Renforcer votre posture de sécurité à la vitesse de l'IA avec Microsoft Copilot for Security

blue soft GROUP
Empower

WEBINAR

Mardi 9 juillet 2024

Sommaire

Romaric MAHUT
Alliance Manager

Jean-François BERENGUER
Directeur des Opérations

Blandine CERVANTES
Consultante Avant-vente

01. Introduction à Copilot

blue soft Empower

Sondage

Quel module de Copilot utilisez-vous ?

- ❑ Copilot
- ❑ Copilot for Microsoft 365
- ❑ Copilot for Studio
- ❑ GitHub Copilot
- ❑ Copilot for Security

blue soft Empower

Nos principaux Copilotes

Microsoft Copilot
Le Copilot du quotidien

GitHub Copilot
Le Copilot du développement

Copilot for Microsoft 365
Le Copilot de la productivité

Copilot Studio
Concevez votre Copilot sur mesure

Copilot for Security
Effectuer des tâches SOC plus rapidement avec Copilot

Les prompts

COPILOT

Grand modèle de langage
(LLM : Large language model)

L'importance du prompt & l'accompagnement utilisateur

OBJECTIF
Qu'attendez-vous de Copilot ?

CONTEXTE
Pourquoi en avez-vous besoin et qui est impliqué ?

ATTENTES
Comment Copiot doit-il vous répondre pour satisfaire pleinement votre demande ?

SOURCES
Quelles informations ou quels exemples voulez-vous que Copilot utilise ?

Sondage

Disposez-vous d'une équipe sécurité opérationnelle ou d'un soc managé ?

- ❑ Soc managé
- ❑ Equipe sécurité interne
- ❑ Rien

02. Copilot for Security

blue soft
Empower

Les défenseurs sont tout simplement dépassés. Les attaquants ont plus de ressources et n'ont pas à jouer selon les mêmes règles.

4,000

Attaques de mots de passe par seconde

72 mins

Temps médian pour qu'un attaquant accède à vos données privées si vous êtes victime d'un e-mail de phishing

3.5M

Pénurie mondiale de professionnels qualifiés en cybersécurité

La consolidation des outils et l'IA générative peuvent transformer la sécurité

CONSOLIDATION DES OUTILS

Défense coordonnée sur tous les vecteurs de menace pour offrir une visibilité et une couverture de bout en bout

IA

Des gains exponentiels en termes d'expertise humaine et d'efficacité pour se défendre à la vitesse et à l'échelle de la machine

Copilot for Security

Protégez à la vitesse et à l'échelle de l'IA

« Il nous faut trois minutes pour faire une tâche qui prenait au moins quelques heures auparavant »

- Copilote pour le client Sécurité

Activez la réponse en quelques minutes, et non en quelques heures

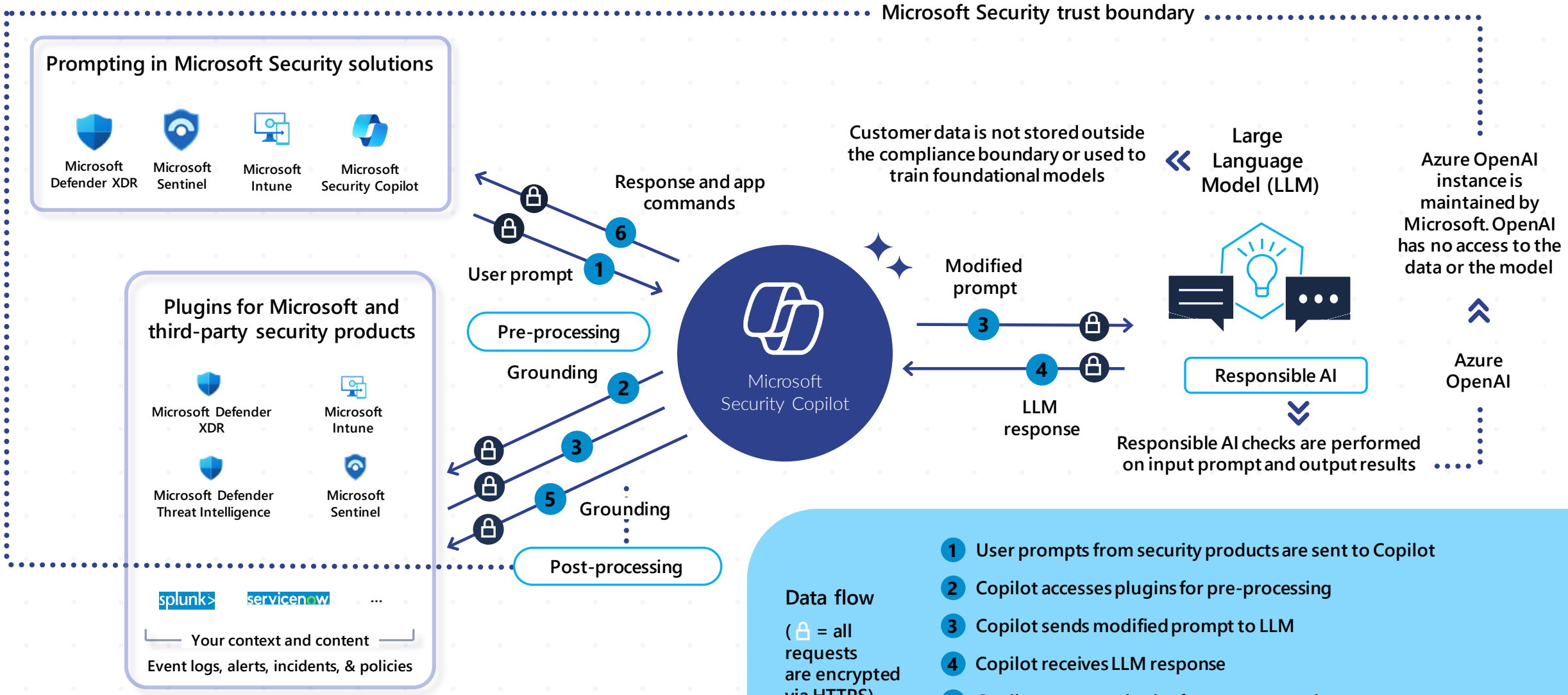
Simplifiez la complexité avec des invites en langage naturel et des rapports faciles

Détectez ce que les autres manquent grâce à une meilleure compréhension de votre entreprise

Renforcer l'expertise des équipes avec des cybercompétences et des guides

Comment Copilot for Security fonctionne ?

Data flow for Microsoft Copilot for Security



Data flow

(🔒 = all requests are encrypted via HTTPS)

1. User prompts from security products are sent to Copilot
2. Copilot accesses plugins for pre-processing
3. Copilot sends modified prompt to LLM
4. Copilot receives LLM response
5. Copilot accesses plugins for post-processing
6. Copilot sends the response, and app command back to security products

Partenaires et plugins

Managed Security Service Providers

accenture
ASCENT SOLUTIONS
avanade
BlueVoyant
BULLETPROOF a GLI company
Capgemini
chorus
CRITICALSTART
DIFENDA
DXC TECHNOLOGY
eSENTIRE
EY Building a better working world
glueck kanja
KPMG
nccgroup
Nedscaper
onevinn
Ontinue AI-Powered MXDR
orange Cyberdefense
pwc
wipro
Quorum Cyber
red canary
SYNERGY ADVISORS
Trustwave

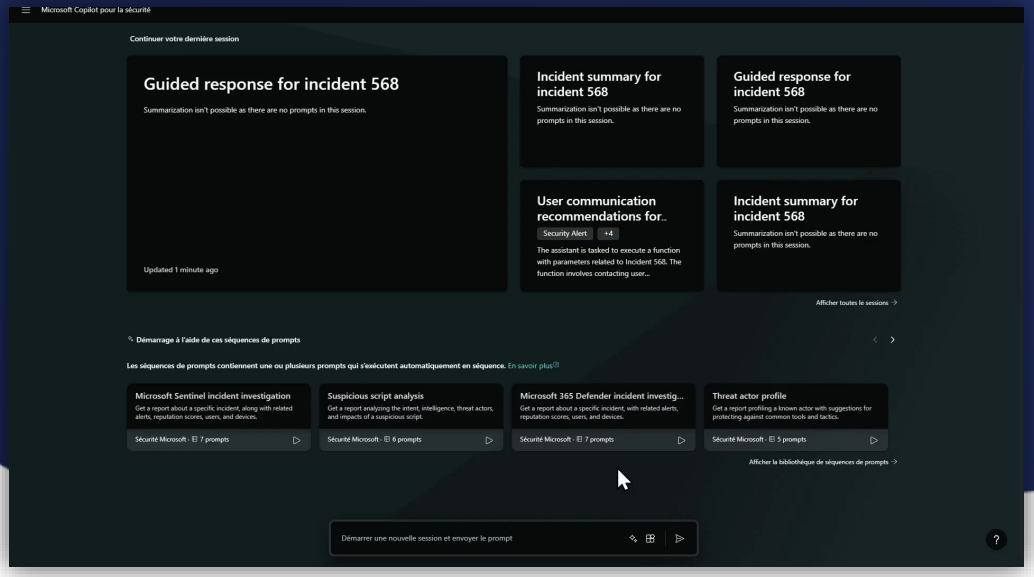
Independent Software Vendors

Arkose Labs
Authomize
BITSIGHT
CEQUENCE
cerby
CHECK POINT
CISCO
CISO GLOBAL
COMMVAULT
CONTRAFORCE
corelight
CYBERARK The Identity Security Company
CYWARE
DARKTRACE
Elevate Security
Gigamon
HUMAN
HYAS
iboss
illumio
jamf PROTECT
LACEWORK
Lenovo
NETACEA
netskope
pathlock
Qualys.
Quest
rubrik
SafeBreach
satori
SAVIYNT
Security Scorecard
sgnl
SpyCloud
STRATA Identity Orchestration
Synack
TANIUM
uptycs
valence
VERSA
vmware
WIZ
ZIMPERIUM
cyclotron
VU

Deux expériences : Autonome et Embarquée

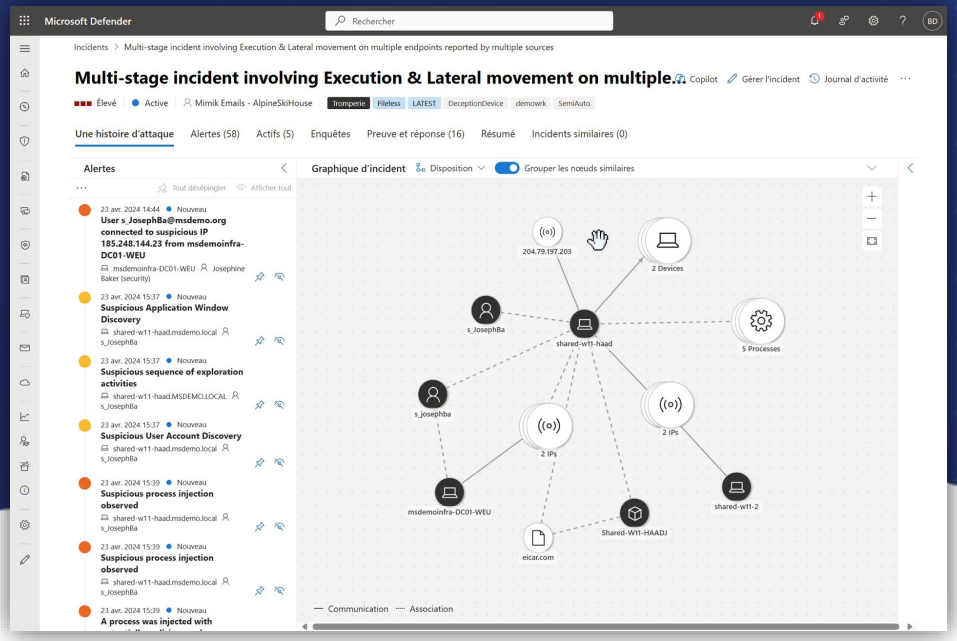
Autonome

Aide les équipes à obtenir un aml rcvrc njsqj_pec pour dépanner et corriger les incidents plus rapidement dans Copilot for Security lui-même, avec rmsqjcqa_qb%rgjgq_rgml cl sl qcsjclbpmgr, ce qui permet d'obtenir des conseils inter-produits enrichis.



Embarqué

Offre l'expérience intuitive d'obtenir des conseils Copilot for Security en mode natif dans les produits sur lesquels les membres de votre équipe travaillent déjà et avec lesquels ils sont familiers.



L'IA générative rencontre le XDR

Examinez les menaces et répondez-y dans une expérience guidée

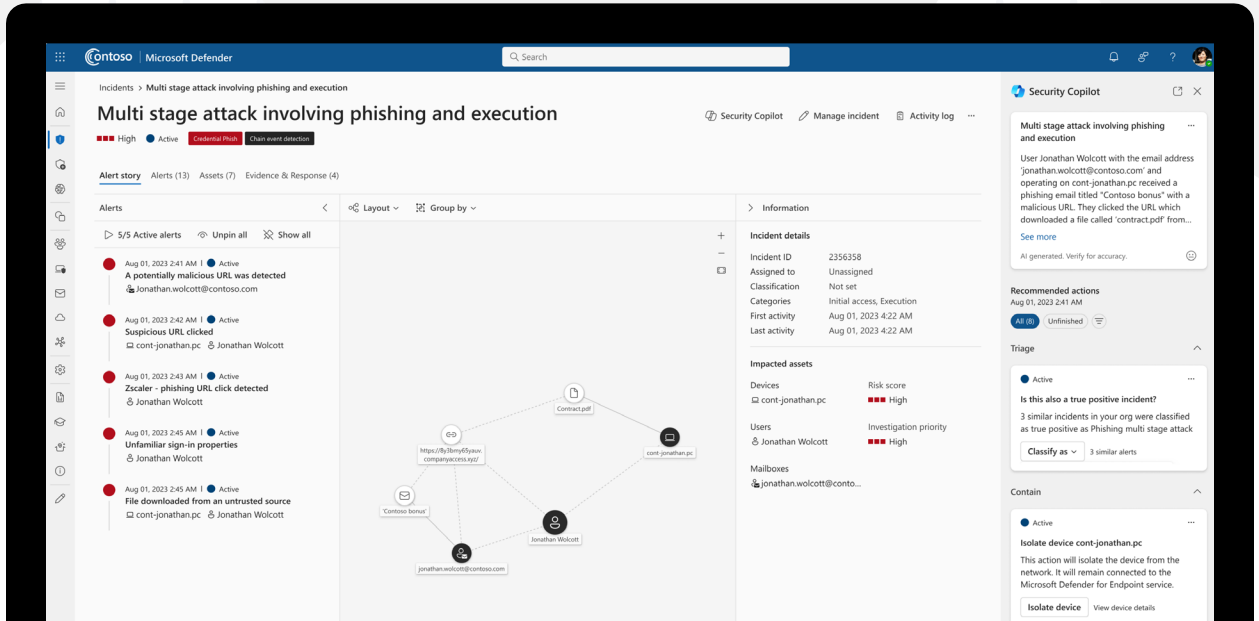
Résumez un incident, analysez l'impact, fournissez des recommandations guidées et générez des rapports pour une investigation et une correction plus rapide.

Améliorez les compétences de votré équipe SecOps

Débloquez de nouvelles compétences pour les analystes grâce à la traduction du langage naturel vers le langage de requête Kusto (KQL) et à l'analyse de scripts qui éliminent le besoin d'analyser manuellement des scripts complexes.

Évaluez les risques grâce à la veille sur les menaces basée sur l'IA

Renseignez-vous en langage naturel sur les menaces émergentes et obtenez des informations contextualisées pour une réponse rapide aux menaces nouvelles et évolutives



Quelques exemples de prompts

- Analyses le script suivant <INSERT SCRIPT>
- Fais-moi un résumé de l'incident Sentinel <SENTINEL_INCIDENT_ID>
- Pourquoi <Utilisateur> a eu une requête MFA ?
- Génère une requête KQL dans pour Sentinel afin de rechercher l'usage des comptes Break-Glass
- Montres-moi les 5 principales alertes DLP que je devrais prioriser aujourd'hui
- Ecris un rapport résumant cette investigation pour une audience non technique
- Si un utilisateur est listé dans les détails de l'incident, montre-moi quel appareil il a utilisé récemment ainsi que sa conformité
- Décris l'impact de cette stratégie sur les utilisateurs et mettez en évidence les conflits de paramètres avec la stratégie existante

Les **Promptbooks** sont un outil puissant pour **rationaliser le flux d'investigation** et tâches en plusieurs étapes.

Les Promptbooks ont été conçus pour **être exécutés avec un seul clic**, ce qui permet aux utilisateurs de gagner un temps précieux.

Copilot comprend de nombreux Promptbooks en standard pour les flux de tâches courants et les utilisateurs peuvent également créer/modifier des Promptbooks personnalisés.

Promptbooks

Example promptbook flow:

- Summarize Sentinel incident <SENTINEL_INCIDENT_ID>
- Tell me about the entities associated with that incident.
- What are the reputation scores for the IPv4 addresses on that incident?
- Show the authentication methods setup for each user involved in that incident. Especially indicate whether they have MFA enabled.
- If a user is listed in the incident details, show which devices they have used recently and indicate whether they are compliant with policies.
- If any devices are listed in the previous output, show details from Intune on the one that checked in most recently. Especially indicate if it is current on all operating system updates.
- Write an executive report summarizing this investigation. It should be suited for a non-technical audience.

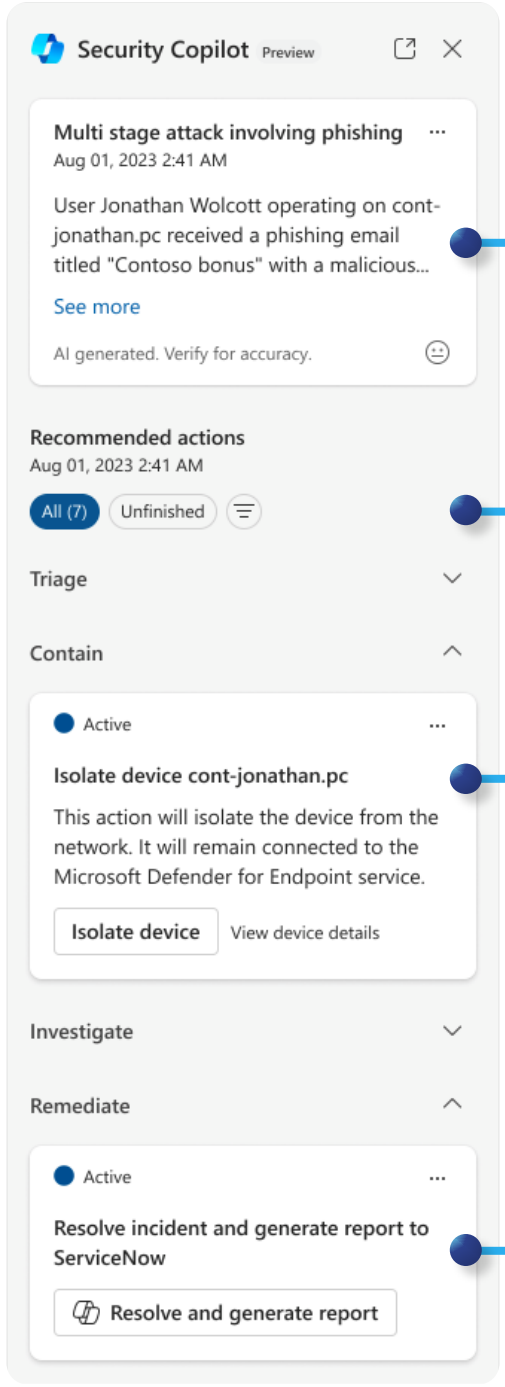
03. Démos

blue soft Empower

Assisted incident investigation and response

Répondez aux menaces à la vitesse de l'IA dans une expérience simplifiée et guidée

- **Incident summary** Transforme les détails complexes de l'attaque en un récit d'attaque clair en quelques secondes, en mettant en évidence les aspects les plus importants pour un triage et une hiérarchisation rapide
- **Guided response** fournit des conseils pratiques étape par étape adaptés à l'incident en cours, en orientant les analystes vers les étapes de triage, d'enquête, de confinement et de remédiation pour une efficacité maximale
- **Incident report** génère un résumé prêt à partager des activités des analystes liées à l'incident, ce qui permet de gagner **des heures sur le résumé de l'incident**

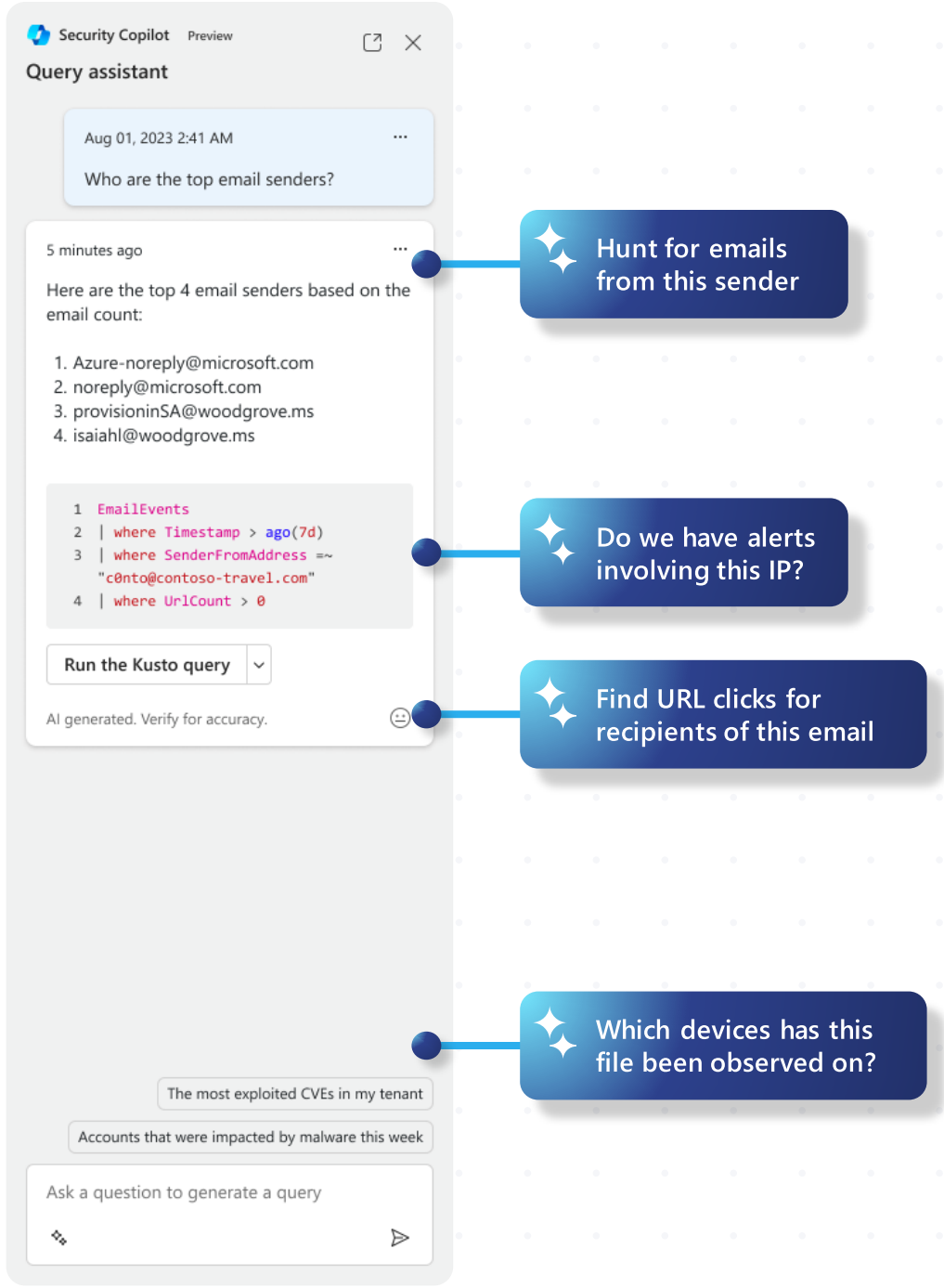


Assisted threat hunting

La chasse aux menaces n'a jamais été aussi simple et rapide

- **Recherchez facilement les menaces** dans plusieurs domaines en utilisant le langage naturel pour créer des requêtes KQL complexes, quel que soit votre niveau de compétence, et obtenir des résultats de requête résumés

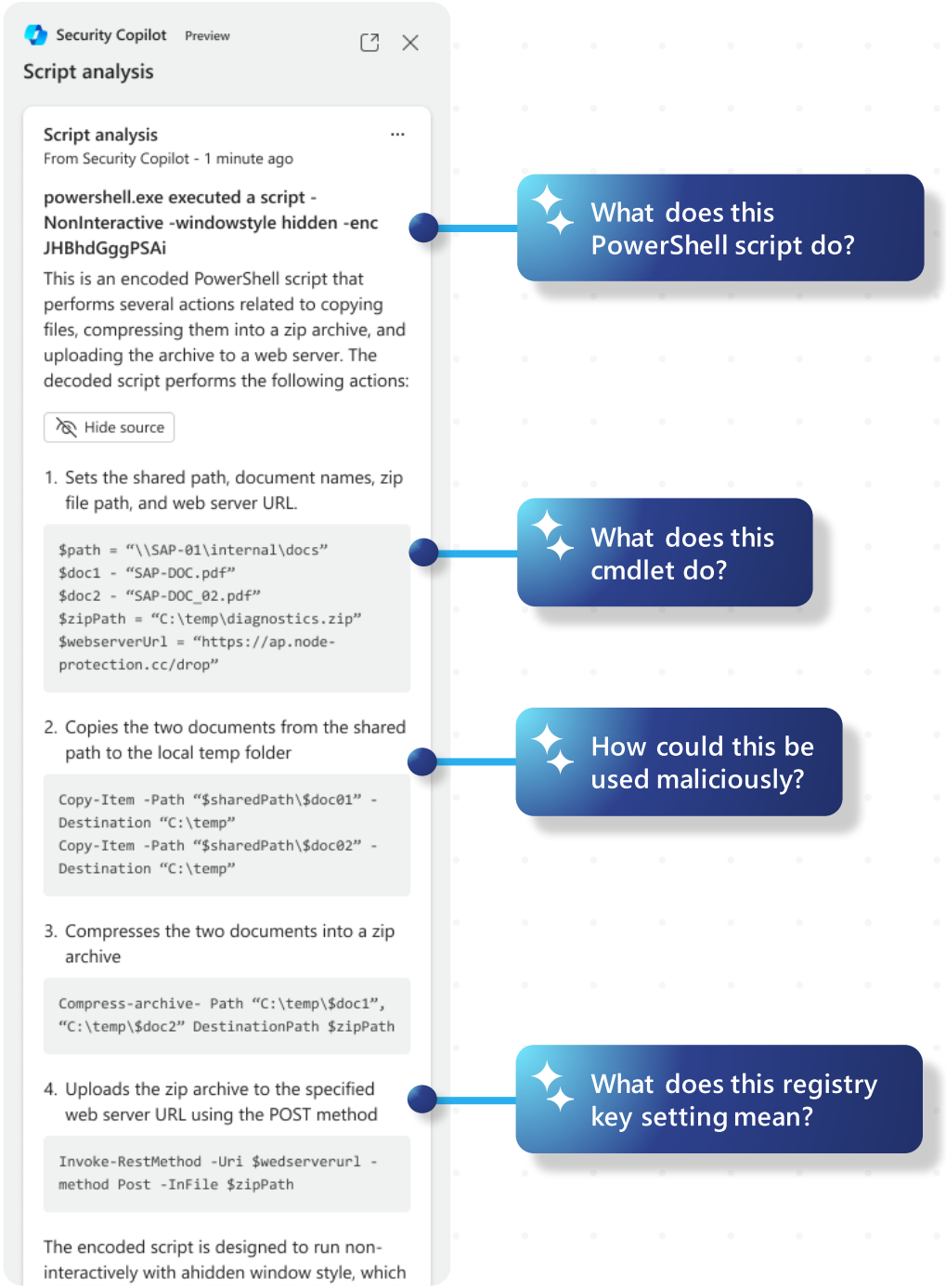
- Éliminez le besoin d'écrire vous-même des requêtes KQL pour localiser les informations dans toutes les données XDR, ce qui permet de gagner un temps considérable et de rendre la chasse accessible et efficace pour tous les niveaux de compétence



Assisted code analysis

Votre expert en scénario à portée de main

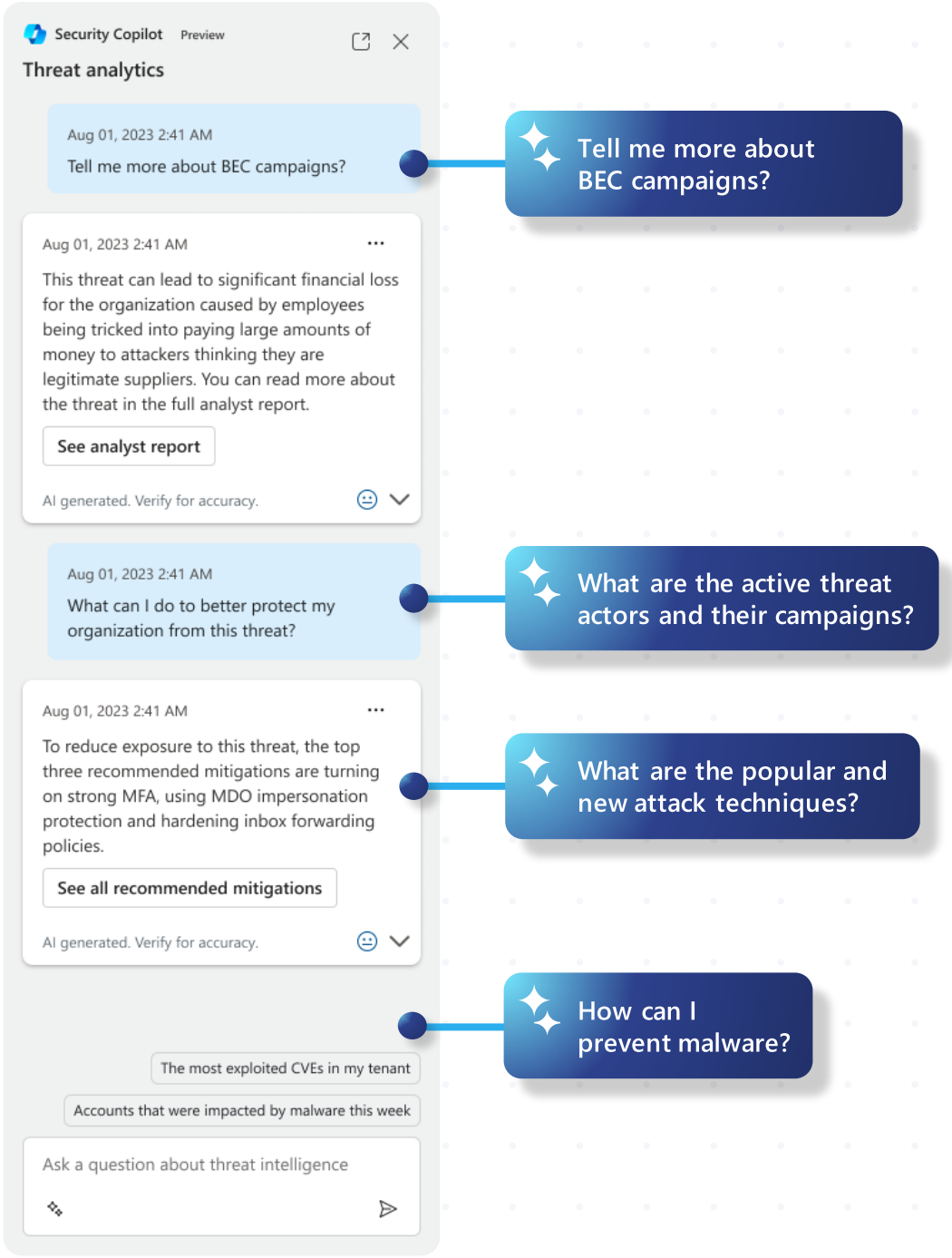
- **Analysez des scripts** et des artefacts de ligne de commande complexes et **traduisez-les en langage naturel** facilement compréhensible tout en offrant des informations sur les actions effectuées par les scripts
- **Éliminez le besoin de rétro-concevoir manuellement** les logiciels malveillants et donnez à chaque analyste les moyens de comprendre facilement les actions exécutées par les attaquants
- **Extrayez et liez** efficacement les indicateurs trouvés dans le script à leurs entités respectives dans votre environnement



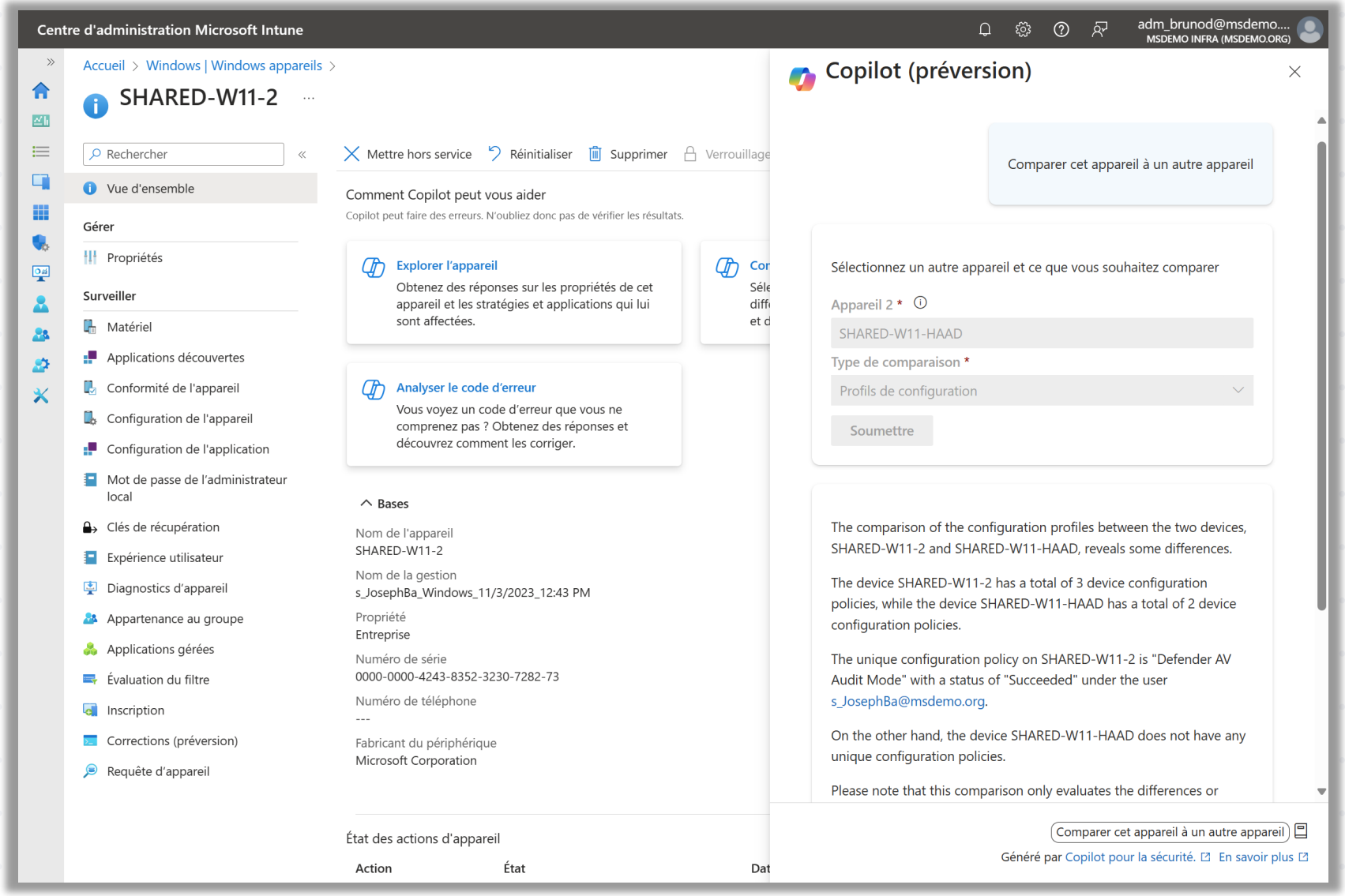
Assisted threat analytics

Gardez une longueur d'avance sur les menaces futures grâce aux renseignements sur les menaces alimentées par l'IA

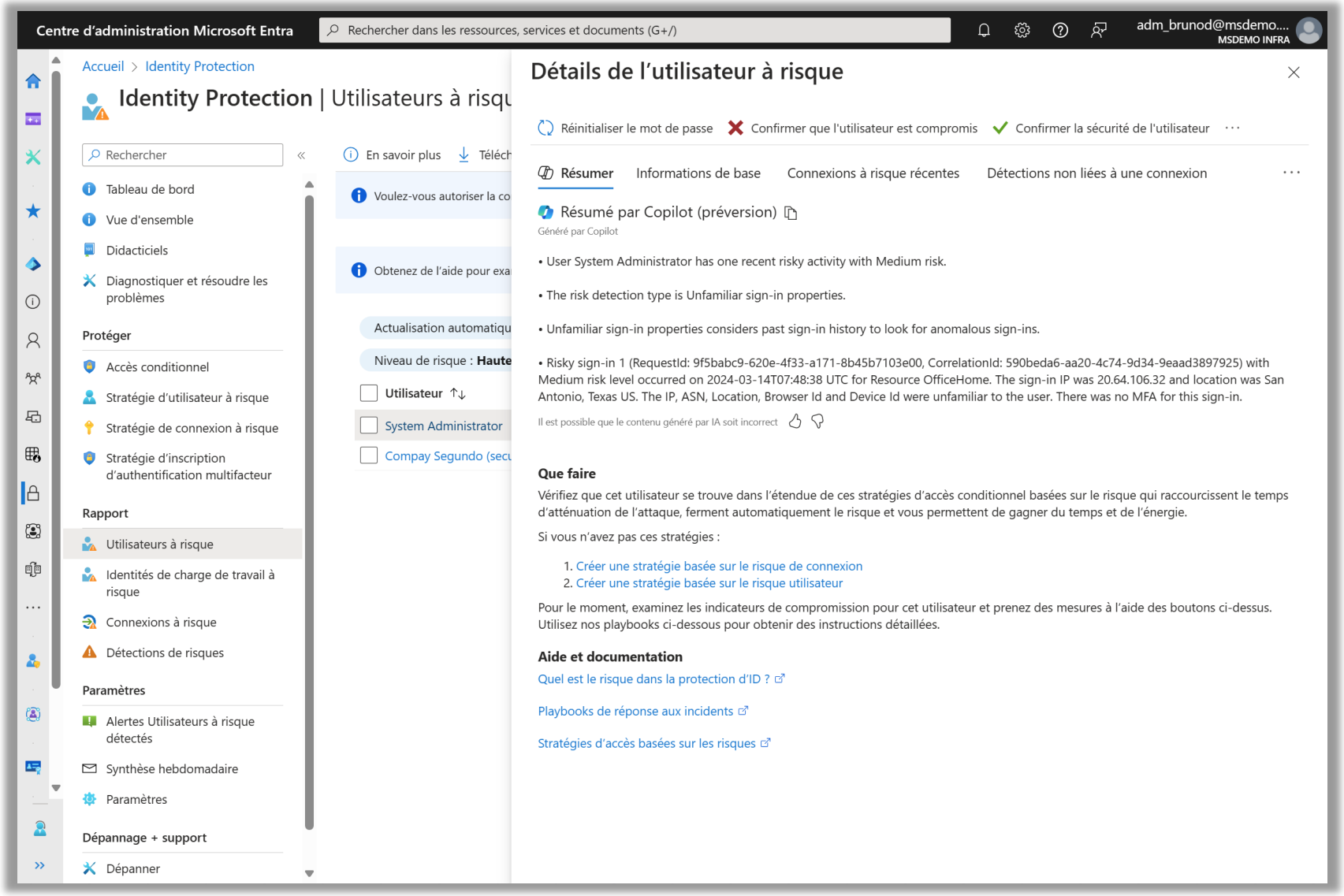
- Renseignez-vous en langage naturel sur les menaces émergentes, les techniques d'attaque et si votre organisation est affectée ou exposée à une menace spécifique
- Identifiez et réagissez plus efficacement aux menaces les plus récentes et émergentes grâce à des informations contextualisées et résumées optimisées par Microsoft Defender Threat Intelligence
- Améliorez votre posture de sécurité grâce à une approche axée sur les menaces et à des recommandations de posture adaptées à votre environnement



Comparaison 2 périphériques avec Intune



Entra ID : Utilisateur à risque



Sondage

Seriez-vous prêt à déployer Copilot for Security ? 🧐

blue soft Empower

04. Licensing

blue soft
Empower

K ga pmqmdr Amn gj mr dmp Qc a s pgr w 8 R_ pgdga _r gml

Microsoft Copilot for Security est facturé en tant que consommation Azure.

Un modèle de facturation unique pour l'ensemble des expériences autonomes (standalone) et intégrées (embedded).

Commencez dès maintenant avec un modèle de consommation, sans frais par utilisateur ou par appareil

Provisionnez des unités de calcul de sécurité (SCU) pour exécuter toutes les charges de travail Copilot for Security

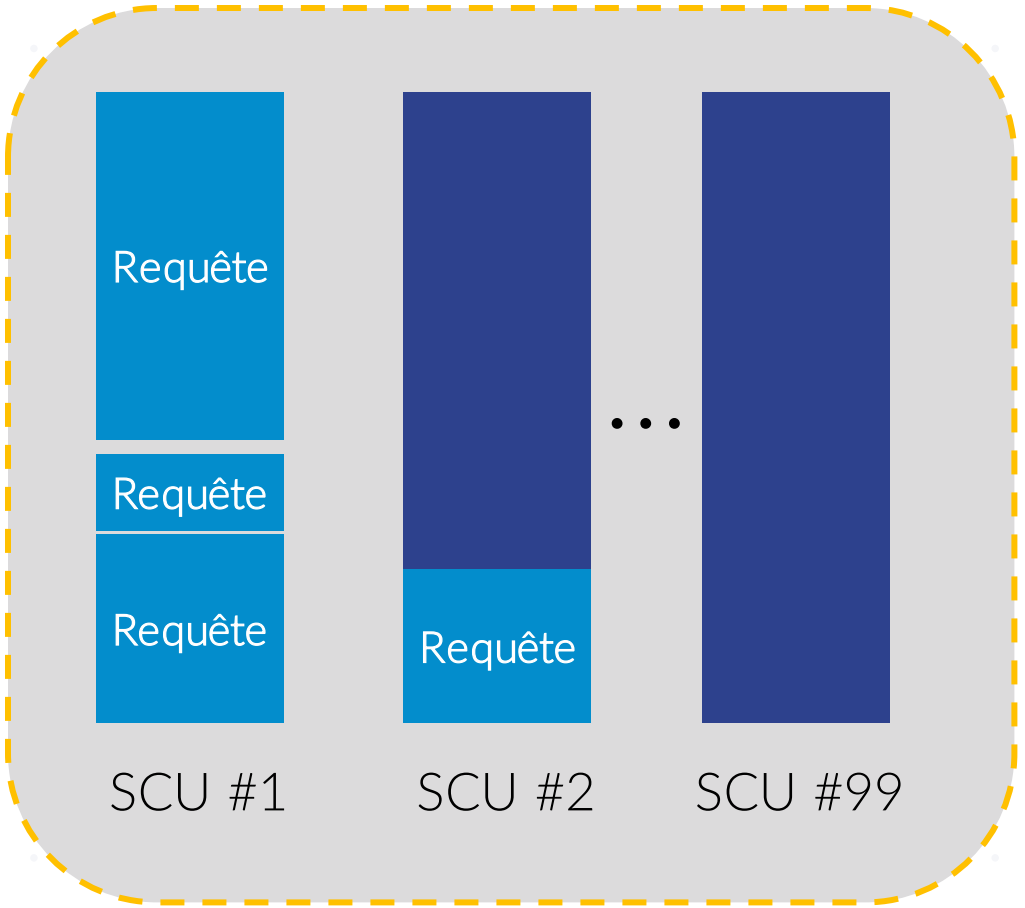
Gérez facilement les coûts grâce à un tableau de bord intégré au produit pour surveiller l'utilisation

Provisionnez de manière flexible des unités de calcul de sécurité (SCU) pour exécuter Copilot pour les charges de travail de sécurité.

Dml argml ck clr

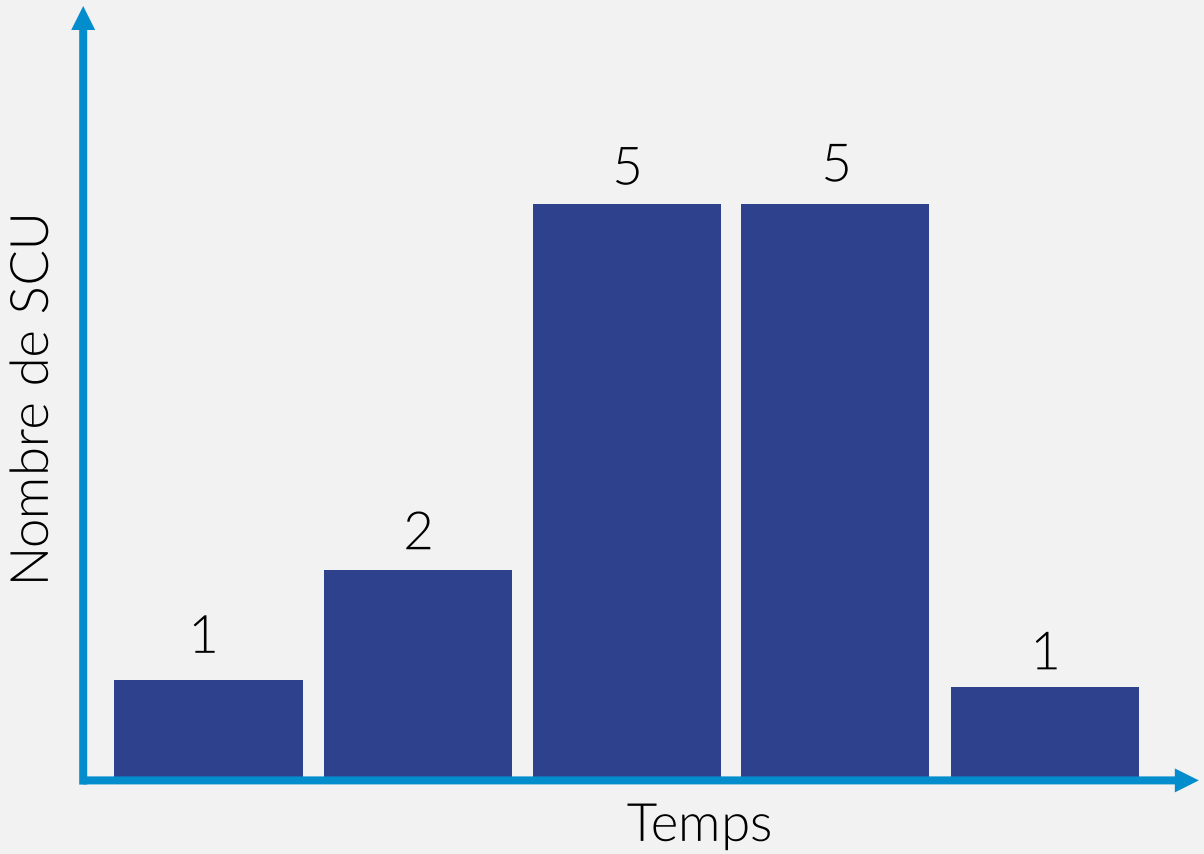
ApŒ_rgml b%slc áa_n_agrŒi
Amngjmr dmp Qcaspgrw

- Chaque capacité peut contenir entre 1 et 99 “SCU” (Unité de calcul sécurité). Une SCU est facturée par heure.
- Chaque requête au service consomme du calcul



Fonctionnement

Possibilité d'ajuster le nombre d'unité de calcul heure par heure



Région :

Europe Ouest

Devise:

Zone Euro - Euro (€) EUR

1 USD = 0.9363 EUR

Capacité de calcul Microsoft Copilot pour la sécurité

Approvisionner la capacité dans les Unités de calcul de sécurité (SCU) pour exécuter des charges de travail Microsoft Copilot pour la sécurité. Ces charges de travail fournissent des insights, évaluer des prompts et les automatiser dans le produit autonome et les expériences dans Sécurité Microsoft.

- Approvisionnez de manière flexible des unités de calcul pour répondre aux besoins de votre organisation.
- Managez facilement les coûts avec un tableau de bord dans le produit.

Référence SKU	Prix par heure	Prix estimé par mois
Provisionné	3,7454 €	2 734,0824 €[1]

[1]L'estimation de la facture mensuelle concerne 1 Unité de calcul de sécurité (SCU) approvisionnée quotidiennement pendant 24 heures pour l'ensemble du mois. Les SCU sont approvisionnées par heure et facturées mensuellement.

Microsoft recommande d'approvisionner 3 Unités de calcul de sécurité par heure pour démarrer votre exploration de Microsoft Copilot pour la sécurité.

Questions ?

Merci !

www.bluesoft-group.com