Aktualizacja 01.09.2021 r.

Stacje robocze Linux

1. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop 18.04 / 20.04 LTS 64-bit, Red Hat Enterprise Linux 7, 8 64-bit, SUSE Linux Enterprise Desktop.
2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.
3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
11. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
12. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
13. Rozwiązanie musi posiadać możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
14. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Administrator musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
15. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
16. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
17. Aktualizacje silnika detekcji muszą być dostępne z Internetu, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
18. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy.
19. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

20. Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień lokalnie oraz zdalnie za pomocą dedykowanego narzędzia.
21. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.