



SCIRGE
SHEDDING LIGHT ON SHADOW IT

**100% magyar tulajdonú és
fejlesztésű technológia**

Publikus hazai referenciák:



Sign In

New User? [Create an Account](#)

Continue

or



Felderítés a böngészőből

- Shadow IT, Cloud, SaaS és Web alkalmazások felderítése dedikált böngészőbővítmény segítségével
- Detekció adatbázis nélkül, email címek és SSO alapján
- Lokális management szerver és adatbázis, egyszerű implementáció és architektúra

 mailchimp.com

<> Sales Marketing

Underutilized

New

 x.ai

<> AI Apps

Underutilized

New

 huggingface.co

<> Unsanctioned

<> AI Apps

△ Fresh Domain

Trending

 simplywall.st

<> Finance

SSO Accounts Only

New

 ingatlan.com

<> Legacy

SSO Accounts Only

New

 skarbe.com

<> Sales Marketing

△ Fresh Domain

SSO Accounts Only

New

 hfecorp.com

<> Unsanctioned

Underutilized

 strava.com

SSO Accounts Only

Nyilvántartások

- Teljeskörű leltár a felhasználók által igénybevett szolgáltatásokról és alkalmazásokról
- Alkalmazás profilok felhasználási trendek, kockázatok, vagy egyedi besorolások szerint
- Licenzgazdálkodás támogatása átfedő vagy kihasználatlan szolgáltatások felderítésével

LDAP Password Reuse Accounts

54

last 90 days (vs. previous period)

Breached Password Accounts

366

last 90 days (vs. previous period)

Shared Account Accounts

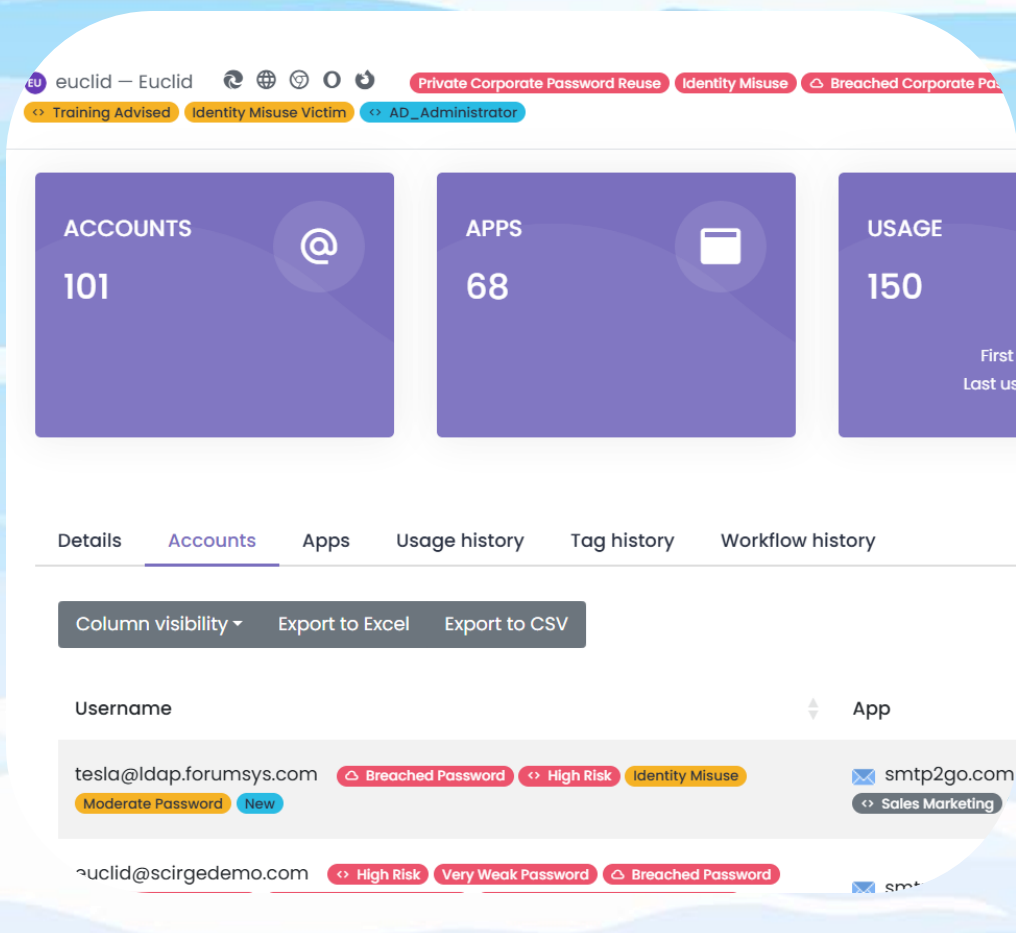
39

Password Reuse Accounts

771

Jelszó Higiénia

- AD, LDAP, OpenID címtárak támogatása
- Minden jelszó ellenőrzése erősség, komplexitás, breach adatbázisok és újrafelhasználás ellen
- Megosztott, böngészőben tárolt, vagy elhagyatott accountok detekciója
- Jelszavak ellenőrzése a böngészőben és hash-ek alapján, jelszó tárolás és felhasználói interakció nélkül



Személyes Leltár

- Leltár minden egyes felhasználóról az általuk használt szolgáltatásokról és accountokról
- Ismeretlen és nem managed fiókok detektálása, kiléptetési folyamat támogatására
- Riasztások a kockázatos jelszavakról és hozzáférésekről

New Accounts

4_{vs.}4

Last 30 days (vs. previous period)

Abandoned Accounts

123

Last 365 days

Shared Account

3

Last 365 days

Abandoned Apps

39

Last 365 days

Password Hygiene P...

3

Last 365 days

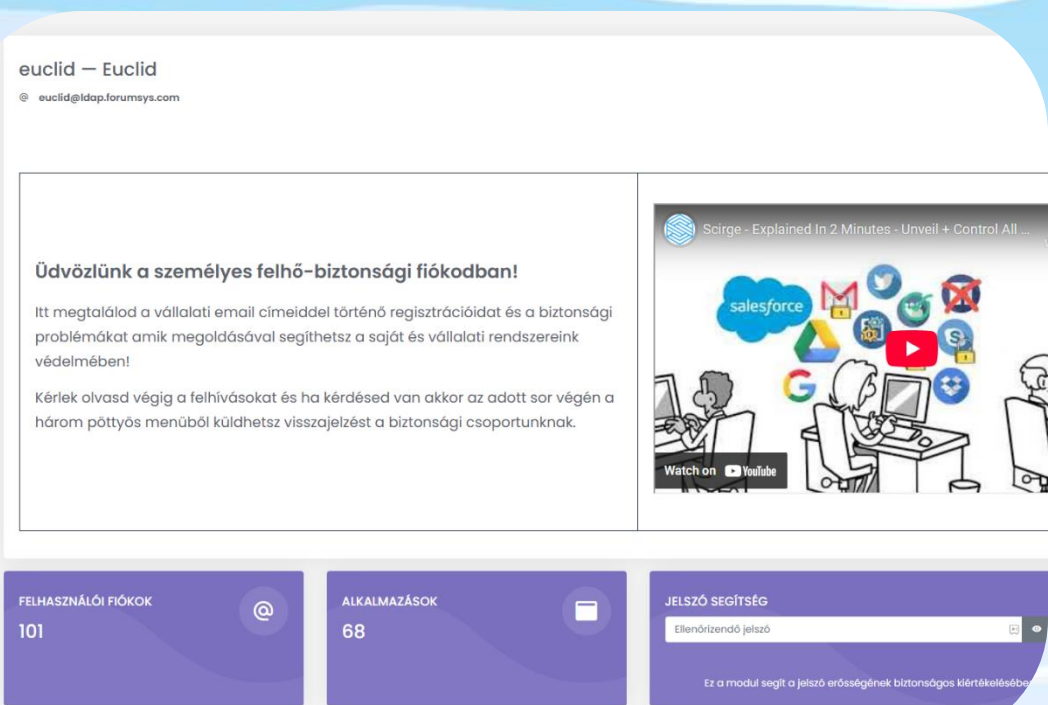
<> Training Advised Pe...

4

Last 365 days

Beszállítói kockázatok és megfelelések

- NIS2, DORA, ISO, MNB és egyéb szabályozások támogatása alkalmazás profilokkal és kategorizációval
- Szerepkörök szerinti riasztások és riportok
- Oktató üzenetek és automatikus értesítések



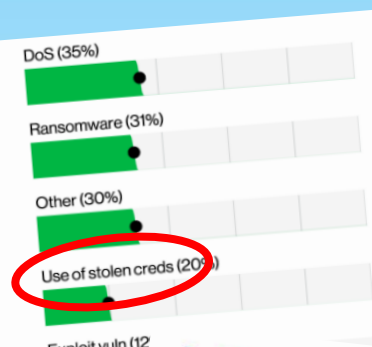
Felhasználói portál

- Valós idejű oktatás a böngészőben
- Egyedi ticketek és riasztások a felhasználók saját hozzáféréseihez kapcsolódóan
- Céges szabályzatok és oktatóanyagok kihelyezése

MITRE | ATT&CK®



Figure 25. Top Action varieties in breaches (n=10,747)



Initial Infection Vector

In contrast to the overall dataset, the most commonly observed initial infection vector for ransomware-related intrusions, when the vector could be identified, was brute-force attacks. Password spraying, virtual private network (VPN) devices compromised through default credentials, and high-volume Remote Desktop Protocol (RDP) login attempts are examples of the types of brute-force attacks that Mandiant observed in 2024. Use of this tactic reinforces the importance of auditing and configuring internet-exposed infrastructure to require multifactor authentication (MFA), to require verification for remote attempts to register MFA on an account for the first time, and to lock accounts after a certain number of failed login attempts.

Stolen credentials and exploits were tied for the second most common initial infection vector for 2024 ransomware-related intrusions at 21% each, followed by prior compromise at 15%, and third-party compromise at 10%.



A támadások jelentős részéért kompromittált jelszavak a felelősek.



Figure 24. Percentage breakdown of GenAI service access account types (each glyph is 0.5%)

A Gen AI hozzáférések 90%-a Shadow IT (Shadow AI)

NIS2

1.5. A szervezet létrehozza és a szervezet EIR-jeiben bekövetkezett változások (pl.: új rendszer bevezetése, meglévő rendszer kivezetése) esetén frissíti, valamint a szervezet **által meghatározott gyakorisággal felülvizsgálja az EIR-ek nyilvántartását**

8.22.1. **Fenntartja a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját**, és ezt a listát a szervezet által meghatározott gyakorisággal frissíti, továbbá minden olyan esetben, amikor a szervezeti jelszavakat közvetlenül vagy közvetett módon veszélyeztetik.

8.22.2. **Ellenőrzi, hogy a felhasználók által létrehozott vagy módosított jelszavak** szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján.

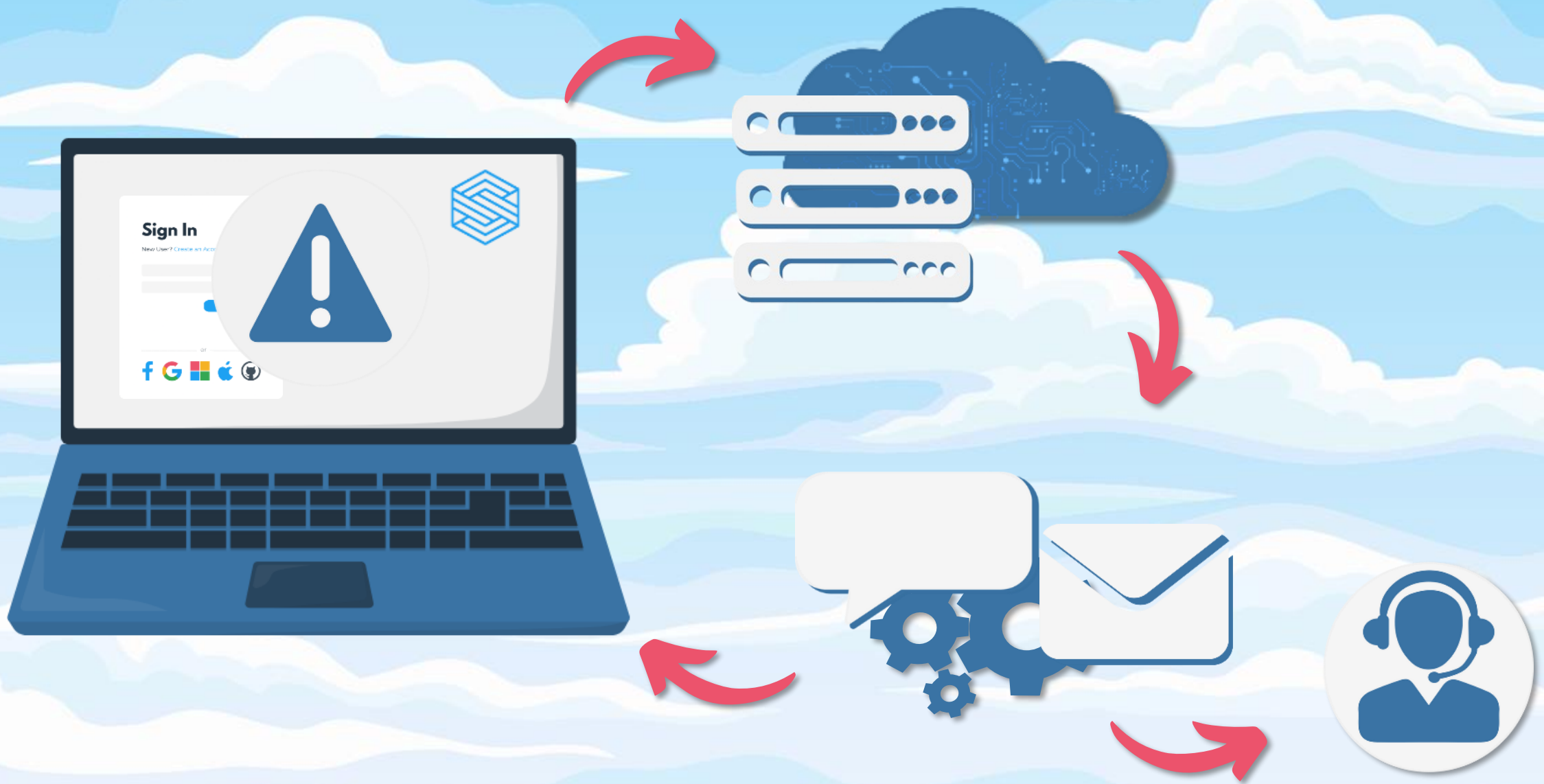
MNB 1/2025 & 2/2025

III.1.4. A felhőszolgáltatás igénybevételével érintett tevékenységek nyilvántartása

14. Az Intézmény naprakész **nyilvántartást vezet az Intézmény, valamint az Intézmény vállalatcsoportja által igénybe vett felhőszolgáltatással érintett** valamennyi olyan tevékenységről – azok lényegességétől függetlenül – amelyek érintik az Intézmény adatait, különös tekintettel az ügyműveletekre

9.4.12. Az intézmény a kockázataival arányos módon gondoskodik az informatikai rendszereiben a **jelszóra vonatkozóan az alábbi szabályok bevezetéséről:**

- a) a jelszó minél több (min. 12, adminisztrátori vagy technikai szerepkörben min. 15.) karaktert vagy jelmondatot tartalmazzon,
- b) a jelszó ne legyen szótár alapú,
- c) a jelszó ne legyen könnyen kitalálható (ne utaljon a felhasználóra, rokonára, tulajdonára stb.)



A Scirge működése

**POC és
további
információk**

