AYI NEDJIMI Consultants

Microsoft Sentinel : SIEM/SOAR Cloud Microso Azure 2026

10 mai 2026 • Mis à jour le 17 mai 2026 • 19 min de lecture • 3971 mots • 7 vu

Guide entity-first 2026 sur Microsoft Sentinel : SIEM/SOAR cloud-native Azure. Architecture Log Analytics, langage KQL, 200+ data connectors, Analytics Rules (Scheduled, NRT, Fusion), UEBA, hunting Notebooks Jupyt automation Logic Apps, unification Defender XDR, pricing Pay-As-You-Go Commitment Tiers, comparatif vs Splunk, Wazuh, IBM QRadar.

Microsoft Sentinel est la plateforme **SIEM (Security Information and Event Management)** et **SOAR (Security Orchestration, Automation and Response)** cloud native de Microsoft, déployée sur Azure et conçue pour collecter, analyser, détecter répondre aux menaces de sécurité à l'échelle du cloud, de l'on-premise et des environnements hybrides. Lancé en 2019 sous le nom *Azure Sentinel* puis renommé *Microsoft Sentinel* en 2021, le produit s'appuie sur le moteur Azure Log Analytics et langage de requête **KQL (Kusto Query Language)** po s téraoctets logs par jour, corréler des événements provenant de ecteurs nati

(Active Directory, Microsoft 365, AWS, GCP, syslog/CEF, Defender XDR), et orche des réponses automatisées via Azure Logic Apps. En 2024, Microsoft a unifié Sen avec la suite Defender XDR au sein du portail *security.microsoft.com*, créant une plateforme unique de détection et de réponse couvrant identités, endpoints, e-ma applications cloud et infrastructure. Sentinel sert aussi bien les PME via des MSSP qu'aux grands comptes en mode multi-tenant, avec un modèle de facturation à la consommation (Pay-As-You-Go) ou par paliers d'engagement (Commitment Tiers) partir de 100 Go/jour. Ce guide détaille l'architecture, les Analytics Rules, le UEBA, hunting, la tarification, les limites et le positionnement face à Splunk, Wazuh et IBM QRadar.

À RETENIR

L'essentiel à retenir

SIEM/SOAR cloud-native : Microsoft Sentinel est entièrement géré sur Azu sans infrastructure à provisionner, avec scalabilité élastique au pétaoctet.

KQL au cœur : toutes les détections, dashboards et hunts reposent sur Kus Query Language, un dialecte SQL-like optimisé pour les séries temporelles les logs.

200+ data connectors : intégrations natives avec Microsoft 365, Defender, Azure AD, AWS, GCP, Cisco, Palo Alto, Fortinet, et tout flux syslog/CEF/RES

Defender XDR unifié 2024 : Sentinel et Defender XDR partagent désormais un portail unique (security.microsoft.com) pour incidents, hunting et automation.

Réponse sous 24h

Devis gratuit →