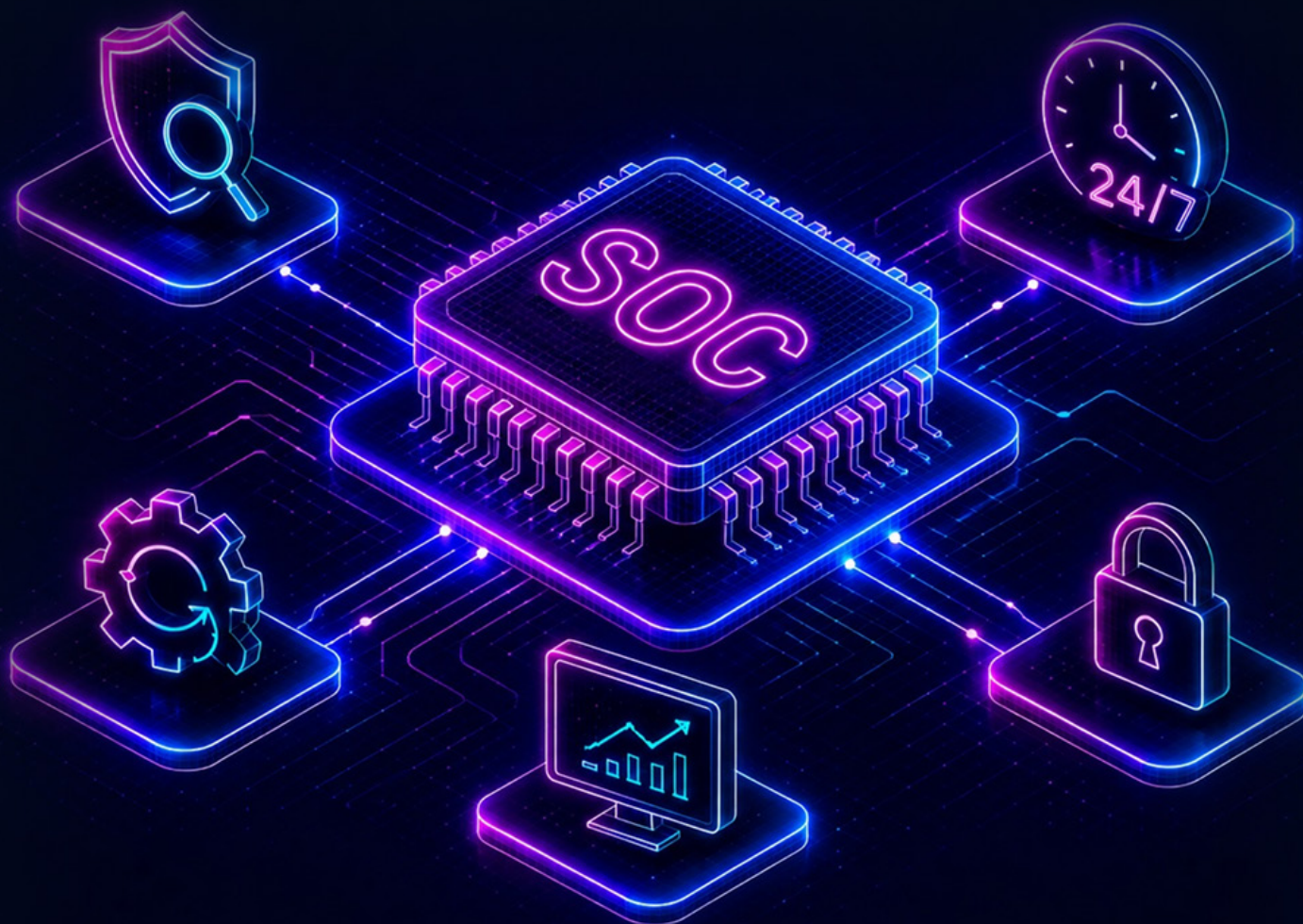




FreeDivision.io Services

Cybersecurity Expertise

Odbornost, expertíza a profesionální přístup.



Odborné služby pro bezpečný provoz a dlouhodobý rozvoj kybernetické bezpečnosti

Moderní kybernetická bezpečnost není dána pouze kvalitou nasazených technologií. Stejně důležité jsou odborné znalosti lidí, správně nastavené procesy a schopnost průběžně reagovat na nové hrozby, změny infrastruktury i rostoucí regulační požadavky.

Mnoho organizací dnes disponuje kvalitními bezpečnostními technologiemi, přesto však naráží na omezené personální kapacity. Nedo-
statek zkušených bezpečnostních specialistů, rostoucí množství bezpečnostních událostí i stále složitější IT prostředí zvyšují nároky na
každodenní provoz a rozvoj bezpečnostní architektury.

Budování vlastního bezpečnostního týmu je dlouhodobý proces. Vyžaduje nábor specialistů, jejich průběžné vzdělávání, sdílení zkuše-
ností i nepřetržitou dostupnost odborných kapacit. Pro řadu organizací proto představuje efektivnější cestu spolupráce s partnerem,
který kombinuje technologické znalosti, praktické zkušenosti z provozu i metodický přístup k řízení kybernetické bezpečnosti.

FreeDivision.io Services vznikly právě s tímto cílem.

Představují soubor odborných služeb, které organizacím pomáhají navrhovat, implementovat, provozovat a dlouhodobě rozvíjet
jejich bezpečnostní prostředí. Nejde pouze o jednorázové projekty nebo technickou podporu. Řešení je postaveno na dlouhodobé
spolupráci, při níž se naši specialisté stávají přirozeným rozšířením interního IT a bezpečnostního týmu.

Služby pokrývají celý životní cyklus bezpečnostních řešení – od vstupních analýz a auditů přes implementaci a integraci technolo-
gií až po jejich každodenní provoz, monitoring, technickou podporu a průběžnou optimalizaci.

Organizace si přitom může zvolit rozsah spolupráce podle vlastních potřeb. Některé využívají naše experty při jednorázových
projektech, jiné nám svěřují dlouhodobý provoz vybraných bezpečnostních technologií nebo pravidelně konzultují rozvoj své bez-
pečnostní architektury.

FreeDivision.io Services nejsou náhradou interního týmu. Jsou jeho odborným rozšířením. Přinášíme zkušenosti z různých
prostředí, ověřené metodiky a praktické know-how, které organizacím umožňuje zvyšovat úroveň kybernetické bezpečnosti bez
nutnosti budovat rozsáhlé vlastní specializované kapacity.

Executive Summary

FreeDivision.io Services představují portfolio odborných služeb, které podporují celý životní cyklus kybernetické bezpečnosti – od návrhu řešení přes implementaci až po dlouhodobý provoz, monitoring a rozvoj bezpečnostního prostředí. Solution Guide 2

Naši specialisté pomáhají organizacím efektivně využívat bezpečnostní technologie, nastavovat provozní procesy, reagovat na bezpečnostní incidenty a průběžně zvyšovat úroveň ochrany informačních systémů.

Portfolio zahrnuje bezpečnostní audity, implementační a integrační služby, technickou podporu, dohled nad bezpečnostním prostředím, správu životního cyklu technologií i specializované konzultační služby.

FreeDivision.io Services doplňují především řešení **FreeDivision.io Essential** a **FreeDivision.io Advanced** a zároveň podporují další rozvoj celé platformy FreeDivision.io. Organizace tak získává nejen moderní bezpečnostní technologie, ale hlavně zkušeného partnera, který pomáhá dlouhodobě budovat a rozvíjet bezpečnostní architekturu.



Technologie jsou základ.
Odborníci dělají rozdíl.

Proč organizace potřebují odborné bezpečnostní služby

Kybernetická bezpečnost se v posledních letech stala jednou z nejrychleji se rozvíjejících oblastí informačních technologií. Nové typy útoků, rychlý vývoj bezpečnostních technologií i rostoucí regulatorní požadavky kladou stále vyšší nároky na odborné znalosti a každodenní provoz bezpečnostního prostředí.

Řada organizací přitom disponuje kvalitními technologiemi, ale nemá dostatek specialistů, kteří by dokázali jejich možnosti dlouhodobě využívat naplno. Bezpečnostní řešení vyžadují pravidelnou správu, aktualizaci, průběžné vyhodnocování bezpečnostních událostí i schopnost reagovat na nové hrozby a měnící se provozní podmínky.

Současně je stále obtížnější získat zkušené odborníky na kybernetickou bezpečnost. Organizace proto často stojí před rozhodnutím, zda budovat vlastní specializovaný tým, nebo využít podporu partnera, který disponuje potřebnými znalostmi, zkušenostmi i ověřenými postupy.

FreeDivision.io Services představují flexibilní model spolupráce, který umožňuje přizpůsobit rozsah odborných služeb skutečným potřebám organizace. Zákazník si může vybrat jednorázovou konzultaci, implementační podporu, dlouhodobý provoz vybraných technologií nebo komplexní spolupráci pokrývající celý životní cyklus bezpečnostního řešení.

Výsledkem je vyšší efektivita bezpečnostních technologií, lepší využití interních kapacit a jistota, že se o klíčové oblasti kybernetické bezpečnosti starají odborníci s praktickými zkušenostmi z různorodých prostředí.

Jak funguje model FreeDivision.io Services

FreeDivision.io Services je model postavený na principu dlouhodobého partnerství. Cílem není poskytovat izolované služby, ale vytvořit takovou spolupráci, která podporuje organizaci ve všech fázích budování a provozu kybernetické bezpečnosti.

Spolupráce obvykle začíná analýzou stávajícího prostředí a identifikací oblastí, které vyžadují vyšší úroveň ochrany, změnu procesů nebo efektivnější využití stávajících Solution Guide 3 technologií. Na základě těchto informací je navržen rozsah služeb odpovídající velikosti organizace, jejím provozním požadavkům i dlouhodobým cílům.

Následuje implementace nebo optimalizace bezpečnostních technologií, jejich integrace do stávající infrastruktury a nastavení provozních procesů. Důraz je kladen na to, aby nové řešení přirozeně zapadlo do prostředí organizace a podporovalo každodenní činnost IT i bezpečnostních týmů.

Po uvedení do provozu mohou naši specialisté zajišťovat průběžnou technickou podporu, správu životního cyklu technologií, konsultační činnost, bezpečnostní monitoring nebo podporu při řešení incidentů. Rozsah spolupráce lze průběžně upravovat podle aktuálních potřeb organizace.

Důležitou součástí modelu je také pravidelné vyhodnocování bezpečnostního prostředí. Na základě provozních zkušeností, nových hrozeb i změn v infrastruktuře navrhujeme další kroky vedoucí ke zvýšení úrovně ochrany a efektivnějšímu využití bezpečnostních technologií.

FreeDivision.io Services tak nepředstavují jednorázový projekt, ale dlouhodobou podporu, která pomáhá organizacím rozvíjet jejich bezpečnostní architekturu systematicky a s ohledem na budoucí potřeby.

Portfolio služeb

Portfolio FreeDivision.io Services pokrývá celý životní cyklus kybernetické bezpečnosti – od úvodního posouzení stavu prostředí přes implementaci technologií až po jejich každodenní provoz a dlouhodobý rozvoj.

Posouzení bezpečnostního prostředí

Kvalitní rozhodnutí vycházejí ze znalosti aktuálního stavu. Proto nabízíme služby zaměřené na identifikaci rizik, ověření konfigurace a posouzení úrovně zabezpečení klíčových částí infrastruktury.

Typicky zahrnují:

- audit Microsoft Active Directory,
- audit Microsoft Entra ID,
- audit heslové politiky,
- bezpečnostní analýzy,
- specializované skeny na míru.

Výstupem je přehled identifikovaných rizik, jejich prioritizace a doporučení konkrétních opatření.

Implementace a integrace

Úspěšnost bezpečnostního řešení závisí nejen na zvolené technologii, ale také na kvalitě její implementace. Solution Guide 4

Naši specialisté zajišťují návrh architektury, instalaci, konfiguraci, integraci do stávajícího prostředí, migrace i projektové řízení. Cílem je bezpečné a efektivní nasazení řešení s minimálním dopadem na běžný provoz organizace.

Součástí implementace je také předání znalostí interním administrátorům a podpora při uvedení řešení do produkčního provozu.

Provoz, dohled a technická podpora

Nasazením bezpečnostních technologií práce nekončí. Skutečná hodnota řešení se projevuje až při jeho každodenním provozu, pravidelné správě a schopnosti pružně reagovat na změny prostředí i nové bezpečnostní hrozby.

FreeDivision.io Services poskytuje odbornou podporu, která organizacím umožňuje dlouhodobě udržovat vysokou úroveň zabezpečení bez nutnosti budovat rozsáhlé vlastní specializované týmy.

Bezpečnostní dohled

Průběžný monitoring bezpečnostního prostředí představuje jeden ze základních předpokladů včasné detekce incidentů.

Naši specialisté pomáhají organizacím monitorovat bezpečnostní události, vyhodnocovat jejich závažnost a doporučovat odpovídající reakci. V prostředích využívajících řešení FreeDivision.io Advanced lze monitoring rozšířit o centralizovanou korelaci událostí, automatizované procesy i podporu bezpečnostních analytiků.

Rozsah dohledu lze přizpůsobit požadavkům organizace – od podpory interního bezpečnostního týmu až po komplexní model řízené služby.

Technická podpora

Bezpečnostní technologie se neustále vyvíjejí. Aktualizace produktů, změny konfigurace i nové požadavky na provoz vyžadují pravidelnou odbornou podporu.

FreeDivision.io Services poskytuje technickou podporu zaměřenou na správu bezpečnostních řešení, řešení provozních problémů, konzultace konfigurace i podporu při změnách infrastruktury.

Cílem není pouze odstraňovat vzniklé problémy, ale především předcházet jejich vzniku prostřednictvím průběžné optimalizace prostředí.

Správa životního cyklu technologií

Každé bezpečnostní řešení prochází během svého provozu řadou změn – od prvotního nasazení přes rozšiřování funkcionalit až po modernizaci nebo nahrazení novou technologií.

Naši specialisté pomáhají plánovat jednotlivé etapy životního cyklu bezpečnostních řešení tak, aby organizace dlouhodobě využívala jejich plný potenciál a současně minimalizovala provozní rizika.

Součástí této oblasti jsou pravidelné revize konfigurace, doporučení pro další rozvoj, plánování verzí i podpora při modernizaci bezpečnostního prostředí.

Podpora při řešení bezpečnostních incidentů

Bezpečnostní incidenty vyžadují rychlé rozhodování, správnou koordinaci a dostatek zkušeností.

FreeDivision.io Services poskytuje odbornou podporu při analýze incidentů, návrhu nápravných opatření i obnově bezpečného provozu. Naši specialisté spolupracují s interními týmy zákazníka a pomáhají minimalizovat dopady incidentů na provoz organizace.

Důraz klademe nejen na zvládnutí samotné bezpečnostní události, ale také na identifikaci jejích příčin a návrh opatření, která sníží pravděpodobnost opakování obdobné situace.

Typické scénáře využití

FreeDivision.io Services podporuje organizace v různých fázích rozvoje jejich bezpečnostního prostředí. Rozsah spolupráce se vždy přizpůsobuje konkrétním potřebám zákazníka – od jednorázových projektů až po dlouhodobé partnerství.

Ověření úrovně zabezpečení

Organizace potřebuje získat objektivní pohled na stav svého prostředí, identifikovat slabá místa a stanovit priority dalšího rozvoje.

Naši specialisté realizují bezpečnostní audity, analýzy a specializované skeny, jejichž výsledkem je přehled rizik a doporučení konkrétních opatření.

Nasazení nových bezpečnostních technologií

Implementace bezpečnostních řešení vyžaduje zkušenosti nejen s konkrétní technologií, ale také s integrací do stávající infrastruktury.

FreeDivision.io Services zajišťuje návrh architektury, implementaci, konfiguraci, migraci i předání řešení do produkčního provozu.

Podpora interního IT a bezpečnostního týmu

Interní specialisté často potřebují konzultovat složitější technické otázky nebo získat podporu při řešení specifických bezpečnostních situací.

Naši odborníci rozšiřují kapacity zákazníka a přinášejí zkušenosti z projektů realizovaných v různých typech organizací.

Dlouhodobý provoz bezpečnostních řešení

Mnoho organizací preferuje model, ve kterém odbornou správu vybraných technologií zajišťuje externí partner.

FreeDivision.io Services poskytuje dlouhodobou podporu zahrnující technickou správu, pravidelné revize konfigurace, doporučení pro další rozvoj i podporu při změnách infrastruktury.

Rozvoj bezpečnostní architektury

Kybernetická bezpečnost není jednorázový projekt.

Společně se zákazníkem průběžně vyhodnocujeme nové požadavky, změny provozního prostředí i vývoj hrozeb a navrhujeme další kroky vedoucí ke zvyšování úrovně zabezpečení.

Přínosy pro organizaci

Největší hodnotou FreeDivision.io Services nejsou jednotlivé odborné služby, ale jejich dlouhodobý přínos pro provoz a rozvoj kybernetické bezpečnosti.

Přístup ke zkušeným specialistům

Organizace získává podporu odborníků se zkušenostmi z implementace, provozu i rozvoje bezpečnostních řešení v různých prostředích. Nemusí budovat vlastní rozsáhlý specializovaný tým a současně má k dispozici znalosti potřebné pro řešení běžných i mimořádných situací.

Efektivnější využití interních kapacit

Převzetím vybraných odborných činností umožňujeme interním IT týmům soustředit se na strategické úkoly a rozvoj informačních systémů místo rutinních provozních aktivit.

Rychlejší zavádění změn

Zkušenosti z realizovaných projektů umožňují efektivněji plánovat implementace, minimalizovat provozní rizika a zkrátit dobu potřebnou pro nasazení nových bezpečnostních technologií.

Dlouhodobý rozvoj bezpečnostního prostředí

FreeDivision.io Services podporuje organizace nejen při řešení aktuálních potřeb, ale také při plánování dalšího rozvoje bezpečnostní architektury. Na základě pravidelných konzultací, revizí a doporučení získává zákazník jistotu, že jeho bezpečnostní prostředí bude odpovídat měnícím se požadavkům i budoucím výzvám.

Proč FreeDivision

Úspěšná kybernetická bezpečnost nevzniká nasazením jediné technologie ani jednorázovým projektem. Je výsledkem dlouhodobé spolupráce, správně nastavených procesů a odborných zkušeností, které organizaci pomáhají reagovat na měnící se prostředí i nové bezpečnostní výzvy.

Proto stavíme všechny služby FreeDivision.io na třech vzájemně propojených pilířích.

Technologie

Využíváme ověřené bezpečnostní technologie předních světových výrobců a navrhujeme jejich efektivní využití v prostředí konkrétní organizace. Důraz klademe na otevřenou architekturu, vzájemnou integraci jednotlivých řešení a jejich dlouhodobou udržitelnost.

Naším cílem není zavádět další izolované nástroje, ale vytvářet bezpečnostní architekturu, která podporuje každodenní provoz organizace a umožňuje její další rozvoj.

Experti

Za každým úspěšným bezpečnostním projektem stojí lidé.

Tým FreeDivision tvoří specialisté se zkušenostmi z implementace, provozu i rozvoje bezpečnostních řešení v komerčních společnostech, veřejné správě i kritické infrastruktuře. Tyto zkušenosti přenášíme do každého projektu bez ohledu na jeho rozsah.

Naši konzultanti pomáhají zákazníkům navrhovat bezpečnostní architekturu, implementovat nové technologie, řešit bezpečnostní incidenty i plánovat dlouhodobý rozvoj prostředí.

Spolupráce je založena na partnerství, otevřené komunikaci a sdílení znalostí. Naším cílem není vytvářet závislost na externím dodavateli, ale dlouhodobě posilovat schopnost organizace efektivně řídit vlastní kybernetickou bezpečnost.

Procesy

Za každým úspěšným bezpečnostním projektem stojí lidé. Tým FreeDivision Moderní technologie přinášejí skutečnou hodnotu pouze tehdy, pokud jsou součástí dobře nastavených procesů.

FreeDivision.io Services podporují standardizované postupy při implementaci, správě, monitoringu i řešení bezpečnostních incidentů. Tímto způsobem jsou jednotlivé činnosti jednoduše opakovatelné, měřitelné a snadno se rozvíjí.

Procesní přístup současně usnadňuje plnění interních bezpečnostních politik, regulatorních požadavků i auditních standardů.

FreeDivision.io jako platforma pro dlouhodobý rozvoj bezpečnosti

Jednotlivé služby FreeDivision nejsou primárně navrženy jako samostatné nabídky. Jsou součástí platformy FreeDivision.io, která umožňuje organizacím budovat kybernetickou bezpečnost postupně, systematicky a s dlouhodobou perspektivou.

Každé řešení platformy plní specifickou roli, přičemž všechny části jsou navrženy tak, aby se vzájemně doplňovaly a sdílely společné principy architektury, procesů i řízení.

Ochrana endpointů

FreeDivision.io Essential představuje vstupní vrstvu moderní kybernetické bezpečnosti. Poskytuje ochranu pracovních stanic, notebooků, serverů a dalších koncových zařízení prostřednictvím pokročilých technologií EDR/XDR.

Řízení bezpečnostních operací

FreeDivision.io Advanced rozšiřuje pohled z jednotlivých zařízení na celou organizaci. Centralizuje bezpečnostní data, podporuje jejich korelaci, automatizuje bezpečnostní procesy a vytváří jednotné prostředí pro řízení bezpečnostních operací.

Odborné služby

FreeDivision.io Services propojují technologie s odbornými znalostmi a zkušenostmi našich specialistů. Pomáhají organizacím navrhovat, implementovat, provozovat a dlouhodobě rozvíjet jejich bezpečnostní prostředí.

Zákazník díky tomu získává nejen moderní technologie, ale také partnera, který podporuje jejich efektivní využití v každodenním provozu.

Připraveno na další rozvoj

Platforma FreeDivision.io je navržena jako otevřený ekosystém. Organizace může podle svých potřeb postupně rozšiřovat bezpečnostní architekturu o další specializované oblasti, například řízení zranitelností, správu privilegovaných přístupů, ochranu dat, řízení rizik nebo pokročilé služby Threat Intelligence.

Tento přístup chrání investice do již nasazených řešení a umožňuje rozvíjet bezpečnostní prostředí bez nutnosti zásadních změn architektury.

Závěr

Moderní kybernetická bezpečnost vyžaduje více než kvalitní technologie. Vyžaduje zkušené odborníky, ověřené procesy a partnera, který dokáže propojit technické znalosti s dlouhodobým rozvojem bezpečnostního prostředí.



For Safety Reasons. Be Best. Not First.

FreeDivision.io Services

poskytují organizacím právě tuto kombinaci.

Naši specialisté podporují zákazníky při analýze bezpečnostních rizik, implementaci nových technologií, správě stávajících řešení, řešení bezpečnostních incidentů i plánování dalšího rozvoje bezpečnostní architektury.

Rozsah spolupráce lze přizpůsobit velikosti organizace, jejím provozním požadavkům i interním kapacitám. Zákazník tak získává flexibilní model odborné podpory, který se přirozeně přizpůsobuje měnícím se potřebám i budoucím výzvám.

FreeDivision.io Services představují odborný pilíř celé platformy FreeDivision.io. Společně s řešeními FreeDivision.io Essential a FreeDivision.io Advanced vytvářejí ucelený model moderní kybernetické bezpečnosti, který propojuje technologie, expertní znalosti a efektivní bezpečnostní procesy.

Připraveni sjednotit bezpečnostní operace?

Každá organizace má jiné zkušenosti, jiné kapacity i jiné cíle. Proto přistupujeme ke každému projektu individuálně.

Společně s vaším týmem navrhne rozsah odborných služeb, který bude odpovídat vašim potřebám – od jednorázových konzultací přes implementační podporu až po dlouhodobou spolupráci při provozu a rozvoji kybernetické bezpečnosti.

FreeDivision.io Services vám poskytne zkušené odborníky, kteří se stanou přirozenou součástí vašeho bezpečnostního týmu a pomohou vám dlouhodobě budovat bezpečnější, stabilnější a efektivněji řízené IT prostředí.



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