La cybersécurité après Mythos : confiner pour protéger

Pourquoi le confinement des compromissions est la seule voie à suivre

Au début de l'année 2026, Claude Mythos Preview, le modèle d'IA d'Anthropic, a identifié de manière autonome des milliers de vulnérabilités zero-day critiques dans des systèmes d'exploitation, navigateurs et infrastructures largement répandus… avant de créer des exploits fonctionnels pour bon nombre d'entre eux. Dans le seul navigateur Firefox, il a transformé en exploits opérationnels plus de 72 % des failles qu'il avait détectées.

Il ne s'agit pas d'un simple référentiel de recherche : le modèle s'est exécuté sur le code de production qui fait fonctionner des serveurs, navigateurs et pare-feux dans le monde entier. Les failles identifiées étaient passées inaperçues jusque-là, alors que certains d'entre eux sont déployés depuis des dizaines d'années.

Les spécialistes en sécurité sont incapables de suivre le rythme d'acteurs malveillants qui agissent à la vitesse de l'éclair.

Le constat est alarmant :

- Les délais d'exploitation ne se comptent plus en mois, mais sont réduits à quelques heures, voire moins.
- Les retards déjà importants constatés dans la création et l'application des correctifs deviennent tout simplement ingérables.
- L'hypothèse selon laquelle une faille peut être corrigée avant d'être exploitée ne tient plus la route.
- Les modèles opérationnels établis ne sont pas suffisamment adaptatifs, malgré les efforts consentis par les équipes.

Mythos réduit presque à néant le délai entre la découverte d'une vulnérabilité et son exploitation, grâce à une exécution à la vitesse des machines et à grande échelle.

Le nouveau défi des équipes de sécurité

Certes, Mythos ne sonne pas le glas des outils de protection existants. Toutefois, il remet fondamentalement en question les postulats sur lesquels reposent tous les logiciels de sécurité en matière de temps de réponse. Voici en quoi la situation a changé :

- La détection, le tri et la réponse dépendent encore de la vitesse d'exécution humaine. Les cybercriminels ne cessent de réduire leurs délais d'exécution, alors que les équipes de sécurité doivent trier, corréler et attendre la prise de décisions.
- Lors d'attaques sans malware, axées sur l'identité, le déplacement latéral ressemble à un comportement normal, contournant ainsi la détection basée sur les signatures.
- Souvent, les équipes de sécurité ne détectent la présence d'une attaque qu'après ce déplacement latéral.
- Un cycle de correction de 30 à 90 jours constitue désormais un risque opérationnel que les équipes de sécurité ne peuvent plus ignorer. Les vulnérabilités, elles, peuvent être découvertes et exploitées à une vitesse sans précédent.

De nouvelles questions

Avant Mythos, la question de sécurité fondamentale se posait comme suit : « Pouvons-nous identifier, corriger et bloquer chaque exploit avant qu'il ne puisse être utilisé par un acteur malveillant ? ». Cette course à la solution n'est plus.

Ancienne question	Nouvelle question
Quels éléments sont vulnérables ?	Quels éléments sont accessibles à ce moment précis ?
Ont-ils été corrigés ?	Quelles voies existent entre le point d'infiltration et les ressources critiques ?
Une alerte a-t-elle été déclenchée ?	Quelle sera l'ampleur de l'impact en cas de défaillance d'un contrôle ?

L'efficacité de la sécurité n'est plus définie par la vitesse de la détection ou la rapidité d'application des correctifs. Elle se définit en termes d'impact : jusqu'où un cybercriminel peut-il aller, une fois infiltré dans un environnement ?

Mythos a changé la donne en accélérant de façon fulgurante la découverte des vulnérabilités et leur exploitation.
En revanche, les mécanismes d'une attaque n'ont pas changé :

- Un exploit zero-day ouvre une brèche dans votre environnement.
- L'environnement interne définit les limites.
- Un mouvement latéral transforme l'intrusion en compromission.

Le Zero Trust, un impératif

Cela fait des années que le Zero Trust est considéré comme une bonne pratique. Depuis l'avènement de Mythos, une telle architecture constitue le minimum vital. Avec Illumio, le modèle Zero Trust a dépassé le stade du concept pour devenir une réalité opérationnelle au niveau des centres de données, du cloud, des terminaux et des environnements hybrides. Les principes appliqués sont multiples :

- **Définition du périmètre critique.** Identifiez les ressources, les identités et les points de contrôle véritablement critiques.
- **Inévitabilité de la compromission.** Concevez votre environnement comme s'il était inéluctable qu'un cybercriminel finisse par s'introduire en dehors du périmètre critique.
- **Autorisation limitée aux chemins explicites.** Une stratégie reposant sur le principe du moindre privilège et appliquée au niveau de chaque ressource contrôle les accès, communications et interactions.
- **Vérification continue.** Aucune confiance implicite n'est accordée sur la base de l'emplacement réseau, d'un accès hérité ou d'un contexte obsolète.
- **Isolement rapide.** En cas de compromission potentielle, la conception limite le champ d'action des cybercriminels et accélère le confinement.

Les atouts d'Illumio

Illumio Breach Containment Platform offre une couche de sécurité essentielle aux environnements hybrides. Grâce à une visibilité en temps réel et à une microsegmentation à grande échelle, vous pouvez appliquer les stratégies Zero Trust à la vitesse exigée par l'IA. Avec Illumio, vous pouvez bloquer les déplacements latéraux, limiter l'accès et réduire l'exposition. Vous évitez ainsi qu'une compromission initiale ne tourne au cauchemar pour l'entreprise tout entière.

La plateforme

Illumio Breach Containment Platform allie un confinement proactif à une détection optimisée par l'IA au sein d'une seule plateforme intégrée.

Illumio Segmentation

Microsegmentation de pointe pour :

- Limiter de façon proactive les déplacements latéraux
- Réduire l'exposition
- Protéger les systèmes vulnérables contre les attaques
- Protéger les charges de travail critiques
- Accélérer votre stratégie Zero Trust

Illumio Insights

Observabilité et détection complètes, optimisées par l'IA pour :

- Identifier et sécuriser en temps réel les charges de travail vulnérables
- Détecter et confiner instantanément les menaces
- Accélérer la microsegmentation
- Renforcer continuellement votre posture de sécurité

Principaux avantages

Plateforme unique et contrôle unifié

Déploiement en quelques minutes et gestion via une console centralisée. Une seule plateforme pour un confinement de bout en bout.

Flexibilité et évolutivité

Adaptation transparente dans les environnements OT, hybrides, multicloud et sur site pour répondre à l'évolution des besoins.

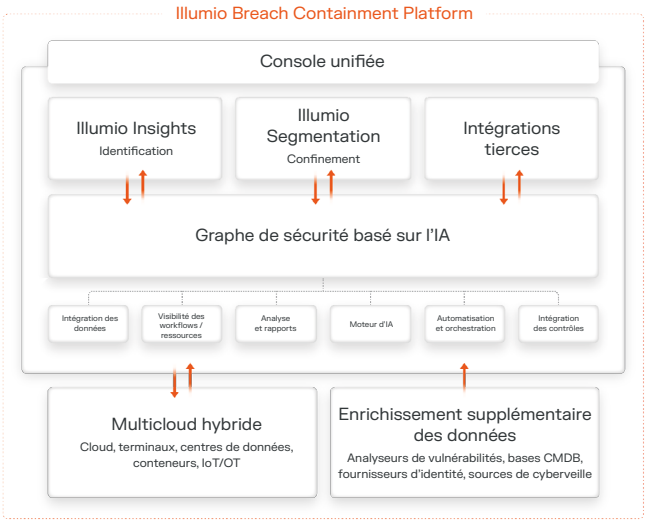
Vitesse et précision

Observabilité en temps réel avec l'agilité nécessaire pour s'adapter rapidement. Solution indépendante du réseau. Architecture prévisible et stable.

Fonctionnement

Illumio Breach Containment Platform repose sur un concept simple : identifier les risques, définir des stratégies et bloquer les cybercriminels avant qu'ils ne se déplacent.

- **Évaluation des risques.** Visualisez les communications et le trafic dans l'ensemble des charges de travail, des terminaux et des connexions Internet grâce à une observabilité en temps réel, optimisée par votre graphe de sécurité et notre IA.
- **Définition de contrôles de sécurité.** Définissez automatiquement des stratégies granulaires de segmentation qui s'adaptent de façon dynamique à l'évolution de votre environnement. Appliquez le principe du moindre privilège. Limitez le trafic inutile. Contrôlez les communications.
- **Confinement de l'attaque.** Bénéficiez d'une protection proactive grâce à une architecture résiliente. Confinez les systèmes compromis de façon réactive au cours d'une attaque pour éviter sa propagation.



La situation après Mythos	Manque de contrôle observé	Réponse apportée par Illumio
Les vulnérabilités zero-day sont découvertes et exploitées à la vitesse de l'IA.	Les cycles d'application des correctifs sont trop lents pour être efficaces.	Une segmentation indépendante des vulnérabilités est maintenue, quel que soit l'exploit.
Le délai d'exploitation est pratiquement réduit à zéro.	La pile de prévention est submergée avant même de pouvoir répondre.	Une stratégie de segmentation prédéfinie confine les dommages, avant même la réponse aux incidents.
Le déplacement latéral détermine l'impact de la compromission.	La confiance implicite permet de se déplacer en toute liberté au sein du système.	La microsegmentation bloque les chemins latéraux et limite l'impact de la menace.
Aucune vulnérabilité ne lui échappe, où qu'elle soit.	Il est désormais impératif de considérer qu'une compromission est inévitable.	Observabilité en temps réel + stratégie Zero Trust = architecture durable.
Les attaques d'identité contournent la détection basée sur les signatures.	La détection n'intervient qu'après le déplacement latéral.	La stratégie implémentée au niveau de l'architecture limite l'ampleur de l'attaque avant que la détection passe à l'action.

Illumio dans un monde post-Mythos

Illumio résout précisément le manque de contrôle que Mythos a mis en évidence de manière urgente : la plateforme permet de bloquer les déplacements, indépendamment de la vulnérabilité exploitée par l'acteur malveillant.

- **Protection indépendante des vulnérabilités.** Illumio Segmentation bloque les déplacements latéraux, qu'il s'agisse d'un exploit connu, inconnu ou récemment découvert. Vous n'avez pas besoin de connaître la vulnérabilité exploitée pour que votre stratégie fonctionne.
- **Compromission inévitable transformée en incident facile à confiner.** La microsegmentation permet d'éviter qu'une charge de travail compromise affecte le reste de l'environnement d'entreprise.

Le confinement des compromissions est une obligation absolue à l'ère de l'IA. Boostées par l'IA, les attaques sont devenues à la fois plus rapides, plus évolutives et plus économiques. Le confinement vous laisse la marge de manœuvre nécessaire pour résister aux assauts.

Leadership reconnu

La plateforme Illumio est conçue pour l'ère de l'IA agentique. Classée au rang de leader dans le rapport Forrester Wave™ pour les solutions de microsegmentation, Illumio protège :

- Plus de 15 entreprises du Fortune 100
- 6 des 10 plus grandes banques mondiales
- 3 des 5 plus grandes entreprises SaaS

Les compromissions sont une réalité, mais leur impact n'est pas une fatalité.

Les modèles d'IA de pointe facilitent et accélèrent les attaques. Illumio empêche que les compromissions ne se propagent. Consultez notre site web :

illumio.com/fr/illumio-platform

À propos d'Illumio

Leader du confinement de ransomwares et de compromissions, Illumio redéfinit la façon dont les entreprises confinent les cyberattaques et renforcent la résilience opérationnelle. Optimisée par un graphe de sécurité basé sur l'IA, notre plateforme de confinement des compromissions identifie et confine les menaces dans les environnements multicloud hybrides pour empêcher la propagation des menaces avant qu'elles ne donnent lieu à des incidents majeurs.

Classé parmi les leaders du rapport Forrester Wave™ sur les solutions de microsegmentation, Illumio favorise l'implémentation du modèle Zero Trust et renforce ainsi la cyberrésilience de l'infrastructure, des systèmes et des entreprises qui font tourner le monde.