***Szczegółowy Opis Przedmiotu Zamówienia***

**1. Wykonanie Diagnozy cyberbezpieczeństwa**Wykonanie diagnozy bezpieczeństwa w oparciu o ankietę zgodności z normami ISO 27001 oraz przekazanie wyniku diagnozy w formie PDF. Wynik diagnozy powinien zawierać rekomendację podniesienia poziomów bezpieczeństwa w każdym z obszarów oraz wykazać stan procentowy zabezpieczeń w każdym obszarze (0%-100%) na dzień przeprowadzenia diagnozy.

Zakres badanych obszarów :

1. Polityka Bezpieczeństwa IT

2. Budowanie świadomości

3. Rola Właściciela Biznesowego

4. Proces zarządzania ryzykiem IT

5. Plan Ciągłości Działania

6. Zewnętrzni dostawcy usług IT

7. Dobre praktyki w obszarze bezpieczeństwa IT

8. Zarządzanie incydentem

9. Zarządzanie uprawnieniami

10. Nadzór nad uprawnieniami

11. Change Management & Software Development

12. Zarządzanie konfiguracją

13. Backup

14. Bezpieczeństwo fizyczne

15. Pomieszczenia techniczne IT

16. Bezpieczeństwo serwerowni

17. Technologie w obszarze bezpieczeństwa IT

18. Bezpieczeństwo infrastruktury LAN/WiFi

19. Bezpieczeństwo usług chmurowych

20. Bezpieczeństwo środowiska pracy

**Termin realizacji usługi : do 3 dni po podpisaniu umowy ; wynik diagnozy wraz z rekomendacjami naprawczymi do 5 dni po podpisaniu umowy.**

**2. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**

Opracowanie dokumentacji i wdrożenie procedur bezpieczeństwa zgodnego z normą ISO 27001

1. Opracowanie dokumentacji wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo, o której mowa w art. 14 ust. 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2020 r., poz. 1369 – zwanej dalej „Ustawą KSC”) w podejmowanych czynnościach i wykonywanych zadaniach nałożonych obowiązkami prawnymi Ustawy KSC, powołanej przez Zleceniodawcę będącego operatorem usługi kluczowej w rozumieniu art. 5 Ustawy KSC t.j. w zakresie dotyczącym:
2. opracowania zasad zgłoszenia incydentu poważnego do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV,
3. opracowania dokumentacji dot. współdziałania wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwa z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV w przypadku wystąpienia incydentu poważnego i incydentu krytycznego,
4. Opracowanie dokumentacji dotyczącej:
5. systemu zarządzania bezpieczeństwem informacji, wytworzonej zgodnie z wymaganiami normy PN-EN ISO/IEC 27001,
6. ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa w zakresie:

- charakterystyki usługi kluczowej oraz infrastruktury,

- szacowania ryzyka dla obiektów infrastruktury,

- oceny aktualnego stanu ochrony infrastruktury (plan postępowania z ryzykiem),

- opisu zabezpieczeń technicznych obiektów infrastruktury,

- zasad organizacji i wykonywania ochrony fizycznej infrastruktury,

1. systemu zarządzania ciągłością działania usługi kluczowej, wytworzonej zgodnie z wymaganiami normy PN-EN ISO 22301;

Wykonawca w ramach wynagrodzenia zobowiązany jest do przeniesienia na Zamawiającego autorskich praw do wszelkiej opracowanej i wytworzonej w ramach niniejszego zamówienia dokumentacji.

**Termin realizacji: do dnia 28 listopada**

**3. Wykonanie Audytu bezpieczeństwa**

Przeprowadzenie audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej (Zamawiającego) zgodnie z wymogami Ustawy o krajowym systemie cyberbezpieczeństwa, aktów powiązanych oraz szablonem sprawozdania z audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa rekomendowanym przez Ministerstwo Cyfryzacji .

Sporządzenie pisemnego sprawozdanie na podstawie zebranych przez audytorów dokumentów i dowodów z przeprowadzonego audytu i przekazanie ich operatorowi usługi kluczowej (Zamawiającemu) wraz z dokumentacją z przeprowadzonego audytu w celu przekazania przez Zamawiającego na wniosek do:  
- organu właściwego do spraw cyberbezpieczeństwa;  
- dyrektora Rządowego Centrum Bezpieczeństwa - w przypadku, gdy operator usługi kluczowej jest jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;  
- Szefa Agencji Bezpieczeństwa Wewnętrznego.

Celem audytu jest również wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z zarządzeniem NR 68/2022/BBIICD (wraz z późniejszymi zmianami) oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

Audyt bezpieczeństwa (zgodnie z załącznikiem do Zarządzenia nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia) może być przeprowadzony przez:

1. jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2. co najmniej dwóch audytorów posiadających:
3. certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
4. co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
5. co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1. Certified Internal Auditor (CIA);
2. Certified Information System Auditor (CISA);
3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
5. Certified Information Security Manager (CISM);
6. Certified in Risk and Information Systems Control (CRISC);
7. Certified in the Governance of Enterprise IT (CGEIT);
8. Certified Information Systems Security Professional (CISSP);
9. Systems Security Certified Practitioner (SSCP);
10. Certified Reliability Professional;
11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

**Termin realizacji: do dnia 28 listopada**

**4.Przeprowadzenie Szkolenia**

W ramach szkolenia zostaną zorganizowane konsultacje z kadrą zarządzającą. Tematem dyskusji będzie kontekst cyberbezpieczeństwa i prewencji w jednostkach ochrony zdrowia oraz tematyka  zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).  
Szkolenie powinno zostać zrealizowane w formie stacjonarnej lub w szczególnym przypadku (np. wystąpienie uwarunkowań epidemiologicznych) w formie online za wcześniejszą zgodą Zamawiającego. Szkolenie dla grupy do 30 osób.

Minimalny zakres szkolenia :

* Badanie potrzeb szkoleniowych uczestników - pretest,
* Dane medyczne i osobowe— kontekst i ryzyka przetwarzanie,
* Zasady postępowania z danymi szczególnie wrażliwymi,
* Zgłaszanie incydentów dot. wycieku danych medycznych i osobowych,
* Przykłady ataków hackerskich na szpitale i placówki ochrony zdrowia,
* Czym jest cyberbezpieczeństwo,
* Metody nieautoryzowanego pozyskania danych wraz z przykładami,
* Zagrożenia w sieci (w tym phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa) wraz z przykładami,
* Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, oraz wewnętrzna bezpieczna komunikacja,
* Bezpieczne hasła, managery haseł, autoryzacja dwuetapowa, klucze sprzętowe,
* Metody obrony oraz przeciwdziałania w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, programowaniem mogącym zablokować dostęp do urządzeń firmowych, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste,
* Bezpieczne korzystanie z mediów społecznościowych,
* Bezpieczne korzystanie ze smartfonów,
* Wskazanie miejsc organizacji, oraz informacji, które należy chronić, by zniwelować ryzyko narażenia firmy na straty finansowe,
* Wskazanie zasad cyberhigieny,
* Ewaluacja szkolenia - posttest.

Wymagania dla trenera :

Szkolenia muszą być przeprowadzone przez trenera, który przeprowadził w przeciągu ostatnich trzech lat:

* co najmniej 3 akredytowane szkolenia audytorów wiodących systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 lub,
* co najmniej 3 akredytowane szkolenia Audytora bezpieczeństwa informacji ISO 27001 lub,
* co najmniej 3 akredytowane szkolenia Managera bezpieczeństwa informacji ISO 27001.

**Minimalny czas trwania szkolenia 1 dzień/6-7h**

**Termin realizacji: do dnia 15 listopada**

**5.Dostawa Systemu ochrony klasy GRC (Governance, risk management and compliance)**

**Minimalne wymagania dla oprogramowania :**

1. Automatyzacja analizy zdarzeń w systemach operacyjnych Microsoft pod kątem identyfikowania zagrożeń i incydentów bezpieczeństwa IT – system musi rozpoznawać zagrożenia wynikające z niestosowania dobrych praktyk w obszarze zarządzania kontami uprzywilejowanymi (np. zagrożenie ujawnienia hasła zapisanego w pliku tekstowym) oraz w zakresie praktyk stosowanych przez użytkowników (np. zagrożenie wykorzystania konta imiennego przez wielu pracowników).
2. System musi zapewniać ochronę użytkownika poprzez blokowanie komunikacji z źródłami zagrożeń wskazanymi przez platformę N6 CERT Polska.
3. System musi umożliwiać zarządzanie podatnościami informatycznymi. Zarządzanie należy interpretować jako funkcjonalność systemu zadaniowego, w którym to menager może wybierać i przypisywać do realizacji operatorom podatności do usunięcia. System powinien także automatyzować tworzenie zadań, jeśli nie zostanie to zrobione w sposób manualny.
4. System powinien analizować pełen kontekst procesu zarządzania bezpieczeństwem IT i w zależności od roli w organizacji, odpowiednio transformować i prezentować informacje odbiorcy. Jako minimum, role w systemie powinny być dwie: 1) Administrator usług IT, dla którego prezentowane są informacje techniczne, umożliwiające reagowanie i usuwanie zagrożenia w środowisku IT; 2) Właściciel Biznesowy usług IT w organizacji (Zarząd), dla którego prezentowane są informacje zarządcze, np. o efektywności procesu zarządzania bezpieczeństwem IT.
5. Samodzielna ocena dojrzałości organizacyjnej w zakresie zarządzania bezpieczeństwem IT. System musi umożliwiać wykonanie samodzielnego audytu w celu identyfikacji słabości organizacyjnych oraz procesowych w odniesieniu do stosowanych w tym zakresie rynkowych praktyk.
6. System musi umożliwiać wybór standardu, normy bądź innego wymogu formalno-prawnego, wobec którego będzie dokonywał oceny zgodności organizacyjnej.
7. System musi umożliwiać tworzenie własnego zakresu audytu, np. na potrzebę weryfikowania zgodności dostawców, z którymi organizacja ma podpisaną umowę.
8. System musi proponować rekomendacje do wskazanych nieprawidłowości.
9. System musi umożliwiać nadzór nad wdrażaniem działań naprawczych do zaobserwowanych nieprawidłowości.
10. System musi posiadać mechanizm tworzenia raportów czytelnie wskazujących jakie obszary były audytowane, jakie rekomendacje zostały wskazane oraz jaki jest status prac nad ich wdrożeniem.
11. System musi umożliwiać bezpieczną autoryzację użytkownika poprzez wieloskładnikowe uwierzytelnianie (bądź zapewnić możliwość integracji z zewnętrznymi systemami autoryzacji MFA).

**Integracje:**

1. System musi zapewniać stały dostęp do informacji o zagrożeniach w polskiej sieci Internet publikowanych poprzez z integrację z platformą N6 CERT Polska.
2. System musi posiadać moduł alarmowania o wybranych incydentach oraz zagrożeniach bezpieczeństwa IT. System powinien posiadać możliwość integracji z wybranymi operatorami bramek sms.

**Termin uruchomienia oprogramowania do 15 listopada 2022r.**

**Licencja na 36 miesięcy.**

**6.Dostawa systemu SIEM (security information and event management​)**

**Wymagania funkcjonalne dla oprogramowania**

1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL;
2. System musi pracować w oparciu o architekturę Linux;
3. System musi mieć możliwość centralnego zbierania i zarządzania logami;
4. System działać w trybie zbliżonym do rzeczywistego;
5. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu;
6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu;
7. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie;
8. System musi zapewniać retencję danych w okresie minimum 365 dni;
9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu;
10. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska;
11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja;
12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu;
13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji ;
14. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu;
15. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.;
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.;
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer;
18. Interfejs musi posiadać angielską lub polską wersję językową;
19. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1);
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem;
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius;
22. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej;
23. System musi wspierać mechanizm logowania typu Single Sign On;
24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników;
25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami;
26. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika;
27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień;
28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych;
29. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie;
30. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant;
31. System musi pozwalać na tworzenie parserów z poziomu GUI;
32. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning;
33. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów;
34. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP;
35. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach;
36. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych;
37. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:

* Syslog,
* WEF,
* Flat file,
* Event log,
* WMI,
* SNMP trap,
* XML,
* JSON,
* JDBC/ODBC
* CSV,
* Email,

Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.

1. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure;
2. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem;
3. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe;
4. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów;
5. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera;
6. System musi posiadać predefiniowany zestaw parserów zdarzeń;
7. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta;
8. System musi wspierać geolokalizację zdarzeń na bazie adresów IP;
9. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania;
10. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach;
11. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach;
12. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
13. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
14. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
15. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
16. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
17. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
18. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
19. Wykrycia dowolnej treści w logach,
20. Wykrycia wystąpienia wartości pola na wybranej liście,
21. Wykrycia niewystępowania wartości pola na wybranej liście,
22. Wykrycia zmiany jednego z kilku pól,
23. Wykrycia zdarzeń występujących z zadaną częstotliwością,
24. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
25. Wykrycia zaniku Wiadomości,
26. Wykrycia nowej wartości pola w zadanym okresie czasu,
27. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
28. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
29. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
30. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
31. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
32. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
33. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
34. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
35. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
36. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
37. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
38. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
39. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
40. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
41. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
42. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
43. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
44. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
45. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
46. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem community producenta na okres 1 roku.
47. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
48. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
49. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
50. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
51. System musi umożliwiać integrację z Mitre ATT@CK.

**Licencja na własność.**

**Termin uruchomienia oprogramowania do 15 listopada 2022 roku**

**7.Dostawa Next Generation Firewall**

**Funkcjonalność urządzenia w zakresie Firewall:**

* Firewall musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2)
* obsługa protokołów dynamicznego routingu: RIP, OSPF i BGP
* Firewall musi obsługiwać policy based routing
* Firewall musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie
* Firewall musi obsługiwać DHPC v6 na zewnętrznym interfejsie
* Firewall musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP, jako bridge (transpartent mode) lub z tym samym adresem IP na wszystkich portach.
* Firewall musi mieć możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu.
* Firewall musi mieć możliwość obsługi łącza zapasowego typu LTE
* Firewall musi obsługiwać Dynamic DNS
* Firewall musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1
* Firewall musi obsługiwać translację portów: PAT
* Firewall musi obsługiwać IPSec NAT Traversa
* Firewall musi obsługiwać mechanizm policy-based NAT
* Firewall musi obsługiwać VLAN 802.1Q
* Firewall musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów
* Firewall musi obsługiwać pracę jako serwer DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
* Firewall musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP
* Firewall musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
* Firewall musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników.
* Firewall musi umożliwiać transparentne uwierzytelnianie użytkowników przez Active Directory.
* Urządzenie musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp
* Urządzenie nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
* Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji
* Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
* Firewall musi obsługiwać mechanizmy Protocol Anomaly Detection (PAD) dla najpopularniejszych protokołów.
* Firewall musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: http, https, ftp, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP
* Firewall musi zapewniać ochronę z wykorzystaniem mechanizmów IPS
* Firewall musi zapewniać ochronę antywirusową dla obsługiwanych protokołów
* Firewall musi zapewniać możliwość filtrowania URL
* Firewall musi zapewniać inspekcję ruchu szyfrowanego https
* Firewall musi zapewniać ochronę przed niechcianą pocztą (AntySPAM)
* Firewall musi zapewniać rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.
* Urządzenie musi mieć możliwość filtrowania treści według typu MIME
* Urządzenie musi umożliwiać sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji
* Firewall musi udostępniać mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych.
* Firewall musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site

**Wydajność firewall**

* Firewall musi zapewnić obsługę na poziomie minimalnym:
* 18 Gpbs dla pracy w trybie firewall,
* 2.4 Gbps dla pracy w trybie UTM (z włączonymi mechanizmami AV and IPS)
* Firewall musi obsługiwać 4 500 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 98 tys. nowych połączeń na sekundę
* Ilość obsługiwanych sieci VLAN: min 100
* Minimalna ilość portów 10/100/1000 BaseT: 8 z możliwością rozbudowy

**Funkcje VPN**

* Urządzenie musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz TLS
* Urządzenie musi w zakresie IPSec site-to-site VPN współpracować z rozwiązaniami innych producentów
* Rozwiązanie musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256
* Rozwiązanie musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert.
* Wsparcie dla Dead Peer Detection (DPD)
* Urządzenie musi obsługiwać IKEv1 i IKEv2
* Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i Web
* Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP
* Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu
* Urządzenie musi obsługiwać statyczne i dynamiczne (routowane) połaczenia VPN do dostawców chmury obliczeniowej (AWS i MS Azzure)
* Urządzenie musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP.
* Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android
* Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu
* Urządzenie ma zapewnia funkcję portalu dostępowego chronionego przez szyfrowanie https (TLS)

**Wydajność VPN**

* Przepustowość VPN nie mniejsza niż 5.2 Gbps
* Obsługa nie mniej niż: 250 tuneli IPSec site-to-site
* Obsługa nie mniej niż: 250 tuneli client-to-site

**Filtrowanie zawartości URL**

* Urządzenie musi umożliwiać filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji
* Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według minimalnie 120 kategorii
* Rozwiązanie musi pozwalać na tworzenie białych list wyjątków dla filtrowania zawartości
* Baza zawartości URL powinna być dostępna on-line lub do ściągnięcia i zainstalowania miejscowo
* Funkcja powinna filtrować treści w wielu językach, w tym w języku polskim
* Filtrowanie musi obsługiwać również protokół https
* Urządzenie musi umożliwiać wyłączenie inspekcji https dla wybranych kategorii stron WWW
* System kategoryzacji stron musi posiadać kategorie: Command&control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware

**Kontrola aplikacyjna**

* System kontroli aplikacyjnej musi rozpoznawać aplikacje oraz kategorie aplikacji
* Aplikacje muszą być rozpoznawana w oparciu o analizę ruchu a nie przez porty i protokoły
* Ilość rozpoznawanych aplikacji nie mniejsza niż 1800
* W ramach konkretnej aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe)
* Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, CryptoAdmin, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online

**Antywirus**

* System musi mieć możliwość uruchomienia co najmniej 2 skanerów antywirusowych
* Aktualizacja plików sygnatur antywirusowych musi się odbywać automatycznie
* Aktualizacja plików sygnatur antywirusowych musi się odbywać nie rzadziej niż co 12 godzin.
* Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail.
* Jeden ze skanerów antywirusowych musi bazować na mechanizmach bezsygnaturowych
* Rozwiązanie musi mieć możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen
* Wykrywanie i blokowanie spyware’u
* Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji
* Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS
* System musi zapewniać możliwość zablokowania ransomware uruchomionego na stacjach roboczych i serwerach.
* Przepustowość AV w urządzeniu nie mniejsza niż 3.1 Gbps

**Antyspam**

* Antyspam ma być oparty na technologii RPD - Recurrent Pattern Detection
* Antyspam ma zapewnić możliwość kwarantanny e-mail
* Antyspam ma posiadać zintegrowaną antywirusową analizę spamu
* Rozwiązanie ma umożliwić blokowanie spamu w wielu językach w tym w języku polskim
* Możliwość blokowania spamu opartego na obrazach graficznych.

**IPS**

* Automatyczna aktualizacja sygnatur IPS
* IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy
* Automatyczne blokowanie znanych źródeł ataków
* System musi pozwalać na blokowanie ataków typu DoS i DDoS
* Przepustowość IPS pełne skanowanie w urządzeniu nie mniejsza niż 3.3 Gbps

**Antymalware**

* System musi zapewniać ochronę przed nieznanym złośliwym oprogramowaniem, na zasadzie analizy behawioralnej (sandbox).
* System musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej)
* Analizie muszą podlegać pliki ściągane przez http(s) i przesyłane pocztą elektroniczną.
* System musi zapewniać ogólne oszacowanie poziomu ryzyka dla analizowanych plików oraz udostępniać szczegółowe informacje o wykrytych działaniach niebezpiecznych.
* System musi mieć możliwość blokowania poczty zawierającej podejrzane załączniki do czasu zakończenia ich analizy
* Skuteczność wykrywania malware’u – minimum 98% (potwierdzone zewnętrznymi testami)

**Ochrona przed phishingiem**

* System musi zapewniać dedykowaną (poza ochroną przed SPAMem) ochronę przed phishingiem
* System winien blokować możliwość dostępu do spreparowanych stron.
* System musi blokować dostęp niezależnie od użytego protokołu czy portu komunikacyjnego
* Zablokowanie dostępu musi być odpowiednio notyfikowane użytkownikowi, którego dotyczy, niezależnie od logów i raportów
* System musi chronić przed nadużyciem protokołu DNS

**Zarządzanie**

* Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania w czasie rzeczywistym.
* Urządzenie musi umożliwiać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH.
* Urządzenie musi umożliwiać zarządzanie za pomocą wbudowanego interfejsu www.
* Interfejs WWW do zarządzania urządzeniem musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
* Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów.
* Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
* Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
* Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według harmonogramu
* System musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
* Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
* System ma posiadać metodę porównywania różnych wersji konfiguracji.
* Obsługa różnych ról administratorów.
* Umożliwia monitorowanie logów ruchu w czasie rzeczywistym.
* System ma posiadać możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty)
* Urządzenie musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
* System zarządzania musi zapewniać korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów
* System zarządzania musi posiadać graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop

**Dzienniki i raporty**

* Rozwiązanie musi umożliwiać zbieranie i przechowywanie dzienników i raportów.
* Rozwiązanie musi umożliwiać przesyłanie logów do co najmniej 2 serwerów dziennika
* Dzienniki transmisji muszą być szyfrowane.
* Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
* Rozwiązanie musi udostępniać narzędzie analizy całości ruchu
* Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa
* Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów czy rozmiaru bazy danych
* Rozwiązanie musi umożliwiać zapis logów w zewnętrznej bazie danych oraz stały dostęp w celu analizy i generowania raportów.
* Rozwiązanie musi posiadać minimum 90 predefiniowanych typów raportów.
* Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie
* System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
* System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail.
* Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
* System raportowania musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników.
* System musi wspierać automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną.
* Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
* System musi umożliwiać pseudoanonimizację użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów
* System musi zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu.
* System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.

**Gwarancja 36 miesięcy.**

**Termin instalacji sprzętu do 30 października 2022r.**

**8.Wykonanie Instalacji i konfiguracji Next Generation Firewall**

**Wsparcie zdalne w zakresie:**

1. instalacji oprogramowania na wskazanym serwerze
2. aktywacji urządzenia i konfiguracji sieciowej
3. konfiguracji polityk bezpieczeństwa Packet Filter / Proxy
4. przygotowania polityk bezpieczeństwa
5. konfiguracji urządzenia,
6. połączenia urządzeń w klaster Active/Passive.
7. implementacji centralnego systemu zbierania logów, zarządzania, raportowania w infrastrukturze klienta (Hyper-V lub Vmware) i zintegrowania z systemem urządzenia

**Minimum 6h wsparcia inżynierskiego autoryzowanego dystrybutora producenta**

**9.Dostawa oprogramowania Antywirusowego**

**Administracja zdalna**

1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
17. Rozwiązanie musi informować administratora o nieaktualnych komponentach w tym przynajmniej JAVA i serwer SQL.

**Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11), MacOS 10.15 lub nowszy.
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:  
   zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
2. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
6. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
7. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

* tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
7. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

**Dodatkowe wymagania dla ochrony serwerów Windows:**

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

**Dodatkowe wymagania dla ochrony serwerów Linux:**

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.
5. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

**Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowiskuMicrosoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

**Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

* usunięcie zawartości urządzenia,
* przywrócenie urządzenie do ustawień fabrycznych,
* zablokowania urządzenia,
* uruchomienie sygnału dźwiękowego,
* lokalizację GPS.

1. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
2. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

* nazwę aplikacji,
* nazwę pakietu,
* kategorię sklepu Google Play,
* uprawnienia aplikacji,
* pochodzenie aplikacji z nieznanego źródła.

**Licencja na 24 miesiące .**

**Liczba stanowisk 200**

**Termin instalacji najpóźniej dzień po podpisaniu umowy.**

**10.Dostawa serwer NAS - Network Attached Storage**

**Specyfikacja techniczna urządzenia**

|  |  |
| --- | --- |
| Procesor | Jeden 8-rdzeniowy/16-wątkowy procesor AMD Ryzen™ 7 3700X lub równoważny procesor szesnastordzeniowy osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 22200 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/high\_end\_cpus.html |
| Obudowa | Rack 2U o wymiarach nie większych niż, 89× 483 × 565 mm  (wys. x szer. x gł.); w zestawie szyny wysuwane do instalacji w szafie RACK |
| Pamięć RAM | 32 GB UDIMM DDR4 z opcja rozszerzenia do 128GB RAM |
| Ilość obsługiwanych dysków | 12 dysków 3,5-calowych 3,5/2,5 dyski SATA |
| Ilość zainstalowanych dysków | 10 dysków o min. pojemności 14TB, MTBF 2,5mil godzin, cache 512MB. Dyski muszą znajdować się na liście zgodności z oferowanym serwerem NAS |
| Interfejsy sieciowe | 2 porty 1Gigabit sieci Ethernet (RJ45)  2 porty 10GbE (SFP+)  2 porty 10GbE (10GBase-T) |
|  |
| Porty | 4 gniazda typu a USB 3.2 Gen 1  1 gniazdo typu C USB 3.2 Gen 2 10 Gb/s  1 gniazdo typu A USB 3.2 Gen 2 10 Gb/s |
| Porty PCIe | 4 gniazd PCIe Gen3 |
| Wskaźniki LED | Dyski, stan, LAN, stan portów rozszerzenia pamięci masowej |
| Obsługa RAID | RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych. |
| System Operacyjny | Apple Mac OS 10.10 lub nowszy  Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux  IBM AIX 7, Solaris 10 lub nowszy UNIX  Microsoft Windows 7, 8, 10  Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019 |
| Stacja monitoringu | Tak, w standardzie 8 darmowych licencji na podłączenie kamer. |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, FC, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu  Windows ACL  Integracja w Windows ADS  Serwer WWW  Serwer plików  Manager plików przez WWW  Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI  Replikacja w czasie rzeczywistym  Serwer RADIUS  Klient LDAP  Serwer Syslog  Container Station |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| Gwarancja i serwis | **36 miesięcy gwarancji producenta** |
| Waga | Nie więcej niż 14 kg (netto) |
| Pobór mocy | Nie więcej niż 110W |
| System plików | Dyski wewnętrzne ZFS, EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| Funkcje ZFS | Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Liczba kont użytkowników | 4096 |
| Liczba grup | 512 |
| Liczba udziałów | 512 |
| Max ilość połączeń (CIFS) | 5000 |
| Max liczba migawek | 65536 |
| Zasilanie | Redundantne 300 W (x2), 200–240 V |
| Wentylatory | 2 x 70mm, 12VDC |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |

**Termin dostawy/instalacji do 30 października 2022r.**

**11.Dostawa Zasilacza awaryjnego UPS**

Zarządzalny zasilacz awaryjny typu on-line o mocy nie mniejszej niż 1500 VA (1.2 kW)  
Obudowa typu Rack, wraz z szynami umożliwiającymi montaż w szafie serwerowej.   
Wysokość nie może przekraczać 2U.

Wejścia: Input C14, 230V, 1 faza

Wyjścia: Output 4 x C13, 230V, 1 faza

Porty komunikacyjne:

* 3 x USB,
* 3 x Universal I/O RJ45,
* 1 x Network RJ45,
* 1 x Console)

**Gwarancja 12 miesięcy.**

**Termin dostawy do 30 października.**

**12.Dostawa Oprogramowania do backupu**

Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk wirtualizacyjnych.

**Wymagania funkcjonalne dla oprogramowania:**

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:
2. Dla hosta:

* VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6,7.
* Hyper-V.
* Citrix XenServer.
* Red Hat Virtualization.
* Linux KVM.
* Oracle VM Server.

1. Dla maszyn wirtualnych:

* Windows XP (SP3) i nowsze.
* Windows Server 2003 i nowsze.
* Windows SBS 2011/2008, 2003/2003R2.
* Windows Storage Server 2012/2012R2, 2008R2/2008/2003.
* Windows MultiPoint Server 2012/2011/2010.
* Linux OS.
* macOS.

1. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
2. Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
3. Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
4. Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.
5. Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
6. Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
7. Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
8. Wsparcie dla Single Sign On dla logowania do systemu.
9. Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
10. Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
11. Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych.
12. Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows.
13. Zdalne uaktualniania agentów kopi zapasowych.
14. Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.
15. Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).
16. Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
17. Centralny katalog wszystkich danych zapisanych w kopiach zapasowych
18. Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
19. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
20. Kopie zapasowe całych dysków i partycji.
21. Kopie zapasowe wybranych plików i folderów.
22. Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi).
23. Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)
24. Kopie zapasowe baz danych Oracle.
25. Kopie zapasowe hostów Hyper-V i VMWare ESXi.
26. Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.
27. Zapis kopi zapasowych na udziały sieciowe.
28. Zapis kopi zapasowych na serwer SFTP..
29. Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
30. Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery).
31. Możliwość wyszukiwania plików w kopiach zapasowych.
32. Szyfrowanie plików kopi zapasowych.
33. Wsparcie dla technologii VSS.
34. Deduplikacjia kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
35. Kompresja plików kopi zapasowych.
36. Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).
37. Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
38. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
39. Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore
40. Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
41. Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej.
42. Odtworzenie poszczególnych plików i folderów.
43. Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
44. Granularne odtwarzanie baz danych Microsoft Exchange.
45. Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.
46. Wyszukiwanie i podgląd odtwarzanych wiadomości email.
47. Granularne odtwarzanie baz danych Microsoft SQL.
48. Granularne odtwarzanie witryn i plików Microsoft SharePoint.
49. Odtwarzanie kontrolerów domeny Microsoft Active Directory.
50. Granularne odtwarzanie baz danych Oracle.
51. Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.
52. Dodatkowe wymagania związane ochroną danych:
53. Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń

**Termin uruchomienia oprogramowania do 30 października 2022r.**

**Licencja na 2 lata (do wykonywania kopii zapasowych dla 8 wirtualnych serwerów).**

**13.Dostawa oprogramowania do wirtualizacji**

**Licencjonowanie:**

* Zakupione w oficjalnym kanale sprzedaży producenta, do którego należy Polska.
* Dostarczona licencja ma upoważniać do użytkowania dostarczonego oprogramowania na czas nieokreślony.
* Licencja powinna umożliwiać instalację oprogramowania na min. 3 fizycznych serwerach posiadających po 2 procesory.
* W ramach dostarczonej licencji ma być zapewnione dodatkowe 12-miesięczne wsparcie producenta.

**Funkcjonalności i kryteria :**

Oprogramowanie powinno poprawnie współpracować z eksploatowanym klastrem opartym o VMware ESXi, 6.5.0 oraz spełnić poniższe kryteria:

* Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w min 6 rdzeni.
* Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
* Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych min 1-4 procesorowych.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-4 wirtualnych kart sieciowych.
* Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
* Potwierdzone przez producenta oprogramowania (np. na jego oficjalnej stronie www.) wsparcie dla następujących Systemów Operacyjnych: Windows XP, Windows Vista, Windows Se1-ver 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2022, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, SLES 11, SLES 10, RHEL 6, RHEL 5, RHEL 4, Debian 7, Mandriva, Fedora, Red Hat, Solaris 11, Ubuntu, FreeBSD I l.x, Mac OS X 10.10.
* Wsparcie dla systemów 32- i 64-bitowych.
* Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
* Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
* Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
* Dostęp do centralnej konsoli zarządzającej musi być możliwy przy wykorzystaniu przeglądarki Internet Explorer lub Firefox.
* Centralna konsola do zarządzania musi posiadać możliwość przydzielania i konfiguracji uprawnień do poszczególnych wirtualnych stacji roboczych lub grup wirtualnych stacji roboczych.
* Centralna konsola do zarządzania musi posiadać możliwość integracji z tokenami RSA celem zapewnienia możliwości autentykacji dwuskładnikowej do wirtualnych stacji roboczych.
* Oprogramowanie do wirtualizacji musi posiadać możliwość instalacji więcej niż jednej instancji serwera zarządzającego połączeniami tak, aby w przypadku awarii takiego se1wera zapewnić możliwość nawiązania nowej sesji przez inny serwer zarządzający.
* Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach).
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania wirtualnych maszyn posiadających min. 512 GB pamięci RAM.
* Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
* Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
* Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
* Rozwiązanie musi zapewnić wbudowany mechanizm do bezpiecznej automatycznej archiwizacji i odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych.
* Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
* Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
* Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) \_aby w przypadku awaru lub niedostępności serwera fizycznego.
* System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.
* Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethemetowego w razie awarii karty sieciowej.
* Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
* Oprogramowanie musi zawierać mechanizmy obsługi przekierowania profili i ustawień użytkownika niezależnie od mechanizmów oferowanych przez system operacyjny w wi1tualnym desktopie (natywna wirtualizacja profili użytkownika).

**Wsparcie i serwis :**

Oprogramowanie musi posiadać 12 miesięczne wsparcie i serwis Producenta o następujących min. parametrach:

* Możliwość aktualizacji oprogramowania do najnowszych wersji bez uiszczania dodatkowych opłat;
* Możliwość zgłaszania problemów z oprogramowaniem (dni powszednie - w godzinach od 7:30 do 15:30);
* Nieograniczona liczba zgłoszeń serwisowych;
* Dostęp online do dokumentacji technicznej, bazy wiedzy i forum dyskusyjnego.

**Licencja 1 rok.**

**Termin dostawy do 30 października 2022.**

**14.Wykonanie Usług w zakresie instalacji i konfiguracji dostarczonego sprzętu i oprogramowania**

1. Środowisko backupowe

Budowa systemu do bezpiecznego archiwizowania środowiska produkcyjnego dla serwerów oraz stacji roboczych. Środowisko tworzone w oparciu o dwa redundantne urządzenia Network Attached Storage połączone za pomocą switcha optycznego (SFP+ - 10Gb/s) i zarządzanego za pomocą oprogramowania do backupu z poziomu konsoli zdalnej.  
Środowisko połączone z 3 fizycznymi serwerami za pomocą światłowodów. Jedno urządzenie NAS wyprowadzone poza główną serwerownie. Wsparte poprzez dodatkowe zasilanie UPS.

1. Usługa aktualizacji oprogramowania serwerowego Vmware do wersji vSphere 6 Essentials Plus.
2. Instalacja i konfiguracja w środowisku produkcyjnym Zamawiającego systemu SIEM (security information and event management).
3. Instalacja i konfiguracja w środowisku produkcyjnym systemu GRC (Governance, risk management and compliance) .

**Termin realizacji do 21 listopada 2022.**