Opis przedmiotu szacowania

Założenia i specyfikacja platformy szkoleniowej

System ma zagwarantować możliwość badania i podnoszenia świadomości użytkowników systemu teleinformatycznego. Główne zadanie ma dotyczyć dostarczenia rozwiązania do szkolenia pracowników w identyfikacji głównych cyberzagrożeń, w tym typu:

- phishing
- oszustwa CEO
- ataków socjotechnicznych
- inżynieria społeczna

Kompleksowy program szkoleniowy ma na celu podniesienie poziomu wiedzy i czujności pracowników wobec zagrożeń socjotechnicznych, takich jak phishing, oraz wdrożenie skutecznych mechanizmów ograniczania ryzyka ludzkiego. Zakres szkolenia ma obejmować:

- pełen zestaw modułów edukacyjnych dotyczących rozpoznawania i reagowania na cyfrowe zagrożenia,
- narzędzia do przeprowadzania symulowanych kampanii phishingowych,
- mechanizmy oceny wiedzy użytkowników i identyfikacji obszarów ryzyka,
- dostęp do biblioteki materiałów szkoleniowych, w tym filmów, quizów i interaktywnych scenariuszy.

Program ma umożliwiać identyfikację ryzyka, zmianę zachowania oraz ograniczenie podatności na ataki, możliwe jest wdrożenie strategii redukcji ryzyka **zorientowanej na pracownika (użytkownika)**. Szkolenie wspiera zgodność z obowiązującymi regulacjami prawnymi i branżowymi, w tym z wymaganiami dotyczącymi prowadzenia cyklicznych szkoleń z zakresu bezpieczeństwa informacji.

Główny nacisk położony ma być na wytrenowanie zachowań każdego pracownika w zakresie bezpieczeństwa cybernetycznego. Z uwagi na mocne zróżnicowanie środowiska odbiorców szkoleń i treningów konieczne jest by system posiadał mechanizmy pozwalające na stosowanie indywidualnych ścieżek szkoleniowych zależnych od charakteru każdego pracownika.

System powinien mieć możliwość wykorzystania pracowników jako sojuszników w walce z atakami opartymi na inżynierii społecznej. System powinien mieć możliwość symulacji rzeczywistych ataków wraz z mierzeniem ich skuteczności.

Rozwiązanie musi obsługiwać minimum 750 użytkowników – pracowników organizacji.
Licencja na okres minimum 36 miesięcy.

Główne założenia mają na celu:

- zwiększanie świadomości zagrożeń cyberbezpieczeństwa wśród pracowników.

- edukację dotyczącą rozpoznawania i przeciwdziałania atakom phishingowym i socjotechnicznym.
- Budowanie kultury bezpieczeństwa w organizacji poprzez ciągłe, dostosowane do ryzyka szkolenia.
- zarządzanie ryzykiem ludzkim i zmiana zachowań w środowisku pracy z cyfrowymi narzędziami.
- testy phishingowe i ocena skuteczności szkoleń.
- krótkie, skoncentrowane moduły szkoleniowe dostosowane do aktualnych zagrożeń.
- możliwość personalizacji treści szkoleń, uwzględniająca brandingu i lokalizację.
- dystrybucję materiałów i interfejs w języku polskim, co ułatwia wdrożenie szkoleń w polskich organizacjach.

Specyfikacja istotnych funkcjonalności

A. Platforma szkoleniowa powinna zapewniać funkcjonalność, które pozwolą administratorowi na prowadzenie skutecznych działań prewencyjnych powiązanych z edukacją pracowników.

lp	Platforma szkoleniowa powinna posiadać	Tak / Nie	ilość
1	Gotowe szablony symulacji phishingowej dostępne w wielu językach min. angielski, polski, niemiecki, czeski, ukraiński, hiszpański, włoski.		750
2	Możliwość dostosowania szablonów do potrzeb organizacji		x
3	Symulacja technik ataku spearphishing		x
4	Symulacja technik ataku BEC (Business Email Compromise)		x
5	Automatyczne kampanie – z możliwością planowania (harmonogram)		x
6	Funkcjonalność automatycznego grupowania użytkowników		x
7	Funkcjonalność nadawania i indeksowania metryk na poziomie działów i grup		x
8	Predefiniowany pulpit nawigacyjny obrazujący stan systemu		x
9	Predefiniowany pulpit nawigacyjny z dostępem opartym o uprawnienia (podział)		x
10	Predefiniowany pulpit nawigacyjny z podziałem funkcji pracownik/dział/oddział		x
11	Możliwość integracji z AD		x
12	Możliwość integracji z Microsoft Azure (Entra ID)		x
12	Możliwość prowadzenia symulacji opartej o wyniki użytkowników		x
13	Możliwość dostosowania nazw domen w symulacjach		x
14	Funkcjonalność automatycznego kierowania treningów do odbiorców		x
15	Wsparcie procesu symulacji oparte o procesy behawioralne – badanie emocji i wrażliwości na phishing		x
16	Możliwość dynamicznego tworzenia symulacji zagrożeń – na podstawie zewnętrznych informacji, aktualnych ataków, kampanii itp		x
17	Możliwość tworzenia kampanii opartych na badaniu ryzyka		x
18	Możliwość tworzenia kampanii wyrównanych dla poszczególnych grup		x
19	Predefiniowany system powiadomień dotyczących kampanii np. dla kierowników		x
20	Możliwość tworzenia kampanii phishingowych na nośnikach USB		x
21	Możliwość tworzenia kampanii 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		x

B. **W ramach kampanii phishingowych rozwiązanie powinno posiadać:**

Lp	Landing pages	Tak/nie	ilość
1	Gotowe szablony stron phishingowych		20
2	Obsługę HTTPS		x
3	Obsługę wielu domen		5
4	Możliwość dostosowania strony docelowej		x
5	Możliwość dostosowania domeny		x
6	Możliwość stosowania niestandardowych formularzy internetowych		x

C. **Moduły treningowe powinny realizować**

Lp	Niezbędne funkcjonalności modułu treningowego:		
1	Możliwość dostarczenia interaktywnych szablonów treningowych – w chwili wymagania (w samą porę)		x
2	Możliwość dostarczenia statycznych materiałów – w chwili kiedy konieczne		x
3	LSM – system zarządzania nauką		x
4	Interaktywne szkolenia z zakresu bezpieczeństwa		x
5	Firmowane - interaktywne szkolenia z zakresu bezpieczeństwa		x
6	Indywidualne interaktywne mikro szkolenia		x
7	Indywidualne materiały szkoleniowe		x
8	Spersonalizowane ścieżki nauki		x
9	Możliwość automatycznego powiadamiania LMS		x
10	Planowanie powiadomień związanych ze szkoleniami		x
11	Powiadamianie o postępach szkoleniowych np. do kierownika działu		x
12	Powiadomienia o stanie prowadzonej kampanii np. dla kadry zarządzającej		x
13	Quizy indywidualne		x
14	Możliwość importowania własnych szkoleń w formacie SCORM 1.2		x
15	Szkolenia dostępne w wielu językach min. angielski, polski, niemiecki, czeski, ukraiński, hiszpański, włoski.		750
16	Automatyczne generowanie certyfikatu po ukończeniu szkolenia.		x

D. **Funkcjonalności ułatwiające i wspierające prowadzenie kampanii phishingowych**

lp	Niezbędne funkcjonalności modułu phishingowe:	Tak/nie	
1	Możliwość Kontroli adresów URL / linków/ załączników		x
2	Dynamiczną listę nadawców zaufanych		x
3	Moduł analizy podejrzanych wiadomości (email clastering analiysys)		x
4	Możliwość automatycznego wyzwalania – zadań treningowych		x
5	Ujednolicony pulpit nawigacyjny		x
6	Automatyczny system raportujący o problemach w konkretnych obszarach		x
7	Możliwość modelowania scenariuszy w odpowiedzi na działania użytkowników		x
8	System inteligentnej dystrybucji materiałów		x

E. **Funkcjonalność platformy szkoleniowej**

lp	Platforma powinien zapewniać:		
1	Możliwość pracy w modelu SAAS		x
2	Mechanizmy wspierające 2FA		x
3	Dostęp do pulpitu oparty prawa dostępu (stopniowanie praw)		x

Specyfikacja istotnych modułów
dla zintegrowanego systemu szkoleniowego

1. **Moduły szkoleniowe**
- Dostęp do ponad 300 interaktywnych modułów edukacyjnych z zakresu cyberbezpieczeństwa
- Tematy obejmują m.in. . phishing, ransomware, bezpieczeństwo danych, prywatność, cyberhigienę
- Możliwość personalizacji treści według branży, roli użytkownika i poziomu ryzyka

2. **Symulacje ataków zintegrowane z modułami szkoleniowymi**
- kampanie testowe z fałszywymi e-mailami **(Phishing Simulations)**
- Symulacje z wykorzystaniem nośników USB
- **Z**aawansowane scenariusze socjotechniczne

3. **Ocena ryzyka i raportowanie**
- testy wiedzy użytkowników (Knowledge Assessments)
- analiza ryzyka na podstawie zachowań pracownika (People Risk Explorer)
- panel zarządzania dla dla zespołów bezpieczeństwa (CISO Dashboard)
- bieżące raporty z kampanii i postępów użytkowników

4. **Integracje i automatyzacja**
- Integracja z **Microsoft Active Directory / Azure AD**
- Obsługa plików **SCORM** dla LMS
- automatyczne usuwanie zgłoszonych wiadomości phishingowych
- Integracja z platformą ochrony przed zagrożeniami (Threat Protection Platform)

5. **Obsługa wielu języków**
- Treści dostępne w **40+ językach, w tym najważniejszy: j.polski, ….**
- Możliwość wyboru języka przez użytkownika
- Obsługa użytkowników w środowiskach wielonarodowych

6. **Narzędzia zarządzania treścią**
- możliwość edycji treści szkoleniowych
- **możliwość** zgłaszania podejrzanych wiadomości phishing
- możliwość przypisywania szkoleń na podstawie wyników testów i zachowania