Sécurité Azure : Parcours TryHackMe

Maîtrise des outils natifs Azure, notamment **Sentinel**, **Defender XDR** et **KQL**, acquise à travers des labs pratiques rigoureux et des scénarios d'attaque réels.

TRYHACKME AZURE SECURITY

Made with GAMMA

Une Maîtrise Complète de la Sécurité Cloud Azure

Sentinel

Supervision SIEM avancée et orchestration de la réponse aux incidents

KQL

Requêtes expertes pour la détection et l'analyse proactive des menaces

Defender XDR

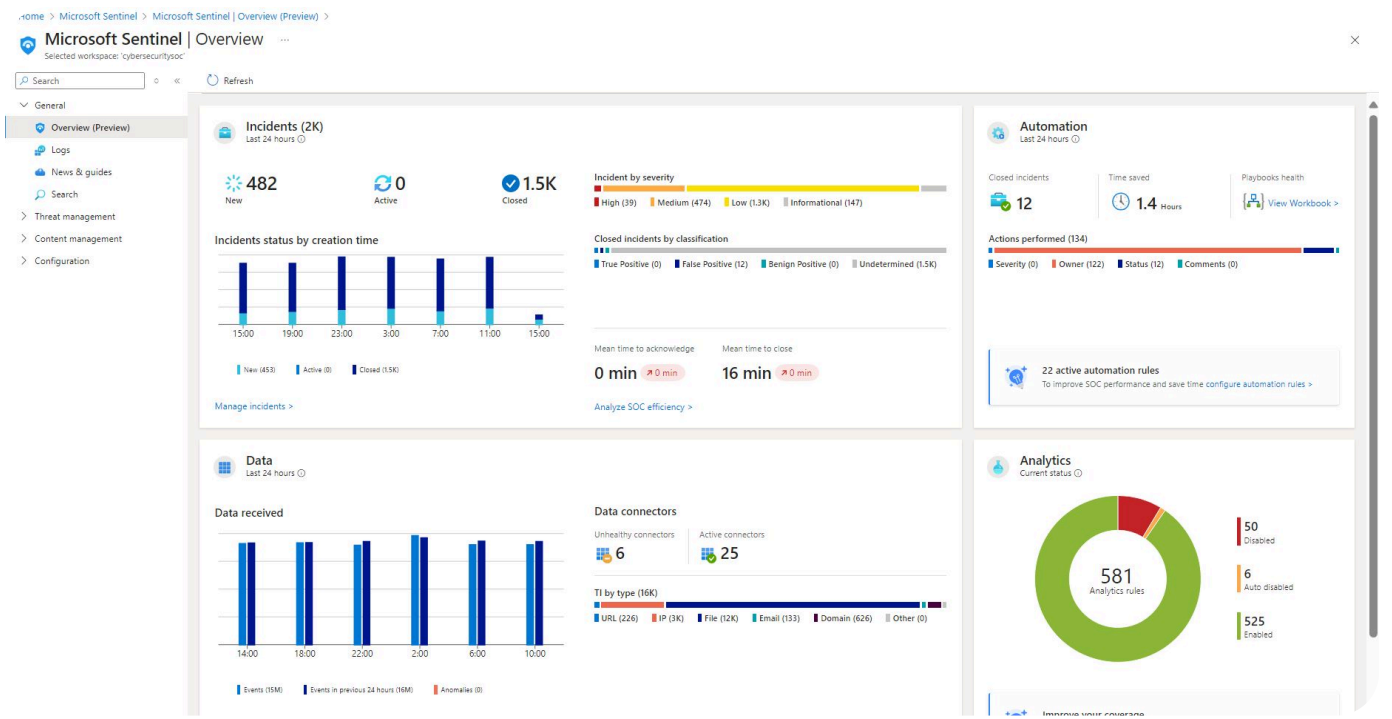
Protection unifiée et corrélée des terminaux, identités et workloads cloud

Défis Pratiques

Compétences validées sur des scénarios d'attaques réels en environnement lab

Made with GAMMA

Microsoft Sentinel



SIEM & SOAR Natif Azure, Sécurité Intelligente à Grande Échelle

- Déploiement et configuration avancée du workspace analytique
- Ingestion centralisée de données depuis des sources multiples et hétérogènes
- Création de règles de détection personnalisées et d'alertes automatisées en temps réel
- Investigation approfondie des incidents et orchestration de la réponse aux menaces

Made with GAMMA

Labs Sentinel Réalisés

Introduction

Prise en main de l'environnement Sentinel et découverte des fonctionnalités clés du SIEM Azure.

Déploiement

Configuration et mise en service du workspace Log Analytics, socle de l'architecture Sentinel.

Ingestion

Connexion et intégration de sources de données multi-environnements via les connecteurs natifs.

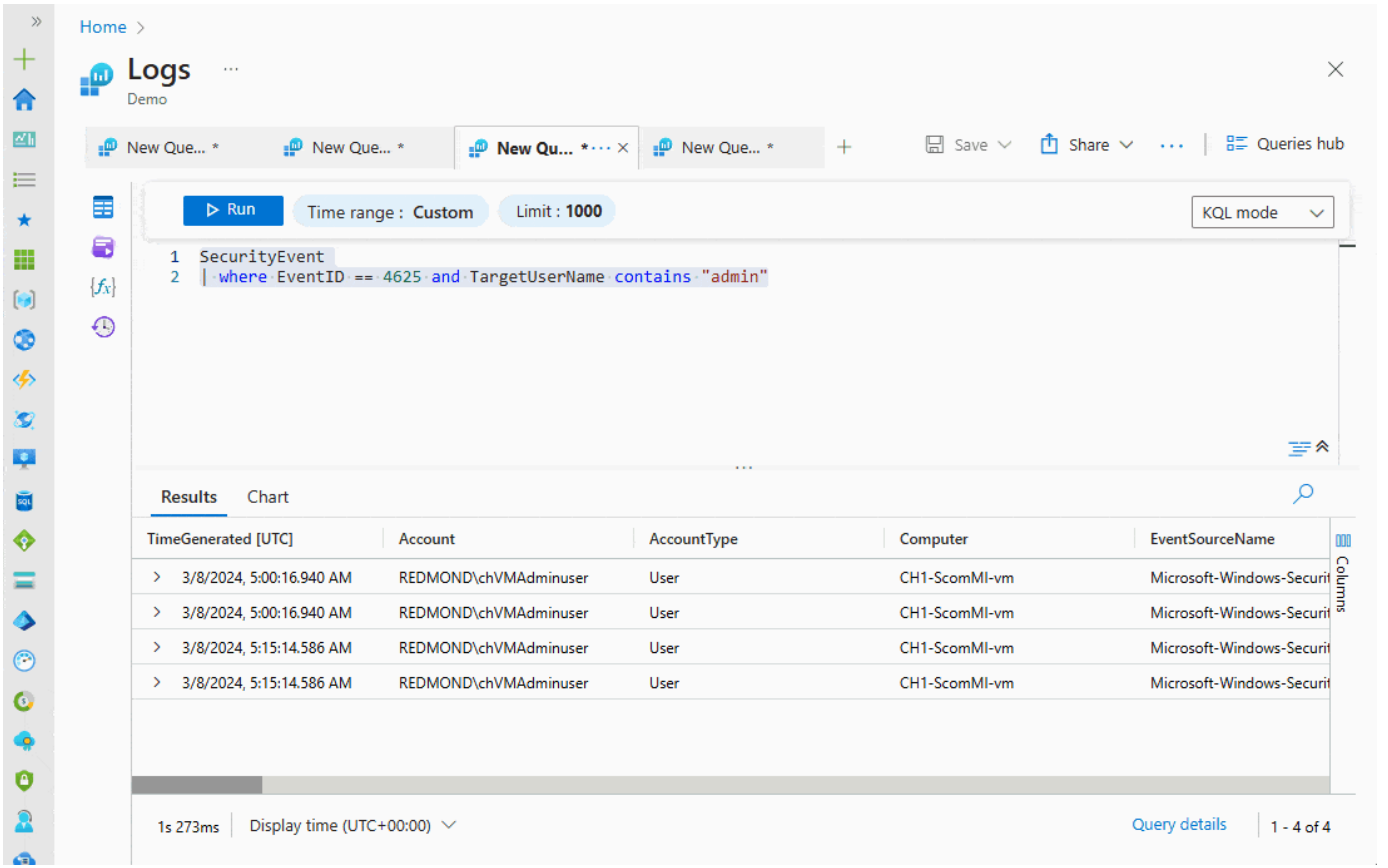
Détection

Création de règles analytiques et de requêtes KQL pour automatiser la détection des menaces.

Enquête

Analyse des incidents de sécurité et orchestration de la réponse grâce aux capacités SOAR.

KQL, Maîtriser l'Analyse des Menaces



Kusto Query Language

- Interroger, filtrer et projeter des données de sécurité avec précision
- Exploiter les jointures et agrégations pour des analyses avancées
- Détecter les anomalies et comportements suspects dans les logs
- Corréler des événements multi-sources pour une investigation approfondie

Labs KQL Réalisés

Introduction à KQL

Maîtrise de la syntaxe fondamentale, des opérateurs clés et de la structure des tables de données

Requêtes de Base

Application du filtrage ciblé, de la projection de données et de l'agrégation pour extraire des indicateurs pertinents

Requêtes Avancées

Exploitation des jointures complexes, sous-requêtes imbriquées et visualisations pour une analyse approfondie des menaces

Microsoft Defender XDR

Une plateforme de protection unifiée contre les menaces avancées, couvrant l'ensemble de la chaîne d'attaque, de l'endpoint jusqu'au cloud.

Défense & Contournement	**Élévation de Privilèges**	**Mouvement Latéral**
Exécution de Code	**Vol de Credentials**	

Labs Defender XDR Complétés

Introduction à XDR

Prise en main de la plateforme Defender XDR et découverte des capacités de détection et réponse unifiées à travers l'ensemble des vecteurs d'attaque.

Défense & Évasion

Analyse des techniques d'évasion antivirus et des mécanismes de défense comportementale pour identifier et contrer les attaques furtives.

Élévation de Privilèges

Exploitation des vulnérabilités et techniques de privilege escalation dans un environnement sécurisé pour comprendre les vecteurs d'attaque critiques.

Mouvement Latéral

Navigation stratégique au sein du réseau et compromission des ressources adjacentes pour simuler les déplacements d'un attaquant persistant.

Exécution de Code

Déploiement et exécution de payloads malveillants avec détection et réponse automatisée pour évaluer les capacités de containment de la plateforme.

Accès aux Credentials

Extraction et exploitation des identifiants pour l'accès persistant aux systèmes critiques, avec analyse des alertes générées par Defender XDR.

Défis de Sécurité Azure

Exploration Sentinel

Prise en main de Microsoft Sentinel et analyse des premières alertes de sécurité

Azure DevSecOps

Intégration de la sécurité dans les pipelines CI/CD et renforcement des pratiques de développement

Détection de Menaces

Identification et analyse proactive des comportements suspects dans l'environnement Azure

Pivotement Azure

Navigation stratégique entre les ressources cloud pour cartographier les vecteurs d'attaque

Exfiltration et Analyse

Détection des tentatives d'exfiltration de données et investigation forensique des incidents

Compétences Maîtrisées

5

Labs Sentinel

Du déploiement complet à la conduite d'enquêtes forensiques

3

Labs KQL

Rédaction de requêtes avancées et analyse proactive des menaces

6

Labs Defender XDR

Simulation de techniques d'attaque et orchestration de la réponse aux incidents

5

Défis Azure

Résolution de scénarios complexes en environnement cloud réel

Pleinement opérationnel pour sécuriser des environnements Azure en production