HORIZON3.ai
~~TRUST BUT~~ VERIFY

Pentest Cloudu s NodeZero

Bezkonkurenční možnosti testování pro cloudová a hybridní prostředí

NodeZero™ platforma poskytuje autonomní penetrační testy z různých perspektiv pro organizace s cloudovou nebo hybridní cloudovou infrastrukturou. Komplexní přístup zajišťuje konzistentní ověřování bezpečnostních politik a hodnocení rizik napříč celým cloudovým stackem.

NodeZero lze nasadit jak z perspektivy interního, tak externího útočníka, aby důkladně otestoval cloudové bezpečnostní kontroly v kontextu celé vaší digitální infrastruktury, nebo se cíleně zaměřil na útočné plochy spojené s identitami v Amazon Web Services (AWS) či Microsoft Azure Entra ID.

Zde NodeZero využívá privilegovanou perspektivu k hlubší analýze prostředí AWS.

Interní Pentest: Nejkomplexnější autonomní penetrační test NodeZero poskytuje ucelený pohled na to, jak mohou útočníci řetězit zranitelnosti napříč celou digitální infrastrukturou, identifikovat komplexní útočné cesty a provádět pivotování mezi on-premise a cloudovými prostředími.

Externí Pentest: Podobný jako interní test, avšak spouštěný z infrastruktury Horizon3.ai za účelem ověření bezpečnosti veřejně dostupných systémů.

AWS Pentest: Využívá AWS CloudFormation k získání privilegované perspektivy a identifikuje zneužitelné zranitelnosti, slabé bezpečnostní kontroly, nezabezpečené IAM politiky a nadměrně vystavená aktiva.

Azure Entra ID Pentest: Zaměřuje se na zabezpečení Azure IAM (Entra ID) z privilegované perspektivy, testuje odolnost vůči nativním útokům v Azure a ověřuje bezpečnost aplikací a služeb využívajících identity Microsoft Entra.

Používejte NodeZero k pravidelnému testování cloudových bezpečnostních kontrol z různých perspektiv:

1 **Interní a externí testování:** NodeZero nasazuje testy buď z interního, nebo externího pohledu, aby ukázal, jak by útočník mohl řetězit zranitelnosti a chybné konfigurace napříč různými prostředími. Tím ověřuje účinnost bezpečnostních řešení a zároveň odhaluje souvislosti mezi zdánlivě nesouvisejícími aktivy, které mohou vést k eskalaci oprávnění a odhalení skrytých útočných cest.

2 **Testování z privilegované perspektivy:** Se zaměřením na konkrétní cloudové poskytovatele využívá NodeZero privilegovanou perspektivu k hlubší analýze prostředí AWS nebo Azure. Tento přístup odhaluje další zranitelnosti, upozorňuje na nadměrně vystavená či chybně nakonfigurovaná aktiva a přesně identifikuje zneužitelné IAM politiky umožňující eskalaci oprávnění. Tyto testy ověřují vícevrstvou obranu, snižují potenciální dopad incidentu a pomáhají čelit interním hrozbám i útokům založeným na kompromitovaných přihlašovacích údajích.

Zde NodeZero z privilegované perspektivy prokazuje, že kombinace komplexního Azure-native útoku a slabých kontrol umožní eskalaci až na úroveň globálního administrátora Entra ID.

Tyto možnosti poskytuje architektura NodeZero, navržená pro škálování, rychlost a komplexní pokrytí cloudových i on-prem prostředí. NodeZero nabízí řadu funkcí, které umožňují nahradit pracné bezpečnostní činnosti proaktivním a autonomním přístupem – od ověření jedním kliknutím až po orchestraci souběžných a rozsáhlých pentestů ve víceklientském prostředí.