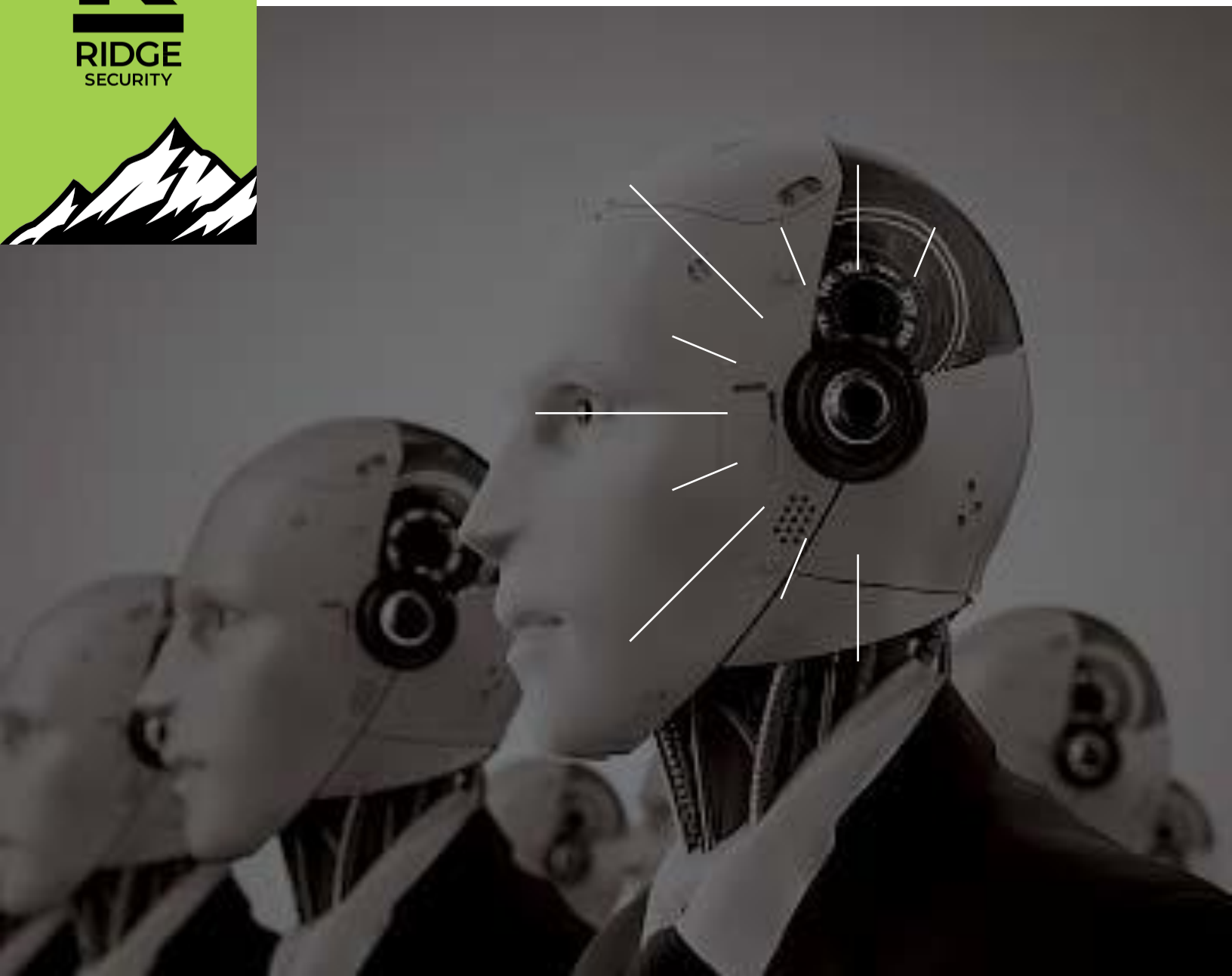
Automatyzacja Weryfikacji Zabezpieczeń Cybernetycznych

RIDGE SECURITY



RidgeBot® automatyzuje proces identyfikacji ryzyka szybciej niż człowiek

RidgeBot® to narzędzie wspierające organizacje sprawdzając bezpieczeństwo infrastruktury zewnętrznej i wewnętrznej. Zgodny z szablonami MITRE ATT&CK oraz OWASP, RidgeBot® pomaga przedsiębiorstwom zweryfikować ekspozycję na ryzyko zewnętrzne i wewnętrzne. Zachowując się jak doświadczony etyczny RidgeBot® wykorzystując uczenie maszynowe identyfikuje zagrożenia, słabe punkty, błędne konfiguracje w celu uwidoczniania zagrożenia. Automatyczne podejście do weryfikacji poprawności zabezpieczeń przedsiębiorstwa sprawia, że jest to rozwiązanie z możliwością działania na duża skalę. Ridge Security umożliwia przedsiębiorstwom, zespołom DevOps, dostawcą oprogramowania, rządom – wszystkim odpowiedzialnym za zapewnienie bezpieczeństwa infrastruktury oraz aplikacji webowych – niedrogie i wydane testowanie ich systemów w czasie rzeczywistym.

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 rozwiązania w zakresie cyberobrony mogą działać zgodnie z oczekiwaniami w zakresie wykrywania i ograniczania zagrożeń wykorzystujące najbardziej aktualne techniki ataków użytkowane przez zaawansowane trwałe zagrożenia (APT) i inne złośliwe podmioty.

Cyberataki są coraz bardziej wyrafinowane i stale się rozwijają, hakerzy opracowują nowe exploity i metody ataków praktycznie codziennie, 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. Bazując na ryzku wiele organizacji szuka zautomatyzowanego systemu testów penetracyjnych, aby sprostać temu wyzwaniu w łatwiejszy w zarządzaniu i ekonomiczny sposób.

Rozwiązanie i kluczowe korzyści

RidgeBot® to system, który automatyzuje proces testów penetracyjnych i emuluje ataki przeciwników w celu sprawdzenia stanu cyberbezpieczeństwa organizacji. Narzędzie zapewnia jaśniejszy obraz krajobrazu luk w zabezpieczeniach i zamyka potencjał dla złośliwych atakujących poprzez zwiększenie częstotliwości testów penetracyjnych, zarządzanie lukami w zabezpieczeniach oparte na ryzyku i testowanie wiedzy praktycznej specjalistów zajmujących się reagowaniem na incydenty za pomocą ćwiczeń. 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

1

Automatyczne testy penetracyjne

- Atak wewnętrzny
- Atak zewnętrzny
- Ruch boczny
- Zarządanie podatnościami

- Walidacja kontroli
- Ciągłe testowanie
- MITRE ATT&CK

Emulacja atakującego

2

RidgeBot® zapewnia 360-stopniową weryfikację bezpieczeństwa

RidgeBot ® Funkcjonalność

Automatyczne testy penetracyjne

W ramach danego zadania RidgeBot® automatyzuje cały proces etycznego hakowania. Podczas połączenia ze wskazanym środowiskiem 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 i ustalanie 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 skompromitowanych obiektów.

Cyberemulacja przeciwnika (ACE)

Kontrole bezpieczeństwa IT to mechanizmy stosowane w celu zapobiegania, wykrywania i łagodzenia zagrożeń. 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 i mapuje swoje skrypty testów oceniających do taktyk i technik MITRE ATT&CK. Zwiększa to widoczność potencjalnych wektorów ataków i identyfikacje ryzyka.

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 możliwość głębszej ingerencji w infrastrukturę.

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

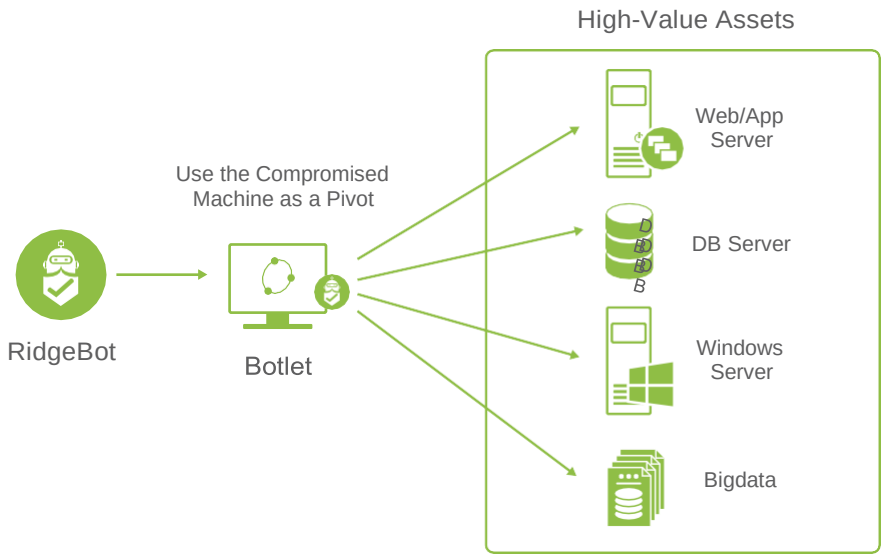
Scenariusze testów penetracyjnych

Atak wewnętrzny. Przeprowadź ataki z wnętrza sieci, 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 agencie. RidgeBot® Botlet można wdrożyć na wielu systemach operacyjnych i w różnych segmentach sieci, aby symulować rzeczywiste zagrożenia 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 do ram MITRE ATT&CK: Ramy MITRE ATT&CK to globalnie dostępna baza wiedzy na temat taktyk i technik oparta na obserwacjach z rzeczywistego świata. Baza wiedzy ATT&CK jest szeroko wykorzystywana przez RidgeBot do tworzenia realistycznych skryptów testowych dla swoich klientów w celu oceniania i optymalizowania kontroli bezpieczeństwa.

Ridge Security

Ridge Security dostarcza etyczne, wydajne rozwiązania do weryfikacji bezpieczeństwa dla małych i dużych przedsiębiorstw. Zapewniamy naszym klientom zgodność 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®, zautomatyzowany system weryfikacji bezpieczeństwa, w pełni automatyzuje proces testowania, łącząc zaawansowane etyczne techniki hakerskie i emulacje przeciwnika. RidgeBoty lokalizują, wykorzystują i dokumentują wykryte zagrożenia biznesowe i luki w zabezpieczeniach, kontrolują ryzyko awarii bezpieczeństwa IT podczas procesu testowania, podkreślając potencjalny wpływ lub szkody.

Skontaktuj się z nami na prezentacje i live demo:

kontakt(at)prianto.pl

PRIANTO