

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 wyształcenie	Wymagane doświadczenie zawodowej	Wymagane umiejętności merytoryczne				
1	Analityk ICS/OT typ 2	Wyższe	Minimum pięcioletnie doświadczenie w obszarze bezpieczeństwa systemów automatyki przemysłowej	<p>1) Doświadczenie w pracy w OT na stanowiskach związanych z bezpieczeństwem</p> <p>2) Dobra znajomość modelu TCP/IP, działania sieci LAN i technologii sieciowych</p> <p>3) Znajomość systemów klasy SIEM</p> <p>4) Znajomość procesów przemysłowych i ich automatyzacji</p> <p>5) Znajomość protokołów komunikacyjnych wykorzystywanych w OT – np. OPC, IEC-104, Modbus, ICCP, Ethernet/IP, Siemens S7, DNP3, IEC-61850</p> <p>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)</p> <p>7) Wiedza w zakresie systemów operacyjnych Windows, Linux, Unix</p> <p>8) Doświadczenie w działaniach operacyjnych związanych z monitoringiem bezpieczeństwa infrastruktury sieciowej</p> <p>9) Znajomość zagrożeń sieciowych oraz systemów i technologii bezpieczeństwa</p> <p>10) Wiedza dotycząca najważniejszych rodzajów cyberzagrożeń, w tym wektorów ataków i mechanizmów funkcjonowania struktur cyberprzestępczych, szczególnie w obszarze OT</p> <p>11) Wiedza w zakresie analizy danych, korelacji logów, scenariuszy ataków na systemy sterowania przemysłowego</p> <p>12) Znajomość systemów obsługi zgłoszeń i narzędzi do rejestracji wykonywanych działań</p> <p>13) Znajomość rozwiązań stosowanych do monitoringu bezpieczeństwa OT, analizy logów i korelacji zdarzeń</p> <p>14) Znajomość języka angielskiego, co najmniej na poziomie zapewniającym swobodne czytanie dokumentacji technicznej</p> <p>Dodatkowymi atutami mogą być:</p> <p>15) Doświadczenie we wdrażaniu narzędzi systemów z obszaru bezpieczeństwa OT</p> <p>16) Posiadanie certyfikatów branżowych z obszaru systemów operacyjnych, sieci, bezpieczeństwa</p> <p>17) Znajomość Cyber Kill Chain oraz MITRE ATT&amp;CK for ICS</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) Prowadzenie badań w zakresie bezpieczeństwa polskich zasobów Internetu.</p> <p>e) Realizacja prac w zakresie badania stosowności narzędzi analitycznych do identyfikacji zagrożeń w zakresie bezpieczeństwa.</p> <p>f) Prace badawcze w zakresie analizy zagrożeń w sieci Internet, zbieranie danych oraz analiza potencjalnych zależności pomiędzy zdarzeniami.</p> <p>g) Prace badawcze w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów.</p> <p>h) Analiza wyników badań oraz doskonalenie założeń produktowych prototypu DAPT, w oparciu o wyniki badań oraz przeprowadzone analizy.</p> <p>i) Realizacja prac badawczych w zakresie opracowania koncepcji i udział w opracowaniu projektu architektury prototypu detektora do wykrywania, zapobiegania i reagowania na ataki APT.</p> <p>j) Współpraca z architektami, programistami oraz testerami w zakresie analizy otrzymanych wyników prac badawczych i rozwojowych.</p> <p>k) Analiza właściwości funkcjonalnych technologii opracowanego rozwiązania, identyfikacja i ograniczenie ryzyk.</p> <p>l) Formułowanie wyników przeprowadzonych prac w ramach opracowań badawczych.</p>	09.2021 - 12.2021	1	80