Załącznik nr II do Zapytania ofertowego nr 6/2022

Specyfikacja wymagań na stanowisko badawcze								
Nr	Nazwa stanowiska badawczego	Kryteria obligatoryjne dopuszczające			Planowany zakres obowiązków w projekcie	Maksymalny okres realizacji prac	Liczba osób do zaangażowania w projekcie	Łączny szacowany wymiar świadczenia usług na osobę w rbg
		Wymagane wykształcenie	Wymagane doświadczenie zawodowej	Wymagane umiejętności merytoryczne				
1	Analityk bezpieczeństwa IT	Wyższe lub w trakcie studiów	Minimum roczne doświadczenie w technologiach informatycznych	1) Dobra znajomość modelu TCP/IP, działania sieci LAN i technologii sieciowych; 2) Dobra znajomość protokołów: HTTP, SSH, DHCP, DNS, CIFS i NFS itp.; 3) Doświadczenie w pracy w środowiskach złożonych z systemów Linux, Windows oraz znajomość konfiguracji monitorowania i stosowanych w tych systemach rozwiązań bezpieczeństwa; 4) Wiedza z zakresu działania rozwiązań klasy SIEM oraz doświadczenie w działaniach związanych z monitoringiem bezpieczeństwa infrastruktury sieciowej i analizą logów; 5) Praktyczna znajomość języka Splunk SPL, budowania zapytań i reguł korelacyjnych monitorujących poziom bezpieczeństwa IT; 6) Znajomość przynajmniej jednego z języków programowania: Python, Bash, JavaScript oraz umiejętność pisania skryptów ułatwiających pracę z logami i automatyzujących codzienną pracę; 7) Znajomość zasad działania systemów i technologii bezpieczeństwa m.in.: Firewall, IPS/IDS, VPN, WAF, DLP; 8) Specjalistyczna wiedza z zakresu bezpieczeństwa IT w jednej z dziedzin: systemy operacyjne Windows / Linux, sieci, bazy danych, systemy SCADA; 9) Wiedza dotycząca najważniejszych rodzajów cyberzagrożeń, w tym wektorów ataków i technik stosowanych przez cyberprzestępców oraz metod obrony przed nimi; 10) Znajomość języka angielskiego, co najmniej na poziomie zapewniającym swobodne czytanie dokumentacji technicznej.	a) Weryfikacja przyjętych wymagań oraz udział w opracowaniu koncepcji funkcjonalnej prototypu systemu DAPT. b) Analiza właściwości funkcjonalnych prototypu na kolejnych poziomach gotowości technologicznej. c) Analiza otrzymanych wyników badań pod względem oceny ich implementacji w prototypie systemu DAPT. d) Realizacja prac w zakresie badania stosowalności narzędzi analitycznych do identyfikacji zagrożeń w zakresie bezpieczeństwa. e) Prace badawcze w zakresie analizy zagrożeń w sieci Internet, zbieranie danych oraz analiza potencjalnych zależności pomiędzy zdarzeniami. f) Prace badawcze w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów. g) Analiza wyników badań oraz doskonalenie założeń produktowych prototypu DAPT, w oparciu o wyniki badań oraz przeprowadzone analizy. h) Realizacja prac badawczych w zakresie opracowania koncepcji oraz udział w opracowaniu projektu architektury prototypu detektora do wykrywania, zapobiegania i reagowania na ataki APT. i) Współpraca z architektami, programistami oraz testerami w zakresie analizy otrzymywanych wyników prac badawczych i rozwojowych. j) Analiza właściwości funkcjonalnych technologii opracowanego rozwiązania, identyfikacja i ograniczanie ryzk. k) Formułowanie wyników przeprowadzonych prac w ramach opracowań badawczych.	05.2022 - 12.2022	1	400