OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego w trybie Zapytania Ofertowego, pod nazwą:

„Przeprowadzenie szkoleń wraz z udostępnieniem platformy szkoleniowej”

realizowanego w ramach projektu

„Cyberbezpieczna Gmina Rajcza”

Zamawiający: Gmina Rajcza, ul. Górska 1, 34-370 Rajcza

Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”

I. SZKOLENIE DLA PRACOWNIKÓW ZAMAWIAJĄCEGO Z CYBERBEZPIECZEŃSTWA

1. Szkolenie dla **58 osób** będzie prowadzone zgodnie z harmonogramem szkoleń ustalonym na etapie realizacji.
2. Szkolenia będą podzielone na 2 grupy szkoleniowe.
3. Szkolenie dla jednej grupy szkoleniowej musi wynosić minimum 2 godziny szkoleniowe.
4. Wszystkie szkolenia muszą być prowadzone w języku polskim na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac z dołączonym zakresem merytorycznym, dostarczonego przez Wykonawcę Zamawiającemu.
5. Zamawiający wymaga prowadzenia dokumentacji Listy obecności uczestników szkolenia.
6. Szkolenia dla pracowników muszą obejmować minimum zagadnienia:
   a) Wprowadzenie do cyberbezpieczeństwa - definicja i znaczenie cyberbezpieczeństwa w administracji publicznej. Omówienie roli i odpowiedzialności pracowników w utrzymaniu bezpieczeństwa informacji.
   b) Podstawowe zasady cyberbezpieczeństwa - omówienie fundamentalnych reguł i procedur dotyczących ochrony danych, zarządzania hasłami, autoryzacji i bezpiecznego korzystania z zasobów informatycznych.
   c) Phishing i inne ataki socjotechniczne - rozpoznawanie i ochrona przed próbami wyłudzenia informacji, atakami phishingowymi oraz innymi technikami socjotechnicznymi.
   d) Zagrożenia związane z oprogramowaniem typu ransomware i malware - identyfikacja, mechanizmy działania oraz metody zapobiegania i reagowania na zagrożenia związane z ransomware i malware.
   e) Bezpieczna obsługa poczty elektronicznej - zasady korzystania z e-maila, rozpoznawanie podejrzanych wiadomości, załączników oraz linków, a także ochrona przed spamem i phishingiem.
   f) Zarządzanie hasłami i autoryzacja - tworzenie silnych haseł, korzystanie z menedżerów haseł, wprowadzenie autoryzacji dwuetapowej oraz znaczenie kluczy sprzętowych.
   g) Ochrona urządzeń mobilnych - zabezpieczanie urządzeń przenośnych przed utratą danych, kradzieżą oraz złośliwym oprogramowaniem.
   h) Bezpieczne przetwarzanie i przechowywanie danych - szyfrowanie danych, zasady bezpiecznego przechowywania informacji, zarządzanie dostępem oraz udostępnianie danych w sposób bezpieczny.
   i) Zarządzanie ryzykiem w cyberbezpieczeństwie - identyfikacja i ocena ryzyka, zarządzanie ryzykiem oraz wdrażanie odpowiednich środków zabezpieczających.
   j) Ochrona przed spoofingiem i atakami telefonicznymi - mechanizmy ochrony przed spoofingiem, fałszowaniem numerów telefonów oraz innymi technikami oszustw telefonicznych.
   k) Zarządzanie dostępem do systemów i informacji - zasady przydzielania uprawnień, kontrola dostępu oraz monitorowanie aktywności użytkowników w systemach informacyjnych.
   l) Bezpieczna komunikacja w środowisku cyfrowym - szyfrowanie komunikacji, korzystanie z bezpiecznych kanałów komunikacyjnych, zabezpieczenie wideokonferencji oraz przesyłania danych.
   m) Ochrona przed wyłudzeniami danych osobowych (PII) - zapobieganie wyłudzeniom danych osobowych za pomocą metod socjotechnicznych oraz przeciwdziałanie kradzieży tożsamości.
   n) Reagowanie na incydenty bezpieczeństwa - procedury postępowania w przypadku incydentu, raportowanie naruszeń, analizowanie przyczyn oraz minimalizowanie skutków.

Zamawiający wymaga, aby szkolenie zostało zaprojektowane w taki sposób, aby nie tylko podnosić świadomość w zakresie cyberbezpieczeństwa, ale także rozwijać praktyczne umiejętności uczestników w rozpoznawaniu i neutralizowaniu zagrożeń. Zakres tematyczny szkolenia winien być zgodny z wymogami projektu i stanowić integralną część strategii podnoszenia poziomu ochrony informacji w administracji publicznej.

II. SZKOLENIA SPECJALISTYCZNE

1. Szkolenie w zakresie systemu XDR

Szkolenie obejmuje następujące zagadnienia realizowane w ciągu 6 godzin zegarowych. Liczba uczestników szkolenia 1 osoba.
Szkolenie w formule online.

Extended Detection & Response (XDR) – wprowadzenie

- Czym jest XDR i jak wpisuje się w model wielowarstwowej ochrony.
- Różnice między EPP, EDR i XDR na przykładzie rozwiązań dostępnych na rynku.
- Korzyści z wdrożenia XDR: szerszy kontekst zagrożeń, korelacja zdarzeń, szybsze podejmowanie decyzji.
- Rola komponentu inspekcyjnego w architekturze XDR.

Omówienie funkcji systemu XDR

- Przegląd interfejsu i głównych modułów systemu.
- Kluczowe możliwości: monitorowanie zachowań, wykrywanie anomalii, reagowanie na incydenty.
- Sposoby prezentacji danych – zdarzenia, incydenty, kontekst użytkownika i maszyny.
- Mechanizmy skanowania zachowań i detekcji offline/online.

Architektura i wdrożenie serwera XDR

- Wymagania sprzętowe i systemowe.
- Modele wdrożeniowe: standalone vs. integracja z konsolą zarządzającą.
- Rola serwera, bazy danych i komunikacji z agentami.
- Planowanie pojemności i optymalizacja dla większych środowisk.
- Najczęstsze błędy wdrożeniowe i jak ich uniknąć.

Instalacja i konfiguracja konektora XDR

- Instalacja komponentu łączącego agenta endpoint z serwerem XDR.
- Konfiguracja źródeł danych i synchronizacji z konsolą zarządzającą.
- Przegląd parametrów komunikacyjnych i zasady działania agenta.
- Testowanie poprawności połączenia i diagnozowanie problemów.

Generowanie i analiza detekcji

- Praktyczne zadania: ręczne wywoływanie detekcji w kontrolowanym środowisku.
- Praca z konsolą XDR: filtrowanie, sortowanie, tworzenie widoków.
- Interpretacja alertów – kontekst, priorytetyzacja, korelacja zdarzeń.
- Analiza śladów ataku – od nietypowych procesów po komunikację sieciową.

Tworzenie reguł i automatyzacja reakcji

- Składnia i logika reguł detekcji – warunki, wyjątki, działania.
- Tworzenie reguł dostosowanych do środowiska klienta.
- Automatyczne działania: powiadomienia, blokady, zgłoszenia do systemu ticketowego.
- Scenariusze automatycznej reakcji w oparciu o klasy incydentów.

Raportowanie i eksport danych

- Tworzenie raportów na potrzeby audytu, zarządu i zespołów SOC.
- Personalizacja raportów i automatyczne generowanie zestawień.
- Eksport danych do SIEM / integracja z narzędziami typu SOAR.
- API i możliwości automatyzacji raportowania w dużych środowiskach.

Zamawiający dopuszcza dostarczenie bonów szkoleniowych do wykorzystania przez administratora w dogodnym okresie, ważnego minimum 5 miesiące.

2. Szkolenie z systemu ochrony DLP

Szkolenie z systemu ochrony DLP Zamawiający wykorzystuje w swojej infrastrukturze oprogramowanie Safetica, w związku z czym zakres merytoryczny szkolenia został dostosowany do tego rozwiązania. Szkolenie obejmuje następujące zagadnienia realizowane w ciągu 2 dni szkoleniowych (minimum 12 godzin zegarowych), Liczba uczestników szkolenia 1 osoba. Szkolenie w formule online.

Wdrożenie rozwiązania Safetica

- Omówienie instalatora – struktura pakietu, dostępne opcje instalacji.
- Wdrożenie serwera Safetica – instalacja, konfiguracja początkowa, weryfikacja poprawności działania.
- Wdrożenie klienta Safetica – instalacja agenta na stacjach końcowych, metody dystrybucji.

Konsola Safetica Maintenance

- Kategoryzacja aplikacji oraz stron internetowych.
- Zarządzanie bazą danych – konfiguracja, optymalizacja, konserwacja.
- Ustawienia klienta Safetica – parametry pracy agenta, polityki lokalne.
- Dezaktywacja modułów klienta Safetica – selektywne włączanie i wyłączanie funkcjonalności.
- Ustawienia integracji Safetica – połączenie z usługami katalogowymi, systemami zewnętrznymi.

Safetica Discovery

- Uruchomienie modułu Discovery – konfiguracja skanowania i zakres analizy.
- Analiza potencjalnych wycieków danych – identyfikacja zagrożeń, ocena ryzyka.
- Dostosowanie konsoli do własnych potrzeb – filtrowanie danych, tworzenie widoków, personalizacja raportów.

Podstawowe DLP

- Strefy – koncepcja stref bezpieczeństwa w Safetica.
- Konfiguracja dostępów dla urządzeń zewnętrznych i portów (USB, Bluetooth, porty komunikacyjne).
- Definiowanie polityk kontroli urządzeń i peryferyjnych.

Zaawansowane DLP

- Reguły DLP – tryby polityk (audyt, powiadamianie, blokowanie).
- Reguły ogólne – definiowanie globalnych zasad ochrony danych.
- Reguły aplikacji – polityki dedykowane dla konkretnych aplikacji i procesów.
- Kategorie danych – klasyfikacja informacji, rola kategorii w budowaniu polityk DLP.
- Inteligentne wykrywanie danych osobowych – mechanizmy automatycznej identyfikacji danych wrażliwych (PESEL, numery dokumentów, dane finansowe).
- Analiza zawartości archiwów – metody detekcji danych wrażliwych w plikach skompresowanych.
- Dzienniki DLP – przegląd, analiza i interpretacja zdarzeń zarejestrowanych przez system.

Zamawiający dopuszcza dostarczenie bonów szkoleniowych do wykorzystania przez Zamawiającego w dogodnym okresie, ważnego minimum 5 miesiące.

III. PLATFORMA SZKOLENIOWA - AUTOMATYCZNE TESTY PHISHINGOWE

1. Celem usługi jest przeprowadzenie kontrolowanych symulacji ataków phishingowych w celu weryfikacji poziomu świadomości cyberbezpieczeństwa wśród pracowników Zamawiającego, identyfikacji obszarów ryzyka oraz dostarczenia rekomendacji dalszych działań prewencyjnych i szkoleniowych.
2. Etapy realizacji usługi

Usługa będzie realizowana w następujących etapach:

Etap 1: Faza przygotowawcza

1) Współpraca z Zamawiającym w celu identyfikacji i zdefiniowania grup docelowych (np. działy, stanowiska) objętych kampanią.
2) Bezpieczne przekazanie przez Zamawiającego i przetwarzanie przez Wykonawcę listy adresów e-mail pracowników przypisanych do poszczególnych grup. Liczba adresów e-mail objętych usługą: 56.
3) Ustalenie z Zamawiającym harmonogramu oraz scenariuszy dla poszczególnych serii ataków.
4) Przekazanie zamawiającemu wymagań konfiguracyjnych.

Etap 2: Przeprowadzenie kampanii phishingowej

1) Wykonawca przeprowadzi kontrolowaną kampanię składającą się z minimum czterech (4) serii symulowanych ataków phishingowych, skierowanych do wszystkich zdefiniowanych użytkowników.
2) Każda z czterech serii musi wykorzystywać co najmniej dwa (2) różne scenariusze ataku, wybrane spośród poniższych typów:
   - Phishing z linkiem (Drive-by): Scenariusz polegający na próbie nakłonienia użytkownika do kliknięcia w link prowadzący do symulowanej, kontrolowanej przez Wykonawcę strony internetowej.
   - Phishing z formularzem (Data Entry): Scenariusz polegający na próbie nakłonienia użytkownika do wprowadzenia danych (np. poświadczeń logowania) na stronie internetowej imitującej autentyczną witrynę.
   - Phishing z załącznikiem klasycznym: Scenariusz polegający na próbie nakłonienia użytkownika do otwarcia symulowanego, złośliwego załącznika w formacie DOC lub HTML, który po otwarciu inicjuje zdefiniowaną akcję edukacyjną.
   - Phishing z załącznikiem biurowym: Scenariusz polegający na próbie nakłonienia użytkownika do otwarcia symulowanego, złośliwego załącznika w formacie PDF, DOCX lub XLSX.

Etap 3: Informacja zwrotna i edukacja

1) W zależności od decyzji Zamawiającego, podjętej na etapie planowania każdej serii kampanii, Wykonawca musi zapewnić możliwość realizacji jednego z dwóch poniższych trybów informacji zwrotnej:
   - Tryb natychmiastowy: Użytkownik, który popełni błąd (np. kliknie w link, wprowadzi dane, otworzy załącznik), jest niezwłocznie informowany o tym fakcie i przekierowywany do dedykowanej strony lub materiału edukacyjnego, wyjaśniającego naturę błędu i zagrożenia.
   - Tryb zbiorczy: Informacje o błędach popełnionych przez poszczególnych użytkowników są dyskretnie gromadzone przez Wykonawcę. Pracownik otrzymuje zbiorczą informację na temat swoich interakcji z symulowanymi atakami dopiero po zakończeniu danej serii lub całej kampanii, co pozwala na analizę zachowań bez natychmiastowej zmiany czujności.
2) Zamawiający ma prawo do zmiany wybranego trybu informacji zwrotnej przed rozpoczęciem każdej kolejnej serii kampanii.

Etap 4: Raportowanie

1) Po zakończeniu całej kampanii Wykonawca jest zobowiązany do przygotowania i przekazania Zamawiającemu szczegółowego raportu końcowego w formacie PDF.
2) Raport końcowy musi zawierać co najmniej:
    - Streszczenie menedżerskie z kluczowymi wnioskami.
    - Szczegółowe wyniki statystyczne dla całej organizacji oraz poszczególnych grup docelowych (np. wskaźnik klikalności, wskaźnik podania danych, wskaźnik otwarcia załącznika dla każdego scenariusza).
    - Analizę wyników, w tym identyfikację najsłabszych punktów, najbardziej podatnych grup oraz najskuteczniejszych scenariuszy ataków.
    - Wnioski i rekomendacje dotyczące dalszych działań szkoleniowych i technicznych w celu wzmacniania świadomości bezpieczeństwa w organizacji.