

AURA

ERKENNUNG UND REAKTION FÜR
MICROSOFT 365, GEHOSTET IN DER
SCHWEIZ

IHR PERIMETER IST HEUTE EINE LOGIN-SEITE.

E-Mails, Dateien, Meetings und Identitäten liegen alle im selben Tenant. Mehr braucht ein Angreifer nicht, und hinein kommt er selten über einen Exploit. Er kommt über eine gestohlene Sitzung, eine App, der jemand Zugriff gewährt hat, eine Weiterleitungsregel, die niemandem aufgefallen ist.

All das steht im Audit-Log. Nur hat niemand die Zeit, es schnell genug zu lesen.

**IHRE LOGS, IHRE DATEN,
IHRE REGELN.**

FAILED SIGN-INS

14

DISTINCT USERS

10

FAILED LOGINS MAP

HOHER SCHWEREGRAD

Unmögliche Reise

2 Länder innert 11 Minuten,
dieselbe Sitzung

Aura nimmt Ihnen das Lesen ab. Es führt das Unified Audit Log, den Exchange Message Trace und Datensätze aus Microsoft Graph in einem Elasticsearch-Cluster zusammen, den EXYS in der Schweiz betreibt oder Sie selbst hosten, gleicht sie laufend mit einem gepflegten Regelwerk ab und gibt den Analysten einen gemeinsamen Arbeitsplatz.

Dort sehen sie, was passiert ist, entscheiden, ob es relevant ist, und halten fest, was unternommen wurde. Alle Daten bleiben in der Schweiz.

ZWANZIG DASHBOARDS AB DEM ERSTEN TAG

Sie fangen nicht bei null an: Aura bringt 20 Dashboards und über 200 Panels mit, zu Anwendungen, Sicherheitslage und Anmeldungen, Governance und Audit sowie Identitäten, vom Risiko in Entra ID Protection bis zu App-Einwilligungen und Postfachregeln. Jedes Panel lässt sich anpassen.

IDENTITÄTSANGRIFFE ERKENNEN

Die Regeln laufen ständig, jeder Alarm bringt die Belege mit: unmögliche Reise, Fehlversuche vor erfolgreicher Anmeldung, eine Postfachregel, die Mails nach aussen weiterleitet, Adminrechte um drei Uhr morgens. Echte Vorfälle werden zu Tickets mit Verantwortlichen und dokumentiertem Ergebnis.

EIGENE FRAGEN STELLEN

Die Explore-Seite arbeitet mit AuraQL, einer kurzen Pipeline-Sprache, gelesen von links nach rechts: erst die Suche, dann, was damit geschieht. Zählen, im Zeitverlauf darstellen, auf einer Karte zeigen. Jedes Ergebnis wird in einem Schritt zum Panel.

WAS SIE BEKOMMEN:

- Microsoft 365 Unified Audit Log, Exchange Message Trace und Graph-Datensätze*
- Gepflegte Erkennungsregeln, ergänzt um Ihre eigenen
- Alarme und Tickets mit Schweregrad, Verantwortlichen und Verlauf
- Benachrichtigungen per Slack, E-Mail oder Webhook
- Betriebsansicht: Dienststatus, Tasks, Versionen und Cluster
- 20 Dashboards und über 200 Panels, alle anpassbar
- Spezielles Regelpaket gegen Token-Diebstahl per Adversary-in-the-Middle
- Geplante PDF-Berichte für alle, die die Konsole nie öffnen
- Drei Rollen: Manager, Analyst und Betrachter
- Betrieb durch EXYS in der Schweiz, oder selbst gehostet per Docker oder als Binary

* Anmeldeprotokolle, Risikoerkennungen und riskante Benutzer setzen Entra ID P1 oder P2 voraus.

MIR SIND FÜR SIE DA.

ADRESSE

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

KONTAKT

Telefon +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA ist nach ISO/IEC 27001 zertifiziert



EXYS
WHERE PASSION
MEETS TECHNOLOGY

AURA-M365-DE 1.v1 20260910