

AURA

IDENTITY THREAT DETECTION AND
RESPONSE - EXYS AURA

IL NUOVO PERIMETRO È L'IDENTITÀ.

Posta, file, riunioni e identità stanno tutti nello stesso tenant. A un intruso non serve altro, e di rado entra con un exploit: entra con una sessione rubata, con un'app a cui un utente ha concesso il consenso OAuth, con una regola di inoltrare che nessuno ha notato.

Tutto finisce nell'audit log. Il difficile è leggerlo prima che sia troppo tardi.

**I VOSTRI LOG, I VOSTRI DATI,
LE VOSTRE REGOLE.**

FAILED SIGN-INS

14

DISTINCT USERS

10

FAILED LOGINS MAP

GRAVITÀ ALTA

Impossible travel

Zurigo e San Paolo a 11 minuti di
distanza, stessa sessione

AURA fa proprio questo. Raccoglie l'audit log, il message trace di Exchange e i dati di Microsoft Graph, arricchisce ogni evento con geolocalizzazione e reputazione di IP e domini e lo analizza in tempo reale con regole selezionate e mantenute da EXYS.

I nostri analisti capiscono cosa è successo, ne valutano la rilevanza e documentano le azioni intraprese. Tutti i dati restano in Svizzera.

VENTI DASHBOARD DAL PRIMO GIORNO

Operativo da subito: 20 dashboard e oltre 200 pannelli su applicazioni, postura di sicurezza e accessi, governance e audit, identità, dal rischio di Entra ID Protection ai consensi alle app e alle regole delle caselle di posta. Ogni pannello è modificabile e se ne possono aggiungere altri.

RILEVAMENTO DEGLI ATTACCHI ALL'IDENTITÀ

Le regole vengono eseguite in tempo reale e ogni alert arriva con le prove: impossible travel, tentativi falliti seguiti da un accesso riuscito, posta inoltrata fuori dall'azienda, ruoli di amministratore assegnati alle tre di notte. Gli alert confermati diventano ticket con un responsabile e un esito documentato.

RICERCHE PERSONALIZZATE

Nella pagina Explore si usa AuraQL, un linguaggio di interrogazione a pipeline che si legge da sinistra a destra: prima la ricerca, poi cosa farne. Contare, rappresentare nel tempo, visualizzare su una mappa. Ogni risultato si salva come pannello in un solo passaggio.

COSA È INCLUSO:

- Audit log unificato di Microsoft 365, message trace di Exchange e dati di Microsoft Graph*
- Regole di rilevamento predefinite e personalizzabili
- Alert e ticket con gravità, responsabile e storico
- Notifiche via email, Slack o webhook
- Arricchimento con geolocalizzazione e reputazione di IP e domini
- 20 dashboard e oltre 200 pannelli, tutti modificabili
- Regole dedicate al furto di token tramite attacchi adversary-in-the-middle (AiTM)
- Report PDF programmati per chi non apre mai la console
- Tre ruoli: responsabile, analista e osservatore
- Gestito dagli analisti EXYS, con tutti i server in Svizzera

* Log di accesso: Entra ID P1 o superiore. Rilevamenti di rischio e utenti a rischio completi: Entra ID P2.

CONTATTI

INDIRIZZO

EXYS SA
Strada Regina 16
CH-6934 Bioggio
Ticino, Svizzera

CONTATTO

Telefono +41 91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA è certificata ISO/IEC 27001



EXYS
WHERE PASSION
MEETS TECHNOLOGY

AURA-M365-IT 1v2 20261015

DISTINCT CLIENT FINGERPRINTS OVER TIME



5 buckets - peak 5 at 27 Aug

