
Fitio
STAY SAFE
STAY FITIO
www.fitio.cz

Představení společnosti

Společnost **Fitio** se specializuje na poskytování komplexních služeb v oblasti **kybernetické bezpečnosti** pro malé a střední firmy, veřejné instituce i komerční subjekty.

Naším cílem je **chránit** systémy, data a uživatele před neustále rostoucími kybernetickými hrozbami a zajistit jejich dlouhodobou bezpečnost.

Fitio se **zavazuje** poskytovat služby nejvyšší kvality s důrazem na dlouhodobou stabilitu a bezpečnost IT systémů svých klientů.

Představení společnosti

Member of Netform Investment

NETFORM INVESTMENT

Full servisová
reklamní agentura

BRANDBOOST

Komplexní služby
kybernetické bezpečnosti

Fitio

Nástroj pro efektivní
plánování rádiové reklamy

adBooster

Nástroj pro rozesílku
e-mailových kampaní

Email Machine.

Naše služby zahrnují:

- **Školení:** Praktické kurzy zaměřené na ochranu firem před kybernetickými hrozbami, jako je phishing, krádež identity nebo zneužití dat.
- **Penetrační testování:** Simulace hackerských útoků za účelem identifikace zranitelností v IT infrastruktuře, včetně testů externích, interních, zátěžových, webových, API či mobilních aplikací.
- **Vstupní analýza:** Rychlé a efektivní posouzení stavu kybernetické bezpečnosti organizace, zahrnující analýzu současných bezpečnostních technologií a procesů a provedení externích penetračních testů nebo skenů sítě.
- **Sociální inženýrství:** Testování odolnosti zaměstnanců vůči phishingovým útokům a dalším technikám sociálního inženýrství.
- **Dodávka technologií:** Implementace a integrace bezpečnostních technologií na míru potřebám klienta.
- **Dotované kurzy:** Nabídka školení v oblasti kybernetické bezpečnosti s možností čerpání dotací.

S kým se ve Fitio můžete potkat?

Na práci se podílí primárně interní tým zkušených specialistů pod vedením **Jakuba Svárovského**– **CEO firmy** a **Maria Rittera**- **CTO firmy.**

Jakub Svárovský je ředitelem společnosti, který řídí projekty u klientů, přímo zjišťuje potřeby a otevírá témata v oblasti kybernetické bezpečnosti. Své zkušenosti s postupy u ZoKB, NIS2, DORA předává klientům a navrhuje udržitelné opatření a vizi do bezpečnější budoucnosti.

Mario Ritter má bohaté zkušenosti z oboru etického hackera a technika IT. Svým vhledem do fungování red teamingu a blue teamingu dokáže nastavit prvotní zrcadlo společnosti.
Mario je držitel prestižního certifikátu OSCP+.

Helena Urbančíkova má přes 25 let zkušeností ze světa kybernetické bezpečnosti a pod rukama ji protekly miliony informací a navrhovaných opatření pro udržitelné a kontinuální zlepšování.
Pomůže vaší společnosti splnit zákonem dané povinnosti a bezpečnostní normy.

Nedílnou součástí týmu Fitio platform, s.r.o. jsou i technici na bezpečnostní technologie, architekti infrastruktury a projektoví manažeři.

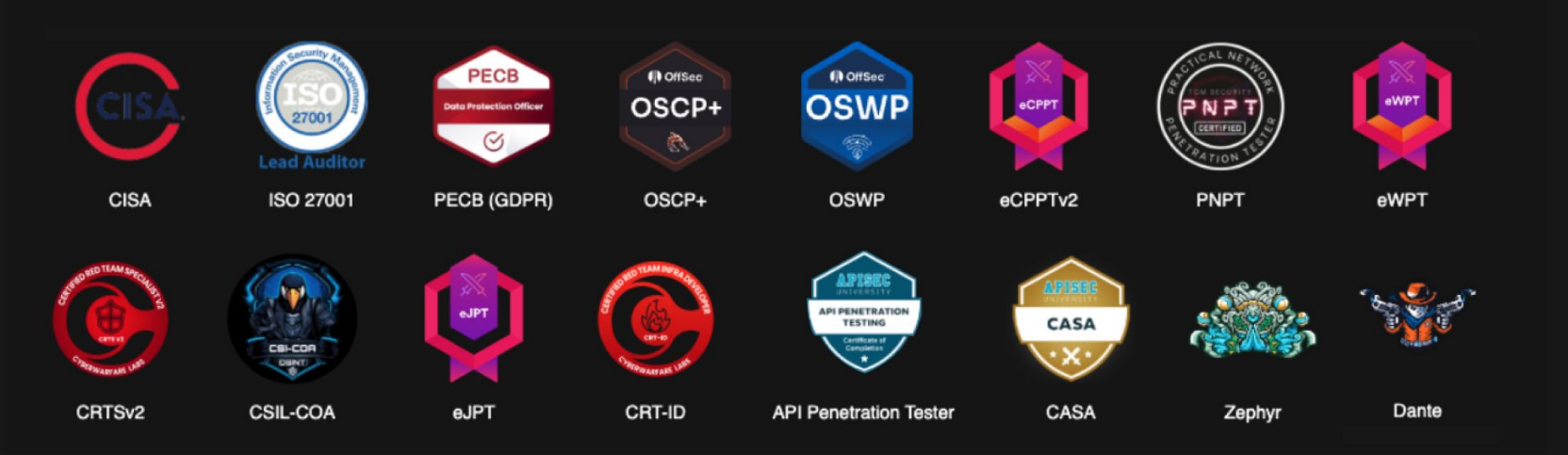
Klienti, kteří nám důvěřují

Fitio

Naše certifikace

Fitio

Disponujeme řadou certifikací v oblasti kybernetické bezpečnosti, včetně CISA, Lead auditor ISO 27001, PECB (GDPR), OSCP+, OSWP, eCPPTv2, PNPT, eWPT, CRTSv2, CSIL-COA, eJPT, CRT-ID, API Penetration Tester, CASA, Zephyr a Dante.



Kyberbezpečnost ČR v číslech

59 000 000 Kč

Nejvyšší škoda v rámci kybernetických útoků

Výkupné je zpravidla
10 % z obratu
a průměrně **6 000 000 Kč**

Přerušení obchodní činnosti na **22 dní.**
Dříve 3 dny

1 571
kyberútoků týdně v ČR

Česko je **pátým**
nejčastějším terčem kybernetických útoků v Evropě.

Nabídka služeb

Naše služby zahrnují:

Penetrační testy

Testování systémů na zranitelnosti.

FIT IO Scan

Rychlý audit kybernetické odolnosti.

SOC

Správa logů a incidentů.

Interim manažer

Dočasné vedení v oblasti bezpečnosti.

Úvodní analýza

Základní hodnocení bezpečnostních potřeb.

Konzultace

Poradenství v oblasti kybernetické bezpečnosti.

Identity management

Řízení přístupu a identit.

Školení

Vzdělávání zaměstnanců o kyber. bezpečnosti.

Phishing

Ověření odolnosti vůči podvodným e-mailům.

Vishing

Ochrana před podvodnými tel. hovory.

Bezpečnostní technologie

Správa bezpečnostních systémů.

Penetrační testy

Penetrační testy simulují r**eálné kybernetické útoky** s cílem identifikovat a odstranit zranitelnosti ve vaší IT infrastruktuře. Naše služby zahrnují externí, interní, zátěžové testy, stejně jako testování webových aplikací, API a mobilních aplikací, čímž pokrýváme všechny klíčové oblasti kybernetické bezpečnosti.

Používáme osvědčené metodiky jako OWASP, OSSTMM a PTES, abychom zajistili komplexní hodnocení bezpečnosti vašich systémů.

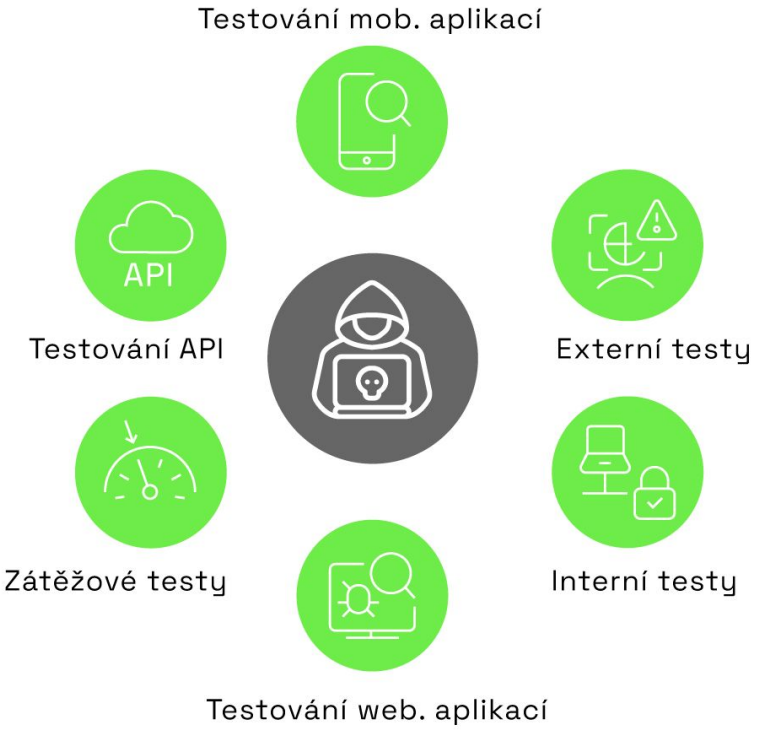
Co získáte díky našim penetračním testům?

- **Přehled o aktuálním stavu bezpečnosti:** Odhalíme slabá místa ve vaší síti a systémech, která by mohla být zneužita kybernetickými útočníky.
- **Minimalizace rizika incidentů:** Identifikací zranitelností umožníme rychlou reakci a zavedení opatření ke zvýšení bezpečnosti.
- **Soulad s normami:** Pomůžeme vám splnit bezpečnostní standardy, jako je ISO 27000, NIS2, DORA či TISAX.

Více informací

Naše služby

Úplný přehled penetračního testování



1. Phishing

Phishingové útoky patří mezi nejzávažnější kybernetické hrozby, které mohou ohrozit citlivé informace a reputaci vaší společnosti.

Provádíme simulované phishingové kampaně, které realisticky prověří připravenost vašich zaměstnanců na tyto útoky a pomohou identifikovat slabá místa v jejich povědomí o kybernetické bezpečnosti.

Poskytujeme podrobnou analýzu, identifikujeme slabiny a navrhujeme cílená školení, která posílí odolnost vašeho týmu proti těmto hrozbám. Díky tomu ochráníte nejen citlivé informace, ale i důvěru svých zákazníků a partnerů.

2. Vishing

Vishing: Kybernetická hrozba přes telefon
Vedle phishingu nabývá na významu také **vishing**, tedy podvodné telefonní hovory, jejichž cílem je vylákat citlivé informace nebo přístupové údaje.

Útočníci se často vydávají za zaměstnance bank, úřadů nebo jiných důvěryhodných institucí a využívají psychologický nátlak k manipulaci obětí.

Naše simulované vishingové kampaně realisticky ověřují schopnost vašich zaměstnanců rozpoznat podvodné telefonáty a správně na ně reagovat.

Poskytujeme podrobnou analýzu, identifikujeme slabiny a navrhujeme cílená školení, která posílí odolnost vašeho týmu proti těmto hrozbám. Díky tomu ochráníte nejen citlivé informace, ale i důvěru svých zákazníků a partnerů.

Konzultace manažera KB

1. Úvodní analýza

Poskytne rychlý a nezávislý přehled o stavu vašich bezpečnostních opatření. Odhalíme rizika a navrhneme konkrétní kroky, jak zvýšit ochranu vašich cenných dat. Naše služby vám umožní bezpečně rozvíjet vaši organizaci a zajistit, aby byla vždy o krok napřed před kybernetickými hrozbami.

.

2. Konzultace

Odborné konzultace k ZoKB, ISMS, ISO 27001, NIS2 a DORA, díky kterým zajistíte soulad s předpisy a posílíte svou kybernetickou bezpečnost. Naše řešení jsou vždy přizpůsobena vašim specifickým potřebám. S našimi experty získáte praktické doporučení pro dlouhodobou odolnost a compliance.

3. Interim manažer KB

Je klíčovým partnerem pro firmy, které potřebují řešit rostoucí kybernetické hrozby. Nabízíme odborné znalosti, know-how, flexibilní zapojení a efektivní řešení projektů bez nutnosti budovat drahé interní kapacity.

Školení

Komplexní školení v oblasti kybernetické bezpečnosti zaměřené na **ochranu vaší firmy** před rostoucími hrozbami. Naši zkušení lektoři vedou praktické kurzy založené na reálných příkladech, které účastníky aktivně zapojují a učí je jak rozpoznat a předcházet rizikům, jako je phishing, krádež identity nebo zneužití dat. Školení je v souladu s požadovaným obsahem ZoKB.

Díky našemu školení získáte:

- **Snížení rizika lidských chyb:** Až 95 % kybernetických incidentů je způsobeno lidskou chybou. Naše školení pomáhají tato rizika minimalizovat.
- **Účinná prevence kybernetických incidentů:** Praktické osvojení dovedností pro rozpoznání a efektivní reakci na kybernetické hrozby.
- **Ochrana nejen pro vaši firmu, ale i pro osobní život vašich zaměstnanců:** Naučíme je bránit se technikám sociálního inženýrství, vytvářet a spravovat silná hesla, chránit soukromí a data online a rozpoznávat rizika na sociálních sítích a mobilních zařízeních.

V dnešní digitální době je ochrana firemních dat a zabezpečení IT infrastruktury důležitější než kdy dříve. S rostoucími hrozbami, jako jsou phishing, ransomware nebo útoky na zranitelnosti IT systémů, se každá organizace stává potenciálním cílem. Předejděte problémům a chraňte své podnikání před rostoucími hrozbami v digitálním světě s Fitio. Udržíme vaše IT ve formě a zajistíme vám bezpečnou budoucnost!

Více informací

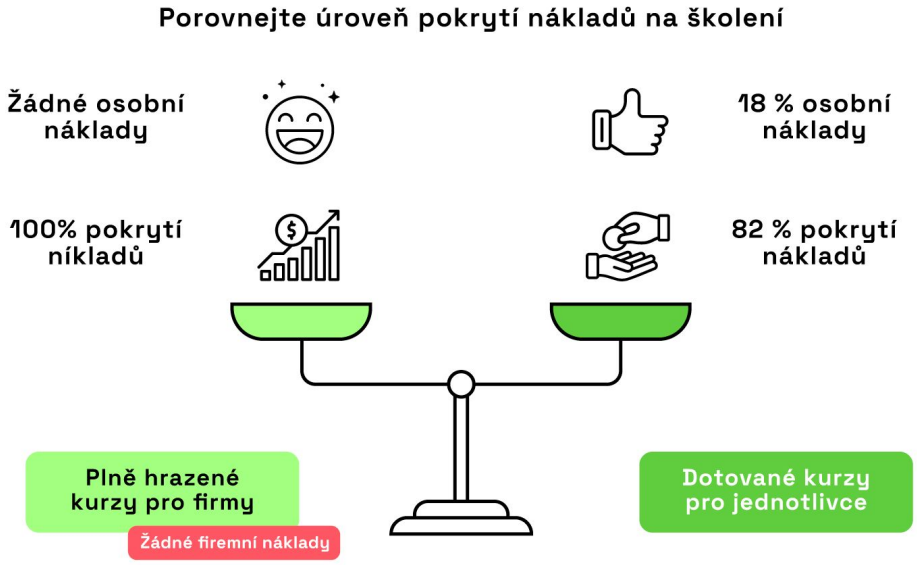
Dotované kurzy

Využijte jedinečnou možnost rozvoje digitálních dovedností s dotovanými kurzy

Dotované kurzy zaměřené na moderní digitální dovednosti, které jsou plně či částečně hrazeny z programů Úřadu práce. Tyto kurzy jsou navrženy tak, aby účastníkům poskytly praktické a inovativní vzdělávání, které zvýší jejich profesní kompetence a usnadní adaptaci na rychle se měnící digitální prostředí.

Kurzy se zaměřují na moderní témata, jako je **umělá inteligence, kybernetická bezpečnost, e-commerce** a efektivní využívání online nástrojů.

Naše vzdělávací programy spojují praktický přístup s inovativními technologiemi, aby pomohli rozšířit vaše profesní kompetence, zvýšily vaši hodnotu na trhu práce a usnadnily adaptaci na rychle se vyvíjející digitální prostředí



Využijte jedinečnou možnost rozvoje digitálních dovedností s dotovanými kurzy

Možnosti dotací:

1. Plně hrazené kurzy pro firmy (100% dotace)

Plně hrazené dotace, **veškeré náklady na kurz uhrazeny Úřadem práce ČR**, takže účastníci neplatí žádné poplatky.

- **Výhody:**
  - 100% pokrytí nákladů na školení.
  - Náhrada za čas strávený na kurzu.
  - Jednoduché zajištění dotace s naší podporou.

Příklad: Kurz „Digitální excelence: Mastering AI a kybernetická bezpečnost“ může být plně hrazen a zcela bez finanční zátěže pro firmu.

2. Kurzy s dotací 82% pro fyzické osoby

Tento typ dotace umožňuje pokrýt **až 82 % nákladů na kurz**, přičemž účastník doplácí pouze **18 % ceny**.

- **Výhody:**
  - **Výrazná úspora** – většinu nákladů na kurz za vás zaplatí Úřad práce.
  - **Minimální doplatek** od účastníka, např. v řádu několika tisíc korun.

Příklad: Kurz „Inovativní digitální výkon: Kybernetická bezpečnost, E-commerce & AI“ – doplatek pouze **2 339 Kč na účastníka**. Plná cena za kurz je 12.999,- Kč

Dotace pro firmy - Digitální transformace ovládněte AI s pocitem bezpečí v online světě.

V dnešní digitální době je zásadní držet krok s rychlým vývojem technologií. Právě proto jsme pro firmy připravili dvoudenní školení **FITIO Digitální transformace**, během kterého získáte klíčové znalosti a dovednosti v oblasti **umělé inteligence (AI) a kybernetické bezpečnosti**.

Tento kurz je **plně dotován Úřadem práce**, což znamená, že vaše firma **za každého účastníka obdrží náhradu ve výši 2 176 Kč za každý školící den**. Nejenže získáte cenné know-how, ale zároveň ušetříte na vzdělávání vašeho týmu.

Benefity kurzu:

Znalosti o AI: Naučíte se, jak využít AI ke zjednodušení rutinních úkolů, zvýšení produktivity a zefektivnění pracovních procesů.

Praktické zkušenosti: Osvojíte si práci s moderními nástroji umělé inteligence pro tvorbu grafického obsahu, videí, automatizovaných překladů a personalizovaných vzdělávacích materiálů.

Kybernetická ochrana: Získáte praktické rady, jak zabezpečit nejen firemní data, ale i svůj osobní digitální prostor a online bezpečnost svých blízkých.

Aktuální přehled: Seznámíte se s nejnovějšími kybernetickými hrozbami a naučíte se, jak se jim účinně bránit pomocí vhodných nástrojů a postupů.

Dotace pro firmy – Digitální transformace ovládněte AI s pocitem bezpečí v online světě.

Cesta k digitální excelenci

- Školení v oblasti digitální transformace
- Umělá inteligence
- Kybernetická bezpečnost
- Dotace Úřadu práce

Posílené dovednosti a úspory

Fitio

SOC – Log management

Naše služby v oblasti správy logů a SIEM systémů poskytují komplexní řešení pro efektivní monitorování, analýzu a správu bezpečnostních událostí. Pomáháme organizacím optimalizovat stávající systémy, zlepšit reakci na hrozby a přeměnit rozsáhlá data na užitečné informace pro strategické rozhodování. Díky centralizaci a automatizaci šetříme čas, náklady a zlepšujeme celkovou bezpečnostní situaci.

Díky SOC – log management od Fitio získáte:

- Centralizace a automatizace logů
- Pokročilá analýza bezpečnostních dat
- Optimalizace využití SIEM systémů
- Efektivní reakce na hrozby

FIT IO Scan – Rychlý audit kybernetické odolnosti vaší firmy

FIT IO Scan je **elementární zkouška zabezpečení** vaší IT infrastruktury, která odhalí rizika, na která může být vaše společnost vystavena.

🔍 Co pro vás otestujeme?

- **Zašifrování dat:** Jak snadno mohou útočníci zašifrovat vaše citlivé informace?
- **Ovládnutí PC útočníkem:** Prověříme, zda je možné převzít kontrolu nad vašimi zařízeními.
- **Zranitelnosti v organizaci:** Odhalíme slabá místa ve vašich systémech a procesech.
- **Bezpečnostní protokol:** Zkontrolujeme, jak efektivní jsou vaše stávající bezpečnostní opatření.

👁️ Odhalte slabiny dřív, než je zneužijí útočníci!

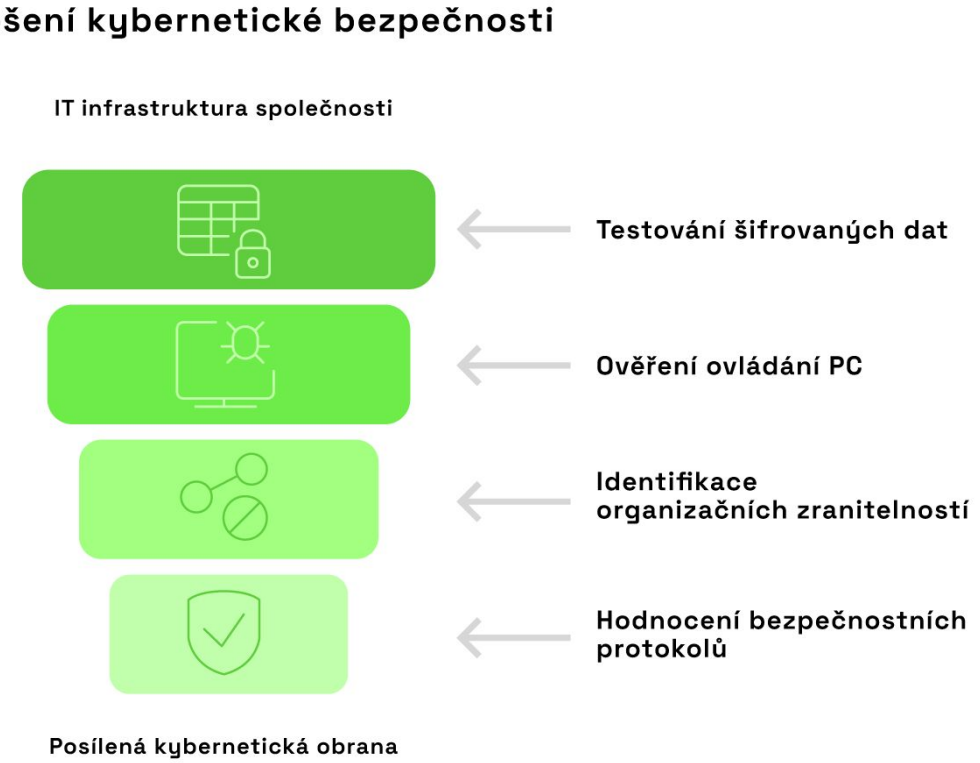
Nečekejte na první incident – 👁️ **Odhalte slabiny dřív, než je zneužijí útočníci!**

Nečekejte na první incident – s FIT IO Scanem získáte přehled o tom, jak zlepšit svou kybernetickou obranu a ochránit tak vaše data i reputaci.

Naše služby

Fitio SCAN

Rychlý audit kybernetické odolnosti vaší firmy



Technologie

Nabízíme integraci předních bezpečnostních řešení pro komplexní ochranu vaší IT infrastruktury.

- **Fortinet** - poskytuje komplexní řešení kybernetické bezpečnosti zahrnující ochranu sítí, endpointů, cloudových prostředí a aplikací prostřednictvím integrované platformy s vysokým výkonem, která využívá pokročilou automatizaci a strojové učení.

- **Burb Suite** - komplexní nástroj pro analýzu a testování bezpečnosti, který nabízí pokročilé možnosti pro identifikaci zranitelností, simulaci útoků a zajištění ochrany digitálních systémů.

- **Node Zero** - pokročilá platforma pro testování a simulaci kybernetických útoků, která umožňuje organizacím identifikovat slabá místa ve své bezpečnostní infrastruktuře a optimalizovat reakce na reálné hrozby.

- **Bitdefender** - nabízí silnou ochranu proti kybernetickým hrozbám, chrání systémy, data a soukromí uživatelů díky sofistikovaným nástrojům pro detekci hrozeb, prevenci útoků a ochranu před malwarem.

S našimi technologiemi zajistíte vysokou úroveň bezpečnosti pro svou organizaci a ochráníte své systémy před neustále se vyvíjejícími kybernetickými hrozbami.

Fitio

Kontaktujte nás:

+420 774 309 858

obchod@fitio.cz

www.fitio.cz

Potkat se s námi může v našich kancelářích:

Václavská 2073/20, Praha 2