

AURA

DETECTION AND RESPONSE FOR
MICROSOFT 365, HOSTED IN
SWITZERLAND

YOUR PERIMETER IS A LOGIN PAGE NOW.

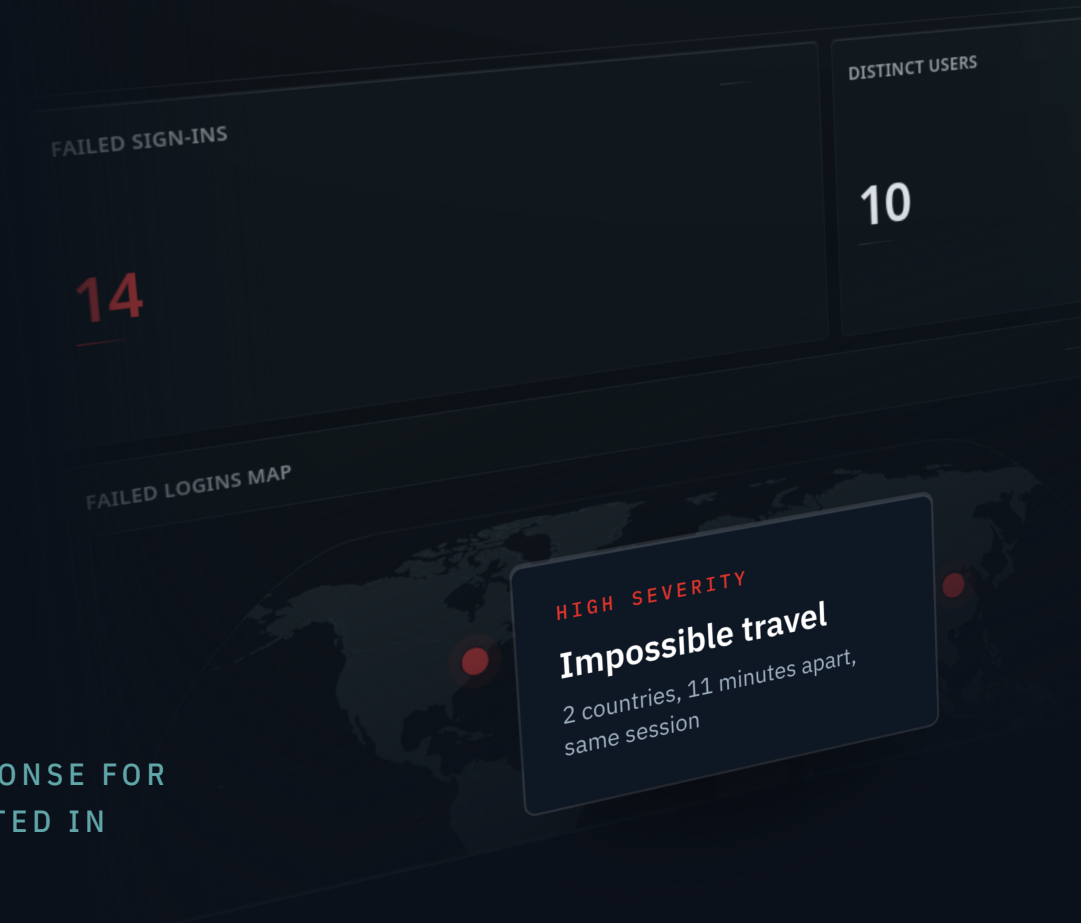
Your mail, your files, your meetings and your identities are all in one tenant. An intruder needs nothing else, and the way in is rarely an exploit. It is a stolen session, an app someone consented to, a forwarding rule nobody noticed.

All of it is written down in the audit log. Reading that log quickly enough is the part nobody has time for.

Aura does the reading. It pulls the unified audit log, the Exchange message trace and Microsoft Graph datasets into an Elasticsearch cluster that EXYS runs in Switzerland or that you host yourself, checks them continuously against a curated rule set, and gives analysts one place to work.

See what happened, decide whether it matters, record what was done about it. All data stays in Switzerland.

**YOUR LOGS, YOUR DATA,
YOUR RULES.**



TWENTY DASHBOARDS, READY ON DAY ONE

No blank canvas. Aura ships with 20 dashboards and more than 200 panels: the applications themselves, security posture and sign-in activity, governance and audit coverage, and identity, from Entra ID Protection risk to app consent and mailbox rules. Every panel is editable and you can add your own.

DETECTION BUILT FOR IDENTITY ATTACKS

Rules run continuously and every alert arrives with its evidence: impossible travel, failures followed by a success, a mailbox rule forwarding mail out of the company, admin roles granted at three in the morning. The real ones become tickets with an owner and a written outcome.

ASK YOUR OWN QUESTIONS

The Explore page speaks AuraQL, a short pipeline language that reads left to right: a search, then what to do with it. Count it, chart it over time, or put it on a world map. Any answer becomes a panel in one step.

WHAT YOU GET:

- Microsoft 365 unified audit log, Exchange message trace and Graph datasets*
- Curated detection rules, plus the ones you write yourself
- Alerts and tickets with severity, owner and analyst history
- Notifications by Slack, email or webhook
- Operations view for service health, tasks, versions and cluster state
- 20 dashboards and more than 200 panels, all editable
- A dedicated pack for adversary-in-the-middle token theft
- Scheduled PDF reports for people who never open the console
- Three roles: manager, analyst and viewer
- Managed by EXYS in Switzerland, or self-hosted with Docker or one binary

* Sign-in logs, risk detections and risky users require Entra ID P1 or P2.

CONTACT US

ADDRESS

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

CONTACT

Phone +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA is ISO/IEC 27001 certified



EXYS
WHERE PASSION
MEETS TECHNOLOGY

AURA-M365 1v1 20260910

DISTINCT CLIENT FINGERPRINTS OVER TIME



buckets - peak 5 at 27 Aug

