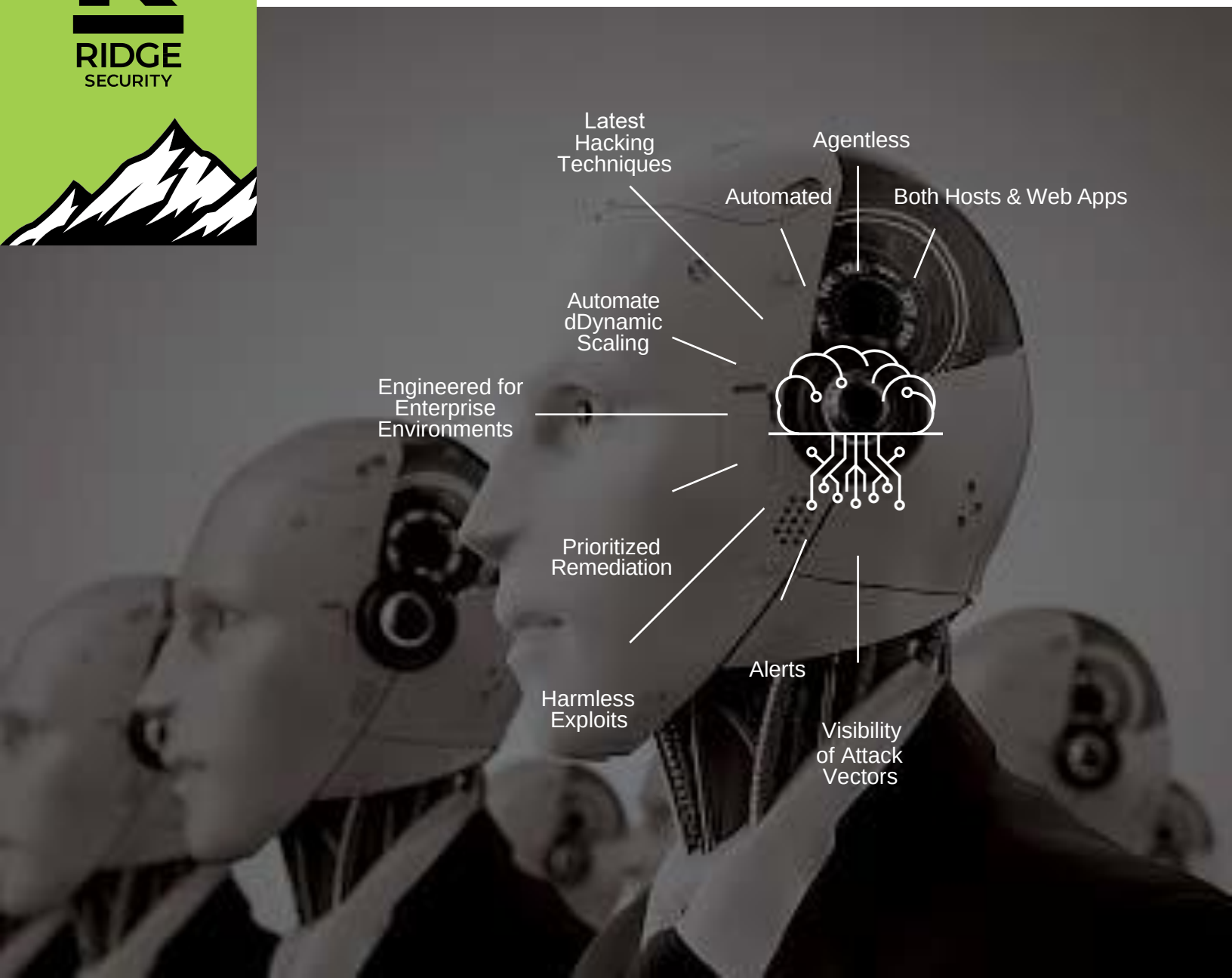
Automatyczna Walidacja Bezpieczeństwa Przedsiębiorstwa

RidgeBot®

RIDGE SECURITY



RidgeBot® automatyzuje proces walidacji bezpieczeństwa 100x szybciej niż człowiek

Ridge Security zmienia reguły gry dzięki RidgeBotowi® , inteligentnemu robotowi sprawdzającemu bezpieczeństwo infrastruktury zewnętrznej i wewnętrznej. Zunifikowany z najnowszymi etycznymi technikami hakerskimi, RidgeBot® pomaga przedsiębiorstwom zweryfikować ekspozycję na ryzyko zewnętrzne i wewnętrzne kontrole bezpieczeństwa. RidgeBot® ma zbiorową wiedzę na temat zagrożeń, słabych punktów, eksploitów, taktyk i technik atakującego. Zachowując się jak doświadczony etyczny atakujący, RidgeBot® nieustannie lokalizuje i dokumentuje luki w zabezpieczeniach, wskazując błędy kontroli bezpieczeństwa. Automatyzacja sprawdzania poprawności zabezpieczeń przedsiębiorstwa sprawia, że jest to niedrogie rozwiązanie z możliwością działania na duża skalę. Działając w określonym zakresie, RidgeBot natychmiast replikuje się aby zająć się bardzo złożonymi strukturami. Ridge Security umożliwia przedsiębiorstwom, zespołom ds. Aplikacji internetowych, DevOps, dostawcą oprogramowania, rządom – wszystkim odpowiedzialnym za zapewnienie bezpieczeństwa infrastruktury oraz aplikacji webowych – niedrogie i wydane testowanie ich systemów.

Wyzwania

Dzisiejsze organizacje stoją w obliczu wyzwań związanych z bezpieczeństwem cybernetycznym z wielu punktów widzenia. Zespoły ds. bezpieczeństwa muszą nie tylko weryfikować, czy infrastruktura IT nie zawiera luk, które mogłyby zostać wykorzystane przez hakera lub oprogramowanie ransomware do naruszenia bezpieczeństwa danych o znaczeniu krytycznym, ale także muszą weryfikować, czy wdrożone drogie rozwiązania w zakresie cyberobrony mogą działać zgodnie z oczekiwaniami w zakresie wykrywania i ograniczania zagrożeń najbardziej aktualne techniki ataków wykorzystywane przez zaawansowane trwałe zagrożenia (APT) i inne złośliwe podmioty.

Cyberataki są coraz bardziej wyrafinowane i stale rosną, hakerzy opracowują nowe exploity i metody ataków co miesiąc, często używając narzędzi do automatycznego przeprowadzania ataków. W odpowiedzi na zagrożenia bezpieczeństwa cybernetycznego większość organizacji stosuje testy bezpieczeństwa (tzw. testy penetracyjne) swoich systemów komputerowych, stron internetowych, aplikacji i sieci, próbując znaleźć zagrożenia, zanim zrobi to haker. Podczas gdy wewnętrzna wiedza zespołów ds. bezpieczeństwa w zakresie testowania za pomocą pióra jest ograniczona i kosztowna, nie stać ich na ciągłą weryfikację bezpieczeństwa. Wiele organizacji szuka zautomatyzowanego systemu testów penetracyjnych, aby sprostać temu wyzwaniu w łatwiejszy w zarządzaniu i ekonomiczny sposób.

Rozwiązanie i kluczowe korzyści

RidgeBot® to zunifikowany system, który automatyzuje proces testów penetracyjnych i emuluje ataki przeciwników w celu sprawdzenia stanu cyberbezpieczeństwa organizacji. Zapewnia jaśniejszy obraz twoich luk w zabezpieczeniach i zamyka okna możliwości dla złośliwych atakujących poprzez zwiększenie częstotliwości testów penetracyjnych, zarządzanie lukami w zabezpieczeniach oparte na ryzyku i szkolenie zespołu obrony za pomocą skutecznych ćwiczeń. RidgeBot® pomaga zespołowi ds. bezpieczeństwa w pokonywaniu ograniczeń i zawsze działa na niezmiennie najwyższym poziomie. Przejście od manualnych, pracochłonnych testów do automatyzacji wspomaganej maszynowo łagodzi obecny poważny niedobór specjalistów ds. bezpieczeństwa. Pozwala ekspertom ds. bezpieczeństwa przenieść zaangażowanie ze żmudnych ciągłych testów do poświęcenia energii na usprawnienia infrastruktury bądź analizę nowych zagrożeń czy technologii.

- Popraw zasięg i wydajność testów bezpieczeństwa
- Stale chroń infrastrukturę IT
- Twórz praktyczne i wiarygodne scenariusze dla różnych interesariuszy

RidgeBot® Zapewnia 360-stopniową weryfikację bezpieczeństwa

greeneris

Greeneris Sp. z o.o. | ul. W. Korfantego 5, 01-496 Warszawa
+48 22 439 03 20 | biuro@greeneris.com |www.greeneris.com

RidgeBot® Funkcjonalność

Automatyczne testy penetracyjne

W ramach danego zadania RidgeBot® automatyzuje cały proces etycznego hakowania. Kiedy łączy się ze środowiskiem IT organizacji, RidgeBot® automatycznie wykrywa wszystkie rodzaje zasobów w sieci, a następnie wykorzystuje zbiorczą bazę danych o lukach w zabezpieczeniach do eksploracji obszarów ataków docelowego systemu. Gdy RidgeBot® zidentyfikuje luki w zabezpieczeniach, wykorzystuje wbudowane techniki hakerskie i biblioteki exploitów, aby przeprowadzić prawdziwy etyczny atak na lukę. Jeśli się powiedzie, luka jest weryfikowana, a cała transakcja typu kill-chain jest dokumentowana. RidgeBot® zapewnia analizę ryzyka do oceny ryzyka i ustalania priorytetów, eksportując kompleksowy raport z poradami dotyczącymi środków zaradczych, udostępniając narzędzia do weryfikacji poprawek.

Profilowanie aktywów— Opierając się na inteligentnych technikach indeksowania i algorytmach odcisków palców, odkrywaj szerokie typy zasobów IT: adresy IP, domeny, hosty, system operacyjny, aplikacje, strony internetowe, bazy danych i urządzenia sieciowe/OT.

Eksploracja luk w zabezpieczeniach — Wykorzystując narzędzia do skanowania, naszą bogatą bazę wiedzy na temat luk w zabezpieczeniach i zdarzeń związanych z naruszeniami bezpieczeństwa, a także różne modelowanie ryzyka.

Wykorzystanie luki w zabezpieczeniach — Korzystaj z technologii wielowątkowej, aby symulować ataki w świecie rzeczywistym za pomocą zestawów narzędzi. Zbierz więcej danych do dalszego ataku na etapie po włamaniu.

Priorytetyzacja ryzyka — Automatycznie twórz widok analityczny, wizualizuj kill chain i wyświetlaj skrypt hakera. Pokaż wyniki hakowania, takie jak dane i eskalowane uprawnienia ze zhakowanych obiektów.

Cyberemulacja przeciwnika (ACE)

Kontrole bezpieczeństwa IT to mechanizmy stosowane w celu zapobiegania, wykrywania i łagodzenia cyberzagrożeń i ataków. RidgeBot® ACE emuluje przeciwnika, naśladując prawdopodobne ścieżki i techniki ataku, aby generować ciągłe dane oceny, które pomagają zidentyfikować awarie kontroli bezpieczeństwa, rozwiązać słabości strukturalne i umożliwić optymalizację kontroli bezpieczeństwa. RidgeBot® ACE dostosował się do struktury MITRE ATT&CK i mapuje swoje skrypty testów oceniających do taktyk i technik MITRE ATT&CK. Zwiększa to widoczność potencjalnych wektorów ataków i poprawia komunikację pomiarów kontroli bezpieczeństwa.

Zarządzanie aktywami

Zarządzanie zasobami RidgeBot® zapewnia scentralizowane repozytorium do zarządzania zasobami informatycznymi przedsiębiorstwa w celu weryfikacji bezpieczeństwa, w tym adresów IP zasobów, nazw hostów, wersji systemu operacyjnego, otwartych portów usług, aktywnych aplikacji z wersjami aplikacji, a także nazw domen witryn internetowych, rozpoznawania DNS i wersje serwera WWW.

Większa precyzja i więcej odkryć dzięki AI Brain

RidgeBot® ma potężny „mózg”, który zawiera sztuczną inteligencję i bazę wiedzy eksperckiej, która pomaga RidgeBot® w znajdowaniu/wybieraniu ścieżki ataku. Uruchamia ataki iteracyjne w oparciu o wiedzę zdobytą na ścieżce, osiągając pełniejszy zakres testów i głębszą inspekcję.

RidgeBot® wdrożenie

On-Premise

Dla środowiska korporacyjnego — wdróż RidgeBot® w siedzibie klienta, zapewnij mniejsze ryzyko wycieku danych Infosec.

Cloud

Dla klientów Cloud i SMB — wdrażaj RidgeBot® w chmurze (AWS EC2, Microsoft Azure i Google Cloud), uzyskaj większą elastyczność przy jednoczesnym zminimalizowaniu początkowej inwestycji CapEx.

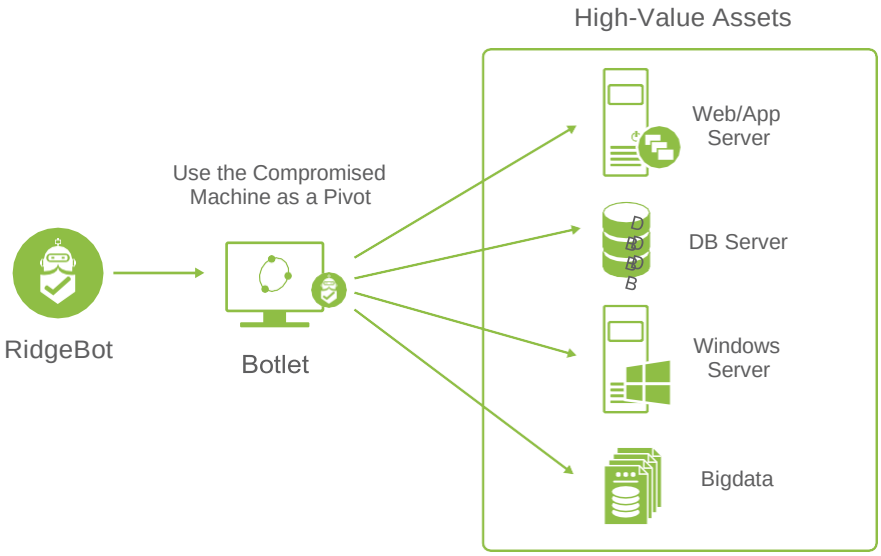
Scenariusze testów penetracyjnych

Atak wewnętrzny. Przeprowadzaj ataki z wnętrza sieci Enterprise za zgodą klienta, koncentrując się na wykorzystaniu luk wykrytych w lokalnej sieci i systemach.

Atak zewnętrzny. Przeprowadzaj ataki spoza sieci korporacyjnej na publicznie dostępne zasoby, takie jak strony internetowe organizacji, udziały plików lub usługi hostowane w chmurze publicznej/CDN.

Ruch boczny. Zwiększ uprawnienia do przejętego zasobu i wykorzystaj przejęty zasób jako punkt zwrotny do przeprowadzenia ataku na sąsiednie sieci; wykrywać i wykorzystywać luki w zabezpieczeniach zasobów znajdujących się głębiej w sieci.

RidgeBot ruch boczny



Cyberemulacja przeciwnika (ACE) z opcjonalnym agentem

Symulacja ataku oparta na agentach: RidgeBot® wykorzystuje Botleta opartego na agentach do symulacji ataków przeciwnika. RidgeBot® Botlet można wdrożyć na wielu platformach operacyjnych i w różnych segmentach sieci, aby symulować rzeczywiste cyberzagrożenia w sposób ciągły lub na żądanie.

Gotowa ocena: RidgeBot® oferuje gotowe szablony testów oceny ACE, ułatwiając ocenę skuteczności w różnych aspektach kontroli bezpieczeństwa. Testy oceniające są kompleksowe i bezpieczne do uruchomienia w środowisku produkcyjnym

Dostosowanie ram MITRE ATT&CK: Ramy MITRE ATT&CK to globalnie dostępna baza wiedzy na temat taktyk i technik przeciwnika oparta na obserwacjach z rzeczywistego świata. Baza wiedzy ATT&CK jest szeroko wykorzystywana przez RidgeBot do tworzenia znaczących i realistycznych skryptów testowych dla swoich klientów w celu kwestionowania, oceniania i optymalizowania kontroli bezpieczeństwa.

Ridge Security

Ridge Security dostarcza etyczne, wydajne i niedrogie rozwiązania do weryfikacji bezpieczeństwa dla małych i dużych przedsiębiorstw. Zapewniamy naszym klientom zgodność, alerty i bezpieczeństwo przez cały czas. Zespół zarządzający ma wieloletnie doświadczenie w sieci i bezpieczeństwie. Ridge Security znajduje się w sercu Doliny Krzemowej i rozszerza swoją działalność na inne obszary, w tym Amerykę Łacińską, Azję i Europę.

RidgeBot®, zrobotyzowany system weryfikacji bezpieczeństwa, w pełni automatyzuje proces testowania, łącząc zaawansowane etyczne techniki hakerskie i cyberemulację przeciwnika. RidgeBoty lokalizują, wykorzystują i dokumentują wykryte zagrożenia biznesowe i luki w zabezpieczeniach, kontrolują awarie bezpieczeństwa IT podczas procesu testowania, podkreślając potencjalny wpływ lub szkody.

Zobacz webinar

Co dają nam testy penetracyjne serwerów i aplikacji webowych?
Przejdź na testy zautomatyzowane dzięki Ridge Security Ridgebot

Na webinarze dowiesz się:

- Jak wykorzystać machine learning w identyfikacji realnych ścieżek ataku na przedsiębiorstwo.
- Jak powstrzymywać ataki przed ich wydarzeniem się.
- Jak zidentyfikować w czasie rzeczywistym ryzyko operacyjne dla organizacji.
- Jak dzięki prostym instrukcją zamykać punkty wejścia dla hakerów do organizacji.
- Jak dzięki RidgeBotowi weryfikować gotowość systemów secuirty, zespołów bezpieczeństwa do efektywnego odpierania zagrożeń.

W celu uzyskania dostępu do materiałów wideo zeskanuj kod QR lub przejdź na stronę https://konferencje.greeneris.com/2023-08-vod-webinar-ridge-security i wypełnij formularz rejestracyjny.

Masz pytania? Skontaktuj się z nami!

Greeneris Sp. z o.o. jest autoryzowanym partnerem firmy Ridge Security. Nasi specjaliści pomogą Państwu w sprecyzowaniu wymagań. Ocenimy bieżące systemy oraz środowisko IT pod kątem potencjalnych zagrożeń oraz pomożemy w doborze najkorzystniejszych rozwiązań prewencyjnych.

Zadzwoń do nas **+48 22 439 03 20** lub napisz **biuro@greeneris.com. www.greeneris.com**

greeneris