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	Wyższe	Minimum pięcioletnie 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 systemów klasy SIEM. 4) Znajomość procesów przemysłowych i ich automatyzacji. 5) Znajomość protokołów komunikacyjnych wykorzystywanych w OT – np. OPC, IEC-104, Modbus, ICCP, Ethernet/IP, Siemens S7, DNP3, IEC-61850. 6) 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). 7) Wiedza w zakresie systemów operacyjnych typu Windows, Linux, Unix. 8) Doświadczenie w działaniach operacyjnych związanych z monitoringiem bezpieczeństwa infrastruktury sieciowej. 9) Znajomość zagrożeń sieciowych oraz systemów i technologii bezpieczeństwa. 10) Wiedza dotycząca najważniejszych rodzajów cyberzagrożeń, w tym wektorów ataków i mechanizmów funkcjonowania struktur cyberprzestępczych, szczególnie w obszarze OT. 11) Wiedza w zakresie analizy danych, korelacji logów, scenariuszy ataków na systemy sterowania przemysłowego. 12) Znajomość systemów obsługi zgłoszeń i narzędzi do rejestracji wykonywanych działań. 13) Znajomość rozwiązań stosowanych do monitoringu bezpieczeństwa OT, analizy logów i korelacji zdarzeń. 14) Doświadczenie we wdrażaniu narzędzi systemów z obszaru bezpieczeństwa OT. 15) Posiadanie certyfikatów branżowych z obszaru systemów operacyjnych, sieci, bezpieczeństwa np. ISA99/IEC 62443 Cyber Security Certificate Program, Certified ICS/SCADA Security Architect (CSSA), SANS Global Industrial Cyber Security Professional. 16) Znajomość Cyber Kill Chain oraz MITRE ATT&CK for ICS. 17) 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) 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 zakresie analizy zagrożeń w sieci Internet, zbieranie danych oraz analiza potencjalnych zależności pomiędzy zdarzeniami. g) Prace badawcze w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów. h) Analiza wyników badań oraz doskonalenie założeń produktowych prototypu systemu DAPT, w oparciu o wyniki badań oraz przeprowadzone analizy. i) Realizacja prac badawczych w zakresie opracowania koncepcji i udział w opracowaniu projektu architektury prototypu detektora do wykrywania, zapobiegania i reagowania na ataki APT. j) Współpraca z architektami, programistami oraz testerami w zakresie analizy otrzymywanych wyników prac B+R. k) Analiza właściwości funkcjonalnych technologii opracowanego rozwiązania, identyfikacja i ograniczanie ryzyk. l) Formułowanie wyników przeprowadzonych prac analitycznych w ramach opracowań badawczych.	08.2021 - 12.2021	1	200