

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



WEBINAR

Mardi 9 juillet 2024

Sommaire

- 01.** Introduction à Copilot
- 02.** Présentation de Copilot for Security
- 03.** Démonstrations
- 04.** Mode de licence
- 05.** Questions & Réponses



Romaric MAHUT
Alliance Manager



Jean-François BERENGUER
Directeur des Opérations



Blandine CERVANTES
Consultante Avant-vente



01. Introduction à Copilot

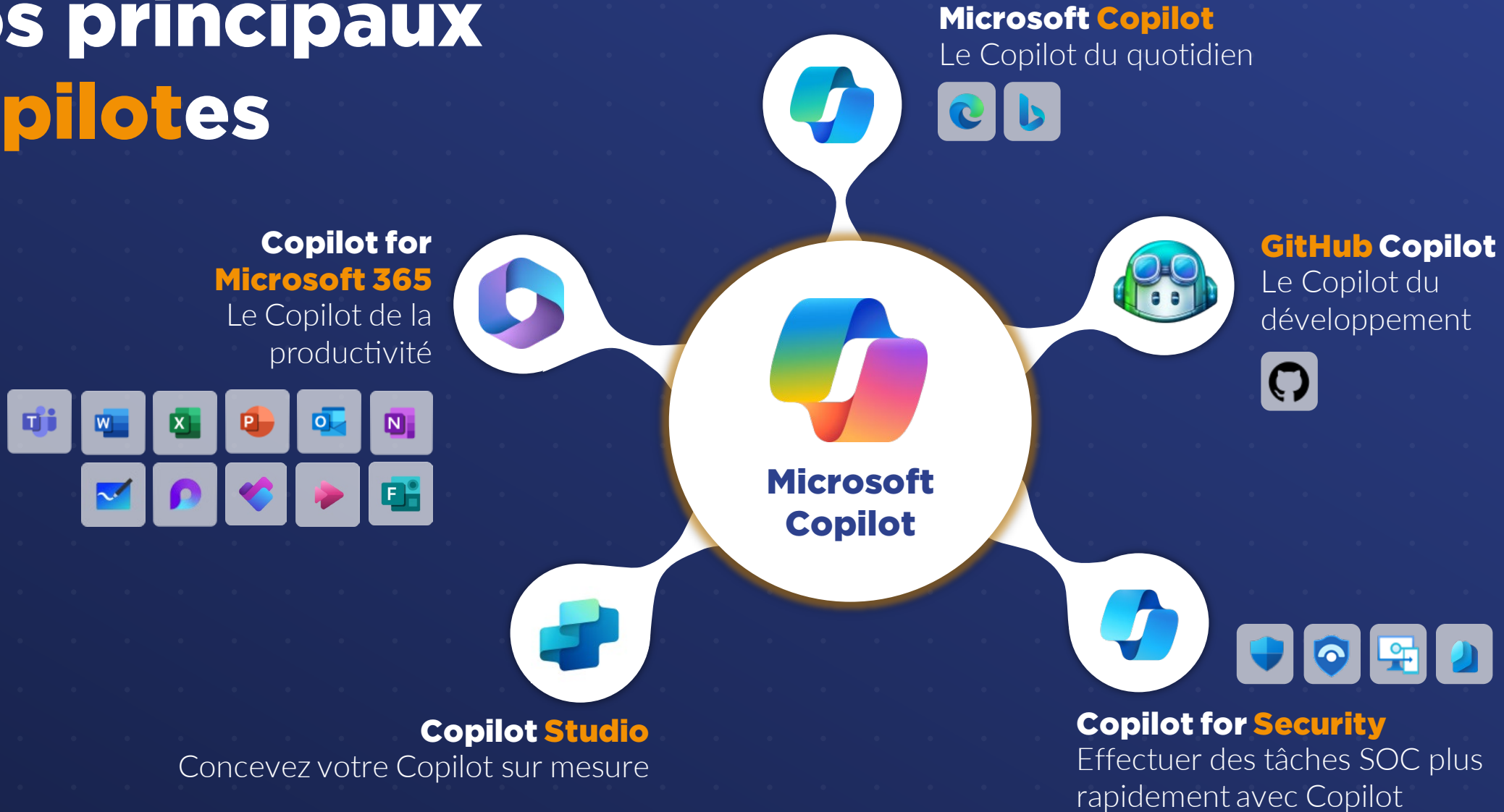
Sondage

Quel module de Copilot utilisez-vous ?

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



Nos principaux Copilotes



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 Copilot
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





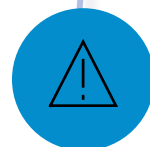
02. Copilot for Security

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

Microsoft Security trust boundary

Prompting in Microsoft Security solutions

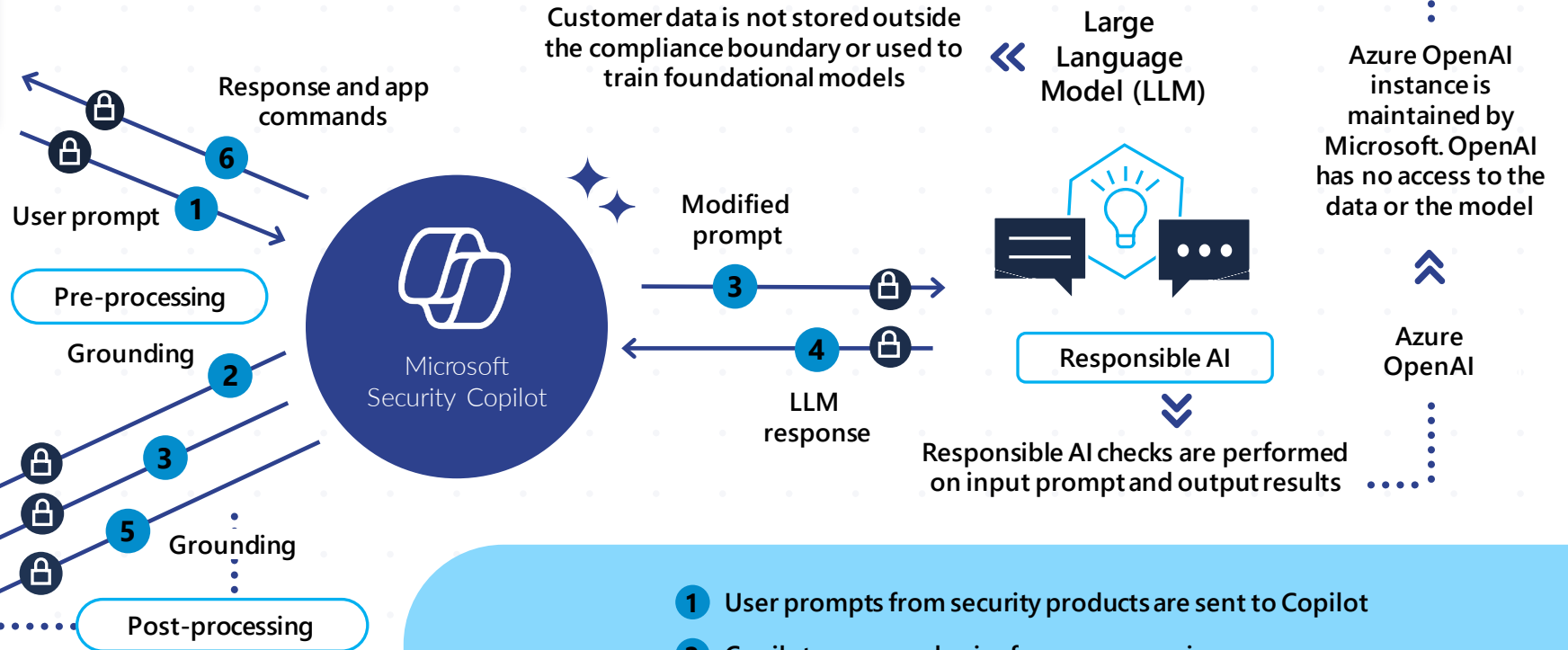


Plugins for Microsoft and third-party security products



splunk> servicenow ...

Your context and content
Event logs, alerts, incidents, & policies



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 Quorum Cyber red canary SYNERGY ADVISORS Trustwave

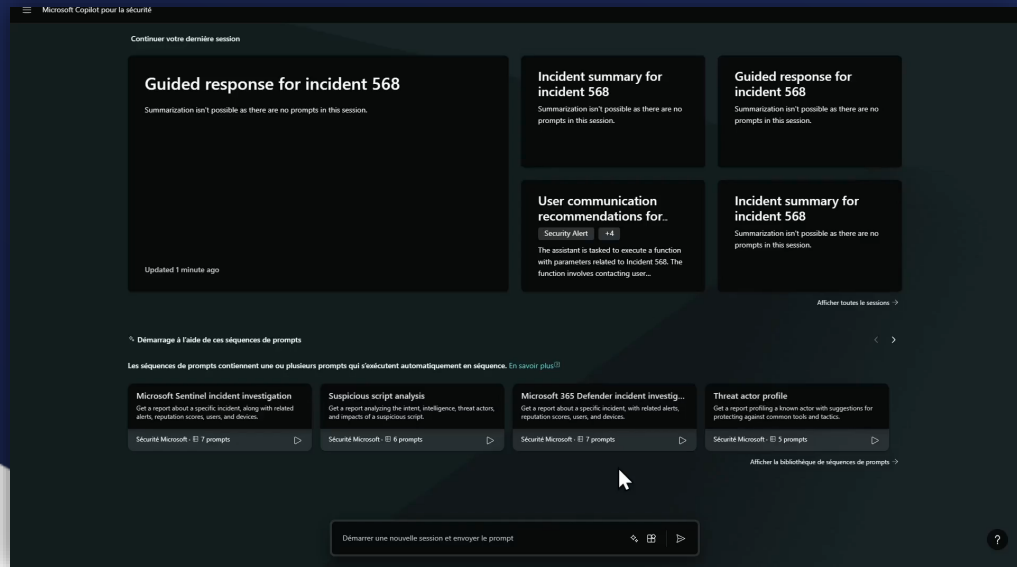
Independent Software Vendors

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 Synack TANIUM uptycs valence VERSA STRATA Identity Orchestration WIZ ZIMPERIUM cyclotron VU

Deux expériences : Autonome et Embarquée

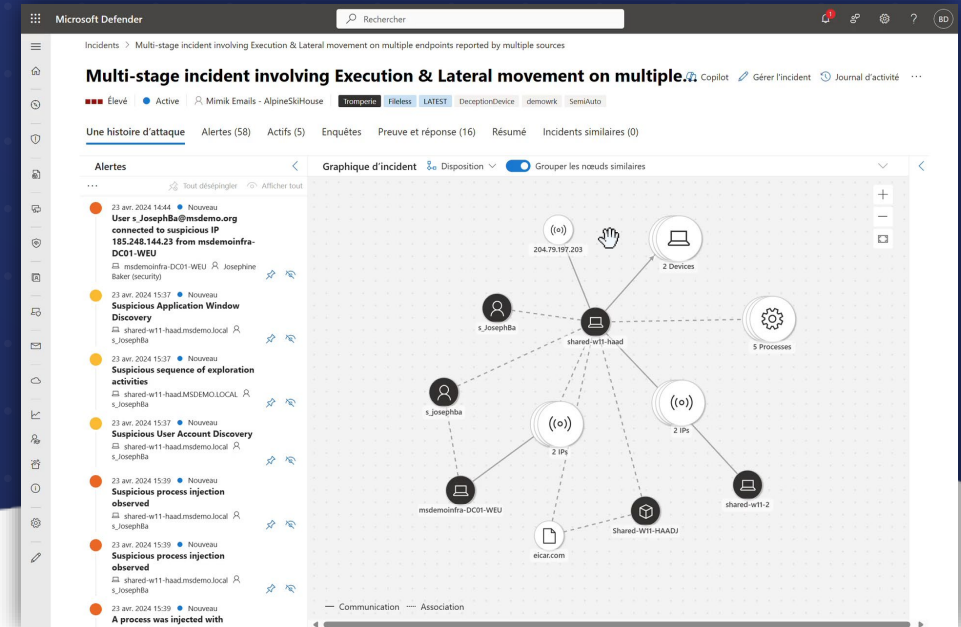
Autonome

Aide les équipes à obtenir un **aml rc vrc njs q j_pe c** pour dépanner et corriger les incidents plus rapidement dans Copilot for Security lui-même, avec **rms q jc q a_q b %r ggg_rgml cl sl qc sj cl b pmgr**, 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

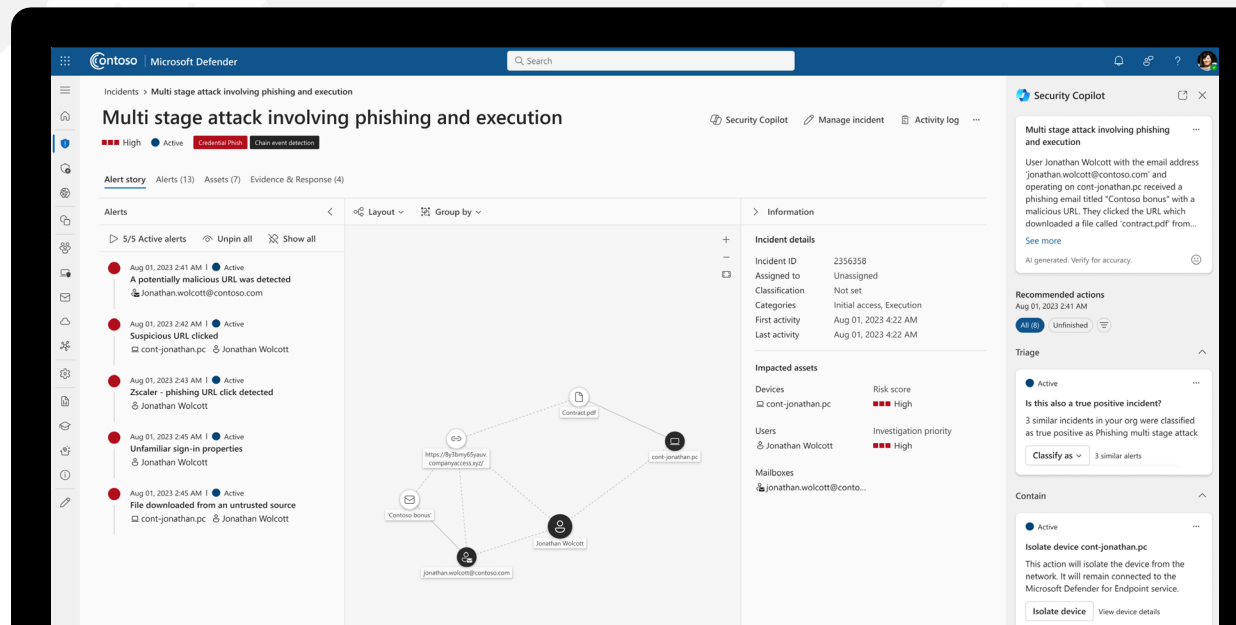
Résumez un incident, analysez l'impact, fournissez des recommandations guidées et générez des rapports pour une investigation et une correction plus rapide.

Améliorez les compétences de votre 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. Demos

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**

The screenshot displays the Security Copilot interface for an incident titled "Multi stage attack involving phishing" on August 01, 2023, at 2:41 AM. The interface is divided into several sections:

- Incident Summary:** A text box containing a summary of the incident: "User Jonathan Wolcott operating on cont-jonathan.pc received a phishing email titled 'Contoso bonus' with a malicious...". Below the text is a "See more" link and a note: "AI generated. Verify for accuracy." with a smiley face icon.
- Recommended actions:** A section with a date and time stamp "Aug 01, 2023 2:41 AM" and a filter for "All (7)" actions, with "Unfinished" actions also visible.
- Triage:** A dropdown menu currently showing "Contain".
- Contain:** A section with an "Active" status and a list of actions. The first action is "Isolate device cont-jonathan.pc", with a description: "This action will isolate the device from the network. It will remain connected to the Microsoft Defender for Endpoint service." Below this action are two buttons: "Isolate device" and "View device details".
- Investigate:** A dropdown menu currently showing "Remediate".
- Remediate:** A section with an "Active" status and a list of actions. The first action is "Resolve incident and generate report to ServiceNow", with a button labeled "Resolve and generate report".

Summarize what happened in this incident using attack story

Tell me what the timeline of this incident was

Isolate device cont-Jonathan.pc

Create an incident report summarizing the actions taken to resolve the 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

Security Copilot Preview

Query assistant

Aug 01, 2023 2:41 AM

Who are the top email senders?

5 minutes ago

Here are the top 4 email senders based on the email count:

1. Azure-noreply@microsoft.com
2. noreply@microsoft.com
3. provisioninSA@woodgrove.ms
4. isaiah@woodgrove.ms

```
1 EmailEvents
2 | where Timestamp > ago(7d)
3 | where SenderFromAddress =~ "c0nto@contoso-travel.com"
4 | where UrlCount > 0
```

Run the Kusto query

AI generated. Verify for accuracy.

The most exploited CVEs in my tenant

Accounts that were impacted by malware this week

Ask a question to generate a query

🌟 Hunt for emails from this sender

🌟 Do we have alerts involving this IP?

🌟 Find URL clicks for recipients of this email

🌟 Which devices has this file been observed on?

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

The screenshot shows the Security Copilot interface with a 'Script analysis' window. The window title is 'Script analysis' and it indicates it was generated '1 minute ago'. The analysis text states: 'powershell.exe executed a script - NonInteractive -windowstyle hidden -enc JHBhdGggPSAi'. It explains that this is an encoded PowerShell script performing actions like copying files, compressing them into a zip archive, and uploading the archive to a web server. Below the text is a 'Hide source' button. The analysis is broken down into four numbered steps, each with a corresponding PowerShell command snippet: 1. Sets the shared path, document names, zip file path, and web server URL. 2. Copies the two documents from the shared path to the local temp folder. 3. Compresses the two documents into a zip archive. 4. Uploads the zip archive to the specified web server URL using the POST method. At the bottom, it notes that the script is designed to run non-interactively with a hidden window style.

What does this PowerShell script do?

What does this cmdlet do?

How could this be used maliciously?

What does this registry key setting mean?

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

The screenshot displays the Security Copilot interface with the following content:

- Header:** Security Copilot Preview
- Section: Threat analytics**
- Query 1:** "Tell me more about BEC campaigns?" (Aug 01, 2023 2:41 AM). Response: "This threat can lead to significant financial loss for the organization caused by employees being tricked into paying large amounts of money to attackers thinking they are legitimate suppliers. You can read more about the threat in the full analyst report." Includes a "See analyst report" button and "AI generated. Verify for accuracy." notice.
- Query 2:** "What can I do to better protect my organization from this threat?" (Aug 01, 2023 2:41 AM). Response: "To reduce exposure to this threat, the top three recommended mitigations are turning on strong MFA, using MDO impersonation protection and hardening inbox forwarding policies." Includes a "See all recommended mitigations" button and "AI generated. Verify for accuracy." notice.
- Additional Insights:** "The most exploited CVEs in my tenant" and "Accounts that were impacted by malware this week".
- Footer:** "Ask a question about threat intelligence" with a search icon.

✦ Tell me more about BEC campaigns?

✦ What are the active threat actors and their campaigns?

✦ What are the popular and new attack techniques?

✦ How can I prevent malware?

Comparaison 2 périphériques avec Intune

The screenshot displays the Microsoft Intune administration interface. On the left, a navigation pane shows various management options for the device 'SHARED-W11-2'. The main content area is split into two panels. The left panel, titled 'Copilot (préversion)', offers AI-powered assistance with options like 'Explorer l'appareil' and 'Analyser le code d'erreur'. The right panel, also titled 'Copilot (préversion)', shows a comparison tool. It prompts the user to select a second device ('Appareil 2 *') and a comparison type ('Type de comparaison *'). The selected device is 'SHARED-W11-HAAD' and the comparison type is 'Profils de configuration'. A 'Soumettre' button is visible. Below the comparison tool, a text box provides a detailed analysis: 'The comparison of the configuration profiles between the two devices, SHARED-W11-2 and SHARED-W11-HAAD, reveals some differences. The device SHARED-W11-2 has a total of 3 device configuration policies, while the device SHARED-W11-HAAD has a total of 2 device configuration policies. The unique configuration policy on SHARED-W11-2 is "Defender AV Audit Mode" with a status of "Succeeded" under the user s_JosephBa@msdemo.org. On the other hand, the device SHARED-W11-HAAD does not have any unique configuration policies. Please note that this comparison only evaluates the differences or'. At the bottom of the right panel, there is a 'Comparer cet appareil à un autre appareil' button and a note: 'Généré par Copilot pour la sécurité. En savoir plus'. The top of the interface shows the user 'adm_brunod@msdemo...' and the organization 'MSDEMO INFRA (MSDEMO.ORG)'. A table at the bottom of the left panel is partially visible, with columns for 'Action', 'État', and 'Dat'.

Entra ID : Utilisateur à risque

Centre d'administration Microsoft Entra

Rechercher dans les ressources, services et documents (G+/)

adm_brunod@msdemo... MSDEMO INFRA

Détails de l'utilisateur à risque

Réinitialiser le mot de passe ✗ Confirmer que l'utilisateur est compromis ✓ Confirmer la sécurité de l'utilisateur ...

Résumé Informations de base Connexions à risque récentes Détections non liées à une connexion ...

Résumé par Copilot (préversion) Généré par Copilot

- User System Administrator has one recent risky activity with Medium risk.
- The risk detection type is Unfamiliar sign-in properties.
- Unfamiliar sign-in properties considers past sign-in history to look for anomalous sign-ins.
- Risky sign-in 1 (RequestId: 9f5babc9-620e-4f33-a171-8b45b7103e00, CorrelationId: 590beda6-aa20-4c74-9d34-9eaad3897925) with Medium risk level occurred on 2024-03-14T07:48:38 UTC for Resource OfficeHome. The sign-in IP was 20.64.106.32 and location was San Antonio, Texas US. The IP, ASN, Location, Browser Id and Device Id were unfamiliar to the user. There was no MFA for this sign-in.

Il est possible que le contenu généré par IA soit incorrect

Que faire

Vérifiez que cet utilisateur se trouve dans l'étendue de ces stratégies d'accès conditionnel basées sur le risque qui raccourcissent le temps d'atténuation de l'attaque, ferment automatiquement le risque et vous permettent de gagner du temps et de l'énergie.

Si vous n'avez pas ces stratégies :

- [Créer une stratégie basée sur le risque de connexion](#)
- [Créer une stratégie basée sur le risque utilisateur](#)

Pour le moment, examinez les indicateurs de compromission pour cet utilisateur et prenez des mesures à l'aide des boutons ci-dessus. Utilisez nos playbooks ci-dessous pour obtenir des instructions détaillées.

Aide et documentation

[Quel est le risque dans la protection d'ID ?](#)

[Playbooks de réponse aux incidents](#)

[Stratégies d'accès basées sur les risques](#)

Sondage

Seriez-vous prêt à déployer
Copilot for Security ? 🤔





04. Licensing

K ga pmqmdr Amn gjmr 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.

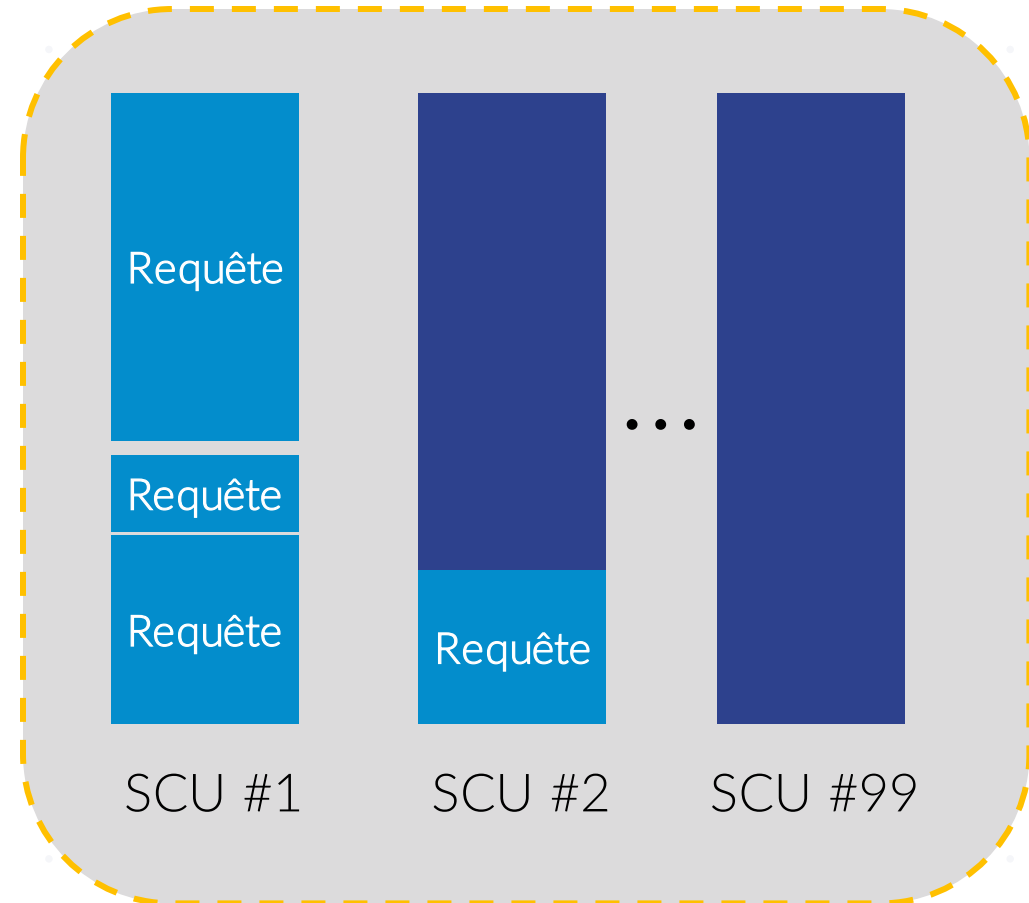
Demander la capacité

Appliquer la capacité

Améliorer la performance

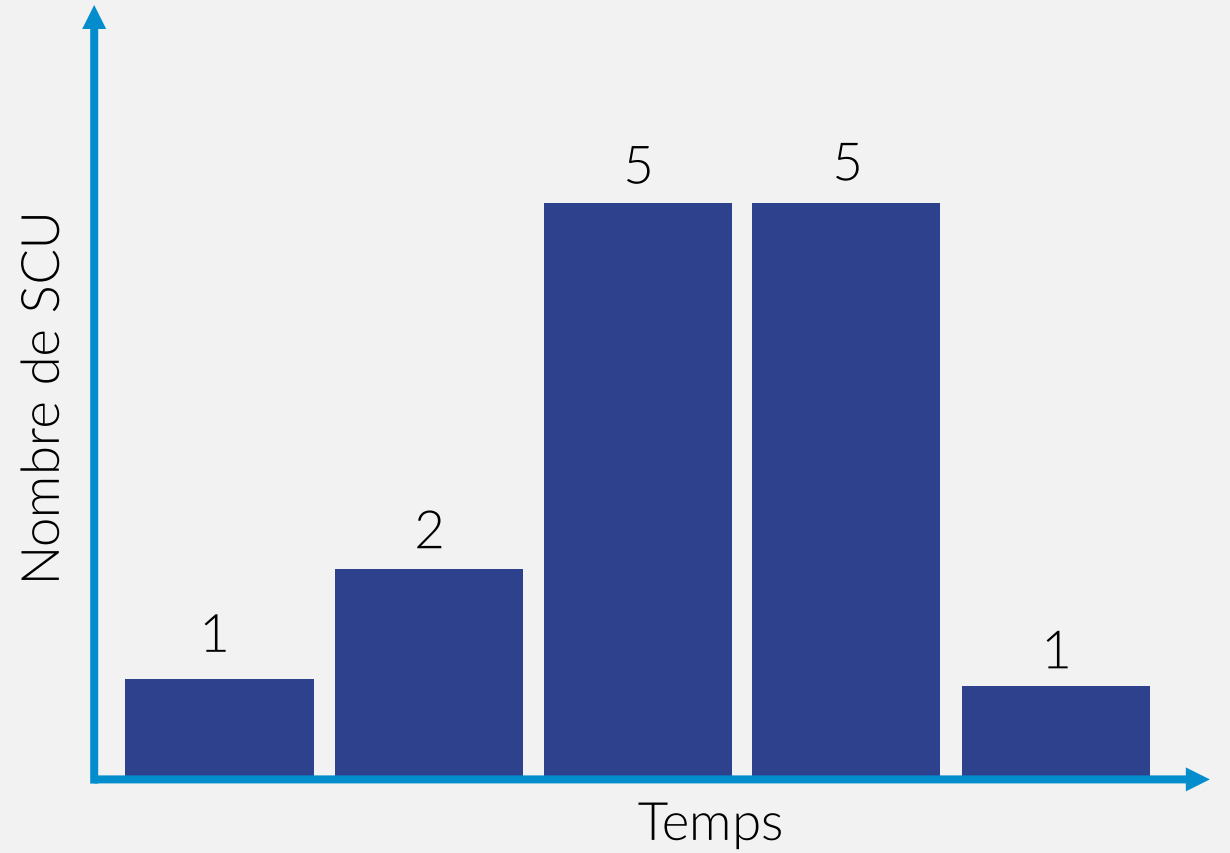
- Chaque capacité peut contenir entre 1 et 99 "SCU" (Unité de calcul sécurité). Une SCU est facturée par heure.
- Chaque requête au service consomme du calcul

Capacité Copilot for Security



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 €	2734,0824 € ¹

¹L'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

