HORIZON3.ai
~~TRUST~~ BUT VERIFY

NodeZero Tripwires™

Odhalte neoprávněný přístup nebo škodlivou aktivitu

Každá minuta, po kterou se útočník nepozorovaně pohybuje ve vaší síti, zvyšuje riziko finančních ztrát a poškození reputace.

NodeZero Tripwires™ využívá autonomní penetrační testování k posílení vašich procesů detekce hrozeb a reakce na incidenty:

- Rychle reagujte na indikátory aktivních hrozeb ve vysoce rizikových částech vašeho prostředí
- Automaticky nasazujte klamavé technologie na ověřených útočných cestách pro maximální účinek
- Integrujte upozornění na škodlivé aktivity do vašich stávajících procesů detekce hrozeb a reakcí na incidenty

Klamavá obrana jinak

NodeZero strategicky nasazuje návnady – například falešné soubory a falešné přihlašovací údaje – podél ověřených útočných cest ve vašem prostředí během autonomních penetračních testů.

Jak to funguje:

- U libovolného interního, externího, Phishing Impact nebo Rapid Response pentestu zvolíte možnost Tripwires, čímž dáte NodeZero svolení během testu rozmístit návnady.
- Během testu NodeZero nasazuje návnady pouze na aktivech, u nichž se prokáže, že jsou zneužitelná.
- Když dojde k aktivaci návnady, jste okamžitě upozorněni a obdržíte relevantní informace pro další reakci.

Automatické nasazení: Díky bezproblémové integraci s autonomním penetračním testováním NodeZero se návnady automaticky nasazují ve vysoce rizikových oblastech tam, kde to má největší smysl.

Upozornění v reálném čase: Když útočník interaguje s návnadou, okamžitě obdržíte upozornění s podrobnými informacemi o pokusu, umístění a možném dopadu.

Nízká míra falešných poplachů: Vysoce kvalitní signál zajišťuje, že upozornění jsou smysluplná a akceschopná, a minimalizuje výskyt falešně pozitivních hlášení.

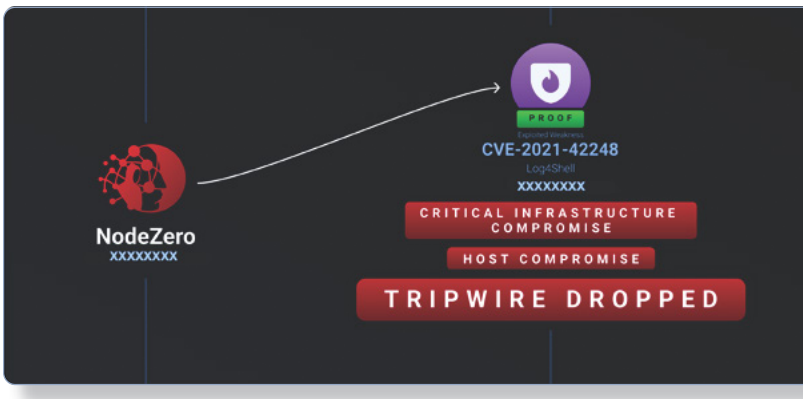
Různorodé typy tripwire: Nasaďte různé typy návnad pro detekci pokusů o neoprávněný přístup napříč různými útočnými vektory. Mezi podporované typy patří AWS API Key, Azure Login Certificate, mysqldump, Windows Suspicious Process Monitor a Kubeconfig.

Snadno použitelná správcovská konzole: Centralizovaný dashboard pro správu všech nasazených návnad a přehled historie upozornění. Jednoduché ovládání notifikací.

Integrace s bezpečnostními nástroji: Tripwires lze snadno integrovat se stávajícími SIEM systémy a dalšími bezpečnostními nástroji v rámci vašich procesů reakce na bezpečnostní incidenty.

Strategické, autonomní nasazování návnad

NodeZero Tripwires využívá jedinečnou schopnost NodeZero nahlížet na prostředí z perspektivy útočníka, aby zlepšil vaši bezpečnostní úroveň. Jak se NodeZero autonomně pohybuje vaším prostředím, NodeZero Tripwires automaticky nasazuje návnady na aktivech, u nichž je vysoká pravděpodobnost, že se stanou cílem útoku.



Příklady postupů

Detekce kompromitace přihlašovacích údajů

Tripwires slouží k detekci kompromitace přihlašovacích údajů napříč celou vaší digitální infrastrukturou. Příklad: Po získání přístupu na úrovni doménového admina se NodeZero přesunul do prostředí Azure Entra ID a kompromitoval účet globálního admina Azure. Během testu NodeZero strategicky umístil návnady typu Windows Suspicious Process Monitor a Azure Login Certificate na účty doménového admina, na stroje globálního admina Azure Entra ID a na další klíčové systémy obsahující citlivá data. NodeZero upozorní tým, když se útočník pokusí použít nastražené přihlašovací údaje nebo spustit monitorovaný proces.

Rozšiřte své phishingové simulace

Rozšiřte přínos testu Phishing Impact tím, že použijete Tripwires k odhalení, zda došlo ke kompromitaci přihlašovacích údajů náchylných k phishingu. Příklad: Během testu Phishing Impact NodeZero získá přihlašovací údaje náchylné k phishingu s administrátorskými oprávněními. Tyto údaje následně využije k nasazení návnad na sdílené síťové úložiště a rozmístí Azure přihlašovací klíče do více uživatelských adresářů, aby dokázal detekovat a upozornit vás na škodlivou aktivitu.

Detekujte hrozby u nových zranitelností

Chraňte svou organizaci v časově kritickém okně mezi identifikací nové hrozby a dostupností bezpečnostní aktualizace. Příklad: Během pentestu Rapid Response NodeZero identifikuje host, který lze kompromitovat pomocí nové zranitelnosti. NodeZero vás okamžitě upozorní, že je vaše organizace touto hrozbou zasažena, a zároveň na daném místě nasadí návnadu. Ještě před dokončením pentestu je váš tým upozorněn ve chvíli, kdy se útočník pokusí spustit proces, který naznačuje škodlivý úmysl. Včasné varování doplněné relevantními detaily vám umožní eskalovat odpovídající reakci právě v tom kritickém časovém okně, které útočníci typicky využívají.