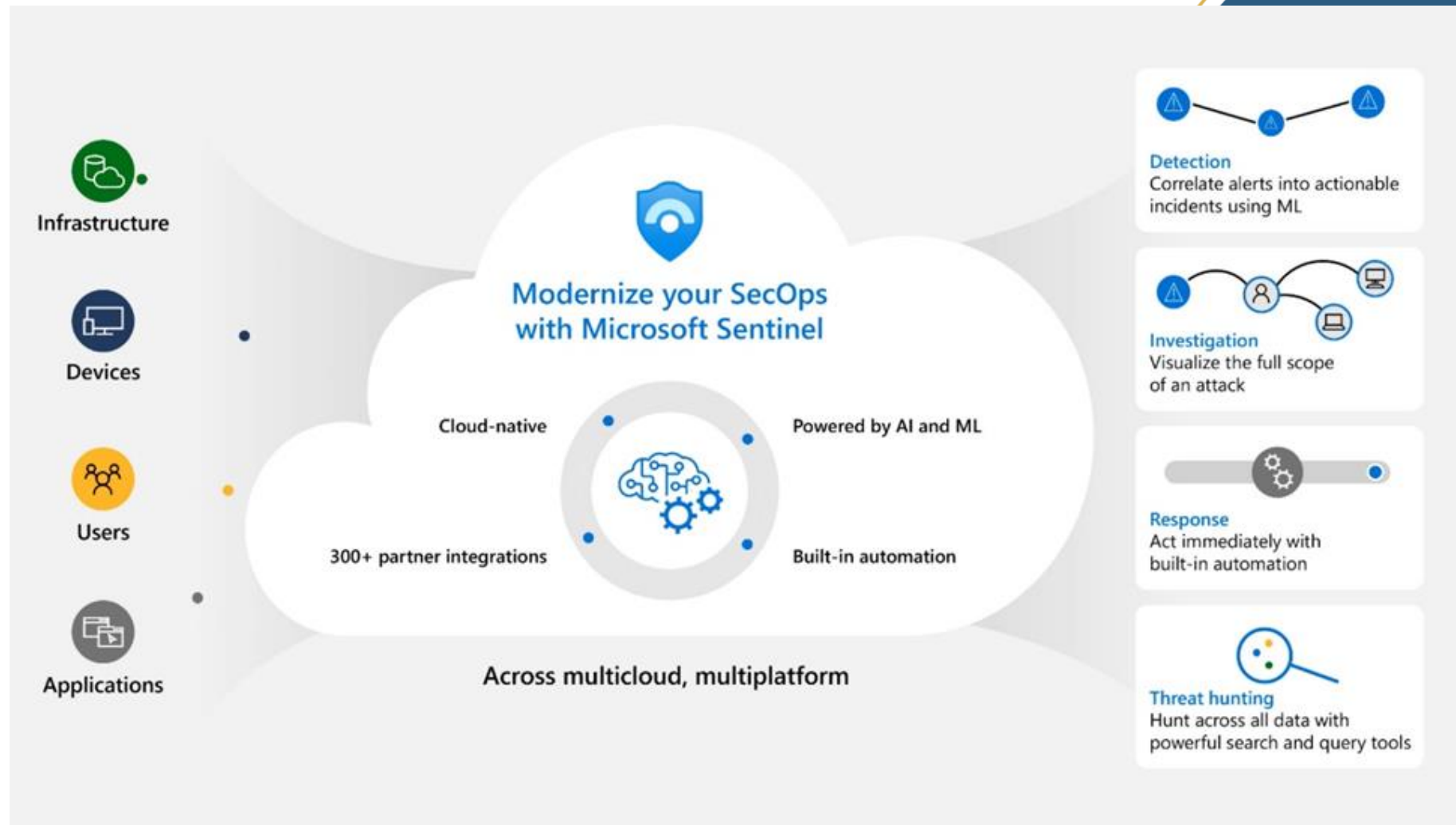
- ❖ Chef d'équipe en sécurité opérationnelle
 - ❖ Certified Incident Responder (eCIR)
 - Formateur en entreprise
 - Expert en Kali Linux, Raspberry Pi 
- ❖ Plus de 15 ans dans le domaine des TI et de la cybersécurité
 - Spécialisation en administration de serveurs et en réseautique
 - Engagé à améliorer continuellement les pratiques de sécurité
- ❖ Père de deux filles sportives   
- ❖ Vous me trouverez là où il y a:
 - Musique 
 - Bière 
 - BBQ 

À propos de David Grandolfo



- ❖ Spécialiste Senior en sécurité Opérationnel
 - Expert en cybersécurité et TI avec plus de 20 ans d'expérience
 - Spécialiste en réponse aux incidents
 - OSCP en cours (Penetration Testing with Kali Linux)
- ❖ Co Fondateur de Groupe ISM
 - Entrepreneur et formateur passionné, guidant les autres à saisir les implications de leurs décisions.
- ❖ Père d'un garçon et d'une fille  
- ❖ Vous me trouverez là où il y a:
 - BBQ en famille  
 - Une forêt et un feu de camp 

Qu'est-ce que Microsoft Sentinel et comment fonctionne-t-il ?



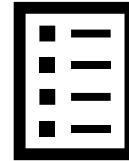
Par où commencer?

- **Évaluation** complète des risques



- **Comprendre** non seulement quels actifs nécessite protection mais **pourquoi** et dans quel contexte

- **Planification** du déploiement



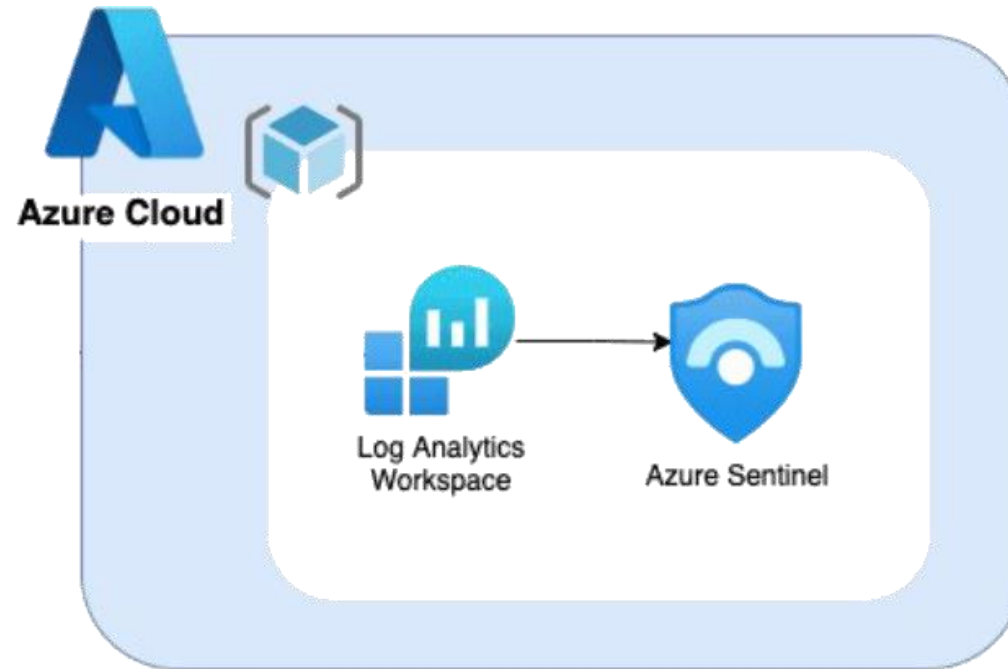
- **Coordination** avec toutes les parties prenantes pour assurer une mise en œuvre qui soutient nos objectifs **sans perturber** les opérations courantes

- **Sensibilisation** des employés

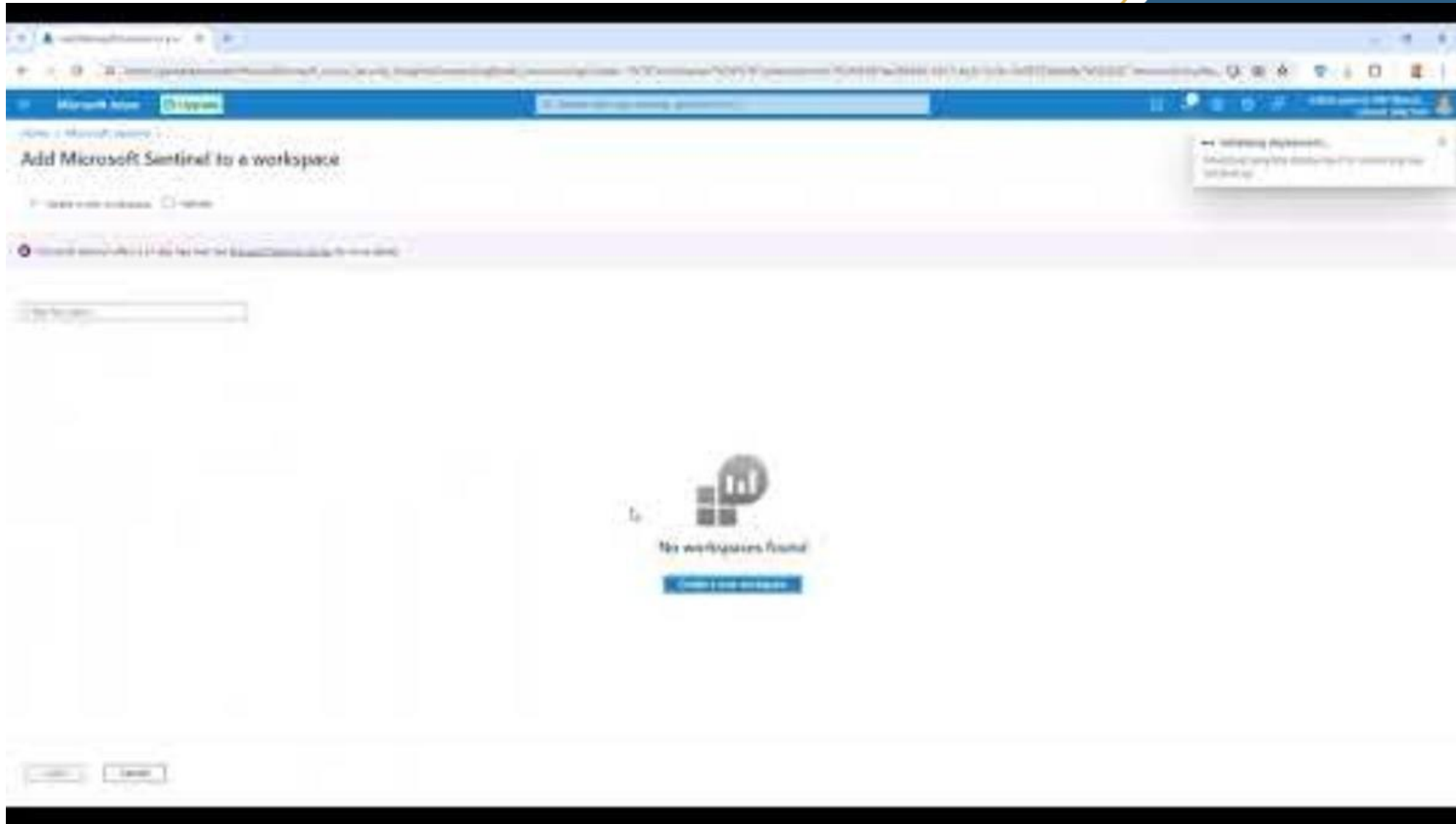


- **Veiller** à ce que tous les employés comprennent leur rôle

Installation de Sentinel



Installation de Sentinel



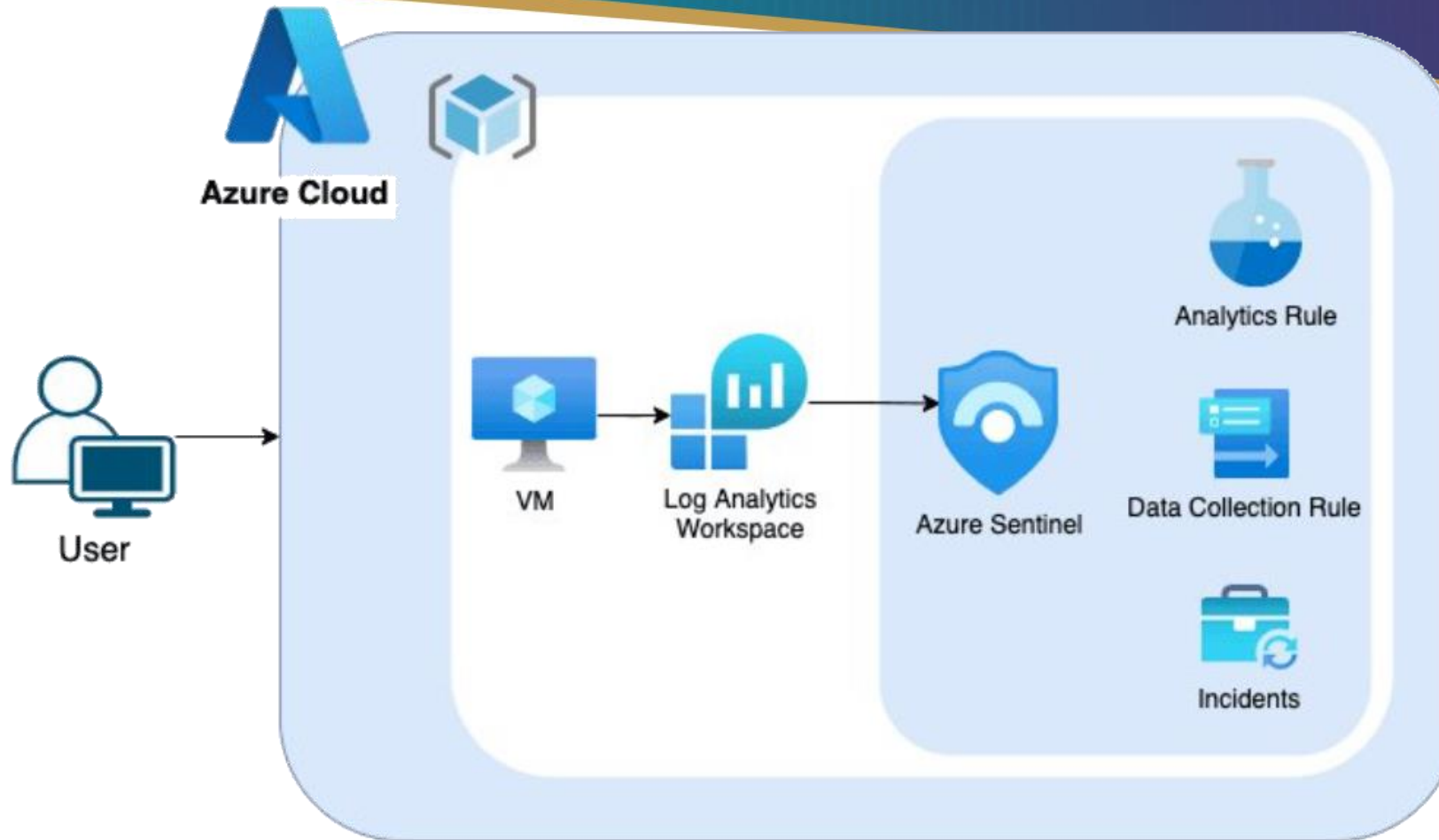
https://youtu.be/CNDv_G-fOjo

Les rôles de Sentinel



- **Collectez des données** à l'échelle du cloud
- **Détectez les menaces** non détectées précédemment
- **Investiguez les menaces** à l'aide de IA
- **Répondez aux incidents** rapidement

Diagramme Sentinel

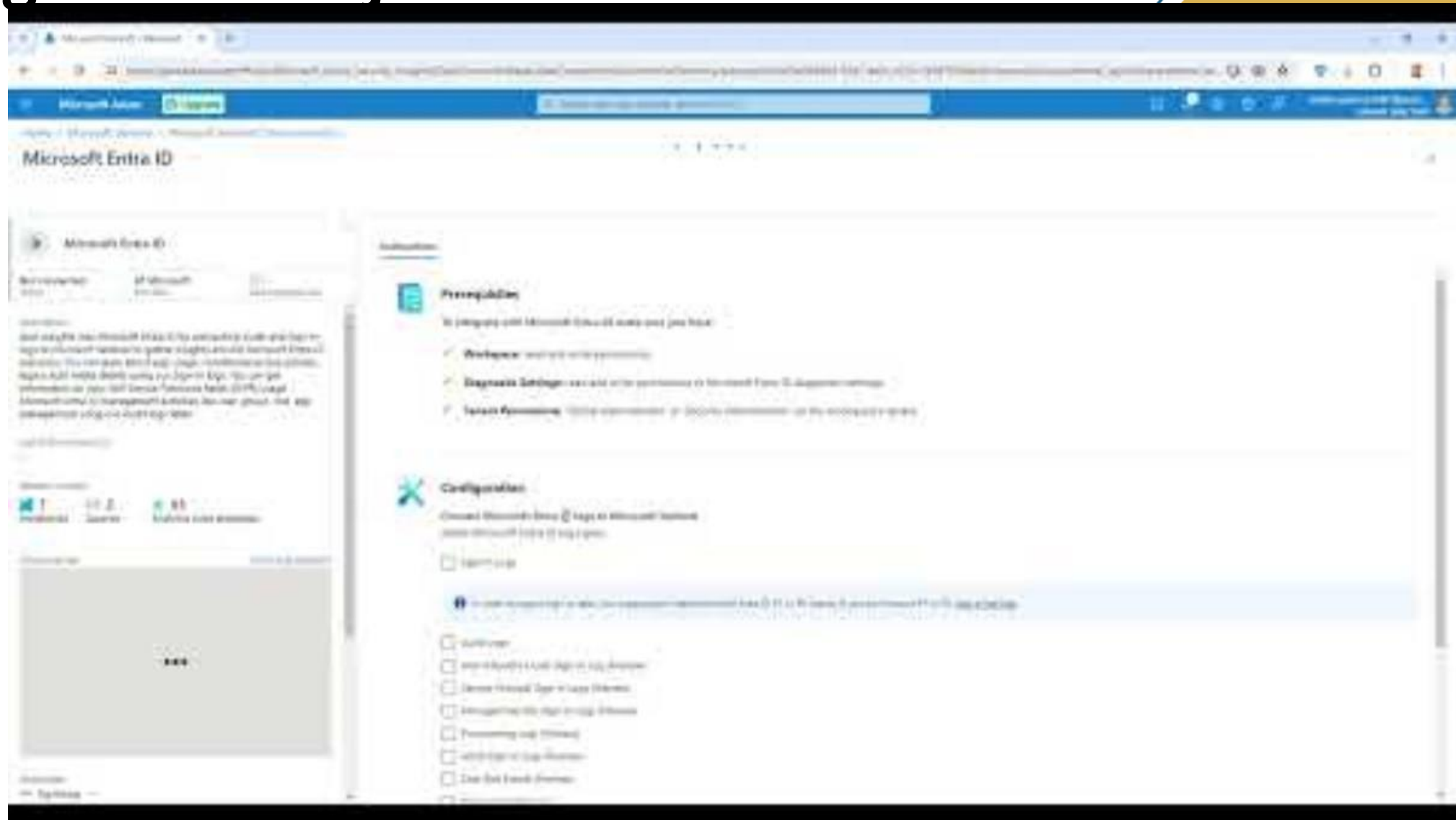


Prix pour Microsoft Sentinel

- Essai gratuit
- **Activez Microsoft Sentinel** sur un workspace Azure Monitor Log Analytics et les premiers **10 Go/jour** sont **gratuits** pendant **31 jours**. Cet essai gratuit est soumis à une **limite de 20 workspace par Azure tenant**.

Tier	Microsoft Sentinel Price	Effective Per GB Price ¹
Pay-As-You-Go	\$4.30 per GB-ingested	\$4.30 per GB-ingested
100 GB per day	\$296 per day	\$2.96 per GB
200 GB per day	\$548 per day	\$2.74 per GB
300 GB per day	\$800 per day	\$2.67 per GB
400 GB per day	\$1,037.33 per day	\$2.60 per GB
500 GB per day	\$1,265 per day	\$2.53 per GB
1,000 GB per day	\$2,480 per day	\$2.48 per GB

Ingestion des journaux d'Entra ID



Une bonne gestion des données et des coûts

1. Identifier les actifs critiques

- Prioriser les actifs critiques
- Pertinence pour la sécurité

2. Utiliser le filtrage pour réduire le volume

- Appliquer des filtres à la source avant l'ingestion
- Éliminer le bruit

3. Gestion des journaux

- Gérer la rétention

4. Gestion et surveillance des coûts

- Définissez un plafond quotidien sur la quantité de données ingérée
- Surveiller régulièrement et ajuster vos stratégies

5. Piloter et échelonner progressivement

- Commencer petit
- Ajouter progressivement au besoin

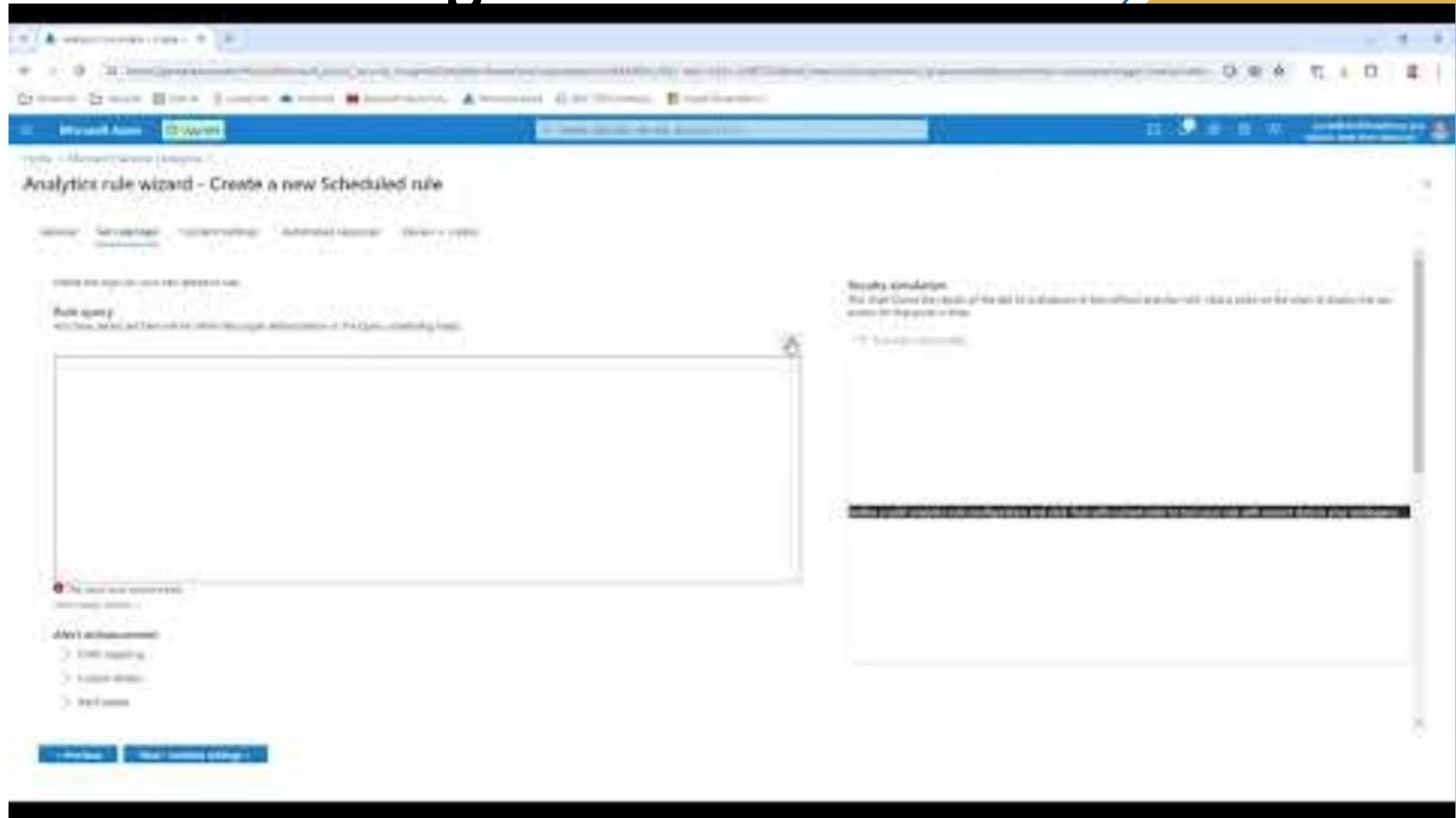


Création d'une règle

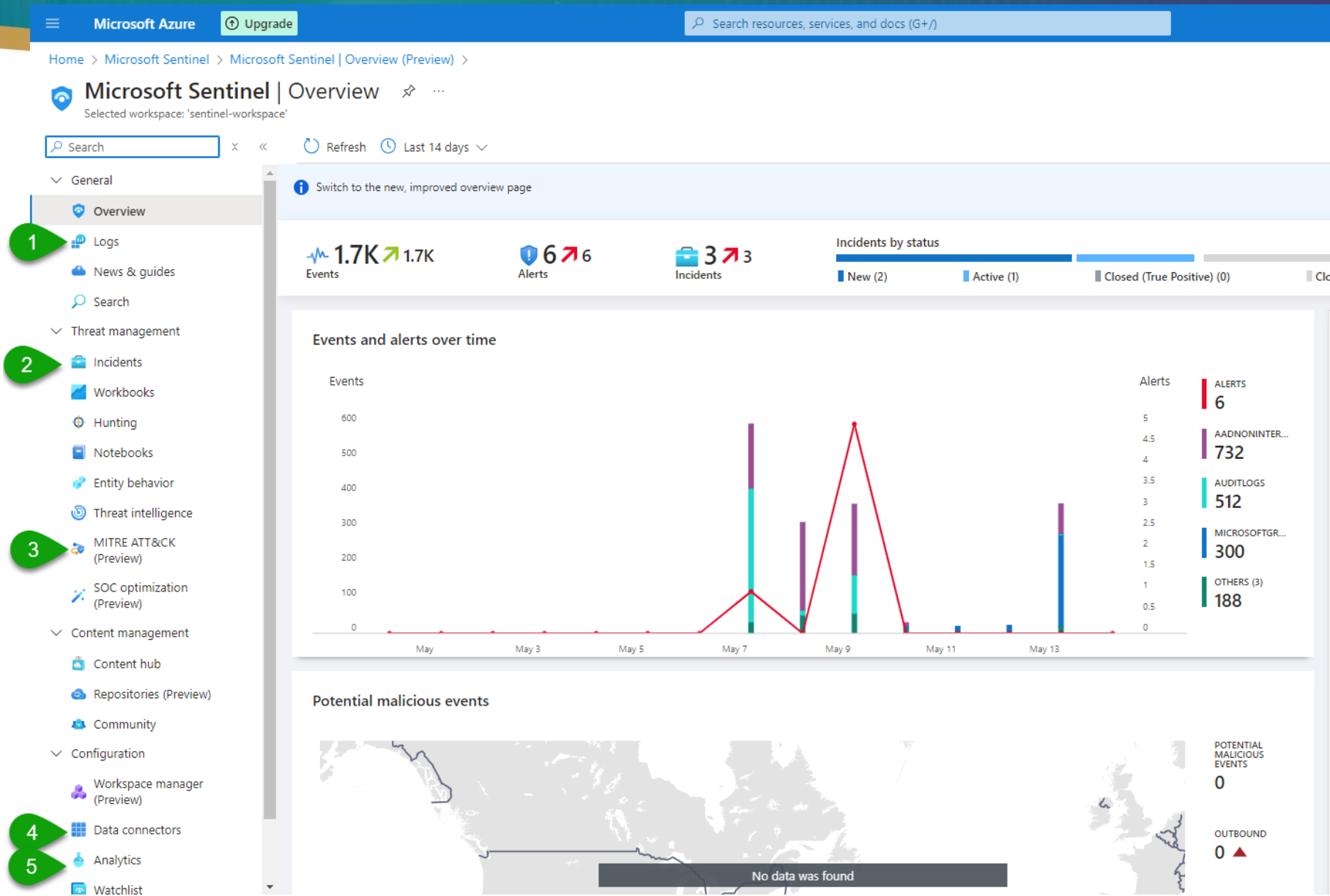
AuditLogs

```
| where OperationName == "Reset user password"  
| extend Username = tostring(TargetResources[0].userPrincipalName)  
| extend InitiatedIP = tostring(parse_json(tostring(InitiatedBy.user)).ipAddress)  
| extend InitiatedBy = tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName)  
| extend Userid = tostring(TargetResources[0].id)  
| extend UserType = tostring(TargetResources[0].type)  
| project TimeGenerated, Username, Userid, UserType, InitiatedIP, InitiatedBy
```

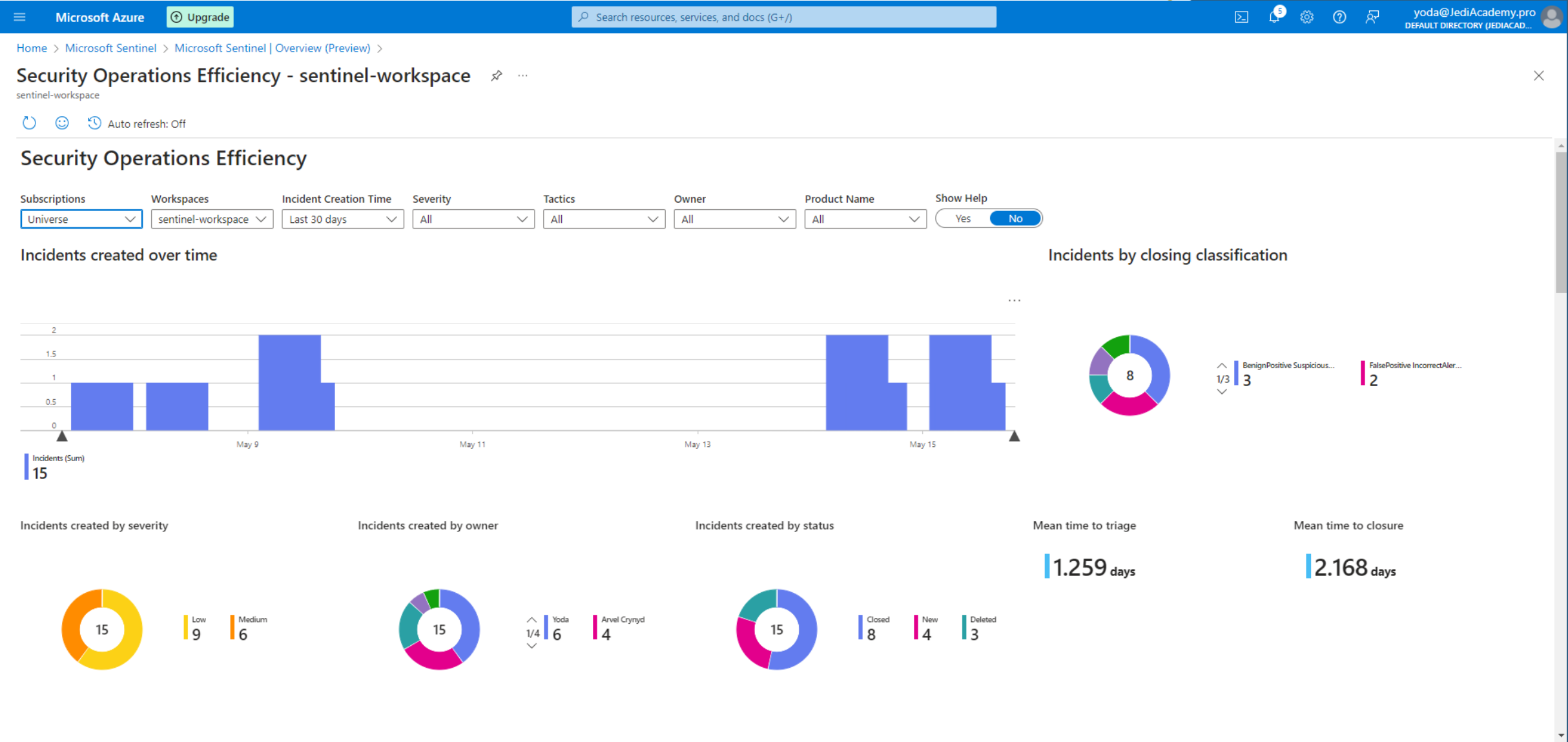

Création d'une règle



Exploration en direct de Sentinel



Analyser l'efficacité du SOC



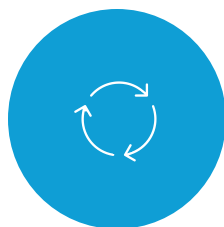
Conclusion



IMPLANTATION 5 MINUTES



COÛT DÉBUTANT À 2\$



NE CHANGEZ PAS POUR
CHANGER



ÉVALUER L'EFFICACITÉ



INDICATEURS DE
PERFORMANCE



AJUSTER VOTRE APPROCHE
EN FONCTION DE
L'ÉVOLUTION DU PAYSAGE
DE LA SÉCURITÉ

Étapes de l'atelier

Connexion et Installation :

- Connectez-vous à Azure Portal.
- Ajoutez Azure Sentinel au groupe de ressources **CreezVotreSentinelXXX**.

Configuration des Connecteurs de Données :

- Intégrez le connecteur Microsoft Entra ID pour collecter les données d'identité.

Règles Analytiques :

- Implémentez une règle analytique existante ou celle présenté.

Règle Analytics 2 (Near Real Time) :

- Configurez une règle NRT pour une surveillance en temps quasi réel.

Automatisation pour Avancés :

- Créez un playbook qui notifie par email ou Microsoft Teams lorsqu'une alerte est générée.
- Ces étapes permettent d'avoir une instance Azure Sentinel opérationnelle avec surveillance active et notifications automatisées.



<https://portal.azure.com>

Utilisateur: luke.skywalker@jediacademy.pro

Mot de passe: +-fXCc8Ku7rD

[Calculer votre coût pour Microsoft Sentinel](#)

Nous contactez:

Patrick Pilotte: <https://www.linkedin.com/in/ppilotte/>

David Grandolfo: <https://www.linkedin.com/in/dgrandolfo/>



Merci!

ITsec

FORMATION