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 świadczenia usług na osobę w rbg
		Wymagane wykształcenie	Wymagane doświadczenie zawodowej	Wymagane umiejętności merytoryczne				
1	Analityk ICS/OT typ 1	Wyższe	Minimum trzyletnie doświadczenie w obszarze bezpieczeństwa systemów automatyki przemysłowej	1) Doświadczenie w pracy w OT na stanowiskach związanych z bezpieczeństwem 2) Dobra znajomość modelu TCP/IP, działania sieci LAN i technologii sieciowych 3)) Znajomość procesów przemysłowych i ich automatyzacji 4) Znajomość protokołów komunikacyjnych wykorzystywanych w OT – np. OPC, IEC-104, Modbus, ICCP, Ethernet/IP, Siemens S7, DNP3, IEC-61850 5) Znajomość komponentów systemów ICS m.in: - Programmable logic controller (PLC), Human Machine Interface (HMI), Remote Terminal Units (RTU), Security Infrastructure Solutions (SIS), Supervisory Control And Data Acquisition (SCADA) 6) Wiedza w zakresie systemów operacyjnych Windows, Linux, Unix 7) Znajomość zagrożeń sieciowych oraz systemów i technologii bezpieczeństwa 8) Wiedza dotycząca najważniejszych rodzajów cyberzagrożeń, w tym wektorów ataków i mechanizmów funkcjonowania struktur cyberprzestępczych, szczególnie w obszarze OT 9) Wiedza w zakresie analizy danych, korelacji logów, scenariuszy ataków na systemy sterowania przemysłowego 10) Znajomość rozwiązań stosowanych do monitoringu bezpieczeństwa OT, analizy logów i korelacji zdarzeń 11) Znajomość języka angielskiego, co najmniej na poziomie zapewniającym swobodne czytanie dokumentacji technicznej Dodatkowymi atutami mogą być: 12) Znajomość Cyber Kill Chain oraz MITRE ATT&CK for ICS	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) Prowadzenie badań w zakresie bezpieczeństwa polskich zasobów Internetu. e) Realizacja prac w zakresie badania stosowalności narzędzi analitycznych do identyfikacji zagrożeń w zakresie bezpieczeństwa. 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) Współpraca z architektami, programistami oraz testerami w zakresie analizy otrzymywanych wyników prac badawczych i rozwojowych. i) Analiza właściwości funkcjonalnych technologii opracowanego rozwiązania, identyfikacja i ograniczanie ryzyk. j) Formułowanie wyników przeprowadzonych prac w ramach opracowań badawczych.	9.2021 - 12.2021	1	170