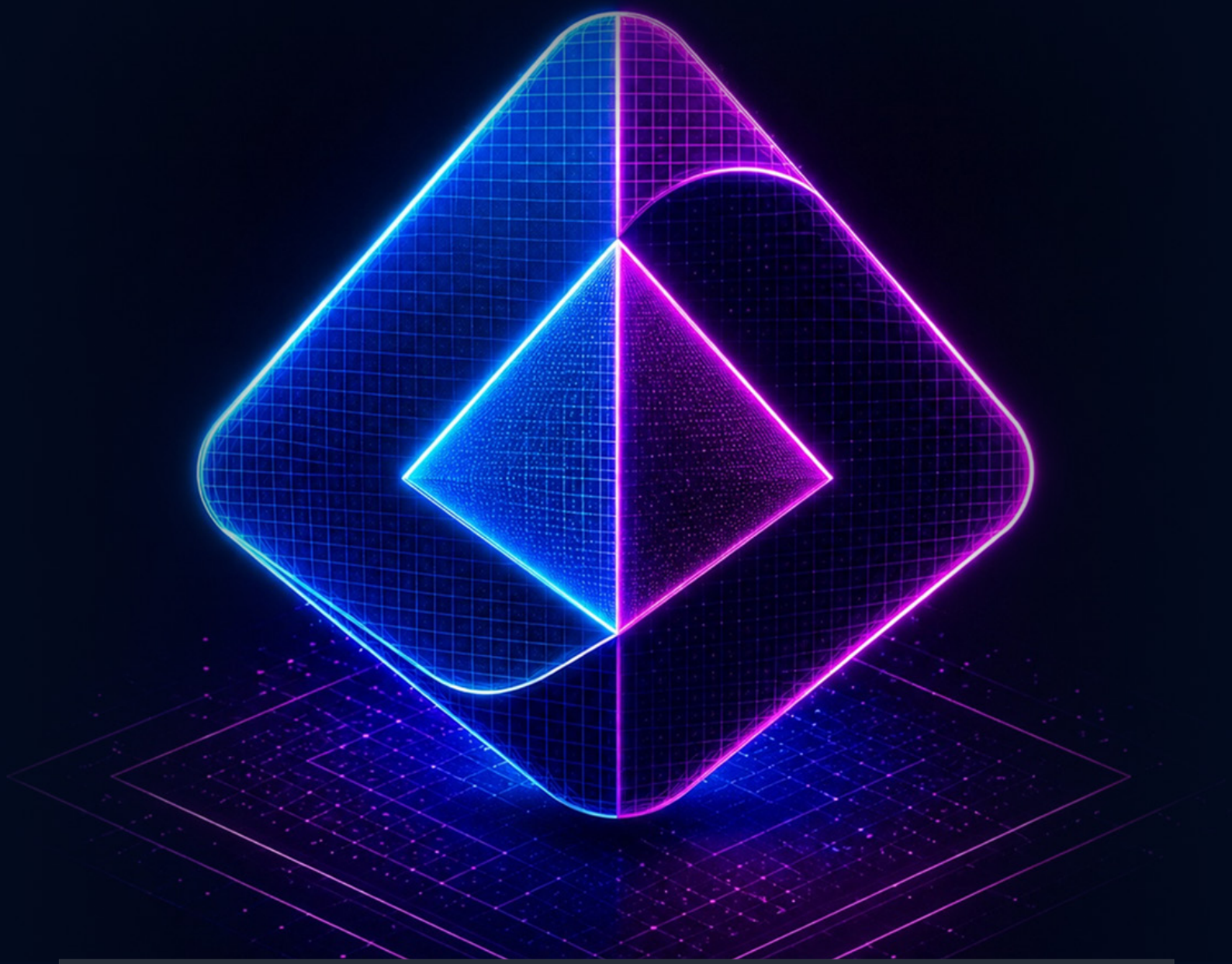
FREEDIVISION

SOLUTION GUIDE



FreeDivision.io AuDit

Identity Security Assesment

Rychlý přehled rizik identit, oprávnění a kvality hesel.

Proč jsou identity nejčastějším cílem útočníků

Většina moderních kybernetických útoků nezačíná kompromitací serveru ani prolomením firewallu.

Začíná kompromitací identity.

Útočníci využívají phishing, krádež přihlašovacích údajů, slabá hesla nebo historické administrátorské účty. Jakmile získají legitimní přístup, mohou se pohybovat prostředím stejně jako běžný uživatel a postupně získávat vyšší oprávnění.

Právě proto dnes ochrana identit představuje jednu z nejvyšších priorit moderní kybernetické bezpečnosti.

Mnoho organizací přitom provozuje Active Directory nebo Entra ID více než deset let. Během této doby vznikají výjimky z bezpečnostních politik, zastaralé administrátorské účty, neaktivní identity, privilegované skupiny bez jasného vlastníka i účty, které používají slabá nebo již kompromitovaná hesla.

Bez pravidelné kontroly se tato rizika postupně kumulují a vytvářejí prostředí, které útočník může snadno zneužít.

Získejte kontrolu nad bezpečností identit dříve, než ji získá útočník.

Executive Summary

Identita se stala novým bezpečnostním perimetrem organizace.

Právě proto představují služby **Microsoft Active Directory a Microsoft Entra ID** jednu z nejkritičtějších součástí bezpečnostní architektury moderní organizace.

FreeDivision.io AuDit poskytuje rychlý a srozumitelný přehled o skutečném stavu identit v organizaci. Kombinuje automatizovanou analýzu prostředí Active Directory a Entra ID s odborným vyhodnocením bezpečnostních specialistů FreeDivision. Výsledkem není pouze seznam technických nálezů, ale prioritizovaný plán nápravy zaměřený na rizika s největším dopadem na bezpečnost organizace.

Řešení lze využít jako jednorázový audit nebo jako pravidelnou kontrolu bezpečnostního stavu identit. Ve spojení s **FreeDivision.io Advanced** se výsledky stávají součástí dlouhodobého řízení bezpečnostních rizik celé organizace.

Jak řešení funguje

FreeDivision.io AuDit je navržen jako rychlá a systematická analýza bezpečnosti identit v prostředí Microsoft Active Directory a Microsoft Entra ID. Jeho cílem není vytvářet rozsáhlé technické reporty, ale poskytnout organizaci jasný přehled o nejvýznamnějších rizicích, jejich prioritě a doporučeném postupu nápravy.

Analýza prostředí identit

Prvním krokem je komplexní analýza prostředí Active Directory a Entra ID.

Řešení mapuje strukturu domén, organizačních jednotek, uživatelských účtů, skupin i vztahů mezi nimi. Současně identifikuje neaktivní identity, zastaralé objekty, historické výjimky a další konfigurace, které mohou představovat bezpečnostní riziko.

Cílem není pouze zjistit, co se v adresářové službě nachází, ale především odhalit prvky, které mohou útočníci využít při kompromitaci infrastruktury.

Kontrola privilegovaných oprávnění

Privilegované účty představují jeden z nejčastějších cílů útočníků.

FreeDivision.io AuDit analyzuje administrátorské skupiny, delegovaná oprávnění i historicky přidělené role. Pomáhá identifikovat nadměrná oprávnění, nevyužívané administrátorské účty nebo skupiny, jejichž členství již neodpovídá skutečným potřebám organizace.

Výsledkem je přehled privilegovaných identit a doporučení, jak jejich správu zjednodušit a současně zvýšit bezpečnost prostředí

Ověření kvality hesel

Kvalita hesel zůstává jedním z nejdůležitějších faktorů ochrany identit.

Řešení bezpečně ověřuje kvalitu hesel prostřednictvím jejich hashů a porovnává je s databázemi známých kompromitovaných hesel. Celý proces probíhá bez přístupu k otevřeným heslům uživatelů, čímž je zachována maximální úroveň ochrany citlivých údajů.

Vedle samotné kvality hesel jsou kontrolovány také zásady jejich správy, historické výjimky z bezpečnostních politik a další konfigurace ovlivňující odolnost identit vůči útokům.

Prioritizace rizik

Ne všechny nalezené problémy mají stejný dopad na bezpečnost organizace.

FreeDivision.io AuDit proto jednotlivé nálezy vyhodnocuje podle jejich závažnosti, potenciálního dopadu i pravděpodobnosti zneužití. Organizace získává jasný přehled o tom, které problémy je vhodné řešit okamžitě a které lze zařadit do dlouhodobého plánu rozvoje bezpečnosti.

Součástí výstupu jsou také doporučení typu **Quick Wins**, tedy opatření s vysokým bezpečnostním přínosem a nízkou implementační náročností.

Manažerské vyhodnocení

Technické informace mají skutečnou hodnotu pouze tehdy, pokud podporují správná rozhodnutí.

Proto je součástí každého auditu přehledné manažerské shrnutí zaměřené na nejvýznamnější rizika, jejich obchodní dopad a doporučené priority nápravy.

Management získává srozumitelný pohled na stav identit v organizaci bez nutnosti studovat rozsáhlé technické výstupy.

Klíčové schopnosti řešení

FreeDivision.io AuDit kombinuje automatizovanou analýzu adresářových služeb s odbornou interpretací výsledků. Organizace tak získává nejen seznam nalezených problémů, ale především doporučení, která pomáhají dlouhodobě zvyšovat bezpečnost identit.

Active Directory a Entra ID

Řešení provádí komplexní kontrolu adresářových služeb, mapuje uživatelské účty, skupiny, oprávnění i vzájemné vztahy mezi objekty. Pomáhá identifikovat zastaralé konfigurace, neaktivní účty a další slabá místa, která mohou zvyšovat bezpečnostní riziko.

Privilegované účty

FreeDivision.io AuDit ověřuje správu administrátorských účtů, členství v privilegovaných skupinách i rozsah přidělených oprávnění. Takto lze snadno odhalit nadměrná oprávnění, historické výjimky nebo účty, které již neodpovídají aktuálním potřebám organizace.

Nastavení hesel

FreeDivision.io AuDit bezpečně kontroluje kvalitu hesel pomocí hashů a porovnává je s databázemi známých kompromitovaných hesel. Současně vyhodnocuje nastavení politik hesel, jejich výjimky a další faktory ovlivňující odolnost identit.

Nálezy a jejich prioritizace

Jednotlivé nálezy jsou rozděleny podle závažnosti a obchodního dopadu. Součástí výstupů jsou doporučení pro rychlá opatření i návrh dlouhodobého plánu zvyšování bezpečnosti identit.

Reporting a podpora auditu

Výsledky auditu jsou prezentovány v přehledné podobě určené jak technickým specialistům, tak managementu. Současně poskytují podklady pro interní audit, regulatorní požadavky, NIS2, zákon o kybernetické bezpečnosti i normu ISO 27001.

Integrace do FreeDivision.io Advanced

V prostředí FreeDivision.io Advanced mohou být výsledky integrovány do jednotného pohledu na bezpečnostní stav organizace a využity při dlouhodobém řízení kybernetických rizik.

Varianty řešení

FreeDivision.io AuDit lze využít jako jednorázové ověření bezpečnostního stavu identit nebo jako pravidelnou službu, která pomáhá dlouhodobě sledovat změny v prostředí Active Directory a Entra ID. Organizace si může zvolit model odpovídající jejím interním kapacitám i požadavkům na řízení bezpečnostních rizik.

[JEDNORÁZOVÝ AUDIT]

Rychlé ověření aktuálního stavu identit

Jednorázový audit je určen organizacím, které chtějí během krátké doby získat objektivní přehled o bezpečnostním stavu Active Directory a Entra ID.

Součástí služby je analýza adresářového prostředí, kontrola privilegovaných účtů a skupin, ověření kvality hesel, identifikace rizikových konfigurací i manažerské shrnutí výsledků. Výstup obsahuje prioritizovaný seznam nálezů a doporučení, která pomohou internímu týmu efektivně plánovat nápravná opatření.

Tato varianta je vhodná například před bezpečnostním auditem, po významných změnách infrastruktury nebo jako výchozí krok při budování programu Identity Security.

[KONTINUÁLNÍ AUDITNÍ SLUŽBA]

Průběžná kontrola bezpečnosti identit

Kontinuální varianta rozšiřuje jednorázový audit o pravidelné opakování kontrol a dlouhodobé sledování bezpečnostního stavu identit.

Řešení průběžně vyhodnocuje změny v prostředí, upozorňuje na nově vzniklá rizika a pomáhá ověřovat účinnost přijatých bezpečnostních opatření. Součástí služby může být také odborná konzultace nad výsledky a doporučení dalších kroků vedoucích ke zvýšení odolnosti organizace.

Výsledky lze integrovat do FreeDivision.io Advanced, kde se stávají součástí jednotného pohledu na bezpečnostní stav organizace a podporují dlouhodobé řízení kybernetických rizik.

Kontinuální auditní služba je ideální pro organizace, které chtějí bezpečnost identit řídit jako průběžný proces, nikoli jako jednorázovou aktivitu.

Typické scénáře využití

FreeDivision.io AuDit nachází uplatnění všude tam, kde organizace potřebuje získat jistotu, že její identity, oprávnění a bezpečnostní politiky odpovídají současným požadavkům na kybernetickou bezpečnost.

Audit Active Directory a Entra ID

Organizace potřebuje typicky ověřit aktuální stav adresářových služeb, identifikovat slabá místa a získat doporučení pro zvýšení jejich bezpečnosti.

FreeDivision.io AuDit poskytuje komplexní přehled o uživatelských účtech, skupinách, oprávněních i konfiguraci prostředí a pomáhá odhalit rizika, která při běžném provozu často zůstávají skrytá.

Ověření bezpečnosti po změnách infrastruktury

Migrace, konsolidace domén, zavedení hybridního prostředí nebo reorganizace IT mohou významně ovlivnit správu identit.

FreeDivision.io AuDit umožňuje ověřit, zda během těchto změn nevznikla nadměrná oprávnění, historické výjimky nebo další konfigurace, které mohou představovat bezpečnostní riziko.

Příprava na audit nebo regulatorní kontrolu

Mnoho organizací potřebuje doložit, že správa identit odpovídá interním politikám i požadavkům regulatorních rámců.

FreeDivision.io AuDit poskytuje přehlednou dokumentaci o stavu identit, přijatých opatřeních i identifikovaných rizicích. Tyto informace lze využít jako podklady pro interní audit, NIS2, zákon o kybernetické bezpečnosti nebo certifikaci podle ISO 27001.

Pravidelné ověřování bezpečnostní hygieny

Bezpečnost identit se mění s každým novým uživatelem, změnou role nebo úpravou oprávnění.

Pravidelná kontrola pomáhá odhalovat zastaralé účty, nadměrná oprávnění, neaktivní identity i další rizikové změny dříve, než mohou být zneužity při skutečném útoku.

Přínosy pro organizaci

Skutečnou hodnotou FreeDivision.io AuDit není pouze identifikace technických problémů. Hlavním přínosem je získání kontroly nad oblastí, která rozhoduje o bezpečnosti celé infrastruktury.

Lepší přehled o identitách

Organizace získává ucelený pohled na uživatelské účty, privilegované skupiny, oprávnění i bezpečnostní konfigurace. Na základě toho lze jednoduše identifikovat kritické slabiny a efektivně plánovat jejich odstranění.

Snížení bezpečnostních rizik

Odhalením slabých nebo kompromitovaných hesel, nadměrných oprávnění, historických výjimek a neaktivních účtů lze výrazně snížit pravděpodobnost zneužití identity i úspěšného laterálního pohybu útočníka v infrastruktuře.

Současně FreeDivision.io AuDit pomáhá odhalit konfigurace, které mohou zvyšovat riziko útoků využívajících techniky, jako je zneužití privilegovaných účtů nebo útoky typu Golden Ticket.

Praktický plán nápravy

Výstupem služby není pouze seznam nálezů, ale především jasně prioritizovaný plán doporučených opatření.

Organizace získává přehled tzv. **Quick Wins**, která lze realizovat s minimálními náklady a okamžitým bezpečnostním přínosem, i doporučení pro dlouhodobé zvyšování úrovně Identity Security.

Podpora compliance

FreeDivision.io AuDit poskytuje doložitelné informace o bezpečnostním stavu identit, identifikovaných rizicích i navržených nápravných opatřeních.

Tyto výstupy usnadňují plnění požadavků NIS2, zákona o kybernetické bezpečnosti, ISO 27001 i dalších interních nebo regulatorních rámců a poskytují managementu i auditorům jasný přehled o úrovni řízení identit v organizaci.

Proč FreeDivision

Bezpečnost identit není jednorázový projekt. Je to dlouhodobý proces, který vyžaduje správnou kombinaci technologií, odborných znalostí a dobře nastavených bezpečnostních postupů.

Proto stavíme všechna řešení platformy FreeDivision.io na třech vzájemně propojených pilířích.

Technologie

FreeDivision.io AuDit využívá moderní nástroje pro analýzu Active Directory, Microsoft Entra ID a správu identit. Automatizovaná kontrola prostředí umožňuje rychle identifikovat rizikové konfigurace, slabá nebo kompromitovaná hesla, nadměrná oprávnění i další slabá místa, která mohou ovlivnit bezpečnost celé infrastruktury.

Kontrola kvality hesel probíhá bezpečně prostřednictvím jejich hashů, bez přístupu k otevřeným heslům uživatelů. Organizace tak získává vysokou úroveň bezpečnosti i důvěryhodné výsledky analýzy.

Experti

Technologie dokáže odhalit problémy, skutečnou hodnotu však přináší jejich správná interpretace.

Specialisté FreeDivision vyhodnocují výsledky analýzy v kontextu konkrétního prostředí zákazníka a pomáhají rozlišit mezi běžnými provozními odchylkami a riziky, která mohou mít zásadní dopad na bezpečnost organizace.

Součástí služby je prioritizace nálezů, doporučení rychlých opatření i návrh dlouhodobého rozvoje bezpečnosti identit. Organizace tak získává jasný plán dalšího postupu namísto rozsáhlého technického reportu bez praktického využití.

Procesy

Správa identit se neustále mění. Přicházejí noví zaměstnanci, mění se pracovní role, vznikají nové administrátorské účty i další bezpečnostní výjimky.

FreeDivision.io AuDit pomáhá zavést pravidelný proces kontroly identit, který umožňuje průběžně sledovat změny, ověřovat účinnost přijatých opatření a dlouhodobě udržovat vysokou úroveň Identity Security.

FreeDivision.io jako platforma pro komplexní kybernetickou bezpečnost

FreeDivision.io AuDit je součástí otevřené platformy FreeDivision.io, která propojuje moderní bezpečnostní technologie, odborné služby a řízené bezpečnostní procesy do jednotného ekosystému.

Každé řešení platformy pokrývá specifickou oblast kybernetické bezpečnosti. Společně vytvářejí architekturu, která organizacím pomáhá předcházet incidentům, efektivně reagovat na hrozby a dlouhodobě zvyšovat jejich kybernetickou odolnost.

Ochrana koncových zařízení

FreeDivision.io Essential poskytuje řízenou ochranu pracovních stanic, notebooků a serverů prostřednictvím moderních technologií EDR/XDR. Pomáhá včas detekovat hrozby, reagovat na incidenty a minimalizovat jejich dopad.

Řízení bezpečnostních operací

FreeDivision.io Advanced centralizuje monitoring, korelaci bezpečnostních událostí, automatizaci reakcí i řízení bezpečnostních operací. Organizace získává jednotný přehled o stavu své bezpečnostní architektury a efektivnější správu bezpečnostních procesů.

Rozvoj bezpečnostního povědomí

FreeDivision.io PhishingGym pomáhá systematicky snižovat rizika spojená s lidským faktorem prostřednictvím phishingových simulací, mikroškolení a průběžného vyhodnocování bezpečnostního povědomí zaměstnanců.

Bezpečnost identit

FreeDivision.io AuDit doplňuje platformu o oblast Identity Security. Poskytuje rychlý přehled o bezpečnostním stavu Active Directory a Entra ID, identifikuje kritická rizika a pomáhá organizacím systematicky zvyšovat úroveň ochrany identit a privilegovaných účtů.

Výsledky z FreeDivision.io AuDit lze integrovat do prostředí FreeDivision.io Advanced, kde jsou informace o identitách propojeny s bezpečnostními událostmi, monitoringem i dalšími oblastmi řízení rizik. Organizace tak získává ucelený pohled na technická rizika i rizika spojená s identitami v jednom prostředí.

For Safety Reasons. Be Best. Not First.

Závěr

Identita dnes představuje jedno z nejcennějších bezpečnostních aktiv každé organizace. Současně je také jedním z nejčastějších cílů moderních kybernetických útoků.

FreeDivision.io AuDit pomáhá organizacím získat kontrolu nad bezpečností Active Directory, Entra ID a nad správou identit. Kombinace automatizované analýzy a odborného vyhodnocení umožňuje rychle identifikovat slabá hesla, nadměrná oprávnění, historické výjimky i další konfigurace, které mohou představovat významné bezpečnostní riziko.

Výsledkem není pouze technický audit, ale především jasný plán nápravy založený na prioritách a skutečném dopadu jednotlivých rizik.

Ve spojení s řešeními **FreeDivision.io Essential, FreeDivision.io Advanced, FreeDivision.io Services** a **FreeDivision.io PhishingGym** představuje FreeDivision.io AuDit důležitou součást komplexní bezpečnostní architektury zaměřené na ochranu technologií, identit i lidí.

Připraveni získat kontrolu nad bezpečností identit?

Každá organizace spoléhá na důvěryhodnost svých identit. Je proto důležité pravidelně ověřovat, že uživatelské účty, oprávnění i zásady správy hesel odpovídají aktuálním bezpečnostním požadavkům.

Společně s vámi provedeme analýzu prostředí Active Directory a Entra ID včetně validace kvality hesel, identifikujeme nejvýznamnější rizika a navrhneme praktická opatření, která pomohou zvýšit úroveň ochrany identit bez zbytečné technické složitosti.

ADRESA

FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

KONTAKT

sales@freedivision.com
+420 220 972 426

www.freedivision.io