Załącznik do rozporządzenia Ministra Edukacji
z dnia … 2026 r. (Dz. U. poz. …)

CHARAKTERYSTYKI EFEKTÓW UCZENIA SIĘ DLA POZIOMÓW SEKTOROWEJ RAMY KWALIFIKACJI W SEKTORZE CYBERBEZPIECZEŃSTWA UJĘTE W KATEGORIACH WIEDZY, UMIEJĘTNOŚCI ORAZ KOMPETENCJI SPOŁECZNYCH

WYZNACZNIK I: WSTĘPNE WYMAGANIA DLA CYBERBEZPIECZEŃSTWA							
NAZWA WIĄZKI		**POZIOM 3**	**POZIOM 4**	**POZIOM 5**	**POZIOM 6**	**POZIOM 7**	**POZIOM 8**
		ZNA I ROZUMIE	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WI1[1)]	**P4SCB_WI1[1)]**	**P5SCB_WI1[1)]**	**P6SCB_WI1[1)]**		
Dane	**WIEDZA**	rodzaje źródeł danych i ich wpływ na system; sposoby generowania danych i obiektów; zasady pobierania i pozyskiwania danych; powody i zasady ochrony danych; podstawowe atrybuty bezpieczeństwa	zasady i protokoły wymiany danych; zasady łączenia danych z granicami procesów realizowanych w ramach obiektów lub między nimi; możliwości narzędzi wykorzystywanych do przetwarzania danych; metody zabezpieczania danych przed uszkodzeniem i wyciekiem; uwarunkowania zewnętrzne potrzebne do przekazania danych	zasady modelu danych w systemach informatycznych; narzędzia do tworzenia i modyfikacji baz danych	model odniesienia IACS		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WI2[1)]	**P5SCB_WI2[1)]**	**P6SCB_WI2[1)]**		
Systemy komunikacji	**WIEDZA**		założenia komunikacji analogowej; założenia komunikacji cyfrowej	metody kompozycji i dekompozycji systemów komunikacji	zależności między komponentami w systemach komunikacji		

[1)] Kod składnika opisu

NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
			P4SCB_WI3[1)]	**P5SCB_WI3[1)]**	**P6SCB_WI3[1)]**		
Architektura komunikacji	**WIEDZA**		architekturę i strukturę sieci teleinformatycznych, w tym model odniesienia ISO/OSI	zasady eksploatacji sieci teleinformatycznych i zarządzania nimi	zasady zachowania zgodności w sieciach teleinformatycznych		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WI4[1)]	**P4SCB_WI4[1)]**	**P5SCB_WI4[1)]**	**P6SCB_WI4[1)]**		
Rodzaje środowisk cyfrowych	**WIEDZA**	rodzaje środowisk cyfrowych i złożonych systemów	metody przenoszenia danych między urządzeniami pracującymi w środowisku cyfrowym	założenia poszczególnych rodzajów środowisk cyfrowych	metody przenoszenia danych między różnymi niezależnymi środowiskami cyfrowymi		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WI5[1)]	**P4SCB_WI5[1)]**	**P5SCB_WI5[1)]**			
Systemy urządzeń elektronicznych	**WIEDZA**	elementy składające się na obszar IT; elementy składające się na obszar OT; elementy składające się na obszar IoT	specyficzne uwarunkowania obszaru IT; specyficzne uwarunkowania obszaru OT; specyficzne uwarunkowania obszaru IoT	zależności między IT, OT i IoT			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WI6[1)]	**P5SCB_WI6[1)]**	**P6SCB_WI6[1)]**	**P7SCB_WI6[1)]**	
Architektura systemów operacyjnych	**WIEDZA**		architekturę systemów operacyjnych, w tym sieciowych; zasady uruchomienia systemu operacyjnego, w tym sieciowego	metody wirtualizacji systemów operacyjnych	metody konteneryzacji aplikacji	metody orkiestracji kontenerów	

NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
		P3SCB_WI7[1)]	P4SCB_WI7[1)]	P5SCB_WI7[1)]	P6SCB_WI7[1)]	P7SCB_WI7[1)]	
Skrypty i aplikacje	WIEDZA	metody uruchomienia poszczególnych skryptów na wybranych systemach operacyjnych; przynajmniej jeden język skryptowy	podstawowe zasady programowania obiektowego; metody uruchomienia oprogramowania opartego na różnych językach skryptowych w jednym środowisku uruchomieniowym	możliwości wykorzystania gotowych bibliotek w projekcie; otoczenie programowe aplikacji, w tym możliwość integracji z narzędziami zewnętrznymi	wzorce projektowe; metody tworzenia aplikacji webowych; metody tworzenia aplikacji mobilnych; metody tworzenia aplikacji desktopowych; zasady zachowania ciągłości działania aplikacji	metody tworzenia innowacyjnych bibliotek programistycznych	
NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
		P3SCB_WI8[1)]	P4SCB_WI8[1)]	P5SCB_WI8[1)]			
Narzędzia wykorzystujące sztuczną inteligencję w systemach cyberbezpieczeństwa	WIEDZA	metody związane z wykorzystaniem sztucznej inteligencji	cechy systemów sztucznej inteligencji, zasady ich funkcjonowania i ograniczenia	grupy zastosowań sztucznej inteligencji w organizacji; grupy zastosowań sztucznej inteligencji w obszarze cyberbezpieczeństwa; formalne wymagania w zakresie systemów sztucznej inteligencji			
NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
		P3SCB_WI9[1)]	P4SCB_WI9[1)]	P5SCB_WI9[1)]	P6SCB_WI9[1)]	P7SCB_WI9[1)]	
Prawo, normy i standardy krajowe, unijne i międzynarodowe	WIEDZA	podstawowe zasady organizacji systemu cyberbezpieczeństwa	zasady, procedury i wymagania dotyczące bezpieczeństwa organizacji; obowiązki raportowania o incydentach dotyczących infrastruktury krytycznej	regulacje prawne określające wymagania dotyczące cyberbezpieczeństwa; krajowe normy dotyczące cyberbezpieczeństwa	międzynarodowe normy i standardy cyberbezpieczeństwa; międzynarodowe standardy audytu wewnętrznego;	zasady i procedury ochrony własności przemysłowej i prawa autorskiego	

					międzynarodowe standardy etyki zawodowej audytorów		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WI10[1)]	**P4SCB_WI10[1)]**	**P5SCB_WI10[1)]**			
Ochrona danych osobowych	**WIEDZA**	podstawowe zagadnienia dotyczące ochrony danych osobowych	zasady, procedury i wymagania ochrony danych osobowych; obowiązki raportowania o incydentach związanych z bezpieczeństwem danych osobowych	regulacje prawne dotyczące ochrony danych osobowych			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WI11[1)]	**P4SCB_WI11[1)]**	**P5SCB_WI11[1)]**	**P6SCB_WI11[1)]**	**P7SCB_WI11[1)]**	
Budowanie świadomości dotyczącej cyberbezpieczeństwa	**WIEDZA**	podstawowe terminy związane z cyberbezpieczeństwem; zasady cyberbezpieczeństwa obowiązujące na danym stanowisku pracy	zasady cyberbezpieczeństwa dla organizacji i społeczeństwa	metody i techniki zabezpieczania infrastruktury i usług; system certyfikacji w sektorze cyberbezpieczeństwa; rolę organizacji zajmujących się cyberbezpieczeństwem na poziomie krajowym	rolę organizacji zajmujących się cyberbezpieczeństwem na poziomie międzynarodowym	trendy w obszarze cyberbezpieczeństwa	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UI1[1)]	**P4SCB_UI1[1)]**	**P5SCB_UI1[1)]**	**P6SCB_UI1[1)]**		
Opracowanie specyfikacji zamówienia	**UMIEJĘTNOŚCI**	przeprowadzić rozeznanie rynku pod kątem pożądanych cech i parametrów	określić parametry i funkcjonalności do specyfikacji warunków zamówienia	określić warunki dostawy towarów i usług	przewidzieć ryzyka, jakie mogą wystąpić w trakcie realizacji umowy		

NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UI2[1)]	P4SCB_UI2[1)]	P5SCB_UI2[1)]	P6SCB_UI2[1)]	P7SCB_UI2[1)]	
Systemy monitorowania, kontroli, raportowania, wizualizacji i reakcji (SOC)	UMIEJĘTNOŚCI	weryfikować sytuacje pod kątem false positive (poziom 1 SOC)	wspierać utrzymanie ciągłości działania zarządzanego obiektu w przypadku wystąpienia anomalii (poziom 1 SOC)	analizować źródła danych, protokoły, procesy zasad działania obiektów i systemów (poziom 2 SOC); wykorzystać narzędzia do analizy stabilności działania, integralności systemów, korelacji zdarzeń i korelacji danych (poziom 2 SOC)	opracować głęboką analitykę danych oraz ich wzajemne relacje (poziom 2 SOC); budować komponenty rozszerzeń systemu bezpieczeństwa (poziom 2 SOC)	opracować systemowe rozwiązania przeciwdziałające wystąpieniu anomalii i ich konsekwencji (poziom 3 SOC)	
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UI3[1)]	P4SCB_UI3[1)]	P5SCB_UI3[1)]	P6SCB_UI3[1)]	P7SCB_UI3[1)]	
Przetwarzanie danych	UMIEJĘTNOŚCI	określać pochodzenie i miejsce docelowe danych; dobierać odpowiednie źródła danych zależnie od systemu; dokonywać selekcji danych oraz porządkować je; wizualizować dane	przetwarzać dane w systemach jednolitych; parować dane	monitorować rozproszone, nienadające się do zarządzania skrypty przetwarzania danych; weryfikować warunki przesyłania danych pod kątem ich bezpieczeństwa	opracować proste programy rozwiązujące problemy z przetwarzaniem danych; implementować dane z wielu miejsc	przetwarzać dane w rozproszonym środowisku	
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UI4[1)]	P4SCB_UI4[1)]	P5SCB_UI4[1)]	P6SCB_UI4[1)]	P7SCB_UI4[1)]	
Korelacja danych	UMIEJĘTNOŚCI	porównać próbkę informacji z określoną sygnaturą; budować informację opartą na pozyskanych danych	dokonać korelacji danych przy pomocy dostępnego oprogramowania	napisać korelator w wybranym języku programowania	opracować informacje i możliwe scenariusze na określonym obiekcie za pomocą matrycy korelacyjnej	zaprojektować model środowiska na podstawie przetwarzanych danych	

NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UI5[1)]	P4SCB_UI5[1)]	P5SCB_UI5[1)]	P6SCB_UI5[1)]	P7SCB_UI5[1)]	
Komunikacja i wymiana danych	UMIEJĘTNOŚCI	wyszukać informacje dotyczące komunikacji i wymiany danych; identyfikować komponenty w wymianie danych między obiektami; posługiwać się aplikacjami do komunikacji i wymiany danych	określić granice transmisji danych; klasyfikować zestaw danych według określonych kryteriów	analizować informacje dotyczące komunikacji i wymiany danych; zarządzać infrastrukturą komunikacyjną	projektować infrastrukturę komunikacyjną	projektować standardy wymiany danych	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
				P5SCB_UI6[1)]	P6SCB_UI6[1)]	P7SCB_UI6[1)]	P8SCB_UI6[1)]
Specjalistyczne słownictwo branżowe w językach polskim i angielskim	UMIEJĘTNOŚCI			komunikować się w zespole w języku angielskim; stosować specjalistyczne słownictwo w komunikacji w języku polskim; korzystać ze specjalistycznej literatury w języku polskim; wykorzystać specjalistyczną dokumentację systemów w języku polskim	stosować specjalistyczne słownictwo podczas komunikacji w języku angielskim; korzystać ze specjalistycznej literatury w języku angielskim	komunikować się w międzynarodowym środowisku biznesowym	komunikować się w międzynarodowym środowisku naukowym
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UI7[1)]	P5SCB_UI7[1)]	P6SCB_UI7[1)]	P7SCB_UI7[1)]	
Środowisko testowe, deweloperskie i produkcyjne	UMIEJĘTNOŚCI		przeprowadzać testy w środowisku testowym lub środowisku deweloperskim	projektować testy w środowisku testowym lub deweloperskim; przeprowadzić testy w środowisku produkcyjnym z możliwością zatrzymania obiektów testowania	przeprowadzić testy w środowisku produkcyjnym i w środowisku pracy ciągłej	projektować testy w środowisku produkcyjnym	
		POTRAFI	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**

NAZWA WIĄZKI				P5SCB_UI8[1)]	P6SCB_UI8[1)]	P7SCB_UI8[1)]	
Zarządzanie środowiskiem zwirtualizowanym	UMIEJĘTNOŚCI			stworzyć i zarządzać maszyną wirtualną; dobrać odpowiednie zastosowanie chmurowe; instalować i zarządzać oprogramowaniem hypervisor	konteneryzować aplikacje; rekomendować zabezpieczenia skonteneryzowanych aplikacji	orkiestrować kontener; tworzyć środowisko maszyn wirtualnych działających w trybie wysokiej dostępności (HA)	
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UI9[1)]	P4SCB_UI9[1)]	P5SCB_UI9[1)]	P6SCB_UI9[1)]		
Tworzenie skryptów i aplikacji	UMIEJĘTNOŚCI	tworzyć proste skrypty	tworzyć skrypty oparte na zewnętrznych bibliotekach	implementować wzorce projektowe w aplikacjach; wykorzystywać frameworki frontendowe	tworzyć aplikacje webowe; tworzyć aplikacje mobilne; tworzyć aplikacje desktopowe; łączyć poszczególne komponenty w celu stworzenia systemu		
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UI10[1)]	P4SCB_UI10[1)]	P5SCB_UI10[1)]	P6SCB_UI10[1)]		
Zarządzanie środowiskiem uruchomieniowym aplikacji	UMIEJĘTNOŚCI	sprawdzać zgodność systemów operacyjnych	identyfikować nieprawidłowości funkcjonowania systemów; zachowywać środki ostrożności niedopuszczające do destabilizacji systemów	reagować na błędy aplikacji występujące po aktualizacji systemów operacyjnych	analizować skutki aktualizacji środowiska uruchomieniowego na aplikację		
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
			P4SCB_UI11[1)]	P5SCB_UI11[1)]			
Rozwój własny	UMIEJĘTNOŚCI		wybrać własną ścieżkę rozwoju; korzystać z programów szkoleniowych w zakresie cyberbezpieczeństwa	wyszukiwać i korzystać ze szkoleń zewnętrznych z zakresu cyberbezpieczeństwa; wykorzystać różne źródła wiedzy, w tym źródła alternatywne;			

			realizowanych w swojej organizacji	pozyskiwać wiedzę na temat nowości sektorowych z różnych źródeł; rozwijać umiejętności z zakresu języka sektorowego, w tym w języku angielskim			
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UI12[1)]	**P5SCB_UI12[1)]**	**P6SCB_UI12[1)]**	**P7SCB_UI12[1)]**	**P8SCB_UI12[1)]**
Wspieranie rozwoju innych osób	**UMIEJĘTNOŚCI**		prowadzić szkolenia z zakresu cyberbezpieczeństwa; opracować szkolenia podstawowe z zakresu cyberbezpieczeństwa	monitorować poziom świadomości użytkowników w zakresie cyberbezpieczeństwa; diagnozować potrzeby szkoleniowe pracowników w obszarze cyberbezpieczeństwa; dzielić się wiedzą i doświadczeniem z innymi osobami; proponować modyfikację szkolenia z zakresu cyberbezpieczeństwa	definiować ścieżki rozwoju zawodowego pracowników; wdrażać system dzielenia się wiedzą i doświadczeniem w organizacji; zarządzać systemem dzielenia się wiedzą i doświadczeniem w organizacji; opracować szkolenia specjalistyczne z zakresu cyberbezpieczeństwa	przekazywać swoją wiedzę i doświadczenie w różnorodnych formach, w tym podczas spotkań sektorowych; projektować plan rozwoju pracowników; projektować system zarządzania kompetencjami pracowników	projektować programy szkoleniowe z cyberbezpieczeństwa dla organizacji
WYZNACZNIK II: IDENTYFIKACJA							
NAZWA WIĄZKI		**POZIOM 3**	**POZIOM 4**	**POZIOM 5**	**POZIOM 6**	**POZIOM 7**	**POZIOM 8**
		ZNA I ROZUMIE	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WII1[1)]	**P4SCB_WII1[1)]**	**P5SCB_WII1[1)]**	**P6SCB_WII1[1)]**	**P7SCB_WII1[1)]**	
Kontekst wewnętrzny i zewnętrzny organizacji	**WIEDZA**	terminy mikroekonomiczne i makroekonomiczne niezbędne do wykonywania zadań w organizacji	standardy biznesowe obowiązujące w organizacji; strukturę organizacyjną i główne procesy organizacji; zasady działania różnych typów podmiotów, w tym przedsiębiorstw, instytucji publicznych i organizacji pozarządowych	oczekiwania podmiotów zewnętrznych wobec usług i produktów organizacji	zasady tworzenia, wdrażania nowych procesów biznesowych; zasady optymalizacji wdrożonych procesów biznesowych	zasady, procesy i przedział czasowy tworzenia standardów biznesowych i regulacji prawnych, z uwzględnieniem kontekstu sektora lub organizacji	

NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
			P4SCB_WII2[1)]	P5SCB_WII2[1)]			
Łańcuch dostaw i wartości	WIEDZA		model łańcucha dostaw organizacji	model łańcucha wartości organizacji			
NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
		P3SCB_WII3[1)]	P4SCB_WII3[1)]	P5SCB_WII3[1)]	P6SCB_WII3[1)]	P7SCB_WII3[1)]	P8SCB_WII3[1)]
Ryzyka w organizacji	WIEDZA	potencjalne ryzyka dla organizacji, w tym źródła ryzyk; metody dokumentowania potencjalnych ryzyk w organizacji; znaczenie monitoringu ryzyk dla cyberbezpieczeństwa	metody i narzędzia służące do identyfikacji ryzyk w organizacji; potrzeby interesariuszy w zakresie monitoringu ryzyk	metody, narzędzia oraz rozwiązania organizacyjne stosowane w celu przeciwdziałania wystąpieniu ryzyk w organizacji	wpływ wystąpienia poszczególnych ryzyk na poziom zagrożenia w przedsiębiorstwie	kierunki rozwoju metod, narzędzi oraz rozwiązań organizacyjnych dotyczących przeciwdziałania wystąpieniu w organizacji ryzyk i ich minimalizacji	najnowsze rozwiązania w zakresie metod, narzędzi oraz rozwiązań organizacyjnych zabezpieczających przed potencjalnym ryzykiem w organizacji
NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
			P4SCB_WII4[1)]	P5SCB_WII4[1)]	P6SCB_WII4[1)]	P7SCB_WII4[1)]	
Wewnętrzne i zewnętrzne procesy, produkty i usługi w organizacji	WIEDZA		wymagania związane z cyberbezpieczeństwem w odniesieniu do procesów, produktów i usług w organizacji i poza nią oraz osób za nie odpowiedzialnych	podstawy i zasady stosowania analizy procesowej; procesy całego cyklu życia kupowanych oraz sprzedawanych produktów i usług z elementami cyfrowymi, w tym projektowania, rozwoju, instalacji, wdrożenia, utrzymania, uaktualniania, serwisu i wycofywania z użytkowania	zasady zarządzania zmianą i implementacji nowych sposobów organizacji pracy na poziomie zespołu lub działu	wpływ ograniczeń finansowych na wdrażanie rozwiązań spełniających wymagania cyberbezpieczeństwa; zasady zarządzania zmianą i implementacji nowych sposobów organizacji pracy na poziomie całej organizacji	
		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE

NAZWA WIĄZKI		P3SCB_WII5[1)]	P4SCB_WII5[1)]	P5SCB_WII5[1)]			
Aktywa w organizacji	WIEDZA	rodzaje aktywów w organizacji	rozwiązania stosowane w organizacji	potencjalne zależności między różnymi aktywami w organizacji istotne ze względu na cyberbezpieczeństwo; znaczenie aktywów finansowych, niematerialnych i prawnych; zasady działania baz CMDB lub innych baz zawierających informacje o użytkownikach i konfiguracjach systemów			
NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
			P4SCB_WII6[1)]	P5SCB_WII6[1)]	P6SCB_WII6[1)]	P7SCB_WII6[1)]	P8SCB_WII6[1)]
Zasady projektowania i konsekwencje wyboru technologii dla produktów i usług w ich cyklu życia	WIEDZA		rolę cyberbezpieczeństwa w projektowaniu produktów i usług z perspektywy ich cyklu życia	wymagania funkcjonalne i niefunkcjonalne odnoszące się do produktów i usług	konsekwencje dla cyberbezpieczeństwa w przypadku zastosowania określonych technologii i narzędzi w perspektywie cyklu życia produktów i usług	zasady integracji wymagań cyberbezpieczeństwa w tworzeniu nowych produktów i usług oraz cyklu ich życia	wymagania cyberbezpieczeństwa w procesie tworzenia i rozwoju technologii
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
			P4SCB_UII1[1)]	P5SCB_UII1[1)]	P6SCB_UII1[1)]	P7SCB_UII1[1)]	P8SCB_UII1[1)]
Identyfikacja komponentów, zdarzeń i obiektów	UMIEJĘTNOŚCI		dobierać narzędzia, procedury i procesy do identyfikacji znanych obiektów, w tym ich cech charakterystycznych oraz grup obiektów; wprowadzać korekty do wyników identyfikacji	profilować znane obiekty lub grupy obiektów; rozszerzać zapisy profilu o nowe cechy	dobierać narzędzia, procedury i procesy do identyfikacji nieznanych obiektów i grup obiektów; profilować systemy i środowiska fizyczne; wizualizować środowiskowo w układzie statycznym i dynamicznym	profilować nieznane obiekty lub grupy obiektów; profilować obiekty eteryczne; przeprowadzać identyfikację głęboką dla protokołów komunikacyjnych i stosów protokołów;	budować narzędzia identyfikacji systemów złożonych i ich powiązań między systemami

						budować narzędzia identyfikacji ze znanych rozwiązań	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UII2[1)]	**P4SCB_UII2[1)]**	**P5SCB_UII2[1)]**			
Usługi katalogowe	**UMIEJĘTNOŚCI**	wykorzystywać usługi katalogowe do identyfikacji aktywów organizacji	wykorzystywać usługi katalogowe do gromadzenia informacji o aktywach w organizacji	konfigurować usługi katalogowe, w tym określać zasady postępowania z obiektami			
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UII3[1)]	**P4SCB_UII3[1)]**	**P5SCB_UII3[1)]**	**P6SCB_UII3[1)]**	**P7SCB_UII3[1)]**	
Identyfikacja aktywów ludzkich organizacji	**UMIEJĘTNOŚCI**	identyfikować kluczowe osoby w poszczególnych procesach	określać rolę i odpowiedzialność osób w poszczególnych procesach, w tym osób kluczowych; określać wymagania, które powinni spełniać dostawcy i partnerzy zewnętrzni oraz pracownicy; określić rolę i zakresy odpowiedzialności osób odpowiedzialnych za cyberbezpieczeństwo, w tym role wynikające z przepisów prawa i dobrych praktyk	identyfikować krytyczne role osób w organizacji; identyfikować istotne powiązania między kluczowymi osobami	opracowywać wymagania cyberbezpieczeństwa, które muszą spełniać osoby kluczowe i pozostali pracownicy	oceniać i kształtować strukturę organizacyjną z perspektywy integracji oraz stosowania wymagań cyberbezpieczeństwa	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UII4[1)]	**P4SCB_UII4[1)]**	**P5SCB_UII4[1)]**	**P6SCB_UII4[1)]**		
Identyfikacja aktywów w postaci sprzętu i oprogramowania organizacji	**UMIEJĘTNOŚCI**	identyfikować sprzęt IT i OT oraz oprogramowanie	identyfikować zależności między systemami, sieciami, urządzeniami i oprogramowaniem	określać kluczowe dla cyberbezpieczeństwa zależności między systemami, sieciami, urządzeniami i oprogramowaniem	opracowywać wymagania cyberbezpieczeństwa odnośnie do systemów, sieci, urządzeń i oprogramowania		

NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UII5[1)]	P4SCB_UII5[1)]	P5SCB_UII5[1)]	P6SCB_UII5[1)]	P7SCB_UII5[1)]	
Identyfikacja aktywów procesowych organizacji	UMIEJĘTNOŚCI	identyfikować ścieżki przepływu informacji	identyfikować strukturę systemów informacyjnych; określać procesy krytyczne	identyfikować krytyczne procesy dla cyberbezpieczeństwa; identyfikować krytyczne zależności	opracowywać wymagania cyberbezpieczeństwa w odniesieniu do procesów krytycznych	wpisywać i integrować wymagania cyberbezpieczeństwa w plany operacyjne	
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
				P5SCB_UII6[1)]	P6SCB_UII6[1)]	P7SCB_UII6[1)]	P8SCB_UII6[1)]
Projektowanie produktów i usług	UMIEJĘTNOŚCI			definiować i integrować typowe wymagania funkcjonalne oraz niefunkcjonalne odnoszące się do produktów i usług	definiować i integrować złożone wymagania funkcjonalne oraz niefunkcjonalne odnoszące się do produktów i usług	definiować i integrować zróżnicowane i niejednorodne technologicznie wymagania funkcjonalne oraz niefunkcjonalne odnoszące się do produktów i usług	tworzyć i rozwijać narzędzia dla zabezpieczenia produktów i usług w ich cyklu życia; uwzględniać zasady cyberbezpieczeństwa w projektowaniu lub rozwijaniu produktów i usług
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
			P4SCB_UII7[1)]	P5SCB_UII7[1)]	P6SCB_UII7[1)]	P7SCB_UII7[1)]	P8SCB_UII7[1)]
Otoczenie społeczno- gospodarcze organizacji	UMIEJĘTNOŚCI		identyfikować wymagania prawne, dobre praktyki i standardy biznesowe mające wpływ na organizację; identyfikacja partnerów zewnętrznych; uzyskać wsparcie prawne w zakresie interpretacji przepisów związanych z cyberbezpieczeństwem w organizacji	wskazywać rozwiązania mające na celu spełnienie wymagań, w tym prawnych	identyfikować i określać zakres potrzeb współpracy, w tym z instytucjami, uczelniami i szkołami	identyfikować nowe koncepcje i technologie, w tym ich wpływ na cyberbezpieczeństwo organizacji	inicjować zmiany, w tym prawne, wpływające na cyberbezpieczeństwo organizacji

NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UII8[1)]	P4SCB_UII8[1)]	P5SCB_UII8[1)]	P6SCB_UII8[1)]		
Łańcuch dostaw	UMIEJĘTNOŚCI	weryfikować wypełnianie umów przez dostawców	ustalać łańcuch dostaw i określać dostawców	identyfikować zależności w łańcuchu dostaw	określać parametry świadczenia usług od dostawców; priorytetyzować zależności w łańcuchu dostaw i wskazywać zależności krytyczne; identyfikować wymagania cyberbezpieczeństwa dla dostawców i dotyczące łańcuchów dostaw		
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UII9[1)]	P4SCB_UII9[1)]	P5SCB_UII9[1)]	P6SCB_UII9[1)]	P7SCB_UII9[1)]	
Ocena ryzyka	UMIEJĘTNOŚCI	identyfikować zewnętrzne i wewnętrzne zagrożenia; określać podatności aktywów i procesów na zidentyfikowane zagrożenia	opracowywać, kategoryzować i dokumentować zidentyfikowane ryzyka	ocenić skalę ryzyka i jego wpływ na organizację; określić skutki i prawdopodobieństwo wystąpienia zagrożenia; priorytetyzować zdiagnozowane potencjalne ryzyka dla przedsiębiorstwa; określić poziom akceptowalnego ryzyka; dobrać metody radzenia sobie z potencjalnym ryzykiem, w tym przeciwdziałania mu, minimalizacji jego wystąpienia I transferowania; opracowywać plan działania wraz z narzędziami odpowiadający na potencjalne ryzyka	opracować politykę postępowania z ryzykiem	opracować strategię przeciwdziałania wystąpieniu ryzyk w organizacji	

NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UII10[1)]	P4SCB_UII10[1)]	P5SCB_UII10[1)]	P6SCB_UII10[1)]	P7SCB_UII10[1)]	
Wprowadzenie wymagań bezpieczeństwa w procesach, produktach i usługach	UMIEJĘTNOŚCI	identyfikować osoby odpowiedzialne za przygotowanie nowych produktów i usług	przedstawić i wyjaśnić osobom odpowiedzialnym za przygotowanie nowych produktów i usług ich zakres obowiązków związanych z obszarem cyberbezpieczeństwa	dopasowywać procesy biznesowe do wymagań cyberbezpieczeństwa w nowych usługach i produktach; monitorować realizację polityki cyberbezpieczeństwa przez osoby odpowiedzialne za tworzenie nowych produktów i usług; analizować i dokumentować procesy mające wpływ na poziom bezpieczeństwa w nowych produktach i usługach	dostosować zakres wymagań w obszarze cyberbezpieczeństwa do nowych produktów i usług; proponować zmiany w strukturze systemu cyberbezpieczeństwa; przeprowadzać zmiany w zakresie zarządzania cyberbezpieczeństwem na poziomie zespołu lub działu	zarządzać budżetem przeznaczonym na wdrażanie rozwiązań spełniających wymagania cyberbezpieczeństwa; przeprowadzać analizę skutków finansowych i organizacyjnych; przeprowadzać zmiany w zakresie zarządzania cyberbezpieczeństwem na poziomie organizacji	
WYZNACZNIK III: OCHRONA							
NAZWA WIĄZKI		POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
		P3SCB_WIII1[1)]	P4SCB_WIII1[1)]	P5SCB_WIII1[1)]			
Tożsamość, uwierzytelnianie i kontrola dostępu, w tym zdalnego	WIEDZA	podstawowe pojęcia związane z tożsamością i uwierzytelnianiem; mechanizmy dostępu, w tym dostępu zdalnego	zasady stosowania jednoskładnikowych i wieloskładnikowych systemów uwierzytelniania oraz systemów biometrycznych	dobre praktyki zarządzania tożsamością, uwierzytelniania i kontroli dostępu, w tym zdalnego			
NAZWA WIĄZKI		ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE	ZNA I ROZUMIE
		P3SCB_WIII2[1)]	P4SCB_WIII2[1)]	P5SCB_WIII2[1)]	P6SCB_WIII2[1)]	P7SCB_WIII2[1)]	P8SCB_WIII2[1)]
Ochrona systemów IT	WIEDZA	powody, dla których systemy IT są chronione	sposoby funkcjonowania i mechanizmy ochrony systemów IT; sposoby ochrony danych przetwarzanych w systemach IT	wymagania wynikające ze stosowania konkretnych systemów ochrony IT; podział odpowiedzialności między mechanizmami ochrony, w tym w systemach chmurowych (między	zaawansowane systemy ochrony, w tym słabości i ograniczenia wynikające z konieczności zachowania ciągłości działania systemów IT	trendy w zakresie rozwoju mechanizmów ochrony systemów IT	nowe obszary zagrożeń, w przypadku których jest konieczne stworzenie mechanizmów ochrony IT

				dostawcą a klientem) w różnych modelach usług chmurowych (SaaS, IaaS, PaaS)			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIII3[1)]	**P4SCB_WIII3[1)]**	**P5SCB_WIII3[1)]**	**P6SCB_WIII3[1)]**	**P7SCB_WIII3[1)]**	**P8SCB_WIII3[1)]**
Ochrona systemów OT	**WIEDZA**	powody, dla których systemy OT są chronione	sposoby funkcjonowania i mechanizmy ochrony systemów OT; specyfikę funkcjonowania systemów OT i wymagania, które muszą spełniać, w tym dotyczące zapewnienia dostępności i bezpieczeństwa realizowanych procesów	działanie systemów ochrony systemów OT; wymagania wynikające ze stosowania konkretnych systemów ochrony OT; zależności między systemami IT a systemami OT stosowanymi w organizacji	zaawansowane systemy ochrony, w tym słabości i ograniczenia wynikające z konieczności zachowania ciągłości działania systemów OT	trendy w zakresie rozwoju mechanizmów ochrony systemów OT	nowe obszary zagrożeń, w przypadku których jest konieczne stworzenie mechanizmów ochrony OT
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIII4[1)]	**P4SCB_WIII4[1)]**	**P5SCB_WIII4[1)]**			
Szkodliwe oprogramowania	**WIEDZA**	podstawowe typy szkodliwego oprogramowania	zasady statycznej i dynamicznej analizy szkodliwego oprogramowania, w tym analizy w systemach sandbox, kodu maszynowego	sposób działania szkodliwego oprogramowania używanego przez atakujących			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIII5[1)]	**P4SCB_WIII5[1)]**	**P5SCB_WIII5[1)]**	**P6SCB_WIII5[1)]**		
Sygnatury dla systemów monitorowaania	**WIEDZA**		typowe sygnatury ataku	metody tworzenia sygnatur rozpoznawania ataków i szkodliwego oprogramowania	metody projektowania nowych rozwiązań lub algorytmów działania sygnatur		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII1[1)]	**P4SCB_UIII1[1)]**	**P5SCB_UIII1[1)]**	**P6SCB_UIII1[1)]**	**P7SCB_UIII1[1)]**	

Zarządzanie kontrolą dostępu zdalnego	**UMIEJĘTNOŚCI**	skonfigurować i zarządzać mechanizmami dostępu zdalnego	zaproponować mechanizm dostępu zdalnego w organizacji, w tym przedstawić jego zalety i wady; zweryfikować przypisane użytkownikom prawa dostępu zdalnego	zaproponować odpowiednie rozwiązania do wdrożenia w organizacji w ramach systemów kontroli dostępu zdalnego; opracować zasady zarządzania kontrolą dostępu zdalnego; weryfikować system zarządzania kontrolą dostępu zdalnego	wdrożyć w organizacji system zarządzania kontrolą dostępu zdalnego	opracować w organizacji system zarządzania kontrolą dostępu zdalnego	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII2[1)]	**P4SCB_UIII2[1)]**	**P5SCB_UIII2[1)]**	**P6SCB_UIII2[1)]**	**P7SCB_UIII2[1)]**	
Zarządzanie tożsamością i uwierzytelnianiem	**UMIEJĘTNOŚCI**	nadawać uprawnienia użytkownikom i grupom użytkowników w systemie operacyjnym	określić i wybrać mechanizm uwierzytelniania dla różnych klas systemów; dobierać urządzenia i techniki autoryzacji; egzekwować zasady długości, złożoności i retencji haseł	zaproponować rozwiązania w organizacji do wdrożenia w ramach systemów zarządzania tożsamością i uwierzytelnianiem; opracować zasady zarządzania tożsamością i uwierzytelnianiem	wdrożyć w organizacji system zarządzania tożsamością i uwierzytelnianiem	opracować w organizacji system zarządzania tożsamością i uwierzytelnianiem	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIII3[1)]	**P5SCB_UIII3[1)]**	**P6SCB_UIII3[1)]**		
Rozwiązania analizujące zachowania użytkowników w systemie informatycznym	**UMIEJĘTNOŚCI**		wykorzystywać rozwiązania analizujące zachowania użytkownikó	skonfigurować rozwiązania analizujące zachowania użytkowników	dopasować i wdrożyć rozwiązania analizujące zachowania użytkowników		

NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII4[1)]	**P4SCB_UIII4[1)]**	**P5SCB_UIII4[1)]**	**P6SCB_UIII4[1)]**		
Środowisko chronione	**UMIEJĘTNOŚCI**	identyfikować granice między komponentami; zainstalować i skonfigurować program antywirusowy; założyć konto z hasłem	identyfikować granice między obiektami	identyfikować granice między systemami	współuczestniczyć w administrowaniu systemami chronionymi w organizacji		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII5[1)]	**P4SCB_UIII5[1)]**	**P5SCB_UIII5[1)]**	**P6SCB_UIII5[1)]**	**P7SCB_UIII5[1)]**	**P8SCB_UIII5[1)]**
Analiza szkodliwego oprogramowania i systemów informatycznych	**UMIEJĘTNOŚCI**	identyfikować typy szkodliwego oprogramowania; wyszukiwać informacje o szkodliwym oprogramowaniu i wykorzystywanych przez niego narzędziach	identyfikować słabe punkty w systemach informatycznych wykorzystywane przez szkodliwe oprogramowanie	analizować szkodliwe oprogramowanie oraz słabe punkty w systemach informatycznych	analizować trendy dotyczące szkodliwego oprogramowania	modyfikować szkodliwe oprogramowanie w celu zwiększenia ochrony systemów	opracować metody zabezpieczania systemów informatycznych przed nieznanym szkodliwym oprogramowaniem
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII6[1)]	**P4SCB_UIII6[1)]**	**P5SCB_UIII6[1)]**			
Monitoring użytkowników i systemów	**UMIEJĘTNOŚCI**	stosować technikę zdalnego i stacjonarnego dostępu	korzystać z urządzeń i oprogramowania do monitoringu systemów, w tym logów	analizować dane z urządzeń i oprogramowania do monitoringu systemów; stosować technikę monitoringu aktywnej sesji użytkownika;			

				korelować zdarzenia z wielu urządzeń i wyciągać wnioski			
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII7[1)]	**P4SCB_UIII7[1)]**	**P5SCB_UIII7[1)]**	**P6SCB_UIII7[1)]**		
Monitoring ryzyk	**UMIEJĘTNOŚCI**	monitorować ryzyka zgodnie z ustalonymi procedurami wykorzystując dostępne narzędzia	raportować wyniki monitoringu interesariuszom, tj. zapewnić dostępność użytecznych, kompletnych i aktualnych informacji o ryzyku	opracować zasady i procedury monitoringu ryzyk; dobrać narzędzia do monitorowania i raportowania ryzyk	opracować narzędzia wspomagające monitoring ryzyk		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII8[1)]	**P4SCB_UIII8[1)]**	**P5SCB_UIII8[1)]**			
Przygotowanie sygnatur dla systemów monitorowania	**UMIEJĘTNOŚCI**	wskazać zachodzący atak lub nietypowe działanie	tworzyć sygnatury dla znanych typów ataków	tworzyć sygnatury dotychczas nieznanych typów ataków			
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIII9[1)]	**P5SCB_UIII9[1)]**	**P6SCB_UIII9[1)]**	**P7SCB_UIII9[1)]**	
Stosowanie narzędzi wykorzystujących sztuczną inteligencję w systemach cyberbezpieczeństwa	**UMIEJĘTNOŚCI**		interpretować informacje otrzymywane z systemów sztucznej inteligencji	parametryzować systemy sztucznej inteligencji i oceniać ich skuteczność działania; utrzymywać efektywność działania systemów sztucznej inteligencji	proponować wykorzystanie metod sztucznej inteligencji do adresowania wielkości, złożoności i czasu przetwarzania zbiorów danych w celu automatyzacji; tworzyć wymagania dla narzędzi opartych na sztucznej inteligencji w celu zapewniania cyberbezpieczeństwa;	implementować rozwiązania w zakresie sztucznej inteligencji z systemami funkcjonującymi w organizacji	

					integrować rozwiązania w zakresie sztucznej inteligencji z systemami funkcjonującymi w organizacj		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIII10[1)]	**P4SCB_UIII10[1)]**	**P5SCB_UIII10[1)]**	**P6SCB_UIII10[1)]**	**P7SCB_UIII10[1)]**	**P8SCB_UIII10[1)]**
Utrzymanie ciągłości działania	**UMIEJĘTNOŚCI[1)]**	wykonywać ustandaryzowane działania w kontekście utrzymania ciągłości działania organizacji	współpracować z zewnętrznymi dostawcami w zakresie utrzymania ciągłości działania w łańcuchu dostaw	określać wymagania w zakresie utrzymania ciągłości działania dla poszczególnych obszarów; zarządzać współpracą z zewnętrznymi dostawcami w zakresie utrzymania ciągłości działania w łańcuchu dostaw; weryfikować utrzymanie ciągłości działania	priorytetyzować obszary, w których jest konieczne zachowanie ciągłości działania	projektować procesy utrzymania ciągłości działania	kreować standardy i rozwiązania specjalistyczne dla procesów utrzymania ciągłości działania
WYZNACZNIK IV: WYKRYWANIE							
NAZWA WIĄZKI		**POZIOM 3**	**POZIOM 4**	**POZIOM 5**	**POZIOM 6**	**POZIOM 7**	**POZIOM 8**
		ZNA I ROZUMIE	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WIV1[1)]	**P5SCB_WIV1[1)]**	**P6SCB_WIV1[1)]**		
Podatności aplikacji webowych i ataki na nie	**WIEDZA**		kategorie podatności aplikacji webowych; kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na aplikacje webowe	typowe podatności i ataki na aplikacje webowe po stronie serwerowej i po stronie klienta, w tym SQL injection, XSS, CSRF, IDOR, Broken Access Control; metodyki testów penetracyjnych aplikacji webowych, w tym OWASP Web Security Testing Guide i OWASP ASVS	złożone ataki na podatności webowe, w tym SSRF, SSTI, błędy deserializacji danych, XXE i padatności API		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WIV2[1)]	**P5SCB_WIV2[1)]**	**P6SCB_WIV2[1)]**		

Podatności systemów i aplikacji mobilnych oraz ataki na nie	**WIEDZA**		kategorie podatności systemów i aplikacji mobilnych; kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na systemy i aplikacje mobilne	typowe podatności aplikacji mobilnych po stronie serwerowej i po stronie klienta oraz ataki na nie; metodyki testów penetracyjnych aplikacji mobilnych, w tym OWASP MASTG i OWASP MASVS	złożone ataki na podatności w aplikacjach mobilnych, w tym podatności API; proces dekompilacji aplikacji mobilnej (reverse engineering)		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIV3[1)]	**P4SCB_WIV3[1)]**	**P5SCB_WIV3[1)]**	**P6SCB_WIV3[1)]**		
Podatności infrastruktury sieciowej i ataki na nią	**WIEDZA**	sposoby rozpoznawania sieci, w tym skanowanie adresów IP, numerów portów aktywnych usług	kategorie podatności infrastruktury sieciowej; kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na infrastrukturę sieciową	typowe podatności infrastruktury sieciowej i ataki na tę infrastrukturę, w tym sieci bezprzewodowe; metodyki testów penetracyjnych infrastruktury sieciowej, w tym OSSTMM	złożone ataki na podatności, np. związane z protokołami i usługami sieciowymi, w tym MitM, DHCP i ARP spoofing		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WIV4[1)]	**P5SCB_WIV4[1)]**	**P6SCB_WIV4[1)]**		
Podatności systemów serwerowych i klienckich oraz ataki na nie	**WIEDZA**		kategorie podatności systemów serwerowych i klienckich; kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na systemy serwerowe i klienckie	typowe podatności i ataki na systemy operacyjne i aplikacje na nich zainstalowane, w tym buffer overflow, format string i escape to shell	złożone ataki na podatności związane z usługami katalogowymi, w tym Active Directory		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WIV5[1)]	**P5SCB_WIV5[1)]**	**P6SCB_WIV5[1)]**		

Podatności środowisk chmurowych i ataki na nie	**WIEDZA**		kategorie podatności w środowiskach chmurowych; kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na środowiska chmurowe	typowe podatności w środowiskach chmurowych i ataki na nie	złożone ataki na podatności związane ze środowiskami chmurowymi		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIV6[1)]	**P4SCB_WIV6[1)]**	**P5SCB_WIV6[1)]**	**P6SCB_WIV6[1)]**		
Analiza kodu	**WIEDZA**	zasady statycznej i dynamicznej analizy kodu	metody statycznej i dynamicznej analizy kodu i narzędzia do tego służące	podatności występujące w kodzie, w tym związane z obsługą pamięci i wprowadzanych danych	proces analizy kodu źródłowego skompilowanego oprogramowania (reverse engineering)		
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIV7[1)]	**P4SCB_WIV7[1)]**	**P5SCB_WIV7[1)]**	**P6SCB_WIV7[1)]**	**P7SCB_WIV7[1)]**	
Zasady projektowania i zarządzania rozwiązaniami IoT	**WIEDZA**	komponenty IoT; protokoły komunikacyjne IoT; rodzaje rozwiązań IoT	zasady budowania środowisk komplementarnych i scentralizowanych w oparciu o komponenty IoT; podstawy komunikacji rozproszonej w IoT; zagadnienia dotyczące zasilania komponentów IoT; podstawowe zagadnienia stabilności działania systemów IoT	zasady monitorowania komponentów oraz środowisk IoT; podstawy projektowania rozwiązań IoT; typowe podatności rozwiązań IoT i ataki na nie	zagadnienia dotyczące zasilania komponentów IoT; sieci specjalistyczne, w tym sieci AIM; zasady zarządzania danymi w środowiskach IoT; zasady projektowania rozwiązań IoT	zasady opracowywania rozwiązań IoT wymagających szczególnej ochrony	
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIV8[1)]	**P4SCB_WIV8[1)]**	**P5SCB_WIV8[1)]**	**P6SCB_WIV8[1)]**	**P7SCB_WIV8[1)]**	

Zasady projektowania i zarządzania rozwiązaniami OT	**WIEDZA**	komponenty OT; protokoły komunikacyjne OT; rodzaje rozwiązań OT	zasady budowania środowisk komplementarnych i scentralizowanych w oparciu o komponenty OT; podstawy komunikacji rozproszonej w OT; podstawowe zagadnienia stabilności działania systemów OT	zasady monitorowania komponentów oraz środowisk OT; podstawy projektowania rozwiązań OT; typowe podatności i ataki na rozwiązań OT i ataki na nie	zagadnienia dotyczące zasilania komponentów OT; sieci specjalistyczne, w tym sieci polowe; zasady zarządzania danymi w środowiskach OT; zasady projektowania rozwiązań OT	zasady opracowywania rozwiązań OT wymagających szczególnej ochrony	
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIV9[1)]	**P4SCB_WIV9[1)]**	**P5SCB_WIV9[1)]**	**P6SCB_WIV9[1)]**	**P7SCB_WIV9[1)]**	**P8SCB_WIV9[1)]**
Zasady projektowania i zarządzania zautomatyzowanymi systemami o dużej skali złożoności	**WIEDZA**	kryteria określające potrzebę stosowania zautomatyzowania pracy; obszary możliwe do automatyzacji pracy	zasady automatyzacji pracy	narzędzia do budowy zautomatyzowanych systemów, w tym opartych na sztucznej inteligencji; podstawy automatyki	zasady projektowania liniowych układów automatyzacji	zasady projektowania automatyzacji w systemach współliniowych, wielowątkowych	zasady integracji systemów niekompatybilnych
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIV10[1)]	**P4SCB_WIV10[1)]**	**P5SCB_WIV10[1)]**			
Symulowany atak hakerski	**WIEDZA**	rodzaje ataków socjotechnicznych; rodzaje oprogramowania wykorzystywanego w ataku redteamingowym w internecie	budowę i sposób funkcjonowania oprogramowania wykorzystywanego w ataku redteamingowym w internecie	założenia testów stosowanych podczas ataku redteamingowego			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WIV11[1)]	**P5SCB_WIV11[1)]**	**P6SCB_WIV11[1)]**		
Symulowany atak fizyczny	**WIEDZA**		metody fizycznego ataku redteamingowego	stosowane zabezpieczenia, systemy alarmowe i metody kontroli dostępu; narzędzia służące do testowania zabezpieczeń,	działanie oraz słabości systemów alarmowych i metod kontroli dostępu		

				systemów alarmowych i metod kontroli dostępu			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WIV12[1)]	**P4SCB_WIV12[1)]**	**P5SCB_WIV12[1)]**			
Socjotechnika	**WIEDZA**	rodzaje testów socjotechnicznych	zasady czytania mowy ciała; typowe zachowania użytkowników sprzyjające manipulacji; techniki manipulacji; narzędzia wykorzystywane do ataków socjotechnicznych	budowę i zasady funkcjonowania oprogramowania wspierającego testy socjotechniczne			
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV1[1)]	**P5SCB_UIV1[1)]**	**P6SCB_UIV1[1)]**	**P7SCB_UIV1[1)]**	**P8SCB_UIV1[1)]**
Obszary bazowe testów penetracyjnych	**UMIEJĘTNOŚCI**		opisać znalezione podatności	ocenić wynik przeprowadzonego testu penetracyjnego; wskazać krytyczne obszary systemów, wymagające szczegółowych testów; przygotować raport z rekomendacjami z przeprowadzonego testu penetracyjnego; tworzyć własne proste narzędzia wspierające prowadzenie testów penetracyjnych, w tym skanery i exploity	przygotować plan testu penetracyjnego; nadzorować prowadzenie testów penetracyjnych przez podległy zespół	modyfikować narzędzia do testów penetracyjnych	opracowywać narzędzia do testów penetracyjnych
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV2[1)]	**P5SCB_UIV2[1)]**	**P6SCB_UIV2[1)]**	**P7SCB_UIV2[1)]**	

Testy penetracyjne aplikacji webowych	**UMIEJĘTNOŚCI**		przeprowadzać testy aplikacji webowych z użyciem zautomatyzowanych narzędzi	przeprowadzać testy aplikacji webowych z wykorzystaniem typowych rodzajów podatności i ataków, w tym SQL injection, XSS, CSRF, IDOR i Broken Access Control; przeprowadzać testy aplikacji webowych zgodnie z określonymi metodykami, w tym OWASP Web Security Testing Guide i OWASP ASVS	przeprowadzać złożone ataki na podatności webowe, w tym SSRF, SSTI, błędy deserializacji danych, XXE, padatności API	wykryć nowe podatności (zero-days) w aplikacjach webowych i wykorzystywać je do ataków	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV3[1)]	**P5SCB_UIV3[1)]**	**P6SCB_UIV3[1)]**	**P7SCB_UIV3[1)]**	
Testy penetracyjne systemów i aplikacji mobilnych	**UMIEJĘTNOŚCI**		przeprowadzać testy systemów i aplikacji mobilnych z wykorzystaniem zautomatyzowanych narzędzi	przeprowadzać ataki na typowe systemy i aplikacje mobilne po stronie serwerowej i po stronie klienta z wykorzystaniem metodyk testów penetracyjnych aplikacji mobilnych, w tym OWASP MASTG i OWASP MASVS	przeprowadzać złożone ataki na aplikacje mobilne, w tym podatności API; przeprowadzać dekompilację aplikacji mobilnej (reverse engineering)	wykryć nowe podatności (zero-days) systemów i aplikacji mobilnych oraz wykorzystywać je do ataków	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV4[1)]	**P5SCB_UIV4[1)]**	**P6SCB_UIV4[1)]**	**P7SCB_UIV4[1)]**	
Testy penetracyjne infrastruktury sieciowej	**UMIEJĘTNOŚCI**		przeprowadzać testy infrastruktury sieciowej z użyciem zautomatyzowanych narzędzi; przeprowadzać rozpoznawanie sieci, w tym skanowanie adresów IP, numerów portów aktywnych usług	przeprowadzać typowe ataki na infrastrukturę sieciową, w tym sieci bezprzewodowe	przeprowadzać ataki związane z protokołami i usługami sieciowymi, w tym MitM, DHCP i ARP spoofing; wykorzystywać sprzęt służący do przeprowadzania ataków związanych z protokołami i usługami sieciowymi	wykryć nowe podatności (zero-days) w infrastrukturze sieciowej i wykorzystywać je do ataków	

NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV5[1)]	**P5SCB_UIV5[1)]**	**P6SCB_UIV5[1)]**	**P7SCB_UIV5[1)]**	
Testy penetracyjne systemów serwerowych i klienckich	**UMIEJĘTNOŚCI**		przeprowadzać testy systemów serwerowych i klienckich z użyciem zautomatyzowanych narzędzi	przeprowadzać ataki na typowe systemy operacyjne i ich aplikacje, w tym buffer overflow, format string i escape to shell	przeprowadzać ataki na usługi katalogowe, w tym Active Directory	wykryć nowe podatności (zero-days) systemów serwerowych i klienckich oraz wykorzystywać je do ataków	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV6[1)]	**P5SCB_UIV6[1)]**	**P6SCB_UIV6[1)]**		
Testy penetracyjne środowisk chmurowych	**UMIEJĘTNOŚCI**		ocenić prawidłowość konfiguracji instancji chmury obliczeniowej pod kątem bezpieczeństwa; przeprowadzać rekonesans publicznych chmur obliczeniowych	zaplanować i dokonać oceny skutków planowanych testów penetracyjnych w środowisku chmurowym	wyciągnąć wnioski z przeprowadzonych testów penetracyjnych poszczególnych instancji chmury obliczeniowej; zaproponować rozwiązania mające na celu zwiększenie bezpieczeństwa instancji chmury obliczeniowej		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV7[1)]	**P5SCB_UIV7[1)]**	**P6SCB_UIV7[1)]**	**P7SCB_UIV7[1)]**	**P8SCB_UIV7[1)]**
Przeprowadzenie analizy kodu	**UMIEJĘTNOŚCI**		przeprowadzić automatyczną analizę kodu; określać kategorie podatności znalezionych za pomocą automatycznego narzędzia	określać konsekwencje wykorzystania znalezionych podatności	analizować zdekompilowany kod; samodzielnie zidentyfikować podatności; weryfikować wyniki automatycznej analizy	wykryć nowe rodzaje podatności w kodzie; rozbudowywać narzędzia do analizy kodu	opracować narzędzia do analizy kodu
		POTRAFI	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**

NAZWA WIĄZKI		P3SCB_UIV8[1)]	P4SCB_UIV8[1)]	P5SCB_UIV8[1)]	P6SCB_UIV8[1)]	P7SCB_UIV8[1)]	P8SCB_UIV8[1)]
Budowa i zarządzanie rozwiązaniami IoT	UMIEJĘTNOŚCI	zbudować prosty system IoT w oparciu o komunikację bezpośrednią	zbudować system IoT w oparciu o algorytmikę postępowania lub scenariusze użycia	monitorować status pracy poszczególnych urządzeń i całego systemu IoT	automatyzować obsługę zagadnień cyberbezpieczeństwa w środowiskach IoT; rozwiązywać zagadnienia związane z podatnościami w środowiskach IoT; zbudować system reakcyjny w środowisku IoT w oparciu o monitorowane parametry	rozwiązywać zagadnienia związane z niestabilnością pracy środowiska IoT; budować systemy procesowe w środowisku IoT	opracowywać rozwiązania IoT wymagające szczególnej ochrony
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
		P3SCB_UIV9[1)]	P4SCB_UIV9[1)]	P5SCB_UIV9[1)]	P6SCB_UIV9[1)]	P7SCB_UIV9[1)]	P8SCB_UIV9[1)]
Budowa i zarządzanie rozwiązaniami OT	UMIEJĘTNOŚCI	zbudować prosty system OT w oparciu o komunikację bezpośrednią	zbudować system OT w oparciu o algorytmikę postępowania lub scenariusze użycia	monitorować status pracy poszczególnych urządzeń i całego systemu OT	automatyzować obsługę zagadnień cyberbezpieczeństwa w środowiskach OT; zbudować system reakcyjny w środowisku OT w oparciu o monitorowane parametry; rozwiązywać zagadnienia związane z podatnościami w środowiskach OT	rozwiązywać zagadnienia związane z niestabilnością pracy środowiska OT; zbudować systemy procesowe w środowisku OT	opracowywać rozwiązania OT wymagające szczególnej ochrony
NAZWA WIĄZKI		POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI	POTRAFI
			P4SCB_UIV10[1)]	P5SCB_UIV10[1)]	P6SCB_UIV10[1)]	P7SCB_UIV10[1)]	P8SCB_UIV10[1)]
Budowa i zarządzanie zautomatyzowanymi systemami o dużej skali złożoności	UMIEJĘTNOŚCI		zbudować algorytmy automatyki o dużej skali złożoności	zbudować typowy system automatyki o dużej skali złożoności; nadzorować i utrzymywać systemy o dużej skali złożoności	zbudować systemy o dużej skali złożoności z wymaganiami dotyczącymi działania w czasie rzeczywistym	projektować systemy o dużej skali złożoności z wymaganiami dotyczącymi działania w czasie rzeczywistym; zastosować sztuczną inteligencję do	integrować systemy niekompatybilne

						zautomatyzowania pracy w systemach o dużej skali złożoności	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIV11[1)]	**P4SCB_UIV11[1)]**	**P5SCB_UIV11[1)]**	**P6SCB_UIV11[1)]**	**P7SCB_UIV11[1)]**	
Wykrywanie zmian	**UMIEJĘTNOŚCI**	wykryć zmiany na poziomie komponentów	wykryć niepożądane zmiany na poziomie kodu	wykryć zmiany na poziomie parametrów pracy systemów	wykryć i kontrolować zmiany po zdarzeniu reakcyjnym	wykryć i nadzorować w trybie ciągłym zmiany w systemach zautomatyzowanych	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV12[1)]	**P5SCB_UIV12[1)]**	**P6SCB_UIV12[1)]**	**P7SCB_UIV12[1)]**	**P8SCB_UIV12[1)]**
Redteaming	**UMIEJĘTNOŚCI**		przeprowadzić rekonesans przed przeprowadzeniem ataku redteamingowego w internecie	przygotować założenia ataku redteamingowego w internecie; dobrać test penetracyjny w ataku redteamingowym w internecie; analizować wyniki ataku redteamingowego w internecie	dostosować oprogramowanie do założeń ataku redteamingowego w internecie; przeprowadzić test penetracyjny w ataku redteamingowym; opracować rekomendacje po ataku redteamingowym	eskalować atak redteamingowy; wykorzystywać nowo znalezione podatności w ataku redteamingowym; wskazać możliwe nowe metody ataków redteamingowych w internecie	stworzyć narzędzia do nowych typów ataków redteamingowych w internecie
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UIV13[1)]	**P5SCB_UIV13[1)]**	**P6SCB_UIV13[1)]**	**P7SCB_UIV13[1)]**	**P8SCB_UIV13[1)]**
Redteaming fizyczny	**UMIEJĘTNOŚCI**		przeprowadzić rekonesans przed fizycznym atakiem redteamingowym	przygotować założenia fizycznego ataku redteamingowego; dobrać test penetracyjny w ataku redteamingowym fizycznym;	przeprowadzić atak fizyczny; ominąć zaawansowane zabezpieczenia, systemy alarmowe i metody kontroli dostępu; dostosować oprogramowanie do założeń	eskalować fizyczny atak redteamingowy; wykorzystywać nowo znalezione podatności w fizycznym ataku redteamingowym;	stworzyć narzędzia do nowych typów ataków fizycznych

				dobrać metody w ataku fizycznym; tworzyć własne proste narzędzia wspierające; ominąć typowe zabezpieczenia, systemy alarmowe i metody kontroli dostępu; korzystać z narzędzi testowania zabezpieczeń, systemów alarmowych i metod kontroli dostępu; analizować wyniki fizycznego ataku redteamingowego; testować kontrolę dostępu w organizacji	fizycznego ataku redteamingowego; przeprowadzić test penetracyjny w ramach redteamingu fizycznego; opracowywać rekomendacje po fizycznym ataku redteamingowym	wskazać możliwe nowe metody ataków fizycznych	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
				P5SCB_UIV14[1)]	**P6SCB_UIV14[1)]**		
Testy socjotechniczne	**UMIEJĘTNOŚCI**			stosować techniki manipulacji; przeprowadzić testy socjotechniczne; tworzyć własne proste narzędzia wspierające prowadzenie testów socjotechnicznych	określić oczekiwane rezultaty testów socjotechnicznych; przygotować plan testów socjotechnicznych; opracować rekomendacje po ataku socjotechnicznym		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UIV15[1)]	**P4SCB_UIV15[1)]**	**P5SCB_UIV15[1)]**	**P6SCB_UIV15[1)]**	**P7SCB_UIV15[1)]**	
Threat modelling	**UMIEJĘTNOŚCI**	rozpoznawać komponenty systemu i ich funkcje	rozpoznawać zależności między komponentami systemów	wykryć typowe zagrożenia związane z architekturą systemów	przeprowadzić analizę ryzyka, w tym ocenić potencjalne skutki ataków, prawdopodobieństwo ich wystąpienia oraz przewidzieć ich wpływ na system; wykorzystywać różne metodyki pracy związane z threat modellingiem, takie	przewidywać nowe obszary, w których mogą wystąpić zagrożenia	

					jak STRIDE, DREAD i OWASP Threat Modeling Guide		
WYZNACZNIK V: REAKCJA							
NAZWA WIĄZKI		**POZIOM 3**	**POZIOM 4**	**POZIOM 5**	**POZIOM 6**	**POZIOM 7**	**POZIOM 8**
		ZNA I ROZUMIE	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WV1[1)]	**P4SCB_WV1[1)]**	**P5SCB_WV1[1)]**			
Terminologia i technologia związana z materiałem dowodowym	**WIEDZA**	rodzaje materiałów dowodowych; typy zabezpieczania materiału dowodowego; podstawową terminologię dotyczącą cyfrowego materiału dowodowego, w tym pojęcia manipulacji i degradacji materiału dowodowego, znacznika czasu, czasu systemowego, ulotnego i nieulotnego materiału dowodowego; algorytmy funkcji skrótu; pojęcia logów oraz konfiguracji systemów i aplikacji	rodzaje informacji przetwarzanych w systemach informatycznych, w tym urządzeniach cyfrowych, bazach danych, dokumentach generowanych przez system, danych generowanych przez użytkownika i danych ulotnych	możliwości audytowania struktury systemu plików; sposoby zabezpieczania informacji przetwarzanych w poszczególnych elementach systemu informatycznego			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WV2[1)]	**P4SCB_WV2[1)]**	**53SCB_WV2[1)]**			
Zabezpieczanie dowodów	**WIEDZA**	podstawowe techniki zabezpieczania różnych typów dowodów; metody określenia wymagań dotyczących zabezpieczania dowodów; wpływ czynników zewnętrznych na materiał dowodowy, takich jak	techniki replikacji materiału dowodowego; standardy certyfikacyjne dotyczące przetwarzania próbek dowodowych w trakcie postępowania; konsekwencje, w tym prawne, błędów wynikających z winy badającego lub otoczenia, wpływających na jakość i	wymagania prawne postępowania z cyfrowym materiałem dowodowym; zależności występujące w poszczególnych grupach informacyjnych i formatach danych; techniki agregacji informacji;			

		wilgoć, temperatura i wstrząsy; techniki transportu materiałów dowodowych w sposób umożliwiający wykorzystanie ich w późniejszym postępowaniu dowodowym	wiarygodność postępowania dowodowego	techniki odbioru i zabezpieczenia informacji do postępowania w laboratorium			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WV3[1)]	**P4SCB_WV3[1)]**	**P5SCB_WV3[1)]**			
Postępowanie z cyfrowym materiałem dowodowym	**WIEDZA**	potencjalne miejsca pozyskania informacji pozwalających na analizę incydentu; wymagania i procedury dotyczące utrzymania łańcucha dowodowego zgodnie z wymaganiami prawnymi; zasady przygotowania do transportu, przesyłania, przekazania i przechowywania cyfrowego materiału dowodowego	zasady analizy cyfrowego materiału dowodowego; zasady generowania dokumentów do celów audytu materiału dowodowego; zasady określania parametrów dokumentacji; zasady zapewniania bezpieczeństwa informacji; zasady zabezpieczania cyfrowego materiału dowodowego	wymagania prawne dotyczące pozyskiwania cyfrowego materiału dowodowego; sposoby zastosowania środków ochrony do zabezpieczenia cyfrowego materiału dowodowego; procedury dokumentowania materiału dowodowego			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WV4[1)]	**P4SCB_WV4[1)]**	**P5SCB_WV4[1)]**			
Systemy reakcji na incydenty	**WIEDZA**	plany reagowania na poszczególne incydenty, w tym tworzone na potrzeby organizacji i jej systemów wewnętrznych; zasady komunikacji zewnętrznej i wewnętrznej dotyczące incydentu	dobre praktyki reakcji na incydenty; zasady przygotowania raportu dotyczącego obsługi incydentów; sposób działania poszczególnych systemów reakcji na incydent	wymogi prawne dotyczące informowania o incydentach; wymogi kontraktowe dotyczące informowania o incydentach			

NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UV1[1)]	**P4SCB_UV1[1)]**	**P5SCB_UV1[1)]**	**P6SCB_UV1[1)]**		
Identyfikowanie materiału dowodowego	**UMIEJĘTNOŚCI**	rozpoznać środowisko, w którym należy zabezpieczyć materiał dowodowy	wskazać systemy wymagające zabezpieczenia materiału dowodowego; zidentyfikować hasła wymagane do analizowanego materiału; identyfikować wpływ konfiguracji systemów i aplikacji na sposób ich działania; zweryfikować informację w trakcie rozmowy, w tym z osobą, której dotyczy materiał dowodowy	agregować pozornie niespójne informacje lub niekompatybilne systemy; połączyć wykryte zdarzenia z wielu źródeł ataku	rozpoznawać poziom ryzyka zagrożeń ze świata zewnętrznego uwzględniając specyfikę organizacji; rozwiązać problem awarii lub niedostępności systemu		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UV2[1)]	**P4SCB_UV2[1)]**	**P5SCB_UV2[1)]**	**P6SCB_UV2[1)]**	**P7SCB_UV2[1)]**	
Zabezpieczenie i pozyskanie materiału dowodowego	**UMIEJĘTNOŚCI**	pozyskać i gromadzić cyfrowy materiał dowodowy według standardowych procedur; zabezpieczyć dane dowodowe zgodnie z przyjętym protokołem; dobrać odpowiednią do sytuacji metodę transportu grup dowodowych	pozyskać i gromadzić analogowy materiał dowodowy wymagany do przeprowadzenia analizy; pozyskać, gromadzić i przetwarzać cyfrowy materiał dowodowy według niestandardowych procedur; udokumentować materiał dowodowy, w tym taki, który nie może być przejęty; dobrać właściwą technikę zabezpieczenia dowodu w określonym środowisku	dobrać narzędzia przeciwdziałające niebezpieczeństwu podważenia materiału dowodowego; przygotować opis incydentu	przydzielać role w procesie zabezpieczenia dowodów; wspierać techników w laboratorium i jego otoczeniu zgodnie z procedurami oraz potrzebami technicznymi po wystąpieniu incydentu bezpieczeństwa	minimalizować potencjalne ryzyka w odniesieniu do materiału dowodowego; zarządzać zespołem w pracy dowodowej w laboratorium informatyki śledczej oraz w terenie	

			systemowym pracującym w konkretnym środowisku fizycznym; wykonać kopię dowodów oraz przekazać ją do innego stanowiska analitycznego; kolekcjonować grupy dowodowe; dobierać techniki odbioru dowodu; wskazać potencjalne materiały dowodowe nie objęte procedurami				
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UV3[1)]	**P5SCB_UV3[1)]**	**P6SCB_UV3[1)]**	**P7SCB_UV3[1)]**	**P8SCB_UV3[1)]**
Analityka zebranego materiału dowodowego	**UMIEJĘTNOŚCI**		ocenić jakość i wiarygodność materiału dowodowego za pomocą konkretnych systemów i rozwiązań wspomagających automatyczną ocenę wykorzystać różnorodne systemy i dane do ekstrakcji informacji i ich transportu	przyjąć grupy dowodowe do laboratorium; wykonać procedurę przejmowania częściowego lub pełnego obrazu z cyfrowego nośnika danych; kwalifikować dowody lub ich grupy; wykorzystywać rozwiązania techniczne służące zwiększeniu efektywności przetwarzania danych dowodowych	analizować pozyskany materiał dowodowy, w tym z wykorzystaniem specjalistycznych narzędzi	zarządzać zespołem w pracy analitycznej	wyszukiwać i analizować niestandardowe dowody; opracować nowe metody służące do poprawnej ekstrakcji danych; opracować nowe rozwiązanie służące do poprawnej ekstrakcji danych
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UV4[1)]	**P4SCB_UV4[1)]**	**P5SCB_UV4[1)]**	**P6SCB_UV4[1)]**	**P7SCB_UV4[1)]**	

Reakcja na zdarzenia i incydenty	**UMIEJĘTNOŚCI**	identyfikować komponenty zdarzenia; współpracować z osobą związaną z incydentem	reagować na zdarzenia zgodnie z procedurami, standardami reakcyjnymi i planami obsługi incydentów; identyfikować korelacje między dwoma zdarzeniami; zweryfikować kompletność planów obsługi incydentów	modernizować procedury, standardy reakcyjne w odpowiedzi na zaistniały incydent; przedstawić informacje o incydencie interesariuszom, w tym kierownictwu, klientom i organom zewnętrznym; analizować i reagować na incydenty z użyciem poszczególnych systemów; koordynować działania związane z reakcją na incydenty; przygotować i przedstawić raport z obsługi incydentu	opracować plany, procedury, scenariusze reakcji na incydent bezpieczeństwa; opracować automatyczne narzędzia odpowiadające na zaistniałe incydenty	opracować standardy reakcji na incydent bezpieczeństwa; określać ścieżki rozwoju systemów, które minimalizują potencjalne skutki incydentów	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UV5[1)]	**P4SCB_UV5[1)]**	**P5SCB_UV5[1)]**	**P6SCB_UV5[1)]**	**P7SCB_UV5[1)]**	**P8SCB_UV5[1)]**
Laboratorium obszaru cyberbezpieczeństwa, w tym informatyki śledczej	**UMIEJĘTNOŚCI**	używać podstawowych narzędzi laboratorium obszaru cyberbezpieczeństwa, w tym informatyki śledczej	dobrać stanowisko do zagadnienia lub celu badania	zaplanować zakres czynności badawczych, uwzględniając specyfikę laboratorium obszaru cyberbezpieczeństwa, w tym informatyki śledczej; przeprowadzić badanie przy wykorzystaniu narzędzi adekwatnych do zebranego materiału dowodowego; przygotować raport z przeprowadzonego badania	wskazać i przypisać konkretne role do osób w laboratorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej; weryfikować prawidłowe użycie narzędzi przez pracowników w laboratorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej	przeprowadzić symulację incydentu bezpieczeństwa, pozwalającą weryfikować działanie badanego systemu w laboratorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej, i minimalizować potencjalne konsekwencje	tworzyć nowe rozwiązania techniczne i proceduralne w celach optymalizacji działania laboratorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej
WYZNACZNIK VI: ODBUDOWA							
NAZWA WIĄZKI		**POZIOM 3**	**POZIOM 4**	**POZIOM 5**	**POZIOM 6**	**POZIOM 7**	**POZIOM 8**
		ZNA I ROZUMIE	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WVI1[1)]	**P4SCB_WVI1[1)]**	**P5SCB_WVI1[1)]**			

Kopie bezpieczeństwa	**WIEDZA**	rodzaje kopii bezpieczeństwa	budowę i ograniczenia nośników danych; metody i systemy wykonywania kopii bezpieczeństwa	zasady budowania zapasowych centrów przetwarzania danych			
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WVI2[1)]	**P5SCB_WVI2[1)]**			
Model ciągłości działania	**WIEDZA**		budowę i ograniczenia modelu ciągłości działania; metody wdrażania modelu ciągłości działania	metody opracowywania modelu ciągłości działania dopasowanego do potrzeb organizacji; potencjalne skutki incydentu dla działania modelu ciągłości działania			
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UVI1[1)]	**P4SCB_UVI1[1)]**	**P5SCB_UVI1[1)]**	**P6SCB_UVI1[1)]**		
Identyfikacja zagadnień ciągłości działania	**UMIEJĘTNOŚCI**	identyfikować rodzaj incydentu	oceniać skalę zagrożenia	reagować na incydent zgodnie z wewnętrznymi procedurami; wprowadzać zmiany w przypadku awarii w celu odtworzenia systemu; monitorować poprawność działania systemów zapasowych	opracowywać i wdrażać procedury przełączenia na systemy zapasowe		
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UVI2[1)]	**P4SCB_UVI2[1)]**	**P5SCB_UVI2[1)]**	**P6SCB_UVI2[1)]**	**P7SCB_UVI2[1)]**	
Ocena incydentu	**UMIEJĘTNOŚCI**	replikować incydent	replikować incydent w ramach weryfikacji działania procedur	analizować incydent i jego skutki	opracować rozwiązania strukturalne w odpowiedzi na zaistniały incydent	rekomendować i inicjować wdrożenie zmian strukturalnych	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UVI3[1)]	**P4SCB_UVI3[1)]**	**P5SCB_UVI3[1)]**	**P6SCB_UVI3[1)]**	**P7SCB_UVI3[1)]**	

Odbudowa modelu ciągłości działania	**UMIEJĘTNOŚCI**	identyfikować podatności modelu działania w kontekście zaistniałego incydentu	opracować propozycje zmian technicznych w odpowiedzi na zaistniały incydent	analizować sytuację pod kątem zaistniałego incydentu oraz wyciągać wnioski; opracować optymalną kolejność działań naprawczych, z uwzględnieniem specyfiki organizacji lub systemów; wprowadzać korekty do modelu działania	modyfikować modele działania, z uwzględnieniem uwarunkowań organizacji i zaistniałego incydentu	tworzyć nowe modele działania, z uwzględnieniem uwarunkowań organizacji i zaistniałego incydentu	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UVI4[1)]	**P4SCB_UVI4[1)]**	**P5SCB_UVI4[1)]**	**P6SCB_UVI4[1)]**	**P7SCB_UVI4[1)]**	
Odtworzenie ciągłości działania	**UMIEJĘTNOŚCI**	monitorować wskaźniki systemów kontroli działania oraz automatyczne wykonywanie kopii bezpieczeństwa; sprawdzać poprawność kopii bezpieczeństwa; odtworzyć kopie bezpieczeństwa	monitorować przełączenie się systemów informatycznych na serwery w zapasowym CPD; monitorować moment odzyskania pełnej sprawności świadczonych usług przez systemy cyfrowe	rekomendować urządzenia oraz oprogramowanie do wykonywania kopii bezpieczeństwa; opracować zasady retencji kopii bezpieczeństwa; opracować plan ciągłości działania	dokonywać krytycznej analizy stosowanych rozwiązań w zakresie polityki tworzenia kopii bezpieczeństwa; wdrażać zmiany w rozwiązaniach z zakresu tworzenia kopii bezpieczeństwa wynikających z przeprowadzonej ewaluacji polityki; dokonywać adaptacji ciągłości działania w ujęciu taktycznym	wdrażać zmiany w rozwiązaniach z zakresu tworzenia kopii bezpieczeństwa wynikających z przeprowadzonej analizy trendów; dokonywać adaptacji planu ciągłości działania w ujęciu strategicznym	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UVI5[1)]	**P4SCB_UVI5[1)]**	**P5SCB_UVI5[1)]**			
Weryfikacja postanowień umów	**UMIEJĘTNOŚCI**	identyfikować postanowienia umów wpływające na zapewnianie ciągłości działania systemów	weryfikować zgodność postanowień umów z działaniami zapewnianiającymi bezpieczeństwo systemów; realizować umowy, w tym OLA i SLA;	rekomendować postanowienia w umowach, w tym OLA i SLA, wspierające zapewnianie ciągłości działania			

			monitorować realizację postanowień umów, w tym OLA i SLA				
WYZNACZNIK VII: AUDYT CYBERBEZPIECZEŃSTWA W RAMACH ZARZĄDZANIA BEZPIECZEŃSTWEM							
NAZWA WIĄZKI		**POZIOM 3**	**POZIOM 4**	**POZIOM 5**	**POZIOM 6**	**POZIOM 7**	**POZIOM 8**
		ZNA I ROZUMIE	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
		P3SCB_WVII1[1)]	**P4SCB_WVII1[1)]**	**P5SCB_WVII1[1)]**	**P6SCB_WVII1[1)]**	**P7SCB_WVII1[1)]**	**P8SCB_WVII1[1)]**
Zasady audytu cyberbezpieczeństwa	**WIEDZA**	cele i zakres działań audytu cyberbezpieczeństwa; rodzaje dokumentacji niezbędnej do przygotowania i przeprowadzenia audytu cyberbezpieczeństwa	procedury audytu cyberbezpieczeństwa; zasady klasyfikacji organizacji; zasadnicze różnice między sektorami, branżami i typami obiektów, w których jest przeprowadzony audyt cyberbezpieczeństwa; narzędzia wykorzystywane w audycie cyberbezpieczeństwa; wymagania związane z pozostałymi wymaganiami bezpieczeństwa, w tym bezpieczeństwa informacji i bezpieczeństwa fizycznego	rekomendacje organów właściwych dla poszczególnych sektorów, stanowiące punkt odniesienia dla audytu; wymagania nadrzędne dla podmiotów audytowanych; wpływ narzędzi audytowych na analizowany obiekt i jego ciągłość działania	wpływ narzędzi audytowych na stabilność pracy systemów złożonych	wpływ narzędzi audytowych na integralność subkomponentów pracujących w ramach systemów złożonych; zasady projektowania narzędzi audytowych	zasady projektowania i kierunki rozwoju specjalistycznych narzędzi audytowych
NAZWA WIĄZKI		**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**	**ZNA I ROZUMIE**
			P4SCB_WVII2[1)]	**P5SCB_WVII2[1)]**	**P6SCB_WVII2[1)]**	**P7SCB_WVII2[1)]**	**P8SCB_WVII2[1)]**
Zarządzanie zespołem audytowym	**WIEDZA**		role występujące w zespole audytowym ze względu na podstawowe różnice sektorowe	role występujące w zespole audytowym ze względu na szczegółowe różnice wewnątrz sektorów	role występujące w zespole audytowym ze względu na różnice specjalistyczne; podstawowe zasady zarządzania zespołem audytowym	zasady zarządzania zespołem audytowym, uwzględniające złożoność organizacji i wpływ na nią	kierunki rozwoju metod audytu
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
			P4SCB_UVII1[1)]	**P5SCB_UVII1[1)]**	**P6SCB_UVII1[1)]**	**P7SCB_UVII1[1)]**	**P8SCB_UVII1[1)]**

Przygotowanie audytu cyberbezpieczeństwa	**UMIEJĘTNOŚCI**		weryfikować spełnienie wymagań formalnych wynikających z zasad przyjętych w organizacji; opracować dokumenty potrzebne do audytu cyberbezpieczeństwa; zidentyfikować ryzyka w badanym obszarze	określać zasoby niezbędne do przeprowadzenia audytu w badanym zakresie; weryfikować spełnienie wymagań prawnych i formalnych przez organizację pod kątem charakteru prowadzonej działalności oraz posiadanej infrastruktury i wyposażenia; weryfikować spełnienie wymagań zgodności z normatywami, standardami i dobrymi praktykami; analizować wyniki poprzednich audytów, w tym zalecenia poaudytowe; uzgadniać plan audytu cyberbezpieczeństwa z organizacją	weryfikować spełnienie obowiązków prawnych i formalnych organizacji pod kątem wymagań nadrzędnych związanych z klasyfikacją organizacji; opracować plan audytu cyberbezpieczeństwa wraz z doborem próby; przygotować zestaw narzędzi do przeprowadzenia audytu	modyfikować zestaw narzędzi potrzebny do przeprowadzenia konkretnego audytu cyberbezpieczeństwa	projektować ekosystemy audytowe i narzędzia do jego przeprowadzenia w branżach, gdzie audyt cyberbezpieczeństwa jest zjawiskiem nowym
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_U.VII2[1)]	**P4SCB_UVII2[1)]**	**P5SCB_UVII2[1)]**	**P6SCB_UVII2[1)]**	**P7SCB_UVII2[1)]**	
Procedury kwalifikacji w audycie	**UMIEJĘTNOŚCI**	zbierać i weryfikować dokumentację projektową, podwykonawczą oraz instrukcje eksploatacyjne obiektu pod kątem zgodności stanu faktycznego z określonymi wymaganiami (DQ)	weryfikować zgodność dokumentacji projektowej, powykonawczej oraz instrukcji eksploatacyjnych z faktycznym ich wdrożeniem w obiekcie (IQ); opracować raport rozbieżności	weryfikować, czy zainstalowane lub zmodyfikowane urządzenie, oprogramowanie lub system działają zgodnie z założeniami podstawowymi grup funkcyjnych oraz systemów (OQ)	weryfikować, czy połączone grupy funkcyjne w określonym czasie i miejscu obiektu właściwie tworzą określony proces generacji oraz dostarczają określony produkt lub półprodukt (PQ)	dopasować działania audytowe do specjalistycznych wymagań konkretnych organizacji	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
		P3SCB_UVII3[1)]	**P4SCB_UVII3[1)]**	**P5SCB_UVII3[1)]**	**P6SCB_UVII3[1)]**	**P7SCB_UVII3[1)]**	**P8SCB_UVII3[1)]**
Przeprowadzenie audytu	**UMIEJĘTNOŚCI**	rozróżniać czynności dla trybu audytu, kontroli i oceny	przeprowadzać zadania audytowe zgodnie z programem; zabezpieczać materiał dowodowy	analizować wnioski z przeprowadzonego audytu oraz proponować rozwiązania; używać narzędzia do audytu cyberbezpieczeństwa zgodnie z ich przeznaczeniem;	opracować raport z audytu bezpieczeństwa wraz z rekomendacjami dotyczącymi niezgodności i obszarów do optymalizacji; określać zakres poszczególnych działań	przeprowadzić transfer wiedzy po dokonaniu audytu cyberbezpieczeństwa; w trakcie audytu elastycznie stosować nowe, niezbędne czynności audytowe, w tym	projektować nowe czynności audytowe

				przygotować raport z audytu bezpieczeństwa; przygotować protokół z kontroli	wynikających z audytu i przydzielać działania do realizacji poszczególnym komórkom organizacji	dobierać adekwatny zakres próby	
NAZWA WIĄZKI		**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**	**POTRAFI**
				P5SCB_UVII4[1)]	**P6SCB_UVII4[1)]**	**P7SCB_UVII4[1)]**	**P8SCB_UVII4[1)]**
Działania po audycie cyberbezpieczeństwa	**UMIEJĘTNOŚCI**			oceniać wdrożenie zaleceń przez jednostkę audytowaną po przeprowadzonym zadaniu audytowym	wdrażać wnioski i rekomendacje z audytu cyberbezpieczeństwa	implementować i nadzorować wdrażanie zasadniczych zmian wynikających z audytu cyberbezpieczeństwa	projektować rozwiązania po przeprowadzeniu audytu cyberbezpieczeństwa
WYZNACZNIK VIII: STANDARDY PRACY							
NAZWA WIĄZKI		**POZIOM 3**	**POZIOM 4**	**POZIOM 5**	**POZIOM 6**	**POZIOM 7**	**POZIOM 8**
		JEST GOTÓW DO	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**
		P3SCB_KSVIII1[1)]	**P4SCB_KSVIII1[1)]**	**P5SCB_KSVIII1[1)]**	**P6SCB_KSVIII1[1)]**	**P7SCB_KSVIII1[1)]**	
Kształtowanie postaw w obszarze cyberbezpieczeństwa	**KOMPETENCJE SPOŁECZNE**	przyjmowania odpowiedzialności za sposób użytkowania produktów i usług	postępowania zgodnie z zasadami i procedurami cyberbezpieczeństwa produktów, usług i organizacji	prowadzenia działań informacyjnych w celu podniesienia poziomu cyberodporonności w użytkowaniu produktów i usług	promowania i komunikowania działań na rzecz podnoszenia poziomu cyberodporności	promowania i kształtowania właściwych postaw w obszarze cyberbezpieczeństwa	
NAZWA WIĄZKI		**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**
				P5SCB_KSVIII2[1)]	**P6SCB_KSVIII2[1)]**		
Normy etyczne	**KOMPETENCJE SPOŁECZNE**			postępowania zgodnie z zasadami etyki zawodowej w cyberprzestrzeni; promowania zasad etycznych w cyberprzestrzeni	rozstrzygania dylematów etycznych związanych z zapewnieniem cyberbezpieczeństwa		

WYZNACZNIK IV: KOMUNIKACJA I WSPÓŁPRACA							
NAZWA WIĄZKI		**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**
			P4SCB_KSIX1[1)]	**P5SCB_KSIX1[1)]**	**P6SCB_KSIX1[1)]**	**P7SCB_KSIX1[1)]**	**P8SCB_KSIX1[1)]**
Odpowiedzialność	**KOMPETENCJE SPOŁECZNE**		świadomego przestrzegania zasad i procedur cyberbezpieczeństwa, z uwzględnieniem ewentualnych konsekwencji nierzetelnego wykonywania zadań	ponoszenia konsekwencji za nierzetelne wykonywanie zadań lub nieprzestrzegania zasad i procedur cyberbezpieczeństwa	promowania postawy odpowiedzialności za procesy zapewniania cyberbezpieczestwa	współtworzenia standardów zachowań projakościowych w obszarze cyberbezpieczeństwa; promowania kultury projakościowej w obszarze cyberbezpieczeństwa	kształtowania kultury projakościowej w obszarze cyberbezpieczeństwa
NAZWA WIĄZKI		**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**
			P4SCB_KSIX2[1)]	**P5SCB_KSIX2[1)]**	**P6SCB_KSIX2[1)]**	**P7SCB_KSIX2[1)]**	
Komunikacja	**KOMPETENCJE SPOŁECZNE**		komunikowania się z różnymi interesariuszami, w tym nieznającymi terminologii sektorowej, w sposób dla nich zrozumiały	komunikowania się w sytuacjach dużego stresu i ryzyka, w tym podczas wystąpienia incydentu bezpieczeństwa; komunikowania współpracownikom ich ról i odpowiedzialności w procesach cyberbezpieczeństwa w organizacji	przedstawiania i uzasadniania zasad funkcjonowania systemu cyberbezpieczeństwa osobom zarządzającym, z uwzględnieniem zakresu ich odpowiedzialności	komunikowania się w międzynarodowym środowisku, z uwzględnieniem różnic kulturowych	
NAZWA WIĄZKI		**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**
			P4SCB_KSIX3[1)]	**P5SCB_KSIX3[1)]**	**P6SCB_KSIX3[1)]**		
Relacje, zachowania, reakcje	**KOMPETENCJE SPOŁECZNE**		ścisłej i efektywnej współpracy z interesariuszami w zadaniach związanych z zapewnieniem cyberbezpieczeństwa;	zmian rozwiązań technicznych i organizacyjnych w systemie cyberbezpieczeństwa; adaptacji w zmieniających się uwarunkowaniach sektora cyberbezpieczeństwa	podejmowania decyzji w zmiennych, nietypowych warunkach w sytuacji wystąpienia incydentu bezpieczeństwa, w warunkach niepełnej informacji i wysokiego ryzyka		

			właściwego działania w warunkach stresowych				
NAZWA WIĄZKI		**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**	**JEST GOTÓW DO**
			P4SCB_KSIX4[1)]	**P5SCB_KSIX4[1)]**			
Prywatność i anonimowość w internecie	**KOMPETENCJE SPOŁECZNE**		korzystania z portali społecznościowych w sposób pozwalający na zachowanie anonimowości i prywatności	zarządzania informacjami na swój temat w internecie			