senhasegura®

Analiza zagrożeń

Automatyczna analiza kluczowych działań

Co to jest?

Monitorowanie środowiska na potrzeby wykrywania i zgłaszania podejrzanych działań wykonywanych z użyciem uprzywilejowanych poświadczeń.

Jak to działa?

Na bieżąco generowana jest lista poleceń i podejrzanych zachowań zaobserwowanych w systemie. Są one klasyfikowane na podstawie stopnia ryzyka, a następnie, w przypadku ich wykrycia, są one konsolidowane i wyświetlane w formie graficznej w panelu administracyjnym.

Funkcje

- Panel kontrolny, na którym w formie graficznej wyświetlane są wszystkie ryzyka i zagrożenia;
- Szczegółowe alerty na temat podejrzanej aktywności;
- Analiza sesji użytkowników;
- Audyt, alarmowanie i blokowanie poleceń;
- Zapisywanie logów poleceń;
- Oznaczanie składni poleceń;
- Identyfikacja ruchu poprzecznego i eskalacji uprawnień;
- Alerty podejrzanej aktywności dla SIEM/SYSLOG.

Funkcje techniczne

- Automatyczne uczenie się zachowań użytkowników i działania urządzeń;
- Blokowanie poleceń na podstawie białej i czarnej listy;
- Automatyczna reakcja w razie wykrycia zagrożenia.

Korzyści

- Odkrywanie potencjalnych podatności
- Przyspieszenie reakcji w przypadku ataku
- Automatyczne blokowanie skradzionych poświadczeń
- Wykrywanie zagrożeń
- Kompletne informacje na temat incydentu