HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

Výrobní sektor

# 5 Pět klíčových benefitů průběžného testování bezpečnosti ve výrobě

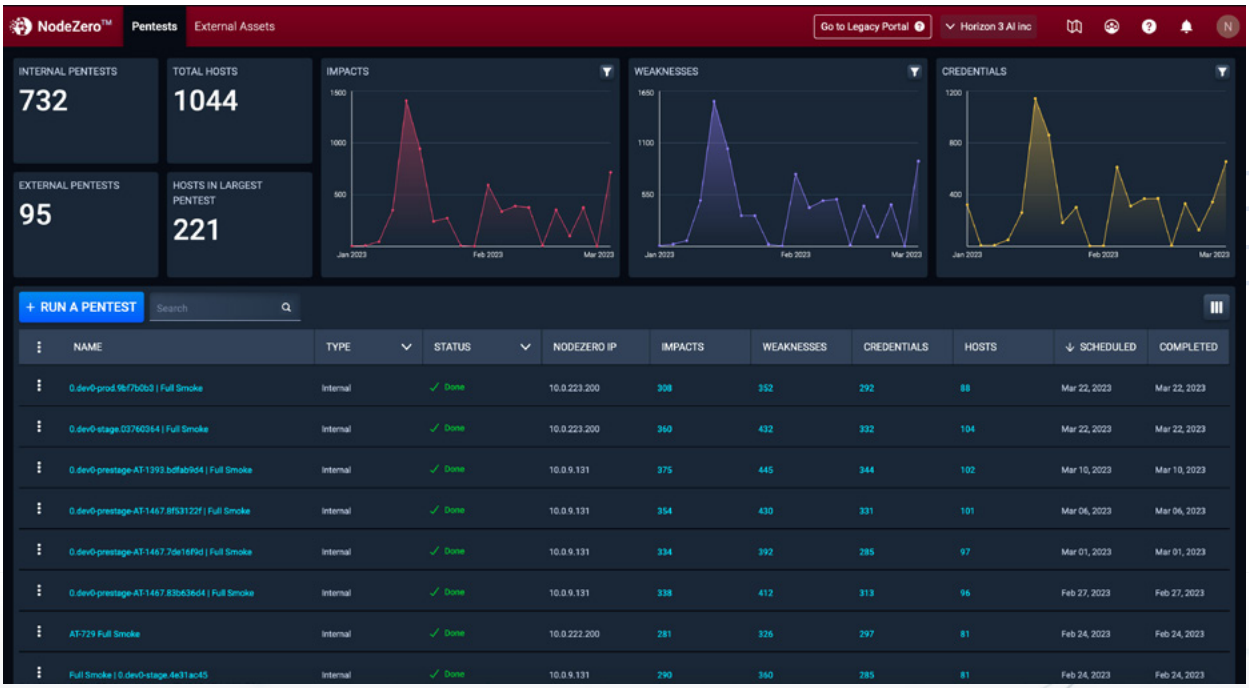
 @Horizon3ai info@horizon3.ai www.horizon3.ai

*Pět klíčových benefitů průběžného testování bezpečnosti ve výrobě*

# Jak autonomní penetrační testování pomáhá výrobcům vyhodnotit a snížit riziko

Historicky čelili výrobní podniky celé řadě překážek – silné konkurenci, neschopnosti se dostatečně rychle modernizovat a také regulacím uvaleným ze strany státu. Ještě donedávna jim vesměs stačilo vyrábět zboží a „informačními" hrozbami se příliš nezaobírali. To se ale zásadně změnilo. Stejně jako ostatní odvětví, i výrobci převzali nové informační technologie (IT), provozní technologie (OT), internet věcí (IoT) a celou řadu dalších technologií, které dnes moderní výrobní firmy potřebují k úspěchu v konkurenčním prostředí.

Zároveň dnešní prostředí kybernetických hrozeb doslova překypuje útočníky, kteří chtějí výrobní podniky odstavit, vydírat je výkupným a poškodit jejich provoz i značku. Z pohledu odolnosti a plánování kontinuity provozu představují výpočetní systémy, které řídí kanceláře, továrny, stroje a všechny ostatní procesy zefektivňující výrobu, zcela novou úroveň významného rizika. Vzhledem k nedávné vlně ransomwarových útoků napříč všemi odvětvími nebylo pro výrobní firmy nikdy větší riziko stát se obětí útoku než dnes.



# Enter NodeZero™

Vzhledem k trvalému tlaku kybernetických hrozeb na výrobní sektor nabízí Horizon3.ai platformu **NodeZero**, která výrobním organizacím pomáhá průběžně hodnotit vlastní odolnost, odhalovat kritické problémy a ověřovat zlepšování bezpečnosti v průběhu času. NodeZero je navržen tak, aby díky autonomnímu penetračnímu testování umožnil vidět a testovat sítě z pohledu útočníka.

Defenzivní kyberbezpečnostní technologie, které jste nasadili ve svém výrobním prostředí, vám mohou pomoci zablokovat útok zvenčí dovnitř. Bohužel ale žádná z těchto technologií neukazuje, kudy ve vašich sítích vedou možné útočné cesty. Právě proto jsme vyvinuli NodeZero. Zviditelní, kde se ve vašich sítích nacházejí zneužitelné zranitelnosti a slabiny, vysvětlí, jak je rychle napravit, a poté ověří, že oprava skutečně fungovala.

Například jeden významný globální výrobce, který dodává komerční, průmyslová i komunální řešení pro vodohospodářství, zvolil agresivní a proaktivní přístup k ověřování bezpečnostních kontrol a politik pomocí NodeZero. Tím, že si do firmy zavedli autonomní pentestingové řešení Horizon3.ai, tato organizace postupně posílila a zvýšila odolnost své kybernetické bezpečnosti — a to rychle i ve velkém měřítku.

S týmem, sestávajícím pouze ze dvou bezpečnostních inženýrů, zahájil výrobce více než 12 000 hodin zcela automatizovaného penetračního testování pomocí NodeZero. Zatímco dříve prováděl pouze 1–2 penetrační testy ročně, od nasazení NodeZero v polovině roku 2021 již v prostředí s přibližně 12 000 hosty realizoval více než 320 penetračních testů. Podle výrobce toto úsilí výrazně snížilo jeho kybernetické riziko.

Díky přijetí purple team kultury dokázala organizace využívat NodeZero jako sparring partnera i jako interního auditora svého souboru bezpečnostních nástrojů, stejně jako politik, postupů a infrastruktury.

> **Díky pravidelnému provádění testů pomocí NodeZero šetří tým IT bezpečnosti čas při ladění detekce, logování, alertingu a blokování škodlivých hrozeb napříč jejich SIEM/SOAR řešeními, EDR nástroji a dalšími obrannými prostředky.**

NodeZero navíc pomohl stát v čele infrastrukturního auditu v rámci nedávno dokončené fúze a akvizice (M&A). Provedením penetračního testu organizace, která měla být akvizicí teprve získána, dokázala kupující společnost proaktivně identifikovat a zmírnit nová rizika ještě před dokončením fúze. Po uzavření M&A došlo k plynulému sloučení IT infrastruktur a všechna aktiva jsou nyní posuzována podle stejných bezpečnostních standardů. Úspory z hlediska snížení rizik i času potřebného k provedení náležité due diligence v rámci fúze byly významné..

# Zvýšená úroveň rizika

Vzhledem k neustálým změnám v oblasti kybernetických hrozeb čelí výrobci řadě specifických výzev v oblasti IT, ale také reálným fyzickým dopadům, které ovlivňují jejich hospodářské výsledky. Dnešní útočníci si tyto nevýhody velmi dobře uvědomují, zejména závislost výrobců na různých výpočetních systémech, zastaralých operačních systémech, komerčních a na míru vytvořených aplikacích a mnoha zařízeních – některých nových a některých neuvěřitelně starých.

Zjednodušeně řečeno, hlavní hrozbou pro výrobní podniky jsou útočníci, kteří získají vzdálený přístup k jakémukoli internímu výpočetnímu zařízení. Jakmile útočník přístup získá, využije jej k ovládnutí sítí a zašifrování kritických systémů. Pokud je útok úspěšný, provoz se zastaví, dokud není zaplaceno výkupné.


**Podle studie společnosti IBM činí průměrné náklady na ransomware útok – bez započtení samotného výkupného – 4,54 milionu USD.**

Ve srovnání s přírodní katastrofou, požárem nebo jinou obdobnou událostí je kybernetický incident, jako je ransomware, který zastaví výrobu, stejně kritický scénář, na který je nutné se připravit – zejména z pohledu řízení rizik a kontinuity podnikání. Klíčem k omezování rizik je průběžně posuzovat vlastní část kybernetického prostředí, identifikovat možné útočné cesty a opravovat to, co má největší dopad. Výsledky mohou být z hlediska zlepšení kybernetické bezpečnosti velmi výrazné.

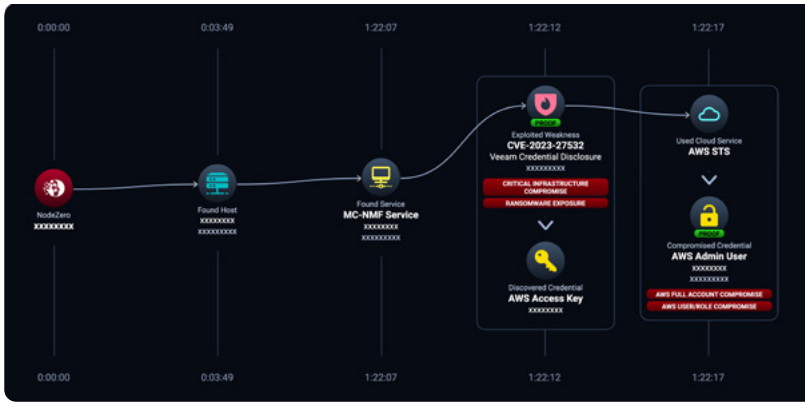
Společnosti jako FM Global, které poskytují pojištění výrobním podnikům, své klienty motivují k rozvoji bezpečnostní kultury a k jasné identifikaci podnikových rizik, včetně kybernetických rizik. To zahrnuje provádění kvalitních bezpečnostních analýz rizik za účelem odhalení slabých míst a následně na jejich odstranění spolupracovat s odborníky. Pojišťovny si jasně uvědomují hodnotu řízení rizik i jejich zmírnění.

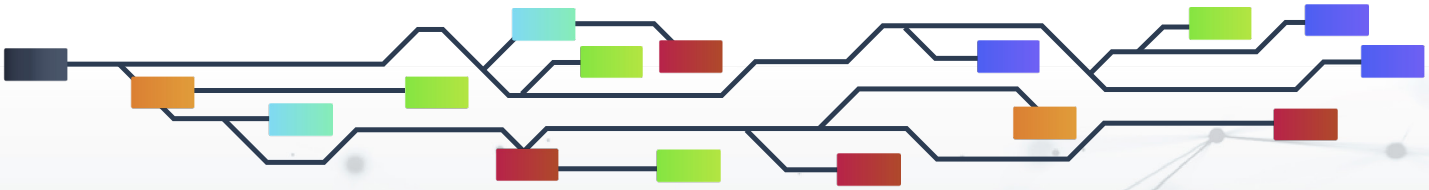
# Cesty útoku v kostce

V kontextu kybernetické bezpečnosti představují cesty útoku grafické znázornění možných tras, kterými se může útočník vydat při zneužití slabin ve vašich počítačích, serverech, aplikacích, infrastruktuře a bezpečnostních kontrolách. Analýza cest útoku upozorňuje na používané slabé přihlašovací údaje, odhaluje chybné konfigurace softwaru, identifikuje známé zranitelnosti aplikací a vyhledává nebezpečná výchozí nastavení produktů.

Existují dva způsoby, jak odhalit cesty útoku – po útoku a před útokem. V případě přístupu „po útoku “ je forenzní specialisté identifikují až poté, co útočníci dokončí svou činnost. Ukazují, co útočník provedl, přičemž odborníci často musí vycházet z určitých předpokladů. Tento typ analýzy je důležitý jako zpětné vyhodnocení, ale neochrání vás před následky útoku.

V dnešním světě, kde se uplatňují ofenzivní bezpečnostní přístupy, je zásadní odhalovat cesty útoku ještě předtím, než se stanou realitou. Tím se snižuje riziko, zvyšuje se odolnost a pomáhá to zajistit kontinuitu podnikání. Proto jsou ve výrobě i ve všech dalších odvětvích vysoce žádaná řešení, která dokážou bezpečně, přesně a průběžně provádět posouzení kritické infrastruktury a sítí, odhalovat cesty útoku, poskytovat doporučení k nápravě a zajistit, že dochází ke skutečnému zlepšování bezpečnosti.





HORIZON3.ai
TRUST BUT VERIFY

# Příklad cesty útoku


*Obrázek 1*

Ačkoli jsou některé cesty útoku poměrně složité, jiné jsou naopak překvapivě snadno pochopitelné. Například obrázek 1 znázorňuje cestu útoku pocházející z penetračního testu provedeného pomocí NodeZero. V tomto případě NodeZero simuloval útočníka, který získal počáteční přístup (foothold) do produkční sítě společnosti.

> **Jakmile NodeZero zahájil svou činnost, byl plně schopen prokázat kompromitaci domény v organizaci a získat oprávnění domain admina přibližně během 25 minut.**

Zajímavé na cestě útoku zobrazené na obrázku 1 je také to, že NodeZero **odhalil H3-2023-0003: Pre-Windows 2000 Computer Set** (viz horní střed obrázku 1), který ovlivňoval přihlašovací údaje konkrétního doménového uživatele.

Poté NodeZero ověřil přihlašovací údaje doménového uživatele zneužitím zranitelnosti H3-2023-0003: Pre-Windows 2000 Computer Set. O několik kroků dál útok NodeZero vyústil v kompromitaci domény a kompromitaci doménového uživatele. (Viz zcela vpravo.)

NodeZero v této síti nalezl počítač běžící na operačním systému z doby před Windows 2000, zneužil jej a nakonec získal oprávnění Domain Admin. V prostředí výrobních podniků je pravděpodobné, že se zde stále používají některé starší počítače s již nepodporovanými operačními systémy. Přestože tyto starší stroje pro své minimální úkoly fungují zcela dostačujícím způsobem, mohou se stát faktorem umožňujícím úspěšné převzetí celé domény.

Jakmile je doména plně kompromitována, je nutné považovat za kompromitované všechny hosty, doménové uživatelské účty, data, infrastrukturu i aplikace, které jsou na tuto doménu navázány. V tomto případě – a v mnoha dalších podobných – platí, že jakmile se útočník stane Domain Adminem, může velmi snadno stahovat data, nasadit ransomware, zašifrovat kritické systémy a následně organizaci vydírat.

# Ransomware lze porazit, jen když víte, kde jste ohroženi

Ransomware je jeden z nejprimitivnějších kyberútoků, přesto patří k nejúčinnějším a nejničivějším. Velmi efektivně dokáže na dlouhou dobu narušit provoz a může organizaci, jako je ta vaše, trvale vyřadit z provozu – zejména pokud odmítnete zaplatit výkupné. Jak tedy funguje ransomware řízený člověkem?

Nejprve si útočníci musí ve vaší síti vytvořit opěrný bod – kompromitovat nějaké zařízení a následně si po určitou dobu udržet vzdálený přístup k tomuto zařízení. Získání opěrného bodu často začíná jednoduchým phishingovým e-mailem, kdy zaměstnanec na něco klikne, útočníci zneužijí zranitelnost typu RCE ve veřejně dostupném systému, nebo využijí slabá či výchozí hesla u síťového zařízení vystaveného do internetu. Ať už k tomu dojde jakkoli, získání opěrného bodu je vždy první krok.

Útočníci se nemusí do systému „hacknout“ – jednoduše se přihlásí. Podle našich pozorování používají útoky založené na přihlašovacích údajích mnohem častěji než zneužívání známých CVE. Například v roce 2022,

> **NodeZero úspěšně provedl více než 6 000 útoků založených na přihlašovacích údajích v sítích zákazníků – bez zneužití jediné CVE.**

Poté, co získají opěrný bod, útočníci toto zařízení využijí jako odrazový můstek – vzdáleně ho ovládají, často přímo skrz vaše perimetrové firewally. Následně začnou budovat útočnou cestu vyhledáváním kritických systémů v síti, jako jsou doménové kontrolery, databázová úložiště, klíčové aplikace a podobně.

Jakmile útočníci tyto systémy najdou, využijí desítky možných metod k získání administrátorských oprávnění. Poté začnou odcizovat data, dokud nesplníte jejich požadavky, nebo nasadí tzv. Locker ransomware, který vám zablokuje přístup ke kritickým systémům. Útočníci mohou také použít crypto ransomware k zašifrování důležitých souborů a databází a dešifrovací klíč poskytnou až poté, co zaplatíte výkupné.

Zpráva CrowdStrike Global Threat Report 2023 ukazuje, že útočníci stále více spoléhají na odcizené přihlašovací údaje – v kriminálním podsvětí byl zaznamenán meziroční nárůst o 112 % v počtu inzerátů na služby tzv. access brokerů. Jinými slovy, útočníci získávají vzdálený přístup do sítí mnoha organizací a tento přístup následně prodávají ransomwarovým gangům.

**Příkladem je červnová zero-day zranitelnost MOVEit z roku 2023, kdy byl ransomwarový gang CLOP, známý také jako Lace Tempest, označen za aktéra, který zranitelnost původně zneužil a pak zveřejnil na své dark web leak stránce vyděračskou zprávu, ve které tvrdil, že disponuje informacemi o stovkách společností.**

Nejúčinnějším způsobem, jak čelit útokům založeným na ransomwaru, je průběžně posuzovat vlastní infrastrukturu, identifikovat útočné cesty, které by mohl útočník využít, tyto slabiny odstranit a následně ověřit, že provedená nápravná opatření skutečně zablokovala zjištěné útočné cesty. Po dokončení je nutné celý proces pravidelně opakovat, aby bylo možné odhalovat nové útočné scénáře. Žádná jiná obranná ani ofenzivní metoda snižování rizika ransomwaru nebude tak účinná jako postup popsaný zde.

# Potřeba průběžného posuzování rizik

Žádné dvě sítě nejsou stejné a s neustále rostoucím využíváním technologií a s tím, jak se ve výrobě technologie vyvíjejí a modernizují, často nejsou stejné ani dva dny. Výrobní podniky se navíc často stávají „oběťmi“ nejnovějších zařízení, senzorů, strojů, procesních technologií či výpočetních přístupů, protože musí integrovat zastaralé technologie s moderními – a výsledkem je řada neznámých, které zvyšují riziko.

V důsledku toho má dřívější posouzení kybernetických rizik z doby před rokem hodnotu pouze tehdy, pokud je stále aktuální. Jakmile se však v síti něco změní nebo do běžného procesu nasadíte novou technologii, přestává původní posouzení poskytovat úplný obraz o vašich rizicích. Přizvání konzultantů na několik dní k posouzení bezpečnostního stavu je bohužel jednorázová záležitost, která je nákladná, časově náročná a přináší jen malou návratnost investice.

Výrobní podniky nutně potřebují průběžně posuzovat rizika tak, aby se tento proces přizpůsoboval jejich růstu a inovacím. Jakmile se v jejich prostředí něco změní, mohou automaticky provést nové posouzení. Další posouzení dává smysl i při fluktuaci zaměstnanců. Pointa je, aby se posuzování stalo samozřejmostí – automatizovanou stejně jako výrobní procesy. Právě zde přináší hodnotu NodeZero.

# Benefity průběžného testování

Začlenění NodeZero do každodenních pracovních postupů prostřednictvím automatizace přináší jasné porozumění tomu, jaké je vaše vystavení riziku – a zároveň poskytuje srozumitelný podklad pro komunikaci a zapojení vedení. Budete schopni ukázat, jak organizaci chráníte, a obhájit investice do kybernetické bezpečnosti. A tato investice není přemrštěná – NodeZero stojí přibližně stejně jako jeden manuální, zúžený a jasně vymezený pentest. S NodeZero můžete své prostředí prověřovat každý den, klidně i opakovaně, bez dalších nákladů.

Přínosy průběžného testování eliminují neznámé a přinášejí jistotu, že se bezpečnost každý den zlepšuje. IT a bezpečnostní týmy už nebudou tápat v tom, kde jsou nejvíce ohroženy. Místo toho budou mít kdykoli k dispozici jasný obraz svého bezpečnostního stavu. Navíc – díky reportům, datovým bodům, trendům, analýzám a identifikovaným útočným cestám – pomůže NodeZero zefektivnit nápravná opatření v personálně poddimenzovaných IT odděleních, která mají zároveň na starosti i bezpečnost.

# Pět klíčových přínosů průběžného testování

Pochopení důvodů, proč průběžné testování bezpečnosti zlepšuje bezpečnostní stav, je zásadní. V kontextu tohoto přístupu jsou níže uvedeny očekávané výsledky a přínosy:

## 1 Snížení rizika

Můžete odhalovat, třídit a eliminovat nové útočné cesty, které vystavují vaši organizaci riziku úspěšného ransomware útoku. Při využití NodeZero, je pravidelné průběžné testování infrastruktury a náprava zjištěných problémů nejspolehlivějším a a skutečně účinným způsobem, jak snižovat kybernetické riziko.

## 2 Prevence drahých výpadků

Můžete zabránit nákladným odstávkám výroby, zamezit krádežím dat, snížit regulatorní sankce, a vyhnout se poškození reputace. Využitím nálezů a podrobných doporučení k nápravě od NodeZero, lze eliminovat nákladná šetření po bezpečnostním incidentu, při zachování provozu a výrobních požadavků.

## 3 Snížení ceny bezpečnosti

Můžete snížit náklady na bezpečnost a ušetřit cenné kapacity IT týmu. S NodeZero lze provádět průběžné penetrační testování bez nutnosti kupovat či instalovat hardware nebo agenty, a zároveň odpadá potřeba rušivých manuálních posouzení či najímání drahých externích pentesterů.

## 4 Zlepšení stavu bezpečnosti

Můžete zkrátit dobu nápravy díky kontextovému stanovení priorit, soustředit se na to, co je nejdůležitější a neplýtvat časem nevyužitelné zranitelnosti. každodenní provoz NodeZero zvyšuje úroveň zabezpečení, odhaluje systémové problémy a zajišťuje efektivní a dobře řízené bezpečnostní iniciativy.

## 5 Měření zlepšování bezpečnosti

Můžete získávat velmi podrobné reporty a trendová data, která prokazují pokrok a zlepšování vašeho programu bezpečnosti. Využití NodeZero ke sledování tohoto pokroku zajišťuje návratnost investice a zároveň dokládá, že dodržujete bezpečnostní osvědčené postupy, oborové standardy, doporučení i regulatorní požadavky.

 @Horizon3ai info@horizon3.ai www.horizon3.ai

HORIZON3.ai
~~TRUST BUT~~ VERIFY

# Povinné bezpečnostní prověrky již brzy

S ohledem na neustále se rozšiřující spektrum kybernetických hrozeb, nárůst finančně motivovaných útočníků a nedávné úspěšné ransomwarové útoky na dodavatelské řetězce je stále důležitější, aby výrobní podniky, státní a místní úřady, zdravotnictví, školství, finanční sektor, kritická infrastruktura i další odvětví braly zabezpečení svého kybernetického prostředí skutečně vážně.

Například v níže uvedených navrhovaných – nebo již platných – regulacích či doporučeních se opakovaně požaduje prověřování v oblasti bezpečnostních kompetencí vedení, kontinuity a odolnosti provozu a celkové kybernetické připravenosti. Vlády chápou, jak kritickou roli technologie hrají, a uznávají význam pravidelných prověrek.

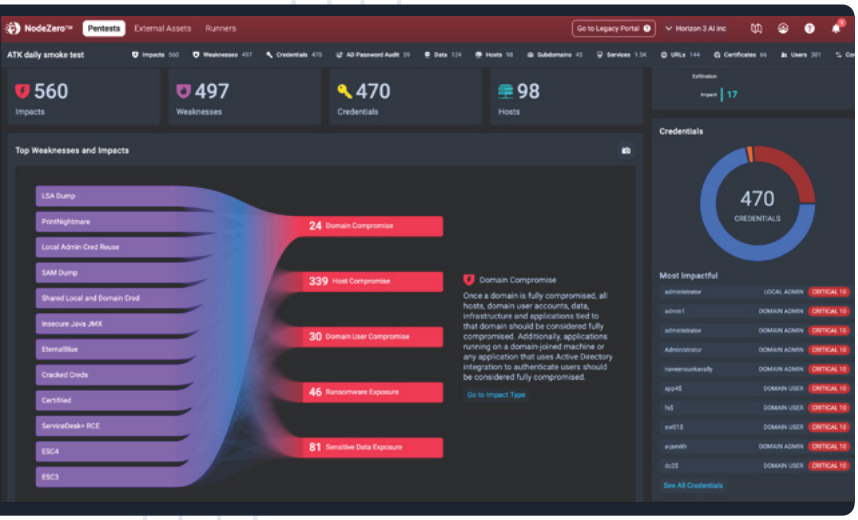
- SEC navrhuje pravilda pro řízení kybernetických rizik, strategii, správu a zveřejňování bezpečnostních incidentů u veřejně obchodovaných společností
- Nařízení o digitální provozní odolnosti (DORA) - nařízení (EU) 2022/2554
- Směrnice NIS2: vysoká společná úroveň kybernetické bezpečnosti v EU
- Ministerstvo obrany USA vydává finální pravidlo aktualizující postupy hodnocení systému řízení rizik výkonnosti dodavatelů (SPRS) pro federální dodavatele
- Zvláštní publikace NIST 800-171r2 - Ochrana řízených neklasifikovaných informací v nefederálních systémech a organizacích

Přestože existuje řada dalších odkazů na regulace a doporučení, hlavní sdělení je zřejmé. Pokud jste veřejně obchodovaný subjekt, spolupracujete s vládními institucemi nebo jste součástí kritické infrastruktury, budete muset provádět průběžné bezpečnostní prověrky a následně doložit aktuální (nikoli historickou) úroveň zabezpečení.

# Zjistěte více o přínosech NodeZero

Organizace, včetně výrobních podniků, které přijaly NodeZero jako součást procesu hodnocení rizik a začlenily jej do svých programů kybernetické bezpečnosti, zaznamenávají následující přínosy – a další navíc.

**Odstraňte rizika a ověřujte bezpečnost průběžným testováním.** Poskytuje důkazy o aktuální úrovni zabezpečení, zdůrazňuje účinná nápravná opatření, sleduje zlepšování v čase a vytváří reporty, kterým rozumějí analytici i auditoři.




**Zlepšete bezpečnostní výkonnost a přehled o úrovni rizik.** Poskytuje reporty, které vedení ocení, ověřuje, že rizika jsou identifikována, prioritizována a řešena, zároveň pomáhá obhájit investice a prokazuje jejich efektivitu.

**Odhalte útočné vektory dříve, než dojde k jejich zneužití, prostřednictvím snadno pochopitelných útočných cest.** Proaktivně identifikuje slabá místa, poskytuje vysokoúrovňový přehled o širších systémových problémech a ukazuje, jak je řešit na makroúrovni pro dlouhodobou kybernetickou odolnost.

**Získejte prioritizovaný seznam toho, co je nutné řešit nejurgentněji.** Eliminuje časově náročné falešné nálezy a zvyšuje kapacitu bezpečnostních a IT týmů bez ohledu na jejich úroveň odbornosti či celkovou velikost týmu.

**Provádějte prověrky na požádání.** Umožňuje týmům libovolně často – a dokonce i souběžně – vyhledávat problémy, opravovat je a ověřovat nápravu, bez dodatečných nákladů, a zároveň snižuje potřebu najímat externí penetrační testery.

To, co NodeZero každý den odhaluje v sítích podobných té vaší, potvrzuje to, co jsme vždy věděli. Abyste skutečně pochopili, co by se stalo, pokud by útočník získal opěrný bod ve vaší síti, je nutné průběžně útočit na vlastní prostředí stejným způsobem, jakým by postupoval útočník. NodeZero umožňuje organizacím všech velikostí bezpečně „útočit samy na sebe“ tak často, jak potřebují.

# Závěrečné poznámky

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Uvědomujeme si dilema, kterému čelí všichni výrobci. Aby bylo možné zefektivnit provoz, je nutné inovovat a využívat technologie naplno. Bez toho není možné obstát na globálním trhu. Zároveň však nikdy v minulosti nebyla hrozba ransomwaru a dalších kybernetických útoků vyšší než dnes.

Věříme, že byste měli mít možnost využívat veškeré dostupné technologie k zajištění svého úspěchu, a naším cílem je pomoci vám činit tak bezpečněji. **NodeZero snižuje riziko, zachovává kontinuitu provozu a naplňuje potřeby výrobních podniků všech velikostí.**

**Chcete-li si NodeZero vyzkoušet přímo ve svém výrobním prostředí, zaregistrujte se brzy k bezplatné zkušební verzi.**

https://sec4good.cz/kontakt

**Chcete-li zjistit, jak může NodeZero pomoci zabezpečit váš výrobní podnik, naplánujte si ještě dnes ukázkové demo.**

https://sec4good.cz/kontakt

Sec4good

  @Horizon3ai info@horizon3.ai www.horizon3.ai

HORIZON3.ai
~~TRUST BUT~~ VERIFY