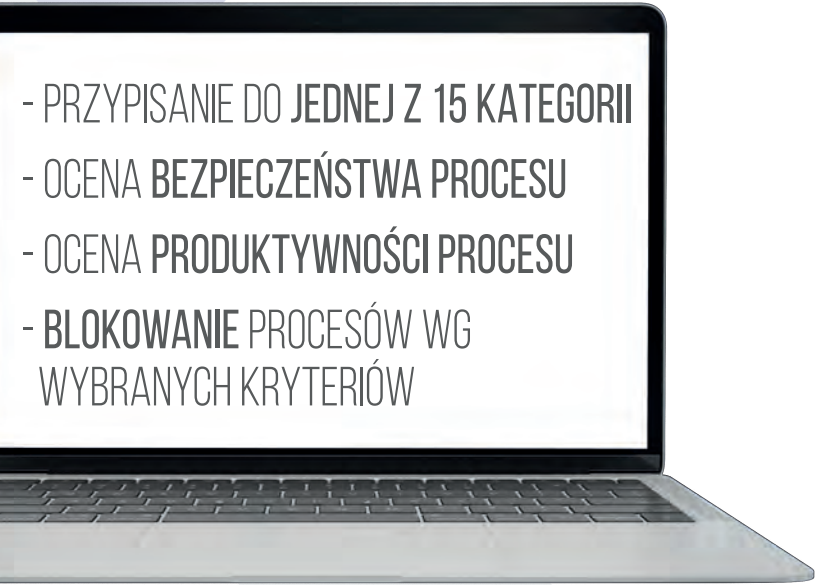


- 
- PRZYPISANIE DO JEDNEJ Z 15 KATEGORII
 - OCENA BEZPIECZEŃSTWA PROCESU
 - OCENA PRODUKTYWNOŚCI PROCESU
 - BLOKOWANIE PROCESÓW WG WYBRANYCH KRYTERIÓW

15 KATEGORII

Procesy klasyfikowane są w oparciu o informacje uzyskane za pośrednictwem wyszukiwarki internetowej Bing oraz przypisywane są do jednej z 15 kategorii.

SKUTECZNOŚĆ > 85%

Wysoka skuteczność klasyfikacji wynika z zastosowanych algorytmów sztucznej inteligencji oraz zbudowanej bazy wzorców słów kluczowych w ramach poszczególnych kategorii.

IŁOŚĆ POZYCJI W KATALOGU

Katalog sklasyfikowanych procesów i aplikacji jest nieustannie rozbudowywany oraz dostępny jest w chmurze celem dowolnego wykorzystania w innych rozwiązaniach poprzez API.

WYSOKA SZYBKOŚĆ

Standardowa szybkość klasyfikacji > 10 procesów / sek.
Może być zwiększona w zależności od potrzeb.

MACHINE LEARNING W KLASYFIKACJI PROCESÓW I APLIKACJI KOMPUTEROWYCH

Klasyfikacja procesów i aplikacji może być przydatna w każdym podmiocie, gdzie nadzór i kontrola aktywności użytkowników może mieć realny wpływ na bezpieczeństwo oraz ocenę produktywności użytkowników. Zaimplementowanie algorytmu uczenia maszynowego pozwala na sprawne i szybkie klasyfikowanie dowolnego procesu pod kątem i przypisania (sklasyfikowania) do odpowiedniej kategorii. Moduł klasyfikacji procesów w systemie eAuditor V7 WEB przygotowany jest na występowanie różnych zdarzeń losowych w taki sposób, aby mimo błędu po stronie serwera nie przerywał działania i poprawnie wykonywał swoje zadanie, przypisując procesy do odpowiednich kategorii.

KLASYFIKATOR PROCESÓW I APLIKACJI KOMPUTEROWYCH

Klasyfikator bayesowski, który bazuje na twierdzeniu Bayesa, nadaje się w szczególności do rozwiązywania problemów o bardzo wielu wymiarach na wejściu. Mimo prostoty metody, często działa ona lepiej od innych, bardzo skomplikowanych metod klasyfikujących. Wspomniany klasyfikator można uczyć w trybie uczenia z nadzorem. Oznacza to, że do poprawnego i jeszcze lepszego działania algorytmu konieczny jest nadzór człowieka, który na bieżąco będzie analizował i poprawiał ewentualne błędy algorytmu. Klasyfikacja jest tak długo poprawna, jak długo poprawna kategoria jest bardziej prawdopodobna od innych.

CZAS KLASYFIKACJI PROCESÓW

Klasyfikacja pojedynczego procesu trwa około 1 sekundy. W praktyce osiąga się wysoką wydajność z uwagi na wielowątkową obsługę procesów klasyfikacji (jednoczesne klasyfikowanie nawet setki procesów).

POPRAWNOŚĆ KLASYFIKACJI PROCESÓW I APLIKACJI KOMPUTEROWYCH

W ramach testu machine learningu w eAuditor V7 WEB skategoryzowano 1000 losowych i mało popularnych procesów. Poprawność przypisania kategorii wynosi **około 85%**. Problem z osiągnięciem lepszych rezultatów nie stoi po stronie algorytmu, gdyż ten stwierdza największe prawdopodobieństwo wystąpienia danej kategorii. Problematyczny jest fakt, że każdy proces jest wyszukiwany w przeglądarce internetowej, a ta z kolei nie zawsze zwraca odpowiednie wyniki wyszukiwania. Zdarza się także, że wyszukiwane procesy mogą odnosić się do różnych programów z różnych kategorii.

Przykładowo proces *win_driver_installer.exe* może być skategoryzowany zarówno jako proces systemowy, jak i jako sterownik.

WYDAJNOŚĆ

W rozwiązaniu zaimplementowano szereg mechanizmów odrzucających procesy, które z dużą pewnością nie zwrócą poprawnych wyników. Pozwala to zaoszczędzić czas i nie angażować algorytmu klasyfikacyjnego do klasyfikowania błędnych procesów. Silnik klasyfikatora jest umiejscowiony w datacenter i obsługiwany jest przez skalowany zestaw serwerów, co zapewnia **nieograniczoną wydajność**.

BTC MACHINE LEARNING PROCESS CLASSIFICATION

JAK DZIAŁA MACHINE LEARNING W KLASYFIKACJI PROCESÓW SYSTEMOWYCH I APLIKACJI?



DLACZEGO WPROWADZILIŚMY MACHINE LEARNING DO SYSTEMU EAUDITOR V7 WEB?

Oto kilka powodów, dla których zastosowaliśmy Machine Learning w systemie eAuditor V7 WEB, zamiast statystycznej bazy danych procesów:

- ✔ automatyczne tworzenie bazy danych z informacjami o procesach, ich kategoriach wraz z oceną produktywności i bezpieczeństwa,
- ✔ odporność na zmianę kategorii w czasie (następuje automatyczna zmiana kategorii),
- ✔ automatyczna, w czasie rzeczywistym, synchronizacja z bazą danych sklasyfikowanych procesów w datacenter.