Platforma kampanii phishingowych oraz platforma szkoleniowa online

Dokument do analizy Rynku, porównania Ofert oraz oceny funkcjonalnej Rozwiązań

Pole	Opis
Zamawiający	Exatel
Cel dokumentu	Pozyskanie porównywalnych odpowiedzi rynkowych dotyczących platformy do prowadzenia kampanii phishingowych oraz edukacji użytkowników.
Charakter postępowania	Rozpoznanie rynku i analiza funkcjonalna i handlowa celem wybrania Dostawcy usługi
Model wykorzystania	Wewnętrznie w Exatel oraz w modelu usługowym dla klientów końcowych (MSSP / white label).

Założenia nadrzędne

- Jedna platforma dla części edukacyjnej i kampanii phishingowych.
- Obsługa wielu klientów w modelu multi-tenant z pełną separacją tenantów.
- Możliwość rozdzielenia licencjonowania części edukacyjnej i phishingowej.
- Pełna obsługa języka polskiego na poziomie platformy, raportów i treści.

ZAŁĄCZNIK NR 1 - Opis założeń i Wymagań Projektowych

1. Informacje ogólne

Niniejszy dokument służy pozyskaniu od wykonawców informacji handlowych, funkcjonalnych, technicznych oraz organizacyjnych dotyczących platformy umożliwiającej realizację kampanii phishingowych i prowadzenie szkoleń online w obszarze cyberbezpieczeństwa.

Zamawiający planuje wykorzystanie rozwiązania zarówno na potrzeby własne, jak i do świadczenia usług dla klientów końcowych w modelu MSSP. Oczekiwane jest rozwiązanie skalowalne, wielodzierżawne, możliwe do oferowania w modelu white label oraz zapewniające rozdzielenie zakresu licencjonowania i funkcji zależnie od potrzeb klienta.

2. Cel i zakres odpowiedzi wykonawcy

Odpowiedź wykonawcy powinna umożliwić porównanie rozwiązań dostępnych na rynku w szczególności w zakresie:

- zgodności z wymaganiami biznesowymi Exatel,
- zakresu funkcjonalnego części phishingowej i edukacyjnej,
- bezpieczeństwa, zgodności prawnej i lokalizacji przetwarzania danych,
- modelu licencyjnego i możliwości świadczenia usług w modelu MSSP,
- czasów wdrożenia, obsługi wielu klientów oraz możliwości white label,
- kosztów wariantu usługowego oraz wariantu wewnętrznego dla 500 pracowników Exatel.

3. Model świadczenia usługi oczekiwany przez Zamawiającego

- obsługa wielu klientów na jednej platformie z pełną separacją tenantów,
- jednoczesne prowadzenie kampanii oraz szkoleń dla wielu klientów,
- możliwość samodzielnego przygotowywania treści, testów i kampanii przez Exatel,
- możliwość udostępnienia platformy pod marką Exatel lub marką klienta,
- model rozliczeniowy umożliwiający wzrost skali w trybie pay as you grow,
- możliwość oferowania wyłącznie modułu edukacyjnego albo wyłącznie modułu phishingowego.

4. Wymagania biznesowe

4.1. Wymagania biznesowe wspólne

1. Platforma powinna umożliwiać obsługę wielu klientów w modelu multi-tenant, z pełną separacją danych, konfiguracji, raportów oraz uprawnień pomiędzy tenantami.
2. Rozwiązanie powinno być dostosowane do świadczenia usług w modelu MSSP, w tym do rozliczeń typu pay as you grow.
3. Zamawiający oczekuje jednej platformy obejmującej zarówno funkcję prowadzenia kampanii phishingowych, jak i funkcję edukacji użytkowników.
4. Platforma powinna umożliwiać wykorzystanie zarówno na potrzeby wewnętrzne Exatel, jak i do świadczenia usług klientom końcowym w modelu white label.
5. Platforma, interfejs administracyjny, materiały edukacyjne, raporty oraz kampanie phishingowe powinny być dostępne w języku polskim.
6. Platforma powinna umożliwiać jednoczesną obsługę wielu klientów i prowadzenie równoległych działań w wielu organizacjach.
7. Platforma powinna zapewniać możliwość rozdzielenia licencjonowania części edukacyjnej od części phishingowej oraz ograniczania funkcjonalności per klient, grupa użytkowników lub użytkownik.
8. Platforma powinna zapewniać automatyczne, ciągłe raportowanie postępów i wyników dla obu obszarów funkcjonalnych.
9. Platforma powinna umożliwiać tworzenie własnych szablonów raportów.

4.2. Wymagania biznesowe – kampanie phishingowe

10. Platforma powinna umożliwiać centralne planowanie, uruchamianie i nadzorowanie kampanii phishingowych dla wielu klientów jednocześnie.
11. Zamawiający oczekuje możliwości prowadzenia dedykowanych kampanii phishingowych dla poszczególnych klientów wraz z odrębnym raportowaniem wyników.
12. Raporty dla klientów powinny umożliwiać dodawanie przez Exatel własnych komentarzy, rekomendacji i wniosków.
13. Rozwiązanie powinno wspierać świadczenie usług w modelu operatorskim, z możliwością budowy własnych scenariuszy i kampanii przez Exatel.
14. Platforma powinna umożliwiać przekierowanie do cześci edukacyjnej użytkowników, którzy byli podatni na przeprowadzoną kampanię phishing automatycznie.

4.3. Wymagania biznesowe – część edukacyjna

15. Platforma powinna umożliwiać udostępnianie klientom materiałów edukacyjnych tworzonych przez Exatel.
16. Materiały edukacyjne powinny być dostępne w formie prezentacji, nagrań wideo oraz materiałów interaktywnych.
17. Platforma powinna umożliwiać prowadzenie testów wiedzy po szkoleniach realizowanych przez trenerów Exatel, zarówno stacjonarnie, jak i zdalnie.
18. Treść testów powinna być tworzona przez Exatel, a ukończenie testu powinno skutkować możliwością wygenerowania certyfikatu potwierdzającego udział lub zaliczenie.
19. Platforma powinna wspierać WCAG 2.1; wykonawca powinien opisać poziom zgodności, zakres wsparcia i ewentualne ograniczenia.

5. Wymagania funkcjonalne

5.1. Wymagania funkcjonalne – kampanie phishingowe

20. Platforma powinna umożliwiać przeprowadzenie jednoczesnej kampanii phishingowej do co najmniej 1000 użytkowników w ramach jednego klienta lub projektu.
21. Platforma powinna umożliwiać tworzenie i realizację dedykowanych kampanii phishingowych przygotowanych przez Exatel, w oparciu o własne scenariusze, w liczbie co najmniej 20–25 scenariuszy.
22. Proces uruchomienia kampanii standardowej nie powinien przekraczać 2 dni roboczych, przy założeniu posiadania przez Zamawiającego gotowych materiałów i scenariuszy. Wykonawca powinien odrębnie wskazać typowy czas uruchomienia kampanii niestandardowej.
23. Platforma powinna umożliwiać wykonanie podglądu oraz testu kampanii przed jej wysyłką.
24. Platforma powinna umożliwiać realizację kampanii niestandardowych obejmujących wiadomości e-mail, załączniki oraz strony docelowe.
25. Platforma powinna umożliwiać prowadzenie kampanii opartych wyłącznie o załącznik, np. spreparowany dokument lub fakturę testową.
26. W przypadku kampanii wykorzystujących załączniki platforma powinna umożliwiać śledzenie interakcji użytkownika z załącznikiem w zakresie dostępnym przez rozwiązanie.
27. Platforma powinna umożliwiać tworzenie własnej szaty graficznej kampanii, w tym edycję treści HTML i CSS wiadomości oraz stron docelowych.
28. Platforma powinna umożliwiać budowę dedykowanych stron docelowych. Wykonawca powinien wskazać, czy dopuszczalne jest stosowanie własnych skryptów, w jakim zakresie oraz z jakimi ograniczeniami bezpieczeństwa.
29. Platforma powinna umożliwiać korzystanie z domen własnych Zamawiającego lub klienta oraz z domen dostarczanych w ramach platformy – zależnie od scenariusza kampanii.

30. Wykonawca powinien opisać proces rejestracji, konfiguracji i obsługi domen, w tym domen .pl, .com i .com.pl, oraz sposób zarządzania reputacją nowej domeny wykorzystywanej do kampanii.
31. Wysyłane wiadomości email muszą przejść walidację mechanizmów SPF, DKIM i DMARC dla domen wykorzystywanych w kampaniach.
32. Wykonawca powinien wskazać wymagania konfiguracyjne po stronie systemów pocztowych klienta, w tym minimalny zakres wyjątków lub whitelistingu niezbędnych do realizacji kampanii, wraz ze sposobem ograniczenia ryzyka i czasem obowiązywania zmian.
33. Platforma powinna umożliwiać integrację z klientem pocztowym użytkownika poprzez mechanizm „Zgłoś phishing".
34. Mechanizm „Zgłoś phishing" powinien umożliwiać przekazanie zgłoszenia do zespołu SOC Exatel albo do zespołu klienta.
35. Platforma powinna umożliwiać pomiar skuteczności zgłoszeń phishingu, w tym identyfikację użytkowników, którzy prawidłowo zgłosili kampanię testow, otworzyli wiadomość, otworzyli spreparowany landingpage i podali dane do logowania.
36. Platforma powinna umożliwiać generowanie raportów zbiorczych dla kadry zarządzającej, prezentujących ogólny poziom świadomości bezpieczeństwa w organizacji.
37. Platforma ogranicza widocznośc landingpage z sieci Internet do ustalonoej adresacji IP lub kraju.

5.2. Wymagania funkcjonalne – część edukacyjna

38. Platforma powinna umożliwiać udostępnianie materiałów edukacyjnych przygotowanych przez Exatel.
39. Platforma powinna umożliwiać import własnych materiałów edukacyjnych; wykonawca powinien wskazać obsługiwane formaty importu.
40. Platforma powinna wspierać co najmniej materiały w formie prezentacji, wideo oraz materiałów interaktywnych.
41. Platforma powinna umożliwiać tworzenie, uruchamianie i ocenianie testów wiedzy przygotowanych przez Exatel.
42. Platforma powinna umożliwiać przypisanie testów do wybranych użytkowników, grup lub klientów.
43. Platforma powinna umożliwiać generowanie certyfikatów po ukończeniu szkolenia lub zaliczeniu testu.
44. Platforma powinna umożliwiać automatyczne raportowanie postępów szkoleniowych, wyników testów oraz poziomu ukończenia materiałów.
45. Platforma powinna umożliwiać raportowanie per klient, per grupa użytkowników i per użytkownik.
46. Platforma powinna umożliwiać wykorzystanie materiałów Exatel w modelu white label dla klientów końcowych.

6. Wymagania bezpieczeństwa, prawne i zgodności

47. Dane i metadane przetwarzane przez platformę powinny być przechowywane na terenie UE/EOG. Wykonawca powinien wskazać, czy możliwe jest ograniczenie lokalizacji danych wyłącznie do Polski na potrzeby projektów administracji publicznej.
48. Wykonawca powinien szczegółowo opisać, jakie dane są zbierane podczas kampanii phishingowych, w tym jakie informacje są rejestrowane po stronie wiadomości, załączników i stron docelowych.
49. Wykonawca powinien wskazać, czy platforma rejestruje dane wpisywane przez użytkowników na stronach docelowych, a jeśli tak – w jakim zakresie i w jakiej formie są one maskowane, anonimizowane lub pseudonimizowane.
50. Platforma powinna mieć możliwość utrwalania pełnych haseł oraz innych danych uwierzytelniających wpisywanych przez użytkowników w ramach kampanii testowych;
51. Platforma powinna umożliwiać maskowanie lub anonimizację wprowadzanych danych przez użytkownika.

52. Zamawiający oczekuje mechanizmów zabezpieczających strony docelowe przed automatycznym ruchem botów, np. przy użyciu CAPTCHA albo mechanizmów równoważnych.
53. Wykonawca powinien opisać model prawny i organizacyjny wykorzystywania elementów graficznych, nazw handlowych i motywów kampanii nawiązujących do rozpoznawalnych marek, wraz ze wskazaniem ograniczeń i odpowiedzialności stron.
54. Wykonawca powinien wskazać mechanizmy ochrony dostępu administracyjnego do platformy, w tym role i uprawnienia, logowanie zdarzeń administracyjnych oraz sposób separacji tenantów.
55. Wykonawca powinien opisać model przetwarzania danych osobowych, rolę stron w rozumieniu RODO, stosowanie podwykonawców i subprocesorów, okresy retencji danych oraz proces usuwania danych po zakończeniu usługi.
56. Wykonawca powinien wskazać posiadane certyfikacje bezpieczeństwa, standardy organizacyjne oraz mechanizmy ciągłości działania i odtwarzania po awarii.

7. Wymagania handlowe, licencyjne i operacyjne

57. Oferta powinna jednoznacznie rozdzielać część edukacyjną od części phishingowej na poziomie funkcji i licencjonowania.
58. Wykonawca powinien wskazać, czy dana funkcja jest dostępna standardowo, konfiguracyjnie czy wymaga prac dodatkowych.
59. Wykonawca powinien wskazać, które elementy są objęte ceną podstawową, a które wymagają dodatkowej licencji, modułu lub usługi profesjonalnej.
60. Wykonawca powinien opisać sposób wdrożenia nowego klienta, czas uruchomienia tenantu, zakres onboardingu oraz szkolenie administratorów Exatel.
61. Wykonawca powinien przedstawić model wsparcia, czasy reakcji, dostępność platformy, okna serwisowe oraz sposób obsługi zgłoszeń.
62. Wykonawca powinien opisać możliwości brandingu w modelu white label, w tym co najmniej: logo, kolorystykę, nazwę platformy, domenę URL, szablony raportów, nadawcę kampanii oraz stopki wiadomości.

8. Potrzeby wewnętrzne Exatel

63. Oferta powinna zawierać odrębną pozycję cenową dla wykorzystania platformy na potrzeby wewnętrzne Exatel dla 500 pracowników.
64. W ramach tej pozycji wykonawca powinien wskazać zakres funkcji, model licencjonowania, limity oraz ewentualne ograniczenia względem wariantu usługowego dla klientów końcowych.

9. Wymagania opcjonalne

65. Wykonawca może przedstawić opcjonalną ofertę rozszerzenia platformy o kampanie socjotechniczne realizowane z użyciem kanałów takich jak smishing.
66. Wykonawca może przedstawić opcjonalną ofertę rozszerzenia platformy o kampanie vishingowe, w tym z wykorzystaniem mechanizmów AI, wraz z opisem ograniczeń prawnych, technicznych i organizacyjnych.

10. Oczekiwany zakres odpowiedzi wykonawcy

Odpowiedź wykonawcy powinna zawierać co najmniej następujące elementy:

- opis rozwiązania i architektury platformy,
- wypełnioną matrycę wymagań z oznaczeniem: spełnia / częściowo spełnia / nie spełnia / wymaga dodatkowych prac,
- opis ograniczeń funkcjonalnych i technicznych,
- opis modelu licencjonowania i wyceny,
- opis lokalizacji przetwarzania danych i modelu bezpieczeństwa,

- opis wdrożenia, utrzymania i wsparcia,
- opis zakresu white label i modelu multi-tenant oraz Ofertę (cena za użytkownika w okresie miesięcznym / rocznym) dla Klinetów Exatel w następujących wariantach

    - *Wariant wyceny dla ilości użytkowników: 1-50;*
    - *Wariant wyceny dla ilości użytkowników: 51-100;*
    - *Wariant wyceny dla ilości użytkowników: 101-250;*
    - *Wariant wyceny dla ilości użytkowników: 251 - 500;*
    - *Wariant wyceny dla ilości użytkowników: 501 – 1000;*
    - *Wariant wyceny dla ilości użytkowników: powyżej 1000;*

- osobną wycenę dla wariantu wewnętrznego Exatel – 500 użytkowników.

Zalecany sposób udzielenia odpowiedzi

- dla każdego wymagania wskazać status realizacji,
- opisać, czy funkcja wymaga osobnego modułu lub licencji,
- wskazać ewentualne ograniczenia lub warunki brzegowe,
- potwierdzić, czy funkcja dostępna jest w języku polskim.

11. Proponowany sposób oceny odpowiedzi

Na potrzeby wewnętrznej analizy porównawczej Zamawiający rekomenduje ocenę ofert z uwzględnieniem poniższych obszarów:

Obszar oceny	Zakres oceny
Dopasowanie funkcjonalne	Zgodność z wymaganiami części phishingowej i edukacyjnej, elastyczność konfiguracji, jakość raportowania.
Model MSSP / multi-tenant	Obsługa wielu klientów, separacja tenantów, delegacja administracji, white label, skalowalność.
Bezpieczeństwo i zgodność	Lokalizacja danych, RODO, anonimizacja danych, kontrola dostępu, audyt działań administracyjnych.
Model handlowy	Przejrzystość licencjonowania, możliwość rozdzielenia modułów, wariant wewnętrzny i usługowy.
Wdrożenie i utrzymanie	Czas aktywacji, onboarding, wsparcie techniczne, szkolenie administratorów, SLA.