Microsoft Sentinel Avancé 2026 : KQL, SOAR et UEBA

> Microsoft Sentinel 2026 — KQL avancé, règles analytiques, SOAR playbooks, UEBA, multi-workspace et connecteurs personnalisés pour SOC français soumis à NIS 2.

En mars 2025, lors d'une mission de renforcement du SOC d'un opérateur d'importance vitale (OIV) français, notre équipe a découvert que Microsoft Sentinel était déployé depuis 18 mois mais que 90% de ses capacités avancées restaient inexploitées : les règles analytiques par défaut généraient des centaines d'alertes quotidiennes non qualifiées, aucun playbook SOAR n'automatisait la réponse, la fonctionnalité UEBA (User and Entity Behavior Analytics) n'était pas activée, et les logs des systèmes critiques OT n'étaient pas encore intégrés. Résultat : l'équipe SOC passait 70% de son temps à traiter des faux positifs au lieu d'investiguer les vraies menaces. Ce syndrome du "SIEM non configuré" est malheureusement très répandu dans les organisations qui déploient Sentinel pour cocher une case NIS 2 mais sans investir dans sa configuration avancée. Mon opinion est tranchée sur ce point : un Sentinel mal configuré est pire qu'une absence de SIEM, car il crée une fausse sensation de sécurité tout en monopolisant les ressources SOC sur du bruit. Ce guide technique approfondi couvre la configuration avancée de **Microsoft Sentinel** en 2026 : l'écriture de requêtes **KQL** (Kusto Query Language) pour la détection de menaces complexes, la création de règles analytiques personnalisées avec entités et tactiques MITRE ATT&CK, l'automatisation avec les **playbooks SOAR** (Logic Apps), la configuration de l'**UEBA** pour la détection comportementale des utilisateurs et entités, la gestion multi-workspace, et les connecteurs personnalisés pour l'ingestion de sources de logs métier. Destiné aux analystes SOC senior et aux architectes sécurité des organisations françaises sous NIS 2.

À RETENIR

À retenir

• **KQL (Kusto Query Language)** est le langage de requête de Sentinel — maîtriser les opérateurs join, summarize, mv-expand et les fonctions de fenêtre temporelle est indispensable pour des règles de détection efficaces

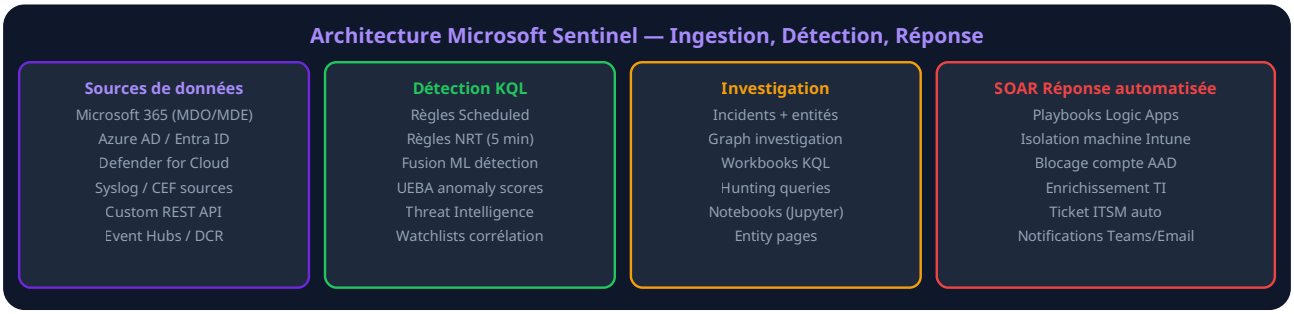
• Les **règles analytiques NRT (Near Real-Time)** de Sentinel permettent une latence de détection inférieure à 5 minutes vs 5-15 minutes pour les règles Scheduled classiques, idéales pour les attaques à progression rapide

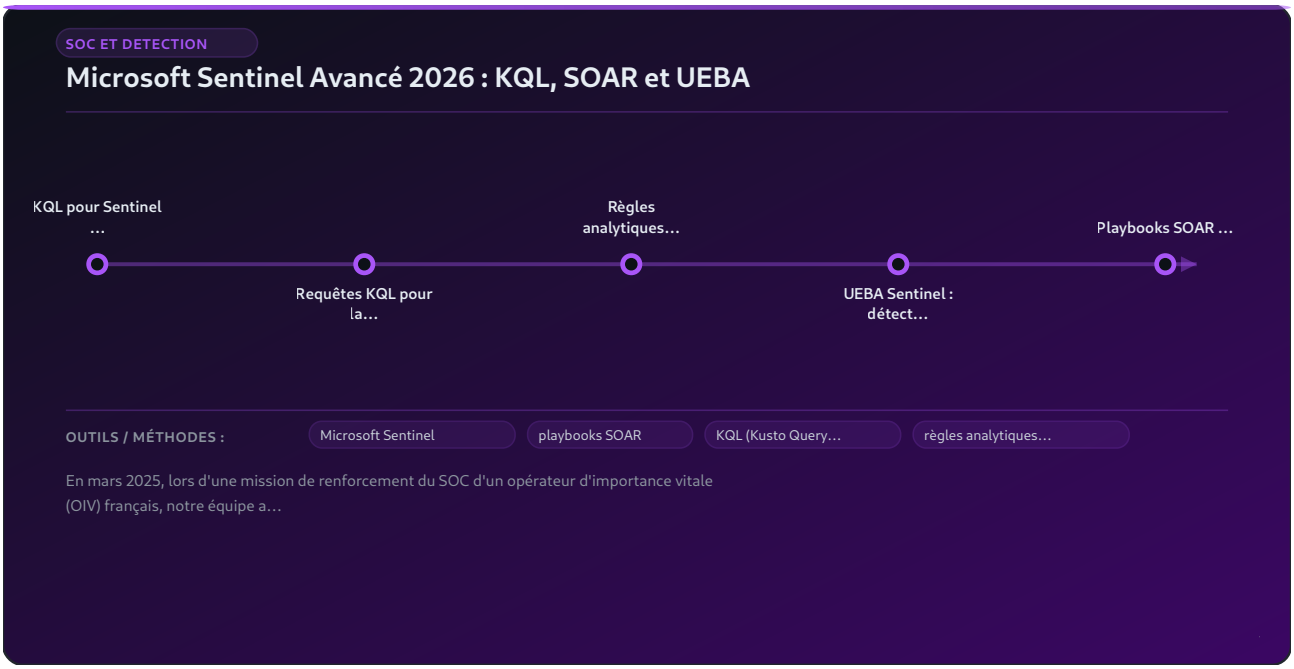
• **UEBA Sentinel** calcule des scores d'anomalie pour les utilisateurs et entités en corrélant les comportements avec des baselines dynamiques — une capacité de détection impossible à reproduire manuellement avec des règles statiques

• Les **playbooks SOAR** (Logic Apps Azure) permettent d'automatiser les réponses aux incidents : enrichissement IOC via Threat Intelligence, isolation d'une machine Intune, désactivation d'un compte AAD, ou création de ticket ServiceNow

• L'architecture **multi-workspace** Sentinel avec un workspace central et des workspaces satellites régionaux ou par BU est la configuration recommandée pour les groupes internationaux soumis à des contraintes de souveraineté des données

• Les **connecteurs de données personnalisés** via l'API REST d'ingestion Sentinel ou via Azure Event Hubs permettent d'intégrer n'importe quelle source de logs métier non couverte par les connecteurs natifs du Content Hub





KQL pour Sentinel : fondamentaux et opérateurs avancés

Le **Kusto Query Language (KQL)** est le langage de requête utilisé par Microsoft Sentinel pour interroger les tables de données dans les workspaces Log Analytics. Contrairement à SQL, KQL est orienté vers l'analyse de séries temporelles de données de sécurité et dispose d'opérateurs spécialisés pour ce cas d'usage. Les opérateurs fondamentaux sont : **where** (filtrage), **project** (sélection de colonnes), **extend** (ajout de colonnes calculées), **summarize** (agrégation), **join** (jointure entre tables), **union** (union de tables), **mv-expand** (expansion de valeurs multiples dans un tableau), et **parse_json** (analyse des champs JSON imbriqués). La maîtrise de ces opérateurs, combinée avec les fonctions de fenêtre temporelle comme `bin(TimeGenerated, 1h)` pour regrouper les événements par heure, est la base de toute règle de détection Sentinel efficace.

Une règle de détection KQL avancée pour la détection d'une attaque BEC (Business Email Compromise) dans Microsoft 365 combine plusieurs tables : `EmailEvents` (événements email Microsoft Defender for Office), `AzureActivity` (activité Azure AD), et `SigninLogs` (connexions utilisateurs). La requête joint ces tables par UPN d'utilisateur pour corréler la réception d'un email de phishing avec une connexion suspecte ultérieure depuis un pays inhabituel, puis avec une règle de redirection d'emails créée dans Outlook — une séquence caractéristique d'un compromis BEC réussi. Ce type de règle multi-table est impossible à écrire sans une bonne

compréhension des opérateurs KQL `join` et des stratégies de performance pour éviter les timeouts sur de grandes tables.

Requêtes KQL pour la détection de menaces complexes

La détection des attaques sophistiquées avec KQL nécessite de penser en termes de **séquences d'événements** plutôt qu'en termes d'événements individuels. L'opérateur **join kind=inner** permet de corréler deux événements liés par un identifiant commun (compte utilisateur, adresse IP, nom de machine) avec une contrainte temporelle via `| where TimeGenerated between(StartTime .. EndTime)`. Pour la détection des mouvements latéraux via Pass-the-Hash (PtH), une requête KQL recherche une séquence d'authentifications Kerberos de type NTLM (Event ID 4624 type 3) depuis un compte machine (`AccountName endswith "$"`) vers plusieurs systèmes cibles dans une fenêtre de 30 minutes — une signature comportementale caractéristique de PtH qui génère très peu de faux positifs dans les environnements d'entreprise.

> ⚡ **Retour terrain**
>
> Dans les SOC que j'accompagne, le principal problème n'est pas le manque d'alertes mais l'excès : 'alert fatigue' systématique, analysts qui désactivent des règles jugées trop bruyantes sans documentation, et faux positifs récurrents qui masquent les vrais incidents. J'ai développé un tableau de bord simple — 3 métriques : taux de faux positifs par règle, MTTD (mean time to detect) sur incidents réels, et ratio alertes/analyst — qui permet en une réunion hebdomadaire de 30 minutes d'identifier les règles à tuner en priorité.

L'opérateur **series_decompose_anomalies** de KQL applique une décomposition en séries temporelles avec détection d'anomalies statistiques basée sur l'algorithme STL (Seasonal-Trend decomposition using Loess). Cette fonction permet de détecter des comportements anormaux

dans des métriques continues comme le volume de transferts de données, le nombre de fichiers accédés par heure, ou le nombre d'authentifications échouées — en comparant automatiquement les valeurs actuelles avec la baseline saisonnière (jour de la semaine, heure de la journée). L'utilisation de `series_decompose_anomalies` dans les règles Sentinel permet de détecter des anomalies contextuelles que les seuils statiques traditionnels manqueraient systématiquement, comme une exfiltration progressive qui augmente graduellement sur 10 jours pour rester sous les seuils d'alerte fixes.

Règles analytiques NRT et Scheduled : configuration optimale

Microsoft Sentinel propose deux types principaux de règles analytiques pour la détection en production. Les **règles Scheduled** s'exécutent à intervalles réguliers définis (de 5 minutes à 24 heures) avec une fenêtre de lookback configurable (jusqu'à 14 jours), permettant la détection de patterns complexes sur de longues périodes mais avec une latence égale à l'intervalle d'exécution. Les **règles NRT (Near Real-Time)**, introduites en 2022, s'exécutent presque en temps réel avec une latence inférieure à 5 minutes dès l'ingestion des données, idéales pour les détections critiques nécessitant une réponse immédiate comme la détection de déploiements de ransomware en cours, d'authentifications depuis des IPs blacklistées connues, ou de creations de comptes administrateurs non autorisées. La limite actuelle des règles NRT est l'absence de support pour certains opérateurs KQL complexes (join, union) et la fenêtre de lookback limitée à 10 minutes.

La configuration des **entités** dans les règles analytiques Sentinel est une étape critique souvent négligée lors de la configuration initiale. Les entités (Account, Host, IP, URL, FileHash, Process, MailMessage, etc.) permettent à Sentinel de relier les alertes individuelles en incidents cohérents via la logique de regroupement d'incidents, et d'alimenter le graphe d'investigation avec des noeuds cliquables. Une règle analytique sans entités correctement configurées génère des incidents "plats" sans contexte graphique, rendant l'investigation beaucoup plus laborieuse pour les analystes SOC. La configuration correcte des entités nécessite de mapper les colonnes KQL appropriées (par exemple, la colonne `AccountName` vers l'entité Account, la colonne `RemoteIP` vers l'entité IP) pour chaque règle, et de configurer les tactiques et techniques MITRE ATT&CK correspondantes pour le suivi de la couverture. La configuration du groupement d'incidents est

également importante : en activant le groupement des alertes partageant les mêmes entités dans une fenêtre temporelle de 5 heures, Sentinel regroupe automatiquement les alertes d'une même attaque multi-étapes en un seul incident, réduisant le nombre d'incidents traités par les analystes et améliorant le contexte de chaque investigation, à condition que le groupement soit configuré avec des fenêtres temporelles et des critères de groupement adaptés à la durée typique des attaques ciblant votre organisation.

UEBA Sentinel : détection comportementale utilisateurs et entités

L'**UEBA (User and Entity Behavior Analytics)** de Microsoft Sentinel analyse les comportements des utilisateurs et des entités (machines, applications, adresses IP) pour établir des baselines comportementales dynamiques et détecter les anomalies statistiquement significatives. Contrairement aux règles de détection basées sur des signatures ou des seuils statiques, l'UEBA détecte les menaces qui se manifestent par des déviations comportementales par rapport à la baseline normale d'un utilisateur spécifique — par exemple, un employé qui accède soudainement à des milliers de documents SharePoint en dehors de ses heures habituelles de travail, ou un compte de service qui commence à se connecter à des machines auxquelles il n'accède jamais habituellement. Ces anomalies sont calculées par des algorithmes de machine learning qui modélisent individuellement le comportement de chaque utilisateur, une capacité impossible à reproduire avec des règles statiques.

L'activation de l'UEBA dans Sentinel nécessite de sélectionner les sources de données à analyser (Azure AD, Active Directory on-premise via Defender for Identity, Microsoft 365, Windows Security Events) et d'attendre la période d'apprentissage initiale de 7 jours pendant laquelle l'UEBA établit les baselines. Les scores d'anomalie UEBA sont accessibles dans les tables `BehaviorAnalytics` et `IdentityInfo` du workspace Sentinel, permettant de les corréler dans des règles KQL personnalisées. Une règle efficace combine un score UEBA élevé (`InvestigationPriority > 5`) avec d'autres signaux de risque comme une connexion depuis un pays inhabituel ou l'utilisation d'un protocole d'authentification legacy (Basic Auth) pour produire des alertes à très haute fidélité avec très peu de faux positifs. Notre service de audit de

sécurité Microsoft 365 inclut une évaluation et activation de l'UEBA Sentinel pour les organisations françaises.

Playbooks SOAR : automatisation de la réponse aux incidents

Les **playbooks SOAR** de Microsoft Sentinel sont des workflows Azure Logic Apps qui s'exécutent automatiquement en réponse à des alertes ou incidents Sentinel, permettant d'automatiser les actions de réponse répétitives : enrichissement d'indicateurs de compromission (IOCs) via des APIs Threat Intelligence, isolation d'une machine compromise via l'API Microsoft Intune, désactivation d'un compte utilisateur compromis via l'API Azure AD, ajout d'une IP malveillante à la liste de blocage du pare-feu, ou création automatique d'un ticket d'incident dans ServiceNow ou Jira. Un playbook SOAR se déclenche en quelques secondes après la création d'une alerte, permettant une réponse initiale automatique bien avant que l'analyste SOC ne prenne connaissance de l'incident — réduisant considérablement le Mean Time To Respond (MTTR).

La création d'un playbook SOAR Sentinel commence par le choix du déclencheur dans Logic Apps : déclencheur basé sur un incident Sentinel (pour les actions sur l'ensemble de l'incident et ses entités) ou déclencheur basé sur une alerte (pour les actions sur une alerte individuelle). Les actions disponibles dans le connecteur Logic Apps Sentinel incluent : ajout de commentaire à l'incident, changement du statut de l'incident, ajout d'un tag, assignation à un analyste, et mise à jour de la sévérité. Combinées avec des actions des connecteurs Azure AD (désactiver compte, révoquer sessions), Microsoft Intune (isoler device), Microsoft Teams (poster notification), et des connecteurs tiers (VirusTotal, AbuseIPDB), ces capabilities permettent de construire des workflows de réponse sophistiqués. Notre service de RSSI externalisé peut concevoir et déployer des playbooks SOAR adaptés aux procédures de réponse aux incidents spécifiques de votre organisation.

Watchlists et Threat Intelligence : corrélation avec les IOCs

Les **Watchlists Sentinel** sont des listes de référence importées dans le workspace Sentinel (au format CSV) et accessibles dans les requêtes KQL via la fonction `_GetWatchlist('nom-watchlist')`. Les cas d'usage les plus courants incluent : liste des adresses IP des VPN d'entreprise autorisés (pour exclure les alertes de connexions VPN légitimes), liste des machines sensibles (DC, jump servers, serveurs OT) pour prioriser les alertes les concernant, liste des comptes de service pour exclure leur comportement automatisé des règles comportementales UEBA, ou encore liste des domaines partenaires légitimes pour filtrer les faux positifs dans les règles de détection d'emails de phishing. Les Watchlists peuvent être mises à jour manuellement via l'interface Sentinel ou automatiquement via l'API REST Watchlist pour synchronisation avec des CMDB ou des bases de données d'actifs externes.

L'intégration de la **Threat Intelligence (TI)** dans Sentinel s'effectue via plusieurs mécanismes : le connecteur natif Microsoft Threat Intelligence qui importe automatiquement les IOCs de Microsoft, les connecteurs TAXII pour importer des feeds TI externes au format STIX 2.0 (comme MISP, Mandiant, Crowdstrike), et l'API REST Sentinel TI pour les IOCs internes. Les IOCs importés dans Sentinel sont stockés dans la table `ThreatIntelligenceIndicator` et peuvent être corrélés avec n'importe quelle table de données via des requêtes KQL utilisant un join sur les adresses IP, les noms de domaine, les URL, ou les hashs de fichiers. Les règles analytiques TI Sentinel font automatiquement ce matching en temps réel, générant des alertes dès qu'un IOC connu apparaît dans les logs ingérés — une capacité de détection basique mais efficace pour les menaces connues publiquement.

Architecture multi-workspace Sentinel : conception et fédération

L'architecture **multi-workspace Sentinel** devient nécessaire pour les organisations multi-entités (groupes avec filiales), les fournisseurs de services managés (MSSP) gérant plusieurs clients, ou les organisations soumises à des contraintes de souveraineté des données qui empêchent la centralisation dans un seul workspace Azure. L'architecture recommandée pour un groupe

international est un workspace Sentinel central pour le SOC groupe avec requêtes cross-workspace, et des workspaces satellites par région ou par filiale pour la conformité RGPD (données clients françaises dans une région Azure France, données allemandes dans une région Germany). Les requêtes KQL cross-workspace utilisent la syntaxe `workspace('workspace-id').TableName` ou la fonction `union workspace('id1').Table, workspace('id2').Table` pour interroger plusieurs workspaces simultanément depuis une seule requête.

La fonctionnalité **Microsoft Sentinel as a service (MSSentinel)** et l'**Azure Lighthouse** permettent aux MSSP de gérer les workspaces Sentinel de leurs clients depuis un seul tenant Azure sans accès direct aux tenants clients. Azure Lighthouse projette les ressources des tenants délégués dans le tenant MSP via des rôles RBAC granulaires, permettant aux analystes SOC du MSSP d'interroger les tables Sentinel des clients, de créer des incidents, de lancer des playbooks SOAR, et de consulter les Workbooks — sans avoir d'identités dans les tenants clients. Pour les groupes français soumis à NIS 2 qui externalisent leur SOC à un MSSP, cette architecture garantit une séparation claire des responsabilités et une auditabilité complète des accès du MSSP aux données de sécurité des clients.

Workbooks Sentinel : dashboards opérationnels et reporting

Les **Workbooks Sentinel** (basés sur Azure Monitor Workbooks) permettent de créer des tableaux de bord interactifs combinant des visualisations KQL (graphiques, tables, métriques) avec des paramètres interactifs (sélecteurs de plage temporelle, filtres par sévérité, par entité). Les templates Workbooks disponibles dans le Content Hub Sentinel couvrent : vue d'ensemble des incidents SOC, couverture MITRE ATT&CK (quelles techniques sont couvertes par les règles analytiques actives), analyse du coût d'ingestion par table et par source (indispensable pour l'optimisation des coûts Sentinel), et vue des entités les plus risquées selon l'UEBA. Les Workbooks peuvent être partagés avec des stakeholders non-techniques (RSSI, direction) via des liens partagés sans accès complet à Sentinel.

La création de Workbooks personnalisés pour le reporting NIS 2 est particulièrement utile pour documenter l'état de la posture de sécurité à intervalles réguliers. Un Workbook de reporting NIS 2 typique inclut : nombre d'incidents critiques/élevés par mois avec temps de résolution moyen,

couverture des systèmes d'information essentiels dans Sentinel (pourcentage des systèmes avec logs ingérés), taux de détection des tests de simulation d'attaque (purple team exercises), et timeline des modifications de configuration Sentinel (nouvelles règles activées, connecteurs ajoutés). Ce type de reporting automatisé réduit considérablement le temps de préparation des audits de conformité NIS 2 et offre une vue objective de la maturité SOC. Notre accompagnement NIS 2 inclut des templates Workbooks de reporting conformité adaptés aux exigences françaises.

Content Hub Sentinel : solutions packagées par technologie

Le **Content Hub Sentinel** (anciennement Azure Sentinel Solutions) est un catalogue de packages de contenu prêts-à-l'emploi pour des technologies spécifiques : chaque solution inclut des connecteurs de données, des règles analytiques préconfigurées, des requêtes de chasse (hunting queries), des Workbooks, et des playbooks SOAR pour une technologie donnée. En 2026, le Content Hub propose plus de 350 solutions couvrant : les équipements réseau (Palo Alto, Fortinet, Check Point, Cisco), les solutions de sécurité (CrowdStrike, SentinelOne, Tenable Nessus), les plateformes Cloud (AWS, GCP via les connecteurs natifs), et les applications métier (SAP, Oracle, Salesforce). L'installation d'une solution Content Hub en un clic déploie automatiquement tous les composants Sentinel correspondants dans le workspace, permettant d'atteindre une couverture de détection significative en quelques heures plutôt qu'en semaines.

Les solutions Content Hub ne sont cependant pas des solutions "set and forget" — elles nécessitent une configuration post-déploiement : ajustement des seuils des règles analytiques aux volumes de données spécifiques de l'organisation, exclusion des entités ou comportements légitimes qui génèrent des faux positifs, et validation que les requêtes KQL des règles correspondent bien aux schémas de données réels ingérés depuis les connecteurs. Un déploiement Content Hub sans phase de tuning génère généralement autant de faux positifs qu'une configuration manuelle non optimisée. Notre approche recommandée est de déployer la solution Content Hub, d'observer le comportement pendant 2 semaines en mode audit, de documenter les faux positifs récurrents, puis d'ajuster les règles concernées via les exclusions KQL appropriées.

Connecteurs de données personnalisés : DCR et REST API

L'ingestion de sources de logs non couvertes par les connecteurs natifs Sentinel s'effectue via deux mécanismes principaux. Le premier est l'**API REST d'ingestion de logs** (anciennement HTTP Data Collector API, maintenant remplacé par l'API Logs Ingestion avec Data Collection Rules) qui permet à n'importe quelle application d'envoyer des logs JSON au workspace Log Analytics via une requête HTTP POST. Le deuxième est l'utilisation d'**Azure Event Hubs** comme intermédiaire : l'application source envoie ses logs à un Event Hub Azure, et un connecteur Sentinel Event Hubs ingère automatiquement ces logs dans une table Log Analytics personnalisée (Custom Log). Les **Data Collection Rules (DCR)** avec les **Data Collection Endpoints (DCE)** constituent l'architecture recommandée en 2026 pour l'ingestion personnalisée, permettant des transformations KQL des données à l'ingestion pour normaliser le schéma avant stockage.

Les cas d'usage des connecteurs personnalisés dans les organisations françaises incluent : ingestion des logs d'accès aux applications métier critiques (ERP SAP, GPAO, outils de supervision OT), des logs des équipements réseau et systèmes industriels ne disposant pas de connecteur Content Hub, des logs des outils de sécurité propriétaires des équipes réseau, et des événements de sécurité provenant d'infrastructures hébergées dans des datacenters privés sans connectivité Azure directe. Pour les *opérateurs d'importance vitale (OIV)* français qui doivent intégrer leurs systèmes OT/SCADA dans leur surveillance de sécurité, les connecteurs CEF (Common Event Format) via des serveurs Syslog relais permettent d'ingérer les logs des équipements industriels Siemens, Schneider Electric, ou Rockwell Automation dans Sentinel sans exposer les réseaux OT à Internet.

Hunting proactif Sentinel : requêtes et notebooks Jupyter

Le **hunting proactif** dans Sentinel consiste à rechercher activement des traces d'attaquants qui seraient passées sous les radars des règles de détection automatisées. Microsoft Sentinel propose un environnement de hunting intégré avec des centaines de requêtes de chasse prédéfinies

organisées par tactique MITRE ATT&CK, que les analystes peuvent exécuter à la demande, modifier, et sauvegarder comme règles analytiques si elles détectent des activités suspectes. Les requêtes de hunting sont généralement plus complexes que les règles analytiques standards et utilisent des opérateurs KQL avancés comme `series_fir` (filtre à réponse impulsionnelle finie pour lissage de séries), `hll_merge` (HyperLogLog pour les comptages approximatifs sur de grandes tables), ou les fonctions de corrélation temporelle comme `scan` (disponible en preview) pour détecter des séquences d'événements ordonnées dans le temps.

Les **Notebooks Jupyter** intégrés à Sentinel (via Azure Machine Learning) permettent aux analystes avancés d'écrire des analyses forensiques et de chasse en Python, avec accès direct aux tables Sentinel via le SDK Python `msticpy` (Microsoft Threat Intelligence Python Security Tools). Les notebooks sont particulièrement utiles pour les analyses complexes nécessitant des bibliothèques Python de machine learning (scikit-learn, TensorFlow), des visualisations avancées (matplotlib, plotly), ou des intégrations avec des APIs externes (Shodan, VirusTotal, MISP). Un notebook de hunting typique pour la détection de C2 via DNS interroge la table `DnsEvents` de Sentinel, applique des algorithmes de détection de Domain Generation Algorithms (DGA) basés sur des modèles de language character-level, et enrichit les domaines suspects via l'API VirusTotal, le tout en Python avec visualisation des résultats dans le notebook lui-même.

Intégration Microsoft Defender XDR : incidents unifiés

L'intégration de **Microsoft Defender XDR** (anciennement Microsoft 365 Defender) avec Sentinel est une configuration critique pour les organisations utilisant l'écosystème Microsoft de bout en bout. Avec l'intégration activée, les incidents Defender XDR — qui agrègent déjà les alertes de Microsoft Defender for Endpoint (MDE), Defender for Identity (MDI), Defender for Office 365 (MDO), et Defender for Cloud Apps (MDA) — sont automatiquement créés comme incidents Sentinel avec toutes leurs alertes constituantes et leurs entités. La table `SecurityIncident` de Sentinel contient les métadonnées des incidents XDR, et la table `SecurityAlert` contient les alertes individuelles avec leurs preuves brutes, permettant des corrélations KQL entre les incidents XDR et les données d'autres sources non-Microsoft ingérées dans Sentinel.

L'**Advanced Hunting** de Microsoft Defender XDR et les requêtes KQL de Sentinel utilisent maintenant le même langage de requête et des schémas de tables similaires (le schéma XDR Advanced Hunting), mais des tables différentes : les tables Advanced Hunting XDR (`DeviceProcessEvents`, `EmailEvents`, `IdentityLogonEvents`) ont une rétention de 30 jours et une latence quasi-temps réel, tandis que les tables Sentinel Log Analytics ont une rétention configurable jusqu'à 2 ans et une latence d'ingestion de quelques minutes. La stratégie recommandée est d'utiliser Advanced Hunting XDR pour les investigations actives en temps réel sur les 30 derniers jours, et Sentinel pour les corrélations historiques, la gestion des incidents à long terme, et l'intégration avec les sources non-Microsoft. Notre guide Microsoft 365 Security détaille cette stratégie d'intégration optimale entre XDR et Sentinel.

Optimisation des coûts Sentinel : commitment tiers et archivage

Les coûts de Microsoft Sentinel peuvent rapidement devenir significatifs pour les organisations avec des volumes d'ingestion élevés. Le modèle de tarification Sentinel se compose de deux parties : le coût d'ingestion Log Analytics (environ 2,50 USD/GB en Pay-as-you-go en région France) et le coût Sentinel lui-même (environ 2,46 USD/GB en PAYG). Les **Commitment Tiers** Log Analytics (100 GB/jour, 200 GB/jour, etc.) offrent des réductions allant jusqu'à 70% par rapport au tarif PAYG pour les engagements fermes sur 31 jours, réduisant considérablement la facture pour les organisations avec des volumes d'ingestion prévisibles. La fonctionnalité **Basic Logs** (1 USD/GB) permet d'ingérer des données peu utilisées pour la détection (logs DNS détaillés, logs de pare-feu volumineux) à un coût réduit, avec une fonctionnalité de recherche KQL à la demande facturée séparément.

L'**archivage Sentinel** permet de conserver les données de sécurité jusqu'à 12 ans à un coût très faible (environ 0,023 USD/GB/mois) après la période de rétention interactive (jusqu'à 2 ans). Les données archivées ne sont pas directement requêtables via KQL standard mais nécessitent l'utilisation de la fonctionnalité "Search Jobs" qui exécute des requêtes asynchrones sur les archives avec des résultats disponibles en quelques minutes à quelques heures selon le volume de données analysées, ou la restauration temporaire vers un espace de travail "chaud" pour investigation approfondie avec requêtes KQL standard. Pour la conformité NIS 2 française qui

requiert la conservation des logs de sécurité pendant une durée suffisante pour les investigations post-incident, l'archivage Sentinel offre une solution économique et conforme pour répondre aux exigences réglementaires sans maintenir de coûteuses infrastructures de stockage de logs on-premise ou en recourant à des solutions SIEM hybrides complexes. Notre service de diagnostic NIS 2 évalue vos besoins de rétention des logs et calcule le coût optimal Sentinel pour votre organisation.

Intégration SOC : ITSM, ticketing et procédures d'escalade

L'intégration de Sentinel dans les processus ITSM (IT Service Management) de l'organisation est une étape fondamentale pour l'industrialisation du SOC. Les connecteurs ITSM natifs de Sentinel supportent **ServiceNow**, **Jira Service Management**, et **Remedy BMC** pour la création automatique de tickets d'incident ITSM dès qu'un incident Sentinel est créé, avec synchronisation bidirectionnelle du statut (un ticket fermé dans ServiceNow ferme automatiquement l'incident Sentinel correspondant et vice versa). Cette intégration permet aux équipes IT opérationnelles de travailler dans leurs outils ITSM habituels sans avoir à accéder directement à Sentinel, tout en maintenant la traçabilité complète des actions dans les deux systèmes pour les audits de conformité.

Pour les organisations françaises soumises à NIS 2 qui doivent notifier l'ANSSI dans les 24 heures suivant la détection d'un incident significatif, l'intégration Sentinel-ITSM permet de générer automatiquement un pre-rempli du formulaire de notification avec les informations extraites de l'incident Sentinel : systèmes affectés (entités de l'incident), première détection, vecteur d'attaque présumé (tactiques MITRE ATT&CK de l'incident), et impact estimé. Cette automatisation réduit considérablement le délai entre la détection de l'incident et la notification réglementaire, critiquement important dans les premières 24 heures d'un incident majeur. Notre service de RSSI externalisé inclut la mise en place de ces workflows de notification NIS 2 automatisés intégrés à Sentinel pour garantir le respect des délais réglementaires.

Fonctionnalité Sentinel	Type	Latence détection	Cas d'usage principal
Règles NRT	Détection	<5 minutes	Menaces critiques temps réel
Règles Scheduled	Détection	5 min – 24h	Patterns complexes multi-tables
UEBA	Comportemental	Quotidien	Insider threats, compromis comptes
Fusion ML	ML correlation	Horaire	Attaques multi-étapes corrélées
TI Matching	IOC matching	<15 minutes	IOCs publics connus
Playbooks SOAR	Automatisation	Secondes	Réponse automatique incidents
Hunting Notebooks	Proactif	Manuel	Investigation approfondie

Couverture MITRE ATT&CK dans Sentinel : mesure et amélioration

La couverture du framework **MITRE ATT&CK** par les règles analytiques Sentinel est une métrique essentielle pour évaluer et communiquer l'efficacité de la détection SOC. Le Workbook "MITRE ATT&CK Coverage" du Content Hub Sentinel visualise automatiquement quelles techniques ATT&CK sont couvertes par les règles analytiques actives dans le workspace, en les mappant sur la matrice ATT&CK Enterprise. Chaque règle analytique Sentinel doit être configurée avec les tactiques et techniques MITRE ATT&CK correspondantes (champs "Tactics" et "Techniques" dans la configuration de la règle) pour que ce mapping soit précis. L'objectif recommandé pour les SOC des organisations sous NIS 2 est une couverture des techniques ATT&CK les plus utilisées dans les attaques ciblant leur secteur, documentées par les rapports de threat intelligence de l'ANSSI et du CERT-FR.

La documentation des techniques ATT&CK non couvertes par les règles Sentinel existantes génère un *gap analysis ATT&CK* qui priorise les efforts de développement de nouvelles règles. La communauté open-source SigmaHQ maintient plus de 3 000 règles de détection au format Sigma — un format de règles de détection générique indépendant de la plateforme SIEM — avec des convertisseurs vers KQL pour Sentinel. Ces règles Sigma constituent un excellent point de départ pour combler les gaps de couverture ATT&CK, en adaptant les requêtes KQL générées

aux spécificités du schéma de données Sentinel de votre organisation. L'intégration des règles Sigma dans un pipeline CI/CD permet de maintenir les règles Sentinel synchronisées avec les nouvelles techniques publiées par la communauté ATT&CK.

Règles d'automatisation Sentinel : orchestration des incidents

Les **règles d'automatisation Sentinel** (Automation Rules) sont distinctes des playbooks SOAR et constituent la couche d'orchestration des incidents. Elles s'exécutent instantanément dès la création ou la modification d'un incident et permettent de : modifier le statut et la sévérité d'un incident selon des conditions (par exemple, passer en "Fermé - Faux positif" les incidents impliquant des IPs connues des systèmes de monitoring), assigner automatiquement les incidents à des analystes selon la sévérité ou la tactique MITRE (les incidents Ransomware assignés à l'équipe Tier 3), ajouter des tags de classification automatique (tag "OIV" pour les incidents impliquant des machines des systèmes critiques), et déclencher des playbooks SOAR conditionnellement. Les règles d'automatisation s'exécutent dans l'ordre de leur priorité définie, permettant de construire des workflows d'orchestration sophistiqués.

Un cas d'usage concret de règle d'automatisation pour les SOC français : une règle qui détecte les incidents Sentinel impliquant des entités machines appartenant à la liste de surveillance "Systèmes NIS 2 essentiels" (via une Watchlist Sentinel), augmente automatiquement leur sévérité à "Critique" quel que soit la sévérité initiale de la règle analytique, assigne l'incident à l'équipe RSSI, et déclenche un playbook SOAR qui envoie une notification Teams au canal d'astreinte de sécurité avec un résumé de l'incident. Cette automatisation garantit qu'aucun incident concernant les systèmes essentiels NIS 2 ne passe inaperçu ou ne reste dans la file d'attente des incidents standards trop longtemps. La documentation complète des règles d'automatisation Sentinel est disponible sur learn.microsoft.com.

Normalisation ASIM : schéma unifié pour toutes les sources

L'**ASIM (Advanced Security Information Model)** est le schéma de normalisation des données de Sentinel qui standardise les champs des événements de sécurité quelle que soit leur source d'origine. Par exemple, les événements d'authentification (login/logout) provenant de Windows, Linux, Azure AD, Okta, Cisco ISE, ou AWS sont tous normalisés dans le schéma ASIM Authentication avec les mêmes noms de champs : `TargetUsername` (au lieu de `AccountName`, `UserPrincipalName`, `user` selon la source), `SrcIpAddr` pour l'adresse IP source, `EventResult` pour le succès/échec. Les règles analytiques KQL écrites avec les parsers ASIM fonctionnent automatiquement sur toutes les sources supportées sans modification, simplifiant considérablement la maintenance des règles dans un environnement multi-sources.

La liste des parsers ASIM disponibles et des tables de schéma normalisé inclut : Authentication (im_Authentication), DNS (im_DNS), NetworkSession (im_NetworkSession), Process (im_Process), FileEvent (im_FileEvent), WebSession (im_WebSession), et Registry (im_Registry). L'utilisation des parsers ASIM dans les règles analytiques est fortement recommandée pour toute nouvelle règle car elle garantit la portabilité : si une nouvelle source de logs est ajoutée (par exemple, un équipement réseau d'un nouveau fournisseur), ses événements sont automatiquement couverts par toutes les règles ASIM existantes sans modification. Ce point est particulièrement important pour les organisations qui font évoluer leur parc technologique fréquemment ou qui intègrent de nouvelles filiales avec des infrastructures hétérogènes dans leur périmètre Sentinel.

Notebooks Sentinel et msticpy : analyse Python avancée

La librairie Python **msticpy (Microsoft Threat Intelligence Python Security Tools)** est la bibliothèque officielle Microsoft pour l'analyse de sécurité dans les notebooks Jupyter intégrés à Sentinel. Elle fournit des classes Python pour : l'interrogation des tables Sentinel via KQL (`qry_prov.query()`), l'enrichissement d'indicateurs via des API tierces (VirusTotal, OTX AlienVault, Shodan, AbuseIPDB), l'analyse d'entités réseau (résolution DNS inverse,

géolocalisation IP, réputation domaine), la visualisation de timelines d'incidents (`nbwidgets.SelectItem`), et l'analyse de processus suspects via des algorithmes de clustering. Les notebooks msticpy permettent aux analystes SOC senior de construire des analyses forensiques répétables et partageables, documentées et versionnées dans Azure Machine Learning ou GitHub.

Un exemple concret d'analyse msticpy dans un notebook Sentinel : détection de C2 via analyse des requêtes DNS. Le notebook interroge la table `DnsEvents` de Sentinel sur les 7 derniers jours (`qry_prov.Network.dns_lookups()`), extrait les domaines avec un score Shannon d'entropie élevé (indicateur de DGA — Domain Generation Algorithms utilisés par les malwares pour contacter leur C2), filtre les domaines non connus des bases de réputation (VirusTotal 0/80 détections), et visualise les résultats dans un graphe de réseau montrant les machines qui ont contacté ces domaines suspects. Ce type d'analyse hunting approfondie est impossible avec les règles KQL standards mais facile à implémenter avec quelques dizaines de lignes Python msticpy. Notre service Microsoft 365 Security avancée inclut des notebooks msticpy personnalisés pour les analyses de chasse spécifiques à votre environnement.

Questions fréquentes sur Microsoft Sentinel

Quelle est la différence entre Microsoft Sentinel et Microsoft Defender XDR ?

Microsoft Defender XDR est un XDR (Extended Detection and Response) natif Microsoft qui agrège les alertes des produits Defender (MDE, MDI, MDO, MDA) avec une corrélation automatisée et un panneau unique. Sentinel est un SIEM cloud complet capable d'ingérer des sources de données de n'importe quel éditeur (Palo Alto, AWS, Okta, etc.) et de créer des règles de détection personnalisées en KQL. Les deux sont complémentaires et sont maintenant intégrés via le portail Defender unifié : XDR pour la détection Microsoft native, Sentinel pour la corrélation étendue et la conformité long terme.

Combien coûte Microsoft Sentinel pour une organisation de 500 utilisateurs ?

Pour une organisation de 500 utilisateurs Microsoft 365, un volume d'ingestion typique est entre 5 et 15 GB/jour selon les sources activées. Avec un Commitment Tier 10 GB/jour (environ 1 300 USD/mois en région France pour Log Analytics + Sentinel combinés), le coût annuel est environ 15 000-20 000 EUR. Ce coût est souvent partiellement couvert par les licences Microsoft 365 E5 Security qui incluent 5 MB/utilisateur/jour d'ingestion Sentinel gratuite pour les données Microsoft natives.

Comment migrer depuis Splunk ou QRadar vers Microsoft Sentinel ?

Microsoft propose des guides de migration officiels et un outil de conversion de règles SPL (Splunk) vers KQL. La migration se décompose en : inventaire des règles existantes et classification par priorité, re-écriture des règles critiques en KQL (les règles basiques sont souvent convertibles automatiquement), migration des sources de données en parallèle avec la phase de configuration et de tuning Sentinel, période de run-in-parallel de 4-8 semaines pour valider l'équivalence de couverture, puis coupure de l'ancien SIEM. La phase la plus délicate est le tuning des règles KQL pour correspondre aux volumes et aux patterns spécifiques de l'environnement cible.

L'UEBA de Sentinel peut-elle remplacer une solution DLP ?

Non, l'UEBA Sentinel et les solutions DLP (Data Loss Prevention) ont des périmètres complémentaires mais distincts. L'UEBA détecte les anomalies comportementales des utilisateurs (volume anormal d'accès, accès depuis des géolocalisations inhabituelles, téléchargements massifs) mais ne peut pas bloquer les actions en temps réel. Les solutions DLP comme Microsoft Purview analysent le contenu des données pour détecter des informations sensibles spécifiques (numéros de cartes, données de santé) et peuvent bloquer activement les transferts. En pratique, les alertes UEBA Sentinel sur des comportements suspects d'accès aux données peuvent déclencher des playbooks SOAR qui activent temporairement des politiques DLP plus restrictives.

Sentinel est-il certifié pour les OIV français ?

Microsoft Sentinel hébergé dans les régions Azure France Centre et France Sud bénéficie des certifications ISO 27001, SOC 2 Type II, et HDS (Hébergeur de Données de Santé) pour les données de santé. Pour les OIV soumis à la LPM (Loi de Programmation Militaire), l'ANSSI recommande de vérifier les conditions spécifiques d'utilisation des solutions cloud pour le traitement des données sensibles des systèmes d'information d'importance vitale (SIIV), notamment via le référentiel SecNumCloud. En 2026, Microsoft travaille activement à l'obtention de la qualification SecNumCloud pour ses services Azure France.

Comment mesurer le ROI d'un déploiement Microsoft Sentinel ?

Le ROI de Sentinel se mesure principalement par la réduction du Mean Time to Detect (MTTD) et du Mean Time to Respond (MTTR), la réduction des heures analyste passées sur les faux positifs après tuning, et l'évitement de coûts d'incident. Une étude Forrester TEI commandée par Microsoft montre un ROI de 201% sur 3 ans pour les organisations ayant correctement déployé et configuré Sentinel, avec une réduction de 70% du temps d'investigation grâce aux playbooks SOAR et à l'investigation graphique des incidents.

Accompagnement Microsoft Sentinel : déploiement et optimisation SOC

La configuration avancée de Microsoft Sentinel — règles KQL performantes, UEBA, playbooks SOAR industrialisés, architecture multi-workspace optimisée — représente un projet d'envergure de 3 à 6 mois pour une organisation de taille moyenne, nécessitant des compétences rares et pointues en KQL avancé, en architecture Azure, et en opérations SOC mature. Notre service de RSSI externalisé propose un accompagnement complet du déploiement Sentinel initial jusqu'à l'optimisation continue, incluant la rédaction des règles analytiques adaptées à votre environnement, la création des playbooks SOAR pour vos procédures de réponse, et la formation des analystes SOC à KQL et à l'investigation Sentinel.

Pour évaluer la maturité de votre déploiement Sentinel actuel ou préparer une migration depuis un SIEM existant, démarrez par notre diagnostic NIS 2 qui évalue votre couverture de surveillance de sécurité et identifie les lacunes prioritaires à combler rapidement. Notre service de pentest Active Directory peut également fournir des règles KQL spécifiques et testées pour détecter les techniques d'attaque AD les plus utilisées, basées sur nos retours d'expérience concrets d'attaques réelles sur des environnements Windows similaires au vôtre.

© Ayi NEDJIMI Consultants — Tous droits réservés