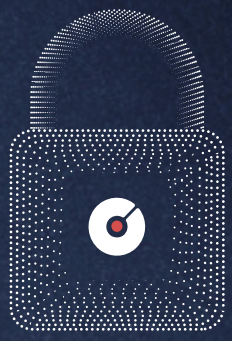
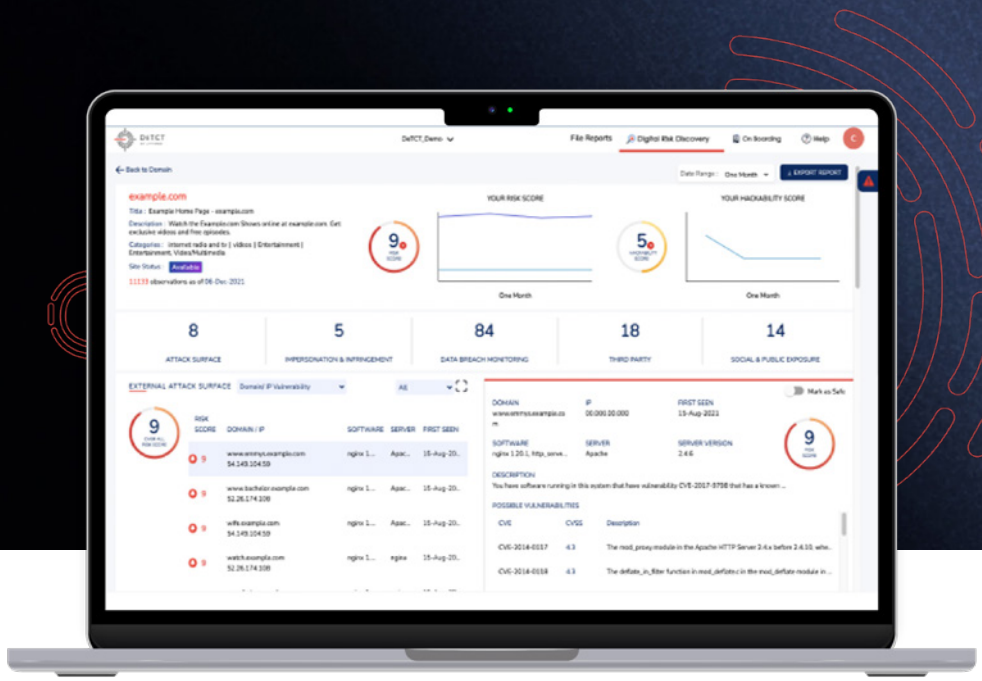
CYFIRMA
DECODING THREATS



„Digitální kontrarozvědka“ odhalí slabá místa v systému a předpoví útoky hackerů

Ukážeme vám, jak pomocí aplikace CYFIRMA
vezmete kybernetickým útočníkům vítr z plachet



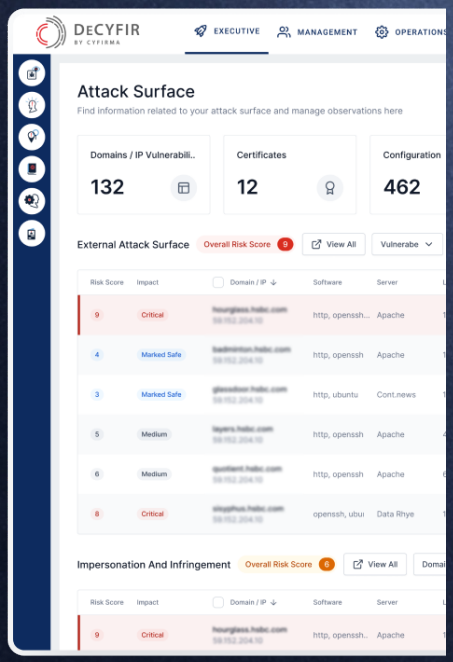
CYFIRMA
DECODING THREATS

Představte si svět, ve kterém budete umět předpovědět útok, který na vaší organizaci někdo potají chystá.

Budete navíc o chystaném útoku znát detaily: KDY, KDE a JAK k němu má dojít.

A navíc budete přesně vědět, KDO je váš nepřítel:

- **Předvídáte** kybernetické útoky a máte kontextové **informace o aktérovi hrozby**, motivu, metodě a kampani.
- Přesně víte, která firemní aktiva je třeba chránit, a znáte útočné vektory ohrožující tato cenná aktiva.
- Umíte zhodnotit rizika nových digitálních iniciativ ve firmě.
- Získáte neprůstřelné argumenty pro odpovídající rozpočty a personál v oblasti bezpečnosti.
- Zajistíte soulad se zásadami zabezpečení a aktualizace všech aspektů bezpečnostních kontrol.
- Efektivněji reagujete na kybernetické incidenty, správy záplat, správy konfigurace, správy verzí aplikací a dalších.



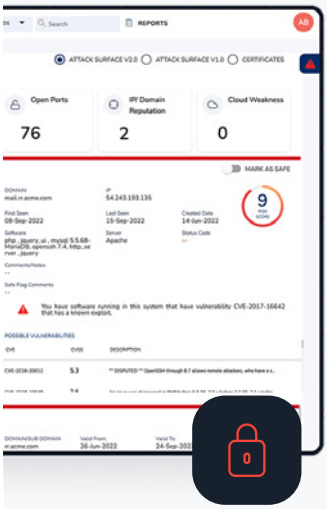
Využijte toho, že hacker připravuje útok vždy „na míru“ do prostředí vaší organizace

Naše služba postavená na základech řešení společnosti CYFIRMA s unikátní službou detekce chystaných kyberútoků je přesně to, co hledáte.

Zabráníte tak drtivým ztrátám v případě kyberútoku, který je dnes pro každou organizaci jen otázkou času (nejde o to, „jestli“ na vás zaútočí, ale „kdy“ se tak stane).

A hlavně...

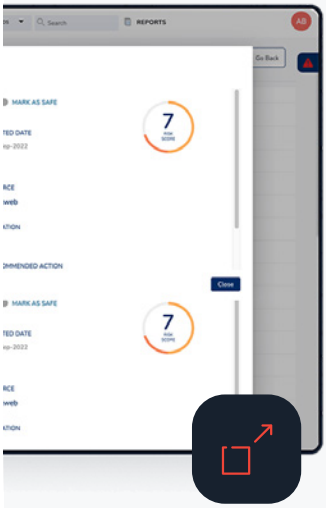
Stanete se žádaným partnerem pro vedoucí jiných oddělení, protože jim poskytnete cenné informace.



Z POHLEDU

Security Operating Center (SOC)

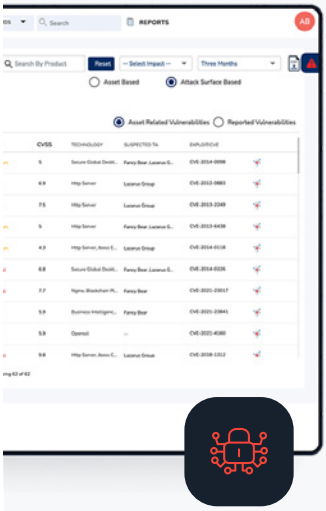
- Vylepšíte **každodenní detekce a reakce** pro udržení bezpečného provozního stavu ve vaší organizaci.
- **Maximalizujete prevenci** incidentů díky lepšímu pochopení aktérů hrozeb, jejich taktik, technik a postupů.
- **Sledujete** signatury malwaru a mutexu, phishingových domén, příkazových a řídicích center botnetu, škodlivých IPS a další.
- Přesně identifikujete potenciálně ohrožené **jednotlivce a digitální aktiva** (firemní know-how, účetní výkaznictví, obch. smlouvy a informace aj.).
- Znáte **cesty útoku** a **metody**, které může protivník použít k zahájení kybernetického útoku.
- Přesně víte, kam umístit bezpečnostní **kontroly** (Sharepoint, notebooky, IoT, PLC výrobní stroje apod.)
- Vždy máte k dispozici použitelné, včasné, strojově upravované poznatky s **podrobnostmi o ploše útoku, digitálním rizikovém profilu** a informacích o kybernetické bezpečnosti.
- Využijete **včasné varování** jako klíčovou funkci pro předvídání kybernetického útoku, a vybavíte SOC tým funkčními nápravnými i preventivními opatřeními.
- Máte v ruce přehledné **statistiky** o prostředí externích hrozeb. Takové informace pomáhají odhalit digitální rizika spojená se zranitelnými místy a odhalenými aktivy.
- Znáte **skóre rizika** pro jednotlivé indikátory hrozeb, což pomáhá SOC týmu snížit počet falešně pozitivních hlášení a neplatných upozornění.



Z POHLEDU

Chief Risk Officera (CRO)

- **Efektivně spravujete registr rizik** pomocí informací o hrozbách v reálném čase.
- **Včasnou identifikací zmírníte či odvrátíte** kybernetické hrozby a rizika.
- Sledujete **profil kybernetického rizika organizace** a díky tomu se vyhnete nákladným překvapením.
- Vždy máte aktuální podklady pro **lepší komunikaci s představenstvem** a zainteresovanými třetími stranami o hrozbách a rizicích, a o plánování odpovídajících iniciativ.
- **Znáte skutečnou hodnotu digitálních aktiv** vaší společnosti a také **spektrum rizik** kybernetické bezpečnosti, ve kterém organizace působí – kritické / vysoké / střední / nízké.
- **Vyhnete se osobní právní odpovědnosti** v případě, že se riziko naplní.



Z POHLEDU

Chief Marketing Officera (CMO)

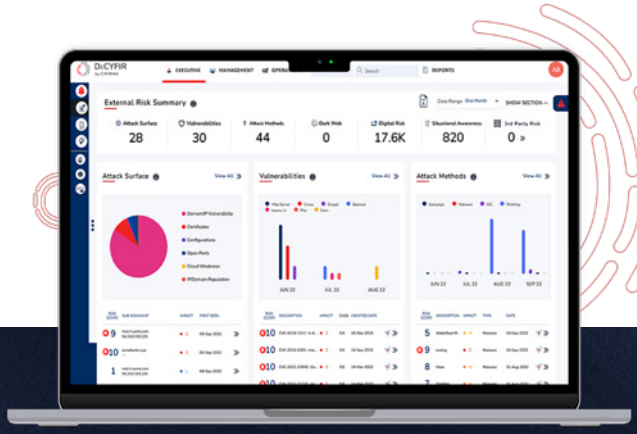
- Ochráníte **značku** před poškozením (např. včas zjistíte, zda nejsou spuštěny **očerňovací kampaně** s cílem napadnout značku).
- Ochráníte **know-how společnosti - produkty a duševní vlastnictví** před kybernetickou krádeží.
- Víte, zda byly vytvořeny **podobné domény nebo webové stránky**. Tím předejdete zneužití vašich webů formou jejich podvržení.
- Zamezíte **krádežím identity** klíčových manažerů na sociálních sítích a dalších platformách.
- Pojistíte si **loajalitu zákazníků** ke značce díky zabezpečení jejich dat a soukromí.

Otestujte bezpečnost vaší organizace třeba už zítra

Řešení **DeTCT** a **DeCYFIR** společnosti CYFIRMA používají unikátní patentovanou technologii. V posledních 4 letech zaznamenaly raketový úspěch a ocenily je renomované analytické společnosti jako jsou Gartner a IDC.

O kvalitách řešení se můžete nejlépe přesvědčit sami. K **otestování bezpečnostní situace vaší organizace** není potřeba z vaší strany investovat žádné finanční prostředky ani čas vašich zaměstnanců, stačí jen váš souhlas.

Test totiž probíhá na základě **cloudové AI analýzy vnějších zranitelností** s využitím pohledu a prostředků potenciálního útočníka pro simulaci kyberútoku.
Zní vám to dobře?



Více na www.cyfirma.cz

Jakub Karvánek
Sales Director FreeDivision
jakub.karvanek@freedivision.com
+420 777 654 144