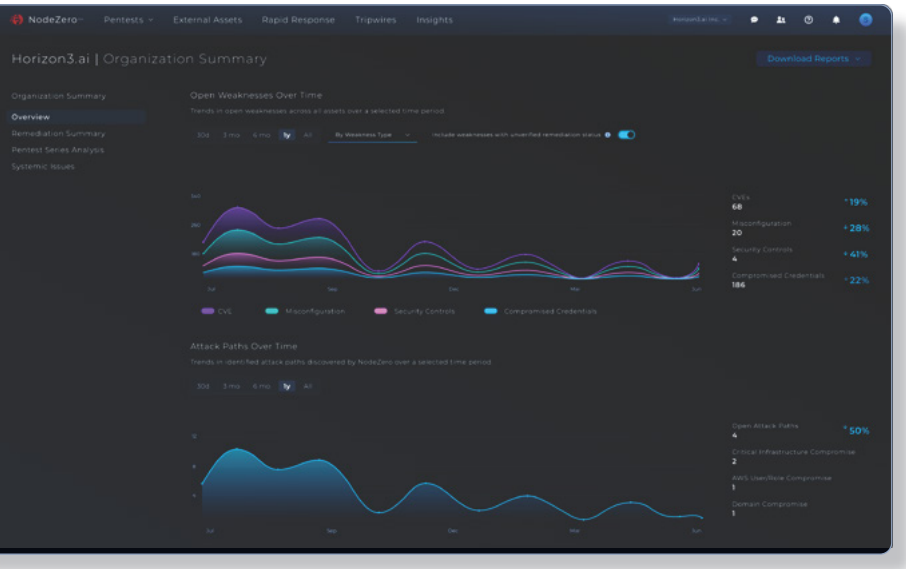
NodeZero Insights™

Rozhodujte lépe díky přehledným a prioritizovaným datům o hrozbách

NodeZero Insights nabízí dynamický, průběžný přehled celkového bezpečnostního stavu organizace a využívá přitom data získaná z autonomního penetračního testování NodeZero. Je navržen pro CIO, CISO a bezpečnostní lídry a umožňuje vám vytvářet a sdílet jasný, akčně využitelný přehled o bezpečnostní situaci organizace prostřednictvím komplexních reportů a vizualizací.

Prioritizujte to podstatné

NodeZero je jediný nástroj pro autonomní penetrační testování na trhu, který průběžně sleduje zneužitelné útočné cesty v infrastruktuře vaší organizace – a upřednostňuje skutečná rizika, místo aby jen vypisoval zranitelnosti, které mohou (ale nemusí) ovlivnit provoz. Insights přiřazuje zjištěným slabinám úrovně závažnosti a upozorňuje na nejkritičtější aktiva vyžadující pozornost. Vedení tak získává přehled na vysoké úrovni o tom, kde jsou slabá místa, a zároveň i detailní informace o tom, jaká opatření se přijímají k jejich odstranění.



HORIZON3.ai
TRUST BUT VERIFY

Klíčové funkce

Zjednodušte reporting pro vedení: Sdílejte aktuální přehledy v reálném čase a zjednodušený pohled na bezpečnostní stav vaší organizace. Vytvářejte manažerská shrnutí, která udrží klíčové stakeholdery informované a sladěné v tom, jak bezpečnost postupuje.

Odstraňte slepá místa v útočné ploše: Průběžně vizualizujte útočné cesty napříč všemi částmi infrastruktury a odhalujte přehlédnuté vstupní body, které mohou vaši organizaci vystavit riziku.

Sledujte pokrok v oblasti bezpečnosti: Sledujte klíčové ukazatele výkonnosti, jako je průměrná doba nápravy a počet otevřených slabin, což týmům umožňuje měřit pokrok v horizontu měsíců nebo čtvrtletí. Tato data podporují lépe informované rozhodování a zvýrazňují efektivitu bezpečnostních iniciativ.

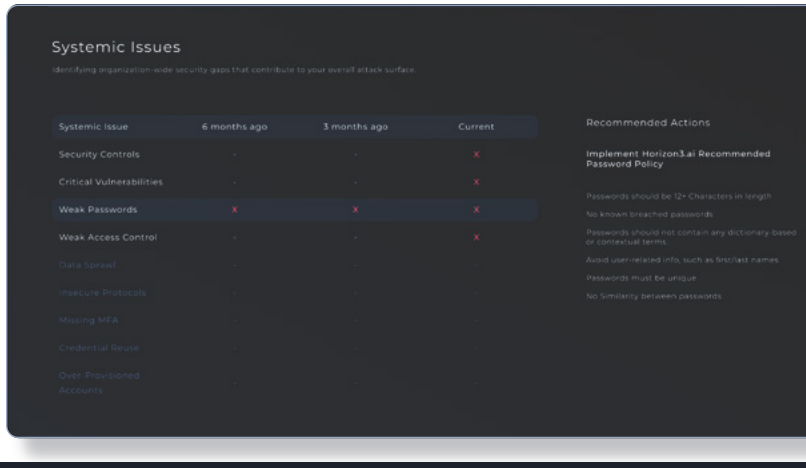
Detailní pohled na trendy slabin: Získejte přehled o nápravných opatřeních analýzou otevřených bezpečnostních slabin v čase – podle typu (např. CVE, chybné konfigurace, mezery v bezpečnostních kontrolách, kompromitované přihlašovací údaje) i podle závažnosti (kritická, vysoká, střední, nízká).

Umožněte týmům efektivně jednat díky prioritizaci: Odstraňte šum tím, že upřednostníte skutečně zneužitelné slabiny, a zaměřte nápravná opatření na problémy, které pro organizaci představují reálné riziko.

Identifikujte systémové problémy: Předcházejte budoucím incidentům řešením systémových slabin, které vyžadují plošné úpravy bezpečnostních politik v celé organizaci – například nahrazení slabých hesel nebo aktualizaci nezabezpečených protokolů.

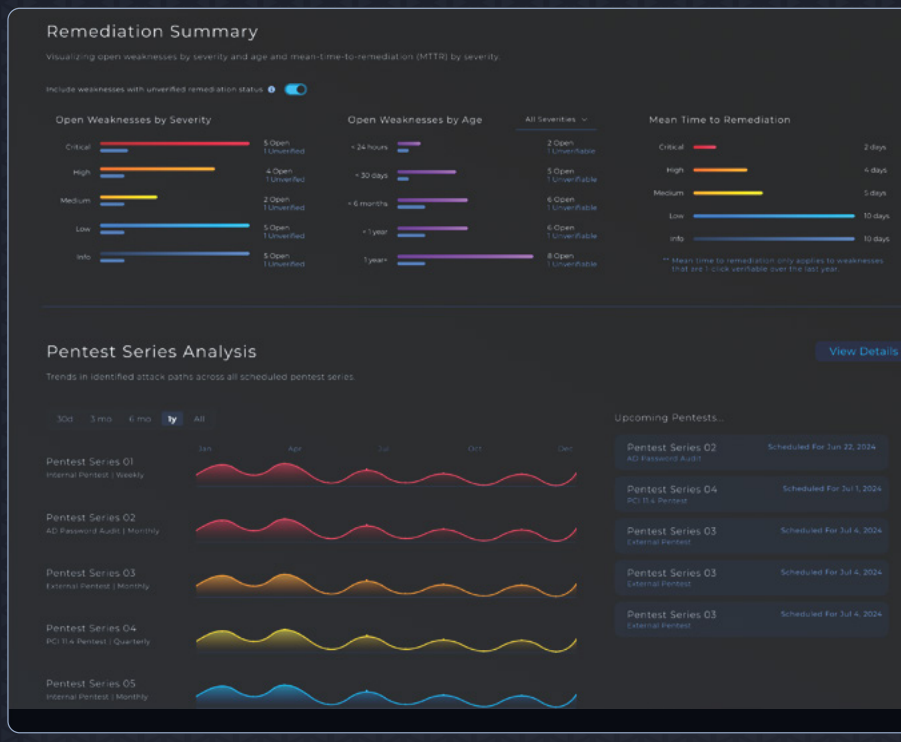
Nedůvěřujte... Ověřujte svůj bezpečnostní stav

V neustále se vyvíjejícím prostředí hrozeb se aplikace a servery aktualizují a přístupová oprávnění se mění. NodeZero Insights poskytuje vedení a bezpečnostním lídrům možnost průběžně měřit a ověřovat bezpečnostní stav jejich organizace a zajišťuje tak, že zůstává odolná vůči nově vznikajícím hrozbám.



Testujte technické cíle

NodeZero Insights propojuje otevřené slabiny s jejich příslušnými útočnými cestami a odhaluje, zda mohou útočníci dosáhnout vysoce závažných dopadů, jako je kompromitace doménového admina, převzetí hosta nebo únik dat. Bezpečnostní týmy tak mohou upřednostnit nápravu tam, kde Insights prokázal skutečnou zneužitelnost prostřednictvím testování v reálných podmínkách.



Testujte provozní bezpečnostní scénáře

Sledujte trendy z plánovaných penetračních testů – týdenních, měsíčních nebo čtvrtletních – a ověřujte tak účinnost segmentace sítě a iniciativ Zero Trust. Zároveň identifikujte potenciální rozsah dopadu při kompromitaci konkrétních přihlašovacích údajů. To umožňuje vedení jemně ladit bezpečnostní kontroly na základě ověřených poznatků, nikoli předpokladů.

Měřte dopad na podnikání

Systémové problémy jsou prezentovány v kontextu možných dopadů na podnikání, jako je riziko narušení dostupnosti služeb nebo ztráty integrity dat. Tyto informace pomáhají CIO a CISO posoudit provozní dopady a přijímat rozhodnutí o bezpečnostních politikách na základě dat, v souladu s cíli kontinuity provozu a odolnosti organizace.

Pro více informací o NodeZero Insights, napište na info@sec4good.cz

Sec4good

HORIZON3.ai
TRUST BUT VERIFY