



Microsoft Sentinel : SIEM/SOAR Cloud Microsoft Azure 2026



10 mai 2026



Mis à jour le 17 mai 2026



19 min de lecture



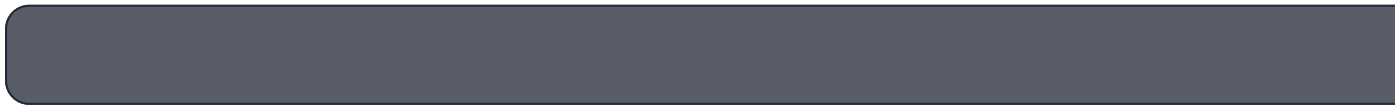
3971 mots



72 vues



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 Jupyter 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 et 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 le langage de requête KQL (Kusto Query Language) pour ingérer des téraoctets de logs par jour, corréler des événements provenant de centaines de connecteurs natifs.

Réponse sous 24h

Devis gratuit →

([Active Directory](#), [Microsoft 365](#), AWS, GCP, syslog/CEF, Defender XDR), et orchestration des réponses automatisées via Azure Logic Apps. En 2024, Microsoft a unifié Sentinel 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-mail, 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) à partir de 100 Go/jour. Ce guide détaille l'architecture, les Analytics Rules, le UEBA, le threat 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 Azure sans infrastructure à provisionner, avec scalabilité élastique au pétaoctet.

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

Un projet cybersécurité ?
Réponse sous 24h

Devis
gratuit →

Réponse sous 24h

Devis
gratuit →