Załącznik nr II do Zapytania ofertowego nr 11/2022

Specyfikacja wymagań na stanowisko badawcze								
Nr	Nazwa stanowiska badawczego	Kryteria obligatoryjne dopuszczające			Planowany zakres obowiązków w projekcie	Planowany przedział czasowy realizacji prac	Liczba osób do zaangażowania w projekcie	Łączny szacowany wymiar zlecenia na osobę w rbg
		Wymagane wysztalcenie	Wymagane doświadczenie zawodowe	Wymagane umiejętności merytoryczne				
1	Inżynier bezpieczeństwa teleinformatycznego	Wyższe lub w trakcie studiów	Minimum dwuletnie 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; 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; 11) Znajomość Cyber Kill Chain oraz MITRE ATT&CK Framework; 12) Doświadczenie we wdrażaniu lub wykorzystaniu narzędzi systemów z obszaru bezpieczeństwa IT.	a) Analiza właściwości funkcjonalnych prototypu na kolejnych poziomach gotowości technologicznej. b) Analiza otrzymanych wyników badań pod względem oceny ich implementacji w prototypie systemu APTD. c) Realizacja prac w zakresie badania stosowalności narzędzi do identyfikacji zagrożeń w zakresie bezpieczeństwa. d) Prace badawcze w zakresie analizy zagrożeń w sieci Internet, zbieranie danych oraz analiza potencjalnych zależności pomiędzy zdarzeniami. e) Prace badawcze w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów. f) Analiza wyników badań oraz doskonalenie założeń produktowych prototypu APTD, w oparciu o wyniki badań oraz przeprowadzone analizy. g) Realizacja prac badawczych w zakresie opracowania koncepcji i udział w opracowaniu projektu architektury prototypu detektora do wykrywania, zapobiegania i reagowania na ataki APT. h) Współpraca z architektami, analitykami, programistami oraz testerami w zakresie analizy otrzymywanych wyników prac badawczych i rozwojowych. i) Analiza właściwości funkcjonalnych technologii opracowanego rozwiązania. j) Formułowanie wyników przeprowadzonych prac w ramach opracowań badawczych.	01.2023-12.2023	1	1 920