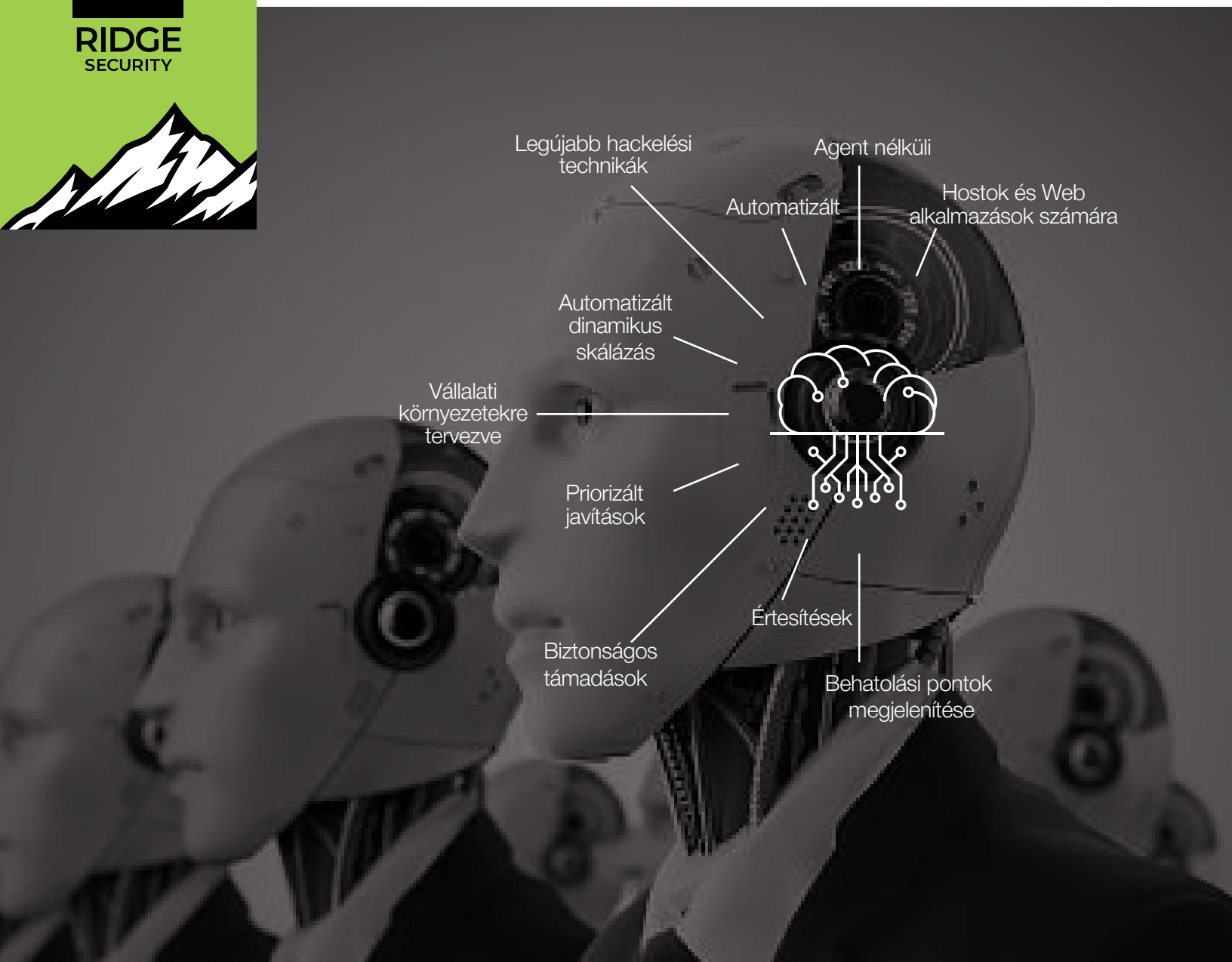
RidgeBOT penetrációs teszt elérhető áron

RIDGE SECURITY

RidgeBOT

Vállalati szintű automatizált penetrációs tesztelési megoldás, intelligens validáló robotokkal



A **RidgeBOT** automatizálja a teljes etikus hackelési folyamatot

100x gyorsabb mint a humán tesztelés

A **RidgeSecurity RidgeBOT** alkalmazása intelligens biztonsági validáló robot segítségével forradalmasítja a folyamatokat. A legmodernebb hackelési technikákkal felszerelt RidgeBOT széleskörű ismerettel rendelkezik a fenyegetések és sérülékenységek terén. A RidgeBOT, mint egy valódi etikus támadó, felkutatja és dokumentálja a feltárt sebezhetőségeket. A penetrációs tesztelés automatizálása költséghatékonyságot, továbbá széleskörű és hatékony tesztelést nyújt. A meghatározott kereteken belül a RidgeBOT azonnal alkalmazkodik és kezeli a rendkívül összetett rendszereket is.

A RidgeSecurity lehetővé teszi a vállalatok, webalkalmazás-fejlesztő csapatok, DevOps-ok, ISV-k, kormányzatok, egészségügyi intézmények, oktatási intézmények és bárki számára, aki felelős a szoftverbiztonság biztosításáért, hogy költséghatékonyan és eredményesen teszteljék rendszereiket.

Kihívások

A legtöbb szervezet biztonsági tesztelést (más néven penetrációs tesztelést) alkalmaz a hálózatuk és rendszereik biztonsági helyzetének validálására. Egy ilyen teszt során a biztonsági tesztelők a hacker szerepét veszik fel, és megpróbálnak behatolni a szervezet informatikai környezetébe, hogy felfedezzék a sérülékenységeket és meghatározzák, hogyan lehetne kihasználni őket egy valós hacker támadás során. Az alapgondolat az, hogy egy jó biztonsági tesztnek fel kell tárnia, hogyan juthatna be egy támadó a szervezet rendszereibe, mielőtt az ténylegesen megtörténne. A megfelelő penetrációs tesztelés segít a szervezeteknek a problémák kezelhetőbb és költséghatékonyabb módon történő megoldásában.

Azonban a támadók folyamatosan új sebezhetőséget és támadási módszereket fejlesztenek, gyakran gépi tanulást használva az automatikus támadások végrehajtására. A vállalati biztonsági csapatok és a szakmai "penetrációs tesztelők" hatalmas nyomás alatt állnak, hogy lépést tartsanak ezzel.

RidgeBOT megoldás és előnyök

A RidgeBOT automatizált biztonsági validálási szolgáltatásokat kínál. Segít a biztonsági tesztelőknek a tudásbeli és tapasztalati korlátok leküzdésében, és mindig egyenletes, magas szinten végzi el a teszteléseket. A manuális, munkaigényes tesztelésről a gép által segített automatizálásra való áttérés enyhíti a biztonsági szakemberek súlyos hiányát. Lehetővé teszi, hogy az emberi biztonsági szakértők megszabaduljanak a napi, munkaigényes feladatoktól, és több energiát fordíthassanak az új fenyegetések és új technológiák kutatására.

- Javítja a biztonsági tesztelés lefedettségét és hatékonyságát
- Csökkenti a biztonsági validálás költségeit
- Folyamatosan védi az IT környezetet
- Hasznos és megbízható eredményeket nyújt különböző érintettek számára

A RidgeBOT az automatizált penetrációs tesztelést minden szervezet számára elérhetővé teszi.

RidgeBOT funkciói

Egy adott feladat során a RidgeBOT automatizálja a teljes etikus hackelési folyamatot. Amikor csatlakozik egy szervezet IT környezetéhez, a RidgeBOT automatikusan felfedezi a hálózaton lévő különböző típusú eszközöket, majd a sérülékenységekről szóló tudásbázis segítségével átvizsgálja a célrendszert. Miután a RidgeBOT azonosítja a sérülékenységeket, beépített hackelési technikákat és exploit kódokat használ, hogy valós etikus támadást indítson a sérülékenység ellen. Ha a támadás sikeres, a sérülékenységet validálja, és az egész támadási lánc tranzakcióját dokumentálja.

A RidgeBOT számos analitikai eszközt biztosít a kockázatértékeléshez és priorizáláshoz, átfogó jelentést nyújt javítási javaslatokkal, és eszközöket kínál a javítások ellenőrzésére.

Eszköz feltárás—Intelligens pásztázó technológia és ujjlenyomat algoritmusok segítségével fedezi fel az IT eszköztípusokat: IP címeket, domaineket, hostokat, operációs rendszereket, alkalmazásokat, weboldalakat, bővítményeket és hálózati eszközöket.

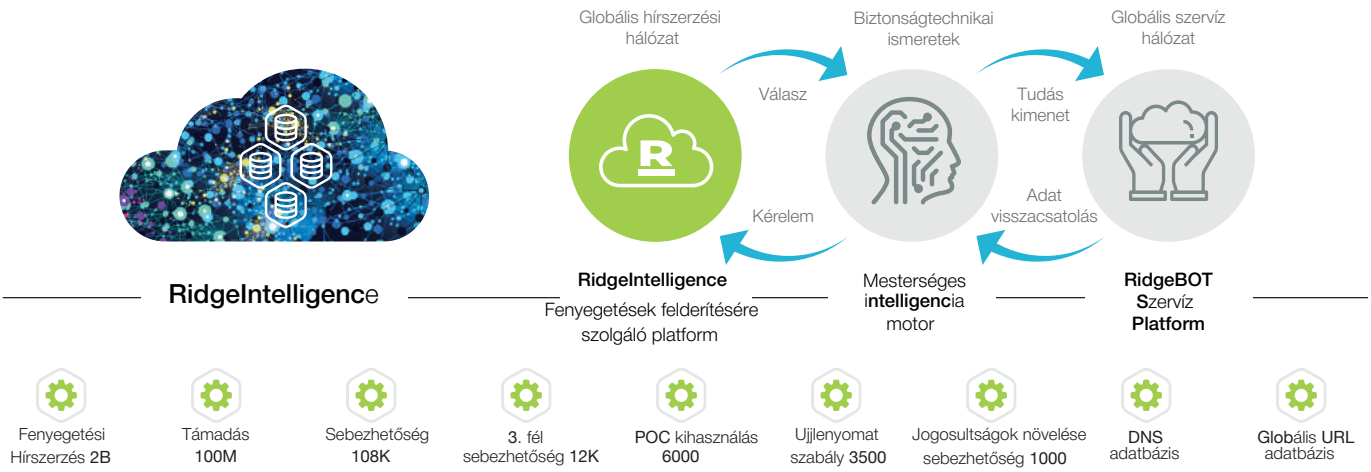
Sérülékenység keresés — A saját fejlesztésű, szabadalmaztatott szkennelőeszközökkel, a sebezhetőségek és a biztonsági résekkel kapcsolatos események széleskörű tudásbázisával, valamint különböző kockázati modellek felhasználásával.

Sebezhetőség kihasználása—Egy intelligens homokozó használatával valós támadások szimulálhatók különböző eszközkészletekkel, melynek segítségével még több adat gyűjthető egy további támadáshoz a betörés utáni szakaszban.

Kockázati prioritás — Automatikusan létrehoz egy elemző nézetet, vizualizálja a támadási láncot és megjeleníti a támadó szkriptjét. Megmutatja a hackelés eredményeként megszerzett érzékeny adatokat és emelt szintű jogosultságokat.

Nagyobb precizitás és még több felfedezés az AI segítségével

A RidgeBOT egy erőteljes, mesterséges intelligencia algoritmusokat és szakértői tudásbázist tartalmazó „agyat” használ, melyek segítik a támadási útvonalak keresésében és kiválasztásában. Iteratív támadásokat indít a tanultak alapján, ezáltal átfogóbb tesztlefedettséget és mélyebb vizsgálatot biztosít.

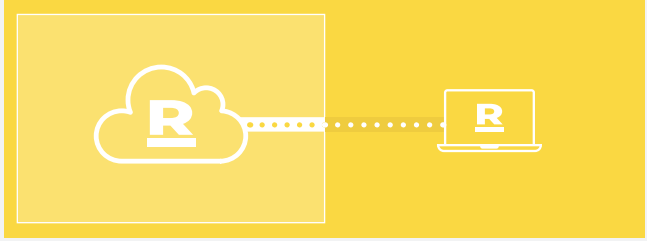


Telepítési lehetőségek

On-Premise Modell

Vállalati környezethez — a RidgeBOT telepíthető fizikai és virtuális szerverekre is egyaránt. Ez a konfiguráció biztosítja a legmagasabb teljesítményt a legalacsonyabb összköltséggel (TOC).

VPN-alapú szerviz



Ad hoc penetrációs teszteléshez VPN-alapú szolgáltatást ajánlunk. Vegye fel velünk a kapcsolatot további információkért.

On-Premise **rendszerkövetelmények**

Helyszíni telepítéshez a RidgeBOT szoftvercsomagot meghatározott fizikai szervereken vagy virtuális gépeken kell telepíteni. A RidgeBOT szoftvercsomag tartalmazza a RidgeIntelligence platformot, a RidgeBrain motort és a RidgeBOT bővítményeket. A szoftverfrissítéseket szolgáltatások biztosítják. A helyszíni telepítés olyan szervezetek számára ajánlott, melyek teljes körű irányítást kívánnak gyakorolni a tesztelési eljárások, az eredmények és az érintett érzékeny adatok felett.

Telepítés fizikai szerverre	**Essential**	**Advanced**
Minimális hardver követelmény	• Intel Xeon CPU legalább 4 magos • 32 GB RAM • 1TB HDD • 2 Ethernet interfész	• Dual Intel Xeon CPUs legalább 6 magos egyenként • 64 GB RAM • 2 X 4TB HDD RAID vezérlővel (RAID 1) • 2 Ethernet interfész
Referencia platformok	Dell PowerEdge, Lenovo ThinkSystem, HP ProLiant	
Egyszerre futó botok száma	16	32

Virtuális gépek telepítése	**Teszt környezet**	**Éles rendszer**
Minimális hardver követelmény	• 8 vCPU • 16 GB RAM • 100 GB tárhely • 2 Ethernet interfész	• 8 vCPU • 32 GB RAM • 100 GB tárhely • 2 Ethernet interfész
Egyszerre futó botok száma	8	16
Támogatott Hypervisorok	• VMware Workstation 15 Pro vagy magasabb verzió • VMware Fusion 11 Pro vagy magasabb verzió • VMware ESXi 5.0 vagy magasabb verzió • Oracle VirtualBox 6.0 vagy magasabb verzió	

RidgeSecurity

A RidgeSecurity a RidgeBOT, egy intelligens biztonsági validációs robot segítségével forradalmasítja a biztonsági tesztelést. A RidgeBOT-ot olyan technikák alapján fejlesztették, melyeket hackerek használnak a rendszerek feltörésére. A telepítés után minden RidgeBOT rendíthetetlenül keresi, kihasználja és dokumentálja az általa talált sebezhetőségeket. Meghatározott kereteken belül dolgoznak, és azonnal képesek replikálódni, hogy a rendkívül összetett struktúrákat is kezelni tudják. A RidgeSecurity lehetővé teszi a vállalatok és webalkalmazások csapatai, független szoftverszállítók, ISV-k, DevOps-ok, kormányzatok, oktatási intézmények és bárki számára, aki felelős a szoftverbiztonság biztosításáért, hogy költséghatékonyan és eredményesen teszteljék rendszereiket.

Az Ön magyarországi partnere:

Nádor Rendszerház Kft.

Cím: 1152 Budapest, Telek u. 7-9

E-mail: info@nador.hu I Web: www.nador.hu

Telefon: +36 1 470-5000