KASPERSKY lab ENTERPRISE

Kaspersky Cloud Sandbox

Zapobieganie współczesnym atakom ukierunkowanym przy wykorzystaniu wyłącznie tradycyjnych narzędzi antywirusowych jest niemożliwe: silniki antywirusowe chronią tylko przed znanymi zagrożeniami oraz ich odmianami, tymczasem wyrafinowane szkodniki używają wszystkich dostępnych sposobów, aby uniknąć automatycznego wykrycia. Straty wynikające z incydentów związanych z bezpieczeństwem informacji są coraz większe, dlatego tak istotne jest, aby zapewnić sobie możliwość natychmiastowego wykrywania zagrożeń, szybkiej reakcji i przeciwdziałania im, zanim wyrządzą jakiekolwiek szkody.

Podejmowanie inteligentnych decyzji w oparciu o zachowanie pliku oraz analizowanie pamięci procesów czy aktywności w sieci umożliwia zrozumienie współczesnych wyrafinowanych, ukierunkowanych i dopasowanych zagrożeń. Surowe dane statystyczne nie zawierają informacji na temat niedawno zmodyfikowanego szkodliwego oprogramowania, dlatego warto korzystać także z technologii piaskownicy. To potężne narzędzie umożliwia analizę pochodzenia próbki pliku, zgromadzenie oznak infekcji na podstawie zachowania oraz wykrycie nieznanego wcześniej szkodliwego obiektu.

Rozwiązanie wykrywa/analizuje:

- Ładowane i uruchomione biblioteki DLL
- Tworzenie wielokrotnych rozszerzeń
- Modyfikowanie i tworzenie kluczy rejestru
- Połączenia z zewnętrznymi nazwami domen i adresami IP
- Żądania i odpowiedzi HTTP oraz DNS
- Procesy utworzone przez pliki wykonywalne
- Tworzenie, modyfikowanie i usuwanie plików
- Zrzuty pamięci procesów pamięci i zrzuty ruchu sieciowego (PCAP)
- Zrzuty ekranu
- Szczegółowa analiza zagrożeń ze wskazówkami reakcji dla każdego ujawnionego wskaźnika włamania (IoC)
- i wiele więcej

Kluczowe korzyści:

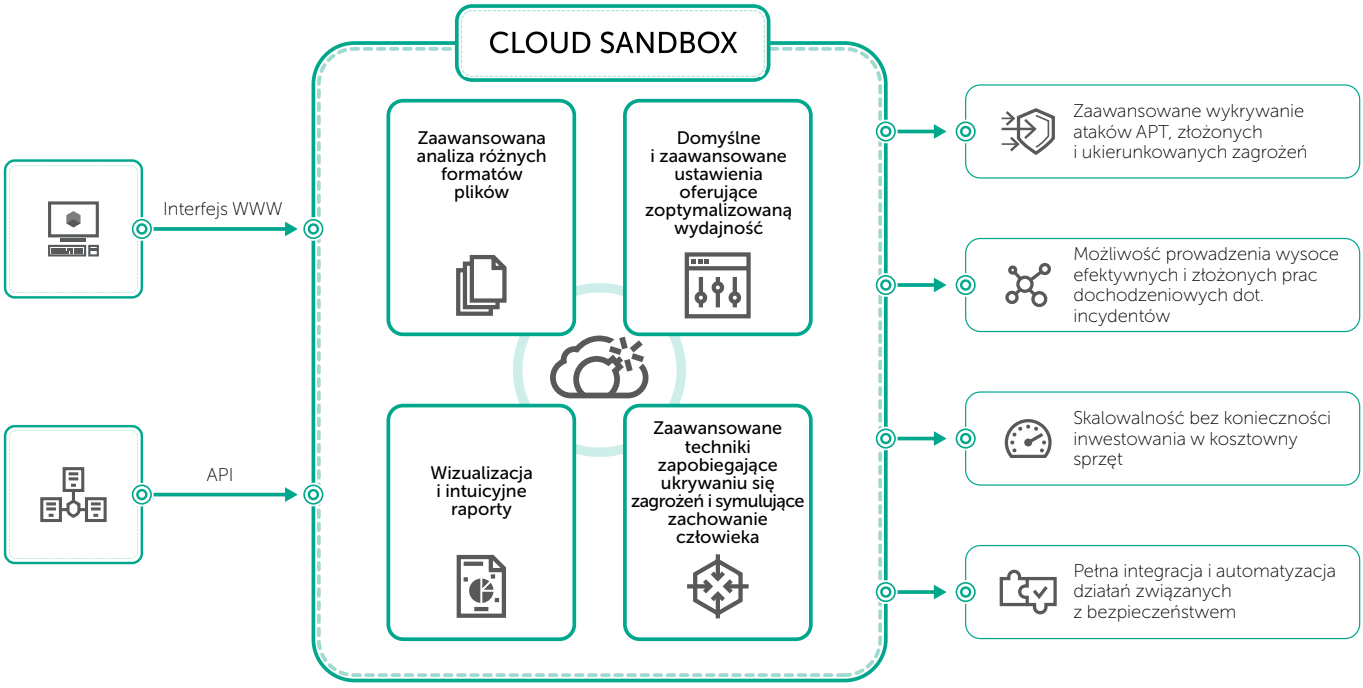
- Zaawansowane wykrywanie ataków APT oraz ukierunkowanych i złożonych zagrożeń
- Możliwość przeprowadzania skutecznej analizy skomplikowanych incydentów
- Skalowalność bez konieczności zakupu kosztownych urządzeń lub martwienia się o zasoby systemowe
- Bezproblemowa integracja i automatyzacja działań bezpieczeństwa

Proaktywne zmniejszanie ryzyka omijania zabezpieczeń przez zagrożenia

Współczesne szkodliwe programy używają całego wachlarza metod, dzięki którym unikają wykonania swojego kodu, jeśli mogłoby to doprowadzić do ujawnienia ich szkodliwej aktywności. Jeśli system nie spełnia wymaganych parametrów, szkodliwy program z dużym prawdopodobieństwem ulegnie samozniszczeniu, nie pozostawiając po sobie śladu. Aby szkodliwy kod został wykonany, środowisko piaskownicy musi dokładnie naśladować tradycyjne zachowania użytkownika.

Kaspersky Cloud Sandbox oferuje podejście hybrydowe, które łączy analizę zagrożeń obejmującą petabajty danych statystycznych (dzięki Kaspersky Security Network i innym autorskim systemom), analizę zachowania oraz system zapobiegający ukrywaniu się zagrożeń, a także technologie naśladujące zachowanie człowieka, takie jak automatyczne klikanie, przewijanie dokumentów czy uruchamianie procesów. W efekcie powstaje narzędzie umożliwiające wykrywanie nieznanych zagrożeń.

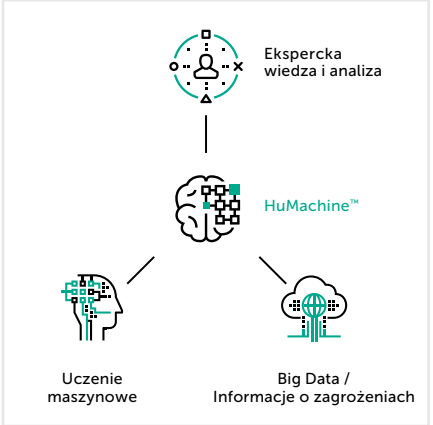
Usługa ta została utworzona bezpośrednio na podstawie piaskownicy, z której korzystamy w naszym laboratorium - technologia ta jest rozwijana od ponad 10 lat. Wykorzystuje ona całą wiedzę firmy Kaspersky Lab na temat zachowania szkodliwego oprogramowania, którą zgromadziliśmy na przestrzeni 20 lat nieprzerwanego badania zagrożeń. Dzięki temu potrafimy wykrywać ponad 360 tysięcy nowych szkodliwych obiektów każdego dnia i możemy oferować naszym klientom najlepsze w branży rozwiązania zabezpieczające.



Kaspersky Cloud Sandbox to najnowszy element serwisu Threat Intelligence Portal, który wynosi skuteczność analizy na nowy poziom. Portal otrzymuje najnowszą szczegółową analizę zagrożeń na temat adresów internetowych, domen, adresów IP, skrótów plików, nazw zagrożeń, danych statystycznych i związanych z zachowaniem, danych WHOIS/DNS itp., a z kolei Cloud Sandbox łączy te informacje ze wskaźnikami włamania wygenerowanymi przez analizowaną próbkę.

To wszystko pozwala przeprowadzić skuteczną i skomplikowaną analizę incydentu, natychmiast poznać naturę zagrożenia, a także dostrzec wzajemne powiązania miedzy oznakami jego obecności.

Kaspersky Cloud Sandbox to idealne narzędzie, aby przyspieszyć reakcję na incydent i przeprowadzić czynności kryminalistyczne, które oferuje skalowalność automatycznego przetwarzania plików bez konieczności zakupu drogich urządzeń czy martwienia się o zasoby systemowe



Ochrona dla małych firm: **kaspersky.pl/ochrona-dla-malego-biznesu**
Ochrona dla średnich firm: **kaspersky.pl/ochrona-dla-sredniego-biznesu**
Ochrona dla korporacji: **kaspersky.pl/ochrona-dla-korporacji**
Unikatowa technologia: **kaspersky.pl/true-cybersecurity**
Wszystko o cyberzagrożeniach: **securelist.pl**
Oficjalny blog: **kaspersky.pl/blog**

Kaspersky Lab Polska sp. z o.o.
ul. Trawiasta 35
04-607 Warszawa

kaspersky.pl