ZAŁĄCZNIK NR 1

Odnowienie licencji na 1 rok, na system ESET PROTECT Enterprise ON-PREM 690 licencji dla serwerów i stacji roboczych lub system równoważny dla **33B-EUD-DPD**, spełniający poniższe kryteria.
Licencja powinna obowiązywać od 1.04.2024r.

Minimalna wymagana funkcjonalność:

- wielowarstwowa ochrona stacji roboczych i serwerów,
- ochrona systemu operacyjnego, przeglądarek WWW, poczty, pamięci operacyjnej,
- możliwość szyfrowania dysków,
- wykrywanie zagrożeń w oparciu o analizę ich zachowania i reputacji,
- ochrona przed złośliwym oprogramowaniem typu ransomware i atakami zero-day,
- zapobieganie atakom bezplikowym,
- możliwość instalowania na stacjach roboczych z systemami Windows 10, Windows 11, Windows Server 2012R2 i późniejszych, macOS, Linux,
- centralna konsola zarządzania licencjami, wykrytymi zagrożeniami, stacjami, użytkownikami, plikami skierowanymi do kwarantanny,
- ochrona plików w czasie rzeczywistym,
- ochrona sektorów startowych, UEFI,
- skanowanie spakowanych plików,
- wykrywanie zagrożeń algorytmami heuterystycznymi,
- wykrywanie zagrożeń na podstawie reputacji aplikacji,
- wykrywanie zagrożeń na podstawie reputacji adresów IP,
- ochrona przed atakami z sieci (IDS),
- ochrona przed atakami typu brute force,
- ochrona przed botnetami,
- możliwość definiowania tzw. czarnej listy adresów IP,
- wykrywanie włamań min. dla protokołów: SMB, RCP, RDP,
- blokowanie niebezpiecznych adresów po wykryciu ataku,
- możliwość definiowania wyłączeń dla w/w ustawień,
- współpraca z domeną Windows AD,
- zdalna konfiguracja stacji roboczych - możliwość definiowania różnych polityk dla różnych grup komputerów, serwerów, itp.,
- możliwość zdalnej instalacji systemu antywirusowego za pomocą WMI,
- możliwość zdalnej instalacji systemu antywirusowego za pomocą GPO,
- możliwość skanowania na żądanie wskazanej stacji roboczej lub serwera,
- możliwość skanowania w trakcie bezczynności komputera,
- możliwość skanowania przy uruchamianiu komputera / serwera,
- możliwość pobierania aktualizacji systemu antywirusowego bez konieczności stałego połączenia z Internetem na stacjach roboczych (np. przez serwer proxy, lokalne repozytorium aktualizacji lub podobne rozwiązanie),
- monitorowanie wersji oprogramowania antywirusowego i jego modułów, raportowanie w konsoli zarządzającej,
- monitorowanie aktualizacji systemu operacyjnego, raportowanie w konsoli zarządzającej,
- monitorowanie zdarzeń systemowych,
- możliwość wycofania aktualizacji modułu systemu antywirusowego w przypadku pojawienia się błędów lub fałszywych alertów,

ul. Koszarowa 5, 51-149 Wrocław
NIP: 895-16-31-106 | Regon: 000290469
Sekretariat: 71 395 74 26 | fax 71 326 06 22
Centrala tel.: 71 326 13 25
sekretariat@szpital.wroc.pl
www.szpital.wroc.pl

DOLNY ŚLĄSK

- możliwość aktywnego filtrowania stron internetowych i poczty elektronicznej,
- możliwość zdefiniowania wyjątków dla aplikacji, wybranych stron i adresów IP,
- ochrona przed atakami typu "phishing",
- tryb prezentacji,
- możliwość konfigurowania systemu i interfejsu użytkownika na stacjach roboczych i serwerach z poziomu centralnej konsoli zarządzającej,
- wysyłanie alertów przez pocztę elektroniczną na wskazane adresy,
- możliwość przygotowania pakietu instalacyjnego dla wybranej grupy urządzeń z uwzględnieniem wymaganych modułów, konfiguracji i polityk,
- moduł analizy danych zbieranych ze stacji roboczych i serwerów w celu korelacji zdarzeń i typowania zagrożeń,
- raportowanie, w formie drzewa, szczegółowych informacji dotyczących wykrytego zagrożenia, w tym: rodzaj zagrożenia, uruchomione procesy, rozpoznane zagrożenia, rozpoznane niepożądane interakcje, odniesienie do MITTRE ATT@CK, data wystąpienia zdarzenia, data wykrycia zdarzenia, zalecane rozwiązania i działania, które zminimalizują lub rozwiążą problem,
- możliwość przypisania automatycznej akcji podejmowanej przez system dla podobnych wystąpień (playbook),
- możliwość wygenerowania listy zainstalowanych aplikacji na stacjach roboczych i serwerze wraz z analizą zagrożeń,
- możliwość przeglądania i filtrowania skryptów wykonywanych na stacjach lub serwerach,
- możliwość blokowania nieautoryzowanych skryptów i aplikacji przed uruchomieniem,
- automatyczne usuwanie niepożądanych aplikacji w ramach stosowanych rozwiązań usuwających wykryte zagrożenie,
- możliwość blokowania aplikacji lub skryptów na podstawie grupy użytkowników lub komputerów,
- możliwość grupowania komputerów na podstawie domeny AD lub ustawień ręcznych,
- możliwość włączenia kwarantanny dla zainfekowanego komputera,
- możliwość połączenia z konsolą zarządzającą za pomocą przeglądarki WWW,
- możliwość wgrania komercyjnych certyfikatów SSL do serwerów odpowiadających za stronę WWW konsoli zarządzającej,
- wykrywanie anomalii w zachowaniach stacji roboczych, programów i skryptów,
- wykrywanie działań naruszających ustanowione polityki,
- określanie stopnia zagrożenia na podstawie punktów ratingowych i progów alarmowych, po przekroczeniu, których będzie wyzwalana akcja lub powiadomienia dla administratora.

ul. Koszarowa 5, 51-149 Wrocław
NIP: 895-16-31-106 | Regon: 000290469
Sekretariat: 71 395 74 26 | fax 71 326 06 22
Centrala tel.: 71 326 13 25
sekretariat@szpital.wroc.pl
www.szpital.wroc.pl