OPIS PRZEDMIOTU DIALOGU

Załącznik nr 2 do Ogłoszenia o dialogu technicznym dotyczącym „ ” zwany dalej „Rozwiązaniem”.

**I WPROWADZENIE: Czym jest wyzwanie, dlaczego jest takie ważne dla organizacji i obywateli?**

Rozwój przestępstw z wykorzystaniem współczesnych narzędzi informatycznych w tym zasobów infrastruktury informatycznej stanowi aktualne wyzwanie cywilizacyjne. Istniejące rozwiązania bezpieczeństwa w znacznej mierze opierają się na regułach korelacyjnych, to znaczy na próbie zidentyfikowania wszystkich możliwych podejrzanych zachowań i w przypadku wystąpienia któregokolwiek z nich poinformowanie pracowników odpowiedzialnych za bezpieczeństwo o potencjalnym incydencie bezpieczeństwa. Wspomniane rozwiązanie posiada kilka niedoskonałości:

1. Nie jesteśmy w stanie przewidzieć i opisać wszystkich podejrzanych zachowań, a co za tym idzie jest kwestią czasu i zaangażowania atakującego, kiedy opracuje on atak, którego my nie przewidzieliśmy i dostanie się do organizacji.
2. Generowanie informacji o potencjalnym incydencie bezpieczeństwa w przypadku każdej anomalii w sieci, powoduje, że specjaliści od cyberbezpieczeństwa zmuszeni są do reagowania na tysiące alarmów, które po przeprowadzeniu dochodzenia okazują się być praktycznie zawsze fałszywe. W efekcie czujność specjalistów ds. cyberbezpieczeństwa spada a co za tym idzie zwiększa się ryzyko przeoczenia prawdziwego incydentu. Dodatkowo każdy potencjalny incydent musi zostać obsłużony a co za tym idzie zwiększa to zapotrzebowanie na potencjał ludzki – etaty.
3. W celu wykrycia podejrzanego zachowania w sieci organizacji konieczne jest monitorowanie i zrozumienie całej infrastruktury i specyfiki systemów, aplikacji oraz pracy użytkowników. W efekcie angażuje to olbrzymie zasoby ludzkie. Dodatkowo w przypadku niejednorodnej struktury która występuję w większości instytucji (np. inną specyfiką sieci charakteryzuje się Ministerstwo Sprawiedliwości a inną każda apelacja) utworzenie centralnego monitoringu incydentów jest niezmiernie trudne.

Bazując na doświadczeniach eksperckich można stwierdzić, że choć nie jesteśmy w stanie przewidzieć wszystkich możliwych sposobów dostania się do organizacji to możemy przewidzieć, że po dostaniu się do niej atakujący zawsze wykonuje te same działanie tj. poszukuje cennych danych. Bazując na tym można wytworzyć system komplementarny do tradycyjnego systemu SIEM (reguł korelacyjnych) bazujących na sieci pułapek wewnątrz organizacji. Pułapki umieszczone w systemie emulują cenne dla włamywacza zasoby (np.: otwarte porty SMB, FTP, hasła, loginy , podatne systemy, stacje końcowe, itd.) do których nie powinien być generowany żaden ruch. Wiedząc, na czym zależy włamywaczom, można stworzyć aktywny system bezpieczeństwa, który wykrywa włamywaczy lub złośliwe oprogramowanie oraz umożliwia zarówno błyskawiczne zareagowanie na ich obecność poprzez odcięcie zarażonych stacji jak i przeniesienie ich do w pełni emulowanego środowiska w celu badania ich zachowania i odkrycia sposobu w jaki dostali się do organizacji.

**II WIZJA: Jaki jest oczekiwany długoterminowy rezultat? Co zostanie wdrożone? Co to zmieni?**

Stworzenie inteligentnego rozwiązania do dezinformacji, które przyciąga i dezorientuje potencjalnych włamywaczy lub złośliwe oprogramowanie z jednoczesną możliwością szybkiej analizy nowych technik ataku i wzmocnieniu skutecznej ochrony. Potencjalne korzyści, jakie niesie wdrożenie opisywanego systemu w danej organizacji to:

1. Zwiększenie bezpieczeństwa sieci poprzez tworzenie warstwy dezinformacji znajdującej się wewnątrz cyberprzestrzeni chronionej organizacji;
2. Opracowanie algorytmu sztucznej inteligencji generującego automatycznie systemy-pułapki o charakterystyce dopasowanej do infrastruktury, w której działa, dzięki czemu są one dla atakującego bardzo trudne do rozróżnienia od systemów produkcyjnych. Jednocześnie wytworzone pułapki rozróżniają oczekiwany i niezbędny ruch dla/z danej infrastruktury od każdej innej ingerencji, co zmniejsza potrzebny nakład pracy analityków;
3. Wytworzenie centralnego systemu zarządzania pułapkami trudnego do wykrycia przez cyberprzestępców oraz inteligentne generowanie alertów i prosta integracja z dowolnymi systemami bezpieczeństwa. Wytworzenie różnych grup pułapek i różnych polityk dla w nich w zależności od typu infrastruktury w której się znajdują - dzięki czemu nie jest generowany istotny narzut dla administratorów rozwiązania;
4. Skierowanie ataku do fałszywej infrastruktury poprzez pułapki instalowane na prawdziwych systemach operacyjnych przyciągające atakujących do systemów-pułapek, odwracając tym samym ich uwagę od krytycznych zasobów w sieci i ułatwiając wykrycie trwającego ataku;
5. Automatyczne śledzenie, wykrywanie włamywaczy i złośliwego oprogramowania w sieciach;
6. Poprawa efektywności i wydajności pracy analityków bezpieczeństwa, redukcję liczby fałszywych alarmów poprzez dostarczenie rozbudowanych informacji o trwającym ataku na system-pułapkę, redukując tym samym prawdopodobieństwo wystąpienia tzw. false-positive;
7. Łatwe i szybkie wdrażanie rozwiązania w środowisku rzeczywistym bez konieczności wprowadzania istotnych zmian w środowisku IT, dzięki czemu nie jest generowany istotny narzut dla administratorów rozwiązania;
8. Inteligentna i adaptacyjna ochrona wykorzystująca dezinformacje, mapowanie łańcuchów ataku (kill chains) w celu wzmocnienia zabezpieczeń – podnoszenie świadomości sytuacyjnej, zwiększanie wiedzy administratorów bezpieczeństwa o aktualnych metodach działania cyberprzestępców.

**III ROZWIĄZANIE: Jakie oczekiwania wobec Rozwiązania definiuje Zamawiający?**

 Optymalne rozwiązanie to inteligentny system do dezinformacji potencjalnych przestępców, który składa się z pakietu oprogramowania sieciowego które symuluje działanie rzeczywistych elementów infrastruktury sieciowej w sieci wewnętrznej i pozwala na pełną analizę ruchu wychodzącego i wchodzącego do tych elementów.

Kluczowe funkcje systemu

* Inteligentne tworzenie symulowanych maszyn sieciowych.
* Monitorowanie ruchu sieciowego symulowanych maszyn
* Alarmowanie o wykryciu podejrzanego ruchu sieciowego.
* Sterowanie i konfiguracja poprzez aplikację webową
* Integracja z systemami klasy SIEM
* Możliwość modyfikacji wzorców maszyn sieciowych
* Możliwość definicji własnych wzorców maszyn sieciowych

Dodatkowe funkcje systemu

* Prowadzenie statystyk rejestrowanego ruchu sieciowego
* Parametryzacja sterowanych maszyn
* Parametryzacja sposobu tworzenia symulowanych maszyn sieciowych
* Dwupoziomowy system uprawnień użytkowników(administrator i użytkownik standardowy).

**IV Użytkownicy rozwiązania**

Użytkownikami rozwiązania będą:

* Wszystkie firmy i instytucje, którym zależy na skutecznym wykrywaniu i ochronie systemów oraz informacji w nich przetwarzanych

Najważniejsze elementy rozwiązania (wartości dla użytkowników) to:

* Rezultaty projektu mogą spowodować wzrost efektywności i skuteczności wykrywania potencjalnych przestępstw w systemach teleinformatycznych dzięki przyśpieszeniu procesu rozwiązania problemu u źródła jakim jest eliminacja fałszywych alarmów redukując ryzyko przeoczenia tych naprawdę ważnych. Podejście to jest szczególnie ważne biorąc pod uwagę charakter grup przestępczych oraz czas poświęcony na analizę zdarzeń niepożądanych w systemach teleinformatycznych.
* Dzięki wysokiej automatyzacji funkcjonowania rozwiązania opartego o algorytmy sztucznej inteligencji może nastąpić znaczne skrócenie czasu wykrycia oraz ilości czasu koniecznego na analizę i obsługę niepożądanych działań odciążając zespoły bezpieczeństwa oraz poprawiając ich skuteczność.
* Wabienie potencjalnych atakujących do systemów-pułapek odciąga ich uwagę od krytycznych systemów i aplikacji oraz spowalnia ich działania, dając czas na wykrycie, analizę i przeciwdziałanie. Dodatkowo zapewniając wgląd w informacje i dane śledcze umożliwiające poznanie taktyk, technik a także poszukiwanych przez atakującego zasobów.
* Dzięki zastosowaniu systemów emulowanych, rozwiązanie umożliwiać będzie bardzo wysoką skalowalność, umożliwi automatycznie dostosowuje do zmian w rzeczywistej infrastrukturze oraz nie będzie powodować negatywnego wpływu na działalność operacyjną ani na przetwarzane prawdziwe dane.
* Niski koszt wdrożenia rozwiązania i utrzymania rozwiązania, minimalny wpływ na zmiany w konfiguracji istniejących środowisk IT oraz szybki czas wdrożenia i dostosowania do specyfiki danego środowiska IT.

**V Mierniki skuteczności wdrożenia**

* Zwiększenie wykrywalności potencjalnych przestępców
* Mniejsza ilość fałszywych alarmów bezpieczeństwa generowanych dla analityków
* Łatwe i tanie wdrożenie systemu do wewnętrznej sieci

Rozważany jest wybór najlepszego Rozwiązania w dwóch etapach. Pierwszy pozwalający szybko ocenić i wybrać 5 najlepiej rokujących propozycji i drugi, prowadzący do wyboru najlepszego wykonawcy/najlepszej pracy konkursowej.

**VI Kryteria I Etapu**:

Pierwszy etap składa się z prezentacji proponowanych rozwiązań, w której powinny zostać zawarte informacje na temat:

* Idei logicznej rozwiązania
* Użytych technologii
* Możliwości rozwojowych danego rozwiązania
* Koszty utrzymania platformy

Ocenie podlega:

* Pomysł na wykonanie rozwiązania
	+ Architektura systemu
	+ Zastosowane rozwiązania techniczne
	+ Sposób tworzenia inteligentnych pułapek
	+ Koszty utrzymaniowe
* Możliwości:
	+ Ilość rodzajów tworzonych pułapek
	+ Możliwości aktualizacji bazy pułapek
	+ Możliwości rozwojowe projektu

**Dane w I Etapie:**

Nie dotyczy

**VII Kryteria II Etapu:**

 Drugi etap konkursu składa się z ewaluacji wyłonionych w 1 etapie rozwiązań na testowej sieci wewnątrz organizacji. Testy będą składać się z symulowanych ataków wewnątrz sieciowych i sprawdzeniu jak ewaluowany system zareaguje na:

* Skanowanie sieci przez atakującego
* Próby nawiązania kontaktu przez atakującego

Dodatkowo system będzie testowany pod kątem łatwości obsługi, integracji z systemami klasy SIEM, możliwością edycji tworzonych pułapek, sposobu tworzenia możliwych pułapek.

Ocenie podlega:

* Wykrywalność zagrożeń przez dany system
* Reakcje systemu na kontakt z atakującym
* Sposób tworzenia pułapek
* Intuicyjność i wygoda obsługi
* Koszt wdrożenia

**Dane w II Etapie:**

Nie dotyczy

**Estymowany budżet przeznaczony na całe postępowanie/konkurs:** ...

**Estymowany czas wdrożenia:** ...

**VIII Przykładowe pytania jakie zadane zostaną w trakcie konsultacji:**

1. Jakie rozwiązania są Państwu znane, które mogą mieć zastosowanie do realizacji Rozwiązania? Czym się wyróżniają, jakie są ich silne i słabe strony?
2. Jaki byłby estymowany koszt wykonania takiego Rozwiązania? Możliwe jest podanie w formie widełek.
	1. Jaki byłby estymowany koszt wykonania wymaganych funkcjonalności bez uzupełniających?
3. Jakie informacje, które mógłby przekazać Zamawiający, pozwoliłyby precyzyjniej określić wycenę?
4. Jak estymują Państwo czas wykonania przedmiotu zamówienia (w miesiącach)? możliwe jest podanie w widełkach.
5. Załóżmy przez moment, że to Państwo prowadzą takie postępowanie dla swojej firmy i planują wybrać wykonawcę. Przy założeniu, że chcą Państwo zweryfikować umiejętność tworzenia najtrudniejszej części dla tego zamówienia – jakie zadanie, by Państwo postawili przed potencjalnymi wykonawcami? Jakie dane udostępnili? Jakimi kryteriami się kierowali?
6. Czy widzą Państwo jakieś zagrożenia wynikające z aktualnie sformułowanych kryteriów?
7. Jak estymują Państwo poziom potrzebnego zaangażowania (czasowy, zasobowy) w przygotowanie rozwiązania na I etap?
8. Jak estymują Państwo poziom potrzebnego zaangażowania w przygotowanie rozwiązania na II etap?
9. Co jest najtrudniejszym elementem proponowanego rozwiązania? Wymagającym największego zaangażowania w wytworzenie/przygotowanie?