**załącznik nr 2**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ wraz z załącznikami i przyszłej Umowy dotyczącej opisanego zamówienia, wymienionym w niniejszym paragrafie pojęciom nadają znaczenie określone poniżej, oraz że użyte w tekście poniżej wymienione pojęcia, rozumiane będą w sposób poniżej zdefiniowany. Dla podkreślenia, że pojęcia te rozumiane są w sposób zdefiniowany, ich pierwsze litery będą pisane w tekście wielką literą.

Strony ustalają następujące definicje:

1. **Zamawiający** – oznacza **Centrum Zdrowia w Mikołowie Sp. z o.o.**
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie niniejszego zamówienia publicznego
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
4. **System informatyczny** - zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. W skład systemu wchodzą najczęściej elementy: Sprzęt komputerowy, Oprogramowanie narzędziowe, Oprogramowanie dziedzinowe.
5. **Infrastruktura sprzętowa -** znajdująca się w dyspozycji Zamawiającego, w tym stanowiąca jego własność oraz dostarczana w ramach realizacji przedmiotu zamówienia infrastruktura przetwarzania danych wszystkie połączenia, urządzenia fizyczne i oprogramowania aplikacyjne, które łącznie współpracując umożliwiają gromadzenie, przechowywanie, wytwarzanie danych i usług oraz udostępnianie danych i usług elektronicznych.
6. **Umowa** – umowa zawarta w ramach realizacji OPZ.
7. **SWZ –** Specyfikacja Warunków Zamówienia
8. **Gwarancja i Serwis Oprogramowania** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie w oraz w projekcie umowy.
9. **Gwarancja i Serwis Infrastruktury Sprzętowej** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie oraz w projekcie umowy.
10. **Sprzęt Komputerowy** – zestaw komputerów (w tym stacje robocze, sprzęt serwerowy, terminale) i oprzyrządowania, na którym pracuje oprogramowanie.
11. **System Komunikacyjny** – infrastruktura telekomunikacyjna, sieciowa, systemy separacji, systemy bezpieczeństwa oraz certyfikaty serwerów WWW, obejmujące elementy lokalnej sieci komputerowej, łącza i urządzenia rozległej sieci transmisji danych oraz urządzenia komutacji pakietów wraz z ich oprogramowaniem, odpowiedzialne za obsługę HIS.
12. **Oprogramowanie Narzędziowe** – elementy oprogramowania zainstalowane na Sprzęcie Komputerowym, obejmujące w szczególności:
    * + systemy operacyjne (np. Windows, LINUX, UNIX),
      + system zarządzania bazą danych (SZBD), zwane też oprogramowaniem bazodanowym (np. MSSQL, Oracle),
      + oprogramowanie służące do administracji i zarządzania Sprzętem Komputerowym, systemem operacyjnym i systemem zarządzania bazą danych,
      + oprogramowanie komunikacyjne umożliwiające podłączenie stacji dostępowych do serwera bazy;
13. **Plan Realizacji Projektu** – Dokument określający zasady współpracy pomiędzy Zamawiającym, a Wykonawcą. Zawiera m.in.:
    * strukturę organizacyjną projektu,
    * produkty projektu,
    * zasady komunikacji w projekcie,
14. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora infrastruktury sprzętowej.
15. **Systemy Zewnętrzne** – systemy z którymi docelowo współpracować będzie wdrażany system.
16. **Wdrożenie** – etap cyklu życia systemu informatycznego, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego oraz testowaniu i uruchomieniu systemu informatycznego.

* Podstawowe etapy procesu wdrożenia:
* Przygotowanie dokumentacji,
* Przygotowanie i skonfigurowanie infrastruktury technicznej,
* Zainstalowanie i skonfigurowanie systemu informatycznego do eksploatacji,
* Testowanie systemu,
* Uruchomienie produkcyjne systemu.

1. **Środowisko Zapasowe** – kopia Środowiska Produkcyjnego lub jego części, służąca do gromadzenia kopii rzeczywistych danych biznesowych Zamawiającego i podjęcia ich przetwarzania w przypadku awarii Środowiska Produkcyjnego lub w celach przeprowadzenia testów wdrożeniowych aktualizacji/nowych funkcjonalności.
2. **Zdalny Dostęp** – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne.
3. **Szczegółowym Harmonogramem Realizacji Zadania** – szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w terminie 14 dni roboczych od zawarcia umowy.
4. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
5. **Etap** – główny element części Zadania, stanowiący funkcjonalną całość, podlegająca odrębnym odbiorom. Każdy Etap stanowi odrębną część (rozdział) niniejszego OPZ.
6. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
7. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
8. **Godziny Robocze** – godziny od 7:30 do 14:30 w każdym Dniu Roboczym.
9. **Kierownik Zamawiającego** – osoba wyznaczona przez Zamawiającego, koordynująca całość przedmiotu danego pakietu, posiadająca odpowiednie pełnomocnictwa. W szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu zamówienia.
10. **Kierownik Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji realizacji prac danego zadania. Upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.

**OPIS RÓWNOWAŻNOŚCI:**

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy PZP, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ

Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.

Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

**DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA**

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w Centrum Zdrowia w Mikołowie Sp. z o.o.

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

* Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2022.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 36 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z segmentacją VLAN, oraz strefą DMZ,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

**Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:**

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:
   * Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
   * Nazwy oraz szczegółowa adresacja poszczególnych elementów,
   * Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
   * Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
   * Harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

1. Konfiguracja serwerów oraz macierzy dyskowej.
2. Instalacja oraz konfiguracji oprogramowania.
3. Testy rozwiązania.
4. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
5. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:
   * Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
   * Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
   * Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
   * Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
   * Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
   * Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
   * Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
   * Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

**Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:**

Wymagania dla Wykonawcy który dostarczy infrastrukturę sprzętową oraz oprogramowanie:

1. **Przedmiotem zamówienia jest system bezpieczeństwa sieciowego (NDR – Network Detection and Response) składający się z następujących komponentów, lub komponentów im równoważnych:**
   1. Urządzenia pasywnego, które zostanie umiejscowione w sieci zamawiającego, analizującego przekazaną do niego kopię ruchu sieciowego, korelującego zdarzenia oraz generowanie powiadomień i zdarzeń (tzw. Eventów)
   2. Urządzenia aktywnego, umiejscowionego pomiędzy urządzeniami sieciowymi (tzw. Tryb in-line), służącego do wykonywania akcji blokowania ruchu, nadesłanych z urządzenia pasywnego.
2. **Minimalne parametry urządzenia pasywnego, analizującego ruch sieciowy:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1. System NDR (Network Detection and Response):**  Producent: ……………………………………………………………………………………………………………………………………………….,  Nazwa produktu, model: ………………………………………………………………………………………………………………………. . | | | | |
| **Dane techniczne** | | | **TAK / NIE** | |
|  | Wysokość 1U do montażu w szafie rack. |  | |
|  | Posiadać co najmniej dwa porty USB |  | |
|  | Urządzenie musi posiadać co najmniej dwa dedykowane porty do zarządzania systemem |  | |
|  | Urządzenie musi posiadać conajmniej jeden port konsoli |  | |
|  | Urządzenie musi posiadać minimum interfejsów: 16 x Gigabit Ethernet, 8 x SFP, 2 x SFP+ |  | |
|  | Urządzenie musi posiadać możliwość rozbudowy interfejsów o conajmniej 4 interfejsy SFP+ |  | |
|  | Musi obsługiwać co najmniej 1T przestrzeni dyskowej. |  | |
|  | Minimum 2 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń |  | |
|  | Proponowane rozwiązanie musi obsługiwać minimum 1,5 miliona jednoczesnych sesji. |  | |
|  | Proponowane rozwiązanie musi obsługiwać 75000 nowych sesji /s w ruchu HTTP. |  | |
| **Usługi sieciowe** | | |  | |
|  | Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta. |  | |
|  | Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi lub systemami IPS tej samej marki w celu ograniczenia zagrożeń |  | |
|  | Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS oraz VXLAN i wykrywania zagrożeń w tych wiadomościach. |  | |
| **Kontrola aplikacji** | | |  | |
|  | Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp. |  | |
|  | Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android. |  | |
|  | Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje. |  | |
| **Wykrywanie zagrożeń** | | |  | |
|  | Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń. |  | |
|  | Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow |  | |
|  | Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp. |  | |
|  | Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku. |  | |
|  | Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS. |  | |
|  | Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS. |  | |
|  | Rozwiązanie musi mieć opcję przechwytywania pakietów |  | |
|  | System musi mapować wykryte zagrożenia na framework MITRE ATT&CK |  | |
| **Skanowanie antywirusowe:** | | |  | |
|  | Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur. |  | |
|  | Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP. |  | |
|  | Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików |  | |
|  | Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur. |  | |
|  | Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP. |  | |
|  | Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików |  | |
| **Wykrywanie botnetów C&C:** | | |  | |
|  | Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C. |  | |
|  | Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C |  | |
|  | Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen. |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS. |  | |
|  | Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA. |  | |
|  | Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS. |  | |
| **Sandbox w chmurze** | | |  | |
|  | Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń |  | |
|  | Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy. |  | |
|  | Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP. |  | |
|  | Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty |  | |
|  | Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików. |  | |
|  | Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie. |  | |
| **Wykrywanie spamu** | | |  | |
|  | Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości. |  | |
|  | Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3 |  | |
|  | Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen. |  | |
| **Dodatkowe funkcje ochrony:** | |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp. |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu. |  | |
|  | Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop |  | |
| **Inteligentne funkcje bezpieczeństwa:** | |  | |
|  | Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki. |  | |
|  | Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym. |  | |
|  | Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp |  | |
|  | Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania |  | |
|  | Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut |  | |
|  | Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów. |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS |  | |
|  | Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji |  | |
|  | Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym |  | |
|  | Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń. |  | |
|  | Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia |  | |
|  | Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta |  | |
|  | Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd. |  | |
|  | Rozwiązanie musi obsługiwać przechwytywanie pakietów online |  | |
|  | Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania |  | |
|  | Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych |  | |
|  | Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę |  | |
|  | Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń. |  | |
| **Widoczność ryzyka/zagrożeń:** | |  | |
|  | Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego. |  | |
|  | Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch. |  | |
|  | Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu. |  | |
|  | Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp. |  | |
|  | Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni. |  | |
|  | Rozwiązanie musi wspierać wskazanie ścieżki ataku. |  | |
| **Analiza i odpowiedzi na incydenty** | |  | |
|  | Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury |  | |
|  | Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach. |  | |
|  | Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie. |  | |
|  | Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania. |  | |
|  | Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpwiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail. |  | |
| **Administracja** | |  | |
|  | Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI) |  | |
|  | Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli |  | |
|  | Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło |  | |
|  | Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów. |  | |
|  | Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych |  | |
|  | Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny |  | |
|  | Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń |  | |
| **Logowanie i raportowanie:** | |  | |
|  | Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP. |  | |
|  | Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp. |  | |
|  | Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS. |  | |
|  | Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń. |  | |
|  | Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje |  | |
|  | Wstępnie zdefiniowane zadania raportowania |  | |
|  | Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni. |  | |
|  | Rozwiązanie musi wspierać restAPI |  | |

1. **Minimalne parametry urządzenia aktywnego, filtrującego ruch sieciowy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **2. System NDR (Network Detection and Response):**  Producent: ……………………………………………………………………………………………………………………………………………….,  Nazwa produktu, model: ………………………………………………………………………………………………………………………. . | | | | |
| **Dane techniczne** | | | **TAK / NIE** | |
|  | Proponowane rozwiązanie powinno mieć maksymalną wysokość 1U. |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej dwa porty USB. |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej jeden port konsoli |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej jeden dedykowany port do zarządzania systemem |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej jeden port przeznaczony do klastrowania (HA) |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej 16 stałych portów Gigabit Ethernet (w tym dwie pary bypass) |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów SFP. |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej 2 stałe porty SFP+. |  | |
|  | Ilość portów może zostać zwiększona, poprzez dodatkowy moduł rozszerzeń, nie mniej niż 4 porty SFP+. Moduł rozszerzeń musi zostać dostarczony wraz z systemem bezpieczeństwa. |  | |
|  | Proponowane rozwiązanie musi posiadać co najmniej 500GB przestrzeni dyskowej. |  | |
|  | Proponowane rozwiązanie musi obsługiwać przepustowość IPS 12 Gb/s |  | |
|  | Proponowane rozwiązanie musi obsługiwać jednoczesne sesje o długości 6 M. |  | |
|  | Proponowane rozwiązanie musi obsługiwać min 65000 nowych sesji/sekundę w ruchu TCP. |  | |
|  | Opóźnienia (tzw. Latency) nie powinny przekraczać 300µs |  | |
|  | Funkcjonalności nie mogą być realizowane na rozwiązaniu NGFW |  | |
| **Usługi sieciowe** | | |  | |
|  | Proponowane rozwiązanie musi być w stanie pracować jednocześnie w trybie warstwy 3 (routing), trybie online (most) i warstwie 2 (kopia ruchu) (bez konieczności wirtualizacji sprzętu) |  | |
| **Kontrola aplikacji** | | |  | |
|  | Rozwiązanie powinno obsługiwać identyfikację IP hostów, ilość endpointów , czasu online, czasu offline. |  | |
|  | Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka. |  | |
|  | Rozwiązanie powinno rozpoznawać aplikacje IPv6. |  | |
|  | Rozwiązanie musi obsługiwać identyfikację aplikacji dla ruchu szyfrowanego SSL |  | |
|  | Rozwiązanie musi wspierać identyfikację aplikacji mobilnych na Androida i iOS. |  | |
|  | Rozwiązanie powinno obsługiwać wyświetlanie opisu, czynników ryzyka, zależności, typowych używanych portów i adresów URL dla dodatkowych odwołań i informacji dla każdej aplikacji w interfejsie WebUI. |  | |
|  | Rozwiązanie musi obsługiwać blokowanie, ponowne uruchamianie sesji, monitorowanie i kształtowanie ruchu dla aplikacji. |  | |
|  | Rozwiązanie musi być w stanie identyfikować i kontrolować aplikacje w chmurze |  | |
| **Ochrona Przed Zagrożeniami** | | |  | |
|  | Rozwiązanie musi obsługiwać ponad 15000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, automatyczne wstawianie lub wyodrębnianie sygnatur oraz zintegrowaną encyklopedię zagrożeń. |  | |
|  | Rozwiązanie musi obsługiwać zapobieganie włamaniom dla ruchu szyfrowanego SSL. |  | |
|  | Rozwiązanie musi obsługiwać ochronę środowiska IPV6. |  | |
|  | Rozwiązanie powinno obsługiwać wykrywanie anomalii protokołu. |  | |
|  | Rozwiązanie musi obsługiwać następujące akcje IPS: monitorowanie, blokowanie, resetowanie (adres IP atakujących lub IP ofiary, interfejs wejściowy) z czasem wygaśnięcia |  | |
|  | Rozwiązanie musi obsługiwać opcję logowania pakietów. |  | |
|  | Rozwiązanie musi obsługiwać profil zabezpieczeń IPS na podstawie ważności, obiektu docelowego, systemu operacyjnego, aplikacji lub protokołu. |  | |
|  | Rozwiązanie musi obsługiwać zapobieganie włamaniom dla protokołów HTTP, SMTP, IMAP. POP3, VOIP, NETBIOS itp. |  | |
|  | Rozwiązanie musi być wspierać weryfikację protokołów http typu Get, Head, Put, Post. |  | |
|  | Rozwiązanie musi obsługiwać wyłączenie IP z określonych sygnatur IPS. |  | |
|  | Rozwiązanie musi obsługiwać tryb działania sniffera IDS. |  | |
|  | Rozwiązanie musi obsługiwać predefiniowaną konfigurację profili IPS. |  | |
|  | Rozwiązanie musi obsługiwać tworzenie zdefiniowanych przez użytkownika sygnatur IPS. |  | |
|  | Proponowane rozwiązanie powinno wspierać szczegółowy opis predefiniowanych profili IPS. |  | |
|  | Rozwiązanie musi obsługiwać rejestrację zagrożeń IPv6: obsługa przechwytywania i pobierania pakietów IPv6 |  | |
|  | Szczegóły zagrożeń muszą obsługiwać identyfikator URI i dekodowanie danych ataków |  | |
|  | Obsługa wykrywania anomalii protokołów HTTP/DNS/FTP/MSRPC/POP3/SMTP/SUNRPC i Telnet |  | |
|  | Obsługa inspekcji Reverse Shell |  | |
|  | Blokowanie plików po rozszerzeniu dla minimum 100 typów plików |  | |
|  | Rozwiązanie musi wykrywać i blokować wrażliwe zrefowanych informacje w przesyłanych plikach dla minimum doc/docx, xls/xlsx, ppt/pptx, txt w protokołach HTTP, FTP, SMTP, POP3, IMAP, SMB |  | |
|  | Ochrona i wykrywanie skanowania protokołow IP oraz UDP |  | |
|  | Rozwiązanie musi mieć możliwość inspekcji payloudu w ramkach MPLS |  | |
|  | System musi mapować wykryte zagrożenia na taktyki MITRE ATT&CK |  | |
| **Polityki Bezpieczeństwa** | | |  | |
|  | Proponowane rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone) 、 użytkownika 、 usługi, aplikacji, IPS, w jednej regule polityki. |  | |
|  | Proponowane rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty |  | |
|  | Proponowane rozwiązanie musi obsługiwać weryfikację nadmiarowości polityki bezpieczeństwa oraz zliczanie trafień polityki przez interfejs WebUI |  | |
|  | Rozwiązanie musi obsługiwać import i eksport polityk |  | |
| **Administrowanie, Logi I Raportowanie** | | |  | |
|  | Rozwiązanie musi być obsługiwane przez WebUI i interfejs wiersza poleceń (CLI) |  | |
|  | Rozwiązanie powinno obsługiwać zarządzanie dostępem przez HTTP/HTTPS, SSH, telnet, konsolę |  | |
|  | Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe: nazwa użytkownika/hasło, plik certyfikatu HTTPS |  | |
|  | Rozwiązanie musi obsługiwać integrację systemu: SNMP, syslog. |  | |
|  | Rozwiązanie musi obsługiwać co najmniej 3 role administratora, w tym administratora, operatora i audytora |  | |
|  | Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów. |  | |
|  | Rozwiązanie musi obsługiwać serwery Radius, AD i LDAP. |  | |
|  | Rozwiązanie musi obsługiwać szybkie wdrażanie poprzez automatyczne instalowanie z USB, uruchamianie skryptów lokalnych i zdalnych. |  | |
|  | Rozwiązanie musi obsługiwać dynamiczny dashboard w czasie rzeczywistym i szczegółowe widżety monitorowania |  | |
|  | Urządzenie musi obsługiwać zarządzanie urządzeniami pamięci masowej: dostosowywanie i alarmowanie progu przestrzeni dyskowej, nakładanie starych danych, zatrzymywanie nagrywania ruchu. |  | |
|  | Urządzenie musi obsługiwać szczegółowe logi ruchu: przekazane, sesje naruszone, ruch lokalny, nieprawidłowe pakiety |  | |
|  | Urządzenie musi obsługiwać pełne logi zdarzeń: audyty aktywności systemu i zarządzania, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z Wi-Fi |  | |
|  | Urządzenie musi obsługiwać opcję rozpoznawania nazw portów usług i adresów IP. |  | |
|  | Rozwiązanie musi mieć możliwość dodania adresów IP lub MAC hostów do czarnej listy, aby zablokować dostęp przez określony czas. |  | |
|  | Rozwiązanie powinno obsługiwać blokowanie konta po kilku niepowodzeniach logowania. |  | |
|  | Rozwiązanie musi obsługiwać konfigurację zadań przechwytywania pakietów z wieloma warunkami przechwytywania pakietów w tym samym czasie oraz ich export |  | |
|  | Rozwiązanie musi obsługiwać standardowy SYSLOG i logowanie w formacie binarnym; rozproszone binarne przechowywanie logów na wielu serwerach logów |  | |
|  | Rozwiązanie powinno obsługiwać logowanie w pamięci lokalnej i/lub serwerach syslog. |  | |
|  | Rozwiązanie musi obsługiwać rejestrowanie zmiany w politykach |  | |
|  | Rozwiązanie musi obsługiwać logowanie zaufane przy użyciu opcji TCP (RFC 3195) |  | |
|  | Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. |  | |
|  | Rozwiązanie musi obsługiwać zaplanowany raport. |  | |
|  | Raport można wyeksportować w formacie PDF/HTML/WORD za pośrednictwem email lub FTP. |  | |
|  | Rozwiązanie musi umożliwić podgląd raportów w formacie HTML i PDF. |  | |
| **Wysoka Dostępność** | | |  | |
|  | Rozwiązanie musi mieć możliwość rozbudowy w tryb wysokiej dostępności |  | |
|  | Rozwiązanie musi wspierać tryby Active/Active i Active/Passive |  | |
|  | Rozwiązanie musi wspierać następujące opcje wdrażania HA: |  | |
|  | - HA z agregacją linków |  | |
|  | - Full mesh HA |  | |
|  | -Geograficznie rozproszony HA |  | |
|  | Musi istnieć możliwość synchronizacji sesji pomiędzy urządzeniami w klastrze |  | |
|  | Failover może zadziałać w przypadku awarii urządzenia lub awarii łącza |  | |

**Dostawa musi zawierać również:**

1. 36-miesięczną gwarancję producenta na wszystkie, dostarczone elementy systemu (w tym urządzenia, wkładki, kable, zasilacze, itp.)
2. Licencje na wszystkie wyszczególnione funkcje bezpieczeństwa na okres min. 36 miesięcy nie mniej niż:

dla urzadzenia pasywnego:

* 1. Threat Detection, IPS, AV, AS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C
  2. Dla urządzenia aktywnego: IPS, Baza Apikacji

1. Wsparcie techniczne dystrybutora rozwiązań w języku polskim
2. **Przedmiotem zamówienia jest stworzenie klastra HA dla urządzeń UTM(UTM – Unified Threat Management)**
3. **Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

1. **Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1. UTM – 1 szt.**  Producent: ……………………………………………………………………………………………………………………………………………….,  Nazwa produktu, model: ………………………………………………………………………………………………………………………. . | | | | |
| **Wymagania** | | | **TAK / NIE** | |
| **System musi wspierać IPv4 oraz IPv6 w zakresie:** | | |  | |
|  | Firewall. |  | |
|  | Ochrony w warstwie aplikacji. |  | |
|  | Protokołów routingu dynamicznego. |  | |
| Wraz z urządzeniem należy dostarczyć 2 wkładki sfp+ SR dedykowane do dostarczanych urządzeń. | | |  | |
| **Redundancja, monitoring i wykrywanie awarii** | | |  | |
|  | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. |  | |
|  | W ramach postępowania system musi zostać dostarczone jedno urządzenie. |  | |
|  | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  | |
|  | Monitoring stanu realizowanych połączeń VPN. |  | |
|  | System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |  | |
| **Interfejsy, Dysk, Zasilanie:** | | |  | |
|  | System realizujący funkcję Firewall musi dysponować minimum: |  | |
|  | Min.16 portami Gigabit Ethernet RJ-45. |  | |
|  | Min. 8 gniazdami SFP 1 Gbps. |  | |
|  | Min. 2 gniazdami SFP+ 10 Gbps. |  | |
|  | System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. |  | |
|  | W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  | |
|  | System musi być wyposażony w zasilanie AC. |  | |
| **Parametry wydajnościowe:** | | |  | |
|  | W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz nie mniej niż 54 tys. nowych połączeń na sekundę. |  | |
|  | Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. |  | |
|  | Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. |  | |
|  | Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps. |  | |
|  | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. |  | |
|  | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. |  | |
|  | Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. |  | |
| **Funkcje Systemu Bezpieczeństwa:** | | |  | |
|  | Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. |  | |
|  | Kontrola Aplikacji. |  | |
|  | Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. |  | |
|  | Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. |  | |
|  | Ochrona przed atakami - Intrusion Prevention System. |  | |
|  | Kontrola stron WWW. |  | |
|  | Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. |  | |
|  | Zarządzanie pasmem (QoS, Traffic shaping). |  | |
|  | Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |  | |
|  | Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. |  | |
|  | Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. |  | |
|  | Analiza ruchu szyfrowanego protokołem SSH. |  | |
|  | Detekcja urządzeń IoT. |  | |
|  | Wsparcie sygnatur dla protokołów OT urządzeń przemysłowych. |  | |
|  | Możliwość konwersji konfiguracji. |  | |
| **Polityki, Firewall** | | |  | |
|  | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. |  | |
|  | System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: |  | |
|  | Translację jeden do jeden oraz jeden do wielu. |  | |
|  | Dedykowany ALG (Application Level Gateway) dla protokołu SIP. |  | |
|  | W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |  | |
|  | Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. |  | |
|  | Amazon Web Services (AWS). |  | |
|  | Microsoft Azure |  | |
|  | Google Cloud Platform (GCP). |  | |
|  | OpenStack. |  | |
|  | VMware NSX. |  | |
| **Połączenia VPN** | | |  | |
|  | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: |  | |
|  | Wsparcie dla IKE v1 oraz v2. |  | |
|  | Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). |  | |
|  | Obsługa protokołu Diffie-Hellman grup 19 i 20. |  | |
|  | Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. |  | |
|  | Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. |  | |
|  | Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. |  | |
|  | Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. |  | |
|  | Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. |  | |
|  | Mechanizm „Split tunneling” dla połączeń Client-to-Site. |  | |
|  | System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: |  | |
|  | Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. |  | |
|  | Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |  | |
|  | Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  | |
| **Routing i obsługa łączy WAN** | | |  | |
|  | W zakresie routingu rozwiązanie powinno zapewniać obsługę: |  | |
|  | Routingu statycznego. |  | |
|  | Policy Based Routingu. |  | |
|  | Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  | |
| **Zarządzanie pasmem** | |  | |
|  | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |  | |
|  | Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. |  | |
|  | System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  | |
| **Ochrona przed malware** | |  | |
|  | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |  | |
|  | System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. |  | |
|  | System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |  | |
|  | System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. |  | |
|  | System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  | |
| **Ochrona przed atakami** | |  | |
|  | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |  | |
|  | System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. |  | |
|  | Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  | |
|  | Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. |  | |
|  | System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |  | |
|  | Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. |  | |
|  | Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  | |
| **Kontrola aplikacji** | |  | |
|  | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |  | |
|  | Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  | |
|  | Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. |  | |
|  | Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |  | |
|  | Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  | |
| **Kontrola WWW** | |  | |
|  | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. |  | |
|  | W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. |  | |
|  | Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. |  | |
|  | Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. |  | |
|  | Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. |  | |
|  | Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |  | |
|  | W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  | |
| **Uwierzytelnianie użytkowników w ramach sesji** | |  | |
|  | System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: |  | |
|  | Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. |  | |
|  | Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. |  | |
|  | Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. |  | |
|  | Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. |  | |
|  | Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  | |
| **Zarządzanie** | |  | |
|  | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. |  | |
|  | Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |  | |
|  | Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |  | |
|  | 4System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. |  | |
|  | System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |  | |
|  | Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |  | |
|  | Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  | |
| **Logowanie** | |  | |
|  | Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. |  | |
|  | W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. |  | |
|  | Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. |  | |
|  | Musi istnieć możliwość logowania do serwera SYSLOG. |  | |
| **Certyfikaty** | |  | |
|  | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: |  | |
|  | ICSA lub EAL4 dla funkcji Firewall. |  | |
| **Serwisy i licencje** | | |  | |
| W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: | | |  | |
|  | Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy. |  | |
| **Gwarancja oraz wsparcie** | | |  | |
| 1. | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  | |

1. **Wymagania dodatkowe**Zamawiający wymaga również aby dostarczone rozwiązanie działało redundantnie z obecnie działającym sprzętem w jednostce Zamawiającego. Ponadto Wykonawca winien zapewnić odpowiednie licencje do poprawnego działania obu urządzeń ale z uwzględnieniem dostarczenia wyższej licencji niż zastosowana obecnie w celu zwiększenie bezpieczeństwa w sieci Zamawiającego.
2. **Stan obecny**Aktualnie Zamawiający posiada urządzenie firmy FortiGate-100F.
3. **Przedmiotem zamówienia jest system klasy EDR**
4. **Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:**

|  |  |  |
| --- | --- | --- |
| **1. System klasy EDR**  Producent: ………………………………………………………………………………………………………………………………………………., | | |
| **Wymagania:** | | **TAK / NIE** |
| **Zamawiający wymaga , aby system KLASY EDR umożliwiał pełne wsparcie dla systemów**  **operacyjnych komputerów:** | |  |
|  | Windows 11 |  |
|  | Windows 10 |  |
|  | Windows 8.1 |  |
|  | Windows 8 |  |
|  | Windows 7 SP1 |  |
| **Zamawiający wymaga , aby system KLASY EDR umożliwiał pełne wsparcie dla systemów**  **operacyjnych serwerów:** | |  |
|  | Windows Server 2016 i nowszych |  |
|  | Oracle Linux 7 i nowszych |  |
|  | CentOS 7 i nowszych. |  |
|  | Ubuntu 16.04. i nowszych |  |
|  | macOS |  |
| **Zamawiający wymaga , aby system KLASY EDR zawierał ochronę środowisk wirtualnych (SVE):** | |  |
|  | VMware vSphere and vCenter Server min wersja 6.5 |  |
|  | Microsoft Hyper-V Server min. 2016(including Hyper-V Hypervisor) |  |
|  | Oracle VM VirtualBox |  |
| **Wymagane warunki bezwzględne ochrony antywirusowej i antyspyware** | |  |
|  | System powinien zawierać pełną ochronę przed wirusami, trojanami, robakami i innymi  zagrożeniami |  |
|  | System powinien zawierać pomoc techniczną, interfejs oraz dokumentacja dostarczoną i  świadczoną w języku polskim. |  |
|  | System powinien zawierać wykrywanie zagrożeń i analizę procesów technikami  Heurystycznymi. |  |
|  | System powinien zawierać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware,  spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. |  |
|  | System powinien zawierać wbudowaną technologie do ochrony przed rootkitami. |  |
|  | System powinien zawierać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i  wykonywanych plików. |  |
|  | System powinien zawierać możliwość skanowania całego dysku, wybranych katalogów lub  pojedynczych plików "na żądanie". |  |
|  | System powinien zawierać skanowanie "na żądanie" pojedynczych plików lub katalogów  przy pomocy skrótu w menu kontekstowym. |  |
|  | System powinien zawierać możliwość skanowania dysków sieciowych i dysków  przenośnych. |  |
|  | System powinien zawierać skanowanie plików spakowanych i skompresowanych. |  |
|  | System powinien zawierać możliwość dodawania wykluczeń na podstawie   * Plik * Folder * Rozszerzenie * Proces * Hash pliku * Hash certyfikatu * Nazwa zagrożenia * Wiersz poleceń * IP/maska |  |
|  | System powinien zawierać skanowanie i oczyszczanie w czasie rzeczywistym poczty  przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook. |  |
|  | System powinien zawierać skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie"  (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego  zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego) |  |
|  | System powinien zawierać automatyczną integrację skanera POP3 z dowolnym klientem  pocztowym bez konieczności zmian w konfiguracji. |  |
|  | System powinien zawierać skanowanie ruchu HTTP na poziomie stacji roboczych.  Zainfekowany ruch powinien być automatycznie blokowany a użytkownikowi wyświetlane  jest stosowne powiadomienie. |  |
|  | System powinien zawierać blokowanie możliwości przeglądania wybranych stron  internetowych. Listę blokowanych stron internetowych określa administrator. |  |
|  | System powinien zawierać automatyczną integrację z dowolną przeglądarką internetową  bez konieczności zmian w konfiguracji. |  |
|  | System powinien zawierać możliwość definiowania czy pliki z kwarantanny mają być  przesyłane do producenta i co jaki czas ma się ta czynność odbywać. |  |
|  | Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych  protokołów HTTPS, RDP, FTPS, SCP/SSH. |  |
|  | Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji  zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. |  |
|  | System powinien zawierać możliwość zabezpieczenia programu przed deinstalacją przez  niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego  administratora, przy próbie deinstalacji program będzie pytał o hasło. |  |
|  | System powinien zawierać po kliknięciu prawym klawiszem myszy na ikonie programu i  wybraniu opcji : O programie” możliwość zdefiniowania przez administratora danych do  3 pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony,  numer telefonu do administratora ochrony. |  |
|  | System powinien zawierać w GUI programu na punkcie końcowym możliwość wyświetlenia  aktualnej wersji produktu i aktualnej wersji silników. |  |
|  | System powinien zawierać w GUI programu możliwość wyświetlenia kiedy była  przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. |  |
|  | System powinien zawierać automatyczną aktualizacje baz wirusów i innych zagrożeń. |  |
|  | System powinien zawierać obsługę pobierania aktualizacji za pośrednictwem serwera proxy. |  |
|  | Praca programu musi być niezauważalna dla użytkownika. |  |
|  | System powinien zawierać dziennik zdarzeń rejestrujący informacje na temat znalezionych  zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio  na stacji roboczej. |  |
|  | Oprogramowanie klienckie powinno posiadać wbudowaną funkcję do komunikacji z  serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na  stacji roboczej. |  |
|  | System powinien zawierać możliwość odblokowania ustawień programu po wpisaniu hasła. |  |
|  | System powinien zawierać wbudowany moduł kontroli urządzeń (możliwość blokowania  całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego  interfejsu w komputerze zostanie podłączone urządzenie). |  |
|  | System powinien zawierać możliwość dodania zaufanych urządzeń bezpośrednio z konsoli  administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia  lub ID produktu. |  |
|  | System powinien zawierać wbudowaną zaporę osobistą, umożliwiającą tworzenie reguł na  podstawie aplikacji oraz ruchu sieciowego. |  |
|  | System powinien zawierać wbudowany IDS. |  |
|  | System powinien zawierać możliwość tworzenia list sieci zaufanych. |  |
|  | System powinien zawierać możliwość dezaktywacji funkcji zapory sieciowej. |  |
|  | System powinien zawierać możliwość ustawienie skanowania z niskim priorytetem  zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. |  |
|  | System powinien zawierać funkcję ochrony przeciwko znanym zagrożeniom typu  ransomware. |  |
|  | System powinien zawierać mechanizm który wspiera powrót do ostatnich działających  wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji. |  |
|  | System powinien umożliwiać użytkownikowi na punkcie końcowym możliwość opóźnienia  restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach  bezpieczeństwa). |  |
|  | System powinien umożliwiać wymuszenie połączenia szyfrowanego dla punktów  końcowych Windows oraz Linux do serwera zarządzającego. |  |
|  | System powinien posiadać system zarządzania ryzykiem – Zintegrowany z konsolą  zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie  punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza  stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:  a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować  z podziałem na typ błędnej konfiguracji:  -Ochrony przeglądarki internetowej  -Sieć i poświadczenia  -Błędna konfiguracja systemu operacyjnego  System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty  procentowe.  b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy  tym numer CVE tych luk.  c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie  podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu  użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.  d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na  podstawie harmonogramu lub pojedynczo utworzonego zadania.  e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i  luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w  procentach.  f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania  oraz jakie jest ich nasilenie |  |
|  | System powinien posiadać wbudowaną ochronę przed exploitami wyposażona w  minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia  każdej z nich oraz dająca możliwość dodania własnych procesów. |  |
|  | System powinien umożliwiać ochronę przed atakami sieciowymi – Mechanizm obronny  przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w  sieci. |  |
|  | System powinien umożliwiać ochronę przed ransomware - możliwość wykrywania i  blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony  lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w  przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.  Formaty plików jakie mogą być odzyskane:  *3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dx*  *f|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|o*  *dm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|ps*  *t|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx*  *|xml|* |  |
|  | System powinien posiadać zintegrowany sandbox po stronie producenta który pozwala na  analizę pliku:  a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie  uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora  b) Możliwość przesłania archiwum zabezpieczonego hasłem  c) Możliwość przesłania adresu URL  d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek  pojedynczo. |  |
|  | Wbudowany sandbox powinien działać w trybie monitorowania i blokowania. |  |
|  | Wbudowany sandbox powinien oferować działania naprawcze takie jak dezynfekcja lub  przeniesienie do kwarantanny. |  |
|  | Wbudowany sandbox powinien oferować opcję wstępnego filtrowania zawartości która  skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego  zachowania. |  |
|  | Wbudowany sandbox powinien posiadać opcję która pozwala na dodanie określonych  rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. |  |
|  | Oprogramowanie powinno pozwalać na skanowanie punktów końcowych pod kątem  wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują: |  |
| **Wymagane warunki bezwzględne ochrony maszyn wirtualnych:** | |  |
|  | System powinien zawierać możliwość określenia jak długo maja być przechowywane  zdarzenia na stacji roboczej. |  |
|  | System powinien zawierać możliwość zabezpieczenia hasłem klienta przed  odinstalowaniem. |  |
|  | System powinien zawierać możliwość wskazania katalogów które mogą być chronione w  czasie rzeczywistym. |  |
|  | System powinien zawierać możliwość określenia co jaki czas mają być wysyłane pliki z  kwarantanny do producenta. |  |
|  | System powinien zawierać możliwość wskazania do jakiego serwera ochrony maja się łączyć  klienci maszyn wirtualnych. |  |
| **Warunki bezwzględne ochrony stacji roboczych i serwerów Windows:** | |  |
|  | System powinien zawierać pełną ochronę przed wirusami, trojanami, robakami i innymi  zagrożeniami. |  |
|  | System powinien zawierać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware,  spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. |  |
|  | System powinien zawierać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i  wykonywanych plików. |  |
|  | System powinien zawierać możliwość skanowania całego dysku, wybranych katalogów lub  pojedynczych plików "na żądanie". |  |
|  | System powinien zawierać skanowanie "na żądanie" pojedynczych plików lub katalogów  przy pomocy skrótu w menu kontekstowym |  |
|  | System powinien zawierać skanowanie plików spakowanych i skompresowanych. |  |
|  | System powinien zawierać oprogramowanie monitora antywirusowego uruchamianego  automatycznie w momencie startu systemu operacyjnego komputera, który działa  nieprzerwanie do momentu zamknięcia systemu operacyjnego. |  |
|  | System powinien zawierać możliwość zablokowania hasłem odinstalowania programu. |  |
|  | System powinien zawierać możliwość raportowania zdarzeń informacyjnych. |  |
|  | Program powinien posiadać możliwość włączenia/wyłączenia powiadomień określonego  rodzaju. |  |
|  | Program powinien posiadać możliwość skanowania jedynie nowych nie zmienionych  plików. |  |
|  | Program powinien mieć wbudowany skaner wyszukiwania rootkitów |  |
|  | Program powinien posiadać możliwość odblokowania ustawień programu po wpisaniu hasła. |  |
|  | Program powinien posiadać możliwość uruchomienia zadania skanowania z niskim  priorytetem |  |
|  | Program powinien posiadać możliwość wykorzystania dodatkowej maszyny wirtualnej  która przejmie role silnika skanującego. |  |
|  | Program powinien posiadać możliwość określenia jak długo maja być przechowywane  zdarzenia na stacji roboczej. |  |
|  | Program powinien posiadać możliwość zabezpieczenia hasłem klienta przed  odinstalowaniem. |  |
|  | Program powinien posiadać dla maszyn z systemem Linux możliwość wskazania katalogów  które mogą być chronione w czasie rzeczywistym. |  |
| **Warunki bezwzględne konsoli zdalnej administracji** | |  |
|  | Program powinien posiadać centralną instalację i zarządzanie programami służącymi do  ochrony stacji roboczych i serwerów plikowych Windows. |  |
|  | Program powinien posiadać centralną konfigurację i zarządzanie ochroną antywirusową,  antyspyware’ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich  stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera  zarządzającego. |  |
|  | Program powinien posiadać możliwość integracji wielu domen Active Directory. |  |
|  | Program powinien posiadać możliwość uruchomienia zdalnego skanowania wybranych  stacji roboczych. |  |
|  | Program powinien posiadać możliwość sprawdzenia z centralnej konsoli zarządzającej  stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy  wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej  aktualizacji oraz przypisanej polityki). |  |
|  | Program powinien posiadać możliwość utworzenia konta użytkownika z rolą administrator  firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi. |  |
|  | Program powinien posiadać możliwość sprawdzenia z centralnej konsoli zarządzającej  podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu  operacyjnego. |  |
|  | Program powinien posiadać możliwość centralnej aktualizacji stacji roboczych z serwera w  sieci lokalnej lub Internetu. |  |
|  | Program powinien posiadać możliwość wysłania linku instalacyjnego bezpośrednio z  poziomu konsoli administracyjnej. |  |
|  | Program powinien posiadać możliwość zmiany konfiguracji na stacjach i serwerach z  poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu  odpowiedniej opcji w politykach bezpieczeństwa. |  |
|  | Program powinien posiadać możliwość uruchomienia centralnej konsoli jedynie z poziomu  przeglądarki internetowej. |  |
|  | Program powinien posiadać możliwość ręcznego (na żądanie) i automatycznego  generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do  formatu: pdf i csv. |  |
|  | Program powinien posiadać raport generowany według harmonogramu z możliwością  automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w  formie archiwum zip. |  |
|  | Program powinien posiadać możliwość dodania etykiety do stacji roboczej. |  |
|  | Program powinien posiadać możliwość dezinstalacji oprogramowania antywirusowego  innych firm w trakcie instalacji zdalnej. |  |
|  | Program powinien posiadać możliwość definiowania czy pliki z kwarantanny mają być  przesyłane do producenta i co jaki czas ma się ta czynność odbywać. |  |
|  | Użytkownik powinien w całym okresie trwania subskrypcji mieć prawo do korzystania z  bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty  elektronicznej. |  |
|  | Program powinien posiadać możliwość automatycznego przypisywania polityk na  podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie:  -Zakres adresów IP/IP  -Adres bramy  -Adres serwera WINS  -Adres serwera DNS  -Połączenie DHCP sufiksów DNS  -Punkt końcowy może rozwiązać hosta  -Typ sieci  -Nazwa hosta |  |
|  | Program powinien posiadać możliwość zablokowania konta w konsoli jeżeli użytkownik  tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem. |  |
|  | Program powinien posiadać funkcję pojedynczego logowania – Single Sign-on (SSO). |  |
|  | Program powinien posiadać możliwość naprawy instalacji z poziomu konsoli. |  |
|  | Program powinien posiadać raport streszczający - Możliwość podglądu raportu który  streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:  -Zarządzane punkty końcowe  -Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows,  serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne  -Pięć najczęściej blokowanych zagrożeń  -Podział zagrożeń na urządzenia takie jak stacje robocze i serwery  -Status incydentów bezpieczeństwa które wystąpiły  -Stan modułów punktów końcowych  -Ocena ryzyka firmy  -Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie,  phishing, oszustwa.  -Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny  dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware |  |
|  | Program powinien posiadać Integracja z vCenter Server. |  |
|  | Program powinien posiadać tworzenie osobnych polityk dla fizycznych komputerów,  urządzeń mobilnych oraz maszyn wirtualnych. |  |
|  | Program powinien posiadać możliwość wygenerowania i pobrania logów ze stacji roboczej  z poziomu konsoli zarządzającej. |  |
|  | Program powinien posiadać funkcję kontroli aplikacji która daje możliwość skanowania  punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub  dostępnych procesów. |  |
|  | Program powinien posiadać Funkcję kontroli aplikacji która pozwala na zablokowanie  wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. |  |
|  | Program powinien posiadać możliwość wyświetlenia czy punkt końcowy jest serwerem czy  stacją roboczą. |  |
|  | Program powinien posiadać możliwość wyświetlenia informacji czy zainstalowany na  punkcie końcowym system operacyjny to Windows, Linux, MacOS. |  |
|  | Program powinien posiadać możliwość wyświetlenia wersji systemu operacyjnego  zainstalowanego na punkcie końcowym. |  |
|  | Program powinien posiadać możliwość filtrowania punktów końcowych, które były online  w ciągu ostatnich 24 godzin, 7 lub 30 dni. |  |
|  | Program powinien posiadać menu tworzenia paczek instalacyjnych dla stacji roboczych  Windows, Serwerów Windows, Linux. |  |
|  | Program powinien posiadać możliwość scentralizowanego podglądu wykrytych zagrożeń z  wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty,  kategorii, typu zagrożenia, działań naprawczych i innych. |  |
|  | Program powinien posiadać oprogramowanie które umożliwia ochronę kontenerów  instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera  Linux i kontenerów w czasie rzeczywistym. |  |
|  | Program powinien posiadać oprogramowanie które musi skanować nośniki USB zanim  użytkownik zaloguje się do systemu Windows. |  |
| **Warunki bezwzględne komponentów EDR** | |  |
| System powinien składać się z elementów: | |  |
|  | Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu  końcowego i zachowania aplikacji. |  |
|  | Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik  EDR. |  |
|  | Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem  Windows, aby rozszerzyć już zainstalowaną ochronę. |  |
| System powinien monitorować zdarzenia na punktach końcowych w poszukiwaniu oznak ataku i  wywoływanie incydentów po wykryciu takiej aktywności. | |  |
|  | Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji. |  |
|  | Zgłaszanie wszystkich naruszeń jako incydent w module EDR. |  |
| **Warunki bezwzględne konsoli zarządzającej**  **(Konsola powinna być w wersji Cloud – serwer administracyjny po stronie producenta)** | |  |
| 1. | Konsola powinna zawierać Telemetrie - Możliwość przesyłania nieprzetworzonych danych  bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM. |  |
| 2. | System zarządzania ryzykiem – Powinien być zintegrowany z konsolą zarządzającą system który  pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka  powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa  większe ryzyko. System ponadto musi posiadać:  a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z  podziałem na typ błędnej konfiguracji:   * Ochrony przeglądarki internetowej * Sieć i poświadczenia * Błędna konfiguracja systemu operacyjnego   System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.  b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym  numer CVE tych luk.  c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje  użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy  oraz jakie jest jego nasilenie.  d) System który pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na  podstawie harmonogramu lub pojedynczo utworzonego zadania.  e) System który pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w  aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.  f) System który pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz  jakie jest ich nasilenie. |  |
| 3. | Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.  a) Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć  kolejnych prób logowania nieprawidłowym hasłem.  b) Możliwość naprawy instalacji z poziomu konsoli.  c) Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z  rozróżnieniem na takie sekcje jak:   * Zarządzane punkty końcowe * Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne * Pięć najczęściej blokowanych zagrożeń * Podział zagrożeń na urządzenia takie jak stacje robocze i serwery * Status incydentów bezpieczeństwa które wystąpiły * Stan modułów punktów końcowych * Ocena ryzyka firmy * Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa. * Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware. |  |
| 4. | Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w  jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych. |  |
| 5. | Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:   * historii powłoki * wczytywania bibliotek .dll z podejrzanej lokalizacji * Sesji logowania z użyciem jawnych danych uwierzytelniających * Elementów startowych Windows * Arp cache * Ip forwarding * Pobierania listy wszystkich otwartych plików dla każdego procesu w systemie docelowym. * Listy zamontowanych nośników * Filtrów ip tables * Połączenia TLS które używają certyfikatów self-signed * Używania rozszerzenia w przeglądarce Chrome * Używania rozszerzenia w przeglądarce Firefox * Używania rozszerzenia w przeglądarce Safari * Źródeł apt w systemach Linux * Wyświetlania zainstalowanych pakietów DEB * Wyświetlania zainstalowanych pakietów RPM * Pakietów Python zainstalowane w systemie * Listy zainstalowanych użytkowników którzy łączyli się z publicznych adresów IP * Listy użytkowników którzy zostali utworzeni w ciągu ostatnich 30 dni(Linux) * Czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS * Czy Kontrola Kont Użytkowników(UAC) jest wyłączona * Czy SecureBoot jest włączony * Listy zapamiętanych połączeń bezprzewodowych * Czy zmienił się domyślny folder startowy użytkownika * Czy zmienił się domyślny folder startowy maszyny |  |