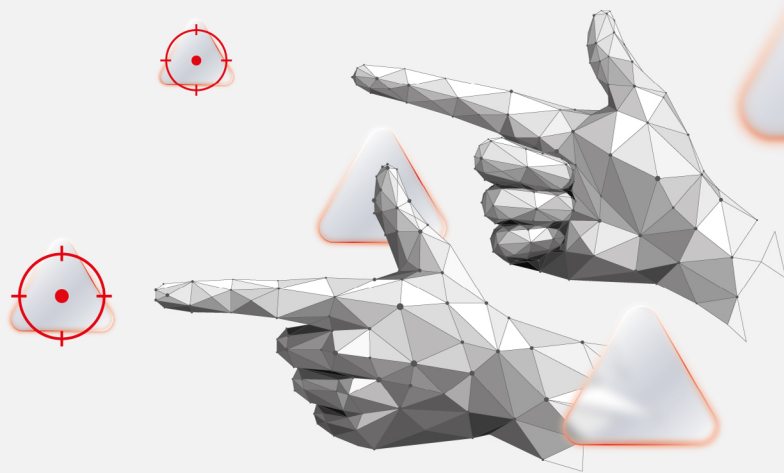




CyberSoldier.AI™

Private Cyber Range

Stale dostępne środowisko do budowania gotowości organizacji na cyberataki



Ciągłe doskonalenie kompetencji zespołów IT, bezpieczeństwa i SOC



Narzędzia detekcji incydentów jak w środowisku produkcyjnym



Testowanie własnych polityk i procedur Incident Response



Realistyczne cyberataki bez angażowania zewnętrznych pentesterów

GŁÓWNE WARTOŚCI ROZWIĄZANIA

✓ Zespoły IT, bezpieczeństwa i SOC zawsze gotowe do reagowania na cyberataki

Gotowe do użycia środowisko cyberpoligonu, dostarczane na dedykowanej platformie sprzętowej, które jest stale dostępne dla pracowników i umożliwia ciągłe doskonalenie umiejętności wykrywania, analizy i reagowania na incydenty.

✓ Ćwiczenia z wykorzystaniem tych samych narzędzi detekcji co w środowisku produkcyjnym

Cyberpoligon jest własnością firmy i umożliwia instalację, konfigurację oraz wykorzystanie tych samych narzędzi detekcyjnych, które są używane w środowisku produkcyjnym, np. SIEM, EDR/XDR czy NDR.

✓ Możliwość testowania własnych polityk i procedur obsługi incydentów

Dzięki stałej dostępności cyberpoligonu wyposażonego w te same narzędzia bezpieczeństwa co środowisko produkcyjne firma może regularnie testować i doskonalić własne polityki oraz procedury Incident Response, wspierając jednocześnie spełnienie wymagań NIS2, DORA i GDPR.

✓ Szybkie i efektywne szkolenie pracowników dzięki automatyzacji i AI

Cyberpoligon jest wyposażony w aplikację CyberSoldier.AI, wspieraną przez lokalny model AI, która automatycznie realizuje realistyczne, wieloetapowe scenariusze cyberataków oraz wyjaśnia wykonywane działania ofensywne.

✓ Gotowość na nowe zagrożenia

Cyberpoligon jest regularnie aktualizowany o nowe ścieżki i scenariusze ataków, które mogą być ćwiczone również w formacie Capture the Flag (CTF), zwiększającej zaangażowanie i efektywność szkolenia.



KLUCZOWE WŁASNOŚCI

Nauka zarządzania incydentami na realistycznych scenariuszach

Wszystkie scenariusze cyberataków dostępne w Private Cyber Range są oparte na wiedzy Threat Intelligence i realizowane w sposób odzwierciedlający działania cyberprzestępców podczas rzeczywistych ataków.

Ćwiczenia Incident Response bez angażowania zewnętrznych pentesterów

Private Cyber Range jest wyposażony w dedykowaną aplikację CyberSoldier.AI Red Team Automation, która automatycznie realizuje realistyczne, wieloetapowe scenariusze cyberataków.

Asystent AI pomaga zrozumieć sposób działania cyberprzestępców

CyberSoldier.AI jest zintegrowany z lokalnym modelem AI, który wyjaśnia uczestnikom aktualny etap scenariusza cyberataku, wykryte podatności, wykorzystane techniki MITRE ATT&CK oraz narzędzia ofensywne użyte do kompromitacji systemów IT.

Lepsze zrozumienie bezpieczeństwa Active Directory

Aplikacja AD Explorer pomaga uczestnikom ćwiczeń Incident Response lepiej zrozumieć złożone aspekty bezpieczeństwa Active Directory oraz przedstawia konfigurację środowiska z perspektywy atakującego.

Możliwość rozszerzenia ćwiczeń Incident Response na środowisko produkcyjne

Narzędzia dostępne w Private Cyber Range mogą być również wykorzystywane przez firmy w środowisku produkcyjnym do dalszego doskonalenia umiejętności zespołów IT, bezpieczeństwa i SOC.

Szkolenie własnego zespołu Red Team

Cyberpoligon może być wykorzystywany do rozwijania umiejętności ofensywnych (hacking, pen-testing) i budowania własnych zespołów testerów bezpieczeństwa.

CO ZAWIERA PRODUKT?

- Platformę sprzętową z zasobami CPU/GPU odpowiednimi do uruchamiania cyberpoligonu oraz lokalnych modeli AI.
- Wstępnie skonfigurowane systemy i aplikacje zawierające podatne komponenty, umożliwiające przeprowadzanie realistycznych cyberataków.
- Aplikacje CyberSoldier.AI wspierające i automatyzujące ćwiczenia ofensywne (hacking).
- Wytyczne dotyczące konfiguracji cyberpoligonu oraz korzystania z aplikacji CyberSoldier.AI.
- Aktualizacje oprogramowania CyberSoldier.AI oraz maszyn wirtualnych cyberpoligonu, dostarczane w ramach usługi utrzymaniowej.

Produkt nie zawiera narzędzi bezpieczeństwa. Integrator lub firma może wdrożyć w środowisku własne narzędzia bezpieczeństwa, takie jak SIEM, EDR, XDR, NDR, firewalle lub inne rozwiązania bezpieczeństwa, albo zakupić wybrane narzędzia bezpieczeństwa razem z produktem.