DECYFIR®
BY CYFIRMA

# DECYFIR®

Organizace se při pohybu v neprobádaných vodách postpandemického a nestabilního geopolitického prostředí ocitají na křižovatce. Strategie kybernetické bezpečnosti, které byly navrženy dříve pro řízení známých hrozeb pomocí běžných nástrojů pro kontrolu zabezpečení, je třeba přehodnotit.

## Bezpečnostní strategie vyžadují agilní přístup

- Nabídky zabezpečení orientované dovnitř společnosti, které nechápou vnější hrozby a jejich korelace.
- Pracují reaktivním způsobem a bezpečnostní mezery identifikují až po útoku.
- Bezpečnostní kontroly jsou zaměřené na události; chybí ucelený pohled na všechny hrozby.
- Vytvářejí tlak na provedení neplánovaných, okamžitých a nákladných nápravných opatření.
- Masivní výdaje na technologie v rámci jednotlivých nabídek a neschopnost odvrátit únik dat nebo útok.
- Iniciativy v oblasti kybernetické bezpečnosti mají omezenou podporu na úrovni vedení a představenstva.

## Výzvy v oblasti kybernetické bezpečnosti

- Nevíte, jestli už na vás protivníci neútočí.
- Rychlá digitalizace a měnící se technologické prostředí vedou k tomu, že bezpečnostní nástroje nejsou optimalizovány nebo konfigurovány tak, aby zvládaly nové hrozby.
- Složité a časově náročné konfigurace systému kybernetické bezpečnosti.
- Omezené znalosti o zapomenutém a stínovém IT.
- Přemíra dat o kybernetické bezpečnosti a nedostatek praktických poznatků, na kterých opravdu záleží.
- Vzestupný trend v oblasti kybernetických zločinů (jako je malware/ransomware) bez kontextových podrobností o povaze útoků.
- Počáteční porozumění rizikům nové doby v oblasti digitálních technologií a značek (včetně třetích stran a dodavatelského řetězce).

## Řešení – platforma pro správu prostředí externích hrozeb

Řešení spočívá ve schopnosti získat přehled o prostředí vnějších hrozeb a neustále se objevujících nových hrozbách a využít prediktivní inteligenci k proaktivnímu přijímání opatření pro zmírnění rizik a odvrácení hrozícího útoku. DeCYFIR poskytuje 6 pohledů na hrozby v jediném okně, a pomáhá tak odhalit hrozící útoky.

PREDIKTIVNÍ | PERSONALIZOVANÉ | OUTSIDE-IN | KONTEXTOVÉ | VÍCEVRSTVÉ

### Odhalení plochy útoku

Objevte externí aktiva, procesy a slabá místa, která mohou hackeři zneužít

### Odhalování digitálních rizik

Dark web, deep web, povrchový web a monitorování sociálních sítí s ohledem na únik dat a identit, důvěrných souborů, zdrojového kódu, odhalení citlivých informací, vydávání se za doménu a další.

### Povědomí o situaci

Porozumění kybernetickým trendům a hrozbám specifickým pro odvětví, technologie a geografickou oblast klienta.

### Informace o zranitelnosti

Zvyšování zranitelnosti díky hrozbám pocházejícím z měnícího se vnějšího kybernetického prostředí. Změna priority identifikovaných zranitelných míst na základě zájmu, přiřazení a asociace kyberzločinců.

### Informace o značce

Monitorování značky, produktu a služby a případů porušení výkonných pravomocí, propojení s probíhajícími kampaněmi proti kyberkriminalitě.

### Kybernetické informace

Prediktivní, personalizované, kontextové, outside-in a vícevrstvá kybernetická inteligence, která u útoků řeší otázky kdo, proč, co, kdy a jak. Získejte akceschopná a prioritní nápravná řešení.

DECYFIR®
BY CYFIRMA

# DECYFIR®

| HLAVNÍ FUNKCE | POPIS | VÝHODY |
|---|---|---|
| **PREDIKTIVNÍ** | Předvídejte blížící se kybernetický útok zaměřený na vaši organizaci a dceřiné společnosti dříve, než kyberzločinci poškodí vaše podnikání. | Včasná varování a výstrahy, které vám pomohou kvantifikovat rizika a připravit se na blížící se kybernetické útoky. |
| **PERSONALIZOVANÉ** | Datové body a přehledy jsou uzpůsobeny tak, aby odpovídaly technologii, kterou používáte, odvětví, ve kterém působíte, a oblasti, kde se nacházíte. | Odstraňte šum a snižte počet falešných poplachů, abyste zajistili, že varování s velkým dopadem nezůstanou bez odezvy. |
| **KONTEXTOVÉ** | Kompletní kontextové podrobnosti o externí hrozbě včetně podrobností o protivníkovi, TTP a souvisejících IoC (škodlivý/neškodný, podrobnosti o poloze, k čemu se používá pro C&C, cesta útoku, škodlivý web hostingu, přidružená kampaň proti kyberkriminalitě atd.). | Důkladně porozumíte kybernetickým hrozbám, aby bylo možné vytvářet účinné obranné strategie. Pomozte podnikům porozumět vyvíjejícím se hrozbám a jejich dopadu na ně. |
| **KYBERNETICKÉ INFORMACE** | Podrobné přehledy o vnějším prostředí hrozeb – kdo jsou kyberzločinci, kteří se o vás zajímají, jaká je jejich motivace, co po vás chtějí, kdy mohou útočit a jak zaútočí, jaké jsou nástroje a techniky, které mohou použít. | Komplexní pohled z venku dovnitř, který zajistí, že kybernetičtí obránci nebudou slepí a budou moci přijmout vhodná proaktivní opatření ke sladění svých kybernetických schopností. |
| **ODHALENÍ PLOCHY ÚTOKU** | Identifikujte externí aktiva a potenciální místa zneužití, jako jsou stínové IT, zapomenuté systémy, nesprávná konfigurace, nezajištěná místa a zranitelné certifikáty. | Získejte povědomí o aktivech směřujících do vnějšího prostředí, které mohou kyberzločinci zneužít, a na základě tohoto přehledu identifikujte způsoby, jak zmenšit plochu útoku, abyste snížili a zmírnili riziko. |
| **INFORMACE O ZRANITELNOSTI** | Identifikujte slabé stránky svého softwaru a externích aktiv, pochopte, jak se kyberzločinci dívají na zneužití zjištěných zranitelných míst. | Optimalizujte zdroje a zaměřte se na nejdůležitější a naléhavé nedostatky. Upřednostněte programy pro správu záplat a zranitelných míst a nápravná opatření. |
| **INFORMACE O ZNAČCE** | Identifikujte případy narušení, předstírání identity související se značkou, produktem, řešením a lidmi. | Snižte riziko pro svoji značku, produkty a řešení. |
| **POVĚDOMÍ O SITUACI** | Poznejte trendy a nové hrozby ve svém oboru, používaný soubor technologií a zeměpisnou oblast, ve které působíte. | Poskytněte přehledy, které mohou vést k důležitým obchodním rozhodnutím, včetně kyberinvestic. |

DECYFIR®
BY CYFIRMA

# DECYFIR®

| HLAVNÍ FUNKCE | POPIS | VÝHODY |
|---|---|---|
| **HLAVNÍ FUNKCE** | Proaktivně identifikujte úniky dat, narušení, předstírání identity značky / výkonného pracovníka, porušování práv k produktu atd. | Omezte digitální slepá místa a riziko, že kyberzločinci poškodí vaši značku, a zabraňte dalšímu poškození pověsti a finančním škodám. |
| **OCHRANA PŘED DIGITÁLNÍMI RIZIKY** | Třívrstvé řídicí panely<br>• Executive View je přístup založený na rizicích, který slouží vedoucím pracovníkům k rychlému pochopení externích rizik a pravděpodobnosti napadení.<br>• Management View je řízený přístup k systematickému procesu nápravy.<br>• Operational View vám poskytne technické podrobnosti o zjištěních a nápravě. | • Executive View – pomozte vedoucím pracovníkům rozdělovat zdroje tak, aby byly v souladu se strategií společnosti.<br>• Management View – poraďte vedoucím pracovníkům v oblasti zabezpečení, jak efektivně řídit nápravu.<br>• Operational View – zaměřte se na aktuální ukazatele a konkrétní potřebné akce. |
| **UZPŮSOBENÝ OVLÁDACÍ PANEL** | Funkce vyhledávání vám pomáhá hledat hrozby, kybernetické útoky a narušení, aktéry hrozeb, malware a phishingové kampaně z jediné platformy. | Můžete okamžitě řešit naléhavé indikátory související s vnějšími hrozbami. |
| **DOKUMENTACE RIZIK** | Dokumentace rizik zobrazující korelaci s IOC, zranitelnými místy, plochou útoku, digitálními riziky a dalšími informacemi. | • Umožňují vám rychle získat holistický pohled na vaše prostředí hrozeb – například jak by mohla být zranitelnost zneužita prostřednictvím konkrétní kampaně, a kteří kyberzločinci za ní stojí.<br>• Pochopte dopad na svá aktiva a získejte ucelený přehled o hrozbách. |
| **CENTRUM VÝSTRAH** | Centrum výstrah je uzpůsobené na míru tak, abyste pochopili, jaké jsou nejdůležitější hrozby a rizika pro vaši organizaci. | Pomůže vám rychle stanovit priority nápravných opatření. |
| **SLUŽBY VYPNUTÍ** | Nabízíme služby vypnutí stejně vypadajících/podvodných domén nebo webových stránek, stránek sociálních sítí, odstranění citlivých údajů na veřejných fórech a webech (podmíněno zásahem vlastníka webu). | Řídíme celý proces od začátku do konce včetně přípravy právních dokumentů, e-mailové komunikace, korespondence a vytváření blacklistů. |
| **INTEGRACE S BEZPEČNOSTNÍMI OVLÁDACÍMI PRVKY** | Poznatky můžete integrovat pomocí rozhraní API kompatibilních se standardy STIX a TAXII do svých bezpečnostních kontrol. | Obohaťte svá data, abyste posílili řízení kybernetické pozice. |
| **REAKCE NA INCIDENTY** | Reakce na incidenty pomocí funkce DeCYFIR pro vyhledávání informací, která poskytuje kompletní kontextové podrobnosti. | Urychlete odezvu na incidenty pomocí analýzy incidentů včetně analýzy prostředí externích hrozeb. |
| **OBJEVOVÁNÍ A MONITOROVÁNÍ RIZIKA PRO TŘETÍ STRANU** | ▪ Pomůžeme vám monitorovat domény třetích stran bez nutnosti složitých a rušivých implementací.<br>▪ Zmapujte jejich profil digitálních rizik a získejte povědomí o tom, zda nedošlo k úniku dat, odhalení zranitelných míst a podobně. | ▪ Zabezpečte svůj digitální ekosystém a získejte přehled o kybernetických rizicích třetích stran.<br>▪ Objevte slabá místa v digitálních aktivech svého dodavatele.<br>▪ Buďte si vědomi kybernetických rizik třetích stran a pochopte, jak by vás mohla ovlivnit. |

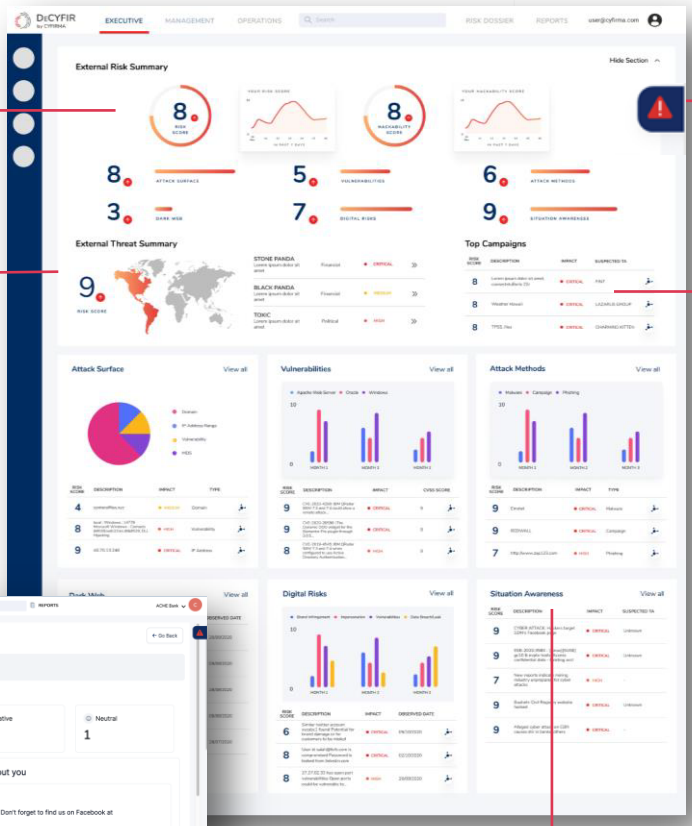
# EXECUTIVE VIEW

Ovládací panel DeCYFIR je aktivně-exekutivní nástroj pro vedoucí pracovníky, který jim pomáhá pochopit měnící se dynamiku a urychlit kritické rozhodování.

- Ovládací panely pro vedoucí pracovníky pomáhají pochopit měnící se dynamiku a urychlit kritické rozhodování
- Skóre rizik a napadnutelnosti hackery pro rychlé pochopení externích kybernetických rizik/hrozeb
- Klíčové ukazatele, trendy, atribuce a korelace
- Přehled kybernetických hrozeb relevantních pro vaši organizaci

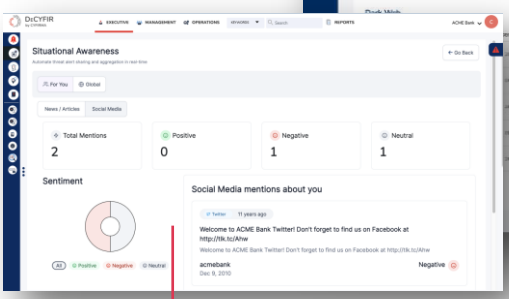
Porozumění **skóre** a trendům **v oblasti rizik a napadnutelnosti.**

Zobrazení **prostředí externích hrozeb** v reálném čase.




Indikátory **kritických hrozeb** se na ovládacím panelu zobrazují zřetelně, což usnadňuje včasné a přesné rozhodování.

**Detailní přehled** o aktérovi hrozby, motivu, kampaních a dopadu.




**Analýza sentimentu** neboli vytěžování názorů je klíčem k pochopení toho, jak vaši organizaci vnímá externí publikum. Přehledy mohou vrhnout světlo na potenciální útoky ze strany protivníků, hacktivistů a dalších.

Poskytuje **situační přehled** o tom, co se děje ve světě a jak tyto změny mohou ohrozit digitální profil organizace. Chápejte rizika, se kterými se můžete setkat, jako možné hrozby.

# MANAGEMENT VIEW

Systematický přístup k řízení bezpečnosti založený na osvědčených postupech usnadňuje zmírňování rizik pomocí návodných postupů. DeCYFIR metodicky odhaluje plochy útoku podle typu a formy jeho vedení, zranitelná místa, metody útoku, digitální rizika, také neustále sleduje aktivity na dark webu a poskytuje situační povědomí.

Podnikněte rychlé kroky ke zmírnění rizik pomocí návodných postupů

Systematicky odhalujte:

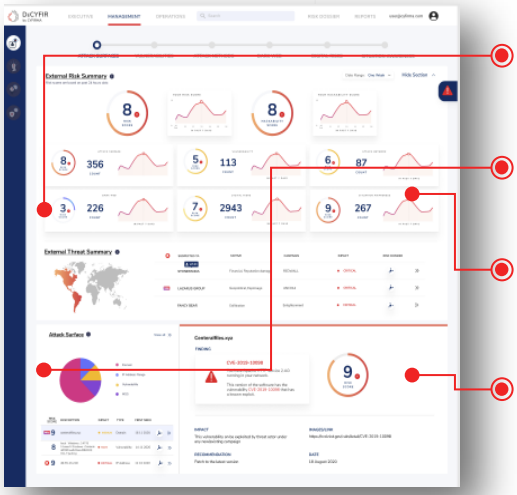
- Plochu útoku
- Zranitelná místa
- Metody útoku
- Expozice digitálním rizikům
- Pozorování z dark webu
- Povědomí o situaci

## 1 IDENTIFIKUJTE PLOCHU ÚTOKU

### IDENTIFIKUJTE POTENCIÁLNÍ VSTUPNÍ BODY

### KDE JSOU „DVEŘE“ A „OKNA“ PRO VSTUP

- Pomozte klientům identifikovat aktiva, jako je doména, subdoména, rozsah IP adres, verze softwaru, zranitelná místa a další body, které jsou vystaveny hackerům.
- Pomozte klientům získat úplný přehled o veřejně vystavených aktivech dostupných útočníkovi, konzultovat metody a vyhodnocovat rizika pro společnost.
- Pomozte klientům vytvořit účinnou bezpečnostní strategii.



„Counts“ - záznamy vás informují o nejnovějších expozicích za posledních 7 dní.

„Attack Surface“ - plocha útoku identifikuje dveře a okna, kterými se hackeři mohou dostat do vaší organizace.

„Trends“ - trendy zobrazují, jak si vedete v konkrétním časovém období v jednotlivých kategoriích.

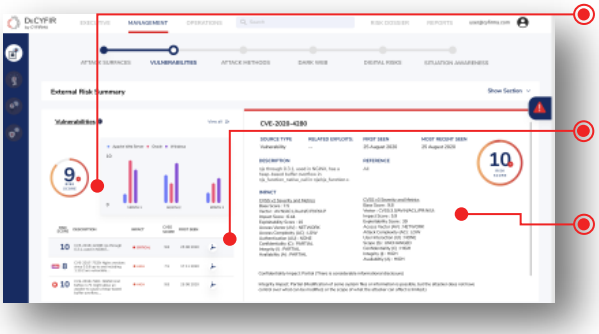
„Detail View“ - detailní pohled na konkrétní plochu útoku vás informuje o závažnosti a souvisejících atributech.

## 2 ODHALTE ZRANITELNÁ MÍSTA

### VEDOUCÍ PRACOVNÍCI V OBLASTI BEZPEČNOSTI SE STANOU PROAKTIVNÍMI PORADCI PRO RIZIKA

### KLÍČE OD „DVEŘÍ“ A „OKEN“, KTERÉ MOHOU ZLOČINCI VYUŽÍT

- Pomozte klientům dívat se pohledem kybernetického útočníka.
- Poznejte slabá místa a potenciální body narušení.
- Informace o zranitelnosti lze použít k vytváření modelů hrozeb a plánování bezpečnosti.



Tříměsíční trend pomáhá manažerům pochopit, která z jejich aktiv jsou zranitelnější.

Seznam kritických zranitelných míst za poslední 3 měsíce, na které by si společnost měla dát pozor

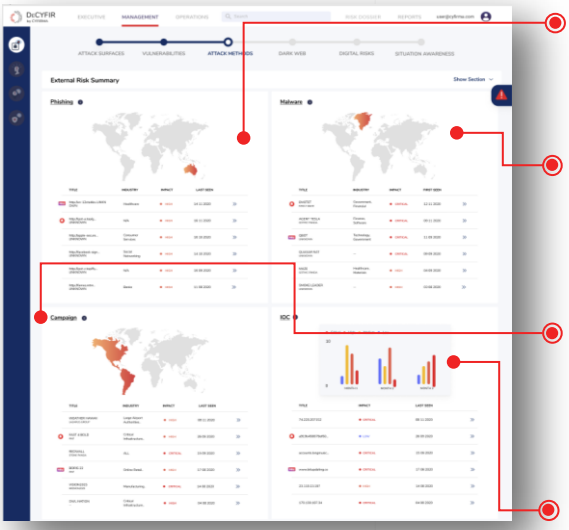
Podrobnosti/atributy kritické zranitelnosti.

## 3 SEZNAMTE SE S METODAMI ÚTOKU

### ROZŠIŘTE BEZPEČNOSTNÍ TELEMETRII O HLUBŠÍ PŘEHLED O POTENCIÁLNÍCH ÚTOCÍCH

## POZNEJTE, JAK HACKEŘI CHTĚJÍ NAPADNOUT VAŠI ODGANIZACI, ABYSTE MOHLI EFEKTIVNĚ REAGOVAT

- Poznejte metody a nástroje používané protivníky.
- Získejte informace o podrobnostech kampaně v rané fázi plánování.



Nejnovější phishingové útoky související s vaší organizací.

Pro manažery je důležité sledovat seznamy nejnovějších malwarů, které hackeři vydávají a které mohou být nebezpečné pro vaši společnost.

Aktéři hrozeb často využívají kybernetické útoky jako součást koordinované kampaně proti vaší společnosti.

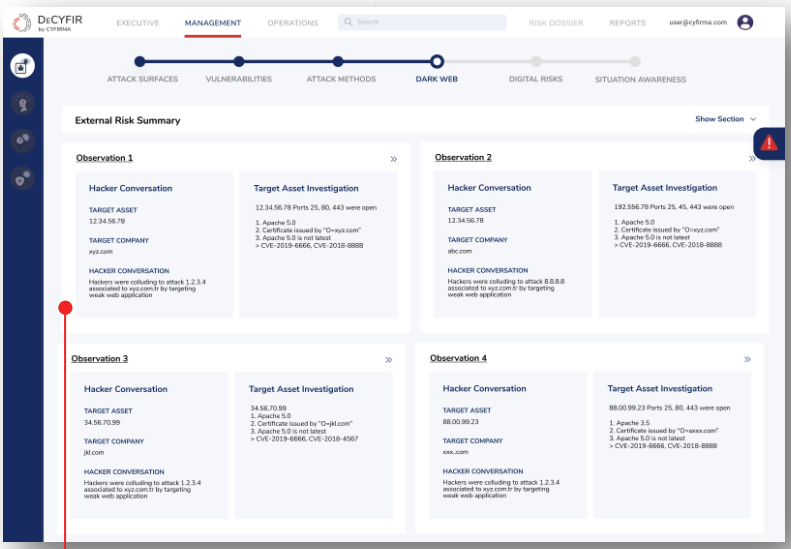
Rozsáhlý seznam relevantních indikátorů narušení - MD5, SHA, IP, DOMÉNA, HOSTNAME, URL, EMAIL, CVE, EXPLOIT, MUTEX, FILE, SSL atd.

## 4 POZOROVÁNÍ Z DARK WEBU

### AI MODULY ODHALUJÍ DŮKAZY INDIKUJÍCÍ KYBERNETICKÉ RIZIKO A ÚTOKY CÍLENÉ NA VÁS

## VSTUPTE MEZI HACKERY A ODHALTE DŮKAZY O POTENCIÁLNÍCH ÚTOCÍCH

- Udržujte si náskok před kyberzločinci tím, že získáte přehled o indikátorech hrozeb.
- Získejte náskok díky využitelným kybernetickým informacím.
- Aktivujte účinnou obrannou strategii pomocí včasných varování.



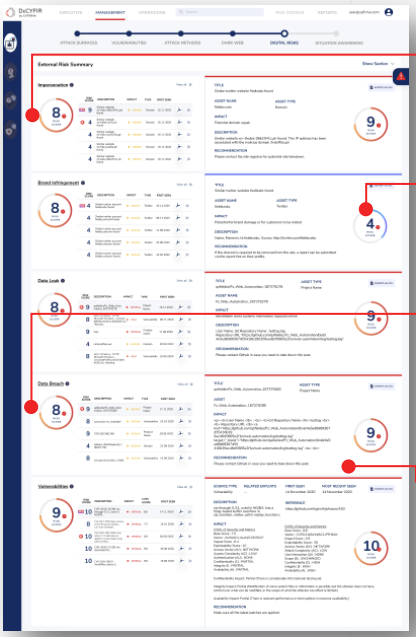

Informace o hrozbách shromážděné z deep/dark webu, z diskuzních fór a uzavřených komunit hackerů.

## 5 PROFIL DIGITÁLNÍCH RIZIK

### PŘIZPŮSOBTE BEZPEČNOSTNÍ ARCHITEKTURY KONTEXTU DIGITÁLNÍCH RIZIK

### PŘEVEZMĚTE ZPĚT KONTROLU NAD SVÝM DIGITÁLNÍM PROSTŘEDÍM

- Odhalte narušení značky/produktu.
- Odhalte kompromitaci vedoucích pracovníků.
- Buďte první, kdo se dozví, že došlo k úniku dat a krádeži identity.
- Vytvořte obrannou strategii, která zabrání opakovanému výskytu.



Všechny online entity, které se vydávají za digitální profil a aktiva organizace na základě poskytnutého názvu domény.

Zjistěte, jaká data vaší společnosti, která mohou hackeři potenciálně použít k útoku na vás, byla narušena. To může zahrnovat soubory / uživatelská jména / hesla atd.

Digitální profily, které mohou potenciálně poškodit vaši značku.

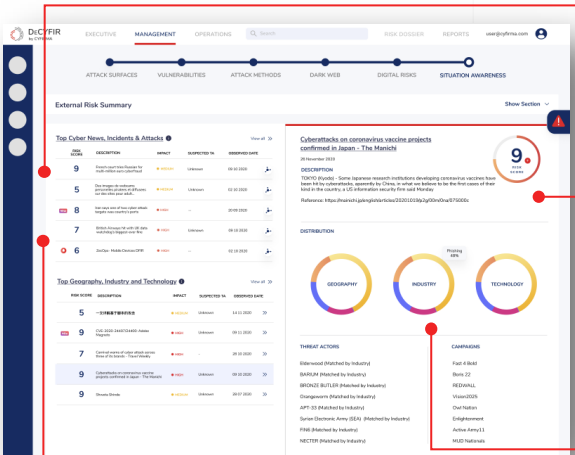
Hackeři mohou zneužít tato zranitelná místa - vektory útoku poškodí vaši organizaci, proniknou k citlivým datům atd.

## 6 POVĚDOMÍ O SITUACI

### DOSÁHNĚTE VYŠŠÍ EFEKTIVITY A PŘESNOSTI PŘI ROZHODOVÁNÍ

### POZNEJTE NOVÉ HROZBY A ZÍSKEJTE KONTROLU NAD RYCHLE SE MĚNÍCÍM PROSTŘEDÍM

- Vyzbrojte se relevantními informacemi o nejnovějších kybernetických útocích ve vašem odvětví, o změnách v kyberzákonech a dalšími základními poznatky.
- Přehledy pro strategické, manažerské a taktické rozhodování.




I v nejlépe financovaných a nejvyspělejších společnostech existují nedostatky v informacích o tom, jaký je současný stav a jaký by měl být ten cílový. Znalost situace se zde stává nezbytností pro kritické rozhodování.

Vybavte svou společnost informacemi o nejnovějším vývoji v oblasti kybernetických hrozeb a pochopte jeho dopad na vaše podnikání.

Hodnocení rizik pro získání konkrétních poznatků, které pomohou stanovit priority zdrojů pro řešení rizik a hrozeb.

Přehledy jsou užitečné pro organizaci, jsou relevantní pro danou geografickou oblast, odvětví a používanou technologii.

Grafické znázornění typů hrozeb a malwaru pro rychlou aktualizaci prostředí hrozeb, zobrazení podle lokality, odvětví a technologie.

# OPERATIONS VIEW

DeCYFIR umožňuje provoznímu týmu zorientovat se v „nepořádku“ a identifikovat zranitelná místa, která vyžadují okamžitou pozornost.

Skóre napadnutelnosti hackery kvantifikuje pravděpodobnost napadení digitálního profilu a aktiv společnosti klienta s ohledem na nedávný škodlivý vývoj v oblasti vnějších hrozeb dané společnosti.

Skóre rizik označuje úroveň rizik, která se vztahuje na společnost klienta v návaznosti na nedávný vývoj v oblasti vnějších hrozeb.

Aktéři hrozeb, jejich kampaně a dopad na vaši společnost.

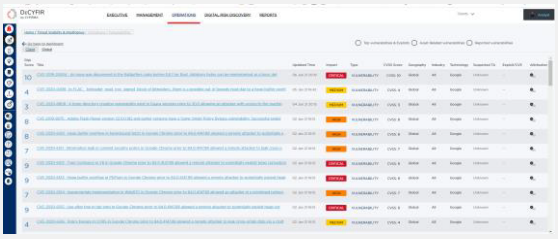
Pokud v organizaci běží více než několik set tisíc programů, middlewaru a hardwaru, je složité udržovat systémy aktualizované. DeCYFIR poskytuje úplný seznam všech vašich postižených systémů a příslušných zranitelných míst. Správa zranitelností je prioritizována na základě potenciálního dopadu a míře dostupnosti zneužitelných míst.

DeCYFIR odhaluje digitální rizika, konkrétně úniky dat, narušení, porušování práv k ochranné známce, krádež identity, expozice na sociálních sítích / darkwebu atd.

Monitorování možného zneužití konkrétních zranitelných míst na vašem webu, který je veřejně indexovatelný, i na dark webu, umožňuje týmu bezpečnostních operací zorientovat se a identifikovat zranitelná místa, která vyžadují okamžitou pozornost.

## PRIORITIZOVANÉ, RELEVANTNÍ A TAKTICKÉ MITIGACE PRO TÝMY SOC

- Provozní týmy mohou optimalizovat zdroje a zvýšit efektivitu
- Poskytování využitelných přehledů o zranitelných místech, IoC a hashech, které jsou relevantní pro váš obor, geografickou oblast a technologii
- DeCYFIR validuje indikátor a propojuje jednotlivé indikátory s kampaněmi, aktéry hrozeb a technikami vedení útoku



Rozsáhlý seznam relevantních indikátorů narušení – MD5, SHA, IP, DOMÉNA, HOSTNAME, URL, EMAIL, CVE, EXPLOIT, MUTEX, FILE, SSL atd.

DECYFIR®
BY CYFIRMA

# DECYFIR®

- Sjednocené 6-pilířové zobrazení eliminuje potřebu používat více nástrojů.
- Vyhledávání informací a hrozeb je rychlejší a přesnější.
- Správa procesů kybernetické bezpečnosti, optimalizace zranitelných míst, správa certifikátů a CMDB jsou bez námahy.
- Identifikuje neznámé útočné plochy, se kterými jste se dosud nesetkali, aby bylo možné přijmout nápravná opatření.
- Poskytuje mnohem efektivnější způsob prioritizace rizik na základě zohlednění vnějších faktorů – získání schopnosti reagovat na hrozby nejen na základě CVE.

- Poskytuje včasné varování k identifikaci hrozeb, které vás ohrožují. (Early Warnings)
- Omezuje digitální rizika vyplývající z úniku dat, z krádeže profilu na sociálních sítích, či z předstírání jiné identity.
- Umožňuje přístup k dokumentaci rizik za účelem propojení aktéra hrozby, jeho motivu, kampaně a metody, aby bylo možné přesně předvídat hrozící kybernetické útoky.
- Platformy CYFIRMA se integrují s dalšími nástroji, aby bylo zajištěno bezproblémové řízení pracovních postupů.
- Poskytuje přehled o rizicích třetích stran a informace, o tom, jak by jejich slabá místa a zranitelné body mohly ovlivnit vaše podnikání.

Pomocí DeCYFIR mohou společnosti zvrátit boj proti kyberzločincům díky kvalitním kybernetickým informacím, které jim umožní vidět situaci optikou protivníka a přijmout nápravná opatření k zastavení útoku v jeho průběhu.

Cloudový produkt SaaS

Subskripční model založený na předplatném

Individuální uživatelský plán na základě požadavků klienta

Jednoduchá implementace s minimálním zásahem do systému

## 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