DeTCT®
BY CYFIRMA

DeTCT®

Vaše firma musí nepřetržitě podávat špičkový výkon. Nenechte se vykolejit digitálními riziky. Převezměte kontrolu nad svými kybernetickými riziky a využijte všech výhod vašeho postavení v digitálním ekosystému. DeTCT je vaše základní platforma pro odhalování digitálních rizik a ochranu před nimi, která neúnavně monitoruje skryté útočné plochy, zranitelné systémy, uniklá data, vydávání se za vedoucí pracovníky nebo porušování práv k ochranným známkám a ověřuje vaše procesy oprav a zranitelných míst, aby vaše kybernetická pozice zůstala silná tváří v tvář novým hrozbám.

DeTCT poskytuje úplný přehled o vaší digitální stopě jako nikdo jiný.

DeTCT je jediná plně automatizovaná, proaktivní monitorovací služba, která funguje nonstop a pomáhá vám udržet si přehled o rostoucích kybernetických hrozbách.

- ❖ Monitorování plochy útoku.
- ❖ Krádež identity a narušování práv.
- ❖ Monitorování v souvislosti s narušením bezpečnosti dat.
- ❖ Monitorování expozice ve veřejném digitálním prostoru, a zvláště na sociálních sítích.
- ❖ Sledování kybernetických rizik třetích stran.

DeTCT vám poskytuje užitečné informace, pomocí kterých můžete stanovit priority nápravných opatření.

Tato služba vznikla, aby chránila vaši značku a digitální aktiva a zároveň umožňovala inovace.

- ❖ Ke každému indikátoru hrozby je přiřazeno skóre rizika, abyste mohli posoudit jeho dopad na vaši firmu.
- ❖ Doporučená nápravná opatření pomohou zabránit úniku vašich dat a narušení bezpečnosti.
- ❖ Panely se skóre rizik a napadnutelnosti umožňují sledovat pokrok v průběhu času.

Cílem DeTCT je pomoci vedoucím pracovníkům zmírnit rostoucí digitální rizika, aby se mohli soustředit na budování prosperující firmy.

CEO/CFO
Jak mohu kvantifikovat rizika a nedostatky před hlavními zainteresovanými stranami / představenstvem, abych získal podporu pro iniciativy na poli kybernetické bezpečnosti?
Čelí moje firma nějakým hrozbám? Na co se musím zaměřit a co mám upřednostnit?

Obchodní a marketingový tým
Hrozí mé značce nějaké riziko útoku nebo napadení? Hrozí jakékoli narušení nebo krádež identity, které by mohly ovlivnit důvěru zainteresovaných stran a narušit loajalitu mých zákazníků?

Tým IT
Mám úplný přehled o vedení a formě chystaného útoku? Jaká jsou moje nejkritičtější zranitelná místa? Jsou mé procesy týkající se správy oprav a zranitelných míst a dodržování zásad účinné? Co musím udělat, abych zlepšil své bezpečnostní kontroly?

Monitorování plochy útoku

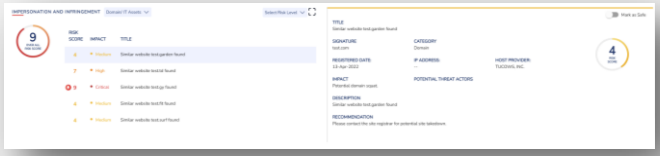
DeTCT monitoruje plochu útoku, abyste nikdy nebyli zaskočeni.

- ❖ Zranitelnost domény/IP
- ❖ Slabé stránky certifikátu
- ❖ Konfigurace: DNS/SMTP/HTTP
- ❖ Reputace IP/domény
- ❖ Otevřené porty
- ❖ Slabé stránky cloudu

Krádež identity a porušování práv

DeTCT skenuje deep/dark/povrchový web a sociální sítě a hledá známky krádeže identity a porušení práv.

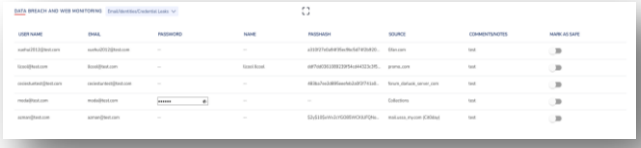
- ❖ Aktiva domény/IP
- ❖ Vedoucí pracovníci / lidé
- ❖ Produkt / řešení
- ❖ Správci sociálních sítí



Monitorování narušení bezpečnosti dat

DeTCT vás upozorňuje na data, která byla ukradena a jsou nabízena k prodeji na nelegálních tržištích. Sem patří také data, která byla exfiltrována ransomwarovými skupinami.

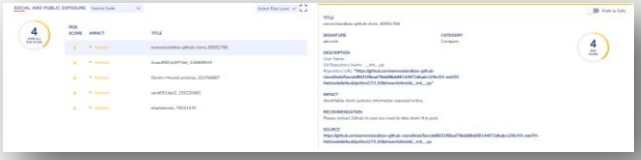
- ❖ E-maily / identity / přihlašovací údaje
- ❖ Úniky
- ❖ Dark web
- ❖ Phishing
- ❖ Ransomwaresítí



Únik dat na sociálních sítích a na veřejnosti

Díky DeTCT budete vždy vědět, zda byla veřejně vystavena vaše IP adresa nebo důvěrná data, včetně napodobujících nebo škodlivých aplikací. Budete také dostávat upozornění na společenské postoje, které by mohly představovat hrozbu pro vás nebo vaši organizaci.

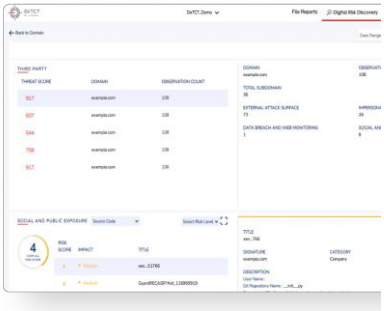
- ❖ Zdrojový kód
- ❖ Důvěrné soubory
- ❖ Výpisy PII/CII
- ❖ Škodlivé mobilní aplikace
- ❖ Společenská hrozba



Sledování rizik třetí strany

DeTCT zabezpečuje váš digitální ekosystém a poskytuje vám přehled o kybernetických rizicích třetích stran.

- ❖ Objevte slabá místa digitálních aktiv vašich dodavatelů.
- ❖ Získávejte upozorněni na úniky a odhalení jejich dat, které by vás mohly ovlivnit.



HLAVNÍ FUNKCE	POPIS	VÝHODY
ODHALENÍ PLOCHY ÚTOKU	▪ Proaktivně identifikujte odhalená externí aktiva, stínové IT a zapomenuté systémy, které mohou kyberzločinci využít. ▪ Vytvořte efektivní program správy útočných ploch s možností průběžného monitorování.	▪ Získejte zpět kontrolu nad tím, že budete mít přehled o svých externích aktivech, a začněte se zajímat o snížení útočné plochy, abyste ochránili svou firmu. ▪ Povědomí o útočných plochách vám pomůže identifikovat potenciální cestu útoku, a vy tak můžete podniknout kroky ke snížení a zmírnění rizik.
ODHALENÁ SLABÁ MÍSTA	▪ Posilujte programy správy zranitelných míst průběžným monitorováním s cílem identifikovat slabá místa ve vašich externích aktivech. ▪ Pochopte, jakým způsobem se kyberzločinci snaží zneužít vaše zranitelná místa. ▪ Vypracujte program správy certifikátů pomocí identifikace slabých a zranitelných certifikátů hostovaných na externích prostředcích.	▪ Zlepšete svůj program správy zranitelných míst tím, že budete znát rizika a hrozby, které je třeba urychleně řešit. ▪ Stanovte priority programu pro správu záplat a náprav. ▪ Rychle odstraňte bezpečnostní mezery, než dojde k dalším škodám.
MONITOROVÁNÍ NARUŠENÍ BEZPEČNOSTI DAT	▪ Zjištění úniku duševního vlastnictví, osobních údajů nebo finančních informací v reálném čase. ▪ U každého narušení a vyzrazení jsou uvedeny základní informace, popis a dopad.	▪ Zjistěte, zda a kdy došlo k úniku vašich dat. ▪ Zajistěte, aby zaměstnanci, obchodní partneři a externí dodavatelé neúmyslně nesdíleli citlivé informace, které by mohly společnost vystavit kybernetickým útokům a rizikům. ▪ Informovanost o e-mailech a přihlašovacích údajích, které byly kompromitovány, vám umožní přijmout opatření na ochranu vaší firmy před phishingem a dalšími útoky sociálního inženýrství. ▪ Zajistěte, aby vaše IP adresy a obchodní tajemství nebyly veřejně vystaveny. ▪ Ujistěte se, že dodržujete předpisy v souladu s platnou regulativou. ▪ Vyhněte se nutnosti zvládat negativní publicitu v případě úniku dat nebo kybernetického útoku.
VYSTAVENÍ NA DARK WEBU	▪ Poskytuje přehled o hackerských konverzacích a podezřelých podvodných aktivitách z dark webu. ▪ Odhalte e-mailové ID a přihlašovací údaje, údaje PII/CII a další citlivé informace, které se prodávají na nelegálních fórech a tržištích.	▪ Buďte první, kdo se dozví, že vaše data byla veřejně vystavena. ▪ Proveďte rychlá opatření, jako je uzavření určitých síťových portů, resetování hesel a přihlašovacích údajů, abyste omezili následky.
ÚNIK DAT NA SOCIÁLNÍCH SÍTÍCH A NA VEŘEJNOSTI	▪ Průběžné sledování falešných a napodobujících domén a subdomén. ▪ DeTCT shromažďuje nově registrované domény i škodlivé domény. ▪ Odhalte falešné profily společnosti a jejích vedoucích pracovníků na sociálních sítích (LinkedIn, Facebook a Twitter).	▪ Zamezte sociálnímu inženýrství a předejděte phishingovým kampaním, které se vydávají za vedoucí pracovníky nebo profil společnosti. ▪ Citlivá data, která unikla, ať už úmyslně nebo náhodně, mohou být aktéry hrozby zneužita k zahájení útoku. Schopnost detekovat tyto úniky vám umožní přijmout nápravná opatření a zabránit velkému útoku.
KRÁDEŽ IDENTITY A PORUŠOVÁNÍ PRÁV	▪ Identifikujte případy porušení práv a krádeže identity související se značkou, produktem, řešením a zaměstnanci. ▪ Jde o indikátory hrozeb, které poukazují na možné phishingové kampaně.	▪ Snižte riziko kopírování vaší značky, produktů a řešení. ▪ Chraňte integritu své značky. Předcházejte narušení své podnikatelské aktivity v důsledku phishingových útoků a útoků sociálního inženýrství, které by mohly narušit důvěru zainteresovaných stran a ovlivnit životaschopnost firmy. ▪ Chraňte své vedoucí pracovníky před krádeží jejich identity online a na sociálních sítích.
OBJEVOVÁNÍ A MONITOROVÁNÍ RIZIKA PRO TŘETÍ STRANU	▪ Pomůžeme vám monitorovat domény třetích stran, s nimiž jste ve styku, bez nutnosti složitých a rušivých implementací. ▪ Zmapujte jejich digitální rizikový profil a získejte povědomí o tom, zda neutrpěli nějaké úniky dat, odhalení zranitelnosti atd.	▪ Zabezpečte svůj digitální ekosystém a získejte přehled o kybernetických rizicích třetích stran. ▪ Objevte slabá místa v digitálních aktivech svého dodavatele. ▪ Poznejte kybernetická rizika třetí strany a pochopte, jak by vás mohla ovlivnit.
SKÓRE RIZIK A NAPADNUTELNOSTI	▪ Získejte rychlý přehled o míře závažnosti svých rizik a napadnutelnosti a zjistěte, jak se vyvíjejí v čase. ▪ Hodnocení rizik se provádí pomocí rámce FAIR (Factor Analysis of Information Risk) a poskytuje se pro každý indikátor hrozby nebo expozice.	▪ Získejte přehled o své rizikové pozici, abyste mohli přijmout opatření ke zmírnění hrozeb, které by mohly způsobit narušení provozu. ▪ Pochopte svůj celkový stav digitálních rizik z pohledu firmy.
DOPORUČENÁ NÁPRAVNÁ OPATŘENÍ	▪ Pro každé související riziko a expozici jsou k dispozici doporučená nápravná opatření, takže týmy mohou rychle začít jednat.	▪ Stanovte priority rychle a rozhodně s jasnými kroky a jejich posloupností. ▪ Aktivujte správné zdroje k odstranění nedostatků v zabezpečení.

O PLATFORMĚ CYFIRMA

CYFIRMA je externí platforma pro správu externích hrozeb. Propojujeme informace o kybernetickém zabezpečení s odhalováním útočných ploch a ochranou před digitálními riziky, abychom poskytli prediktivní, personalizované, kontextové, outside-in a vícevrstvé poznatky. Využíváme naši cloudovou analytickou platformu založenou na AI a ML, abychom společnostem pomohli proaktivně identifikovat potenciální hrozby ve fázi plánování kybernetických útoků. Náš jedinečný přístup, který spočívá v poskytování pohledu hackera a hlubokého přehledu o vnějším kybernetickém prostředí, pomohl klientům připravit se na budoucí útoky.

CYFIRMA spolupracuje s mnoha společnostmi ze seznamu Fortune 500.
Společnost má pobočky v zemích APAC, USA a EU.

www.freedivision.com | +420 220 972 426

FREEDIVISION
for safety reasons