RelNethic szolgáltatás

A RelNet behatolás-tesztelés szolgáltatása:

A szolgáltatás egy átfogó belső behatolás-teszt a Pentera speciális szoftvereszközével. A validáció során a Pentera szoftver ellenőrzi az infrastruktúra, szerverek, munkaállomások és hálózati eszközök biztonságát, emellett elvégzi az Active Directory validációját is. A teszt eredménye egy átfogó jelentés, amely prezentálja a tesz során feltárt sebezhetőségeket, hiányosságokat és egyéb megállapításokat, a hozzájuk tartozó korrekciós intézkedésekre vonatkozó ajánlásokkal. A teszt végeredményeként generált jelentés vizuálisan megmutatja hogyan épülnek egymásra a feltárt sérülékenységek, emellett a kihasználhatóság tükrében is priorizálja azokat.

A RelNet szolgáltatása és a NIS 2 megfelelés

A NIS2 irányelvre való felkészülés egyik első lépése a szervezet biztonsági állapotának felmérése. A RelNet szolgáltatásának igénybevételével egy szervezet pontos képet kaphat a rendszere valós védelmi állapotáról, így **a „megfelelőségi önértékelés" is pontosabban elvégezhető.**
Az állapotfelmérés mellett **a behatolás-teszt megmutatja, mely területeken szükséges erősíteni a védelmi szintet,** a kiberbiztonsági tanúsítás releváns **megbízhatósági szintjének megfelelően.**

A Pentera Megoldása:

A Pentera platform egy automatizált behatolás-tesztet végrehajtó megoldás, amely segít a szervezeteknek valós időben feltárni a valós biztonsági kockázataikat. Mindezt úgy teszi, hogy biztonságos etikus támadásokat futtat le az infrastruktúra minden kiberbiztonsági rétegén, kockázatkezelési ütemtervet kínálva az IT-szakembereknek. A Pentera fejlett algoritmusokat használ a hálózatok átvilágításához és az etikus támadásához, amelyhez a legújabb hackertaktikákat és -technikákat veszi alapul. A szoftver a teszt folyamat során megpróbál a teljes hálózaton átívelő támadási vektorokat, úgynevezett „kill chain"-eket felderíteni, amiken keresztül a hackerek bejuthatnak és kárt tehetnek a hálózatunkban.
Az automatizált biztonsági validáció a valódi sérülékenységekre összpontosít, és elősegíti azok költséghatékony kezelését. A validáció által szolgáltatott adatok a fenyegetéseknek az üzletmenetre mért tényleges hatását jelzik, és ezen friss adatok birtokában a szakemberek tűpontos biztonsági műveleteket képesek végrehajtani.

A Pentera megoldása a következő előnyöket nyújtja:

Mélyreható hálózatbiztonsági validációt biztosít

A Pentera megoldása segít feltérképezni a belső támadási felületeket és átvilágítani a belső hálózat minden szegletét. Segítségével információk gyűjthetők a felhasználókról, hostokról, hálózatokról, annak elsődleges szervereiről és az alkalmazások konfigurációjáról.

Safe-by-Design

A Pentera automatizált tesztelési megoldása teljes mértékben úgy lett kialakítva, hogy semmiképpen se befolyásolja negatívan az üzletmenet folyamatosságát és az eszközöket. **Nem felhőalapú, minden tesztelési művelet helyben történik, alapértelmezetten külső hálózati/internet kapcsolat nélkül.**

Priorizálja a fenyegetettségek elhárításának sorrendjét

A Pentera megoldása a teszt folyamán feltár a teljes hálózaton átívelő támadási vektorokat és pontosan meghatározza azok kiváltó okát, majd rangsorolja a sérülékenységek javítására tett lépéseket.

Szabványosított átvilágítást biztosít

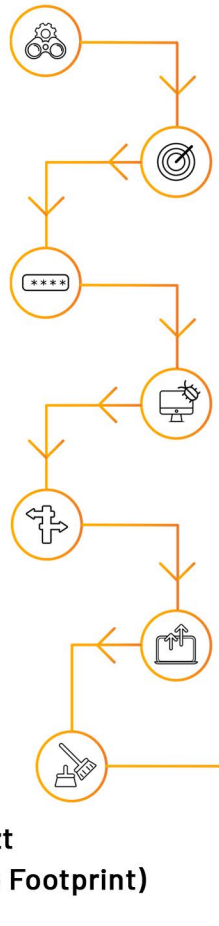
A Pentera minden tesztelési riportja szerkezeti és tartalmi értelemben is konzisztens, sztenderdizált eredményt biztosít az ügyfelek számára.

Iparági normáknak való megfelelés

A Pentera által vizsgált támadási vektorok a mindenkori iparági normákra épülnek, beleértve a MITRE-t, a CVE-ket, a NIST-et, a CISA-t és az általános kiberközösségi fórumokat.

A TESZTFOLYAMAT LEÍRÁSA

A szervezet teljes támadási felületének feltérképezése



Sebezhetőségi vizsgálat lefuttatása

Az összegyűjtött hitelesítési adatok ellenőrzése

Végpontok ellenállóképességének tesztelése biztonságos, hatástalanított malware-ek bejuttatásával

Lateral movement - hálózati szegmensek közötti átjárhatóság tesztelése oldalirányú mozgással

Adatok kiszivárogtathatóságának megállapítása, az adatszivárgás elleni védelem ellenőrzése

Clean up, Takarítás – A tesztelés végeztével a Pentera megtisztítja a vizsgált hálózatotunk azoktól az adatoktól és kódoktól, amiket a teszt folyamán juttatott a hálózatba (Zero Footprint)

A fenyegetettségek elhárítási lépéseinek priorizálása és jelentés készítése a teszt eredményekről

A szolgáltatás keretében elérhető teszt forgatókönyvek:

Alap tesztforgatókönyvek:

Automatizált Black Box teszt - A behatolásvizsgálat nem igényel hitelesítő adatokat. A teszt célja, hogy bármilyen előzetes információ nélkül felderítse legkritikusabb kihasználható sebezhetőségeket hálózatunkban lévő eszközökön.

Automatizált What-If/Gray Box teszt - Célja, hogy fókuszáltabb terjedelmű tesztelési forgatókönyveket futtasson egy előre meghatározott kiindulópontból feltételezett betörési lehetőségeket követve. Célja a belső, infrastruktúrán belüli fenyegetések és támadások utánzása. E tesztforgatókönyvnél meghatározhatók a támadás kiindulópontja, például, hogy a támadó már megszerezte a hozzáférést egy szerverhez, emellett definiálható egy végcél is, például bizonyos fájlok megszerzése.

Targeted test - Automatizált célzott teszt - Előre meghatározott tesztelési forgatókönyvek és támadási vektorok segítségével célzott behatolás-tesztek is végezhetők. E tesztforgatókönyv célja, hogy előre meghatározott támadási vektorok, illetve támadási technikák milyen veszélyeket jelenthetnek hálózatunkra.

Opcionális teszt forgatókönyvek:

Ransomware támadások emulációja - A ransomware emulációs tesztelés ellenőrzi a szervezet hálózatát a legnépszerűbb zsarolóvírus-támadások vonatkozásában. A RelNet szolgáltatásának keretében elérhető Pentera RansomwareReady technológia, aminek támadásokat emuláló teszt forgatókönyve segít a szervezeteknek ellenőrizni ellenállóképességüket a ma ismert, legveszélyesebb zsarolóvírus-támadásokkal szemben. A szolgáltatás keretében zajló teszt a ma már jól ismert zsarolóvírus-kampányok végponttól végpontig terjedő támadási folyamatait emulálja és ellenőrzi biztonsági intézkedéseket.

Active Directory jelszó erősség értékelés - A felhasználói könyvtárba található jelszavak erősségének ellenőrzése és értékelésére szolgál. Ez a tesztelési forgatókönyv egy emelt szintű jogosultságokkal rendelkező felhasználói fiókot használ a teljes jelszóadatbázis megszerzésére és egy offline jelszófeltörési teszt elvégzésre. Ez a teszt olyan fiókokat tár fel, amelyek jelszavai megfelelnek a szervezet biztonsági szabályzatának, de a hackerek mégis nagy eséllyel feltörhetik őket.

BEVEZETÉSI AKCIÓ: A RelNet egy korlátozott idejű bevezetési akció keretében a 2024.06.30-ig beérkező rendelések mellé ajándékba szolgáltatja az ügyfeleknek egy szabadon választott opcionális tesztforgatókönyv lefuttatását bármely szabadon választott alap tesztforgatókönyv mellé.

RelNet technológia

https://relnet.hu
+36(1)4848300
kereskedelem@relnet.hu