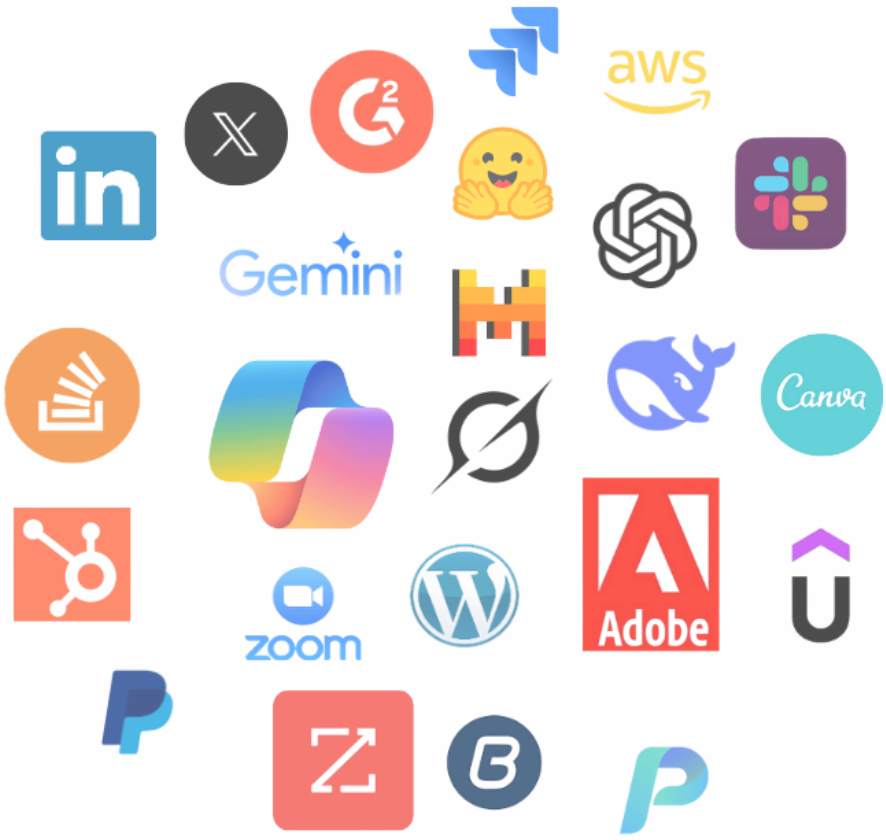
SCIRGE

SHEDDING LIGHT ON SHADOW IT

A felügyelet nélküli Shadow IT-fiókok, AI és egyéb webes alkalmazások támadási felületet, hatékonysági és megfelelőségi kockázatokat hoznak létre.

A Scirge támogatja a technológiai, jogi és biztonsági döntéshozókat a digitális ellátási láncok átláthatóvá tételében, valamint a felhasználói identitások és azonosítók hatékony védelmében.



Shadow IT Láthatóság

A Scirge a SaaS és a felhőalapú webes alkalmazásokat egy menedzselt böngésző-bővítményen keresztül azonosítja. A detekció a bejelentkezéskor használt vállalati e-mail domain, Single Sign-On vagy Passkey alapján történik, így a rendszer előre definiált adatbázis nélkül képes bármely webes szolgáltatás felismerésére.

App leltárak

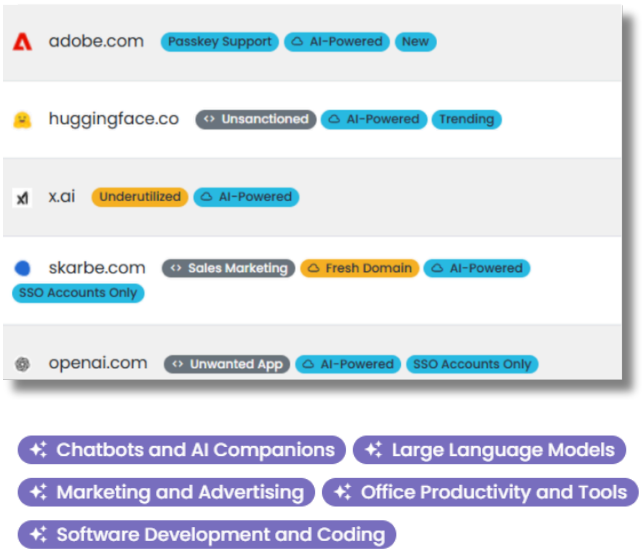
A központi leltárakban az alkalmazások URL-címeit a böngészőből gyűjtött metaadatokkal, valamint a felhasználási trendek adataival bővítjük.

A Scirge Horizon Cloud Intelligence szolgáltatás segítségével létrehozzuk az alkalmazások biztonsági profilját. Többek között ellenőrizzük a domain életkorát, az SSL tanúsítvány megbízhatóságát, feketelistákat és egyéb kockázati paramétereket.

AI katalógus

Az AI-alapú alkalmazásokat egyedileg kategorizáljuk a kockázatos vagy új felhasználási területek könnyebb felismerésének támogatására. Az AI alapú megoldásokat a tevékenységük alapján profilozzuk a potenciális felhasználási területek azonosítására.

Alkalmazás és AI katalógus



Vállalati azonosítók védelme

Az alkalmazottak által létrehozott egyedi fiókok a vállalatok legsérülékenyebb pontjai. A Scirge minden egyes, a böngészőben használt hozzáférést és jelszót felügyeli, hogy megelőzze az olyan gyakori támadási vektorokat, mint például a fiókátvétel, az adathalászat, a zsarolóprogramok telepítése és a belső visszaélések.

Jelszó higiénia

A szabályozási követelményeknek való megfelelés érdekében egyedi jelszókomplexitási szabályokat definiálhatunk. A jelszavak újrafelhasználását, megosztását, valamint korábban ellopott jelszavak használatát biztonságos hash-ek segítségével detektáljuk.

Domain hozzáférések védeleme

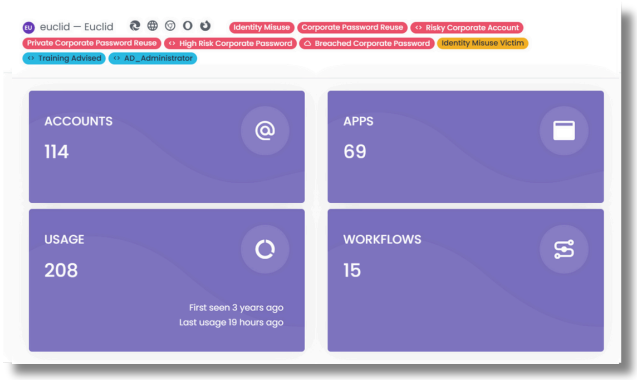
A vállalati domainekhez vagy identity providerekhez tartozó jelszavak minősítése, valamint újrafelhasználásuk azonosítása segít megelőzni a ransomware és egyéb, távoli hozzáféréseken alapuló támadásokat.

Kilépési folyamat támogatása

Az egyedileg létrejött Shadow IT-hozzáférések esetében különösen fontos, hogy a távozó kollégák esetében a szenzitív, licenckötelés vagy szabályozás alá eső hozzáféréseket kezelhessük.

A felhasználói leltárak segítenek átlátni azon hozzáféréseket, amelyeket a felhasználók távozásuk után is szabadon elérhetnének.

Felhasználói hozzáférések profilja



Megfelelőség

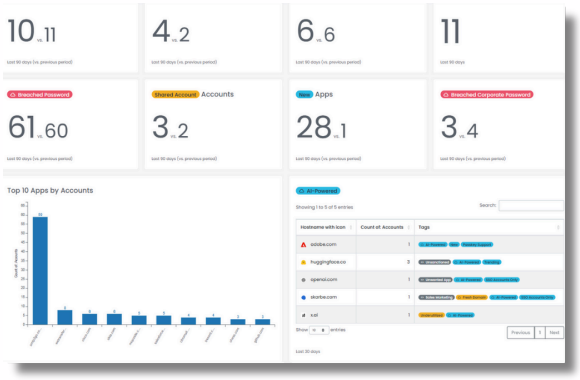
A beszállítók által kiadott ÁSZF-ek és irányelvek a földrajzi és bizalmi adatokkal együtt begyűjtésre kerülnek, hogy a kockázatértékelés és az auditok számára kontextust biztosítsanak.

Az automatikus figyelmeztetések és jelentések lehetővé teszik az érdekeltek és a GRC-szakemberek számára, hogy naprakészek maradjanak a szervezeten belül megjelenő Shadow IT- és AI-szolgáltatásokkal kapcsolatban.

A fiókmegosztási és használati trendek láthatósága lehetővé teszi a szabálytalanságok vagy belső csalások korai felismerését. A kiléptetési folyamatok során a kezeletlen identitások átadása vagy törlése is lehetővé válik.

A NIS2, MNB, DORA és egyéb megfelelőségek Shadow IT-vonatkozásáról további dokumentáció érhető el a scirge.hu weboldalon.

Egyedi riportok



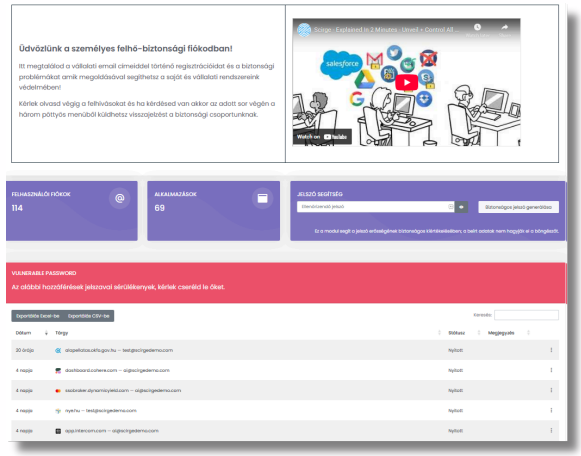
Biztonságtudatosság testreszabva

A különböző üzleti területeken eltérő tapasztalattal és szakmai háttérrel dolgozó munkatársak egyedi megközelítést igényelnek a biztonsági oktatásban is. A Scirge lehetővé teszi, hogy testre szabjuk az oktatási üzeneteinket a kockázatok, valamint a célközönség alapján.

A felhasználók saját tevékenységük alapján kaphatnak figyelmeztetéseket a meglévő ticketingrendszereken keresztül, e-mailben, vagy akár a Scirge személyes ticketingportálján keresztül.

A gyenge vagy újrafelhasznált jelszavak, nem támogatott alkalmazások vagy régen használt belépési adatok kezelésére a szervezet igényei szerint építhetünk egyedi riasztásokat és hibajegyeket.

Személyre szabott oktatás



Architektúra és biztonság

A Scirge egy könnyen telepíthető böngészőbővítmény formájában hajtja végre a központi szabályokat a végpontokon. Az alkalmazásokat és fiókokat a vállalati e-mail címek alapján azonosítja, és a szerveren rendezi leltárakba.

A menedzsment és konfiguráció natív felhőszolgáltatásként, helyben telepíthető appliance-verzióban, valamint menedzselt szolgáltatásként is elérhető. A rendszer a Chrome, Edge és Firefox, valamint a menedzselhető Chromium böngészőket támogatja a főbb végponti operációs rendszereken.

Bizalmasság és adatvédelem

A végpontok a házirendek által szabályozott módon az adatok korlátozott körét gyűjtik össze. Cleartext jelszavak soha nem kerülnek tárolásra. A végpontokon, a hálózati forgalomban és a kiszolgálón is hashelés és titkosítás biztosítja az adatok bizalmasságát és integritását.

A rendszer menedzsmentje adminisztratív szerepkörökkel szabályozható, a személyes adatok védelme automatikus adattárolási szabályokkal és anonimizációval is megerősíthető. Az adatok bizalmasságát mozgatás és tárolás közben is titkosítással védjük.

Tesztelés és további információ

Konzultációért, 30 napos ingyenes tesztidőszakért vagy további információért lépjen velünk kapcsolatba a **hello@scirge.com** címen.

Scirge folyamat

Trusted by

Szellemi Tulajdon Nemzeti Hivatala

Szerencsejáték Zrt.

HOLD

simplepay otp group

kontron The Power of IoT

ALFA VIENNA INSURANCE GROUP

GIRO

BAYER CONSTRUCT