HORIZON3.ai

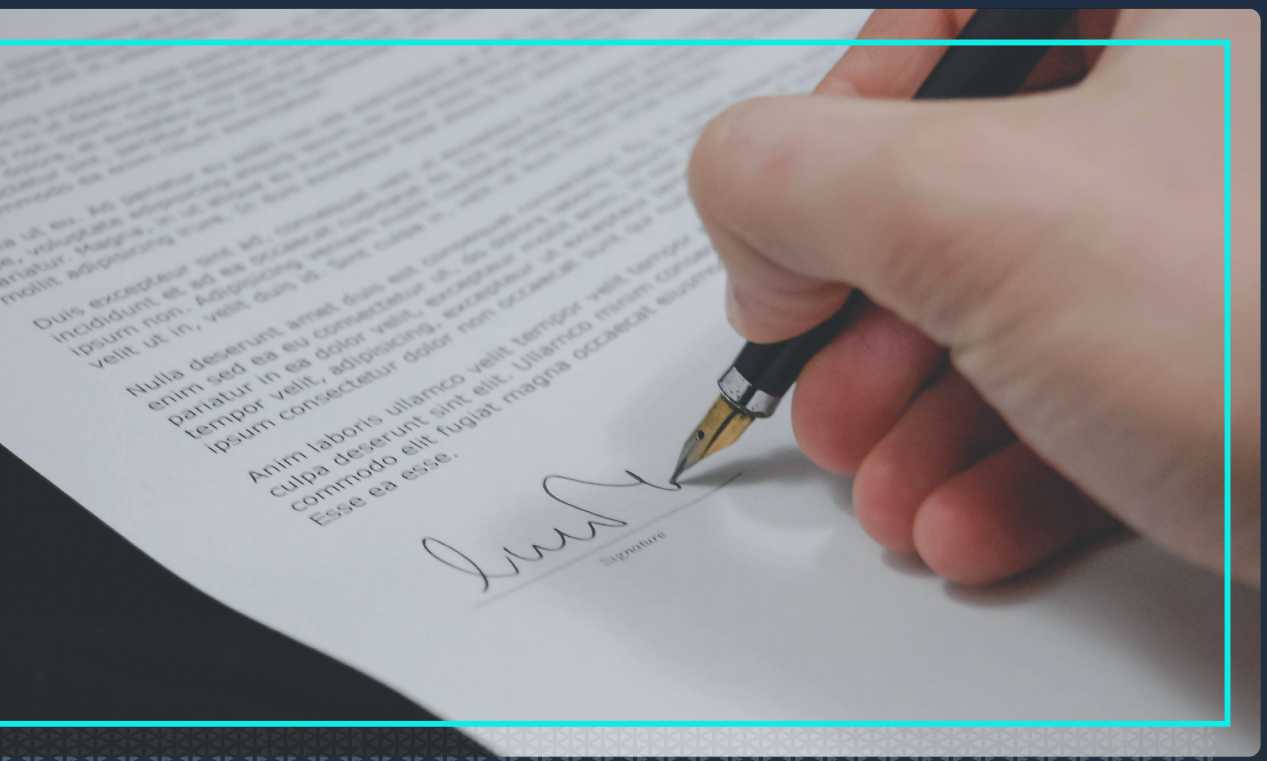
~~TRUST~~ BUT VERIFY

WHITE PAPER

Odolnost dle DORA

Prokazování odolnosti podle DORA v právním sektoru

Jak mohou právnické firmy podporovat finanční klienty pomocí bezpečnostní strategie založené na CTEM a důkazech



Nová úroveň kontroly

Nařízení EU o digitální provozní odolnosti (DORA) nově definuje, jak musí finanční instituce řídit kybernetická rizika – nejen uvnitř vlastních organizací, ale napříč celým ekosystémem třetích stran. Právnické firmy jsou nyní klíčovou součástí této rovnice jako správci citlivých informací a zprostředkovatelé transakcí s vysokou hodnotou.

Podle nařízení DORA se od finančních institucí očekává, že zajistí, aby jejich dodavatelé s přístupem k ICT byli odolní, bezpeční a průběžně testovaní. Pro poskytovatele právních služeb to znamená zásadní změnu – od občasné due diligence k průběžnému ověřování.

Není již přijatelné jednoduše tvrdit, že jsou zavedena ochranná opatření. Klienti očekávají důkazy a regulační orgány je stále častěji vyžadují. Právnické firmy, které chtějí zůstat důvěryhodnými partnery, musí prokázat svou schopnost odolat taktikám, technikám a postupům, které dnešní útočníci aktivně používají.

Nejde už jen o teoretickou hrozbu. Řada advokátních kanceláří se stala terčem mediálně sledovaných incidentů, při nichž došlo k odhalení důvěrných klientských dat, spisového materiálu chráněného mlčenlivostí a interní komunikace – často v důsledku phishingu, zneužití přístupů zevnitř nebo nedostatečných kontrol u dodavatelů třetích stran.

Od jednorázového ověření k průběžnému zajištění

Zvýšený dohled nad právními dodavateli není dán jen regulací – odráží i měnící se charakter moderních hrozeb. Právnické firmy často pracují s distribuovaným přístupem, hybridními pracovními silami a nástroji pro spolupráci třetích stran, což vše rozšiřuje zneužitelnou útočnou plochu.

Špatně nakonfigurované řízení přístupu, nesegmentované interní sítě, opakovaně použité nebo ohrožené přihlašovací údaje a náchylnost k phishingu se staly běžnými vstupními body pro útočníky. Útočníci navíc často vnímají právní kanceláře jako snazší cíl než silně regulované banky a investiční společnosti, kterým poskytují služby.

A regulační orgány si toho všímají: některé firmy již obdržely formální napomenutí nebo finanční pokuty za nedodržování základní kybernetické hygieny – zejména v případech, kdy se jednalo o externí IT poskytovatele nebo nedostatečně monitorované procesy.

Aby si firmy udržely náskok, musí překročit rámec tradičních auditů a skenování zranitelností. Je zapotřebí neustálé testování s ohledem na útočníky, které ukazuje, co lze skutečně zneužít – nejen co by mohlo být zranitelné. To je podstata kontinuálního řízení expozice hrozbám (CTEM).

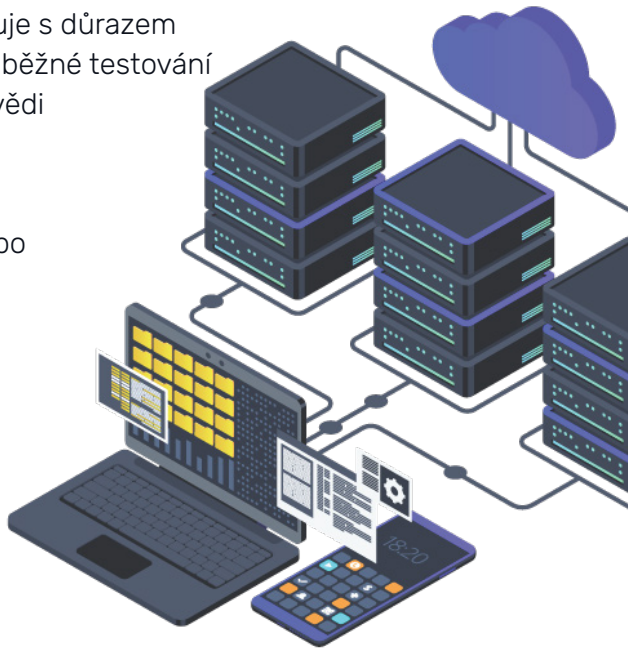
CTEM: Strategie odolnosti v reálném světě

Kontinuální řízení expozice hrozbám - Continuous Threat Exposure Management (CTEM), , jak je definováno společností Gartner®, je programový model, který umožňuje organizacím odhalovat, ověřovat a snižovat reálná bezpečnostní rizika. Jedná se o strategický, iterativní přístup složený z pěti klíčových fází:

Fáze 1	Fáze 2	Fáze 3	Fáze 4	Fáze 5
Určení Rozsahu digitálního prostředí k posouzení	Identifikace vystavených systémů a slabých míst	Prioritizace zneužitelných rizik s vysokým dopadem	Validace pomocí simulace reálných útoků	Mobilizace s cílenou nápravou a ověřováním

Pro právnické firmy představuje CTEM plán, jak skutečně prokázat odolnost – nejen dosáhnout souladu s předpisy. Dokonale se shoduje s důrazem nařízení DORA na řízení ICT rizik, provozní kontinuitu a průběžné testování bezpečnosti. Dobře nastavený CTEM program dává odpovědi na otázky, které si regulátoři i klienti už dnes kladou:

- Jsou vaše zranitelnosti skutečně zneužitelné?
- Může útočník zvýšit svá oprávnění nebo se dál šířit po interní síti?
- Jaký dopad by měla kompromitace přihlašovacích údajů?
- Testujete pravidelně a realisticky vaše prostředí?
- Dokážete předložit ověřené důkazy o úrovni své bezpečnosti?



Právě zde se platforma NodeZero® stává nepostradatelnou.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

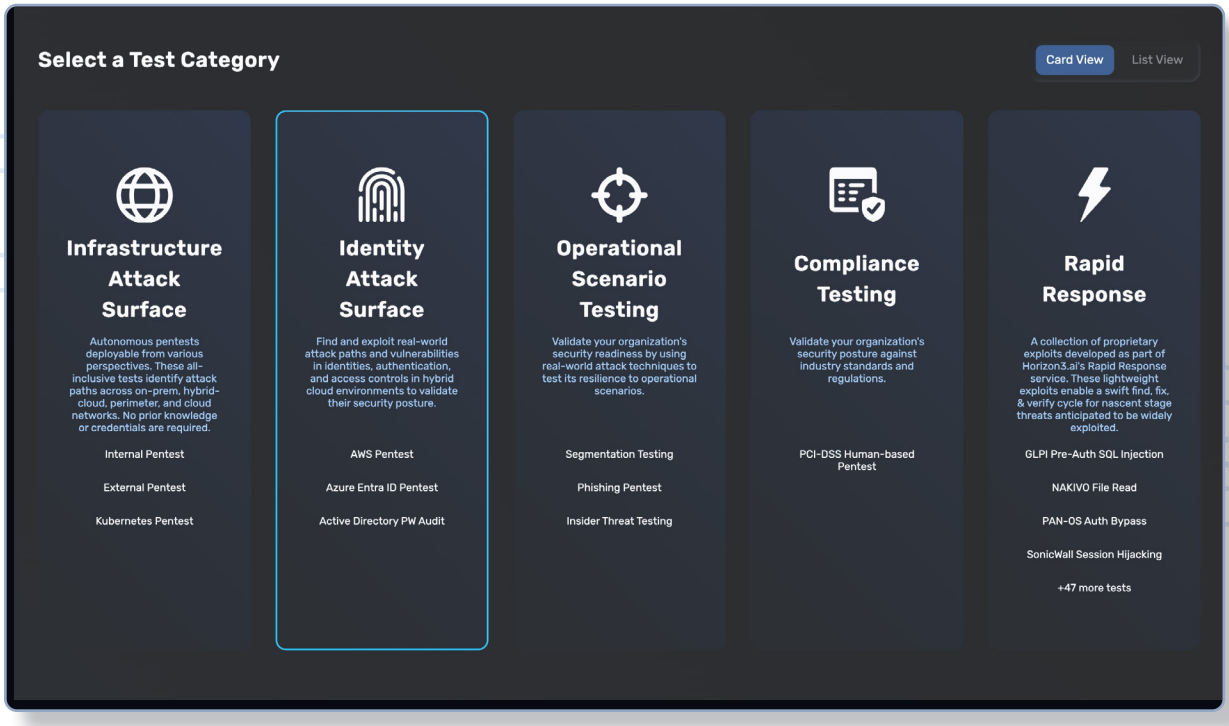
NodeZero ®: Autonomní důkaz bezpečnosti

NodeZero od Horizon3.ai je autonomní platforma pro penetrační testování, která se chová jako útočník – řetězí slabé přihlašovací údaje, špatnou segmentaci, vystavené služby a nemonitorovaný administrátorský přístup, aby přesně ukázala, jak by k narušení mohlo dojít.

Na rozdíl od tradičních posouzení se NodeZero neopírá o domněnky. Pro každý zjištěný problém dodá důkaz, cestu útoku a dopad – a to průběžně, bezpečně a bez nutnosti externích konzultantů nebo speciálních softwarových agentů.
NodeZero pomáhá právním firmám:

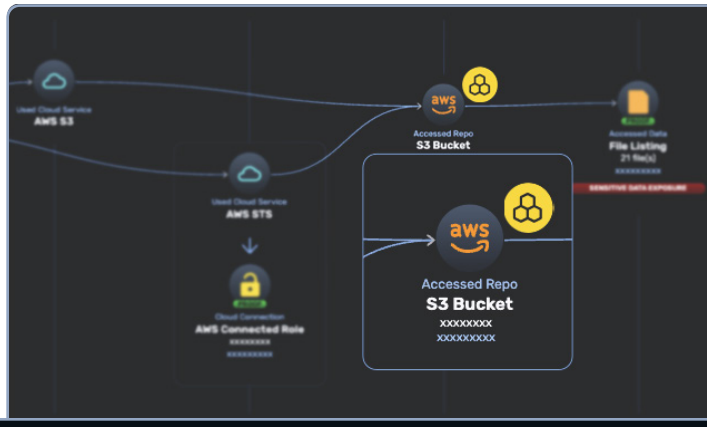
- Simulovat chování reálného útočníka přímo ve vlastní infrastruktuře
- Identifikovat zneužitelné mezery v eskalaci oprávnění, segmentaci nebo v opětovném použití přihlašovacích údajů
- Prioritizovat nápravná opatření podle jejich skutečného dopadu na byznys
- Okamžitě znovu otestovat opravy a ověřit jejich účinnost
- Připravovat důkazy podložené reporty pro audity, klienty a interní stakeholdery
- Ověřovat externí IT služby a poskytovatele bezpečnostního dohledu přímým testováním jejich kontrol a procesů

Ať už jde o hledání příležitostí k laterálnímu pohybu útočníka po phishingem získaném přihlášení, nebo o testování segmentace mezi souborovými sdílenými úložišti a klíčovou infrastrukturou, NodeZero poskytuje firmám opakovatelný a dobře obhajitelný postup ke snižování rizik.



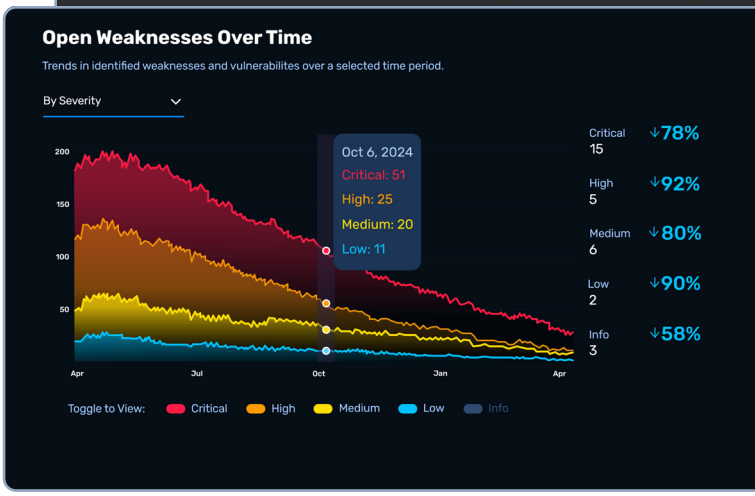
HORIZON3.ai
~~TRUST BUT~~ VERIFY

Pokročilé funkce, které zvyšují laťku



Několik pokročilých funkcí dělá z NodeZero mimořádně cenný nástroj pro právní služby, které podporují finanční instituce:

Tripwires™ nasazuje klamné artefakty – například falešné přihlašovací údaje nebo soubory – podél zjištěných útočných cest. Pokud s těmito návnadami pracuje útočník nebo škodlivý insider, NodeZero odešle okamžité upozornění s minimem falešně pozitivních nálezů.



NodeZero Insights™ převádí detailní zjištění do přehledných dashboardů a KPI. Bezpečnostní manažeři tak mohou sledovat trendy, jako je průměrný čas nápravy, neuzavřené exploitační cesty a systémové problémy – a získávají tak jasný přehled o tom, jak se situace v čase zlepšuje.

Překonejte shodu s předpisy. Poskytněte jistotu.

Právnické firmy už nestojí jen „vedle“ odolnosti finančního sektoru – jsou jejím středem. S nástupem DORA musí být schopné prokázat svou připravenost jak klientům, tak regulátorům.

NodeZero to umožňuje – poskytuje průběžné, autonomní ověřování úrovně zabezpečení pomocí simulace útočníka a testování v reálném prostředí. Právním týmům tak umožňuje posunout se od teoretických hodnocení rizik k prakticky doložitelnému důkazu odolnosti.

840 Impacts
677 Weaknesses
706 Credentials
1K Protected Data Items
84 Compromised Hosts

NodeZero pomáhá poskytovatelům právních služeb nejen dodržovat předpisy, ale také získávat důvěru, získávat zakázky a aktivně se podílet na ochraně provozu svých klientů.