Cyberbezpieczne Wodociągi

ZP 2.2026

Załącznik nr 10

Część 1

1. Dostawa i wdrożenie systemu monitorowania sieci przemysłowej.

Przedmiotem zamówienia jest:
Wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS):

1. dostawa licencji oraz sond sprzętowych,
2. udzielenie wsparcia dla administratorów Zamawiającego,
3. organizacja i realizacja szkoleń dla administratorów Zamawiającego.

1. Funkcjonalność i specyfikacja.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:
    a. pasywne monitorowanie sieci przemysłowej Zamawiającego,
    b. automatyczne tworzenie graficznej mapy urządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
    c. szczegółową inwentaryzację urządzeń,
    d. automatyczne odzwierciedlenie połączeń komunikacyjnych,
    e. informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
    f. wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując

powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,

g. budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
h. obsługę LLDP, CDP, CIP, SSDP.

10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line" przy wpięciu do linii.
15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17. System IDS powinien być oparty na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog).
20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody/techniki behawioralne.
21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem ważności, typem, czasem wystąpienia.
22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.
26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.
27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.
28. System IDS musi wykrywać zagrożenia min.:
    a. malware/"zero-day",
    b. atak DOS/DDOS,
    c. atak typu APT,
    d. spyware, skanowanie sieci,
    e. zagrożenia Man-in-the-Middle,
    f. anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność komend, skanowanie PLC, skanowanie urządzeń sterujących,
    g. wykrywanie połączeń do innej sieci LAN/internet,
    h. wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.
29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.

32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.
34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BORADCAST.
35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.
36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.
38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.
40. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.
43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
44. Sonda sprzętowa musi być zabezpieczona przed ingerencją tzn.: dane muszą zostać skasowane przy próbie odczytu pamięci FLASH.
45. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
49. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
50. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
51. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
52. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

2. Dostawa, wdrożenie.

1. Wykonawca dostarczy:

   a. sondy sprzętowe w liczbie 3 szt. do monitorowania sieci przemysłowej,
   b. licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń,
   c. usługi wsparcia serwisowego producenta systemu IDS na okres nie przekraczając 31.12.2026

   serwis producenta systemu IDS ma obejmować:

   - Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
   - Dostęp do nowych wersji systemu IDS.
   - Dostęp do aktualizacji i poprawek systemu IDS.
   - Dostęp do aktualizacji oprogramowania sond sprzętowych.
   - Wymianę uszkodzonych sond sprzętowych w razie awarii.
   - Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
   - Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.

- Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.

2. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.

3. Licencje systemowe oraz sprzęt serwerowy zapewni Zamawiający.

4. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.

5. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.

6. Wykonawca przekaże Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.

7. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.

8. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.

9. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w późniejszym terminie pomiędzy Zamawiającym a Wykonawcą.

10. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

Część 2

1. **Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach oraz urządzeniach sieciowych – 13 sztuk.**

Informacje Ogólne.

- Dostarczone licencje na oprogramowanie są bezterminowe.

- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
- Oprogramowanie współpracuje z serwerem SQL Server 2019, SQL Server 2017, SQL Server 2016 SP3, SQL Server 2014 SP3, Oracle 19c, Oracle 12c R2.
- Oprogramowanie serwera aplikacji umożliwia wysyłanie powiadomień mailowych.
- Oprogramowanie posiada system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli.
- Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
- Oprogramowanie realizuj zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej.
- Oprogramowanie agenta realizuje wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
- Oprogramowanie pozwala export do Excel'a dowolnego widoku konsoli administracyjnej.
- Oprogramowanie pozwala zarządzać z jednej konsoli zarówno stacjami klienckimi, serwerami jak i urządzeniami mobilnymi z systemami operacyjnymi Android oraz iOS.
- Oprogramowanie, niezależnie od ilości funkcjonalności lub zarządzanych urządzeń końcowych działa w oparciu o 1 oprogramowanie typu Agent na urządzeniu końcowym.
- Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
- Oprogramowanie działa na minimalnych wymaganiach sprzętowych:

  Wymagania sprzętowe:
  - procesor minimum 2 rdzenie;
  - 8 GB wolnej pamięci- rekomendowane 16 GB;
  - karta sieciowa min 1 Gigabit;
  - przestrzeń w celu instalacji: minimum 5 GB;

  Wymagane oprogramowanie dla Serwera:
  - Serwer OS - od Windows Server 2016 (64-Bit);
  - od 5 GB wolnej przestrzeni dyskowej na instalacje serwera;
  - Baza Danych - od SQL Server 2014 SP3;

  Wymagania dla stacji klienckiej:
  - od Intel Pentium IV procesor z 1GHz;
  - od 256 MB wolnej pamieci RAM;
  - od 200 MB wolnego miejsca na dysku twardym;

- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.

- Oprogramowanie umożliwia dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również takich jak InnoSetup, InstallShield i inne.
- Oprogramowanie umożliwia automatyzowanie instalatorów wraz z możliwością customizowania instalatorów w taki sposób, żeby można było nadpisywać pola opisowe, zmieniać dowolne wartości, w tym miejsce zapisu na dysku na urządzeniu końcowym.
- Oprogramowanie umożliwia administratorowi zautomatyzowanie procesu instalacji, w taki sposób, by nagrany został cały proces instalacji w taki sposób, by w momencie instalacji na urządzeniu końcowym nie było wymagane podanie jakichkolwiek opcji.
- Oprogramowanie musi umożliwiać zautomatyzowania zdalnej instalacji dowolnego oprogramowania w taki sposób, by oprogramowanie można było zainstalować zdalnie w trybie cichym (Silent Mode) lub graficznym.
- Oprogramowanie musi umożliwiać dodawanie takich opcji w instalatorach jak:
  - blokowanie klawiatury i myszki,
  - zmiany w ustawieniach w rejestracji na stacjach klienckich,
  - działania na plikach i folderach na stacji klienckiej,
  - dodanie skryptu np. w PowerShellu
  - zatrzymanie/wznowienie usług oraz procesów na stacji klienckiej"
- Zdalna dystrybucja oprogramowania musi wykorzystywać natywną inteligencję instalatora. Nie może wykorzystywać Snapshotingu.
- Zdalna dystrybucja oprogramowania musi mieć opcje schedullingu:
  - w zadanym przedziale czasowym;
  - wprowadzenie cykliczności (np. wybrany dzień tygodnia o wybranej godzinie);
  - połączenie dwóch powyższych;
  - na żądanie w danym momencie;
- Oprogramowanie musi umożliwiać wzbudzanie stacji klienckich metodą Wake-On-LAN.
- Oprogramowanie musi umożliwiać administratorowi podgląd co do Statusu danego taska per maszyna w czasie rzeczywistym, a w przypadku błędu w wykonaniu - zwrócić informację co było przyczyną błędu.
- W przypadku dokupienia nowych funkcjonalności/modułów oprogramowania, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- W przypadku zwiększenia ilości zarządzanych maszyn w dowolnym momencie, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera(wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- Oprogramowanie musi umożliwiać zdalną dystrybucję oprogramowania z jednej konsoli zarówno na stacjach klienckich (jak PC I laptop/notebook) jak i urządzeniach mobilnych z systemem Android.
- Oprogramowanie dostarczy administratorowi informacji o dacie ostatniego uruchomienia aplikacji na stacji klienckiej PC per każda stacja kliencka.
- Dystrybucja agentów na stacjach klienckich musi być możliwa zarówno w sposób automatyczny jak i ręczny.

- Oprogramowanie umożliwia integrację z Active Directory oraz pobranie informacji z AD i automatyczne zarejestrowanie urządzeń z AD w serwerze.
- Zarówno w przypadku stacji klienckich PC, jak i urządzeń mobilnych z systemem Android, oprogramowanie musi umożliwiać administratorowi dostarczenie użytkownikowi końcowemu interfejsu typu self-service, w którym będzie miał listę dostępnych instalatorów z możliwością ich dociągnięcia i zainstalowania; Musi istnieć możliwość automatycznej personalizacji takiej listy per grupa lub konkretne urządzenie końcowe.
- Oprogramowanie musi posiadać otwarte API do integracji z zewnętrznymi serwerami, np. poprzez Web Service'y.
- Oprogramowanie musi umożliwiać również tworzenie własnych skryptów, które następnie można automatycznie instalować na urządzeniach końcowych, typu stacja kliencka.
- W przypadku automatycznej zdalnej instalacji oprogramowania na stacjach klienckich, oprogramowanie musi dać opcje tworzenia listy oprogramowania zależnego, tzn. w przypadku gdy do poprawnego działania aplikacja X wymaga instalacji aplikacji Y, Oprogramowanie musi dawać opcję ustalenia listy takiego oprogramowania zależnego na poziomie konfiguracji aplikacji X z poziomu konsoli. W przypadku dystrybucji aplikacji X, gdy na stacji klienckiej nie będzie zainstalowana aplikacja Y, serwer automatycznie wypchnie na tą stację paczkę instalacyjną aplikacji Y .
- Oprogramowanie musi dawać administratorowi możliwość przypisywania wykonywania tasków zarówno na urządzeniach końcowych spełniających wybrane warunki dynamiczne (np. Wolne miejsce na dysku C, wersja systemu operacyjnego itp.), jak i urządzeniach przypisanych do konkretnych grup, jak w AD.
- Oprogramowanie musi posiadać środowisko skryptowe, umożliwiające tworzenie własnych skryptów i w łatwej dystrybucji skryptów z poziomu konsoli.
- Oprogramowanie musi posiadać możliwość automatycznego skanowania komputerów i serwerów pod kątem podatności i przestrzegania wytycznych dotyczących bezpieczeństwa i zgodności z wykorzystaniem standardowych zbiorów reguł, które są utrzymywane przez certyfikowane organizacje i firmy zajmujące się bezpieczeństwem cybernetycznym (proces wyszukiwania podatności musi bazować na minimum 25000 stale aktualizowanych reguł) oraz reguł definiowanych przez użytkownika.

Architektura Platformy.

- Oprogramowanie wspiera MsSQL-Server (również w wersji Express);
- Oprogramowanie posiada konsolę zarządzającą jako część oprogramowania (nie tylko interfejs webowy);
- Oprogramowanie posiada Agenta dla systemów klienckich Windows od Windows oraz Windows Server;
- Oprogramowanie wspiera więcej niż jeden serwer-repozytorium (DIP-Server) ;
- Oprogramowanie wspiera PXE-Relay;
- Oprogramowanie wspiera WakeUp-Points;
- Oprogramowanie posiada możliwość integracji z Active Directory;

Komunikacja (server-clients).

- Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów i przesyłania informacji o statusach
- Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza)
- Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu
- Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN
- Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown)
- Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS

Operacje wykonywane przez Oprogramowanie.

- Oprogramowanie umożliwia pracę wielu administratorów równocześnie na jednej konsoli
- Oprogramowanie posiada wsparcie dla LAN, zdalne i OFFLINE stanowiska pracy
- Oprogramowania umożliwia wyświetlenie informacji i stanu/statusów dostępnych w czasie rzeczywistym ze znacznikiem czasowym
- W przypadku zakończenia wykonania zadania na stacji z błędem, administrator widzi w konsoli administracyjnej szczegółowe przyczyny błędu, które spowodowały niewykonanie danego zadania
- Komunikaty o błędach są generowane natychmiast (wraz z informacją o docelowym systemie OS)
- Dowolnie definiowane dodatkowe pola (Variable/Zmienne) przechowywane w tej samej bazie danych (np. Informacje o gnieździe sieciowym, danych dotyczących wynajmu, informacje supportowe)
- Rozbudowane funkcjonalności dotyczące zarządzania uprawnieniami
- Wsparcie dla grup dynamicznych na potrzeby indywidualnych informacji/widoku
- Oprogramowanie musi zawierać opcję ukrywania danych osobowych użytkowników (takich jak imię, nazwisko, login) dla wybranych administratorów
- Oprogramowanie musi umożliwiać przyznawanie i blokowanie dostępu do wybranej części infrastruktury oraz wybranych części funkcjonalności oprogramowania wskazanym administratorom.

Minimum możliwości w zakresie zadań jakie powinno spełniać oprogramowanie.

- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Push";
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Pull";
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "shutdown".;
- Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji;
- Oprogramowanie umożliwia wysyłanie polecenia Wake-on LAN;
- Oprogramowanie umożliwia automatyczne generowanie i wysyłanie powtarzających się zadań (recurring Jobs);
- Oprogramowanie umożliwia uruchomienie zadania z poziomu użytkownika końcowego poprzez Kiosk samoobsługowy SelfService (dostępny przez Web);

- Zadania mogą być inicjowane z poziomu aplikacji selfservice - konsoli Webowej;
- Zawartość aplikacji SelfService (Kiosku) może być definiowana zarówno per User/Grupa Userów jak i per PC/Organisation Unit;

Instalacja Oprogramowania (uwagi i wymagania minimalne).

- Kreator do tworzenia pakietów, w skład których wchodzi różnorodne oprogramowanie;
- Detekcja oraz wsparcie kreatory dla wielu mechanizmów instalacji: MSI, InnoSetup, NullSoft, Wise-Installer i inne;
- Uzupełnienie instalacji oprogramowania na urządzeniu końcowym o dodatkowe kroki ze strony użytkownika końcowego (np.: deaktywacja okna powitalnego, itp);
- Integracja procedury odinstalowania;
- Natywna instalacja pakietów (a nie tylko wrap aplikacji w innym skrypcie instalacyjnym);
- Transparentna instalacja (w Logach znajduje się informacja dotycząca instalacji np.: msiexec.exe /i \\...\software-xyz.msi /qn /noreboot);
- Indywidualna konfiguracja zależności (np.:uprzednia instalacja .net (w przypadku, jeśli takowa nie miała jeszcze miejsca), następnie instalacja docelowego oprogramowania);
- Ustawianie zachowań w trakcie Reboot również dla oprogramowania;
- Możliwość użycia własnych skryptów, żeby np: customizować Linki, Rejestry, Working Directories, itd.;
- Użycie narzędzia do tworzenia własnych skryptów w celu tworzenia własnych pakietów instalacyjnych (np.: "kopiuj pliki z .. , stwórz ikonę Start");
- Dostarczenie narzędzia do nagrywania kroków instalacji oprogramowania, tak, by administrator mógł przejść wszystkie kroki instalatora i wypchnąć tak wyklikany instalator zdalne;
- Różnorodna weryfikacja instalacji (np.: jaka jest wartość zwrotna programu instalacyjnego, czy istnieje jakiś określony wpis do rejestru lub usługa);
- Ustawienie dowolnego kontekstu security/uprawnień z jakimi dana paczka ma zostać zainstalowana na urządzeniu końcowym;

Automatyczna dystrybucja poprawek dla systemów MS / Patch Management

- Oprogramowanie umożliwia dystrybucji patchy Windows bez WSUS;
- Oprogramowanie umożliwia triggerowanie z poziomu WSUS;
- Oprogramowanie umożliwia obsługę systemów operacyjne Microsoft — Windows Server 2008, Windows 7, Windows 8, Windows 10, Windows 11, Windows Server 2008R2, Windows Server 2012, Windows Server 2019 z natywną instalacją;
- Producent oprogramowania zapewnia stały dostęp do bazy danych z poprawkami Microsoft - baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez Microsoft;
- Oprogramowanie umożliwia określenie ścisłych wymagań czasowych dla instalacji poprawek Microsoft i te wymagania kontrolować. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach;
- Oprogramowanie pozwala administratorowi zarządzać aktualizacją systemów: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą

być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT;

- Oprogramowania pozwala by metodą drag and drop w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora kreator skryptów, konfiguracji pakietów i autmatyzacja dowolnych procesów / Automate i Package Studio;
- Oprogramowanie pozwala na tworzenie plików transformacji (MST), które umożliwiają niezawodne dopasowanie do każdego MSI;
- Oprogramowanie pozwala na tworzenie kreatora instalacji dla dowolnej aplikacji - nie wymaga paczki MSI;
- Oprogramowanie pozwala tworzyć pakiety instalacyjne, gdzie w ramach procesu można zainstalować "n" aplikacji lub wykonać szereg dodatkowych funkcji związanych np. z inwentaryzacją;
- Oprogramowanie obsługuje wszystkie powszechnie dostępne na rynku systemy operacyjne Microsoft — Windows Vista i Server 2008, Windows 7, Windows 8, Windows10, Windows 11, Windows Server 2008R2, Windows Server 2012 i Windows 2019;
- Oprogramowanie umożliwia tworzenie plików sterujących (tansform);
- Oprogramowanie pozwala na automatyzacje niemal każdego procesu wykonywanego ręcznie na komputerze;
- Oprogramowania pozwala na proste tworzenie skryptów metodą drag and drop;
- Oprogramowanie zawiera standardowy zestaw poleceń;
- Oprogramowanie posiada możliwość sterowania również interfejsami niezgodnymi ze standardem (np. Java);
- Oprogramowanie posiada pomoc kontekstową;
- Oprogramowanie posiada tryb testowy step by step;

Moduły

- Identyfikacja urządzeń SNMP, takich jak drukarki, routery, przełączniki inne urządzenia sieciowe;
- Wizualizacja topologii sieci;
- Automatyczne skanowanie sieci firmowej;
- Identyfikacja stopnia wykorzystania oprogramowania;
- Automatyczna i natywna instalacja systemów operacyjnych;
- Bezpośrednie połączenie z urządzeniami końcowymi w sieci;
- Rejestracja zużycia energii na stanowiskach pracy;
- Kontrola przypisanych licencji do konta;
- Automatyczne skanowanie pod kątem podatności;
- Podniesienie poziomu bezpieczeństwa;

2. Oprogramowanie antywirusowe – 13 sztuk.

Oprogramowanie musi zostać dostarczone na okres nie przekraczający 31.12.2026 r.
Minimalne wymagania Zamawiającego:
Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość dodawania wykluczeń na podstawie

a. Plik
b. Folder
c. Rozszerzenie
d. Proces
e. Hash pliku
f. Hash certyfikatu
g. Nazwa zagrożenia
h. Wiersz poleceń
i. IP/maska

13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
14. 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).
15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
20. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

22. 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.
23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
28. Praca programu musi być niezauważalna dla użytkownika.
29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
32. Możliwość odblokowania ustawień programu po wpisaniu hasła.
33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
34. 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).
35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
40. Wbudowany IDS
41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.
42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji.
43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
44. Możliwość tworzenia list sieci zaufanych.
45. Możliwość dezaktywacji funkcji zapory sieciowej.
46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.
49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa)

50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
52. 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

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

a. Możliwość wymuszenia funkcji DEP systemu Windows
b. Możliwość wymuszenia relokacji modułów (ASLR)

Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.

54. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:

- Wczesny dostęp
- Dostęp do poświadczeń
- Wykrycie
- Crimeware

55. Ochrona 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|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

56. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:
a. Ukierunkowane ataki
b. Podejrzane pliki i ruch w sieci
c. Exploity
d. Ransomware
e. Grayware
57. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego
58. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:
a. Tolerancyjny
b. Normalny
c. Agresywny
59. 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.
60. Wbudowany sandbox musi działać w trybie monitorowania i blokowania
61. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny
62. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
63. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
64. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB
65. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.
66. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).
67. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

Maszyny Wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu).
2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem.
4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.
5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.

Stacje robocze i serwery Windows

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.

3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.
4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.
5. Możliwość skanowania w poszukiwania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.

11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. Dwa typy konsoli administracyjnej:

- Konsola Cloud – serwer administracyjny po stronie producenta
- Konsola On-premise – lokalny serwer administracyjny

2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
3. Centralna konfiguracja 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.
4. Możliwość integracji Domeny Active Directory w obu typach konsoli.
5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
6. 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).
7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
15. Możliwość generowania raportu co godzinę.
16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
18. Możliwość dodania etykiety do stacji roboczej.
19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
20. Możliwość przechowywania kwarantanny maksymalnie 180 dni
21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
24. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[2]

25. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
26. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
27. 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

28. Integracja z serwerem Syslog.
29. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator.
30. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
31. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
32. Funkcja pojedynczego logowania – Single Sign-on (SSO).
33. Możliwość naprawy instalacji z poziomu konsoli.
34. 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

35. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:

a. Pakiety
b. Sieć
c. Kwarantanna
d. Licencjonowanie
e. Integracje
f. Polityki
g. Raporty
h. Konta
i. Firmy

36. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na

określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na określenie godziny kiedy te maszyny będą usuwane

37. Możliwość określenia własnego serwera NTP.
38. Integracja z vCenter Server.
39. Integracja z Xen Server.
40. Integracja z nutanix Prism Element.
41. Możliwość integracji z Amazon EC2.
42. Intergracja z Azure.
43. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne.
44. Serwer centralnej administracji musi posiadać funkcje przełączenia się między widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.
45. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.
46. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
47. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
48. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
49. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:

a. Lotnictwo
b. Rolnictwo
c. Automotive
d. Usługi komercyjne
e. Doradztwo
f. Energia
g. Usługi finansowe
h. Rząd
i. Opieka zdrowotna
j. Technologie
k. Transport
l. Non-profit
m. Górnictwo
n. Media

50. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
51. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym.
52. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
53. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
54. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
55. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
56. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
57. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.

58. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
59. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.
60. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
61. Możliwość skanowania SSL dla połączeń RDP.
62. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
63. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
64. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych.
65. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie.
66. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
67. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.

EDR-Endpoint Detection and Response

Produkt musi zapewnić szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze
Wspierane systemy operacyjne

A. Systemy desktopowe

- Windows 11 (initial)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial)
- Windows 8.1
- Windows 8
- Windows 7 SP1

B. Systemy operacyjne dla serwerów:

- Windows Server 2022
- Windows Server 2019 Core
- Windows Server 2019

- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

C. MacOS:

- macOS Monterey (12.x)
- macOS Big Sur (11.x)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

D. Linux

- RHEL 7.x & 8.x ; 3.10.0-957 - 4.18.0
- RHEL 9x 5.14.x
- Oracle Linux 7.x (UEK +RHCK) ; 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) ; 3.10.0-957 - 4.18.0
- CentOS 7.x ; 3.10.0-957 - 4.18.0
- CentOS 8.x ; 3.10.0-957 - 4.18.0
- Debian 10 ; 4.19
- Debian 11 ; 5.10
- Ubuntu 16.04.x ; 4.8 / 4.10 / 4.13 / 4.15
- Ubuntu 18.04.x ; 5.0 / 5.3 / 5.4
- Ubuntu 20.04.x ; 5.4 / 5.8 / 5.11 / 5.13
- Ubuntu 22.04.x ; 5.15
- SLES 12 SP4 ; 4.12.14-x
- SLES 12 SP5 ; 4.12.14-x
- SLES 15 SP1 ; 4.12.14-x
- SLES 15 SP2 ; 5.3.18-x
- SLES 15 SP3 ; 5.3.18-x
- openSUSE Leap 15.2 ; 5.3.18
- AWS Bottlerocket 2020.03 ; 5.4.x, 5.10.x
- Amazon Linux v2 ; 4.14.x / 4.19.x
- Google COS Milestones 77, 81, 85 ; 4.19.112 / 5.4.49
- Fedora 31 – 36 ; Wspierane do wygaśnięcia.
- AlmaLinux 8.x ; 4.18.0
- Rocky Linux 8.x ; 4.18.0
- CloudLinux 8.x ; 4.18.0
- CloudLinux 7.x ; 3.10
- Pardus 21 ; 5.10
- Linux Mit 20.3 ; 5.4.0

Komponenty EDR

Główne elementy:

1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.

2. Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.

Wykrywanie podejrzanej aktywności

1. Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.
2. Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
3. Zgłaszanie wszystkich naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
2. Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:

a. Karta Podsumowanie zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
b. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
c. Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.

<u>Incydenty</u>

1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:

a. Filtrowania zdarzeń
b. Blokowania procesów
c. Dodawanie procesów do czarnej listy
d. Dodawanie procesów do białej listy
e. Izolacja hosta
f. Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)
g. Przesłanie pliku do Sandbox
h. Sprawdzenie informacji o pliku w Google
i. Sprawdzenie informacji o pliku w VirusTotal

2. Filtrowanie zdarzeń odbywa się na podstawie:

a. Ocena zagrożenia od 10 do 100 punktów
b. Data wykrycia
c. Status
d. ID
e. Nazwa punktu końcowego
f. Typ ataku

- Ransomware
- Potencjalnie niechciana aplikacja
- Malware
- Exploit
- Fileless

- Password stealer
- Downloader
- Inne
- Zdefiniowane przez użytkownika

3. Wyszukiwanie zdarzeń może odbywać się na podstawie:
a. Nazwa alertu
b. IP punktu końcowego
c. Hash MD5
d. Hash SHA256
e. Nazwa użytkownika
4. Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem.
5. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.
6. Możliwość wyświetlenia zablokowanych hashy plików.
7. Możliwość dodania własnych hashy MD5 oraz SHA256
8. Możliwość importu hashy z pliku CSV
9. Możliwość filtrowania dodanych hashy na podstawie:
a. Typu hashu
b. Wartości hash
c. Źródło dodania
d. Informacje o źródle
e. Nazwa pliku
f. Firma której dotyczy wpis
g. Możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie.

3. Oprogramowanie do wykonywania kopii zapasowych – 2 sztuki.

Lp.	Minimalne wymagania Zamawiającego
I. **Wymagania ogólne**	
1.	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie: - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
II. **Całkowite koszty posiadania**	

1.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2.	Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
4.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
5.	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
6.	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
7.	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
8.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
10.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
11.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
12.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
14.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
15.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
16.	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
17.	Dostarczone licencje na oprogramowanie są bezterminowe.

4. Oprogramowanie przeciwdziałające wyciekowi danych – 20 sztuk.

1. System operacyjny:
    a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,
    b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,
    c. MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach:
    a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
    a. MS SQL Server 2016 lub nowsze,
    b. MS SQL Express,
    c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e- mail oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20.Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak
i nowo powstałych na bazie już skategoryzowanych plików.

25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania.
27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN.
29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych 31 Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
32.Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej.
38.System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia.
39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego.
40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik.
41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem.
42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej.
43. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń.
44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana.
45. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP.

46. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf.
47. Dostarczone licencje na oprogramowanie są bezterminowe.

5. Platforma szkoleniowa – 30 użytkowników.

„Kompleksowa Usługa Podnoszenia Świadomości Bezpieczeństwa" (zwana też Security Awareness Training, SAT), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w Internecie, bezpieczeństwa informacji podczas pracy zdalnej czy też przy bezpieczeństwa IT przy codziennych obowiązkach.
Platforma jest dostępna za pomocą dowolnej, nowoczesnej przeglądarki internetowej (Chrome, Firefox, Edge) a sama usługa jest świadczona z centrum danych znajdującym się na terenie Unii Europejskiej.
Podczas tworzenia użytkownika, jest możliwość wyboru domyślnego języka, w którym będzie on otrzymywał powiadomienia, kampanie phishingowe, oraz w którym będzie miał dostęp do szkoleń.
Usługa zawiera poszczególne komponenty:

1. Platforma szkoleniowa
    a. Platforma zawiera minimum 250 szkoleń, dostępnych w 40 językach
    b. Szkolenia są dostępne w postaci filmów, plików audio, prezentacji, broszur oraz interaktywnych gier, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.
    c. Szkolenia zapewniają zakres tematyczny co najmniej w ujęciu:
        i. Ryzyka związanego z AI
        ii. Bezpieczeństwa informacji
        iii. Klasyfikacji informacji
        iv. Cyklu życia informacji
        v. Własności intelektualnej
        vi. Haseł
        vii. Kontroli dostępu
        viii. Poczty Email
        ix. Bezpieczeństwa w Internecie
        x. Inżynierii społecznej/socjotechnik
        xi. Prywatności
        xii. Danych płatniczych
        xiii. Phishingu
        xiv. Malware/Wirusów/Ransomware
        xv. Kradzieży tożsamości
        xvi. Mediów społecznościowych
        xvii. Pracy zdalnej
        xviii. Urządzeń mobilnych
        xix. Wycieku danych
        xx. Otwartych sieci WiFi
        xxi. Usług chmurowych
        xxii. Personalnych urządzeń w organizacji (BYOD)
        xxiii. Bezpieczeństwa w podróży

   d. To samo szkolenie może być dostępne zarówno w trybie wymagającym interakcji (np. odtworzenie filmu w całości by móc przejść dalej) jak i w trybie przeglądu, który nie wymaga konieczności interakcji by przejść szkolenie.
   e. System daje możliwość podzielenia użytkowników na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.
   f. Łączny czas trwania wszystkich materiałów szkoleniowych w języku polskim wynosi co najmniej 10 godzin.
2. Moduł Quizów
   a. System pozwala na stworzenie quizu, niezwiązanego z żadnym szkoleniem
   b. Quizy są dostępne w trzech formatach: ogólnodostępne, tylko dla wybranych użytkowników lub tylko dostępne za pośrednictwem linku
   c. Administrator może wybrać czy quiz wymaga pewnej punktacji do zaliczenia czy też nie.
   d. Administrator może wybrać, czy quiz można powtarzać w przypadku niepowodzenia.
   e. Pytania do quizów może tworzyć ręcznie administrator lub mogą one być zaciągane z innych modułów systemu.
3. Moduł narzędzi dodatkowych
   a. Narzędzia dodatkowe zawierają w sobie grafiki, ulotki, animacje, pozwalające na ich wydruk lub umieszczenie w interaktywnych elementach infrastruktury zamawiającego. Przykładem może być gif umieszczony w stopce maila, informując o zagrożeniach lub prowadzonej kampanii edukacyjnej.
4. Dedykowana platforma phishingowa
   a. Platforma phishingowa pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi (wedle ich domyślnego języka) oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:
      i. z linkiem prowadzącym do stronnym internetowej,
      ii. z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
      iii. z załącznikiem zawierającym potencjalnie niebezpieczny kod,
      iv. z załącznikiem w postaci dokumentu Word, Excel, PowerPoint, PDF, ZIP zawierającym potencjalnie niebezpieczny kod
   b. W przypadku, gdy użytkownik pozwoli się oszukać, platforma posiada możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.
   c. Maile phishingowe mają możliwość dystrybucji w czasie, tak by nie wszyscy użytkownicy dostali tą samą wiadomość w jednej chwili.
   d. Platforma posiada rozbudowaną bazę szablonów maili oraz stron phishingowych, co najmniej maili pochodzących od:
      i. Microsoft/Office365
      ii. Microsoft/Teams
      iii. Microsoft/Sharepoint
      iv. Microsoft/OneDrive
      v. DHL
      vi. Limitu skrzynki pocztowej
      vii. Zoom
      viii. Google Drive
      ix. Apple

e. Platforma pozwala na wgranie własnego szablonu wiadomości Email

5. Moduł raportujący obejmujący minimum:
   a. status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
   b. status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, kto wpisał dane w formularzu jaka była platforma oraz przeglądarka z której wykonał tę akcję oraz szczegółowe daty wykonania tych operacji.

Informacje dodatkowe:

- Wszystkie moduły (platforma zarządzająca, szkoleniowa, phishingowa, moduł raportowania, moduł quizów, moduł narzędzi dodatkowych) pochodzą od jednego producenta i są świadczone w trybie 24/7/365.
- Kursy, Quizy oraz Phishing mogą zostać połączone w jedną, spójną kampanię, wykonywaną krok po kroku wedle ustalonego wcześniej harmonogramu, bez konieczności interakcji z zewnątrz

6. Szkolenie z cyberbezpieczeństwa dla menadżerów.

Cel szkolenia:
Przekazanie menedżerom zaawansowanej wiedzy i narzędzi niezbędnych do efektywnej ochrony przed rosnącymi zagrożeniami cybernetycznymi, poprzez pogłębione rozumienie ryzyk, strategii obronnych, regulacji prawnych oraz najnowszych trendów w cyberbezpieczeństwie.

Struktura programu szkoleniowego:
Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.

W ramach przeprowadzonego szkolenia wykonawca

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:
- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.
- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji:
- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).

- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.
- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:
    - ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
    - ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
    - zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
    - akceptowalna polityka szyfrowania SANS;
    - techniki kryptograficzne - ENISA ;
    - ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.

- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.
3. Omówienie zaawansowanych strategii ochrony organizacji:
- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.
- Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.
- Szczegółowy opis i kroki zarządzania incydentami:
    - wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
    - rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
    - analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
    - klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
    - priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
    - podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
    - ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.
- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:
    - Priorytet krytyczny - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
    - Priorytet wysoki - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
    - Priorytet średni - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.
- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.
- Lista omówionych kompetencji w szkoleniu:
    - Szef działu bezpieczeństwa (kierownik, dyrektor);

- Pełnomocnik ds. Bezpieczeństwa Informacji;
- Specjalista ds. Zarządzania Ryzykiem;
- Specjalista ds. Zgodności;
- Specjalista ds. Bezpieczeństwa Fizycznego;
- Architekt Systemów Bezpieczeństwa;
- Koordynator Programu Bezpieczeństwa;
- Analityk Bezpieczeństwa (II linia wsparcia);
- Inżynier ds. Bezpieczeństwa (II linia wsparcia);
- Administrator Systemów Bezpieczeństwa (II linia wsparcia);
- Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
- Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
- Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

4. Regulacje prawne i compliance:
- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.
- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.
- Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.
- Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.
- Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.
- Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO), wraz z przeprowadzaniem testów penetracyjnych i socjotechnicznych, mających na celu weryfikację skuteczności implementowanych środków ochrony.
- Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.
- Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.
- Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).
- Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.
- Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.

- Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.
- Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom

5. Zarządzanie bezpieczeństwem w praktyce:
- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:
    - Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.
    - Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.
    - Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.
    - OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.
    - BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.
    - Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowego korzystania z zasobów.
- Techniki hardeningu: Wzmocnienie infrastruktury IT oraz zarządzanie patchami bezpieczeństwa.
- Testy penetracyjne i socjotechniczne: Organizacja i przeprowadzanie testów w celu oceny gotowości organizacji

Szkolenie powinno odbyć się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem conajmniej 4 przerw po 15 minut. Po szkoleniu przewidziano 30 minut na pytania i odpowiedzi uczestników.

7. Wdrożenie oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach oraz urządzeniach sieciowych.

Usługi wdrożeniowe oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej.

a. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
b. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
c. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

d. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając w to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
e. Wykonawca zainstaluje oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej, na wskazanym serwerze lokalnym lub w chmurze i skonfiguruje je zgodnie z wymaganiami i najlepszymi praktykami.
f. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.
g. Wykonawca przeprowadzi konfigurację strefy DMZ dla wymaganych usług.
h. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
i. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze.
j. Wykonawca przeprowadzi testy zarządzania urządzeniami, w tym możliwość dodawania, usuwania i zarządzania urządzeniami w konsoli administracyjnej oprogramowania oraz poprawność wykonywania instalacji, aktualizacji i usuwania oprogramowania. Wykonawca przetestuje, że konfiguracje mogą być efektywnie stosowane na wybranych urządzeniach.
k. Wykonawca przeprowadzi testy zdalnego zarządzania poprzez zdalne sterowanie komputerem oraz zdalne wsparcie ekranowe. Wykonawca w ramach tego zadania zweryfikuje dodatkowo czy można efektywnie udzielać pomocy technicznej użytkownikom poprzez konsolę oprogramowania.
l. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje na temat stanu infrastruktury IT oraz czy możliwość monitorowania wydajności urządzeń i systemów za pomocą narzędzi dostępnych w oprogramowaniu działa prawidłowo, zgodnie z założeniami prawidłowego działania oprogramowania.
m. Wykonawca przeprowadzi testy zabezpieczeń, weryfikując czy zastosowane zabezpieczenia, takie jak zasady bezpieczeństwa i ochrona antywirusowa, są skutecznie wdrażane na urządzeniach.
n. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
o. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii

8. Segmentacja sieci IT/OT.

Usługa kompleksowej segmentacji sieci teleinformatycznej (IT/OT)

1. CEL ZAMÓWIENIA

Przedmiotem zamówienia jest przeprowadzenie kompleksowej segmentacji infrastruktury sieciowej Zamawiającego obejmującej środowiska IT oraz OT, w celu:

- zwiększenia poziomu bezpieczeństwa systemów informatycznych i przemysłowych,
- zapewnienia kontroli dostępu między strefami IT i OT,
- ograniczenia ryzyka propagacji zagrożeń (w tym ransomware) pomiędzy segmentami,
- spełnienia dobrych praktyk (m.in. ISA/IEC 62443, NIST SP 800-82),
- zapewnienia ciągłości działania systemów przemysłowych.

2. ZAKRES USŁUGI

2.1. Analiza infrastruktury sieciowej (IT/OT)

Wykonawca przeprowadzi szczegółową inwentaryzację i analizę obejmującą:

Środowisko IT:

- Identyfikację urządzeń aktywnych i pasywnych
- Analizę przepływów sieciowych i wzorców ruchu
- Ocenę aktualnego stanu segmentacji i mechanizmów bezpieczeństwa
- Pomiar przepustowości i wydajności kluczowych łączy

Środowisko OT:

- Identyfikację systemów przemysłowych (SCADA, DCS, PLC, HMI, RTU, systemy telemetryczne)
- Mapowanie komunikacji przemysłowej (np. Modbus, Profinet, OPC, DNP3)
- Identyfikację zależności między systemami OT a IT
- Ocenę istniejących mechanizmów izolacji (jeśli występują)
- Analizę wymagań dostępności i deterministyczności systemów OT

2.2. Klasyfikacja zasobów i analiza ryzyka (IT/OT)

Wykonawca dokona klasyfikacji zasobów oraz analizy ryzyka:

- Otrzymanie od Zamawiającego zidentyfikowanych i skategoryzowanych zasobów krytycznych
- Otrzymanie klasyfikacji zasobów wg metodyki CIA (poufność, integralność, dostępność)
- Klasyfikacja danych, systemów IT i OT według poziomów wrażliwości

Dodatkowo dla OT:

- Klasyfikacja systemów pod kątem krytyczności operacyjnej (bezpieczeństwo procesów, wpływ na produkcję)
- Analiza ryzyka dla systemów ICS (uwzględniająca zagrożenia specyficzne dla OT)
- Identyfikacja punktów styku IT/OT (tzw. conduits)

2.3. Projekt architektury segmentacji (IT/OT)

Wykonawca opracuje szczegółowy projekt segmentacji obejmujący:

Model segmentacji IT:

- Definicję stref bezpieczeństwa (minimum):
    - DMZ
    - sieć produkcyjna IT
    - sieć biurowa
    - sieć zarządzania
    - sieć gości
    - sieć IoT

Model segmentacji OT (zgodny z ISA/IEC 62443):

- Podział na poziomy (Purdue Model), w tym:
    - Level 0/1 – urządzenia polowe
    - Level 2 – sterowanie (PLC, HMI)

    - Level 3 – systemy operacyjne (SCADA/MES)
    - Level 3.5 – Industrial DMZ (IDMZ)
    - integracja z IT (Level 4/5)
- Definicja stref i kanałów komunikacyjnych (zones & conduits)
- Zaprojektowanie Industrial DMZ (IDMZ) pomiędzy IT i OT

Wspólne elementy:

- Polityki kontroli dostępu (IT/OT)
- Reguły firewall i ACL (w tym firewalle przemysłowe)
- Segmentacja logiczna (VLAN, VRF, mikrosegmentacja)
- Rekomendacje technologii (NGFW, NAC, IDS/IPS, rozwiązania OT-aware)
- Plan adresacji IP dla wszystkich segmentów
- Strategia mikrosegmentacji dla zasobów krytycznych (IT i OT)
- Mechanizmy monitoringu ruchu IT/OT

2.4. Wdrożenie i konfiguracja (IT/OT)

Wykonawca przeprowadzi wdrożenie zaprojektowanej segmentacji:

- Konfiguracja urządzeń sieciowych i bezpieczeństwa
- Wdrożenie polityk bezpieczeństwa i reguł filtracji ruchu
- Segmentacja ruchu IT/OT zgodnie z zasadą least privilege
- Implementacja IDMZ oraz separacji IT/OT
- Integracja z istniejącymi systemami zarządzania i monitoringu

Dla OT:

- Wdrożenie z uwzględnieniem ciągłości procesów przemysłowych
- Prace realizowane w oknach serwisowych lub trybie bezprzerwowym (jeśli wymagane)
- Minimalizacja wpływu na systemy sterowania i produkcję

2.5. Testowanie i weryfikacja (IT/OT)

Wykonawca przeprowadzi kompleksowe testy:

- Testy komunikacji między segmentami (IT i OT)
- Weryfikacja reguł filtracji i kontroli dostępu
- Testy izolacji między strefami (w tym IT ↔ OT)
- Walidacja poprawności działania systemów OT po segmentacji

Dodatkowo dla OT:

- Testy bezpieczeństwa komunikacji przemysłowej
- Weryfikacja braku wpływu na deterministykę i opóźnienia systemów sterowania
- Testy scenariuszy awaryjnych i redundancji

3. DODATKOWE WYMAGANIA (NOWA SEKCJA – REKOMENDOWANA)

- Zgodność z normami:
    - ISA/IEC 62443
    - NIST SP 800-82
    - ISO 27001 (dla IT)
- Uwzględnienie:
    - systemów legacy w OT
    - ograniczeń patchowania w OT
    - monitoringu pasywnego (np. NDR dla OT)
- Dokumentacja powdrożeniowa obejmująca:
    - mapę segmentacji IT/OT

- listę reguł firewall
- diagramy stref i przepływów
- procedury zarządzania zmianą

4. REZULTATY USŁUGI

- Wdrożona segmentacja IT i OT
- Oddzielenie i kontrola komunikacji IT ↔ OT
- Zmniejszenie powierzchni ataku
- Zwiększona odporność na incydenty cyberbezpieczeństwa
- Pełna dokumentacja architektury

9. Utrzymanie systemów teleinformatycznych.

Przedmiotem zamówienia jest świadczenie usług stałej opieki informatycznej dla Zamawiającego, obejmujących w ilości 300 godzin oraz w okresie do 31.12.2026 r.:

- pomoc zdalna w rozwiązywaniu problemów z serwerami i oprogramowaniem serwerowym;
- monitorowanie dostępności serwerów i usług;
- reagowanie na problemy związane z dostępnością serwerów;
- zarządzanie zmianami i wersjami oprogramowania serwerowego;
- instalacja i konfiguracja nowego oprogramowania i sprzętu;
- zarządzanie patchami i aktualizacjami oprogramowania;
- backup i odzyskiwanie danych;
- monitorowanie wydajności systemów i aplikacji;
- diagnozowanie i rozwiązywanie problemów z wydajnością;
- zarządzanie konfiguracją systemów i aplikacji;
- automatyzacja rutynowych zadań operacyjnych;
- analiza i interpretacja logów systemowych i aplikacji;
- reagowanie na alerty bezpieczeństwa generowane przez SIEM;
- analiza trendów i przewidywanie przyszłych problemów;
- wdrażanie i zarządzanie kontenerami i usługami mikrousług;
- konfiguracja i zarządzanie sieciami wirtualnymi;
- zarządzanie certyfikatami SSL/TLS;
- wdrażanie zasad bezpieczeństwa i konfiguracji firewalli;
- audyt konfiguracji i zabezpieczeń systemów;
- przeprowadzanie testów penetracyjnych i ocen ryzyka;
- zarządzanie użytkownikami i uprawnieniami;
- zarządzanie bazami danych (backup, tuning, aktualizacje);
- zarządzanie środowiskami deweloperskimi, testowymi i produkcyjnymi;
- wsparcie dla procesów CI/CD (Continuous Integration/Continuous Deployment);
- doradztwo w zakresie architektury systemów i aplikacji;
- optymalizacja kosztów usług chmurowych;
- zarządzanie kluczami szyfrowania i dostępem do danych wrażliwych;
- planowanie i testowanie ciągłości działania (DR/BCP);
- zarządzanie incydentami bezpieczeństwa i reagowanie na nie;
- konsultacje w zakresie najlepszych praktyk DevOps i bezpieczeństwa IT;
- analiza przyczynowa (Root Cause Analysis) dla incydentów IT;
- zarządzanie dokumentacją techniczną i operacyjną;
- wsparcie przy migracjach systemów i aplikacji;

- ocena zgodności z wymaganiami regulacyjnymi i standardami branżowymi;
- szkolenia użytkowników i personelu technicznego w zakresie obsługi systemów;
- monitorowanie zagrożeń w cyberprzestrzeni i aktualizacja zabezpieczeń;
- zarządzanie konfiguracją sieci i urządzeń sieciowych;
- ocena skuteczności zaimplementowanych środków bezpieczeństwa;
- wsparcie dla procesów skalowania infrastruktury IT;
- analiza potrzeb biznesowych i doradztwo technologiczne;
- optymalizacja procesów biznesowych za pomocą technologii IT;
- przeglądy architektury systemów pod kątem najlepszych praktyk i zaleceń;
- wsparcie w zakresie integracji systemów i aplikacji;
- zarządzanie środowiskami wirtualnymi i chmurowymi;
- ocena wykorzystania zasobów IT i rekomendacje dotyczące optymalizacji;
- zarządzanie zmianą w infrastrukturze IT i procesach operacyjnych.

Zadania będą realizowane selektywnie i niezwłocznie na każde wezwanie Zamawiającego w godzinach 8:00 – 16:00 oraz w przypadku problemów krytycznych, przez całą dobę.

10. Utrzymanie systemów teleinformatycznych.

Utrzymanie stałego wsparcia technicznego i organizacyjnego w zakresie utrzymania i doskonalenia wdrożonych standardów bezpieczeństwa

1. Cel zamówienia.
Celem zamówienia jest wzmocnienie mechanizmów bezpieczeństwa oraz poprawa zgodności operacyjnej systemów teleinformatycznych Zamawiającego z wymogami stawianymi przez ROZPORZĄDZENIE 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, zwłaszcza w zakresie monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, w oparciu o normy:
PN-ISO/IEC 27001 - w odniesieniu do formy systemu zarządzania bezpieczeństwem informacji;
PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
3) PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
2. Zakres zamówienia.
Usługa będzie obejmować stałe doradztwo i wsparcie w ilości 300 godzin oraz w okresie do 31.12.2026 r., w celu optymalizacji procesów zarządzania bezpieczeństwem informacji przez zespół co najmniej 2 certyfikowanych audytorów, pełniących rolę Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, posiadających łącznie co najmniej poniższe certyfikaty:
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 (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
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.
Usługa obejmować będzie również:

zapewnienie aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia;
kontrolę aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację;
przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz sugerowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób, o których mowa w podpunkcie d;
zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
wsparcie w zakresie aktualizacji technicznych i organizacyjnych środków ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez monitorowanie dostępu do informacji, działania zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
wsparcie merytoryczne w zakresie zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
weryfikację zapisów w umowach serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji;
ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
wsparcie merytoryczne w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w szczególności w obszarach: dbałości o aktualizację oprogramowania, minimalizowania ryzyka utraty informacji w wyniku awarii, ochrony przed błędami, utratą, nieuprawnioną modyfikacją, stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, zapewnienia bezpieczeństwa plików systemowych, redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, niezwłocznego podejmowania działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
w przypadku pojawienia się incydentów naruszenia bezpieczeństwa informacji, wsparcie w bezzwłocznym zgłaszaniu w określony i z góry ustalony sposób do właściwych organów, umożliwiającym szybkie podejmowanie działań korygujących.

11. Wdrożenie oprogramowania do wykonywania kopii zapasowych.

1. Planowanie i Przygotowanie:

- Określenie wymagań dotyczących backupu i replikacji, w tym ilość danych do przechowywania, czas przywracania, dostępność i inne czynniki.
- Weryfikacja posiadania odpowiedniej ilości przestrzeni dyskowej i zasobów sieciowych do przechowywania kopii zapasowych.

- Pobranie niezbędnego oprogramowania do wykonywania kopii zapasowych i przeczytanie jego dokumentacji.

2. Instalacja i Konfiguracja:

- Uruchomienie instalatora wybranego oprogramowania do wykonywania kopii zapasowych na wybranym serwerze.
- Postępuj zgodnie z kreatorami instalacji, akceptując licencję, wybierając komponenty do zainstalowania i konfigurując ustawienia.
- Konfiguracja połączenia ze swoim środowiskiem wirtualizacji.

3. Konfiguracja Backupu:

- Konfiguracja planów backupu, określając harmonogramy, miejsca przechowywania i inne parametry.
- Wybranie, które maszyny wirtualne lub inne zasoby będą chronione za pomocą kopii zapasowych.
- Ustawienie retencji danych i polityki przechowywania, aby dostosować je do wymagań firmy.

4. Konfiguracja Replikacji (opcjonalnie):

- Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
- Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5. Testowanie i Wdrażanie:

- Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania.
- Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność i skuteczność.

6. Monitorowanie i Administracja:

- Regularne monitorowanie wykonywanych kopii zapasowych i replikacji, w celu weryfikacji ich poprawności i zgodności z planem.
- Weryfikacja raportów i dzienników zdarzeń oprogramowania do wykonywania kopii zapasowych, aby szybko reagować na jakiekolwiek problemy.

12. Usługa SOC.

1. Cel zamówienia

1.1. Celem zamówienia jest zapewnienie Zamawiającemu kompleksowej usługi typu Security Operations Center (SOC) polegającej na stałym monitorowaniu, analizie oraz reagowaniu na zdarzenia i incydenty naruszenia bezpieczeństwa informacji w środowisku teleinformatycznym Zamawiającego.

1.2. Usługa ma zapewnić:

1) skrócenie czasu wykrywania oraz obsługi incydentów bezpieczeństwa,

2) centralny wgląd w zdarzenia bezpieczeństwa pochodzące z wielu źródeł,

3) wykorzystanie zaawansowanych mechanizmów korelacji, analizy behawioralnej oraz sztucznej inteligencji (moduł AI platformy SOC, przetwarzany w centrum danych na terytorium UE, sklasyfikowany jako system ograniczonego ryzyka w rozumieniu AI Act),

4) wsparcie Zamawiającego w spełnieniu wymagań wynikających z przepisów prawa, w szczególności w zakresie bezpieczeństwa systemów teleinformatycznych, ochrony danych osobowych, przepisów sektorowych oraz ustawy o krajowym systemie cyberbezpieczeństwa (KSC/NIS2),

5) wsparcie Zamawiającego w realizacji obowiązków związanych z raportowaniem incydentów do właściwego CSIRT, w tym w terminach określonych w ustawie o KSC.

1.3. Zakres monitoringu SOC obejmuje zdarzenia bezpieczeństwa rejestrowane w dziennikach zdarzeń (logach) systemów Zamawiającego. SOC nie dekoduje danych zaszyfrowanych ani nie przetwarza treści danych chronionych — analiza opiera się na metadanych, logach zdarzeń oraz wskaźnikach kompromitacji (IoC). Zasady przetwarzania danych chronionych i sektorowych zostaną określone w umowie powierzenia przetwarzania danych.

2. Zakres przedmiotu zamówienia (etapy realizacji)

2.1. Etap 1: Analiza przedwdrożeniowa i projekt

1) inwentaryzacja systemów, aplikacji, urządzeń sieciowych i bezpieczeństwa oraz innych źródeł logów, które mają zostać objęte monitoringiem SOC,

2) identyfikacja usług krytycznych z punktu widzenia działalności Zamawiającego,

3) analiza wymagań regulacyjnych i organizacyjnych Zamawiającego oraz istniejących procedur bezpieczeństwa, w tym wymagań wynikających z ustawy o KSC,

4) dostosowanie platformy SIEM/SOAR Wykonawcy do środowiska Zamawiającego, obejmujące w szczególności:

a) model zbierania i przekazywania logów,

b) model budowy profili zasobów (assets) oraz ich klasyfikacji pod kątem krytyczności,

c) katalog scenariuszy detekcji (use cases) i poziomów istotności incydentów,

5) przygotowanie planu wdrożenia, w tym harmonogramu, podziału prac i odpowiedzialności,

6) uzgodnienie wzorów protokołów odbioru oraz wzorów raportów okresowych.

Uwaga: Zamawiający zobowiązany jest do współpracy w zakresie udostępnienia źródeł logów, dokumentacji środowiska oraz zapewnienia połączenia sieciowego umożliwiającego przekazywanie logów do platformy SOC Wykonawcy.

2.2. Etap 2: Wdrożenie i konfiguracja platformy SIEM/SOAR/AI

1) konfiguracja środowiska dla systemu klasy SIEM wraz z komponentami odpowiedzialnymi za:

a) zbieranie, normalizację i składowanie logów z wykorzystaniem odpowiednich mechanizmów zbierania, dobieranych w zależności od typu źródła,

b) budowę i utrzymywanie profili zasobów z wykorzystaniem mechanizmów analitycznych platformy, w tym AI,

2) podłączenie wskazanych przez Zamawiającego źródeł logów, dostępnych w infrastrukturze Zamawiającego, oraz weryfikacja poprawności ich działania. W przypadku braku gotowości technicznej źródeł logów po stronie Zamawiającego, Wykonawca wskaże wymagania techniczne niezbędne do ich uruchomienia,

3) konfiguracja mechanizmów korelacji zdarzeń i tworzenia incydentów złożonych, w tym:

a) reguł korelacji opartych o sekwencje oraz złożone zależności czasowe pomiędzy zdarzeniami,

b) przypisywania priorytetu i wagi incydentów z uwzględnieniem wartości biznesowej zasobów oraz poziomu ryzyka,

c) mechanizmów łączenia powiązanych incydentów w większe scenariusze ataku,

4) wdrożenie modułu SOAR, w tym:

a) integracja z systemami Zamawiającego w uzgodnionym zakresie, z uwzględnieniem możliwości technicznych i zgody Zamawiającego, obejmująca w szczególności: system uwierzytelniania platformy SOC (konta tworzone w ramach platformy Wykonawcy), system powiadomień Wykonawcy, system zgłoszeniowy/ITSM Zamawiającego (o ile Zamawiający udostępni interfejs integracyjny API),

b) zdefiniowanie oraz implementacja playbooków (scenariuszy reakcji) dla typowych incydentów bezpieczeństwa, z podziałem na czynności automatyczne, półautomatyczne oraz ręczne,

c) konfiguracja obsługi incydentów w postaci spraw (case management) z możliwością przypisywania zadań, prowadzenia dziennika działań, załączania materiału dowodowego i tworzenia linii czasu,

5) wdrożenie modułu analitycznego z wykorzystaniem mechanizmów sztucznej inteligencji, w tym:

a) konfiguracja funkcji automatycznego wzbogacania incydentów o kontekst pochodzący z wewnętrznych i zewnętrznych źródeł informacji o zagrożeniach,

b) konfiguracja możliwości zadawania zapytań w języku naturalnym przez analityków SOC Wykonawcy, dotyczących incydentów, zasobów, kampanii ataków i wskaźników kompromitacji,

c) konfiguracja mechanizmów automatycznego wyszukiwania powiązań pomiędzy incydentami z wykorzystaniem wnioskowania AI, operującego na zanonimizowanych metadanych i wskaźnikach kompromitacji przetwarzanych w centrum danych na terytorium UE.

2.3. Etap 3: Świadczenie bieżącej usługi SOC

1) stałe monitorowanie zdarzeń bezpieczeństwa w trybie 24/7/365,

2) realizacja następujących czynności operacyjnych:

a) przyjmowanie, rejestrowanie i wstępne kwalifikowanie zdarzeń w ramach platformy SOC Wykonawcy,

b) tworzenie i obsługa incydentów bezpieczeństwa, w tym analiza przyczyn i skutków,

c) wykonywanie działań reakcyjnych zgodnie z uzgodnionymi playbookami, po uprzednim uzyskaniu zgody Zamawiającego w przypadku działań wymagających interakcji ze środowiskiem Zamawiającego,

d) eskalacja incydentów do Zamawiającego zgodnie z matrycą eskalacji opracowaną wspólnie z Zamawiającym na etapie wdrożenia,

3) przekazywanie Zamawiającemu rekomendacji działań naprawczych i doskonalających, wraz z uzasadnieniem wynikającym z analizy danych,

4) wsparcie Zamawiającego w przygotowaniu zgłoszeń incydentów do właściwego CSIRT, zgodnie z wymaganiami ustawy o KSC (wczesne ostrzeżenie — do 24 godzin, zgłoszenie — do 72 godzin, raport końcowy — do 1 miesiąca).

2.4. Etap 4: Raportowanie, przeglądy i doskonalenie

1) przygotowywanie raportów okresowych (miesięcznych i kwartalnych — szczegółowe okresy zostaną określone w umowie), generowanych z platformy SOC, zawierających co najmniej:

a) liczbę i klasyfikację incydentów,

b) czasy reakcji i obsługi,

c) opis najważniejszych incydentów oraz podjętych działań,

d) rekomendacje zmian konfiguracji i polityk bezpieczeństwa,

2) bieżące przeglądy konfiguracji reguł korelacji, scenariuszy detekcji i playbooków, realizowane w trybie ciągłym w ramach procesu doskonalenia usługi,

3) aktualizację listy źródeł logów i zakresu monitoringu w uzgodnieniu z Zamawiającym.

3. Wymagania funkcjonalne systemu klasy SIEM

3.1. System klasy SIEM musi zapewniać co najmniej:

1) gromadzenie, normalizację i korelację logów z systemów operacyjnych, urządzeń sieciowych, systemów bezpieczeństwa, aplikacji, baz danych, systemów katalogowych oraz innych wskazanych źródeł, z wykorzystaniem odpowiednich mechanizmów zbierania dobieranych w zależności od typu źródła (agenty, syslog, API, kolektory),

2) przetwarzanie logów w silniku korelacji z możliwością obsługi danych o ruchu sieciowym (flow), o ile zbieranie flow zostanie uzgodnione z Zamawiającym i wdrożone na etapie integracji,

3) możliwość tworzenia profili zasobów (assets) z wykorzystaniem mechanizmów analitycznych platformy, w tym AI, na podstawie logów oraz wyników skanów podatności (o ile udostępnione przez Zamawiającego), wraz z przypisaniem im poziomu ważności biznesowej,

4) możliwość nadawania incydentom złożonym wagi (np. w skali punktowej) w oparciu o:

a) liczbę oraz rodzaj zdarzeń składowych,

b) krytyczność dotkniętych zasobów,

c) wykryte podatności oraz znane techniki ataku,

5) mechanizmy łączenia powiązanych incydentów i zdarzeń w scenariusze ataków, w celu ograniczenia liczby zgłoszeń wymagających analizy manualnej,

6) możliwość wykonywania zaawansowanych zapytań analitycznych do zgromadzonych danych (język zapytań umożliwiający złożone filtrowanie, agregację oraz analizy przekrojowe),

7) możliwość prowadzenia korelacji historycznej (ponownego przeliczenia reguł na dane z przeszłości) w okresie co najmniej 24 miesięcy, zgodnie z wymaganiami Krajowych Ram Interoperacyjności oraz ustawy o KSC. Okres retencji może zostać dostosowany do wymagań regulacyjnych właściwych dla sektora Zamawiającego,

8) interfejs użytkownika umożliwiający:

a) przegląd bieżących incydentów z podziałem na priorytety i statusy,

b) szczegółowy widok incydentu z listą zdarzeń składowych, osią czasu i widokiem dotkniętych zasobów,

c) tworzenie raportów,

9) mechanizmy zarządzania uprawnieniami użytkowników z możliwością nadawania ról i profili dostępu,

10) rejestrowanie wszystkich działań administracyjnych i operacyjnych w dzienniku audytowym.

3.2. System musi umożliwiać przechowywanie danych dzienników zdarzeń w sposób zapewniający ich integralność, rozliczalność i możliwość odtworzenia chronologii zdarzeń przez okres co najmniej 24 miesięcy, z zachowaniem logicznej separacji danych pomiędzy klientami usługi SOC. Wydłużenie okresu retencji jest możliwe na wniosek Zamawiającego, na warunkach uzgodnionych odrębnie, w tym w zakresie kosztów dodatkowej przestrzeni dyskowej.

4. Wymagania funkcjonalne modułu SOAR

4.1. Moduł orkiestracji i automatyzacji reakcji (SOAR) musi zapewniać:

1) zarządzanie incydentami w postaci spraw (case management) z możliwością:

a) przypisywania właścicieli i zespołów,

b) definiowania i śledzenia zadań,

c) dodawania notatek, załączników oraz materiału dowodowego,

2) definiowanie oraz wykonywanie playbooków reakcji na incydenty, w tym:

a) czynności wykonywane automatycznie na podstawie zdarzeń w systemie SIEM,

b) czynności wymagające akceptacji użytkownika (workflow zatwierdzeń),

c) czynności manualne wspierane listami kontrolnymi,

3) integrację z systemami Zamawiającego w uzgodnionym zakresie, na podstawie odrębnie uzgodnionych uprawnień i procedur autoryzacji. Wykonywanie automatycznych akcji w środowisku Zamawiającego (np. blokada adresu IP, zablokowanie konta, otwarcie/aktualizacja zgłoszenia) wymaga uprzedniej formalnej zgody Zamawiającego oraz udostępnienia dedykowanych kont serwisowych o określonym zakresie uprawnień,

4) rejestrowanie pełnej historii działań w ramach obsługi incydentu, z datą, godziną, osobą/rolą i opisem wykonanej czynności, zgodnie z procedurami operacyjnymi Wykonawcy, w tym procedurami zarządzania zmianami personalnymi na dyżurach,

5) możliwość budowania raportów z przebiegu obsługi incydentów, generowanych automatycznie z rejestru działań platformy SOAR.

5. Wymagania dotyczące modułu analitycznego z wykorzystaniem sztucznej inteligencji

5.1. Moduł analityczny musi:

1) wykorzystywać mechanizmy uczenia maszynowego oraz przetwarzania języka naturalnego do:

a) automatycznego wyszukiwania powiązań pomiędzy incydentami i zdarzeniami,

b) wzbogacania incydentów o informacje pochodzące z wewnętrznych i zewnętrznych źródeł wiedzy o zagrożeniach,

c) generowania syntetycznych podsumowań incydentów oraz rekomendowanych działań,

2) umożliwiać analitykom SOC Wykonawcy zadawanie zapytań w języku naturalnym dotyczących:

a) zgromadzonych danych i incydentów,

b) znanych technik ataku oraz kampanii,

c) powiązań pomiędzy wskaźnikami kompromitacji,

3) działać w sposób, który nie powoduje przesyłania do środowiska zewnętrznego pełnych dzienników zdarzeń ani danych osobowych. Moduł AI przetwarza wyłącznie zanonimizowane wskaźniki kompromitacji i metadane w centrum przetwarzania danych zlokalizowanym na terytorium Unii Europejskiej (Frankfurt, Niemcy).

6. Wymagania organizacyjne i SLA

6.1. Usługa SOC musi być świadczona w trybie 24/7/365.

6.2. Wykonawca zapewni poziomy istotności incydentów oraz odpowiadające im maksymalne czasy reakcji i czasy podjęcia działań. Minimalne wymagane parametry SLA określa poniższa tabela (szczegółowe parametry zostaną doprecyzowane w umowie):

Poziom	Opis	Czas reakcji	Czas podjęcia działań
Krytyczny (P1)	Incydent zagrażający ciągłości działania usług krytycznych	≤ 30 minut	≤ 2 godzin
Wysoki (P2)	Incydent o istotnym wpływie na bezpieczeństwo	≤ 1 godziny	≤ 4 godzin
Średni (P3)	Incydent o umiarkowanym wpływie	≤ 2 godzin	≤ 8 godzin
Niski (P4)	Zdarzenie informacyjne, brak bezpośredniego zagrożenia	≤ 8 godzin	Następny dzień roboczy

6.3. Wykonawca zapewni:

1) dedykowany punkt kontaktowy dla Zamawiającego (dane kontaktowe zostaną przekazane na etapie wdrożenia),

2) możliwość zgłaszania incydentów poprzez: portal zgłoszeniowy (priorytetowy kanał komunikacji), pocztę elektroniczną oraz telefonicznie (dla incydentów krytycznych P1),

3) okresowe spotkania robocze (co najmniej kwartalne) w celu omówienia wyników pracy SOC.

7. Wymagania w zakresie bezpieczeństwa i zgodności

7.1. Wykonawca zobowiązany jest do świadczenia usługi zgodnie z obowiązującymi przepisami prawa, w szczególności w zakresie:

1) ochrony danych osobowych (RODO),

2) bezpieczeństwa systemów teleinformatycznych jednostek sektora publicznego,

3) ustawy o krajowym systemie cyberbezpieczeństwa (KSC) wdrażającej dyrektywę NIS2,

4) przepisów sektorowych właściwych dla Zamawiającego.

7.2. Dane Zamawiającego muszą być przetwarzane i przechowywane w centrach przetwarzania danych zlokalizowanych na terytorium państw członkowskich Unii Europejskiej lub Europejskiego Obszaru Gospodarczego. Przetwarzanie danych przez moduł AI odbywa się w centrum danych we Frankfurcie (Niemcy).

7.3. System SOC musi zapewniać:

1) rejestrowanie działań użytkowników i administratorów,

2) kontrolę dostępu opartą o indywidualne konta i uprawnienia,

3) możliwość przeprowadzenia audytu ścieżki postępowania z incydentem (pełna ścieżka audytowa realizowana przez moduł SOAR).

7.4. Dzienniki zdarzeń objęte usługą SOC muszą być przechowywane przez okres co najmniej 24 miesięcy, z zachowaniem logicznej separacji danych pomiędzy klientami usługi SOC. Zamawiający może wymagać dłuższego okresu przechowywania, o czym poinformuje Wykonawcę na etapie postępowania lub realizacji umowy; warunki dłuższej retencji, w tym koszty dodatkowej przestrzeni dyskowej, zostaną określone odrębnie.

8. Wymagania dotyczące personelu Wykonawcy

8.1. Wykonawca musi dysponować zespołem realizującym usługę SOC, w skład którego wchodzą osoby posiadające doświadczenie i kwalifikacje adekwatne do powierzonych zadań.

8.2. Zamawiający wymaga, aby w zespole Wykonawcy (liczonym łącznie dla wszystkich osób zaangażowanych w realizację umowy) znajdowały się osoby posiadające następujące certyfikaty:

1) co najmniej 2 osoby z ważnym certyfikatem Audytora Wiodącego systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001 lub certyfikatem równoważnym,

2) co najmniej 1 osoba z ważnym certyfikatem Audytora Wiodącego systemu zarządzania ciągłością działania zgodnego z normą ISO/IEC 22301 lub certyfikatem równoważnym,

3) co najmniej 1 osoba z ważnym certyfikatem OSCP lub certyfikatem równoważnym, potwierdzającym zaawansowane kompetencje w zakresie testów penetracyjnych,

4) co najmniej 1 osoba z ważnym certyfikatem OSCE lub certyfikatem równoważnym, potwierdzającym zaawansowane kompetencje w zakresie technik ataku i obrony,

5) co najmniej 1 osoba z ważnym certyfikatem eWPTXv2 lub certyfikatem równoważnym, potwierdzającym kompetencje w zakresie zaawansowanego testowania bezpieczeństwa aplikacji webowych,

6) co najmniej 1 osoba z ważnym certyfikatem eCPPTv2 lub certyfikatem równoważnym, potwierdzającym kompetencje w zakresie kompleksowych testów penetracyjnych,

7) co najmniej 1 osoba z ważnym certyfikatem eCDFP lub certyfikatem równoważnym, potwierdzającym kompetencje w zakresie informatyki śledczej i analizy powłamaniowej.

8.3. Dopuszcza się, aby jedna osoba posiadała więcej niż jeden z wyżej wymienionych certyfikatów, pod warunkiem spełnienia minimalnych wymagań liczbowych dla każdego certyfikatu.

8.4. Zamawiający zastrzega sobie możliwość określenia dodatkowych wymagań dotyczących kwalifikacji i certyfikacji personelu Wykonawcy na etapie postępowania lub negocjacji, w szczególności w odniesieniu do:

1) zarządzania incydentami bezpieczeństwa,

2) zarządzania ryzykiem,

3) specjalistycznych szkoleń i certyfikatów produktowych.

9. Odbiór, testy i dokumentacja

9.1. Odbiór etapu wdrożeniowego nastąpi na podstawie protokołu odbioru (wzór protokołu zostanie uzgodniony na etapie Etapu 1) po pozytywnym przeprowadzeniu testów akceptacyjnych, obejmujących co najmniej:

1) weryfikację poprawności zbierania logów z ustalonych źródeł,

2) weryfikację poprawności działania reguł korelacji oraz tworzenia incydentów złożonych,

3) weryfikację działania wybranych playbooków w module SOAR,

4) weryfikację działania modułu analitycznego SI (np. generowanie podsumowań i powiązań dla przykładowych incydentów),

5) weryfikację możliwości generowania raportów zgodnie z uzgodnionymi wzorami.

9.2. Wykonawca przekaże dokumentację powykonawczą na poziomie funkcjonalnym, bez ujawniania szczegółów konfiguracji stanowiących know-how Wykonawcy, obejmującą co najmniej:

1) opis architektury rozwiązania (na poziomie logicznym),

2) wykaz podłączonych źródeł logów i zakres zbieranych danych,

3) opis kluczowych reguł korelacji (na poziomie funkcjonalnym),

4) opis wdrożonych playbooków oraz zasad obsługi incydentów,

5) procedury współpracy Zamawiającego z SOC (eskalacje, komunikacja, raportowanie),

6) opis polityki retencji danych.

9.3. W trakcie świadczenia usługi Wykonawca będzie przekazywał Zamawiającemu raporty okresowe w uzgodnionej formie i terminach.

10. Postanowienia końcowe

10.1. Wszelkie wymagania określone w niniejszym OPZ stanowią wymagania minimalne Zamawiającego i zostały opisane w sposób funkcjonalny, bez wskazywania konkretnych producentów lub nazw handlowych.

10.2. Dopuszcza się zaoferowanie rozwiązań równoważnych, spełniających w co najmniej równym stopniu wszystkie wymagania określone w OPZ, a także parametrów lepszych niż wymagane, pod warunkiem zachowania zgodności z przepisami prawa oraz zasadami uczciwej konkurencji.

10.3. Szczegółowe warunki współpracy, w tym parametry SLA, zasady odpowiedzialności, tryb eskalacji, zasady przetwarzania danych oraz umowa powierzenia przetwarzania danych osobowych, zostaną określone w umowie zawartej z wybranym Wykonawcą.

10.4. Usługa SOC jest świadczona w modelu zdalnym, z wykorzystaniem platformy SIEM/SOAR zlokalizowanej w centrum danych Wykonawcy na terytorium UE. Zamawiający zapewnia połączenie sieciowe umożliwiające bezpieczne przekazywanie logów do platformy SOC.

13. Opracowanie i wdrożenie dokumentacji SZBI.

W ramach warsztatów prowadzonych z osobą prowadzącą w obszarze Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) przewiduje się przegląd oraz omówienie przykładowej dokumentacji SZBI. Uczestnicy warsztatów zostaną również zaangażowani w proces opracowania nowej dokumentacji, dostosowanej do specyficznych potrzeb organizacji, zgodnie z obowiązującymi normami oraz wymaganiami.

Celem warsztatów jest przekazanie praktycznej wiedzy z zakresu opracowania, ustanawiania, wdrażania, eksploatacji, monitorowania i przeglądu, a także utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji, zapewniającego poufność, dostępność i integralność informacji, z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność oraz niezawodność.

Dokumentacja musi zawierać następujące kryteria:

1. Ewidencja Obszaru Przetwarzania Informacji:

- Dokument musi zawierać ewidencję obszarów przetwarzania informacji, obejmującą lokalizacje wraz z oznaczeniami, nazwami, kondygnacjami i adresami.
- Dokument powinien służyć do monitorowania i zarządzania miejscami, w których przetwarzane są chronione informacje.

2. Wprowadzenie do Systemu Zarządzania Bezpieczeństwem informacji

- Dokument musi definiować podstawowe zasady Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym ochronę aktywów informacyjnych, monitorowanie ryzyk oraz wdrażanie zabezpieczeń.
- Dokument powinien opisywać procesy zarządzania bezpieczeństwem informacji, bazujące na cyklu PDCA (Plan-Do-Check-Act), obejmujące szacowanie ryzyka, monitorowanie skuteczności zabezpieczeń i ich doskonalenie.

3. Terminy stosowane w Systemie Zarządzania Bezpieczeństwem Informacji

- Dokument musi zawierać definicje terminów stosowanych w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI), takich jak ryzyko, aktywa informacyjne, incydent bezpieczeństwa oraz cyberbezpieczeństwo.

- Każdy termin powinien być dokładnie opisany, uwzględniając jego znaczenie oraz zastosowanie w kontekście zarządzania bezpieczeństwem informacji.

4. Kontekst Organizacji

- Dokument musi opisywać czynniki zewnętrzne i wewnętrzne wpływające na organizację w kontekście Systemu Zarządzania Bezpieczeństwem Informacji, w tym aspekty prawne, regulacyjne, technologiczne, społeczne oraz finansowe.

- Dokument powinien określać zakres Systemu Zarządzania Bezpieczeństwem Informacji, uwzględniając lokalizacje, procesy, zasoby oraz jednostki organizacyjne, które są objęte systemem.

5. Zarządzanie Ryzykiem w Bezpieczeństwie informacji

- Dokument musi opisywać proces zarządzania ryzykiem w bezpieczeństwie informacji, obejmujący identyfikację, analizę, ocenę oraz postępowanie z ryzykiem, w tym kryteria oceny ryzyka i akceptacji ryzyka.

- Dokument powinien definiować metodykę szacowania ryzyka, w tym sposób określania prawdopodobieństwa, skutków oraz przypisywania wartości ryzyka, a także wytyczne dotyczące akceptowania, monitorowania i przeglądu ryzyka.

6. Instrukcja Szacowania i Postępowania z Ryzykiem w Bezpieczeństwie Informacji

- Instrukcja musi opisywać proces szacowania i postępowania z ryzykiem w bezpieczeństwie informacji, obejmujący identyfikację zagrożeń, podatności oraz aktywów i ich zabezpieczeń, których ryzyko dotyczy.

- Dokument powinien zawierać szczegółowe wytyczne dotyczące analizy ryzyka, w tym oszacowanie następstw, prawdopodobieństwa, poziomów ryzyka oraz metody określania i dokumentowania działań w zakresie postępowania z ryzykiem.

7. Działania odnoszące się do Ryzyk i Szans Systemu Zarządzania Bezpieczeństwem Informacji.

- Dokument musi opisywać działania odnoszące się do zidentyfikowanych ryzyk i szans w Systemie Zarządzania Bezpieczeństwem Informacji, w tym określenie sposobów realizacji działań oraz ich integrację z procesami SZBI.

- Dokument powinien zawierać wytyczne dotyczące oceny skuteczności działań, uwzględniając monitorowanie, pomiary, audyty oraz przeglądy zarządzania, aby zapewnić zgodność z wymaganiami prawnymi oraz bezpieczeństwo informacji.

8. Deklaracja Stosowania Opracowana

- Dokument musi zawierać wykaz zabezpieczeń stosowanych w Systemie Zarządzania Bezpieczeństwem Informacji, wraz z uzasadnieniem ich wyboru oraz oceną wdrożenia lub wyłączenia, zgodnie z Załącznikiem A normy ISO/IEC 27001.

- Dokument powinien opisywać sposób wdrożenia zabezpieczeń, wskazując ich cel, specyfikę działalności oraz wyniki analizy ryzyka, a także uzasadniać ewentualne wyłączenia zabezpieczeń.

9. Cele bezpieczeństwa informacji

- Dokument musi określać cele bezpieczeństwa informacji, które obejmują zarządzanie ryzykiem, incydentami, zgodność z przepisami oraz zapewnienie ciągłości działania i bezpieczeństwa aktywów.

- Dokument powinien zawierać mierzalne wskaźniki realizacji celów, w tym liczbę audytów, szkoleń, zgłoszeń incydentów, a także utrzymywanie odpowiednich rejestrów i ewidencji aktywów.

10. Plan osiągniecia Celów Bezpieczeństwa Informacji

- Dokument musi zawierać plan realizacji celów bezpieczeństwa informacji, określając zadania, wskaźniki oraz harmonogram ich realizacji i weryfikacji, zgodnie z raportami z monitorowania i pomiarów systemu zarządzania bezpieczeństwem informacji.

- Plan powinien przypisywać odpowiedzialność za realizację poszczególnych zadań oraz wskazywać kluczowe cele, takie jak zarządzanie ryzykiem, incydentami, ciągłością działania oraz zgodność z wymaganiami prawnymi i regulacyjnymi.

11. Monitorowanie, Pomiary, Analiza i Ocena Systemu Zarządzania Bezpieczeństwem Informacji

- Dokument musi opisywać proces monitorowania, pomiarów, analizy i oceny Systemu Zarządzania Bezpieczeństwem Informacji, obejmujący zgodność z wymaganiami prawnymi oraz skuteczność w osiąganiu celów bezpieczeństwa informacji.

- Dokument powinien zawierać wskaźniki monitorowania oraz określać odpowiedzialność Pełnomocnika ds. Bezpieczeństwa Informacji za utrzymywanie raportów i ich przekazywanie Najwyższemu Kierownictwu.

12. Raport z Monitorowania, Pomiarów, Analizy i Oceny Systemu Zarządzania Bezpieczeństwem informacji

- Raport musi zawierać wyniki monitorowania, pomiarów, analizy i oceny Systemu Zarządzania Bezpieczeństwem Informacji, w tym liczbę audytów, działań zaradczych, incydentów oraz wskaźniki ryzyka i zgodności z wymaganiami prawnymi.

- Dokument powinien zawierać przegląd zapisów i wskaźników monitorowania z poprzedniego roku oraz przypisywać odpowiedzialność za realizację poszczególnych działań związanych z zarządzaniem bezpieczeństwem informacji.

13. Raport z Audytu Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji

- Raport z audytu wewnętrznego musi zawierać ocenę zgodności Systemu Zarządzania Bezpieczeństwem Informacji z wymaganiami prawnymi i regulacyjnymi, a także oceniać jego skuteczność w osiąganiu zamierzonych celów.

- Dokument powinien przedstawiać ustalenia audytu, w tym wykryte zgodności i niezgodności, dowody potwierdzające oraz zalecenia audytora dotyczące doskonalenia systemu.

14. Audyty Wewnętrzne Systemu Zarządzania Bezpieczeństwem Informacji

- Dokument musi definiować zasady i procedury przeprowadzania audytów wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z normami ISO oraz wymogami prawnymi, w tym zasady rzetelności, poufności, niezależności i podejścia opartego na dowodach.

- Dokument powinien opisywać zarządzanie programem audytów, w tym jego tworzenie, zatwierdzanie, przygotowanie planów audytów, przeprowadzanie działań audytowych oraz działania poaudytowe, wraz z odpowiedzialnością za realizację i doskonalenie audytów.

15. Plan Audytu Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji.

- Plan Audytu Wewnętrznego musi określać cele, zakres, kryteria oraz metody przeprowadzania audytu, w tym audyty na miejscu i zdalne, a także analizę dokumentów, obserwację pracy i rozmowy z personelem.

- Dokument powinien zawierać informacje o odpowiednich wymaganiach prawnych i regulacyjnych, procesach do audytu, oraz wskazywać lokalizacje i osoby odpowiedzialne za poszczególne etapy audytu.

16. Program Audytów Wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji

- Program Audytów Wewnętrznych musi zawierać liczbę i rodzaje zaplanowanych audytów, ich cele, zakres oraz kryteria, zgodnie z wymaganiami prawnymi i regulacyjnymi dotyczącymi Systemu Zarządzania Bezpieczeństwem Informacji.

- Dokument powinien definiować metody audytu, takie jak wizyty, przegląd dokumentów, rozmowy oraz analizę danych, a także przypisywać odpowiedzialność za realizację audytów Pełnomocnikowi ds. Bezpieczeństwa Informacji.

17. Przegląd Zarządzania

- Dokument Przegląd Zarządzania musi zawierać coroczną ocenę przydatności, adekwatności i skuteczności Systemu Zarządzania Bezpieczeństwem Informacji, w tym analizę działań korygujących, doskonalących oraz wdrożonych w wyniku incydentów i audytów wewnętrznych.

- Dokument powinien obejmować przegląd zmian czynników zewnętrznych i wewnętrznych, analizę wyników monitorowania systemu, cele bezpieczeństwa oraz informacje zwrotne od stron zainteresowanych.

18. Raport z Przeglądu Zarządzania

- Raport z Przeglądu Zarządzania musi zawierać ocenę działań podjętych po wcześniejszych przeglądach zarządzania, analizę czynników zewnętrznych i wewnętrznych oraz informacje o działaniach korygujących i doskonalących w obszarze bezpieczeństwa informacji.

- Dokument powinien obejmować wyniki audytów wewnętrznych, analizę celów bezpieczeństwa informacji, a także możliwości doskonalenia systemu wynikające z raportów oraz przeglądów.

19. Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji

- Dokument musi opisywać procedury identyfikacji, korygowania i doskonalenia niezgodności w Systemie Zarządzania Bezpieczeństwem Informacji, w tym działania eliminujące przyczyny niezgodności oraz ocenę skuteczności wdrożonych środków korygujących.

- Dokument powinien obejmować proces ciągłego doskonalenia systemu poprzez regularne przeglądy, monitorowanie, analizę oraz raportowanie działań doskonalących i korygujących.

20. Polityka Bezpieczeństwa Informacji

- Polityka Bezpieczeństwa Informacji musi określać ogólne kierunki i wytyczne w zakresie ochrony informacji, w tym zarządzanie poufnością, integralnością, dostępnością oraz innymi atrybutami bezpieczeństwa, takimi jak autentyczność, rozliczalność i niezaprzeczalność.

- Dokument powinien obejmować zasady zarządzania ryzykiem, incydentami oraz ciągłością bezpieczeństwa informacji, a także uwzględniać wymagania prawne, regulacyjne i umowne, zgodnie z przyjętymi celami bezpieczeństwa informacji.

21. Raport z Przeglądu Udokumentowanych Informacji Systemu Zarządzania Bezpieczeństwem Informacji

- Raport z Przeglądu Udokumentowanych Informacji musi obejmować ocenę zgodności udokumentowanych informacji Systemu Zarządzania Bezpieczeństwem Informacji, zidentyfikowane modyfikacje oraz propozycje aktualizacji w przypadku stwierdzenia potrzeby zmiany.

- Dokument powinien zawierać przegląd poszczególnych polityk, procedur, rejestrów i planów, w tym propozycje aktualizacji wynikające z analizy ryzyk, audytów wewnętrznych i przeglądów zarządzania.

22. Rejestr Właścicieli Udokumentowanych Informacji Systemu Zarządzania Bezpieczeństwem Informacji

- Rejestr Właścicieli Udokumentowanych Informacji musi zawierać wykaz dokumentów Systemu Zarządzania Bezpieczeństwem Informacji wraz z przypisanymi do nich właścicielami, odpowiedzialnymi za ich utrzymanie, aktualizację i zgodność z systemem.

- Dokument powinien wskazywać funkcje i stanowiska osób odpowiedzialnych za poszczególne udokumentowane informacje, aby zapewnić nadzór i odpowiedzialność nad ich prawidłowym zarządzaniem.

23. Role, Odpowiedzialność i Uprawnienia w Systemie Zarządzania Bezpieczeństwem Informacji

- Dokument musi definiować role, odpowiedzialność i uprawnienia związane z zarządzaniem bezpieczeństwem informacji, w tym Najwyższe Kierownictwo, Pełnomocnika ds. Bezpieczeństwa Informacji, Inspektora Ochrony Danych, Administratora Systemów Informatycznych oraz inne osoby przetwarzające informacje.

- Dokument powinien określać obowiązki związane z nadzorem nad zarządzaniem ryzykiem, incydentami, bezpieczeństwem aktywów, a także zobowiązania do raportowania, przeglądów i doskonalenia systemu zarządzania bezpieczeństwem informacji.

24. Polityka Stosowana Urządzeń Mobilnych

- Polityka Stosowania Urządzeń Mobilnych musi określać zasady zarządzania i zabezpieczania urządzeń mobilnych oraz zewnętrznych nośników danych, w tym autoryzację ich użytkowania poza organizacją, zgodnie z wymaganiami Polityki Zarządzania Aktywami.

- Dokument powinien zawierać wytyczne dotyczące ochrony informacji przechowywanych w urządzeniach mobilnych, w tym ich szyfrowania, zabezpieczania przed utratą, kradzieżą lub nieuprawnionym dostępem, zgodnie z Polityką Kryptografii i innymi regulacjami bezpieczeństwa.

25. Polityka Pracy Zdalnej

- Polityka Pracy Zdalnej musi określać zasady świadczenia pracy zdalnej, w tym wytyczne dotyczące zabezpieczenia aktywów oraz informacji przetwarzanych poza siedzibą organizacji, zgodnie z wymaganiami prawnymi i regulacyjnymi.

- Dokument powinien zawierać wytyczne dotyczące kontroli bezpieczeństwa, użycia narzędzi pracy oraz odpowiednich zabezpieczeń technicznych i organizacyjnych, zapewniając ochronę danych osobowych oraz tajemnic prawnie chronionych.

26. Polityka Bezpieczeństwa Zasobów Ludzkich

- Polityka Bezpieczeństwa Zasobów Ludzkich musi określać zasady zarządzania personelem w zakresie bezpieczeństwa informacji, w tym procesy rekrutacji, szkolenia, świadomości oraz procedury postępowania przed, w trakcie i po zakończeniu zatrudnienia.

- Dokument powinien zawierać wytyczne dotyczące weryfikacji kandydatów, nadawania i odbierania uprawnień, zarządzania incydentami bezpieczeństwa oraz zobowiązań personelu do przestrzegania zasad bezpieczeństwa informacji, także po zakończeniu zatrudnienia.

27. Wniosek o Nadanie, Zmianę lub Odebranie Dostępu do Systemów Informatycznych

- Wniosek o Nadanie, Zmianę lub Odebranie Dostępu do Systemów Informatycznych musi zawierać dane dotyczące systemów informatycznych, w tym nazwę systemu, identyfikator użytkownika oraz dane uwierzytelniające, a także określać rodzaj wnioskowanej operacji (nadanie, zmiana, odebranie dostępu).

- Dokument powinien być zatwierdzany przez kierującego jednostką organizacyjną oraz Administratora Systemów Informatycznych, potwierdzając nadanie, zmianę lub odebranie dostępu do wskazanych systemów.

28. Oświadczenie o Przestrzeganiu Wymagań Dotyczących Bezpieczeństwa Informacji

- Oświadczenie o Przestrzeganiu Wymagań Dotyczących Bezpieczeństwa Informacji musi zobowiązywać pracowników do przestrzegania wymagań prawnych, regulacyjnych i umownych dotyczących bezpieczeństwa informacji, w tym ochrony danych osobowych.

- Dokument powinien określać obowiązek stosowania środków technicznych i organizacyjnych, zgłaszania incydentów oraz zachowania poufności przetwarzanych informacji, także po zakończeniu współpracy.

29. Upoważnienie do Przetwarzania Informacji

- Upoważnienie do Przetwarzania Informacji musi zawierać dane osoby upoważnionej, stanowisko, funkcję oraz zakres przetwarzania informacji, w tym procesy i cele przetwarzania, a także daty obowiązywania upoważnienia.

- Dokument powinien być podpisany przez osobę upoważniającą oraz osobę upoważnioną, potwierdzając wydanie i odbiór upoważnienia, a wszelkie wcześniejsze upoważnienia tracą ważność.

30. Polityka Zarządzania Aktywami

- Polityka Zarządzania Aktywami musi definiować zasady inwentaryzacji, klasyfikacji oraz odpowiedzialności za aktywa organizacji, w tym identyfikację właścicieli aktywów i procedury zarządzania nimi w celu zapewnienia ich ochrony.

- Dokument powinien zawierać wytyczne dotyczące bezpiecznego użytkowania, przechowywania oraz wycofywania aktywów, w tym nośników informacji, zgodnie z wymaganiami prawnymi i regulacyjnymi.

31. Ewidencja Aktywów Podstawowych

- Ewidencja Aktywów Podstawowych musi zawierać identyfikację procesów, ich właścicieli oraz szczegółowe dane na temat rodzaju i typów procesów, w tym cele przetwarzania informacji, źródła danych, metody monitorowania oraz kontrolowania przebiegu procesów.

- Dokument powinien zawierać opisy mierników wejściowych i wyjściowych oraz określać powiązania między procesami, wskazując na ich wpływ i zależności, a także odpowiedzialność za nadzór nad aktywami i ich bezpieczeństwo.

32. Ewidencja Obszaru Przetwarzania Informacji

- Ewidencja Obszaru Przetwarzania Informacji musi zawierać oznaczenia, lokalizacje, kondygnacje oraz adresy fizycznych miejsc, w których przetwarzane są informacje w ramach Systemu Zarządzania Bezpieczeństwem Informacji.

- Dokument powinien umożliwiać identyfikację obszarów przetwarzania informacji, co pozwala na ich ewidencjonowanie i nadzór nad bezpieczeństwem fizycznym przetwarzanych danych.

33. Polityka Kontroli Dostępu

- Polityka Kontroli Dostępu musi definiować zasady autoryzacji i ograniczania dostępu do aktywów oraz informacji, zgodnie z wymaganiami prawnymi, regulacyjnymi i umownymi, aby zapewnić, że dostęp mają tylko uprawnieni użytkownicy.

- Dokument powinien obejmować procedury bezpiecznego logowania, zarządzania hasłami, kontrolę dostępu do systemów i aplikacji oraz odpowiedzialność użytkowników za poufne informacje uwierzytelniające.

34. Wymagania w Dostępie do Aktywów dla Personelu

- Dokument Wymagania w Dostępie do Aktywów dla Personelu musi określać zasady przyznawania dostępu do aktywów wyłącznie dla uprawnionych osób, zgodnie z nadanymi upoważnieniami oraz zabezpieczeniami wdrożonymi w organizacji.

- Dokument powinien zawierać wytyczne dotyczące zabezpieczania nośników informacji, stosowania polityki czystego biurka i ekranu, a także obowiązek zgłaszania incydentów bezpieczeństwa zgodnie z Polityką Zarządzania Incydentami.

35. Wymagania w Dostępie do Aktywów dla Podmiotów Zewnętrznych

- Dokument Wymagania w Dostępie do Aktywów dla Podmiotów Zewnętrznych musi określać zasady dostępu podmiotów zewnętrznych do aktywów organizacji, ograniczając dostęp do zakresu niezbędnego do realizacji określonych działań zgodnie z umowami, w tym Umowami o Zachowaniu Poufności oraz Umowami Przetwarzania Danych Osobowych.

- Dokument powinien zawierać wytyczne dotyczące nadzoru nad przetwarzaniem informacji przez podmioty zewnętrzne oraz obowiązek zgłaszania wszelkich stwierdzonych lub domniemanych nieprawidłowości związanych z przetwarzaniem aktywów.

36. Procedura Dostępu do Sieci i Usług Sieciowych

- Procedura Dostępu do Sieci i Usług Sieciowych musi określać zasady przyznawania dostępu do sieci i usług sieciowych wyłącznie uprawnionym użytkownikom, zgodnie z wymaganiami dotyczącymi identyfikacji, uwierzytelniania i autoryzacji.

- Dokument powinien zawierać wytyczne dotyczące sposobów dostępu, takich jak sieci przewodowe, bezprzewodowe, VPN, oraz połączenia zdalne, a także nadzór nad połączeniami przez Administratora Systemów Informatycznych.

37. Procedura Zarządzania Dostępem Użytkowników

- Procedura Zarządzania Dostępem Użytkowników musi określać zasady rejestrowania, wyrejestrowywania, przydzielania i odbierania praw dostępu użytkownikom systemów informatycznych, zgodnie z upoważnieniami oraz Wnioskami o Nadanie, Zmianę lub Odebranie Dostępu.

- Dokument powinien zawierać wytyczne dotyczące zarządzania prawami uprzywilejowanego dostępu, przeglądów praw dostępu użytkowników oraz bezpiecznego przydzielania poufnych informacji uwierzytelniających.

38. Instrukcja Szyfrowania Informacji w Postaci Cyfrowej z Wykorzystaniem Aplikacji 7-Zip

- Instrukcja musi opisywać proces szyfrowania informacji w postaci cyfrowej przy użyciu aplikacji 7-Zip, w tym instalację oprogramowania oraz procedurę szyfrowania plików z zastosowaniem odpowiednich zabezpieczeń.

- Dokument powinien zawierać wytyczne dotyczące tworzenia bezpiecznych haseł zgodnie z Zasadami Tworzenia i Postępowania z Hasłami oraz sposób odszyfrowania plików przy użyciu właściwego hasła.

39. Polityka Kryptografii

- Polityka Kryptografii musi określać zasady stosowania kryptografii do ochrony poufności, autentyczności i integralności informacji, w tym wymagania dotyczące szyfrowania informacji na nośnikach wymiennych i urządzeniach przenośnych.

- Dokument powinien zawierać wytyczne dotyczące zarządzania kluczami kryptograficznymi, w tym ich generowanie, przechowywanie, archiwizowanie, dystrybucję oraz bezpieczne niszczenie po wycofaniu z użytku.

40. Polityka Bezpieczeństwa Fizycznego i Środowiskowego

- Polityka Bezpieczeństwa Fizycznego i Środowiskowego musi określać zasady zabezpieczania obszarów, w których przetwarzane są informacje, w tym zabezpieczenia wejść, ochronę przed zagrożeniami zewnętrznymi i środowiskowymi oraz kontrolę dostępu do obszarów bezpiecznych.

- Dokument powinien zawierać wytyczne dotyczące ochrony sprzętu, monitorowania warunków środowiskowych, bezpieczeństwa okablowania oraz zasad wynoszenia i zbywania aktywów, w tym stosowanie polityki czystego biurka i czystego ekranu.

41. Polityka Bezpiecznej Eksploatacji

- Polityka Bezpiecznej Eksploatacji musi definiować zasady bezpiecznej eksploatacji systemów informacyjnych, w tym dokumentowanie procedur operacyjnych, zarządzanie zmianami oraz monitorowanie wydajności i pojemności systemów.

- Dokument powinien obejmować wytyczne dotyczące ochrony przed szkodliwym oprogramowaniem, rejestrowania zdarzeń, zarządzania kopią zapasową oraz odpowiedzialności za instalację, konserwację i audyt systemów informacyjnych.

42. Czynności Zabronione

- Dokument "Czynności Zabronione" musi zawierać wykaz działań niedozwolonych w zakresie przetwarzania informacji, takich jak nieujawnianie haseł, niewykorzystywanie nieautoryzowanego oprogramowania oraz obowiązek stosowania polityki czystego biurka i ekranu.

- Dokument powinien określać zasady ochrony urządzeń przed nieuprawnionym dostępem, zakaz używania tego samego hasła w wielu systemach oraz obowiązek szyfrowania chronionych informacji na nośnikach danych i podczas ich przesyłania.

43. Procedura Instalacji i Konfiguracji Systemów Informacyjnych

- Procedura Instalacji i Konfiguracji Systemów Informacyjnych musi definiować zasady instalacji i konfiguracji oprogramowania oraz sprzętu komputerowego przez Administratora Systemów Informatycznych lub inny upoważniony personel, uwzględniając wymagania bezpieczeństwa wynikające z polityk organizacji.

- Dokument powinien zawierać wytyczne dotyczące zarządzania zmianami oprogramowania, utrzymywania poprzednich wersji oraz nadzoru nad dostępem serwisantów dostawców, aby zapobiegać incydentom związanym z bezpieczeństwem informacji.

44. Procedura Konserwacji i Napraw Urządzeń Komputerowych

- Procedura Konserwacji i Napraw Urządzeń Komputerowych musi definiować zasady wykonywania konserwacji i napraw urządzeń komputerowych przez Administratora Systemów Informatycznych lub podmioty zewnętrzne, zgodnie z warunkami określonymi przez producenta.

- Dokument powinien zawierać wytyczne dotyczące nadzoru nad naprawami realizowanymi przez podmioty zewnętrzne oraz obowiązek usunięcia nośników danych lub informacji przed przekazaniem urządzeń do serwisu zewnętrznego.

45. Procedura Obsługi Nośników Informacji

- Procedura Obsługi Nośników Informacji musi określać zasady ochrony nośników informacji przed ich utratą, zniszczeniem, nieuprawnionym odczytem oraz modyfikacją, zarówno dla nośników analogowych, jak i cyfrowych.

- Dokument powinien zawierać wytyczne dotyczące niszczenia uszkodzonych nośników danych, trwałego usuwania informacji przed przekazaniem nośników innym osobom lub podmiotom oraz zgodności z Polityką Zarządzania Aktywami.

46. Procedura Użytkowania Systemów Informacyjnych

- Procedura Użytkowania Systemów Informacyjnych musi definiować zasady korzystania z systemów informacyjnych wyłącznie przez uprawniony personel, zgodnie z przydzielonymi upoważnieniami oraz Polityką Kontroli Dostępu, obejmując autoryzację i uwierzytelnianie.

- Dokument powinien zawierać wytyczne dotyczące odpowiedzialności użytkowników za poufność danych uwierzytelniających, zgłaszanie awarii oraz zgodność użytkowania z warunkami określonymi przez organizację

47. Procedura uruchamiania i Zatrzymania Komputera

- Procedura Uruchamiania i Zatrzymania Komputera musi definiować zasady prawidłowego uruchamiania komputera, w tym sprawdzenie połączeń, włączanie zasilania oraz proces uwierzytelniania użytkownika przy dostępie do systemu operacyjnego.

- Dokument powinien zawierać wytyczne dotyczące bezpiecznego zamykania systemu, odłączania urządzeń przenośnych oraz wyłączania komputera, zabraniając wyłączania poprzez bezpośrednie użycie przycisku zasilania poza sytuacjami awaryjnymi

48. Zasady Tworzenia i Postępowania z Hasłami

- Dokument "Zasady Tworzenia i Postępowania z Hasłami" musi definiować wytyczne dotyczące tworzenia silnych haseł, ich długości (minimum 16 znaków) oraz stosowania wieloskładnikowego uwierzytelniania (MFA) tam, gdzie to możliwe.

- Dokument powinien zawierać zasady poufności haseł, zakaz ich zapisywania w przeglądarkach, wymóg regularnej zmiany haseł co 90 dni oraz zakaz używania tych samych haseł w różnych systemach informatycznych.

49. Polityka Zarządzania Bezpieczeństwem Sieci

- Polityka Zarządzania Bezpieczeństwem Sieci musi definiować zasady ochrony sieci organizacji, w tym zarządzanie urządzeniami sieciowymi, stosowanie zapór sieciowych, monitorowanie oraz uwierzytelnianie dostępu do sieci.

- Dokument powinien zawierać wytyczne dotyczące rozdzielania (segmentacji) sieci, bezpieczeństwa usług sieciowych oraz mechanizmów uwierzytelniania, szyfrowania i ograniczania dostępu do usług, zgodnie z umowami SLA i najlepszymi praktykami.

50. Polityka Przesyłania Informacji

- Polityka Przesyłania Informacji musi definiować zasady ochrony informacji przesyłanych wewnątrz organizacji oraz do podmiotów zewnętrznych, w tym wymóg stosowania ochrony kryptograficznej i zabezpieczeń przed złośliwym oprogramowaniem.

- Dokument powinien zawierać wytyczne dotyczące zawierania porozumień w zakresie przesyłania chronionych informacji, określających środki komunikacji, nadawców, odbiorców oraz mechanizmy ochrony danych.

51. Zasady korzystania z poczty Elektronicznej

- Zasady Korzystania z Poczty Elektronicznej muszą definiować zasady przesyłania informacji chronionych, w tym wymóg stosowania kryptografii i podpisów elektronicznych, gdy wymaga tego prawo lub procedury organizacji.

- Dokument powinien zawierać wytyczne dotyczące korzystania z poczty elektronicznej wyłącznie w celach służbowych, zakaz używania prywatnej poczty elektronicznej na urządzeniach organizacji oraz zasady bezpiecznego postępowania z załącznikami i odnośnikami od nieznanych nadawców.

52. Zasady Korzystania z Internetu

- Zasady Korzystania z Internetu muszą definiować korzystanie z Internetu wyłącznie w celach służbowych, z zakazem pobierania i instalowania nieautoryzowanych plików oraz aplikacji, a także zakazem korzystania z zasobów o treściach przestępczych, pornograficznych lub zakazanych.

- Dokument powinien zawierać wytyczne dotyczące stosowania szyfrowanych połączeń (HTTPS), zakaz używania funkcji autouzupełniania i zapamiętywania haseł w przeglądarkach oraz obowiązek zgłaszania nieprawidłowości do Administratora Systemów Informatycznych.

53. Umowa o Zachowaniu Poufności

- Umowa o Zachowaniu Poufności musi określać zasady ochrony informacji chronionych prawnie, zobowiązując Strony do przetwarzania tych informacji zgodnie z przepisami prawa, wymaganiami regulacyjnymi oraz umownymi, wyłącznie przez upoważniony personel.

- Dokument powinien zawierać wytyczne dotyczące odpowiedzialności za naruszenie poufności, w tym kary umowne i odszkodowania, a także okres obowiązywania zobowiązania do zachowania poufności po zakończeniu realizacji celu umowy.

54. Wymagania Związane z Bezpieczeństwem Systemów Informacji

- Wymagania Związane z Bezpieczeństwem Systemów Informacyjnych muszą obejmować zasady zabezpieczania systemów informacyjnych na każdym etapie ich cyklu życia, w tym identyfikację użytkowników, autoryzację, rejestrowanie działań oraz zarządzanie ryzykiem.

- Dokument powinien zawierać wytyczne dotyczące ochrony usług aplikacyjnych w sieciach publicznych, stosowania kryptografii oraz zabezpieczania transakcji, zapewniając poufność, integralność i dostępność przetwarzanych informacji.

55. Polityka bezpieczeństwa Informacji w Procesach Rozwoju i Wsparcia

- Polityka Bezpieczeństwa w Procesach Rozwoju i Wsparcia musi definiować zasady wprowadzania bezpieczeństwa informacji w całym cyklu życia systemów informacyjnych, w tym podczas prac rozwojowych, testowania i wdrożenia systemów.

- Dokument powinien zawierać wytyczne dotyczące bezpiecznego programowania, zarządzania zmianami w systemach, kontroli wersji oraz testów bezpieczeństwa, zarówno wewnętrznych, jak i zleconych podmiotom zewnętrznym.

56. Wymagania dotyczące Ochrony Danych Testowych

- Wymagania Dotyczące Ochrony Danych Testowych muszą określać zasady doboru, ochrony i nadzoru nad danymi używanymi w procesach testowych, minimalizując użycie rzeczywistych danych osobowych lub chronionych informacji.

- Dokument powinien zawierać wytyczne dotyczące stosowania procedur kontroli dostępu w środowiskach testowych oraz obowiązek usuwania rzeczywistych danych po zakończeniu testów.

57. Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami

- Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami musi określać wymagania związane z bezpieczeństwem informacji w relacjach z dostawcami, w tym zobowiązanie do ochrony poufności, integralności i dostępności aktywów organizacji.

- Dokument powinien zawierać wytyczne dotyczące monitorowania i kontroli dostępu dostawców do informacji, zarządzania ryzykiem związanym z łańcuchem dostaw technologii informacyjnych oraz zapewnienia odpowiedniego poziomu bezpieczeństwa w umowach z dostawcami.

58. Zarządzanie Bezpieczeństwem Informacji przez Dostawcę

- Dokument Zarządzanie Bezpieczeństwem Informacji przez Dostawcę musi zawierać szczegółową ankietę oceniającą dostawcę pod kątem zgodności z wymaganiami dotyczącymi bezpieczeństwa informacji, w tym stosowania polityk ochrony danych osobowych, zarządzania ryzykiem oraz incydentami cyberbezpieczeństwa.

- Dokument powinien obejmować pytania dotyczące wdrożenia systemu zarządzania bezpieczeństwem informacji, zarządzania dostępem, szyfrowania oraz przestrzegania zasad „Privacy by design" i „Privacy by default".

59. Procedura zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT

- Procedura Zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT musi definiować zasady inicjowania, realizacji i weryfikacji zakupów oprogramowania, urządzeń komputerowych oraz usług IT, w tym wymagania dotyczące bezpieczeństwa informacji zgodne z regulacjami prawnymi i wewnętrznymi.

- Dokument powinien zawierać wytyczne dotyczące sporządzania wniosku o zakup, który musi uwzględniać specyfikacje techniczne, planowane zabezpieczenia, potencjalnych dostawców oraz wymagania dotyczące bezpieczeństwa informacji i danych osobowych.

60. Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami

- Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami musi określać zasady postępowania w przypadku incydentów związanych z bezpieczeństwem informacji, w tym ich zgłaszania, oceny, podejmowania decyzji oraz działań zaradczych i korygujących.

- Dokument powinien zawierać wytyczne dotyczące zgłaszania naruszeń danych osobowych do odpowiednich organów w terminie nie dłuższym niż 72 godziny oraz procedury reagowania na incydenty cyberbezpieczeństwa zgodnie z wymogami prawnymi.

61. Zgłoszenie Incydentu, Zdarzenia, Niezgodności, Słabości

- Dokument "Zgłoszenie Incydentu, Zdarzenia, Niezgodności, Słabości" musi umożliwiać zgłaszanie incydentów bezpieczeństwa, zdarzeń, niezgodności z wymaganiami regulacyjnymi oraz słabości w zabezpieczeniach, obejmując opis istoty problemu, aktywów i procesów, których dotyczy.

- Formularz powinien zawierać szczegółowe wytyczne dotyczące dat i okoliczności incydentu, przyczyn jego wystąpienia, rodzaju naruszenia (np. ujawnienie informacji, utrata danych) oraz dane zgłaszającego, świadków i sprawców, umożliwiając anonimowe zgłoszenia.

62. Rejestr Incydentów, Zdarzeń, Niezgodności, Słabości, Działań Zaradczych, Korygujących i Doskonalących

- Rejestr Incydentów, Zdarzeń, Niezgodności, Słabości, Działań Zaradczych, Korygujących i Doskonalących musi zawierać szczegółowy zapis wszystkich incydentów, zdarzeń, niezgodności oraz słabości dotyczących bezpieczeństwa informacji, wraz z datą, opisem problemu oraz podjętymi działaniami.

- Dokument powinien umożliwiać śledzenie działań zaradczych, korygujących i doskonalących, mających na celu poprawę poziomu bezpieczeństwa informacji oraz eliminację zidentyfikowanych problemów.

63. Polityka Ciągłości Bezpieczeństwa Informacji

- Polityka Ciągłości Bezpieczeństwa Informacji musi definiować zasady zapewnienia ciągłości bezpieczeństwa informacji, uwzględniając planowanie, wdrożenie i utrzymanie procesów oraz środków gwarantujących bezpieczeństwo informacji w przypadku zakłóceń, takich jak incydenty czy katastrofy.

- Dokument powinien zawierać wytyczne dotyczące tworzenia planów zarządzania ciągłością działania oraz odtwarzania po katastrofie, weryfikacji zdolności organizacji do zapewnienia ciągłości oraz nadmiarowości zasobów przetwarzania informacji.

64. Ewidencja Aktywów Wspierających Zapewniających Utrzymanie Procesów Krytycznych po Katastrofie

- Ewidencja Aktywów Wspierających Zapewniających Utrzymanie Procesów Krytycznych po Katastrofie musi zawierać identyfikację i szczegółowy opis aktywów niezbędnych do utrzymania ciągłości procesów krytycznych, takich jak pomieszczenia, sprzęt, urządzenia komputerowe, oprogramowanie, nośniki informacji oraz personel.

- Dokument powinien określać minimalne zasoby, w tym powierzchnię, rodzaj sprzętu, liczbę pracowników oraz wymagania dotyczące sieci, niezbędne do realizacji procesów po wystąpieniu katastrofy.

65. Plan Zarządzania Ciągłością Działania

- Plan Zarządzania Ciągłością Działania musi określać zasady postępowania w przypadku zakłóceń procesów krytycznych, w tym procedury odzyskiwania i przywracania działania urządzeń, oprogramowania, sieci, personelu oraz lokalizacji przetwarzania informacji.

- Dokument powinien zawierać wytyczne dotyczące Recovery Time Objective (RTO), Recovery Point Objective (RPO), maksymalnego tolerowanego okresu zakłócenia (MTPD) oraz minimalnego poziomu działalności (MBCO), niezbędnych do zapewnienia ciągłości działania.

66. Plan Zarządzania Odtwarzaniem po Katastrofie

- Plan Zarządzania Odtwarzaniem po Katastrofie musi zawierać zasady przywracania krytycznych procesów organizacji po katastrofie, w tym identyfikację i zabezpieczenie niezbędnych aktywów, takich jak budynki, sprzęt komputerowy, oprogramowanie, nośniki danych oraz personel.

- Dokument powinien określać rodzaje katastrof, takich jak klęski żywiołowe, awarie techniczne, ataki terrorystyczne, oraz procedury reagowania, obejmujące zapewnienie zasobów zastępczych oraz nadzorowanie realizacji planów odtwarzania.

67. Polityka Zgodności

- Polityka Zgodności musi określać zasady monitorowania i przestrzegania wymagań prawnych, regulacyjnych oraz umownych związanych z bezpieczeństwem informacji, w tym ochronę praw własności intelektualnej oraz prywatności danych osobowych.

- Dokument powinien zawierać wytyczne dotyczące regularnych przeglądów zgodności, w tym niezależnych audytów oraz przeglądów technicznych systemów informacyjnych, w celu zapewnienia zgodności z politykami bezpieczeństwa i standardami.

68. Informacje o Przetwarzaniu Danych Osobowych Zbieranych bezpośrednio

- Dokument "Informacje o Przetwarzaniu Danych Osobowych Zbieranych Bezpośrednio" musi określać zasady informowania osób, których dane są przetwarzane, o celach, podstawach prawnych, odbiorcach oraz czasie przechowywania danych osobowych, zgodnie z przepisami RODO.

- Dokument powinien zawierać wytyczne dotyczące praw osób, których dane dotyczą, takich jak prawo do dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu wobec przetwarzania oraz cofnięcia zgody na przetwarzanie danych osobowych.

69. Informacje o Przetwarzaniu Danych Osobowych Zbieranych Pośrednio

- Dokument "Informacje o Przetwarzaniu Danych Osobowych Zbieranych Pośrednio" musi określać zasady informowania osób, których dane zostały pozyskane pośrednio, o celach, podstawach prawnych, odbiorcach oraz czasie przechowywania danych, zgodnie z przepisami RODO.

- Dokument powinien zawierać wytyczne dotyczące praw osób, których dane dotyczą, w tym prawa do dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu oraz cofnięcia zgody na przetwarzanie, a także informacje o zautomatyzowanym podejmowaniu decyzji i profilowaniu.

70. Polityka Ochrony Danych Osobowych

Polityka Ochrony Danych Osobowych musi definiować zasady przetwarzania danych osobowych zgodnie z wymaganiami prawnymi, regulacyjnymi i umownymi, a także zapewniać ochronę danych identyfikujących osoby fizyczne poprzez odpowiednie środki techniczne i organizacyjne.

Dokument powinien zawierać wytyczne dotyczące zarządzania danymi, w tym prawa osób, których dane dotyczą, przetwarzanie danych wyłącznie przez upoważniony personel oraz wdrażanie zasad „Privacy by design" i „Privacy by default".

71. Raport z Oceny Skutków Przetwarzania dla Ochrony Danych Osobowych

Raport z Oceny Skutków Przetwarzania dla Ochrony Danych Osobowych musi zawierać systematyczny opis przetwarzania danych, celów przetwarzania oraz ocenę proporcjonalności i konieczności w stosunku do tych celów, zgodnie z przepisami RODO.

Dokument powinien zawierać ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz określenie środków planowanych lub zastosowanych w celu zaradzenia tym ryzykom, wraz z ewentualnymi wnioskami dotyczącymi konieczności konsultacji z organem nadzorczym.

72. Rejestr Czynności Przetwarzania Danych Osobowych

Rejestr Czynności Przetwarzania Danych Osobowych musi zawierać szczegółowe informacje o wszystkich czynnościach przetwarzania danych osobowych, w tym cele przetwarzania, kategorie osób, których dane dotyczą, kategorie danych oraz kategorie odbiorców, którym dane są ujawniane.

Dokument powinien obejmować opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych w celu ochrony danych osobowych, a także informacje o przekazaniach danych do państw trzecich i planowanych terminach usunięcia danych

73. Rejestr Wszystkich Kategorii czynności Przetwarzania Dokonywanych w Imieniu Administratora

Rejestr Wszystkich Kategorii Czynności Przetwarzania Dokonywanych w Imieniu Administratora musi zawierać szczegółowy opis wszystkich kategorii czynności przetwarzania realizowanych przez podmiot przetwarzający na rzecz administratora, w tym dane kontaktowe stron oraz kategorie przetwarzanych danych.

Dokument powinien obejmować informacje o przekazaniach danych do państw trzecich, planowane terminy usunięcia danych oraz opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych w celu ochrony przetwarzanych danych osobowych.

74. Rejestr Zbiorów Danych Osobowych

Rejestr Zbiorów Danych Osobowych musi zawierać identyfikację wszystkich zbiorów danych osobowych przetwarzanych przez organizację, w tym ich nazwy, cele przetwarzania oraz czynności przetwarzania realizowane w ramach każdego procesu.

Dokument powinien zawierać informacje o administratorze danych, identyfikatory zbiorów oraz procesy związane z przetwarzaniem danych, zapewniając pełną ewidencję przetwarzanych danych osobowych w organizacji.

75. Test Równowagi

Test Równowagi musi zawierać ocenę prawnie uzasadnionych interesów realizowanych przez administratora w odniesieniu do interesów, podstawowych praw i wolności osób, których dane dotyczą, w celu ustalenia, czy przetwarzanie danych osobowych na tej podstawie jest zgodne z RODO.

Dokument powinien uwzględniać analizę korzyści i ryzyk związanych z przetwarzaniem, w tym ocenę możliwości naruszenia prywatności, anonimowości oraz innych praw osób, których dane dotyczą, aby zdecydować o zastosowaniu prawnie uzasadnionego interesu jako podstawy prawnej przetwarzania.

76. Umowa Przetwarzania Danych Osobowych w Imieniu Administratora

Umowa Przetwarzania Danych Osobowych w Imieniu Administratora musi określać zasady przetwarzania danych osobowych przez podmiot przetwarzający, zgodnie z wytycznymi administratora, w tym cel przetwarzania, rodzaje danych oraz kategorie osób, których dane dotyczą.

Dokument powinien zawierać wytyczne dotyczące obowiązków obu stron, w tym wymogi dotyczące bezpieczeństwa, obowiązek raportowania naruszeń oraz możliwość audytu zgodności z przepisami o ochronie danych osobowych.

77. Zawiadomienia Osoby, Której Dane Dotyczą o Naruszeniu Ochrony Danych Osobowych

Zawiadomienie Osoby, Której Dane Dotyczą, o Naruszeniu Ochrony Danych Osobowych musi informować osobę o charakterze naruszenia, możliwych konsekwencjach dla niej oraz środkach zastosowanych przez administratora w celu zaradzenia skutkom naruszenia, zgodnie z art. 34 RODO.

Dokument powinien zawierać szczegółowy opis incydentu, obejmujący datę, czas, okoliczności, kategorie dotkniętych danych oraz zalecenia dla osoby, której dane dotyczą, w celu zminimalizowania negatywnych skutków naruszenia.

78. Wycofanie Zgody na Przetwarzanie Danych Osobowych

Dokument "Wycofanie Zgody na Przetwarzanie Danych Osobowych" musi umożliwiać osobom wycofanie zgody na przetwarzanie ich danych osobowych, zgodnie z art. 7 RODO, poprzez złożenie odpowiedniego wniosku zawierającego dane osoby oraz zakres wycofanej zgody.

Dokument powinien zawierać sekcje umożliwiające określenie rodzaju danych, których przetwarzanie zostaje wycofane, oraz cele przetwarzania, z których osoba chce wycofać swoją zgodę

79. Zgoda na Przetwarzanie Danych Osobowych

Dokument "Zgoda na Przetwarzanie Danych Osobowych" musi umożliwiać osobie wyrażenie dobrowolnej i świadomej zgody na przetwarzanie jej danych osobowych, zgodnie z art. 6 RODO, z wyszczególnieniem rodzajów danych oraz celów ich przetwarzania.

Dokument powinien zawierać informację o prawie osoby do wycofania zgody w dowolnym momencie, bez wpływu na zgodność z prawem wcześniejszego przetwarzania, oraz o łatwości wycofania zgody na równi z jej wyrażeniem.

14. Projektowanie polityki ciągłości działania.

Cel Usługi:
Podstawowym celem niniejszej usługi jest skonstruowanie polityki ciągłości działania dla systemów informatycznych oraz infrastruktury telekomunikacyjnej Zamawiającego. Taka polityka aspiruje do gwarantowania bezusterkowego dostępu do esencjonalnych usług oraz danych w przypadku wystąpienia wszelakich awarii, kataklizmów bądź innych nieoczekiwanych wydarzeń, co ma za zadanie zredukować potencjalne ryzyko przestojów i asocjowanych z nimi strat.

Zakres Usługi:

1. Analiza Stanu Istniejącego i Identyfikacja Wymagań:
   - Egzekucja wnikliwej analizy aktualnego stanu infrastruktury ICT oraz przegląd dotychczasowych strategii z zakresu ciągłości działania, mających na celu zdiagnozowanie potencjalnych luk i niedoskonałości.
   - Rozpoznanie i wyróżnienie kluczowych procesów biznesowych oraz zasobów informatycznych, które są nieodzowne dla bieżącej operacyjności Zamawiającego.
   - Realizacja oceny ryzyka i analizy wpływu na działalność (BIA - Business Impact Analysis) z perspektywy ciągłości funkcjonowania organizacji.
2. Projektowanie Polityki Ciągłości Działania:
   - Stworzenie strategii mającej na celu zapewnienie nieprzerwanej ciągłości usług ICT, określając cele odnoszące się do czasu przywrócenia działania oraz punktu odzyskiwania danych.
   - Zdefiniowanie procedur interwencyjnych, planów awaryjnych oraz procedur odzyskiwania funkcjonalności po wystąpieniu katastroficznych zdarzeń.
3. Integracja z Istniejącymi Systemami Zarządzania:
   - Zapewnienie kompleksowej integracji nowo opracowanej polityki z obecnymi systemami zarządzania bezpieczeństwem informacji, zarządzaniem ryzykiem oraz innymi procedurami operacyjnymi, w celu stworzenia spójnego i efektywnego ekosystemu ciągłości działania.
4. Testowanie i Walidacja Polityki:
   - Opracowanie i egzekucja testów scenariuszy awaryjnych mających na celu zweryfikowanie efektywności i praktycznej użyteczności formułowanej polityki ciągłości działania.
   - Analiza rezultatów testów i modyfikacja polityki w oparciu o zgromadzone dane i obserwacje, celem optymalizacji jej skuteczności.
5. Dokumentacja i Rekomendacje:
   - Stworzenie pełnej dokumentacji dotyczącej polityki ciągłości działania, zawierającej detaliczne instrukcje, procedury i wytyczne, które będą stanowić kompendium wiedzy dla Zamawiającego.
   - Przedstawienie rekomendacji dotyczących przyszłych działań, potencjalnych udoskonaleń oraz strategii utrzymania gotowości operacyjnej na najwyższym poziomie.

15. Wsparcie lokalne przy wdrożeniu.

W ramach wsparcia lokalnego przewiduje się realizację prac wdrożeniowych związanych z podłączeniem sprzętu informatycznego na warstwie fizycznej oraz instalacją oprogramowania. Prace te będą prowadzone w trybie hybrydowym – częściowo w siedzibie Zamawiającego, a częściowo zdalnie, przy wykorzystaniu połączenia z systemami Zamawiającego.

Wsparcie lokalne dotyczy wyłącznie czynności realizowanych na warstwie fizycznej, w szczególności podłączenia, montażu i uruchomienia sprzętu, i powinno być zapewnione przez minimum 3 dni robocze lub

do momentu zakończenia podłączania całego sprzętu dostarczonego w ramach zamówienia – w zależności od tego, które z tych zdarzeń nastąpi wcześniej.

16. Testy penetracyjne.

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

- wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
- skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
- weryfikacje domyślnych haseł według zadanego słownika;
- skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
- ustawienia harmonogramu skanowań;
- możliwość porównania wyników poszczególnych skanowań;
- możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
- możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
- precyzyjna konfiguracja reguł przechwytywania wiadomości;
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
- żądania i odpowiedzi dostępne w edytorze http;
- narzędzie do ręcznej edycji i ponownego wstawiania żądań;
- narzędzie do analizy statystycznej tokenów sesji;
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;

możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
możliwość analizy docelowej aplikacji internetowych.
narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity).
Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych. Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.
W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

Rekonesans.
Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.
Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
Sprawdzenie występowania w wyciekach znalezionych loginów.

Enumeracja zasobów.
Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
Skanowanie publicznej infrastruktury.
Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.

Eksploitacja.
Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).

Eskalacja uprawnień.
Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).

Raport z testu penetracyjnego.

Wykonawca dostarczy raport zawierający:
Podsumowanie dla kierownictwa.
Opis zakresu wykonanych prac.
Wyłączenia z testów jeżeli były.

Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
Listę znalezionych podatności wraz z określoną dla niej waga zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
Szczegółowy opis znalezionych podatności.
Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

17. Testy socjotechniczne.

Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami:

Przygotowanie kampanii socjotechnicznej;
- wybór i zakup przez Wykonawcę domeny (łudząco podobnej do domeny Zamawiającego), która zostanie wykorzystana do kampanii socjotechnicznej;
- opracowanie bazy mailingowej pracowników objętych kampanią socjotechniczną oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;
- wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
- wsparcie w zakresie dodania domeny wybranej do przeprowadzenia kampanii socjotechnicznej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców).

Przygotowanie spreparowanych zasobów służących wyłudzaniu informacji:
- serwer strony www z bazą danych powiązany z domeną, która została zakupiona w celu przeprowadzenia kampanii socjotechnicznej;
- wykonanie kopii strony internetowej Zamawiającego i umieszczenie jej pod spreparowanym adresem;
- wygenerowanie niezbędnych certyfikatów SSL;
- przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);
- utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;
- przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;
- przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary").

Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
Wykonanie raportu z testu socjotechnicznego w języku polskim.
Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:
- wprowadzenie do cyberbezpieczeństwa:
  - czym jest cyberbezpieczeństwo;
  - dlaczego cyberbezpieczeństwo jest ważne;
  - kluczowe zagadnienia związane z cyberbezpieczeństwem;

przegląd statystyk i trendów w cyberbezpieczeństwie.

typy zagrożeń w cyberprzestrzeni:
- malware (wirusy, trojany, robaki itp.);
- ataki typu phishing i spear phishing;
- ataki DDoS;
- ataki ransomware;
- zagrożenia związane z sieciami społecznościowymi.

zasady bezpieczeństwa i praktyki:
- zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
- zasady bezpieczeństwa e-mail;
- bezpieczeństwo w sieciach bezprzewodowych;
- bezpieczne przeglądanie internetu;
- backup i odzyskiwanie danych.

reagowanie na incydenty i planowanie awaryjne:
- jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
- zasady reagowania na incydenty;
- planowanie awaryjne i kontynuacja działalności;
- Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Czas trwania szkolenia przewidziano na co najmniej dwie grupy po 4 godziny robocze każda z uwzględnieniem przerw 15 minut w każdym szkoleniu. Po szkoleniu Wykonawca udostępni co najmniej 30 minut na pytania i odpowiedzi uczestników.

18. Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych.

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

- Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
- Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
- Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
- Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając w to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
- Wykonawca zainstaluje oprogramowanie przeciwdziałające wyciekowi danych.
- Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów

z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

- Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.
- Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
- Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.
- Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:
- Numery kart kredytowych
- Numery IBAN
- Numery dowodów osobistych
- Polski numer paszportu
- Numer PESEL
- Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.
- Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.
- Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.
- Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.
- Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.
- Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
- Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

19. Wdrożenie klastra serwerów.

Krok 1: Planowanie i Przygotowanie:

Określenie wymagań dotyczących infrastruktury, w tym sprzętu, sieci i przechowywania.
Wybranie serwerów, które zostaną użyte jako węzły klastra. Upewnij się, że są one zgodne z wymaganiami wybranego oprogramowania.
Skonfigurowanie łącza sieciowego i przestrzeni dyskowej, aby zapewnić odpowiednią przepustowość i pojemność.
Zainstalowanie systemu operacyjnego na każdym węźle klastra.

Krok 2: Instalacja roli oprogramowania do wirtualizacji:

Instalacja odpowiedniej roli za pomocą menedżera serwerów lub PowerShell.
Konfiguracja ustawień sieciowych i przechowywania na węzłach klastra, tak aby były zgodne z wymaganiami projektu.

Krok 3: Konfiguracja klastra:

Uruchomienie kreatora konfiguracji klastra w menedżerze serwerów na jednym z węzłów.
Dodanie pozostałych węzłów klastra do konfiguracji.
Konfiguracja ustawień klastra, takie jak nazwa klastra, adresy IP i konfiguracja przechowywania współdzielonego.

Krok 4: Konfiguracja wysokiej dostępności klastra:

Włączenie funkcji wysokiej dostępności dla maszyn wirtualnych na klastrze.
Konfiguracja ustawień zapasowych dla klastra, aby zapewnić ochronę przed awariami węzłów.

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi:

Utworzenie nowych maszyn wirtualnych na klastrze z wykorzystaniem oprogramowania do wirtualizacji.
Konfiguracja ustawień maszyn wirtualnych, takich jak liczba procesorów, ilość pamięci i przypisywanie zasobów sieciowych.
Zarządzanie maszynami wirtualnymi, monitorowanie ich wydajności i wykonywanie niezbędnych operacji konserwacyjnych jest kluczowe w zapewnieniu prawidłowo funkcjonującego środowiska wirtualnego uruchomionego w klastrze.

Krok 6: Testowanie i Monitorowanie:

Testowanie działania klastra, w tym jego zdolność do migracji wirtualnej i przywracania po awariach.
Konfiguracja narzędzi monitorujących, w celu śledzenia wydajności i dostępności klastra oraz maszyn wirtualnych.
Regularnie przeglądanie logów i raportów, w celu szybkiego reagowania na ewentualne problemy.

20. Wdrożenie menadżera haseł.

Menedżer haseł hostowany lokalnie ma zapewnić bezpieczne, elastyczne i skalowalne rozwiązanie służące do zarządzania hasłami i innymi danymi uwierzytelniającymi. Dzięki architekturze szyfrowania end-to-end, kontrolowanemu dostępowi i wsparciu dla pracy zespołowej, zapewnić ma wysoki poziom bezpieczeństwa i wygodę użytkowania, pozostając jednocześnie pod pełną kontrolą organizacji. Jest to szczególnie wartościowe rozwiązanie dla firm i zespołów, którym zależy na bezpieczeństwie, prywatności i zgodności z regulacjami.

Menedżera haseł hostowany lokalnie ma spełniać poniższe kluczowe cechy:
Samodzielna kontrola danych: Dane są przechowywane w infrastrukturze własnej organizacji, co minimalizuje ryzyko wycieku do zewnętrznych dostawców i pozwala dostosować zabezpieczenia do wewnętrznych polityk.
Szyfrowanie end-to-end: Wszystkie hasła i tajne dane są szyfrowane po stronie klienta przy użyciu kluczy GPG, które nigdy nie opuszczają urządzenia użytkownika. Nawet administrator serwera czy osoba mająca dostęp do bazy danych nie może odczytać zaszyfrowanych informacji.
Wielopłaszczyznowa kontrola dostępu: System zarządzania uprawnieniami pozwala przypisywać prawa do zasobów na poziomie indywidualnym lub grupowym, umożliwiając granularne udostępnianie haseł i innych sekretów.
Wsparcie dla zespołów: Możliwość współdzielenia haseł pomiędzy użytkownikami i grupami znacząco usprawnia pracę zespołową i zmniejsza liczbę ręcznych wymian danych.
Interfejs webowy i rozszerzenia przeglądarki: Dostęp przez przeglądarkę internetową oraz dedykowane rozszerzenia umożliwiają łatwe logowanie, autouzupełnianie i zarządzanie hasłami w codziennej pracy.

Audyt i logowanie aktywności: Każde działanie w systemie jest rejestrowane, co pozwala na monitoring i zachowanie zgodności z politykami bezpieczeństwa.
Wymagania techniczne: Do działania wymagany jest serwer WWW, baza danych, serwer SMTP do komunikacji e-mail oraz certyfikat SSL, gwarantujący bezpieczne połączenie HTTPS.
Minimalizacja ryzyka wycieku dzięki zastosowaniu silnego szyfrowania, ograniczeniu dostępu i kontroli fizycznej nad serwerem.
Możliwość zarządzanie wieloma typami sekretów, w tym tokenami API oraz innymi danymi uwierzytelniającymi.

Klient zobowiązuje się do:
dostarczenia wszystkich właściwy danych do serwera SMTP celem wysyłania linków aktywacyjnych i powiadomień.
W przypadku podjęcia decyzji o używaniu pełnej kwalifikowalnej nazwy dla menadżera haseł w ramach istniejącej internetowej domeny dostarczenia właściwego certyfikatu SSL/TLS
Dostarczenia odpowiednich zasobów umożliwiających wdrożenie menedżera haseł hostowanego lokalnie
Stosowania separacji sieciowej – np. umieszczenie serwera menedżera haseł w wewnętrznej sieci VPN lub DMZ z ograniczonym dostępem.

Przedmiotom wdrożenia menedżera haseł hostowanego lokalnie będzie:
Przegotowanie odpowiedniego, dedykowanego serwer opartego o system operacyjny GNU/Linux.
Konfiguracja serwera WWW (Nginx lub Apache HTTP) obsługującego HTTPS z certyfikatem SSL/TLS (np. Let's Encrypt).
Konfigurację bazy danych MySQL lub MariaDB.
Instalację i konfigurację wymaganego oprogramowania.
Instalację oraz konfigurację wymaganych usługi, w tym użycie istniejącego serwera SMTP w ramach zasobów klienta do wysyłania e-maili aktywacyjnych i powiadomień.
Konfiguracja powiadomień m.in. przy tworzeniu kont, resetowaniu haseł czy zmianach w zasobach.
Weryfikacja działania aplikacji przez przeglądarkę
Testowanie środowiska przed udostępnieniem go całemu zespołowi, by upewnić się, że wszystkie mechanizmy działają poprawnie
Szkolenie użytkowników z zasad bezpieczeństwa i obsługi menedżera haseł

Opcjonalnym zadaniem może być utrzymanie i aktualizacja menedżera haseł poprzez:
Aktualizacje oprogramowania i systemu operacyjnego, aby zapewnić poprawki bezpieczeństwa i nowe funkcje.
Backup danych i kluczy szyfrujących, co jest kluczowe, gdyż bez tych danych odtworzenie haseł jest niemożliwe.
Monitorowanie logów i stanu serwera, aby zapobiegać awariom i zagrożeniom bezpieczeństwa.
W razie potrzeby rozbudowa infrastruktury, np. o redundancję lub balansowanie obciążenia.
Regularne przeglądy uprawnień, by zapobiegać nadmiernemu dostępowi do haseł.

21. Wdrożenie kontrolera domeny.

Etap 1: Analiza Wstępna i Planowanie Wdrożenia
1.1. Analiza Stanu Obecnego:

- Ocena istniejącej infrastruktury IT, w tym systemów operacyjnych, sieci, aplikacji i baz danych.

- Identyfikacja istniejących rozwiązań zarządzania tożsamościami i bezpieczeństwem oraz ich ewentualnych ograniczeń.

1.2. Wymagania Organizacyjne i Techniczne:

- Konsultacje z interesariuszami w celu zrozumienia potrzeb biznesowych i oczekiwań dotyczących infrastruktury IT.
- Identyfikacja wymagań dotyczących zarządzania tożsamościami użytkowników, zasobami sieciowymi i politykami bezpieczeństwa.

1.3. Opracowanie Planu Wdrożenia:

- Sporządzenie szczegółowego planu projektowego uwzględniającego harmonogram, zadania, zasoby i odpowiedzialności.
- Określenie struktury domen, schematu nazewnictwa i strategii replikacji dla środowiska Active Directory.

Etap 2: Instalacja i Konfiguracja Środowiska Active Directory

2.1. Instalacja Roli AD DS:

- Konfiguracja serwera Windows Server jako kontrolera domeny, włączając rolę Active Directory Domain Services.

2.2. Konfiguracja DNS:

- Ustawienie serwera DNS zgodnie z wymaganiami Active Directory.
- Konfiguracja strefy forward i reverse DNS dla domeny.

2.3. Tworzenie Dominy lub Integracja:

- Utworzenie nowej domeny Active Directory lub integracja z istniejącymi domenami w środowisku.

2.4. Konfiguracja Zasad Replikacji:

- Określenie i skonfigurowanie zasad replikacji między kontrolerami domeny w różnych lokalizacjach.

Etap 3: Strukturyzacja i Organizacja Domeny

3.1. Projektowanie Struktury Organizacyjnej:

- Tworzenie jednostek organizacyjnych (OU) odpowiadających strukturze organizacyjnej firmy.
- Utworzenie kont użytkowników, grup i zasobów oraz ich odpowiednie uporządkowanie w hierarchii.

3.2. Konfiguracja Polityk Grupowych (GPO):

- Ustanowienie zasad dostępu, konfiguracji użytkowników i komputerów za pomocą GPO.
- Implementacja polityk bezpieczeństwa dotyczących haseł, dostępu i innych ustawień

Etap 4: Zabezpieczenie Active Directory

4.1. Wdrożenie Zaawansowanych Mechanizmów Zabezpieczeń:

- Konfiguracja zasad kont haseł, polityk blokowania kont, kontroli dostępu.
- Implementacja szyfrowania komunikacji i audytu zdarzeń w AD.

4.2. Konfiguracja Środków Obronnych:

- Wdrożenie mechanizmów zabezpieczeń przed atakami, w tym monitorowanie logów, wykrywanie zagrożeń i zapobieganie atakom.

Etap 5: Walidacja i Optymalizacja Konfiguracji

5.1. Testowanie Funkcjonalności i Bezpieczeństwa:

- Przeprowadzenie testów weryfikujących działanie i bezpieczeństwo środowiska AD.
- Identyfikacja i rozwiązywanie ewentualnych problemów lub luk w zabezpieczeniach.

5.2. Optymalizacja Wydajności:

- Optymalizacja konfiguracji AD w celu zapewnienia efektywności i wydajności działania.
- Integracja z istniejącymi systemami i aplikacjami w celu zapewnienia spójności działań.

Etap 6: Dokumentacja Techniczna

6.1. Sporządzenie Dokumentacji:

- Przygotowanie szczegółowej dokumentacji technicznej, zawierającej opisy konfiguracji, ustawień polityk, procedur bezpieczeństwa i architektury systemu.
- Dokumentacja będzie służyć jako punkt odniesienia dla administratorów IT i personelu technicznego.

Cel Końcowy Usługi

Finalizacja usługi zapewni pełne wdrożenie systemu Active Directory, skonfigurowane zgodnie z najlepszymi praktykami branżowymi, gotowe do efektywnego zarządzania środowiskiem IT. System będzie przygotowany do zapewnienia wysokiego poziomu bezpieczeństwa, stabilności operacyjnej i skalowalności, odpowiadając na bieżące oraz przyszłe potrzeby organizacji.

22. Wdrożenie U2F.

1. Cel zamówienia

Celem zamówienia jest podniesienie poziomu bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego poprzez wdrożenie silnego uwierzytelniania (MFA) w oparciu o klucze sprzętowe U2F. Realizacja obejmuje zaprojektowanie i wdrożenie hierarchicznej infrastruktury klucza publicznego (PKI), integrację z usługą katalogową Active Directory oraz konfigurację stacji końcowych.

2. Zakres prac (Etapy realizacji)

Etap 1: Analiza przedwdrożeniowa i Projekt

Wykonawca zobowiązany jest do przeprowadzenia audytu środowiska i przygotowania projektu technicznego.

- Analiza infrastruktury: Ocena obecnego stanu Active Directory, poziomu funkcjonalności domeny i lasu oraz usług DNS pod kątem wdrożenia PKI.
- Wymagania organizacyjne: Uzgodnienie z Zamawiającym polityk bezpieczeństwa dotyczących cyklu życia certyfikatów oraz procedur wydawania i unieważniania kluczy U2F.
- Projekt architektury PKI: Opracowanie schematu dwustopniowego urzędu certyfikacji (Offline Root CA oraz Enterprise Sub CA) zgodnie z najlepszymi praktykami bezpieczeństwa Microsoft.

Etap 2: Budowa i konfiguracja infrastruktury PKI

Zgodnie z wymaganiami technicznymi, Wykonawca przeprowadzi instalację ról serwerowych niezbędnych do obsługi logowania kartą inteligentną/kluczem U2F.

2.1. Główne Centrum Certyfikacji (Root CA):

- Instalacja systemu operacyjnego i przygotowanie dedykowanej maszyny (lub maszyny wirtualnej) dla roli Root CA.
- Instalacja i konfiguracja roli Active Directory Certificate Services (AD CS) w trybie Standalone Root CA.
- Wygenerowanie głównego certyfikatu Root CA o odpowiedniej długości klucza i algorytmie (min. RSA 4096-bit lub ECDSA).
- Konfiguracja punktów dystrybucji list CRL (CDP) oraz dostępu do informacji o urzędach (AIA).

2.2. Dystrybucja zaufania w domenie:

- Opublikowanie certyfikatu Root CA w kontenerze konfiguracji Active Directory.
- Konfiguracja GPO w celu automatycznej dystrybucji certyfikatu Root CA do magazynu „Zaufane główne urzędy certyfikacji” na wszystkich stacjach roboczych i serwerach w domenie.

2.3. Podrzędne Centrum Certyfikacji (Sub CA - Issuing CA):

- Instalacja i konfiguracja serwera w roli Enterprise Subordinate CA.
- Wygenerowanie żądania certyfikatu i podpisanie go przez Root CA.
- Konfiguracja usług sieciowych (Web Enrollment, OCSP - jeśli wymagane) dla obsługi żądań użytkowników.

Etap 3: Konfiguracja Active Directory i szablonów certyfikatów

Wykonawca dokona integracji infrastruktury PKI z mechanizmami uwierzytelniania domeny.

- Szablony certyfikatów: Utworzenie i konfiguracja dedykowanych szablonów certyfikatów (Certificate Templates) dla logowania kartą inteligentną/kluczem FIDO2, uwzględniając wymagania kluczy U2F.
- Uprawnienia: Nadanie odpowiednich uprawnień (Read, Enroll) dla grup użytkowników i komputerów upoważnionych do korzystania z kluczy.
- Konfiguracja Kontrolerów Domeny: Wystawienie i dystrybucja certyfikatów "Domain Controller Authentication" (lub Kerberos Authentication) dla wszystkich kontrolerów domeny, aby umożliwić obsługę logowania certyfikatem.
- Mapowanie certyfikatów: Konfiguracja usługi *name mapping* (jeśli wymagana) w celu poprawnego przypisywania certyfikatów z kluczy U2F do kont użytkowników w AD.

Etap 4: Wdrożenie polityk (GPO) i konfiguracja klientów

- Opracowanie i wdrożenie obiektów GPO wymuszających lub umożliwiających logowanie za pomocą klucza sprzętowego na stacjach roboczych.
- Wsparcie w konfiguracji stacji roboczych do obsługi minidriverów lub sterowników niezbędnych dla kluczy U2F (jeśli dotyczy).
- Wsparcie w konfiguracji wygaszacza ekranu i blokady stacji po wyjęciu klucza (opcjonalnie, zgodnie z ustaleniami z Etapu 1).

Etap 5: Testy i Walidacja

Wykonawca przeprowadzi szczegółowe testy wdrożonego rozwiązania w środowisku testowym, a następnie produkcyjnym.

- Testy propagacji: Weryfikacja, czy certyfikaty Root CA i Sub CA są poprawnie widoczne na stacjach końcowych.
- Testy logowania: Przeprowadzenie prób logowania do systemu Windows za pomocą klucza U2F na różnych typach stacji roboczych.
- Testy dostępu do zasobów: Weryfikacja dostępu do zasobów sieciowych (pliki, aplikacje intranetowe) po zalogowaniu kluczem, w celu potwierdzenia poprawnego działania Kerberos.
- Scenariusze awaryjne: Test zachowania systemu w przypadku niedostępności serwera Sub CA lub CRL (sprawdzenie *cache'owania* poświadczeń).

Etap 6: Dokumentacja i Szkolenia

- Dokumentacja powykonawcza: Dostarczenie dokumentacji technicznej zawierającej opis konfiguracji PKI, parametry szablonów certyfikatów, konfigurację GPO oraz procedury awaryjne (Backup/Restore CA).
- Instrukcja dla użytkownika: Opracowanie skróconej instrukcji dla użytkownika końcowego dotyczącej rejestracji i użycia klucza.
- Szkolenie administratorów: Przeprowadzenie warsztatu (min. 4 godziny) dla zespołu IT Zamawiającego obejmującego zarządzanie cyklem życia certyfikatów, obsługę konsoli PKI i rozwiązywanie problemów z logowaniem.

3. Wymagania dotyczące Wykonawcy

- Wykonawca zapewni wsparcie techniczne (gwarancję) na wdrożoną konfigurację przez okres 12 miesięcy od daty podpisu protokołu odbioru.

4. Terminy i Odbiór

- Odbiór prac nastąpi na podstawie protokołu zdawczo-odbiorczego po pomyślnym przeprowadzeniu testów akceptacyjnych opisanych w Etapie 5.

23. Wdrożenie XDR.

Krok 1: Instalacja

- Pobranie i instalacja najnowszej wersji oprogramowania XDR, zgodnie z licencją i specyfikacją techniczną produktu.

- Instalacja agentów systemu XDR na wszystkich kluczowych urządzeniach w sieci, które mają być monitorowane. Urządzenia te obejmują serwery, stacje robocze i urządzenia mobilne.

Krok 2: Konfiguracja

- Skonfigurowanie agentów do komunikacji z centralnym serwerem XDR oraz zintegrowanie systemu XDR z istniejącymi narzędziami bezpieczeństwa, w tym z systemami Security Information and Event Management (SIEM) oraz innymi platformami zarządzania zabezpieczeniami.

Krok 3: Testowanie i optymalizacja

- Przeprowadzenie serii testów operacyjnych, aby upewnić się, że wszystkie komponenty systemu XDR pracują poprawnie i są w stanie efektywnie zbierać, analizować oraz reagować na zgromadzone dane.
- Modyfikacja i dostosowanie wewnętrznych zasad wykrywania zagrożeń systemu XDR, aby maksymalnie wykorzystać jego potencjał w kontekście specyfiki infrastruktury i oczekiwanych zagrożeń

Krok 4: Dokumentacja techniczna

- Zapewnienie pełnej dokumentacji technicznej i operacyjnej, która pomoże w zrozumieniu zasad działania systemu XDR oraz w przyszłym rozwiązywaniu problemów i zarządzaniu systemem.

Krok 5: Monitorowanie i utrzymanie

- Ustawienie i konfiguracja dashboardów monitorujących, które będą na bieżąco raportować stan systemu, aktywności i wszelkie wykryte anomalie.
- Regularne przeprowadzanie aktualizacji systemowych, patchy bezpieczeństwa oraz konserwacji sprzętu, aby system XDR pozostał aktualny i odporny na nowe zagrożenia.
- Systematyczna analiza zarejestrowanych incydentów, wdrażanie działań naprawczych oraz ciągłe doskonalenie procesów i zasad bezpieczeństwa w odpowiedzi na ewoluujące zagrożenia i wynikające z nich wnioski.

Krok 6: Ocena i dostosowanie

- Okresowa ocena skuteczności wdrożonego oprogramowania XDR, analizując liczbę i rodzaj wykrytych zagrożeń oraz czas reakcji na incydenty.
- Udoskonalanie procesów związane z zarządzaniem bezpieczeństwem informacji na podstawie wniosków i doświadczeń zdobytych z korzystania z XDR.

Podsumowanie

Wdrożenie systemu XDR to krytyczny element strategii bezpieczeństwa cyfrowego Zamawiającego, mający na celu zwiększenie odporności organizacji na cyberataki oraz usprawnienie procesów wykrywania, analizy i reakcji na incydenty bezpieczeństwa. W ramach tego zamówienia oczekuje się nie tylko technicznej implementacji, ale również wsparcia strategicznego i operacyjnego, które pomoże w maksymalnym wykorzystaniu potencjału wdrożonego rozwiązania.