

AURA

DÉTECTION ET RÉPONSE POUR
MICROSOFT 365, HÉBERGÉ EN SUISSE

VOTRE PÉRIMÈTRE EST Désormais une page de connexion.

Vos e-mails, vos fichiers, vos réunions et vos identités se trouvent tous dans le même tenant. Un intrus n'a besoin de rien d'autre, et il passe rarement par un exploit. Il lui suffit d'une session volée, d'une application à laquelle quelqu'un a accordé des droits, d'une règle de transfert passée inaperçue.

Tout cela figure dans le journal d'audit. Encore faut-il avoir le temps de le lire assez vite.

**VOS JOURNAUX, VOS DONNÉES,
VOS RÈGLES.**



Aura s'en charge. Il rassemble le journal d'audit unifié, le suivi des messages Exchange et les données Microsoft Graph dans un cluster Elasticsearch, exploité par EXYS en Suisse ou hébergé chez vous, les passe en continu au crible d'un ensemble de règles éprouvées et offre aux analystes un espace de travail commun.

Ils y voient ce qui s'est passé, décident si c'est important et consignent ce qui a été fait. Toutes les données restent en Suisse.

VINGT TABLEAUX DE BORD PRÊTS À L'EMPLOI

Inutile de partir de zéro : Aura est livré avec 20 tableaux de bord et plus de 200 panneaux sur les applications, la posture de sécurité et les connexions, la gouvernance et l'audit, et l'identité, du risque Entra ID Protection aux consentements d'applications et aux règles de boîte aux lettres. Tout est modifiable, et vous pouvez ajouter vos panneaux.

DÉTECTER LES ATTAQUES SUR LES IDENTITÉS

Les règles tournent en permanence et chaque alerte arrive avec ses preuves : voyage impossible, série d'échecs puis connexion réussie, règle qui transfère le courrier hors de l'entreprise, rôle d'administrateur attribué à trois heures du matin. Les alertes fondées deviennent des tickets, avec un responsable et une conclusion écrite.

POSEZ VOS PROPRES QUESTIONS

La page Explore utilise AuraQL, un langage en pipeline qui se lit de gauche à droite : d'abord la recherche, puis ce qu'on en fait. Compter, suivre dans le temps, afficher sur une carte. Chaque résultat devient un panneau en une étape.

CE QUI EST INCLUS :

- Journal d'audit unifié Microsoft 365, suivi des messages Exchange et jeux de données Graph*
- Règles de détection éprouvées, complétées par les vôtres
- Alertes et tickets avec gravité, responsable et historique
- Notifications par Slack, e-mail ou webhook
- Vue d'exploitation : services, tâches, versions et cluster
- 20 tableaux de bord et plus de 200 panneaux, tous modifiables
- Règles dédiées au vol de jetons adversary-in-the-middle
- Rapports PDF planifiés pour qui n'ouvre jamais la console
- Trois rôles : manager, analyste et lecteur
- Exploité par EXYS en Suisse, ou auto-hébergé via Docker ou un binaire

* Journaux de connexion, détections de risques et utilisateurs à risque : Entra ID P1 ou P2 requis.

CONTACTEZ-NOUS

ADRESSE

EXYS SA
Strada Regina 16
CH-6934 Bioggio
Tessin, Suisse

CONTACT

Tél. +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA est certifiée ISO/IEC 27001



EXYS
WHERE PASSION
MEETS TECHNOLOGY

AURA-M365-FR 1v1 20260910