

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 wykształcenie	Wymagane doświadczenie zawodowe	Wymagane umiejętności merytoryczne				
1	Analityk bezpieczeństwa IT	Wyższe lub w trakcie studiów	Minimum roczne doświadczenie w technologiach informatycznych	<p>1) Dobra znajomość modelu TCP/IP, działania sieci LAN i technologii sieciowych;</p> <p>2) Dobra znajomość protokołów: HTTP, SSH, DHCP, DNS, CIFS i NFS itp.;</p> <p>3) Doświadczenie w pracy w środowiskach złożonych z systemów Linux, Windows oraz znajomość konfiguracji monitorowania i stosowanych w tych systemach rozwiązań bezpieczeństwa;</p> <p>4) Wiedza z zakresu działania rozwiązań klasy SIEM oraz doświadczenie w działaniach związanych z monitoringiem bezpieczeństwa infrastruktury sieciowej i analizą logów;</p> <p>5) Praktyczna znajomość języka Splunk SPL, budowania zapytań i reguł korelacyjnych monitorujących poziom bezpieczeństwa IT;</p> <p>6) Znajomość przynajmniej jednego z języków programowania: Python, Bash, JavaScript oraz umiejętność pisanie skryptów ułatwiających pracę z logami i automatyzujących codzienną pracę;</p> <p>7) Znajomość zasad działania systemów i technologii bezpieczeństwa m.in.: Firewall, IPS/IDS, VPN, WAF, DLP;</p> <p>8) Specjalistyczna wiedza z zakresu bezpieczeństwa IT w jednej z dziedzin: systemy operacyjne Windows / Linux, sieci, bazy danych, systemy SCADA;</p> <p>9) Wiedza dotycząca najważniejszych rodzajów cyberzagrożeń, w tym wektorów ataków i technik stosowanych przez cyberprzestępców oraz metod obrony przed nimi;</p> <p>10) Znajomość języka angielskiego, co najmniej na poziomie zapewniającym swobodne czytanie dokumentacji technicznej.</p>	<p>a) Weryfikacja przyjętych wymagań oraz udział w opracowaniu koncepcji funkcjonalnej prototypu systemu DAPT.</p> <p>b) Analiza właściwości funkcjonalnych prototypu na kolejnych poziomach gotowości technologicznej.</p> <p>c) Analiza otrzymanych wyników badań pod względem oceny ich implementacji w prototypie systemu DAPT.</p> <p>d) Realizacja prac w zakresie badania stosowalności narzędzi analitycznych do identyfikacji zagrożeń w zakresie bezpieczeństwa.</p> <p>e) Prace badawcze w zakresie analizy zagrożeń w sieci Internet, zbieranie danych oraz analiza potencjalnych zależności pomiędzy zdarzeniami.</p> <p>f) Prace badawcze w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów.</p> <p>g) Analiza wyników badań oraz doskonalenie założeń produktowych prototypu DAPT, w oparciu o wyniki badań oraz przeprowadzone analizy.</p> <p>h) Realizacja prac badawczych w zakresie opracowania koncepcji oraz udział w opracowaniu projektu architektury prototypu detektora do wykrywania, zapobiegania i reagowania na ataki APT.</p> <p>i) Współpraca z architektami, programistami oraz testerami w zakresie analizy otrzymywanych wyników prac badawczych i rozwojowych.</p> <p>j) Analiza właściwości funkcjonalnych technologii opracowanego rozwiązania, identyfikacja i ograniczanie ryzyk.</p> <p>k) Formułowanie wyników przeprowadzonych prac w ramach opracowań badawczych.</p>	01.2023- 04.2023	1	200