Załącznik nr 4 – Opis przedmiotu zamówienia

w ramach zapytania ofertowego nr 3/S/FEPW-1.2/2025 z dnia 30.04.2025r r.

Przedmiot zamówienia:

Usługi doradcze - Audyt Cyberbezpieczeństwa – 1. Szt. - audyt infrastruktury i konfiguracji IT pod kątem wydajności, pojemności i konfiguracji pod względem cyberbezpieczeństwa zarówno w zakresie IT jak i OT w celu zapewnienia bezpieczeństwa cyfrowego działalności firmy SEGER.

1. Zakres usługi:

Pełna analiza środowiska informatycznego, środowiska sieci przewodowej i bezprzewodowej, środowiska serwerowego i wirtualizacji, kopii zapasowych i przestrzeni dyskowych, bezpieczeństwa użytkowników końcowych, bezpieczeństwa formalnego (dokumentacja, procedury, regulaminy i umowy z dostawcami usług IT), usług chmurowych (jeśli występują), skanowanie podatności wybranych aplikacji z zewnątrz lub z wewnątrz systemu, szczegółowy raport z przeprowadzonych prac, wskazania dot. obszarów wymagających uwagi i poprawy, spotkanie podsumowujące, omówienie stanu infrastruktury.

2. Szczegółowy zakres audytu:

- Określenie poziomu zabezpieczeń środowiska IT, identyfikacja potencjalnych zagrożeń oraz rekomendacja działań naprawczych,
- Kontekst Organizacyjny,
- Opis odpowiedzialności i podziału ról w obrębie działu IT oraz współpracy z innymi działami,
- Opis sieci, serwerów, urządzeń końcowych,
- Systemy sterowania i monitoringu (np. SCADA, systemy automatyki przemysłowej),
- Integracja systemów IT i OT (technologii operacyjnych),
- Analiza dokumentacji, wywiady z pracownikami, obserwacja konfiguracji systemów.
- Przegląd Polityk i Procedur Bezpieczeństwa, w tym ocena istniejących polityk i ich zgodności z najlepszymi praktykami, procedury zarządzania incydentami, mechanizmy wykrywania, reagowania i raportowania incydentów,
- Opis rekomendowanego procesu wdrażania modyfikacji w systemach IT bez obniżania poziomu bezpieczeństwa,
- Ocena Zabezpieczeń Fizycznych i Środowiskowych,
- Ocenę Zabezpieczeń Sieciowych,
- Ocenę Systemów i Aplikacji,
- Zarządzanie Tożsamością i Dostępem,
- Zarządzanie Ryzykiem w odniesieniu do wskazanych w dokumencie zagrożeń z rekomendacjami planu reagowania i zapobiegania,
- Audyt Systemu Dziedzinowego ERP XL w zakresie Zarządzania dostępem, aktualizacji i łatek,
- Integracja z innymi systemami: Bezpieczne interfejsy API, szyfrowanie przesyłanych danych,
- Rejestrowanie działań użytkowników oraz monitorowanie nietypowych zachowań,

- Audyt Systemu Obiegu Dokumentów Webcon,
- Audyt Oprogramowania CAD/CAM,
- Opracowanie polityk bezpieczeństwa dedykowanych projektom, audyty licencyjne oraz monitoring dostępu do danych,
- Bezpieczeństwo Pracowników Zdalnych, zdalny dostęp, ochrona „endpointów”,
- Audyt Zabezpieczeń Urządzeń Mobilnych,
- Audyt pod kontem wykorzystywanych Produktów Microsoft – M365,
- Opis scenariusza działania dla Sytuacji Awaryjnej: Brak Prądu,
- Audyt dostępnych narzędzi gwarantujących dostępność dokumentacji technicznej i cyfrowego wsparcia operatora na stanowiskach – PDM,
- Audyt systemu zarzadzania magazynem WMS, integracji z ERP, MES i podsystemem regałów automatycznych Kardex,
- Ocena ryzyka dostępu do systemów i danych: ataki typu denial-of-service (DoS), przeciążenia platform, uszkodzenie infrastruktury telekomunikacyjnej,
- Naruszenie przepisów ochrony danych, takich jak RODO,
- Rekomendacje i Plan Działań Naprawczych.

3. Dodatkowe działania w ramach audytu:

- Przeprowadzenie warsztatów podsumowujących z kluczowymi pracownikami w organizacji składające się z min. 3 spotkań z zarządem firmy, min.3 spotkań z kierownikami sekcji lub wydziałów oraz 2 spotkań z pracownikami realizującymi zadania w lokalizacji zdalnej, przy czym każdorazowo pojedyncze spotkanie nie może przekroczyć 3 godzin roboczych,
- Obserwacja min.3 pracowników pod kątem potencjalnych zachowań niebezpiecznych związanych z pozostawieniem niezabezpieczonego sprzętu, łączenia się do potencjalnie niebezpiecznych sieci, i inne formy narażania na ataki cyberprzestępców,
- Przeprowadzenie ankiet bezpieczeństwa z użytkownikami końcowymi, w minimum 2 wybranych obszarach, przy czym 1 z tych obszarów musi dotyczyć warstwy sprzętowej, a drugi programowej wraz z opracowaniem wyników ankiet.
- Weryfikacja procedur, dokumentacji, regulaminów pod kątem zgodności z wnioskami z audytu, wskazania dot. obszarów wymagających uwagi i poprawy w formie raportu podsumowującego-
1 spotkanie podsumowujące, w siedzibie firmy, w celu omówienia stanu infrastruktury z osobą pełniącą rolę koordynatora, projektanta w tym zakresie i głównego administratora.

4. Raport końcowy z audytu musi obejmować podsumowanie, przedstawienie wyników, procesów naprawczych w celu poprawy bezpieczeństwa firmy SEGER, tj.:

- Szczegółowe wyniki wizji lokalnej,
- Wyróżnienie obszarów wymagających uwagi oraz silnych stron zabezpieczeń fizycznych,
- Lista konkretnych podatności z ich nazwami, numerami CVE (Common Vulnerabilities and Exposures), szczegółowymi opisami, oraz rekomendacjami ich usunięcia lub zminimalizowania skutków zidentyfikowanej podatności,
- Załączenie zrzutów ekranu, logów oraz innych danych wspierających identyfikację podatności.
- Wskazanie liczby podatności sklasyfikowanych jako niskie, średnie, wysokie i krytyczne,

- Opis potencjalnych skutków wykorzystania każdej podatności (np. utrata danych, przerwy w dostępności, ataki hakerskie),
- Wskazanie, które podatności powinny być naprawione jako pierwsze, bazując na ich krytyczności i potencjalnych skutkach,
- Rekomendacje szkoleń z cyberbezpieczeństwa dla pracowników, które pozwoli na zapewnienie, że wszyscy pracownicy są świadomi zagrożeń i wiedzą, jak postępować w przypadku podejrzanych aktywności,
- Rekomendacje w zakresie bezpieczeństwa w odniesieniu do integracji systemu WMS z systemami śledzenia ruchu materiałowego oparte o RFID,

5. Uwarunkowania prawne przeprowadzenia audytu:

Audyt bezpieczeństwa ma zostać przeprowadzony w oparciu o Standardy:

1. Norma PN-EN ISO/IEC 27001:2023
2. Norma PN-EN ISO 22301:2020
3. Wytyczne NIST (National Institute of Standards and Technology),
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).

6. Sposób realizacji usługi:

Wszystkie prace związane z realizacją zamówienia wykonywane będą w sposób następujący:
1. Audyt opierać się będzie na wizji lokalnej przeprowadzonej przez wskazane przez Wykonawcę osoby w lokalizacji Zamawiającego. Ponadto analiza oparta będzie o wywiad i oświadczenia wskazanych przez Zamawiającego osób. Opracowanie końcowej dokumentacji, wykonane zostanie w siedzibie Wykonawcy,
2. Audyt będzie prowadzony na poziomie trzech warstw: metodologicznej, organizacyjnej, dokumentacyjnej,
3. Zamawiający wymaga, aby przedmiotowa analiza i ocena cyberbezpieczeństwa realizowana była w oparciu o standardy określone w pkt. 5- powyżej.

Nie dopuszcza się realizacji audytu w sposób zdalny.
Główne miejsce realizacji audytu – siedziba Zamawiającego.

8. Opis infrastruktury informatycznej objętej audytem:

- 2 serwery HP z macierzą Huwawei w klastrze HA,
- Sieć przewodowa oparta o przełączniki zarządzalne w 2 lokalizacjach, w ilości 9 szt.
- Połączenie światłowodowe pomiędzy lokalizacjami,
- Sieć bezprzewodowa oparta o urządzenia UbiQuiti, - 13 szt.
- Serwerownia w oddzielnym pomieszczeniu, punkty dystrybucji połączeń sieciowych w 3 lokalizacjach,
- Końcówki (komputery, laptopy) w ilości minimum 50% posiadanych przez firmę w ciągłym użyciu – firma posiada 96szt. w tym 15 szt. poza główną lokalizacją.
- Systemy oparte na wirtualizacji HyperV – 7 szt.
- Kopie zapasowe oparte o system Nakivo – retencja kopii:

a) NAS1:
- zachowanie 11 ostatnich punktów kopii,
- zachowaj jeden punkt odzyskiwania dziennie przez 7 dni,
- zachowaj jeden punkt odzyskiwania tygodniowo przez 4 tygodnie,
- zachowaj jeden punkt odzyskiwania miesięcznie przez 1 miesiąc,
b) NAS2:
- zachowanie 10 ostatnich punktów kopii,
- zachowaj jeden punkt odzyskiwania dziennie przez 7 dni,
- zachowaj jeden punkt odzyskiwania tygodniowo przez 3 tygodnie,
c) NAS3:
- zachowanie 10 ostatnich punktów kopii

- 3 urządzenia klasy NAS w tym w jedna lokalizacji zdalnej,
- Weryfikacja posiadanego przez firmę oprogramowania dziedzinowego ERP XL, w zakresie Zarządzania dostępem, aktualizacji i łatek, integracji z innymi systemami poprzez bezpieczne interfejsy API, szyfrowanie przesyłanych danych – w zakresie następujących stanowisk:

NUMER	MODUŁ	ILOŚĆ
44	XL HR Kasa/Bank	2
56	XL HR Płace i Kadry	2
5601	Płace i Kadry Plus - Opcja współpracy z Comarch ERP XL	1
0	Business Intelligence - Obszar analityczny Magazyn	1
	Business Intelligence - Obszar analityczny Zamówienia	1
21	XL Licencja stanowiskowa	37
22	XL Administracja	37
23	XL Sprzedaż	10
24	XL Księgowość	3
25	XL Kompletacja	1
26	XL Środki Trwałe	2
27	XL Business Intelligence - Księga Raportów	2
28	XL Import	4
30	XL Menadżer baz	37
31	XL Zamówienia	13
32	XL Serwis	1
39	XL Produkcja	7
126	XL Business Intelligence - Point	1
136	XL MES	15
201	Business Intelligence - Obszar analityczny Logistyka	1
210	Business Intelligence - Obszar analityczny Produkcja	1
215	XL Business Intelligence - e-BI Standard	1
301	ECOD - Współpraca z dostawcami	1000
302	ECOD - Współpraca z odbiorcami	1000
307	Sprzedaż (moduł Reklamacje)	1000

312	XL e-Sprawozdania	1000
501	Administrator (moduł Definiowanie Interfejsu)	1000
602	Business Intelligence - Obszar analityczny Umowy	1
604	Business Intelligence – Obszar analityczny Reklamacje	1

- Weryfikacja posiadanego przez firmę oprogramowania EOD Webcon – 47 licencji typu CAL +1 szt. Server +1 szt. Designer +1 szt. server test,
- Weryfikacja posiadanego przez firmę oprogramowania CAD/CAM – 8 szt.
- Weryfikacja posiadanego przez firmę oprogramowania PDM licencje: 16 szt.
- Weryfikacja posiadanego przez firmę oprogramowania Biurowego M365,
- Weryfikacja monitoringu wizyjnego –46 kamer 2 urządzeń nagrywających,
- Weryfikacja urządzeń i oprogramowania do obsługi kontroli dostępu,
- Weryfikacja zabezpieczeń w zakresie posiadanego oprogramowania antywirusowego dla serwerów i końcówek,
- Weryfikacja urządzeń mobilnych (telefony komórkowe i tablety) w ilości minimum 50% posiadanych przez firmę w ciągłym użyciu – 40 szt.
- Weryfikacja końcówek cyfrowych dostępnych w ramach parku maszynowego – 34 szt.
- Weryfikacja podatności dla posiadanych drukarek ZEBRA - 5 szt.