

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

UMOWA NR 2023

zawarta w dniu 2023r. we Wschowie
pomiędzy Gminą Wschowa
zwaną dalej ZAMAWIAJĄCYM,
reprezentowaną przez:
Zastępcę Burmistrza Miasta i Gminy - Marka Kraśnego
przy kontrasygnacie
Skarbnika Gminy – Justyny Staszak

a

.....
.....,

zwanym dalej WYKONAWCĄ reprezentowanym przez:

.....

§1. Przedmiot umowy

1. Przedmiotem umowy jest **Zakup oraz dostawa urządzenia do ochrony infrastruktury typu NDR, Hillstone I-1870 BDS (server breach detection system)**

2. Zakres przedmiotu umowy, o którym mowa w ust. 1 obejmuje:

Urządzenie sBDS – 1 sztuka.

Nazwa producenta:

Typ produktu, model:

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

Parametr	Charakterystyka
	<ul style="list-style-type: none"> • Wysokość 1U do montażu w szafie rack. • Posiadać co najmniej dwa porty USB • Urządzenie musi posiadać minimum interfejsów: 8x GE, 8x SFP, 2x SFP+ • Urządzenie musi posiadać minimum jeden dedykowany port GE do zarządzania • Musi obsługiwać co najmniej 1T przestrzeni dyskowej. • Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń • Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji. • Proponowane rozwiązanie musi obsługiwać 32 000 nowych sesji /s w ruchu HTTP.
Usługi sieciowe	<ul style="list-style-type: none"> • Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta. • Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń • Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS oraz VXLAN i wykrywania zagrożeń w tych wiadomościach.
Kontrola aplikacji	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediiów itp. • Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android. • Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
Wykrywanie zagrożeń	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń. • Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

	<ul style="list-style-type: none"> • Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA • Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp. • Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku. • Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS. • Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS. • Rozwiązanie musi mieć opcję przechwytywania pakietów • System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
Skanowanie antywirusowe:	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur. • Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP. • Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach • Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
Wykrywanie botnetów C&C:	<ul style="list-style-type: none"> • Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C. • Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C • Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen. • Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

	<ul style="list-style-type: none"> Rozwiązanie musi wspierać włączenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA. Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
Sandbox w chmurze	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanymi zagrożeń Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR, SWF oraz skrypty Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików. Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznanymi zagrożenie.
Wykrywanie spamu	<ul style="list-style-type: none"> Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości. Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3 Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
Dodatkowe funkcje ochrony:	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp. Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
Inteligentne funkcje bezpieczeństwa:	<ul style="list-style-type: none"> Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

	<ul style="list-style-type: none">• Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.• Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanymi rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp• Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania• Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.• Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów.• Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS• Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanymi aplikacji• Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym• Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.• Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia• Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta• Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.• Rozwiązanie musi obsługiwać przechwytywanie pakietów online• Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania
--	---

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych • Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę • Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekho, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalności funkcji śledzenia zagrożeń.
Widoczność ryzyka/zagrożeń:	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego. • Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch. • Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu. • Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp. • Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni. • Rozwiązanie musi wspierać wskazanie ścieżki ataku.
Analiza i odpowiedzi na incydenty	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury • Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach. • Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie. • Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania. • Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpowiedź w odpowiednim czasie zgodnie z metodą działania określoną w

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

	<p>regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.</p>
Administracja:	<ul style="list-style-type: none"> • Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI) • Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli • Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło • Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów. • Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych • Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny • Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
Logowanie i raportowanie:	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP. • Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp. • Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS. • Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń. • Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje • Wstępnie zdefiniowane zadania raportowania • Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni. • Rozwiązanie musi wspierać restAPI
Gwarancja/dostawa:	<p>Dostawa musi zawierać również:</p> <ul style="list-style-type: none"> • 12-miesięczną gwarancję producenta na dostarczone elementy systemu

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

	<ul style="list-style-type: none">• Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 12 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)• Wsparcie techniczne dystrybutora rozwiązań w języku polskim
--	---

§2

Termin realizacji

WYKONAWCA zobowiązuje się wykonać przedmiot zamówienia określony w §1, w terminie do **21 dni od podpisania umowy**.

§3

Wartość przedmiotu umowy

1. WYKONAWCY za wykonanie czynności określonych §1 niniejszej umowy przysługuje **wynagrodzenie** w wysokości **zł netto** (słownie:) co stanowi łącznie **kwotę brutto** w wysokości: **zł** (słownie złotych:).
2. Wynagrodzenie, o którym mowa w pkt.1 obejmuje wszelkie koszty i czynności WYKONAWCY i jest niezmiennie do zakończenia realizacji umowy.

§4

Zapłata wynagrodzenia

1. Wynagrodzenie za czynności określone w §1 płatne będzie po wykonaniu całego zakresu umowy określonego w §1 w terminie do 21 dni, po przedstawieniu faktury ZAMAWIAJĄCEMU.
2. Wynagrodzenie, o którym mowa w §3 ust.1 zostanie przekazane na rachunek bankowy WYKONAWCY
Nr

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

3. W przypadku zwłoki w zapłacie faktury WYKONAWCA może żądać od ZAMAWIAJĄCEGO zapłaty odsetek ustawowych.

§5

Nadzór nad wykonawstwem

1. Strony zobowiązane są, każda w swoim zakresie, do współdziałania przy wykonywaniu niniejszej umowy.
2. Koordynatorem warunków umownych ze strony ZAMAWIAJĄCEGO są pracownicy Referatu Informatycznego: Krystian Raburski i Aleksander Trzcński.

§6

Kary umowne

1. WYKONAWCA zobowiązuje się zapłacić ZAMAWIAJĄCEMU następujące kary umowne:
 - a) w przypadku nienależytego wykonania obowiązków umownych, bądź niewykonania tych obowiązków w ogóle, WYKONAWCA zobowiązuje się zapłacić ZAMAWIAJĄCEMU karę umowną w wysokości 30% wynagrodzenia brutto określonego w §3 ust. 1 niniejszej umowy,
 - b) za odstąpienie od umowy lub jej wypowiedzenie wskutek okoliczności, za które odpowiada WYKONAWCA - w wysokości 30% wynagrodzenia brutto określonego w §3 ust. 1 niniejszej umowy,
 - c) za opóźnienie w wykonaniu przedmiotu umowy, o którym mowa w §1 umowy w wysokości 0,5% wynagrodzenia brutto określonego w §3 ust. 1 niniejszej umowy, za każdy dzień opóźnienia,
2. Jeżeli kara umowna nie pokrywa poniesionej szkody, strony mogą dochodzić odszkodowania uzupełniającego.
3. ZAMAWIAJĄCY zastrzega sobie prawo potrącenia naliczonych kar umownych z faktury wystawionej przez WYKONAWCĘ, a WYKONAWCA niniejszym wyraża zgodę na takie potrącenia.

§7

Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Załącznik Nr 3 do Zapytania ofertowego nr 4/2023

Zmiana umowy

Zmiana niniejszej umowy wymaga formy pisemnej pod rygorem nieważności.

§8

Sprawy sporne

1. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu Cywilnego.
2. Spory między stronami mogące wyniknąć z realizacji umowy rozstrzygać będzie Sąd właściwy miejscowo dla ZAMAWIAJĄCEGO.

§9

Umowę niniejszą sporządzono w dwóch jednobrzmiących egzemplarzach, dwa dla ZAMAWIAJĄCEGO jeden dla WYKONAWCY.

ZAMAWIAJĄCY:

WYKONAWCA: