Opis przedmiotu zamówienia

Część I: Świadczenie usług utrzymania środowiska SIEM/SOC wraz z dostawą i wdrożeniem serwera

Przedmiotem zamówienia jest:

1. **Świadczenie usług utrzymania systemu Zarządzania Informacjami i Zdarzeniami Bezpieczeństwa (SIEM) oraz Centrum Operacji Bezpieczeństwa (SOC)** – obejmujące obsługę incydentów bezpieczeństwa, raportowanie, regularne aktualizacje, konserwację, wsparcie techniczne oraz monitorowanie działania przez okres 20 miesięcy (**przeważający element zamówienia**)
2. **Dostawa i wdrożenie serwera wraz z oprogramowaniem dla środowiska SIEM/SOC** – obejmujące dostawę, instalację oraz konfigurację sprzętu komputerowego, zgodnie z określoną specyfikacją techniczną

I.1. Zakres zamówienia

- **Dostawa serwera**
  - Specyfikacja techniczna

Element Specyfikacji	**Opis**
Typ Serwera	Serwer rackowy, 1U, 8 kieszeni na dyski 2,5" SFF
Procesory	
Ilość:	2
Typ:	12-rdzeniowy procesor o taktowaniu min. 2.30 GHz, pamięć podręczna L3 min. 16.5 MB
Maksymalne TDP:	120 W
Obsługa pamięci:	DDR4-2400
Liczba kanałów pamięci:	min. 6
Pamięć RAM	
Ilość modułów:	4

Pojemność jednego modułu:	16 GB
Typ:	DIMM PC4 DDR4 Registered ECC
Kontroler RAID	
Przepustowość:	min. 12 Gb/s SAS, min. 6 Gb/s SATA
Pamięć cache:	min. 2 GB NV
Obsługiwane poziomy RAID:	0, 1, 5, 6, 10, 50, 60
Dyski serwerowe SAS/SATA/SSD	
Ilość:	4
Typ:	SSD SATA
Pojemność:	480 GB
Format:	2,5" SFF
Montaż:	w ramce 2,5"
Riser Card	
Ilość:	1
Typ:	2 sloty niskoprofilowe PCIe
Zdalne zarządzanie	
Funkcjonalność:	Pełne zdalne zarządzanie, monitorowanie i diagnostyka sprzętu
Dedykowana karta LAN	
Ilość:	1
Typ:	Karta sieciowa z 2 portami 1 Gb Ethernet RJ45
Zasilanie	
Ilość zasilaczy:	2
Moc:	min. 550 W każdy
Funkcjonalność:	Redundancja zasilania, możliwość wymiany hot-swap
Szyny rack	

Ilość:	1 komplet
Typ:	Szyny montażowe do szafy rack 19"
Front Panel / Maskownica	
Ilość:	1
Typ:	Panel przedni
Gwarancja	
Okres:	12 miesięcy
Dodatkowe Wymagania	
Komponenty:	Wszystkie komponenty muszą być oryginalne i kompatybilne z serwerem
Stan:	Serwer musi być nowy, nieużywany
Kompatybilność:	Serwer musi być kompatybilny z szafami rack 19"
Zdalne zarządzanie:	Zdalne zarządzanie musi zapewniać pełną funkcjonalność w zakresie monitorowania, zarządzania i diagnostyki sprzętu
System zasilania:	System zasilania musi zapewniać redundancję i możliwość hot-swap wymiany zasilaczy
Dyski SSD:	Dyski SSD muszą posiadać wsparcie dla funkcji TRIM
Instalacja:	Instalacja serwera w racku oraz konfiguracja podstawowa powinna być wykonana przez Wykonawcę w miejscu wskazanym przez Zamawiającego

- Zainstalowane oprogramowanie do zarządzania wirtualizacją (tzw. **Hypervisor typu 1**), posiadającej funkcjonalność Snapshotów maszyn wirtualnych, wbudowane mechanizmy do tworzenia kopii zapasowych i odzyskiwania danych oraz wsparcie dla „**migracji na żywo**”. Oprogramowanie do zarządzania wirtualizacją **nie ma posiadać opłat licencyjnych**.

- **Wdrożenie serwera wraz z oprogramowaniem dla środowiska SIEM/SOC o następujących cechach**:
    - Scentralizowany system o pojedynczym interfejsie zarządzającym i umieszczonych w sieci agentach
    - Wykrywający nieautoryzowane próby dostępu, zmiany konfiguracji systemu, a także podejmujący automatyczne działania w odpowiedzi na te incydenty
    - Monitorujący zmiany w plikach i katalogach, co pozwala na szybkie wykrycie potencjalnych naruszeń bezpieczeństwa
    - Zbierający i analizujący logi z różnych źródeł, takich jak systemy operacyjne, aplikacje, urządzenia sieciowe i inne, w celu identyfikacji potencjalnych zagrożeń
    - Wspierający zapewnienie zgodności z różnymi standardami i przepisami, takimi jak RODO/GDPR, poprzez monitorowanie i raportowanie stanu zabezpieczeń
    - Chroniący urządzenia końcowe przed różnymi zagrożeniami, takimi jak malware, ransomware
    - Oferujący zaawansowane narzędzia raportowania i analizy, które pomagają w monitorowaniu stanu bezpieczeństwa i identyfikacji trendów w zakresie zagrożeń
    - Zainstalowane jako maszyna wirtualna na platformie do zarządzania wirtualizacją (tzw. Hypervisor typu 1)
    - Instalacja agentów na urządzeniach końcowych (do 70 hostów / serwerów).
    - Oprogramowanie w języku polskim
    - Brak opłat licencyjnych

- **Świadczenie usług utrzymania systemu Zarządzania Informacjami i Zdarzeniami Bezpieczeństwa (SIEM) oraz Centrum Operacji Bezpieczeństwa (SOC)**
    - Skonfigurowanie w ramach platformy witalizacyjnej funkcjonalności kopii zapasowych i odzyskiwania plików i danych oprogramowania dla środowiska SIEM/SOC
    - Opracowanie i wdrożenie planu zarządzania podatnościami. Wykonawca opracuje i przedstawi plan działania na wypadek krytycznych incydentów bezpieczeństwa, który będzie obejmował:
        - Procedury natychmiastowej reakcji na incydenty,
        - Procedury powiadamiania odpowiednich służb i zespołów reagowania,
        - Plany przywracania działania systemów po incydentach,
        - Procedury analizy incydentów po ich wystąpieniu oraz wdrażania działań zapobiegawczych.
    - Monitorowanie, analiza oraz odpowiedź na incydenty bezpieczeństwa w postaci przekazania pełnej informacji do zespołu IT Zleceniodawcy

- Sporządzanie **okresowych raportów**:
  - **Comiesięczne** raporty szczegółowe z działania systemu SOC/SIEM (20 raportów w ciągu 20 miesięcy)
  - **Kwartalne** raporty podsumowujące (1-2 strony) z zaleceniami
- **Wdrożenie zaleceń z raportów kwartalnych**, wykonane przez 2-osobowy zespół Wykonawcy w ścisłej współpracy z zespołem IT Zamawiającego

I.2. Warunki realizacji

- Wykonawca zobowiązany jest do wykonania usługi zgodnie z najlepszymi praktykami i standardami bezpieczeństwa obowiązującymi w branży IT.
- Wykonawca zobowiązany jest do zachowania poufności wszelkich informacji dotyczących infrastruktury IT Zamawiającego.
- Wykonawca zobowiązany jest do współpracy z Zamawiającym na każdym etapie realizacji usługi.
- Wszelkie zmiany w zakresie usługi wymagają pisemnej zgody Zamawiającego

I.3. Harmonogram realizacji

- Etap 1: Dostawa i instalacja serwera (0-0.5 miesiąc)
  - Dostawa sprzętu i oprogramowania,
  - Instalacja i konfiguracja sprzętu oraz oprogramowania,
  - Przeprowadzenie testów akceptacyjnych.
- Etap 2: Wdrożenie systemu SIEM/SOC (0.5-1 miesiąc)
  - Konfiguracja systemu SIEM/SOC,
  - Instalacja agentów na urządzeniach końcowych,
- Etap 3: Utrzymanie i wsparcie techniczne (2-20 miesiąc)
  - Opracowanie i wdrożenie planu zarządzania podatnościami
  - Monitorowanie i zarządzanie incydentami bezpieczeństwa,
  - Sporządzanie i przekazywanie raportów miesięcznych i kwartalnych,
  - Wdrażanie zaleceń z raportów,
  - Aktualizacje i konserwacja systemu.

I.4. Sposób realizacji

Raporty szczegółowe i kwartalne mają być przygotowywane i podpisywane imiennie przez specjalistę IT o niezbędnych kompetencjach z zakresu bezpieczeństwa IT i posiadającą co

najmniej 2 z poniższych certyfikacji branżowych (ie. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:

- EC-Council CEH: Certified Ethical Hacker
- Cisco CCNP Security
- Cisco CCNA CyberOps
- PCNSE: Palo Alto Networks Certified Network Security Engineer
- Fortinet Certified Expert (FCX) in Cybersecurity
- OSCP: Offensive Security Certified Professional

Wdrażanie zaleceń z raportów kwartalnych zostanie realizowane przez zespół co najmniej 2 specjalistów IT o następujących kompetencjach:

- Osoba 1 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 2 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:
  - EC-Council CEH: Certified Ethical Hacker
  - Cisco CCNP Security
  - Cisco CCNA CyberOps
  - PCNSE: Palo Alto Networks Certified Network Security Engineer
  - Fortinet Certified Expert (FCX) in Cybersecurity
  - OSCP: Offensive Security Certified Professional
- Osoba 2 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:
  - EC-Council CEH: Certified Ethical Hacker
  - Cisco CCNP Security
  - Cisco CCNA CyberOps
  - PCNSE: Palo Alto Networks Certified Network Security Engineer
  - Fortinet Certified Expert (FCX) in Cybersecurity
  - OSCP: Offensive Security Certified Professional
  - LPIC-1 Certified Linux Administrator

Efektem przeprowadzonych prac będą dokumenty przygotowane przez Wykonawcę przekazane Zamawiającemu w formie papierowej i elektronicznej: pliki *.pdf oraz wersje edytowalne (w formatach *.odt i .docx):

1. Dokumentacja powykonawcza
   - Pełny opis konfiguracji systemu SIEM/SOC.
   - Procedury operacyjne.
   - Instrukcje obsługi systemu.

2. Raporty okresowe:
    - Comiesięczne raporty szczegółowe z działania systemu SOC/SIEM (20 raporty w ciągu 20 miesięcy):
        - Analiza incydentów bezpieczeństwa.
        - Statystyki wykrytych zagrożeń i podjętych działań.
        - Stan zabezpieczeń systemu.
    - Kwartalne raporty podsumowujące (1-2 strony) z zaleceniami (7 raportów w ciągu 20 miesięcy):
        - Przegląd najważniejszych incydentów i trendów.
        - Rekomendacje dotyczące dalszych działań i optymalizacji systemu.

I.5. Harmonogram płatności

- Płatności będą realizowane **co kwartał w równych ratach**. Łączny koszt realizacji zamówienia zostanie podzielony na **7 równych płatności**, rozłożonych na okres 20 miesięcy. Każda rata będzie stanowiła równą część całkowitej wartości umowy.

Część II: Audyt bezpieczeństwa infrastruktury IT zgodny z wymogami Krajowymi Ramami Interoperacyjności (KRI) oraz wdrożenie zaleceń poaudytowych.

Przedmiotem zamówienia jest przeprowadzenie **audytu bezpieczeństwa infrastruktury IT** zgodnego z wymogami Krajowymi Ramami Interoperacyjności (KRI) oraz **wdrożenie zaleceń poaudytowych** w organizacji Zamawiającego. Celem audytu jest zidentyfikowanie potencjalnych luk i słabości w systemach, aplikacjach oraz konfiguracjach urządzeń sieciowych, a następnie wdrożenie odpowiednich środków zaradczych, aby zapewnić zgodność z aktualnymi standardami bezpieczeństwa systemów teleinformatycznych.

II.I. Zakres usługi

Usługa obejmuje audyt infrastruktury IT:

- Serwery fizyczne i wirtualne (do 10 sztuk)
- Routery i firewalle (do 4 sztuk)
- Przełączniki sieciowe L2 i L3 (do 12 sztuk)
- Inne urządzenia sieciowe (drukarki, kamery IP, itp.) (do 5 sztuk)
- Urządzenia końcowe (do 70 sztuk)

Usługa obejmuje następujące działania:

- **Audyt bezpieczeństwa infrastruktury IT**:
    - Przegląd i analiza aktualnej infrastruktury IT
        - Dokumentacja i schematy topologii sieci
        - Inwentaryzacja urządzeń i systemów
    - Przegląd architektury sieci pod kątem bezpieczeństwa teleinformatycznego
        - Analiza segmentacji sieci
        - Ocena mechanizmów kontroli dostępu
    - Ocena polityk bezpieczeństwa i procedur, w szczególności przeprowadzenie audytu polityki kopii zapasowych i backup-ów, audyt procedur na wypadek awarii
        - Przegląd polityk zarządzania hasłami
        - Ocena procedur zarządzania incydentami
    - Testy penetracyjne wewnętrzne i analiza podatności
        - Analiza zabezpieczeń urządzeń sieciowych
        - Analiza podatności systemów operacyjnych
        - Testy aplikacji webowych i usług sieciowych
    - Testy penetracyjne zewnętrzne i analiza podatności
        - Testy zabezpieczeń firewalli i routerów
        - Symulacja ataków z zewnątrz
    - Przegląd konfiguracji urządzeń sieciowych i usług
        - Ocena zabezpieczeń protokołów sieciowych
        - Sprawdzenie konfiguracji urządzeń pod kątem zgodności z najlepszymi praktykami
    - Ocena zgodności z KRI
- Przygotowanie **raportu z audytu**:
    - Szczegółowy raport zawierający wyniki audytu
    - Wizualizacja luk i podatności na schematach sieci
    - Identyfikacja luk i podatności w systemach wraz z wyjaśnieniem ich znaczenia i oceną ryzyka (prawdopodobieństwo/zagrożenie)
    - Określenie priorytetów dla działań naprawczych

    - Wnioski i rekomendacje w celu dokładnego rozpoznania i redukcji zidentyfikowanych ryzyka, zagrożeń i podatności oraz wskazanie adekwatnych działań (**zaleceń**) mających na celu jak najszybsze ich wyeliminowanie
- **Wdrożenie zaleceń**, wykonane przez **3-osobowy zespół** Wykonawcy w ścisłej współpracy z zespołem IT Zamawiającego:
    - Analiza możliwości technicznych implementacji zaleceń, pod względem urządzeń, konfiguracji, licencji, ciągłości działania sieci i ciągłości dostępu do usług.
    - Dostosowanie infrastruktury do wdrożenia zaleceń
        - Modyfikacja konfiguracji sieci
        - Aktualizacja oprogramowania i firmware'u
    - Przygotowanie scenariuszy wdrożenia zaleceń, wraz z procedurami roll-back
    - Wykonanie kopii zapasowych wraz z testami odtworzeniowymi
    - Kontrolowane wdrożenie zaleceń w oknach serwisowych (22:00 – 6:00)
    - Monitorowanie i weryfikacja wdrożonych zaleceń
- Przygotowanie **raportu z wdrożenia zaleceń**

II.2. Warunki realizacji

- Wykonawca zobowiązany jest do wykonania usługi zgodnie z najlepszymi praktykami i standardami bezpieczeństwa obowiązującymi w branży IT.
- Wykonawca zobowiązany jest do zachowania poufności wszelkich informacji dotyczących infrastruktury IT Zamawiającego.
- Wykonawca zobowiązany jest do współpracy z Zamawiającym na każdym etapie realizacji usługi.
- Wszelkie zmiany w zakresie usługi wymagają pisemnej zgody Zamawiającego
- Całość prac musi zostać zrealizowana w ciągu 90 dni od daty podpisania umowy, rozpoczęta nie później niż 59 dnia od podpisania umowy

II.3. Sposób realizacji

Usługa będzie realizowana w siedzibie Zamawiającego (nie zdalnie), w czasie nie dłuższym niż 31 dni kalendarzowych ciągiem. Harmonogram realizacji usługi zostanie uzgodniony z Zamawiającym przed rozpoczęciem prac. Zamawiający zastrzega sobie prawo do monitorowania postępów prac na każdym etapie realizacji oraz do wprowadzania modyfikacji w harmonogramie w uzasadnionych przypadkach.

Usługa zostanie zrealizowana przez zespół co najmniej 3 specjalistów IT o następujących kompetencjach:

- Osoba 1 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 2 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:
  - EC-Council CEH: Certified Ethical Hacker
  - Cisco CCNP Security
  - Cisco CCNA CyberOps
  - PCNSE: Palo Alto Networks Certified Network Security Engineer
  - Fortinet Certified Expert (FCX) in Cybersecurity
- Osoba 2 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:
  - EC-Council CEH: Certified Ethical Hacker
  - Cisco CCNP Security
  - Cisco CCNA CyberOps
  - PCNSE: Palo Alto Networks Certified Network Security Engineer
  - Fortinet Certified Expert (FCX) in Cybersecurity
  - LPIC-1 Certified Linux Administrator
- Osoba 3 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:
  - EC-Council CEH: Certified Ethical Hacker
  - Cisco CCNP Security
  - Cisco CCNA CyberOps
  - PCNSE: Palo Alto Networks Certified Network Security Engineer
  - Fortinet Certified Expert (FCX) in Cybersecurity
  - MCSA: Windows Server 2016

Zamawiający nie dopuszcza możliwości **łączenia funkcji** przez osoby wskazane przez Wykonawcę na potwierdzenie spełnienia ww. warunku. Minimalna liczba wymaganych osób wynosi: **3**.

Efektem przeprowadzonych prac będą dokumenty przygotowane przez Wykonawcę przekazane Zamawiającemu w formie papierowej i elektronicznej: pliki *.pdf oraz wersje edytowalne (w formatach *.odt i .docx):

1. Raport z audytu bezpieczeństwa infrastruktury IT
2. Raport z wdrożenia zaleceń poaudytowych
3.

Część III: Usługa szkoleniowa z zakresu Cyberbezpieczeństwa

Przedmiotem zamówienia jest przeprowadzenie 12 szkoleń z tematyki Cyberbezpieczenstwa na przestrzeni 18 miesięcy:

- **ABC Cyberbezpieczeństwa**, czas trwania: 2h zegarowe, 4 szkolenia
- **Liderzy Cyberbezpieczeństwa: Szkolenie dla Zarządu**, czas trwania: 2h zegarowe, 4 szkolenia
- **Bezpieczeństwo Infrastruktury IT**, czas trwania: 2h zegarowe, 4 szkolenia

III.1. Zakres usługi

Cechy wspólne szkoleń:

- Forma stacjonarna „onsite" na terenie Gminy Rudniki (woj. opolskie)
- Ilość uczestników: do 50 osób
- Szkolenia będą odbywały się w różne dni, nie będą łączone
- Forma prezentacji połączonej z warsztatami, co najmniej 40% zawartości szkolenia mają to być treści praktyczne, aktualne, angażujące i aktywizujące uczestników szkolenia
- Wykonawca w ramach usługi szkoleniowej zapewni uczestnikom wydrukowane materiały szkoleniowe, materiały papiernicze, przybory do pisania, środki dydaktyczne, narzędzia i sprzęt niezbędny do realizacji szkoleń
- Szkolenia kończą się testem weryfikującym skuteczność szkolenia i ankietą wśród uczestników
- Uczestnikom szkolenia zostaną wydane imienne certyfikaty potwierdzające jego ukończenie
- Do każdego szkolenia zapewnione jest uczestnikom szkolenia wsparcie po jego zakończeniu (np. konsultacje) do 2h zegarowych w formie stacjonarnej lub zdalnej z zakresu tematycznego szkolenia
- Wymaganym jest przedstawienia po zakończeniu szkolenia raportu zawierającego informacje o przebiegu szkolenia, ocenie jego skuteczności oraz rekomendacji dotyczące dalszych działań w zakresie cyberbezpieczeństwa i ewentualnych modyfikacji zakresu szkolenia
- Wykonawca musi zagwarantować pełną poufność przekazywanych informacji podczas szkoleń
- Instruktor ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 2 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid") w chwili składania oferty:
    - EC-Council CEH: Certified Ethical Hacker
    - Cisco CCNP Security
    - Cisco CCNA CyberOps

- PCNSE: Palo Alto Networks Certified Network Security Engineer
- Fortinet Certified Expert (FCX) in Cybersecurity
- OSCP: Offensive Security Certified Professional

III.2. Szczegółowe programy szkoleń

- **ABC Cyberbezpieczeństwa**

  Szkolenie typu "Security Awareness". Szkolenia z zakresu security awareness są skierowane do wszystkich pracowników organizacji, niezależnie od ich roli czy poziomu zaawansowania technicznego. Zawartość szkolenia obejmuje:

  - Podstawy bezpieczeństwa informacji
  - Typy zagrożeń, takie jak phishing, malware, ataki man-in-the-middle
  - Zasady korzystania z haseł i zarządzania nimi
  - Bezpieczne korzystanie z sieci Wi-Fi i VPN
  - Ochrona danych osobowych i wrażliwych informacji
  - Postępowanie w przypadku incydentu związanego z bezpieczeństwem informacji
  - Analiza przypadków

- **Liderzy Cyberbezpieczeństwa: Szkolenie dla Zarządu**

  Szkolenie z zakresu cyberbezpieczeństwa dla kadry zarządczej jest bardziej zaawansowane i dostosowane do specyfiki ich roli w organizacji. Elementy zawarte w szkoleniu:

  - Zarządzanie ryzykiem cyberbezpieczeństwa, metodyki i praktyki zarządzania ryzykiem.
  - Strategie i polityki bezpieczeństwa. Jak rozwijać i wdrażać strategie bezpieczeństwa na poziomie organizacyjnym.
  - Omówienie przepisów prawa dotyczących cyberbezpieczeństwa i ochrony danych, takich jak RODO czy ISO 27001.
  - Zarządzanie incydentami, sposoby reagowania na incydenty związane z bezpieczeństwem, zarządzanie kryzysowe i komunikacja wewnętrzna oraz zewnętrzna.
  - Analiza zagrożeń, metody zbierania i analizy informacji o potencjalnych zagrożeniach oraz sposoby ich wykorzystania w procesie decyzyjnym.
  - Zasady korzystania z narzędzi bezpieczeństwa.
  - Ochrona własności intelektualnej.
  - Zarządzanie zasobami ludzkimi.

- Etyka i odpowiedzialność.
- Analiza przypadków - Studia przypadków dotyczące realnych incydentów bezpieczeństwa

- **Bezpieczeństwo Infrastruktury IT**

  Szkolenie typu "Bezpieczeństwo Infrastruktury IT dla Informatyków" ma zaawansowany charakter i skierowane jest do osób z doświadczeniem technicznym. Zawartość:

  - Architektura bezpieczeństwa, omówienie najlepszych praktyk w projektowaniu i implementacji bezpiecznej architektury sieciowej i systemowej.
  - Ochrona na poziomie sieci, zaawansowane techniki zabezpieczeń sieciowych, takie jak firewalle, IDS/IPS, VPNy oraz monitorowanie ruchu sieciowego.
  - Uwierzytelnienie i autoryzacja. 2FA, SSO oraz zaawansowane metody uwierzytelniania.
  - Zarządzanie dostępem, implementacja i zarządzanie politykami bezpieczeństwa i uprawnieniami użytkowników.
  - Ochrona danych. Szyfrowanie danych przechowywanych i transmistowanych, backupy testy odtworzeniowe oraz plany odzyskiwania po awariach.
  - Wykrywanie i reakcja na incydenty. Narzędzia do wykrywania intruzów, SIEM, oraz procedury reagowania na incydenty.
  - Zarządzanie podatnościami. Metody wyrywania podatności, zarządzanie aktualizacjami.
  - Bezpieczeństwo aplikacji i baz danych. Techniki hardeningu, kontroli dostępu, i zabezpieczania interfejsów API.
  - Bezpieczeństwo w chmurze. Specyfika zabezpieczania infrastruktury w chmurze, w tym konteneryzacja i zarządzanie politykami dostępu.
  - Aspekty prawne, omówienie przepisów prawa i standardów branżowych dotyczących bezpieczeństwa informacji.
  - Analiza przypadków - Praktyczne ćwiczenia i scenariusze.

III.3. Harmonogram płatności

- Płatności będą realizowane **co rok.** Łączny koszt realizacji zamówienia zostanie podzielony na **2 równe płatności** po wykonaniu usługi w każdym roku. Każda rata będzie stanowiła równą część całkowitej wartości umowy.

Część IV: Zabezpieczenie infrastruktury IT – Device Hardening

Przedmiotem zamówienia jest usługa **zabezpieczenia infrastruktury IT** poprzez zastosowanie procesu **device hardening** (uszczelnienia urządzeń) w celu zwiększenia odporności na potencjalne zagrożenia. Usługa obejmuje szereg działań mających na celu zmniejszenie powierzchni ataku oraz wdrożenie mechanizmów ochrony w urządzeniach takich jak:

- Serwery fizyczne i wirtualne (do 4 sztuk)
- Routery i firewalle (do 4 sztuk)
- Przełączniki sieciowe L2 i L3 (do 12 sztuk)
- Inne urządzenia sieciowe (drukarki, kamery IP, itp.) (do 5 sztuk)

IV.1. Zakres usługi

Usługa device hardening obejmuje następujące działania:

1. **Analiza i inwentaryzacja urządzeń:**
    - Identyfikacja wszystkich urządzeń wchodzących w skład infrastruktury IT
    - Określenie typu, modelu, systemu operacyjnego i roli każdego urządzenia
    - Analiza konfiguracji urządzeń pod kątem potencjalnych luk w zabezpieczeniach
2. **Opracowanie planu zabezpieczeń:**
    - Opracowanie indywidualnego planu device hardening dla każdego typu urządzenia
    - Uwzględnienie specyfiki i wymagań poszczególnych urządzeń oraz całej infrastruktury
    - Konsultacje z Zamawiającym w celu dostosowania planu do jego potrzeb
3. **Wdrożenie zabezpieczeń:**
    - Wyłączenie zbędnych usług i protokołów
    - Aktualizacja oprogramowania i firmware'u do najnowszych wersji
    - Utworzenie i egzekwowanie polityki silnych haseł
    - Wdrożenie mechanizmów uwierzytelniania dwuskładnikowego (2FA)
    - Konfiguracja logowania i monitorowania zdarzeń
    - Wdrożenie mechanizmów ochrony przed atakami DDoS
    - Inne działania mające na celu zwiększenie bezpieczeństwa urządzeń

4. **Testowanie i weryfikacja:**
    - Przeprowadzenie testów penetracyjnych w celu weryfikacji skuteczności wdrożonych zabezpieczeń
    - Analiza wyników testów i ewentualne wprowadzenie dodatkowych zabezpieczeń
    - Sporządzenie raportu z testów i rekomendacji

IV.2. Warunki realizacji

- Wykonawca zobowiązany jest do wykonania usługi zgodnie z najlepszymi praktykami i standardami bezpieczeństwa obowiązującymi w branży IT.
- Wykonawca zobowiązany jest do zachowania poufności wszelkich informacji dotyczących infrastruktury IT Zamawiającego.
- Wykonawca zobowiązany jest do współpracy z Zamawiającym na każdym etapie realizacji usługi.
- Wszelkie zmiany w zakresie usługi wymagają pisemnej zgody Zamawiającego.

IV.3. Sposób realizacji

Usługa będzie realizowana w siedzibie Zamawiającego (nie zdalnie), w ciągu 4 dni roboczych ciągiem od dnia rozpoczęcia prac. Harmonogram realizacji usługi zostanie uzgodniony z Zamawiającym przed rozpoczęciem prac.

Wykonawca zobowiązany jest zrealizować usługę (zakończyć) w terminie do 2 miesięcy od dnia zawarcia umowy, przy czym za dzień zrealizowania usługi (zakończenia) Strony zgodnie przyjmują datę podpisania protokołu odbioru końcowego **Raportu końcowego z wykonania usługi, zawierającego szczegółowy opis przeprowadzonych działań** bez uwag i zastrzeżeń

Usługa zostanie zrealizowana przez zespół co najmniej 2 specjalistów IT o następujących kompetencjach:

- Osoba 1 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 2 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:
    - EC-Council CEH: Certified Ethical Hacker
    - Cisco CCNP Security
    - Cisco CCNA CyberOps
    - PCNSE: Palo Alto Networks Certified Network Security Engineer
    - Fortinet Certified Expert (FCX) in Cybersecurity

  - OSCP: Offensive Security Certified Professional
- Osoba 2 ma posiadać kompetencje z zakresu bezpieczeństwa IT i posiadać co najmniej 1 z poniższych certyfikacji branżowych (tj. zdany egzamin), wskazane certyfikacje muszą być ważne (tzw.„valid”) w chwili składania oferty:
  - EC-Council CEH: Certified Ethical Hacker
  - Cisco CCNP Security
  - Cisco CCNA CyberOps
  - PCNSE: Palo Alto Networks Certified Network Security Engineer
  - Fortinet Certified Expert (FCX) in Cybersecurity
  - OSCP: Offensive Security Certified Professional
  - LPIC-1 Certified Linux Administrator