AYI NEDJIMI Consultants

Threat Hunting Microsoft 365 | Guide Microsoft 365

Catégorie : Microsoft 365 Lecture : 8 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Guide expert du threat hunting dans Microsoft 365 : utilisation de Defender XDR et Sentinel, requêtes KQL avancées, chasse aux menaces proactive et...

Cette analyse detaillee de Threat Hunting Microsoft 365 s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

Cette analyse technique de Threat Hunting Microsoft 365 s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels.

1 Fondamentaux du Threat Hunting dans Microsoft 365

Le threat hunting, ou chasse aux menaces, représente une approche proactive de la cybersécurité qui va au-delà de la simple détection automatisée. Dans l'écosystème Microsoft 365, cette discipline prend une dimension particulière en raison de la richesse des données disponibles et de la complexité des environnements hybrides. Le threat hunting s'appuie sur l'hypothèse fondamentale que des menaces poussées ont déjà pénétré le système et évoluent discrètement.

🎯 Objectifs du Threat Hunting

- • **Détection Proactive :** Identifier les menaces avant qu'elles ne causent des dommages
- • **Réduction du Dwell Time :** Diminuer le temps de persistance des attaquants
- • **Amélioration des Défenses :** Enrichir les règles de détection automatisée
- • **Intelligence des Menaces :** Comprendre les TTPs (Tactics, Techniques, Procedures)
- • **Validation des Contrôles :** Tester l'efficacité des mesures de sécurité

Référence du Hunting Moderne

Le threat hunting moderne s'éloigne des approches traditionnelles basées sur les signatures pour adopter une méthode centrée sur les comportements et les anomalies. Cette évolution est particulièrement pertinente dans Microsoft 365, où les menaces exploitent souvent des fonctionnalités légitimes de manière malveillante.

🔍 Hunting Hypothétique

Formulation d'hypothèses basées sur les TTPs connus et les renseignements de menaces

- • Hypothèses MITRE ATT&CK
- • Scénarios d'attaque probables
- • Patterns de comportement suspects

📊 Hunting Analytique

Utilisation de l'analyse statistique et de l'apprentissage automatique pour identifier les anomalies

- • Analyse des écarts statistiques
- • Détection d'outliers
- • Machine learning supervisé/non-supervisé

🤖 Hunting Assisté par IA

Exploitation des capacités d'intelligence artificielle pour guider et automatiser la chasse

- • UEBA (User Entity Behavior Analytics)
- • Corrélation d'événements intelligente
- • Recommandations contextuelles

🔄 Cycle de Vie du Threat Hunting

1. Préparation et Renseignement
Collecte de renseignements sur les menaces, analyse du contexte organisationnel, définition des hypothèses de chasse

2. Identification des Hypothèses
Formulation de scenarii d'attaque basés sur les TTPs observés et les vulnérabilités connues

3. Collecte et Analyse des Données
Extraction et corrélation des logs provenant de tous les services Microsoft 365

4. Investigation et Validation
Approfondissement des anomalies détectées et validation des hypothèses

5. Réponse et Remédiation
Actions correctives immédiates et amélioration des défenses

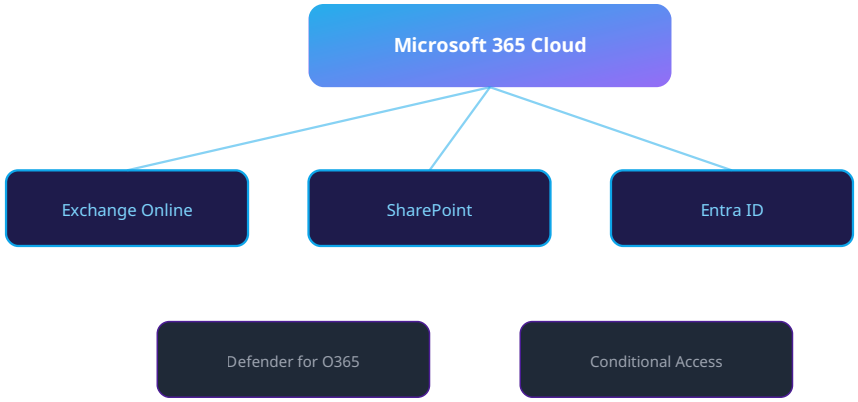
6. Documentation et Apprentissage
Capitalisation des connaissances et enrichissement des règles de détection

📈 Métriques de Performance

Mean Time to Detection (MTTD) < 24h
False Positive Rate < 5%
Hypothèses validées > 15%
Couverture MITRE ATT&CK > 70%

🛠️ Outils et Plateformes

- **Microsoft Defender XDR :** Corrélation cross-domain
- **Microsoft Sentinel :** SIEM et orchestration
- **KQL (Kusto) :** Langage de requête avancé
- **PowerShell & Graph API :** Automatisation
- **MITRE ATT&CK Navigator :** Mapping TTPs



Architecture Microsoft 365 - Services et securite

2 Microsoft Defender XDR - Plateforme Unifiée

🛡️ Architecture Microsoft Defender XDR

Microsoft Defender XDR (eXtended Detection and Response) représente l'évolution naturelle des solutions de sécurité Microsoft vers une approche unifiée de détection et de réponse aux menaces. Cette plateforme intègre nativement les données provenant de tous les composants de l'écosystème Microsoft 365, offrant une vue holistique des activités suspectes et des campagnes d'attaque avancées.

🎯 Composants Intégrés

Defender for Identity

Surveillance des environnements Active Directory on-premises et hybrides, détection des attaques par identité

Defender for Office 365

Protection avancée contre les menaces email, collaboration Teams et SharePoint

Defender for Endpoint
Sécurité des terminaux avec EDR avancé et threat hunting intégré

Defender for Cloud Apps
CASB pour la visibilité et le contrôle des applications cloud et SaaS

⚡ Capacités Avancées

🔗 Corrélation Cross-Domain
Analyse des patterns d'attaque traversant plusieurs services et vecteurs d'entrée

🤖 IA et Machine Learning
Détection comportementale basée sur l'analyse des signaux Microsoft globaux

⚡ Réponse Automatisée
Actions de remédiation coordonnées à travers tous les domaines de sécurité

📊 Threat Analytics
Renseignements contextuels et évaluation de l'exposition aux menaces émergentes

Requête KQL : Détection d'activité suspecte cross-domain

```
// Corrélation d'événements suspects à travers Defender XDR
let suspiciousTimeframe = 1h;
let riskThreshold = 5;

// 1. Utilisateurs avec connexions à risque (Identity)
let riskySignins =
    SigninLogs
    | where TimeGenerated > ago(suspiciousTimeframe)
    | where RiskLevelDuringSignIn == "high" or RiskLevelAggregated == "high"
    | summarize RiskySignins = count(),
                Countries = dcount(LocationDetails.countryOrRegion),
                IPs = dcount(IPAddress)
              by UserPrincipalName
    | where RiskySignins >= 3 or Countries >= 2;

// 2. Activité email anormale (Office 365)
let suspiciousEmail =
    EmailEvents
    | where TimeGenerated > ago(suspiciousTimeframe)
    | where ThreatTypes has_any ("Malware", "Phish", "HighConfPhish")
    | summarize SuspiciousEmails = count(),
                ExternalRecipients = dcountif(RecipientEmailAddress,
RecipientEmailAddress !contains "contoso.com")
              by SenderFromAddress
    | where SuspiciousEmails >= 5 or ExternalRecipients >= 10;

// 3. Activités fichiers suspectes (Cloud Apps)
let suspiciousFiles =
    CloudAppEvents
    | where TimeGenerated > ago(suspiciousTimeframe)
    | where ActionType in ("FileDownloaded", "FileUploaded", "FileShared")
    | where RawEventData.FileSizeBytes > 100000000  // > 100MB
    | summarize LargeFileOps = count(),
                UniqueFiles = dcount(ObjectName),
                DataVolume = sum(todouble(RawEventData.FileSizeBytes))
              by AccountDisplayName
    | where LargeFileOps >= 20 or DataVolume >= 1000000000;  // > 1GB

// 4. Détections endpoint critiques (Defender for Endpoint)
let endpointThreats =
    DeviceEvents
    | where TimeGenerated > ago(suspiciousTimeframe)
    | where ActionType has_any ("ProcessCreated", "FileCreated", "NetworkConnectionSeen")
    | where ProcessCommandLine has_any ("powershell", "cmd", "wscript", "rundll32")
    | where ProcessCommandLine contains "-enc" or ProcessCommandLine contains "IEX"
    | summarize SuspiciousProcesses = count(),
                UniqueCommands = dcount(ProcessCommandLine)
              by DeviceName, AccountName
    | where SuspiciousProcesses >= 5;

// 5. Corrélation et scoring final
riskySignins
| join kind=fullouter (
    suspiciousEmail | project-rename UserPrincipalName = SenderFromAddress
) on UserPrincipalName
| join kind=fullouter (
    suspiciousFiles | project-rename UserPrincipalName = AccountDisplayName
) on UserPrincipalName
| join kind=fullouter (
    endpointThreats | project-rename UserPrincipalName = AccountName
) on UserPrincipalName
| extend RiskScore =
```

```
    (iif(isnotempty(RiskySignins), RiskySignins * 2, 0)) +
    (iif(isnotempty(SuspiciousEmails), SuspiciousEmails, 0)) +
    (iif(isnotempty(LargeFileOps), LargeFileOps / 5, 0)) +
    (iif(isnotempty(SuspiciousProcesses), SuspiciousProcesses * 3, 0))
| extend ThreatIndicators = pack_array(
    iif(isnotempty(RiskySignins), "Risky SignIn", ""),
    iif(isnotempty(SuspiciousEmails), "Suspicious Email", ""),
    iif(isnotempty(LargeFileOps), "Data Exfiltration", ""),
    iif(isnotempty(SuspiciousProcesses), "Malicious Process", "")
)
| where RiskScore >= riskThreshold
| project-away UserPrincipalName1, UserPrincipalName2, UserPrincipalName3
| sort by RiskScore desc
| limit 50
```

🎯 Hunting avec Advanced Hunting

La fonctionnalité Advanced Hunting de Defender XDR offre un environnement de requête KQL puissant permettant d'explorer jusqu'à 30 jours de données brutes. Cette capacité transforme le threat hunting de réactif à proactif, permettant aux analystes de formuler et tester des hypothèses complexes.

📊 Tables de Données

- • **DeviceEvents :** Activités endpoint
- • **EmailEvents :** Événements messagerie
- • **CloudAppEvents :** Apps cloud/SaaS
- • **IdentityLogonEvents :** Authentifications
- • **AlertInfo :** Alertes consolidées

🔍 Capacités de Recherche

- • Requêtes sur 30 jours de données
- • Corrélation temporelle avancée
- • Fonctions d'agrégation complexes
- • Visualisations intégrées
- • Export et partage de requêtes

⚙️ Automatisation

- • Requêtes programmées
- • Règles de détection personnalisées
- • API d'intégration
- • Webhooks et notifications
- • Playbooks de réponse

🧪 Exemples de Requêtes de Hunting

Détection de Lateral Movement

```
// Détection de mouvements latéraux via authentification
IdentityLogonEvents
| where TimeGenerated > ago(24h)
| where LogonType == "Network"
| where ActionType == "LogonSuccess"
| summarize
    LogonCount = count(),
    DistinctComputers = dcount(DestinationDeviceName),
    ComputerList = make_set(DestinationDeviceName)
  by AccountName, AccountDomain
| where DistinctComputers >= 5  // Plus de 5 machines différentes
| where LogonCount >= 20       // Plus de 20 authentifications
| sort by LogonCount desc
```

Hunting des Living-off-the-Land Attacks

```
// Détection d'abus d'outils légitimes (LOLBAS)
DeviceProcessEvents
| where TimeGenerated > ago(7d)
| where ProcessCommandLine has_any (
    "certutil", "bitsadmin", "regsvr32", "rundll32",
    "mshta", "wmic", "forfiles", "pcalua"
)
| where ProcessCommandLine has_any (
    "http://", "https://", "ftp://", "-decode",
    "-encode", "/c ", "/k ", "javascript:", "vbscript:"
)
| extend SuspiciousIndicators = pack_array(
    iif(ProcessCommandLine contains "http", "HTTP_URL", ""),
    iif(ProcessCommandLine contains "-decode", "DECODE_FUNCTION", ""),
    iif(ProcessCommandLine contains "javascript:", "JAVASCRIPT_EXEC", "")
)
| project TimeGenerated, DeviceName, AccountName, ProcessCommandLine, SuspiciousIndicators
| sort by TimeGenerated desc
```

Element	Description	Priorite
Prevention	Mesures proactives de reduction de la surface d'attaque	Haute
Detection	Surveillance et alerting en temps reel	Haute
Reponse	Procedures d'incident response et remediation	Critique
Recovery	Plan de reprise et continuite d'activite	Moyenne

Notre avis d'expert

La prévention de fuite de données (DLP) dans Microsoft 365 est puissante sur le papier, mais son efficacité dépend entièrement de la qualité de la classification des données en amont. Nos missions montrent que moins de 20% des organisations ont une politique de classification opérationnelle.

Avez-vous vérifié les permissions effectives de vos comptes de service Azure AD ?

3 Microsoft Sentinel - SIEM Cloud Avancé

⛈️ Architecture et Positionnement

Microsoft Sentinel complète parfaitement Defender XDR en offrant des capacités SIEM étendues au-delà de l'écosystème Microsoft. Alors que Defender XDR excelle dans la corrélation native des produits Microsoft, Sentinel brille par sa capacité à intégrer des sources de données hétérogènes et à offrir des capacités de hunting à très grande échelle.

🔗 Sources de Données

Microsoft 365

- • Office 365 Activity Logs
- • Azure Active Directory
- • Microsoft Defender XDR
- • Azure Information Protection

Infrastructure

- • Windows Security Events
- • Linux Syslog
- • Network Security Groups
- • Azure Activity Logs

Tiers & Cloud

- • AWS CloudTrail
- • Google Cloud Platform
- • Firewalls (Palo Alto, Fortinet)
- • CEF/Syslog générique

🎯 Capacités Distinctives

📊 Azure Data Explorer

Moteur analytique haute performance pour le traitement de téraoctets de logs

🤖 Machine Learning

Détection d'anomalies basée sur l'IA avec apprentissage continu

🔄 SOAR Intégré

Orchestration et automatisation de la réponse aux incidents

🎨 Workbooks

Visualisations interactives et dashboards personnalisables

🔍 Threat Hunting dans Sentinel

Hunting Query : Détection d'exfiltration de données M365

```
// Détection d'exfiltration potentielle via SharePoint/OneDrive
let timeRange = 24h;
let volumeThreshold = 100; // MB
let fileCountThreshold = 50;

OfficeActivity
| where TimeGenerated > ago(timeRange)
| where OfficeWorkload in ("SharePoint", "OneDriveForBusiness")
| where Operation in ("FileDownloaded", "FileUploaded", "FileSyncDownloadedFull")
| extend FileSizeMB = todouble(Size_) / (1024 * 1024)
| summarize
    TotalDownloadsMB = sum(FileSizeMB),
    FileCount = count(),
    UniqueFiles = dcount(OfficeObjectId),
    DistinctSites = dcount(Site_Url),
    IpAddresses = make_set(ClientIP),
    UserAgents = make_set(UserAgent)
  by UserId, bin(TimeGenerated, 1h)
| where TotalDownloadsMB > volumeThreshold or FileCount > fileCountThreshold
| extend RiskScore =
    (TotalDownloadsMB / 10) +
    (FileCount / 5) +
    (DistinctSites * 2) +
    (array_length(IpAddresses) * 3)
| where RiskScore > 20
| sort by RiskScore desc, TotalDownloadsMB desc
| project-away TimeGenerated1
```

🧠 Analytical Rules et ML

📋 Types de Règles

Scheduled Queries

Requêtes KQL exécutées selon une planification définie pour détecter des patterns spécifiques

Anomaly Detection

Règles basées sur l'apprentissage automatique pour identifier des comportements anormaux

Fusion Rules

Corrélation avancée d'alertes multiples pour détecter des attaques multi-étapes

Threat Intelligence

Détection basée sur les indicateurs de compromission (IoCs) actualisés

🤖 Machine Learning Intégré

UEBA (User Entity Behavior Analytics)

- • Modélisation comportementale des utilisateurs
- • Détection d'anomalies de peer group
- • Scoring de risque dynamique
- • Timeline d'investigation automatique

Anomaly Templates

- • **SSH Brute Force :** Tentatives de connexion anormales
- • **Rare Process :** Exécution de processus inhabituels
- • **Data Exfiltration :** Transferts de données suspects
- • **Privileged Account :** Usage anormal de comptes privilégiés

🎯 Threat Hunting Microsoft 365 Expert

Formation spécialisée et mise en œuvre de stratégies de threat hunting avancées. Maîtrisez Defender XDR, Sentinel, et développez vos propres règles de détection KQL.

Cas concret
Les campagnes de phishing via Microsoft Teams se sont multipliées en 2024, avec des attaquants créant des tenants externes pour envoyer des messages directement aux employés ciblés. L'exploitation de la fédération Teams par défaut a permis de contourner les protections email traditionnelles.

4 Maîtrise du KQL pour le Hunting

Le Kusto Query Language (KQL) constitue le langage universel de requête pour l'ensemble des plateformes Microsoft de sécurité. Sa maîtrise est indispensable pour un threat hunting efficace.

🔍 **Fonctions de Base**

- • where, project, extend
- • summarize, count, dcount
- • join, union, lookup
- • sort, top, limit

⚡ **Fonctions Avancées**

- • regex, parse, extract
- • datetime, timespan
- • arrays, pack/unpack
- • statistical functions

🎯 **Hunting Patterns**

- • Time-based correlation
- • Baseline establishment
- • Anomaly detection
- • IOC matching

5 Méthodologies de Chasse Avancées

🎯 Threat-Led Hunting

Chasse basée sur les renseignements de menaces et les TTPs connus

MITRE ATT&CK Mapping
Threat Intelligence Feeds
IOC Enrichment

📊 Data-Driven Hunting

Approche analytique basée sur l'analyse statistique et les anomalies

Statistical Analysis
Baseline Deviation
Pattern Recognition

7 Analyse Comportementale et UEBA

🧠 User Entity Behavior Analytics

Baseline Establishment

- • Profils utilisateurs normaux
- • Patterns temporels habituels
- • Géolocalisation typique
- • Applications utilisées

Anomaly Detection

- • Déviations comportementales
- • Activités inhabituelles
- • Peer group analysis
- • Risk scoring dynamique

Threat Indicators

- • Impossible travel
- • After-hours activity
- • Mass data access
- • Privilege escalation

11 Cas d'Études Pratiques

🎭 Cas 1 : Business Email Compromise (BEC)

🔍 Indicateurs Détectés

- • Connexions depuis pays inhabituels
- • Création de règles de redirection email
- • Modification des paramètres de délégation
- • Envoi d'emails suspects vers l'externe

🎯 Techniques MITRE ATT&CK
T1078 - Valid Accounts T1114 - Email Collection T1566 - Phishing T1020 - Automated Exfiltration

Articles connexes

Approfondissez vos connaissances en sécurité Microsoft 365 avec ces guides experts :

🔗 Détection Compromission Identités

Détectez les compromissions d'identités avec des techniques de threat hunting ciblées sur Azure AD.

🛡️ Corrélation des Journaux M365

Techniques avancées de corrélation des logs M365 pour alimenter vos campagnes de threat hunting.

🔐 Automatisation Audit PowerShell

Automatisez la collecte de données pour le threat hunting avec PowerShell et l'API Microsoft Graph.

🎯 Outils d'Analyse Sécurité M365

Découvrez les outils essentiels pour enrichir vos capacités de threat hunting dans Microsoft 365.

12 Conclusion et Évolutions du Threat Hunting

🎯 Points Clés

- • **Approche Proactive :** Ne pas attendre les alertes automatiques
- • **Corrélation Multi-Sources :** Defender XDR + Sentinel
- • **KQL Expertise :** Langage essentiel pour le hunting
- • **MITRE ATT&CK :** Framework de référence
- • **Amélioration Continue :** Learning loops

🚀 Évolutions Futures

- • **AI/ML Avancé :** Détection de plus en plus élaborée
- • **Automated Hunting :** Hunters augmentés par l'IA
- • **Threat Intelligence :** Intégration temps réel
- • **Cross-Platform :** Hunting multi-cloud natif
- • **Community Hunting :** Partage de connaissances

> **Ressources open source associées :**
>
> - KQLHunter — Générateur de requêtes KQL avec IA (Python)
> - SOC-Assistant — Assistant SOC RAG (Python)
> - ThreatIntel-GPT — Intelligence de menaces avec IA (Python)
> - m365-security-fr — Dataset sécurité M365 (HuggingFace)
> - threat-hunting-soc-fr — Dataset threat hunting/SOC (HuggingFace)

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Sources et références : Microsoft Security Docs · CERT-FR

Conclusion

Cet article a couvert les aspects essentiels de Articles connexes. La mise en pratique de ces recommandations permet de renforcer significativement la posture de securite de votre organisation.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr