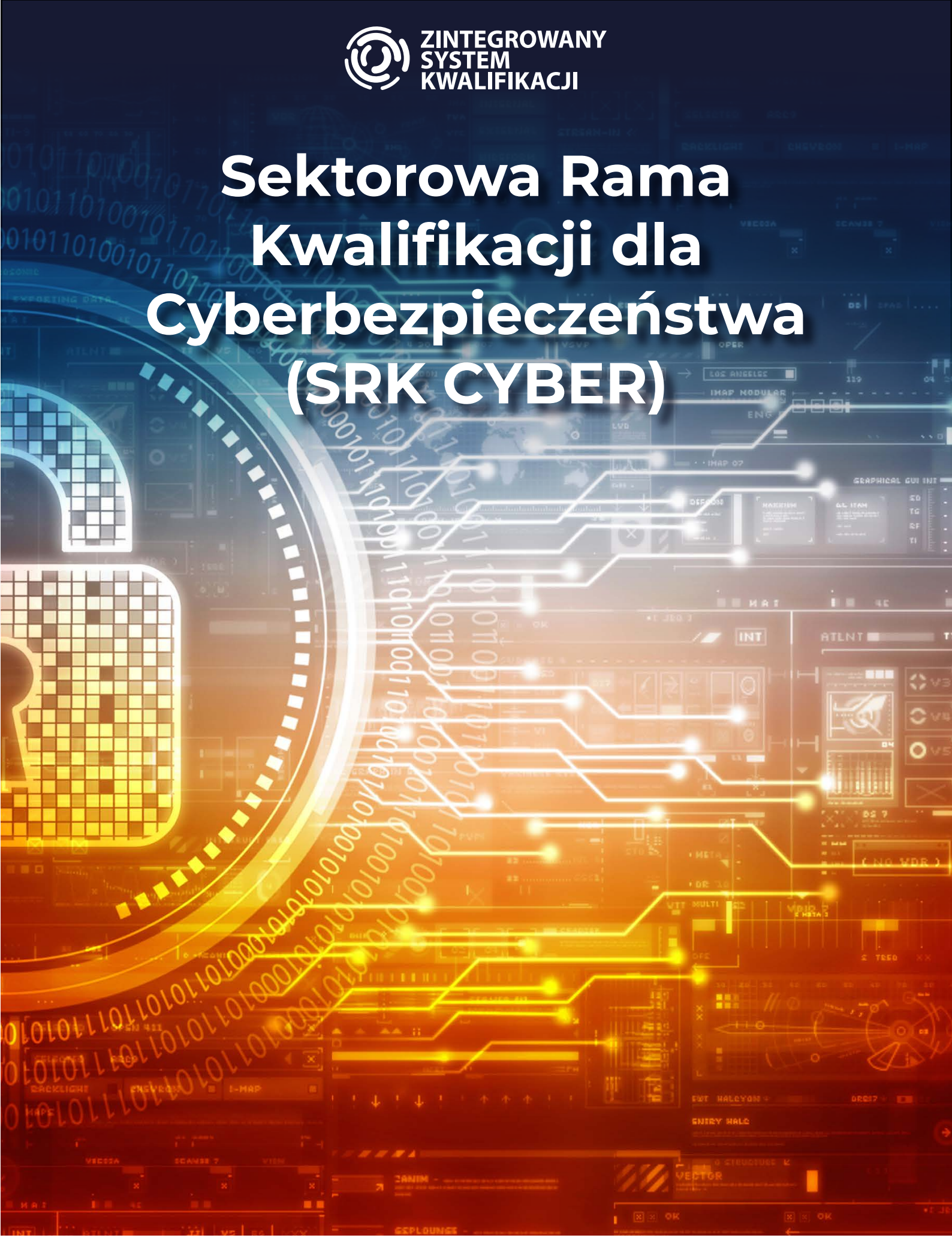
ZINTEGROWANY SYSTEM KWALIFIKACJI

Sektorowa Rama Kwalifikacji dla Cyberbezpieczeństwa (SRK CYBER)



Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
IBE kwalifikacje dla każdego
Unia Europejska Europejski Fundusz Społeczny

Autorzy:
Edyta Cieszkowska, Andrzej Cieślak, Monika Drzymulska-Derda, dr Dawid Dymkowski, dr inż. Przemysław Jatkiewicz, Łukasz Jaworski, Tomasz Klekowski, dr inż. Rafał Kołodziejczyk, Beata Ostrowska, Mateusz Panowicz, Damian Parol, Mateusz Przywara, Dariusz Słomkowski, Sławomir Smugowski, Dawid Suder

Redakcja językowa: Elżbieta Łanik, Monika Niewielska

Projekt okładki i skład: Wojciech Maciejczyk

Zdjęcie na okładce: Shutterstock.com

ISBN: 978-83-67385-62-6

Wzór cytowania: Cieszkowska, E., Cieślak, A., Drzymulska-Derda, M., Dymkowski, D., dr inż. Jatkiewicz, P., Jaworski, Ł., Klekowski, T., Kołodziejczyk, R., Ostrowska, B., Panowicz, M., Parol, D., Przywara, M., Słomkowski, D., Smugowski, S., Suder, D. (2023). *Sektorowa Rama Kwalifikacji dla Cyberbezpieczeństwa*. Instytut Badań Edukacyjnych.

Wydawca:
Instytut Badań Edukacyjnych
ul. Górczewska 8
01-180 Warszawa
www.ibe.edu.pl

IBE INSTYTUT BADAŃ EDUKACYJNYCH

Publikacja powstała w ramach realizacja projektu systemowego „Wspieranie funkcjonowania i doskonalenie ZSK na rzecz wykorzystania oferowanych w nim rozwiązań do realizacji celów strategii rozwoju kraju" współfinansowanego ze środków Europejskiego Funduszu Społecznego.

Egzemplarz bezpłatny

Spis treści

Definicja sektora 4

Instrukcja korzystania z Sektorowej Ramy Kwalifikacji dla Cyberbezpieczeństwa 5

Możliwości wykorzystania Sektorowej Ramy Kwalifikacji dla Cyberbezpieczeństwa w praktyce 8

Sektorowa Rama Kwalifikacji dla Sektora Cyberbezpieczeństwa 11

Słownik pojęć stosowanych w Sektorowej Ramie Kwalifikacji dla Cyberbezpieczeństwa 43

Definicja sektora

Sektor cyberbezpieczeństwa obejmuje podmioty/organizacje/osoby prowadzące działania w celu ochrony systemów informacyjnych, usług i produktów przed cyberzagrożeniami dla zapewnienia niezakłóconego funkcjonowania podmiotów/organizacji/osób.

Przez **cyberzagrożenia** rozumie się wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę w systemach, usługach, produktach, spowodować zakłócenia w nich lub w inny sposób niekorzystnie wpłynąć na nie oraz ich interesariuszy.

Działania w celu ochrony systemów, usług i produktów rozumie się jako czynności wykonywane na etapach identyfikacji, ochrony, wykrywania, reakcji, odbudowy procesu cyberbezpieczeństwa oraz audytu; działania te realizowane są zarówno podczas wdrażania systemu, usługi lub produktu, ich eksploatacji, jak i wycofania tego systemu, usługi lub produktu z użytkowania.

System informacyjny rozumie się jako strukturę obejmującą komponenty techniczne i organizacyjne, pozwalającą na przetwarzanie informacji.

Instrukcja korzystania z Sektorowej Ramy Kwalifikacji dla Cyberbezpieczeństwa

Sektorowa Rama Kwalifikacji dla Sektora Cyberbezpieczeństwa (SRK CYBER) to uporządkowany zestaw kompetencji specyficznych dla sektora cyberbezpieczeństwa. Kompetencje w SRK CYBER podzielone zostały na 9 następujących wyznaczników sektorowych tj. głównych obszarów działalności sektora:

Wstępne wymagania dla cyberbezpieczeństwa
Identyfikacja
Ochrona
Wykrywanie
Reakcja
Odbudowa
Audyt cyberbezpieczeństwa w ramach zarządzania bezpieczeństwem
Standardy pracy
Komunikacja i współpraca

Z uwagi na fakt, że struktura sektorowych ram kwalifikacji nie uwzględnia konkretnych rozwiązań biznesowych, SRK CYBER jest uniwersalnym narzędziem do zarządzania kompetencjami w branży. Wśród wielu funkcjonalności tego narzędzia wymienia się m.in. wyszukiwanie kompetencji w poszczególnych obszarach i procesach sektora oraz wyszukiwanie konkretnych kompetencji w SRK CYBER.

Wyszukiwanie kompetencji w poszczególnych obszarach i procesach sektora

KROK 1:

Zapoznaj się z definicją sektora i zastanów, czy poszukiwany obszar, proces należą do sektora.

KROK 2:

Wybierz odpowiedni wyznacznik sektorowy.

KROK 3:

Wyznaczniki sektorowe składają się z wiązek kompetencji, tj. procesów, podprocesów charakterystycznych dla sektora. W zależności od rodzaju kompetencji podzielone są one na poszczególne kategorie: wiedza (zna i rozumie…), umiejętności (potrafi…) lub kompetencje społeczne (jest gotów do…).

Wybierz odpowiednie wiązki kompetencji. Pamiętaj, że często dopiero połączenie wiązek z obszaru wiedzy oraz umiejętności pozwala w pełni opisać określony proces.

KROK 4:

W wybranych wiązkach znajdują się poszukiwane kompetencje ułożone zgodnie ze stopniem ich złożoności (im wyższy poziom, tym większy stopień złożoności) opisujące określony proces (nazwa wiązki) występujący w sektorze.

Co ważne, kompetencje w SRK CYBER na poszczególnych poziomach odpowiadają poziomom (1–8) Polskiej Ramy Kwalifikacji II stopnia o charakterze zawodowym.

Wyszukiwanie konkretnych kompetencji w SRK CYBER

KROK 1:

Zapoznaj się z definicją sektora i zastanów się, czy kompetencja, której szukasz, wchodzi w jej zakres.

KROK 2:

Przypisz poszukiwaną przez siebie kompetencję do jednego z wyznaczników sektorowych.

KROK 3:

W zależności od rodzaju poszukiwanej kompetencji poruszaj się w odpowiedniej kategorii kompetencji tego wyznacznika: wiedzy (zna i rozumie…), umiejętności (potrafi…) lub kompetencji społecznych (jest gotów do…).

KROK 4:

Wyznaczniki sektorowe są podzielone na wiązki kompetencji, tj. zbiory kompetencji powiązanych ze sobą tematycznie, tworzących logiczny ciąg zapisów o rosnącym stopniu złożoności. Przypisz poszukiwaną przez siebie kompetencję do wiązki kompetencji, która znajduje się w wybranym wyznaczniku sektorowym.

KROK 5:

Znajdź wyszukiwaną przez siebie kompetencję na poziomach od 3 do 8 SRK CYBER. Jeśli nie możesz znaleźć poszukiwanej kompetencji, to być może nie jest ona kompetencją specyficzną dla sektora cyberbezpieczeństwa, tylko jest: kompetencją przekrojową (vide: Polska Rama Kwalifikacji II stopnia o charakterze zawodowym), kompetencją z pokrewnego sektora (np. SRK dla IT lub Telekomunikacji) lub została zaszyta w innych komórkach ramy (wtedy powtórz kroki 1–4).

KROK 6:

W miarę potrzeb doprecyzuj zapisy znalezionej kompetencji.

KROK 7:

Przepisz kod znajdujący się przy znalezionej kompetencji. W ten sposób łatwiej będzie Ci znaleźć ją następnym razem. Przykładowo kod P3SCB_UII5(2) wskazuje kompetencje „(potrafi) określać procesy krytyczne" znajdującą się w wyznaczniku „Identyfikacja", w wiązce „Identyfikacja aktywów procesowych organizacji" SRK CYBER. Poszczególne elementy kodu oznaczają:

- P3 – poziom 3 kompetencji,
- SCB – symbol Sektorowej Ramy Kwalifikacji dla Sektora Cyberbezpieczeństwa,
- U – kompetencja z obszaru umiejętność; analogicznie symbol W oznacza wiedzę, a KS kompetencje społeczne,
- II – liczba rzymska oznaczająca drugi wyznacznik ramy,
- 5 – liczba arabska oznaczająca piątą wiązkę z obszaru umiejętności danego wyznacznika,
- (2) – w przypadku, gdy w danym polu SRK CYBER znajduje się kilka kompetencji, dopisujemy w nawiasie liczbę porządkową.

Jednym z elementów SRK CYBER jest słownik pojęć stosowanych w ramie, w którym wyjaśniono pojęcia niejednoznaczne lub specjalistyczne. Znajduje się on na str. 43.

Możliwości wykorzystania Sektorowej Ramy Kwalifikacji dla Cyberbezpieczeństwa w praktyce

Sektorowa Rama Kwalifikacji dla Cyberbezpieczeństwa to uniwersalne narzędzie do zarządzania kompetencjami w sektorze cyberbezpieczeństwa. Dzięki temu, że budowa SRK CYBER nie narzuca określonych rozwiązań biznesowych, może być wykorzystywana w dowolny sposób przez wielu różnych odbiorów.

Pracodawcy

Za pomocą SRK CYBER pracodawcy mogą szerzej spojrzeć na kompetencje branżowe występujące w swoim środowisku biznesowym, a dzięki temu efektywniej zarządzać zasobami ludzkimi i skuteczniej konkurować na rynku pracy. Do największych zalet wynikających z korzystania z tego narzędzia zalicza się wsparcie w procesach analizy luk kompetencyjnych branży czy firmy, planowania rozwoju zasobów ludzkich oraz siatki płacowej ich stanowisk, a także rekrutacji i selekcji personelu.

Tabela kompetencji pozwoliła mi określić kryteria rekrutacji pracowników w oparciu o kluczowe kompetencje w branży, a także przygotować opisy stanowisk pracy.

Pracownik działu HR w dużym przedsiębiorstwie

Po zidentyfikowaniu głównych luk kompetencyjnych w branży rozpoczęliśmy program praktyk zawodowych, które mają za zadanie przygotować naszych uczniów do efektywnego wejścia na rynek pracy tuż po zakończeniu edukacji.

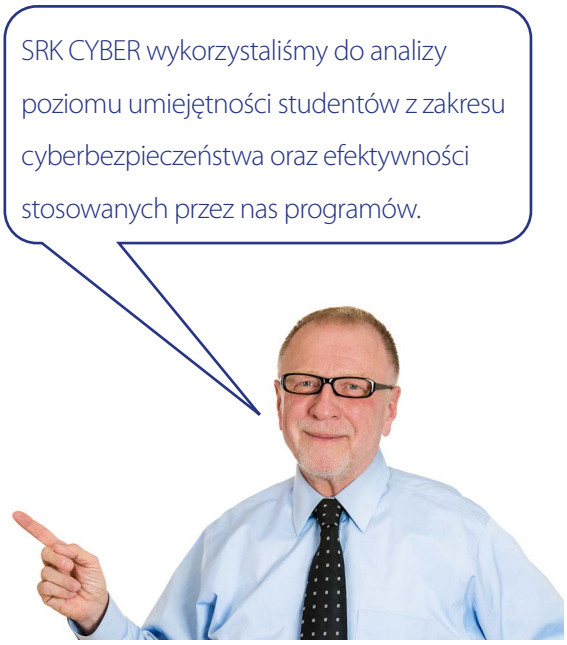
Dyrektor szkoły branżowej

Szkoły i placówki oświatowe

W oparciu o SRK CYBER szkoły i placówki oświatowe mogą dostosowywać realizowane programy nauczania do aktualnych i realnych potrzeb rynku pracy. Oznacza to, że tabela kompetencji wspiera te podmioty przy poszerzaniu i modyfikacji realizowanych programów nauczania oraz uzupełnianiu luk kompetencyjnych uczniów, np. dotyczących umiejętności praktycznych czy miękkich. Dodatkowo może być przydatna w doradztwie zawodowym dla uczniów czy monitorowaniu sukcesów absolwentów szkół.

Uczelnie wyższe

SRK CYBER jest narzędziem, które wspiera uczelnie wyższe w dopasowaniu programów kierunku studiów do bieżących trendów w rozwoju branży. Dzięki temu studenci mogą być lepiej przygotowani do wejścia na rynek pracy i osiągnięcia sukcesu zawodowego. Tabele kompetencji umożliwiają także monitorowanie postępów studentów oraz ocenę efektywności programów kierunków studiów.



Rektor uczelni wyższej

Właścicielka firmy szkoleniowej

Firmy szkoleniowe

Firmy szkoleniowe, przy wykorzystaniu SRK CYBER, mogą skutecznie projektować specjalistyczne szkolenia, dzięki czemu są w stanie przygotować ofertę szytą na miarę potrzeb konkretnej branży oraz oczekiwań swoich klientów. Przy pomocy sektorowej ramy kwalifikacji mogą wybierać poszczególne kompetencje i dobierać je do efektów danego programu szkoleniowego. Mogą także przygotowywać egzaminy weryfikujące zdobytą wiedzę, umiejętności oraz kompetencje społeczne. Dzięki gradacji złożoności kompetencji w SRK CYBER łatwiej im również przygotowywać ofertę szkoleniową z podziałem na różne poziomy zaawansowania.

Interesariusze ZSK

Wśród szerokiego grona odbiorców ZSK, grupy, które w największym stopniu mogą skorzystać na opracowanej SRK CYBER, to organizacje branżowe oraz osoby opisujące kwalifikacje wolnorynkowe lub sektorowe. Zadaniem tych pierwszych jest m.in. nawiązywanie porozumień edukacyjnych zacieśniających współpracę pomiędzy szkołami a pracodawcami oraz przekazywanie informacji na temat zapotrzebowania na kompetencje sektorowe instytucjom edukacyjnym lub instytucjom rynku pracy. Z kolei osoby opisujące kwalifikacje wolnorynkowe i sektorowe mogą korzystać z przygotowanego materiału w celu łatwiejszego definiowania zestawów efektów uczenia się.

Inne podmioty

SRK CYBER może być wykorzystywana do wielu innych celów w zależności od aktualnych potrzeb branży. W przypadku sektora cyberbezpieczeństwa może to być narzędzie pomocnicze do przygotowania materiałów weryfikujących wiedzę pracowników danej firmy dotyczącą zagrożeń w internecie, gdyż współcześnie każdy pracownik jest narażony na atak w cyberprzestrzeni. Weryfikacja jego podstawowych kompetencji z zakresu cyberbezpieczeństwa może ustrzec firmę przed negatywnymi konsekwencjami w przyszłości.
Co więcej, aktualnie sektor cyberbezpieczeństwa boryka się z niedoborem pracowników. Sektorowa Rama Kwalifikacji dla Cyberbezpieczeństwa może posłużyć do przekwalifikowania się i rozpoczęcia kariery zawodowej osób z bliskich merytorycznie sektorów, np. IT.

Menedżer zespołu IT

Sektorowa Rama Kwalifikacji dla Cyberbezpieczeństwa

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Wstępne wymagania dla cyberbezpieczeństwa**	Dane	**P3SCB_WI1**	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	**P4SCB_WI1**	zasady i protokoły wymiany danych zasady łączenia danych z granicami procesów realizowanych w ramach obiektów lub pomiędzy nimi możliwości narzędzi wykorzystywanych do przetwarzania danych metody zabezpieczania danych przed uszkodzeniem i wyciekiem uwarunkowania zewnętrzne potrzebne do przekazania danych	**P5SCB_WI1**	zasady modelu danych w systemach informatycznych narzędzia do tworzenia i modyfikacji baz danych	**P6SCB_WI1**	model odniesienia IACS				
		Systemy komunikacji			**P4SCB_WI2**	założenia komunikacji analogowej założenia komunikacji cyfrowej	**P5SCB_WI2**	metody kompozycji i dekompozycji systemów komunikacji	**P6SCB_WI2**	zależności pomiędzy komponentami w systemach komunikacji				
		Architektura komunikacji			**P4SCB_WI3**	architekturę i strukturę sieci teleinformatycznych, w tym model odniesienia ISO/OSI	**P5SCB_WI3**	zasady eksploatacji sieci teleinformatycznych i zarządzania nimi	**P6SCB_WI3**	zasady zachowania zgodności w sieciach teleinformatycznych				
		Rodzaje środowisk cyfrowych	**P3SCB_WI4**	rodzaje środowisk cyfrowych i złożonych systemów	**P4SCB_WI4**	metody przenoszenia danych pomiędzy urządzeniami pracującymi w środowisku cyfrowym	**P5SCB_WI4**	założenia poszczególnych rodzajów środowisk cyfrowych	**P6SCB_WI4**	metody przenoszenia danych pomiędzy różnymi niezależnymi środowiskami cyfrowymi				
		Systemy urządzeń elektronicznych	**P3SCB_WI5**	elementy składające się na obszar IT elementy składające się na obszar OT elementy składające się na obszar IoT	**P4SCB_WI5**	specyficzne uwarunkowania obszaru IT specyficzne uwarunkowania obszaru OT specyficzne uwarunkowania obszaru IoT	**P5SCB_WI5**	zależności pomiędzy IT, OT i IoT						

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Wstępne wymagania dla cyberbezpieczeństwa**	Architektura systemów operacyjnych			**P4SCB_WI6**	architekturę systemów operacyjnych, w tym sieciowych zasady uruchomienia systemu operacyjnego, w tym sieciowego	**P5SCB_WI6**	metody wirtualizacji systemów operacyjnych	**P6SCB_WI6**	metody konteneryzacji aplikacji	**P7SCB_WI6**	metody orkiestracji kontenerów		
		Skrypty i aplikacje	**P3SCB_WI7**	metody uruchomienia poszczególnych skryptów na wybranych systemach operacyjnych przynajmniej jeden język skryptowy	**P4SCB_WI7**	podstawowe zasady programowania obiektowego metody uruchomienia oprogramowania opartego na różnych językach skryptowych w jednym środowisku uruchomieniowym	**P5SCB_WI7**	możliwości wykorzystania gotowych bibliotek w projekcie otoczenie programowe aplikacji, w tym możliwość integracji z narzędziami zewnętrznymi	**P6SCB_WI7**	wzorce projektowe metody tworzenia aplikacji webowych metody tworzenia aplikacji mobilnych metody tworzenia aplikacji desktopowych zasady zachowania ciągłości działania aplikacji	**P7SCB_WI7**	metody tworzenia innowacyjnych bibliotek programistycznych		
		Narzędzia wykorzystujące sztuczną inteligencję w systemach cyberbezpieczeństwa	**P3SCB_WI8**	metody związane z wykorzystaniem sztucznej inteligencji	**P4SCB_WI8**	cechy systemów sztucznej inteligencji, zasady ich funkcjonowania i ograniczenia	**P5SCB_WI8**	grupy zastosowań sztucznej inteligencji w organizacji grupy zastosowań sztucznej inteligencji w obszarze cyberbezpieczeństwa formalne wymagania w zakresie systemów sztucznej inteligencji						
		Prawo, normy i standardy krajowe, unijne i międzynarodowe	**P3SCB_WI9**	podstawowe zasady organizacji systemu cyberbezpieczeństwa	**P4SCB_WI9**	zasady, procedury i wymagania dotyczące bezpieczeństwa organizacji obowiązki raportowania o incydentach dotyczących infrastruktury krytycznej	**P5SCB_WI9**	regulacje prawne określające wymagania dotyczące cyberbezpieczeństwa krajowe normy dotyczące cyberbezpieczeństwa dobre praktyki w obszarze cyberbezpieczeństwa	**P6SCB_WI9**	międzynarodowe normy i standardy cyberbezpieczeństwa międzynarodowe standardy audytu wewnętrznego międzynarodowe standardy etyki zawodowej audytorów	**P7SCB_WI9**	zasady i procedury ochrony własności przemysłowej i prawa autorskiego		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Wstępne wymagania dla cyberbezpieczeństwa**	Ochrona danych osobowych	**P3SCB_WI10**	podstawowe zagadnienia dotyczące ochrony danych osobowych	**P4SCB_WI10**	zasady, procedury i wymagania ochrony danych osobowych obowiązki raportowania o incydentach związanych z bezpieczeństwem danych osobowych	**P5SCB_WI10**	regulacje prawne dotyczące ochrony danych osobowych						
		Budowanie świadomości dotyczącej cyberbezpieczeństwa	**P3SCB_WI11**	podstawowe terminy związane z cyberbezpieczeństwem zasady cyberbezpieczeństwa obowiązujące na danym stanowisku pracy	**P4SCB_WI11**	zasady cyberbezpieczeństwa dla organizacji i społeczeństwa	**P5SCB_WI11**	metody i techniki zabezpieczania infrastruktury i usług system certyfikacji w sektorze cyberbezpieczeństwa rolę organizacji zajmujących się cyberbezpieczeństwem na poziomie krajowym	**P6SCB_WI11**	rolę organizacji zajmujących się cyberbezpieczeństwem na poziomie międzynarodowym	**P7SCB_WI11**	trendy w obszarze cyberbezpieczeństwa		
Potrafi:														
UMIEJĘTNOŚCI:	**Wstępne wymagania dla cyberbezpieczeństwa**	Opracowanie specyfikacji zamówienia	**P3SCB_UI1**	przeprowadzić rozeznanie rynku pod kątem pożądanych cech i parametrów	**P4SCB_UI1**	określić parametry i funkcjonalności do specyfikacji warunków zamówienia	**P5SCB_UI1**	określić warunki dostawy towarów i usług	**P6SCB_UI1**	przewidzieć ryzyka, jakie mogą wystąpić w trakcie realizacji umowy				
		Systemy monitorowania, kontroli, raportowania, wizualizacji, reakcji (SOC)	**P3SCB_UI2**	weryfikować sytuacje pod kątem false positive (poziom 1 SOC)	**P4SCB_UI2**	wspierać utrzymanie ciągłości działania zarządzanego obiektu w przypadku wystąpienia anomalii (poziom 1 SOC)	**P5SCB_UI2**	analizować źródła danych, protokoły, procesy zasad działania obiektów i systemów (poziom 2 SOC wykorzystać narzędzia do analizy stabilności działania, integralności systemów, korelacji zdarzeń, korelacji danych (poziom 2 SOC)	**P6SCB_UI2**	opracować głęboką analitykę danych oraz ich wzajemne relacje (poziom 2 SOC) budować komponenty rozszerzeń systemu bezpieczeństwa (poziom 2 SOC)	**P7SCB_UI2**	opracować systemowe rozwiązania przeciwdziałające wystąpieniu anomalii i ich konsekwencji (poziom 3 SOC)		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Wstępne wymagania dla cyberbezpieczeństwa**	Przetwarzanie danych	**P3SCB_UI3**	określać pochodzenie i miejsce docelowe danych dobierać odpowiednie źródła danych zależnie od systemu dokonywać selekcji danych oraz porządkować je wizualizować dane	**P4SCB_UI3**	przetwarzać dane w systemach jednolitych parsować dane	**P5SCB_UI3**	monitorować rozproszone, nienadające się do zarządzania skrypty przetwarzania danych weryfikować warunki przesyłania danych pod kątem ich bezpieczeństwa	**P6SCB_UI3**	opracować proste programy rozwiązujące problemy z przetwarzaniem danych implementować dane z wielu miejsc	**P7SCB_UI3**	przetwarzać dane w rozproszonym środowisku		
		Korelacja danych	**P3SCB_UI4**	porównać próbkę informacji z określoną sygnaturą budować informację opartą na pozyskanych danych	**P4SCB_UI4**	dokonać korelacji danych przy pomocy dostępnego oprogramowania	**P5SCB_UI4**	napisać korelator w wybranym języku programowania	**P6SCB_UI4**	opracować informacje i możliwe scenariusze na określonym obiekcie za pomocą matrycy korelacyjnej	**P7SCB_UI4**	zaprojektować model środowiska na podstawie przetwarzanych danych		
		Komunikacja i wymiana danych	**P3SCB_UI5**	wyszukać informacje dotyczące komunikacji i wymiany danych identyfikować komponenty w wymianie danych pomiędzy obiektami posługiwać się aplikacjami do komunikacji i wymiany danych	**P4SCB_UI5**	określić granice transmisji danych klasyfikować zestaw danych według określonych kryteriów	**P5SCB_UI5**	analizować informacje dotyczące komunikacji i wymiany danych zarządzać infrastrukturą komunikacyjną	**P6SCB_UI5**	projektować infrastrukturę komunikacyjną	**P7SCB_UI5**	projektować standardy wymiany danych		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Potrafi:														
UMIEJĘTNOŚCI:	**Wstępne wymagania dla cyberbezpieczeństwa**	Specjalistyczne słownictwo branżowe w językach polskim i angielskim					**P5SCB_UI6**	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	**P6SCB_UI6**	stosować specjalistyczne słownictwo podczas komunikacji w języku angielskim korzystać ze specjalistycznej literatury w języku angielskim	**P7SCB_UI6**	komunikować się w międzynarodowym środowisku biznesowym	**P8SCB_UI6**	komunikować się w międzynarodowym środowisku naukowym
		Środowisko testowe, developerskie, produkcyjne			**P4SCB_UI7**	przeprowadzać testy w środowisku testowym lub developerskim	**P5SCB_UI7**	projektować testy w środowisku testowym lub developerskim przeprowadzić testy w środowisku produkcyjnym z możliwością zatrzymania obiektów testowania	**P6SCB_UI7**	przeprowadzić testy w środowisku produkcyjnym w środowisku pracy ciągłej	**P7SCB_UI7**	projektować testy w środowisku produkcyjnym		
		Zarządzanie środowiskiem zwirtualizowanym					**P5SCB_UI8**	stworzyć i zarządzać maszyną wirtualną dobrać odpowiednie zastosowanie chmurowe instalować i zarządzać hypervisorem	**P6SCB_UI8**	konteneryzować aplikacje rekomendować zabezpieczenia skonteneryzowanych aplikacji	**P7SCB_UI8**	orkiestrować kontenery tworzyć środowisko maszyn wirtualnych działających w trybie wysokiej dostępności (HA)		
		Tworzenie skryptów i aplikacji	**P3SCB_UI9**	tworzyć proste skrypty	**P4SCB_UI9**	tworzyć skrypty oparte na zewnętrznych bibliotekach	**P5SCB_UI9**	implementować wzorce projektowe w aplikacjach wykorzystywać frameworki frontendowe	**P6SCB_UI9**	tworzyć aplikacje webowe tworzyć aplikacje mobilne tworzyć aplikacje desktopowe łączyć poszczególne komponenty w celu stworzenia systemu				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Wstępne wymagania dla cyberbezpieczeństwa**	Zarządzanie środowiskiem uruchomieniowym aplikacji	**P3SCB_UI10**	sprawdzać zgodność systemów operacyjnych	**P4SCB_UI10**	identyfikować nieprawidłowości funkcjonowania systemów zachowywać środki ostrożności niedopuszczające do destabilizacji systemów	**P5SCB_UI10**	reagować na błędy aplikacji występujące po aktualizacji systemów operacyjnych	**P6SCB_UI10**	analizować skutki aktualizacji środowiska uruchomieniowego na aplikację				
		Rozwój własny			**P4SCB_UI11**	wybrać własną ścieżkę rozwoju korzystać z programów szkoleniowych w zakresie cyberbezpieczeństwa realizowanych w swojej organizacji	**P5SCB_UI11**	wyszukiwać i korzystać ze szkoleń zewnętrznych z zakresu cyberbezpieczeństwa wykorzystać różne źródła wiedzy, w tym źródła alternatywne pozyskiwać wiedzę na temat nowości sektorowych z różnych źródeł rozwijać umiejętności z zakresu języka sektorowego, w tym w języku angielskim						
		Wspieranie rozwoju innych osób			**P4SCB_UI12**	prowadzić szkolenia z zakresu cyberbezpieczeństwa opracować szkolenia podstawowe z zakresu cyberbezpieczeństwa	**P5SCB_UI12**	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	**P6SCB_UI12**	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	**P7SCB_UI12**	przekazywać swoją wiedzę i doświadczenie w różnorodnych formach, w tym podczas spotkań sektorowych projektować plan rozwoju pracowników projektować system zarządzania kompetencjami pracowników	**P8SCB_UI12**	projektować programy szkoleniowe z cyberbezpieczeństwa dla organizacji

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Identyfikacja**	Kontekst wewnętrzny i zewnętrzny organizacji	**P3SCB_WII1**	terminy mikro- i makroekonomiczne niezbędne do wykonywania zadań w organizacji	**P4SCB_WII1**	standardy biznesowe obowiązujące w organizacji strukturę organizacyjną i główne procesy organizacji zasady działania różnych typów podmiotów, w tym przedsiębiorstw, instytucji publicznych, organizacji pozarządowych	**P5SCB_WII1**	oczekiwania podmiotów zewnętrznych wobec usług i produktów organizacji	**P6SCB_WII1**	zasady tworzenia, wdrażania nowych procesów biznesowych zasady optymalizacji wdrożonych procesów biznesowych	**P7SCB_WII1**	zasady, procesy i przedział czasowy (timeline) tworzenia standardów, regulacji oraz prawa z uwzględnieniem kontekstu sektora/ organizacji		
		Łańcuch dostaw i wartości			**P4SCB_WII2**	model łańcucha dostaw organizacji	**P5SCB_WII2**	model łańcucha wartości organizacji						
		Ryzyka w organizacji	**P3SCB_WII3**	potencjalne ryzyka dla organizacji, w tym źródła ryzyk metody dokumentowania potencjalnych ryzyk w organizacji znaczenie monitoringu ryzyk dla cyberbezpieczeństwa	**P4SCB_WII3**	metody i narzędzia służące do identyfikacji ryzyk w organizacji potrzeby interesariuszy w zakresie monitoringu ryzyk	**P5SCB_WII3**	metody, narzędzia oraz rozwiązania organizacyjne stosowane w celu przeciwdziałania wystąpieniu ryzyk w organizacji	**P6SCB_WII3**	wpływ wystąpienia poszczególnych ryzyk na poziom zagrożenia w przedsiębiorstwie	**P7SCB_WII3**	kierunki rozwoju metod, narzędzi oraz rozwiązań organizacyjnych dotyczących przeciwdziałania wystąpieniu w organizacji ryzyk i ich minimalizacji	**P8SCB_WII3**	najnowsze rozwiązania w zakresie metod, narzędzi oraz rozwiązań organizacyjnych zabezpieczających przed potencjalnym ryzykiem w organizacji
		Wewnętrzne i zewnętrzne procesy, produkty i usługi w organizacji			**P4SCB_WII4**	wymagania związane z cyberbezpieczeństwem w odniesieniu do procesów, produktów i usług w organizacji i poza nią oraz osób za nie odpowiedzialnych	**P5SCB_WII4**	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	**P6SCB_WII4**	zasady zarządzania zmianą i implementacji nowych sposobów organizacji pracy na poziomie zespołu/działu	**P7SCB_WII4**	wpływ ograniczeń finansowych na wdrażanie rozwiązań spełniających wymagania cyberbezpieczeństwa zasady zarządzania zmianą i implementacji nowych sposobów organizacji pracy na poziomie całej organizacji		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Identyfikacja**	Aktywa w organizacji	**P3SCB_WII5**	rodzaje aktywów w organizacji	**P4SCB_WII5**	rozwiązania stosowane w organizacji	**P5SCB_WII5**	potencjalne zależności pomiędzy 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						
		Zasady projektowania i konsekwencje wyboru technologii dla produktów i usług w ich cyklu życia			**P4SCB_WII6**	rolę cyberbezpieczeństwa w projektowaniu produktów i usług z perspektywy ich cyklu życia	**P5SCB_WII6**	wymagania funkcjonalne i niefukcjonalne odnoszące się do produktów i usług	**P6SCB_WII6**	konsekwencje dla cyberbezpieczeństwa w przypadku zastosowania określonych technologii i narzędzi w perspektywie cyklu życia produktów i usług	**P7SCB_WII6**	zasady integracji wymagań cyberbezpieczeństwa w tworzeniu nowych produktów i usług oraz cyklu ich życia	**P8SCB_WII6**	wymagania cyberbezpieczeństwa w procesie tworzenia i rozwoju technologii
Potrafi:														
UMIEJĘTNOŚCI:	**Identyfikacja**	Identyfikacja komponentów, zdarzeń, obiektów			**P4SCB_UII1**	dobierać narzędzia, procedury i procesy do identyfikacji znanych obiektów, w tym ich cech charakterystycznych oraz grup obiektów wprowadzać korekty do wyników identyfikacji	**P5SCB_UII1**	profilować znane obiekty lub grupy obiektów rozszerzać zapisy profilu o nowe cechy	**P6SCB_UII1**	dobierać narzędzia, procedury i procesy do identyfikacji nieznanych obiektów i grup obiektów profilować systemy, środowiska fizyczne wizualizować środowiskowo w układzie statycznym i dynamicznym	**P7SCB_UII1**	profilować nieznane obiekty lub grupy obiektów profilować obiekty eteryczne przeprowadzać identyfikację głęboką dla protokołów komunikacyjnych i stosów protokołów budować narzędzia identyfikacji ze znanych rozwiązań	**P8SCB_UII1**	budować narzędzia identyfikacji systemów złożonych i ich powiązań między systemami

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Identyfikacja**	Usługi katalogowe	**P3SCB_UII2**	wykorzystywać usługi katalogowe do identyfikacji aktywów organizacji	**P4SCB_UII2**	wykorzystywać usługi katalogowe do gromadzenia informacji o aktywach w organizacji	**P5SCB_UII2**	konfigurować usługi katalogowe, w tym określać zasady postępowania z obiektami						
		Identyfikacja aktywów ludzkich organizacji	**P3SCB_UII3**	identyfikować kluczowe osoby w poszczególnych procesach	**P4SCB_UII3**	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	**P5SCB_UII3**	identyfikować krytyczne role osób w organizacji identyfikować istotne powiązania pomiędzy kluczowymi osobami	**P6SCB_UII3**	opracowywać wymagania cyberbezpieczeństwa, które muszą spełniać osoby kluczowe i pozostali pracownicy	**P7SCB_UII3**	oceniać i kształtować strukturę organizacyjną z perspektywy integracji oraz stosowania wymagań cyberbezpieczeństwa		
		Identyfikacja aktywów w postaci sprzętu i oprogramowania organizacji	**P3SCB_UII4**	identyfikować sprzęt IT i OT oraz oprogramowanie	**P4SCB_UII4**	identyfikować zależności pomiędzy systemami, sieciami, urządzeniami i oprogramowaniem	**P5SCB_UII4**	określać kluczowe dla cyberbezpieczeństwa zależności pomiędzy systemami, sieciami, urządzeniami i oprogramowaniem	**P6SCB_UII4**	opracowywać wymagania cyberbezpieczeństwa odnośnie do systemów, sieci, urządzeń i oprogramowania				
		Identyfikacja aktywów procesowych organizacji	**P3SCB_UII5**	identyfikować ścieżki przepływu informacji	**P4SCB_UII5**	identyfikować strukturę systemów informacyjnych okreslać procesy krytyczne	**P5SCB_UII5**	identyfikować krytyczne procesy dla cyberbezpieczeństwa identyfikować krytyczne zależności	**P6SCB_UII5**	opracowywać wymagania cyberbezpieczeństwa w odniesieniu do procesów krytycznych	**P7SCB_UII5**	wpisywać i integrować wymagania cyberbezpieczeństwa w plany operacyjne		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Potrafi:														
UMIEJĘTNOŚCI:	**Identyfikacja**	Projektowanie produktów i usług					**P5SCB_UII6**	definiować i integrować typowe wymagania funkcjonalne oraz niefunkcjonalne odnoszące się do produktów i usług	**P6SCB_UII6**	definiować i integrować złożone wymagania funkcjonalne oraz niefunkcjonalne odnoszące się do produktów i usług	**P7SCB_UII6**	definiować i integrować zróżnicowane i niejednorodne technologicznie wymagania funkcjonalne oraz niefunkcjonalne odnoszące się do produktów i usług	**P8SCB_UII6**	tworzyć i rozwijać narzędzia dla zabezpieczenia produktów i usług w ich cyklu życia uwzględniać zasady cyberbezpieczeństwa w projektowaniu lub rozwijaniu produktów i usług
		Otoczenie społeczno-gospodarcze organizacji			**P4SCB_UII7**	identyfikować wymagania prawne, dobre praktyki i standardy biznesowe mające wpływ na organizację identyfikować partnerów zewnętrznych uzyskać wsparcie prawne w zakresie interpretacji przepisów związanych z cyber-bezpieczeństwem w organizacji	**P5SCB_UII7**	wskazywać rozwiązania mające na celu spełnienie wymagań, w tym prawnych	**P6SCB_UII7**	identyfikować i określać zakres potrzeb współpracy, w tym z instytucjami, uczelniami, szkołami branżowymi	**P7SCB_UII7**	identyfikować nowe koncepcje i technologie, w tym ich wpływ na cyberbezpieczeństwo organizacji	**P8SCB_UII7**	inicjować zmiany, w tym prawne, wpływające na cyberbezpieczeństwo organizacji
		Łańcuch dostaw	**P3SCB_UII8**	weryfikować wypełnianie umów przez dostawców	**P4SCB_UII8**	ustalać łańcuch dostaw i określać dostawców	**P5SCB_UII8**	identyfikować zależności w łańcuchu dostaw	**P6SCB_UII8**	określać parametry świadczenia usług od dostawców priorytetyzować zależności w łańcuchu dostaw i wskazywać zależności krytyczne identyfikować wymagania cyberbezpieczeństwa dla dostawców i dotyczące łańcuchów dostaw				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
				Potrafi:										
UMIEJĘTNOŚCI:	**Identyfikacja**	Ocena ryzyka	**P3SCB_UII9**	identyfikować zewnętrzne i wewnętrzne zagrożenia określać podatności aktywów i procesów na zidentyfikowane zagrożenia	**P4SCB_UII9**	opracowywać, kategoryzować i dokumentować zidentyfikowane ryzyka	**P5SCB_UII9**	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, transferowania opracowywać plan działania wraz z narzędziami, odpowiadający na potencjalne ryzyka	**P6SCB_UII9**	opracować politykę postępowania z ryzykiem	**P7SCB_UII9**	opracować strategię przeciwdziałania wystąpieniu ryzyk w organizacji		
		Wprowadzenie wymagań bezpieczeństwa w procesach, produktach i usługach	**P3SCB_UII10**	identyfikować osoby odpowiedzialne za przygotowanie nowych produktów i usług	**P4SCB_UII10**	przedstawić i wyjaśnić osobom odpowiedzialnym za przygotowanie nowych produktów i usług ich zakres obowiązków związanych z obszarem cyberbezpieczeństwa	**P5SCB_UII10**	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	**P6SCB_UII10**	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/ działu	**P7SCB_UII10**	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 SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Ochrona**	Tożsamość, uwierzytelnianie i kontrola dostępu, w tym zdalnego	**P3SCB_WIII1**	podstawowe pojęcia związane z tożsamością i uwierzytelnianiem mechanizmy dostępu, w tym dostępu zdalnego	**P4SCB_WIII1**	zasady stosowania jedno- i wieloskładnikowych systemów uwierzytelniania oraz systemów biometrycznych	**P5SCB_WIII1**	dobre praktyki zarządzania tożsamością, uwierzytelniania i kontroli dostępu, w tym zdalnego						
		Ochrona systemów IT	**P3SCB_WIII2**	powody, dla których systemy IT są chronione	**P4SCB_WIII2**	sposoby funkcjonowania i mechanizmy ochrony systemów IT sposoby ochrony danych przetwarzanych w systemach IT	**P5SCB_WIII2**	wymagania wynikające ze stosowania konkretnych systemów ochrony IT podział odpowiedzialności pomiędzy mechanizmami ochrony, w tym w systemach chmurowych (między dostawcą a klientem) w różnych modelach usług chmurowych (SaaS, IaaS, PaaS)	**P6SCB_WIII2**	zaawansowane systemy ochrony, w tym słabości i ograniczenia wynikające z konieczności zachowania ciągłości działania systemów IT	**P7SCB_WIII2**	trendy w zakresie rozwoju mechanizmów ochrony systemów IT	**P8SCB_WIII2**	nowe obszary zagrożeń, w przypadku których konieczne jest stworzenie mechanizmów ochrony IT
		Ochrona systemów OT	**P3SCB_WIII3**	powody, dla których systemy OT są chronione	**P4SCB_WIII3**	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	**P5SCB_WIII3**	działanie systemów ochrony systemów OT wymagania wynikające ze stosowania konkretnych systemów ochrony OT zależności pomiędzy systemami IT a systemami OT stosowanymi w organizacji	**P6SCB_WIII3**	zaawansowane systemy ochrony, w tym słabości i ograniczenia wynikające z konieczności zachowania ciągłości działania systemów OT	**P7SCB_WIII3**	trendy w zakresie rozwoju mechanizmów ochrony systemów OT	**P8SCB_WIII3**	nowe obszary zagrożeń, w przypadku których konieczne jest stworzenie mechanizmów ochrony OT
		Szkodliwe oprogramowania	**P3SCB_WIII4**	podstawowe typy szkodliwego oprogramowania	**P4SCB_WIII4**	zasady statycznej i dynamicznej analizy szkodliwego oprogramowania, w tym analizy w systemach sandbox, kodu maszynowego	**P5SCB_WIII4**	sposób działania szkodliwego oprogramowania używanego przez atakujących						

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Ochrona**	Sygnatury dla systemów monitorowania			**P4SCB_WIII5**	typowe sygnatury ataku	**P5SCB_WIII5**	metody tworzenia sygnatur rozpoznawania ataków i szkodliwego oprogramowania	**P6SCB_WIII5**	metody projektowania nowych rozwiązań/ algorytmów działania sygnatur				
Potrafi:														
UMIEJĘTNOŚCI:	**Ochrona**	Zarządzanie kontrolą dostępu zdalnego	**P3SCB_UIII1**	skonfigurować i zarządzać mechanizmami dostępu zdalnego	**P4SCB_UIII1**	zaproponować mechanizm dostępu zdalnego w organizacji, w tym przedstawić jego zalety i wady zweryfikować przypisane użytkownikom prawa dostępu zdalnego	**P5SCB_UIII1**	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	**P6SCB_UIII1**	wdrożyć w organizacji system zarządzania kontrolą dostępu zdalnego	**P7SCB_UIII1**	opracować w organizacji system zarządzania kontrolą dostępu zdalnego		
		Zarządzanie tożsamością i uwierzytelnianiem	**P3SCB_UIII2**	nadawać uprawnienia użytkownikom i grupom użytkowników w systemie operacyjnym	**P4SCB_UIII2**	określić i wybrać mechanizm uwierzytelniania dla różnych klas systemów dobierać urządzenia i techniki autoryzacji egzekwować zasady długości, złożoności i retencji haseł	**P5SCB_UIII2**	zaproponować w organizacji rozwiązania do wdrożenia w ramach systemów zarządzania tożsamością i uwierzytelnianiem opracować zasady zarządzania tożsamością i uwierzytelnianiem	**P6SCB_UIII2**	wdrożyć w organizacji system zarządzania tożsamością i uwierzytelnianiem	**P7SCB_UIII2**	opracować w organizacji system zarządzania tożsamością i uwierzytelnianiem		
		Rozwiązania analizujące zachowania użytkowników w systemie informatycznym			**P4SCB_UIII3**	wykorzystywać rozwiązania analizujące zachowania użytkowników	**P5SCB_UIII3**	skonfigurować rozwiązania analizujące zachowania użytkowników	**P6SCB_UIII3**	dopasować i wdrożyć rozwiązania analizujące zachowania użytkowników				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Ochrona**	Środowisko chronione	**P3SCB_UIII4**	identyfikować granice pomiędzy komponentami zainstalować i skonfigurować program antywirusowy założyć konto z hasłem	**P4SCB_UIII4**	identyfikować granice pomiędzy obiektami	**P5SCB_UIII4**	identyfikować granice pomiędzy systemami	**P6SCB_UIII4**	współuczestniczyć w administrowaniu systemami chronionymi w organizacji				
		Analiza szkodliwego oprogramowania i systemów informatycznych	**P3SCB_UIII5**	identyfikować typy szkodliwego oprogamowania wyszukiwać informacje o szkodliwym oprogramowaniu i wykorzystywanych przez niego narzędziach	**P4SCB_UIII5**	identyfikować słabe punkty w systemach informatycznych wykorzystywane przez szkodliwe oprogramowanie	**P5SCB_UIII5**	analizować szkodliwe oprogramowanie oraz słabe punkty w systemach informatycznych	**P6SCB_UIII5**	analizować trendy dotyczące szkodliwego oprogramowania	**P7SCB_UIII5**	modyfikować szkodliwe oprogramowanie w celu zwiększenia ochrony systemów	**P8SCB_UIII5**	opracować metody zabezpieczania systemów informatycznych przed nieznanym szkodliwym oprogramowaniem
		Monitoring użytkowników i systemów	**P3SCB_UIII6**	stosować technikę zdalnego i stacjonarnego dostępu	**P4SCB_UIII6**	korzystać z urządzeń i oprogramowania do monitoringu systemów, w tym logów	**P5SCB_UIII6**	analizować dane z urządzeń i oprogramowania do monitoringu systemów stosować technikę monitoringu aktywnej sesji użytkownika korelować zdarzenia z wielu urządzeń i wyciągać wnioski						
		Monitoring ryzyk	**P3SCB_UIII7**	monitorować ryzyka zgodnie z ustalonymi procedurami, wykorzystując dostępne narzędzia	**P4SCB_UIII7**	raportować wyniki monitoringu interesariuszom, tj. zapewnić dostępność użytecznych, kompletnych i aktualnych informacji o ryzyku	**P5SCB_UIII7**	opracować zasady i procedury monitoringu ryzyk dobrać narzędzia do monitorowania i raportowania ryzyk	**P6SCB_UIII7**	opracować narzędzia wspomagające monitoring ryzyk				
		Przygotowanie sygnatur dla systemów monitorowania	**P3SCB_UIII8**	wskazać zachodzący atak lub nietypowe działanie	**P4SCB_UIII8**	tworzyć sygnatury dla znanych typów ataków	**P5SCB_UIII8**	tworzyć sygnatury dotychczas nieznanych typów ataków						

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Ochrona**	Stosowanie narzędzi wykorzystujących sztuczną inteligencję w systemach cyberbezpieczeństwa			**P4SCB_UIII9**	interpretować informacje otrzymywane z systemów sztucznej inteligencji	**P5SCB_UIII9**	parametryzować systemy sztucznej inteligencji i oceniać ich skuteczność działania utrzymywać efektywność działania systemów sztucznej inteligencji	**P6SCB_UIII9**	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 integrować rozwiązania w zakresie sztucznej inteligencji z systemami funkcjonującymi w organizacji	**P7SCB_UIII9**	implementować rozwiązania w zakresie sztucznej inteligencji z systemami funkcjonującymi w organizacji		
		Utrzymanie ciągłości działania	**P3SCB_UIII10**	wykonywać ustandaryzowane działania w kontekście utrzymania ciągłości działania organizacji	**P4SCB_UIII10**	współpracować z zewnętrznymi dostawcami w zakresie utrzymania ciągłości działania w łańcuchu dostaw	**P5SCB_UIII10**	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	**P6SCB_UIII10**	priorytetyzować obszary, w których konieczne jest zachowanie ciągłości działania	**P7SCB_UIII10**	projektować procesy utrzymania ciągłości działania	**P8SCB_UIII10**	kreować standardy i rozwiązania specjalistyczne dla procesów utrzymania ciągłości działania

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Wykrywanie**	Podatności aplikacji webowych i ataki na nie			**P4SCB_WIV1**	kategorie podatności aplikacji webowych kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na aplikacje webowe	**P5SCB_WIV1**	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, OWASP ASVS	**P6SCB_WIV1**	złożone ataki na podatności webowe, w tym SSRF, SSTI, błędy deserializacji danych, XXE, podatności API				
		Podatności systemów i aplikacji mobilnych i ataki na nie			**P4SCB_WIV2**	kategorie podatności systemów i aplikacji mobilnych kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na systemy i aplikacje mobilne	**P5SCB_WIV2**	typowe podatności aplikacji mobilnych po stronie serwerowej oraz po stronie klienta i ataki na nie metodyki testów penetracyjnych aplikacji mobilnych, w tym OWASP MASTG, OWASP MASVS	**P6SCB_WIV2**	złożone ataki na podatności w aplikacjach mobilnych, w tym podatności API proces dekompilacji aplikacji mobilnej (reverse engineering)				
		Podatności infrastruktury sieciowej i ataki na nią	**P3SCB_WIV3**	sposoby rozpoznawania sieci, w tym skanowanie adresów IP, numerów portów aktywnych usług	**P4SCB_WIV3**	kategorie podatności infrastruktury sieciowej kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na infrastrukturę sieciową	**P5SCB_WIV3**	typowe podatności infrastruktury sieciowej i ataki na tę infrastrukturę, w tym sieci bezprzewodowe metodyki testów penetracyjnych infrastruktury sieciowej, w tym OSSTMM	**P6SCB_WIV3**	złożone ataki na podatności, np. związane z protokołami i usługami sieciowymi, w tym MitM, DHCP i ARP spoofing				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Wykrywanie**	Podatności systemów serwerowych i klienckich i ataki na nie			**P4SCB_WIV4**	kategorie podatności systemów serwerowych i klienckich kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na systemy serwerowe i klienckie	**P5SCB_WIV4**	typowe podatności i ataki na systemy operacyjne i aplikacje na nich zainstalowane, w tym buffer overflow, format string, escape to shell	**P6SCB_WIV4**	złożone ataki na podatności związane z usługami katalogowymi, w tym Active Directory				
		Podatności środowisk chmurowych i ataki na nie			**P4SCB_WIV5**	kategorie podatności w środowiskach chmurowych kategorie testów penetracyjnych i narzędzia do ich przeprowadzania na środowiska chmurowe	**P5SCB_WIV5**	typowe podatności w środowiskach chmurowych i ataki na nie	**P6SCB_WIV5**	złożone ataki na podatności związane ze środowiskami chmurowymi				
		Analiza kodu	**P3SCB_WIV6**	zasady statycznej i dynamicznej analizy kodu	**P4SCB_WIV6**	metody statycznej i dynamicznej analizy kodu i narzędzia do tego służące	**P5SCB_WIV6**	podatności występujące w kodzie, w tym związane z obsługą pamięci i wprowadzanych danych	**P6SCB_WIV6**	proces analizy kodu źródłowego skompilowanego oprogramowania (reverse engineering)				
		Zasady projektowania i zarządzania rozwiązaniami IoT	**P3SCB_WIV7**	komponenty IoT protokoły komunikacyjne IoT rodzaje rozwiązań IoT	**P4SCB_WIV7**	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	**P5SCB_WIV7**	zasady monitorowania komponentów oraz środowisk IoT podstawy projektowania rozwiązań IoT typowe podatności rozwiązań IoT i ataki na nie	**P6SCB_WIV7**	zagadnienia dotyczące zasilania komponentów IoT sieci specjalistyczne, w tym sieci AIM zasady zarządzania danymi w środowiskach IoT zasady projektowania rozwiązań IoT	**P7SCB_WIV7**	zasady opracowywania rozwiązań IoT wymagających szczególnej ochrony		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Wykrywanie**	Zasady projektowania i zarządzania rozwiązaniami OT	**P3SCB_WIV8**	komponenty OT protokoły komunikacyjne OT rodzaje rozwiązań OT	**P4SCB_WIV8**	zasady budowania środowisk komplementarnych i scentralizowanych w oparciu o komponenty OT podstawy komunikacji rozproszonej w OT podstawowe zagadnienia stabilności działania systemów OT	**P5SCB_WIV8**	zasady monitorowania komponentów oraz środowisk OT podstawy projektowania rozwiązań OT typowe podatności i ataki na rozwiązań OT i ataki na nie	**P6SCB_WIV8**	zagadnienia dotyczące zasilania komponentów OT sieci specjalistyczne, w tym sieci polowe zasady zarządzania danymi w środowiskach OT zasady projektowania rozwiązań OT	**P7SCB_WIV8**	zasady opracowywania rozwiązań OT wymagających szczególnej ochrony		
		Zasady projektowania i zarządzania zautomatyzowanymi systemami o dużej skali złożoności	**P3SCB_WIV9**	kryteria określające potrzebę stosowania zautomatyzowania pracy obszary możliwe do automatyzacji pracy	**P4SCB_WIV9**	zasady automatyzacji pracy	**P5SCB_WIV9**	narzędzia do budowy zautomatyzowanych systemów, w tym opartych na sztucznej inteligencji podstawy automatyki	**P6SCB_WIV9**	zasady projektowania liniowych układów automatyzacji	**P7SCB_WIV9**	zasady projektowania automatyzacji w systemach współliniowych, wielowątkowych	**P8SCB_WIV9**	zasady integracji systemów niekompatybilnych
		Symulowany atak hakerski	**P3SCB_WIV10**	rodzaje ataków socjotechnicznych rodzaje oprogramowania wykorzystywanego w ataku redteamingowym w internecie	**P4SCB_WIV10**	budowę i sposób funkcjonowania oprogramowania wykorzystywanego w ataku redteamingowym w internecie	**P5SCB_WIV10**	założenia testów stosowanych podczas ataku redteamingowego						
		Symulowany atak fizyczny			**P4SCB_WIV11**	metody fizycznego ataku redteamingowego	**P5SCB_WIV11**	stosowane zabezpieczenia, systemy alarmowe i metody kontroli dostępu narzędzia służące do testowania zabezpieczeń, systemów alarmowych i metod kontroli dostępu	**P6SCB_WIV11**	działanie oraz słabości systemów alarmowych i metod kontroli dostępu				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Wykrywanie**	Socjotechnika	**P3SCB_WIV12**	rodzaje testów socjotechnicznych	**P4SCB_WIV12**	zasady czytania mowy ciała typowe zachowania użytkowników sprzyjające manipulacji techniki manipulacji narzędzia wykorzystywane do ataków socjotechnicznych	**P5SCB_WIV12**	budowę i zasady funkcjonowania oprogramowania wspierającego testy socjotechniczne						
Potrafi:														
UMIEJĘTNOŚCI:	**Wykrywanie**	Obszary bazowe testów penetracyjnych			**P4SCB_UIV1**	opisać znalezione podatności	**P5SCB_UIV1**	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, exploity	**P6SCB_UIV1**	przygotować plan testu penetracyjnego nadzorować prowadzenie testów penetracyjnych przez podległy zespół	**P7SCB_UIV1**	modyfikować narzędzia do testów penetracyjnych	**P8SCB_UIV1**	opracowywać narzędzia do testów penetracyjnych
		Testy penetracyjne aplikacji webowych			**P4SCB_UIV2**	przeprowadzać testy aplikacji webowych z użyciem zautomatyzowanych narzędzi	**P5SCB_UIV2**	przeprowadzać testy aplikacji webowych z wykorzystaniem typowych rodzajów podatności i ataków, w tym SQL injection, XSS, CSRF, IDOR, Broken Access Control przeprowadzać testy aplikacji webowych zgodnie z określonymi metodykami, w tym OWASP Web Security Testing Guide, OWASP ASVS	**P6SCB_UIV2**	przeprowadzać złożone ataki na podatności webowe, w tym SSRF, SSTI, błędy deserializacji danych, XXE, padatności API	**P7SCB_UIV2**	wykryć nowe podatności (zero-days) w aplikacjach webowych i wykorzystywać je do ataków		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Wykrywanie**	Testy penetracyjne systemów i aplikacji mobilnych			**P4SCB_UIV3**	przeprowadzać testy systemów i aplikacji mobilnych z wykorzystaniem zautomatyzowanych narzędzi	**P5SCB_UIV3**	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, OWASP MASVS	**P6SCB_UIV3**	przeprowadzać złożone ataki na aplikacje mobilne, w tym podatności API przeprowadzić dekompilację aplikacji mobilnej (reverse engineering)	**P7SCB_UIV3**	wykryć nowe podatności (zero-days) systemów i aplikacji mobilnych oraz wykorzystywać je do ataków		
		Testy penetracyjne infrastruktury sieciowej			**P4SCB_UIV4**	przeprowadzać testy infrastruktury sieciowej z użyciem zautomatyzowanych narzędzi przeprowadzać rozpoznawanie sieci, w tym skanowanie adresów IP, numerów portów aktywnych usług	**P5SCB_UIV4**	przeprowadzać typowe ataki na infrastrukturę sieciową, w tym sieci bezprzewodowe	**P6SCB_UIV4**	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	**P7SCB_UIV4**	wykryć nowe podatności (zero-days) w infrastrukturze sieciowej i wykorzystywać je do ataków		
		Testy penetracyjne systemów serwerowych i klienckich			**P4SCB_UIV5**	przeprowadzać testy systemów serwerowych i klienckich z użyciem zautomatyzowanych narzędzi	**P5SCB_UIV5**	przeprowadzać ataki na typowe systemy operacyjne i ich aplikacje, w tym buffer overflow, format string, escape to shell	**P6SCB_UIV5**	przeprowadzać ataki na usługi katalogowe, w tym Active Directory	**P7SCB_UIV5**	wykryć nowe podatności (zero-days) systemów serwerowych i klienckich oraz wykorzystywać je do ataków		
		Testy penetracyjne środowisk chmurowych			**P4SCB_UIV6**	ocenić prawidłowość konfiguracji instancji chmury obliczeniowej pod kątem bezpieczeństwa przeprowadzać rekonesans publicznych chmur obliczeniowych	**P5SCB_UIV6**	zaplanować i dokonać oceny skutków planowanych testów penetracyjnych w środowisku chmurowym	**P6SCB_UIV6**	wyciągnąć wnioski z przeprowadzonych testów penetracyjnych poszczególnych instancji chmury obliczeniowej zaproponować rozwiązania mające na celu zwiększenie bezpieczeństwa instancji chmury obliczeniowej				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Wykrywanie**	Przeprowadzenie analizy kodu			**P4SCB_UIV7**	przeprowadzić automatyczną analizę kodu określać kategorie podatności znalezionych za pomocą automatycznego narzędzia	**P5SCB_UIV7**	określać konsekwencje wykorzystania znalezionych podatności	**P6SCB_UIV7**	analizować zdekompilowany kod samodzielnie zidentyfikować podatności weryfikować wyniki automatycznej analizy	**P7SCB_UIV7**	wykryć nowe rodzaje podatności w kodzie rozbudowywać narzędzia do analizy kodu	**P8SCB_UIV7**	opracować narzędzia do analizy kodu
		Budowa i zarządzanie rozwiązaniami IoT	**P3SCB_UIV8**	zbudować prosty system IoT w oparciu o komunikację bezpośrednią	**P4SCB_UIV8**	zbudować system IoT w oparciu o algorytmikę postępowania lub scenariusze użycia	**P5SCB_UIV8**	monitorować status pracy poszczególnych urządzeń i całego systemu IoT	**P6SCB_UIV8**	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	**P7SCB_UIV8**	rozwiązywać zagadnienia związane z niestabilnością pracy środowiska IoT budować systemy procesowe w środowisku IoT	**P8SCB_UIV8**	opracowywać rozwiązania IoT wymagające szczególnej ochrony
		Budowa i zarządzanie rozwiązaniami OT	**P3SCB_UIV9**	zbudować prosty system OT w oparciu o komunikację bezpośrednią	**P4SCB_UIV9**	zbudować system OT w oparciu o algorytmikę postępowania lub scenariusze użycia	**P5SCB_UIV9**	monitorować status pracy poszczególnych urządzeń i całego systemu OT	**P6SCB_UIV9**	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	**P7SCB_UIV9**	rozwiązywać zagadnienia związane z niestabilnością pracy środowiska OT zbudować systemy procesowe w środowisku OT	**P8SCB_UIV9**	opracowywać rozwiązania OT wymagające szczególnej ochrony

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Wykrywanie**	Budowa i zarządzanie zautomatyzowanymi systemami o dużej skali złożoności			**P4SCB_UIV10**	zbudować algorytmy automatyki o dużej skali złożoności	**P5SCB_UIV10**	zbudować typowy system automatyki o dużej skali złożoności nadzorować i utrzymywać systemy o dużej skali złożoności	**P6SCB_UIV10**	zbudować systemy o dużej skali złożoności z wymaganiami dotyczącymi działania w czasie rzeczywistym	**P7SCB_UIV10**	projektować systemy o dużej skali złożoności z wymaganiami dotyczącymi działania w czasie rzeczywistym zastosować sztuczną inteligencję do zautomatyzowania pracy w systemach o dużej skali złożoności	**P8SCB_UIV10**	integrować systemy niekompatybilne
		Wykrywanie zmian	**P3SCB_UIV11**	wykryć zmiany na poziomie komponentów	**P4SCB_UIV11**	wykryć niepożądane zmiany na poziomie kodu	**P5SCB_UIV11**	wykryć zmiany na poziomie parametrów pracy systemów	**P6SCB_UIV11**	wykryć i kontrolować zmiany po zdarzeniu reakcyjnym	**P7SCB_UIV11**	wykryć i nadzorować w trybie ciągłym zmiany w systemach zautomatyzowanych		
		Redteaming			**P4SCB_UIV12**	przeprowadzić rekonesans przed przeprowadzeniem ataku redteamingowego w internecie	**P5SCB_UIV12**	przygotować założenia ataku redteamingowego w internecie dobrać test penetracyjny w ataku redteamingowym w internecie analizować wyniki ataku redteamingowego w internecie	**P6SCB_UIV12**	dostosować oprogramowanie do założeń ataku redteamingowego w internecie przeprowadzić test penetracyjny w ataku redteamingowym opracować rekomendacje po ataku redteamingowym	**P7SCB_UIV12**	eskalować atak redteamingowy wykorzystywać nowo znalezione podatności w ataku redteamingowym wskazać możliwe nowe metody ataków redteamingowych w internecie	**P8SCB_UIV12**	stworzyć narzędzia do nowych typów ataków redteamingowych w internecie

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
								Potrafi:						
UMIEJĘTNOŚCI:	Wykrywanie	Redteaming fizyczny			P4SCB_UIV13	przeprowadzić rekonesans przed fizycznym atakiem redteamingowym	P5SCB_UIV13	przygotować założenia fizycznego ataku redteamingowego dobrać test penetracyjny w ataku redteamingowym fizycznym 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	P6SCB_UIV13	przeprowadzić atak fizyczny ominąć zaawansowane zabezpieczenia, systemy alarmowe i metody kontroli dostępu dostosować oprogramowanie do założeń fizycznego ataku redteamingowego przeprowadzić test penetracyjny w ramach redteamingu fizycznego opracowywać rekomendacje po fizycznym ataku redteamingowym	P7SCB_UIV13	eskalować fizyczny atak redteamingowy wykorzystywać nowo znalezione podatności w fizycznym ataku redteamingowym wskazać możliwe nowe metody ataków fizycznych	P8SCB_UIV13	stworzyć narzędzia do nowych typów ataków fizycznych
		Testy socjotechniczne					P5SCB_UIV14	stosować techniki manipulacji przeprowadzić testy socjotechniczne tworzyć własne proste narzędzia wspierające prowadzenie testów socjotechnicznych	P6SCB_UIV14	określić oczekiwane rezultaty testów socjotechnicznych przygotować plan testów socjotechnicznych opracować rekomendacje po ataku socjotechnicznym				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Potrafi:														
UMIEJĘTNOŚCI:	**Wykrywanie**	Threat modelling	**P3SCB_UIV15**	rozpoznawać komponenty systemu i ich funkcje	**P4SCB_UIV15**	rozpoznawać zależności między komponentami systemów	**P5SCB_UIV15**	wykryć typowe zagrożenia związane z architekturą systemów	**P6SCB_UIV15**	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 jak STRIDE, DREAD, OWASP Threat Modeling Guide	**P7SCB_UIV15**	przewidywać nowe obszary, w których mogą wystąpić zagrożenia		
Zna i rozumie:														
WIEDZA:	**Reakcja**	Terminologia i technologia związana z materiałem dowodowym	**P3SCB_WV1**	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	**P4SCB_WV1**	rodzaje informacji przetwarzanych w systemach informatycznych, w tym urządzeniach cyfrowych, bazach danych, dokumentach generowanych przez system, danych generowanych przez użytkownika i danych ulotnych	**P5SCB_WV1**	możliwości audytowania struktury systemu plików sposoby zabezpieczania informacji przetwarzanych w poszczególnych elementach systemu informatycznego						

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Reakcja**	Zabezpieczanie dowodów	**P3SCB_WV2**	podstawowe techniki zabezpieczania różnych typów dowodów metody określenia wymagań dotyczących zabezpieczania dowodów wpływ czynników zewnętrznych, takich jak wilgoć, temperatura i wstrząsy na materiał dowodowy techniki transportu materiałów dowodowych w sposób umożliwiający wykorzystanie ich w późniejszym postępowaniu dowodowym	**P4SCB_WV2**	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 wiarygodność postępowania dowodowego	**P5SCB_WV2**	wymagania prawne postępowania z cyfrowym materiałem dowodowym zależności występujące w poszczególnych grupach informacyjnych, formatach danych techniki agregacji informacji techniki odbioru i zabezpieczenia informacji do postępowania w laboratorium						
		Postępowanie z cyfrowym materiałem dowodowym	**P3SCB_WV3**	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	**P4SCB_WV3**	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	**P5SCB_WV3**	wymagania prawne dotyczące pozyskiwania cyfrowego materiału dowodowego sposoby zastosowania środków ochrony do zabezpieczenia cyfrowego materiału dowodowego procedury dokumentowania materiału dowodowego						

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Reakcja**	Systemy reakcji na incydenty	**P3SCB_WV4**	plany reagowania na poszczególne incydenty, w tym tworzone na potrzeby organizacji i jej systemów wewnętrznych zasady komunikacji zewnętrznej i wewnętrznej dotyczące incydentu	**P4SCB_WV4**	dobre praktyki reakcji na incydenty zasady przygotowania raportu dotyczącego obsługi incydentów sposób działania poszczególnych systemów reakcji na incydent	**P5SCB_WV4**	wymogi prawne dotyczące informowania o incydentach wymogi kontraktowe dotyczące informowania o incydentach						
Potrafi:														
UMIEJĘTNOŚCI:	**Reakcja**	Identyfikowanie materiału dowodowego	**P3SCB_UV1**	rozpoznać środowisko, w którym należy zabezpieczyć materiał dowodowy	**P4SCB_UV1**	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	**P5SCB_UV1**	agregować pozornie niespójne informacje lub niekompatybilne systemy połączyć wykryte zdarzenia z wielu źródeł ataku	**P6SCB_UV1**	rozpoznawać poziom ryzyka zagrożeń ze świata zewnętrznego, uwzględniając specyfikę organizacji rozwiązać problem awarii lub niedostępności systemu				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
								Potrafi:						
UMIEJĘTNOŚCI:	Reakcja	Zabezpieczenie i pozyskanie materiału dowodowego	P3SCB_UV2	pozyskać i gromadzić cyfrowy materiał dowodowy według standardowych procedur zabezpieczyć dane dowodowe zgodnie z przyjętym protokołem dobrać odpowiednią do sytuacji metodę transportu grup dowodowych	P4SCB_UV2	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 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 nieobjęte procedurami	P5SCB_UV2	dobrać narzędzia przeciwdziałające niebezpieczeństwu podważenia materiału dowodowego przygotować opis incydentu	P6SCB_UV2	przydzielać role w procesie zabepieczenia dowodów wspierać techników w laboratorium i jego otoczeniu zgodnie z procedurami oraz potrzebami technicznymi po wystąpieniu incydentu bezpieczeństwa	P7SCB_UV2	minimalizować potencjalne ryzyka w odniesieniu do materiału dowodowego zarządzać zespołem w pracy dowodowej w laboratorium informatyki śledczej oraz w terenie		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
						Potrafi:								
UMIEJĘTNOŚCI:	**Reakcja**	Analityka zebranego materiału dowodowego			**P4SCB_UV3**	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	**P5SCB_UV3**	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	**P6SCB_UV3**	analizować pozyskany materiał dowodowy, w tym z wykorzystaniem specjalistycznych narzędzi	**P7SCB_UV3**	zarządzać zespołem w pracy analitycznej	**P8SCB_UV3**	wyszukiwać i analizować niestandardowe dowody opracować nowe metody służące do poprawnej ekstrakcji danych opracować nowe rozwiązanie służące do poprawnej ekstrakcji danych
		Reakcja na zdarzenia i incydenty	**P3SCB_UV4**	identyfikować komponenty zdarzenia współpracować z osobą związaną z incydentem	**P4SCB_UV4**	reagować na zdarzenia zgodnie z procedurami, standardami reakcyjnymi, planami obsługi incydentów identyfikować korelacje pomiędzy dwoma zdarzeniami zweryfikować kompletność planów obsługi incydentów	**P5SCB_UV4**	modernizować procedury, standardy reakcyjne w odpowiedzi na zaistniały incydent przedstawić informacje o incydencie interesariuszom, w tym kierownictwu, klientom, 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	**P6SCB_UV4**	opracować plany, procedury, scenariusze reakcji na incydent bezpieczeństwa opracować automatyczne narzędzia odpowiadające na zaistniałe incydenty	**P7SCB_UV4**	opracować standardy reakcji na incydent bezpieczeństwa określać ścieżki rozwoju systemów, które minimalizują potencjalne skutki incydentów		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Potrafi:														
UMIEJĘTNOŚCI:	**Reakcja**	Laboratorium obszaru cyberbezpieczeństwa, w tym informatyki śledczej	**P3SCB_UV5**	używać podstawowych narzędzi laboratorium obszaru cyberbezpieczeństwa, w tym informatyki śledczej	**P4SCB_UV5**	dobrać stanowisko do zagadnienia lub celu badania	**P5SCB_UV5**	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	**P6SCB_UV5**	wskazać i przypisać konkretne role do osób w laboratorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej weryfikować prawidłowe użycie narzędzi przez pracowników w labolatorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej	**P7SCB_UV5**	przeprowadzić symulację incydentu bezpieczeństwa, pozwalającą weryfikować działanie badanego systemu w labolatorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej, i minimalizować potencjalne konsekwencje	**P8SCB_UV5**	tworzyć nowe rozwiązania techniczne i proceduralne w celach optymalizacji działania labolatorium w obszarze cyberbezpieczeństwa, w tym informatyki śledczej
Zna i rozumie:														
WIEDZA:	**Odbudowa**	Kopie bezpieczeństwa	**P3SCB_WVI1**	rodzaje kopii bezpieczeństwa	**P4SCB_WVI1**	budowę i ograniczenia nośników danych metody i systemy wykonywania kopii bezpieczeństwa	**P5SCB_WVI1**	zasady budowania zapasowych centrów przetwarzania danych						
		Model ciągłości działania			**P4SCB_WVI2**	budowę i ograniczenia modelu ciągłości działania metody wdrażania modelu ciągłości działania	**P5SCB_WVI2**	metody opracowywania modelu ciągłości działania dopasowanego do potrzeb organizacji potencjalne skutki incydentu dla działania modelu ciągłości działania						

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
								Potrafi:						
UMIEJĘTNOŚCI:	**Odbudowa**	Identyfikacja zagadnień ciągłości działania	**P3SCB_UVI1**	identyfikować rodzaj incydentu	**P4SCB_UVI1**	oceniać skalę zagrożenia	**P5SCB_UVI1**	reagować na incydent zgodnie z wewnętrznymi procedurami wprowadzać zmiany w przypadku awarii w celu odtworzenia systemu monitorować poprawność działania systemów zapasowych	**P6SCB_UVI1**	opracowywać i wdrażać procedury przełączenia na systemy zapasowe				
		Ocena incydentu	**P3SCB_UVI2**	replikować incydent	**P4SCB_UVI2**	replikować incydent w ramach weryfikacji działania procedur	**P5SCB_UVI2**	analizować incydent i jego skutki	**P6SCB_UVI2**	opracować rozwiązania strukturalne w odpowiedzi na zaistniały incydent	**P7SCB_UVI2**	rekomendować i inicjować wdrożenie zmian strukturalnych		
		Odbudowa modelu ciągłości działania	**P3SCB_UVI3**	identyfikować podatności modelu działania w kontekście zaistniałego incydentu	**P4SCB_UVI3**	opracować propozycje zmian technicznych w odpowiedzi na zaistniały incydent	**P5SCB_UVI3**	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	**P6SCB_UVI3**	modyfikować modele działania z uwzględnieniem uwarunkowań organizacji i zaistniałego incydentu	**P7SCB_UVI3**	tworzyć nowe modele działania z uwzględnieniem uwarunkowań organizacji i zaistniałego incydentu		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
								Potrafi:						
UMIEJĘTNOŚCI:	Odbudowa	Odtworzenie ciągłości działania	P3SCB_UVI4	monitorować wskaźniki systemów kontroli działania oraz automatyczne wykonywanie kopii bezpieczeństwa sprawdzać poprawność kopii bezpieczeństwa odtworzyć kopie bezpieczeństwa	P4SCB_UVI4	monitorować przełączanie się systemów informatycznych na serwery w zapasowym CPD monitorować moment odzyskania pełnej sprawności świadczonych usług przez systemy cyfrowe	P5SCB_UVI4	rekomendować urządzenia oraz oprogramowanie do wykonywania kopii bezpieczeństwa opracować zasady retencji kopii bezpieczeństwa opracować plan ciągłości działania	P6SCB_UVI4	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	P7SCB_UVI4	wdrażać zmiany w rozwiązaniach z zakresu tworzenia kopii bezpieczeństwa wynikających z przeprowadzonej analizy trendów dokonywać adaptacji planu ciągłości działania w ujęciu strategicznym		
		Weryfikacja zapisów umów	P3SCB_UVI5	identyfikować zapisy umów wpływające na zapewnianie ciągłości działania systemów	P4SCB_UVI5	weryfikować zgodność zapisów umów z działaniami zapewniającymi bezpieczeństwo systemów realizować umowy, w tym OLA i SLA monitorować realizację zapisów umów, w tym OLA i SLA	P5SCB_UVI5	rekomendować zapisy w umowach, w tym OLA i SLA, wspierające zapewnianie ciągłości działania						

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Zna i rozumie:														
WIEDZA:	**Audyt cyberbezpieczeństwa w ramach zarządzania bezpieczeństwem**	Zasady audytu cyberbezpieczeństwa	**P3SCB_WVII1**	cele i zakres działań audytu cyberbezpieczeństwa rodzaje dokumentacji niezbędnej do przygotowania i przeprowadzenia audytu cyberbezpieczeństwa	**P4SCB_WVII1**	procedury audytu cyberbezpieczeństwa zasady klasyfikacji organizacji zasadnicze różnice między sektorami, branżami, typami obiektów, gdzie przeprowadzony jest audyt cyberbezpieczeństwa narzędzia wykorzystywane w audycie cyberbezpieczeństwa wymagania związane z pozostałymi wymaganiami bezpieczeństwa, w tym bezpieczeństwa informacji, bezpieczeństwa fizycznego	**P5SCB_WVII1**	rekomendacje organów właściwych dla poszczególnych sektorów, stanowiące punkt odniesienia dla audytu wymagania nadrzędne dla podmiotów audytowanych wpływ narzędzi audytowych na analizowany obiekt i ciągłość jego działania	**P6SCB_WVII1**	wpływ narzędzi audytowych na stabilność pracy systemów złożonych	**P7SCB_WVII1**	wpływ narzędzi audytowych na integralność subkomponentów pracujących w ramach systemów złożonych zasady projektowania narzędzi audytowych	**P8SCB_WVII1**	zasady projektowania i kierunki rozwoju specjalistycznych narzędzi audytowych
		Zarządzanie zespołem audytowym			**P4SCB_WVII2**	role występujące w zespole audytowym ze względu na podstawowe różnice sektorowe	**P5SCB_WVII2**	role występujące w zespole audytowym ze względu na szczegółowe różnice wewnątrz sektorów	**P6SCB_WVII2**	role występujące w zespole audytowym ze względu na różnice specjalistyczne podstawowe zasady zarządzania zespołem audytowym	**P7SCB_WVII2**	zasady zarządzania zespołem audytowym uwzględniające złożoność organizacji i wpływ na nią	**P8SCB_WVII2**	kierunki rozwoju metod audytu

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Potrafi:												
UMIEJĘTNOŚCI:	**Audyt cyberbezpieczeństwa w ramach zarządzania bezpieczeństwem**	Przygotowanie audytu cyberbezpieczeństwa			**P4SCB_UVII1**	weryfikować spełnienie wymagań formalnych wynikających z zasad przyjętych w organizacji opracować dokumenty potrzebne do audytu cyberbezpieczeństwa zidentyfikować ryzyka w badanym obszarze	**P5SCB_UVII1**	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	**P6SCB_UVII1**	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	**P7SCB_UVII1**	modyfikować zestaw narzędzi potrzebny do przeprowadzenia konkretnego audytu cyberbezpieczeństwa	**P8SCB_UVII1**	projektować ekosystemy audytowe i narzędzia do jego przeprowadzenia w branżach, gdzie audyt cyberbezpieczeństwa jest zjawiskiem nowym
		Procedury kwalifikacji w audycie	**P3SCB_UVII2**	zbierać i weryfikować dokumentację projektową, podwykonawczą oraz instrukcje eksploatacyjne obiektu pod kątem zgodności stanu faktycznego z określonymi wymaganiami (DQ)	**P4SCB_UVII2**	weryfikować zgodność dokumentacji projektowej, powykonawczej oraz instrukcji eksploatacyjnych z faktycznym ich wdrożeniem w obiekcie (IQ) opracować raport rozbieżności	**P5SCB_UVII2**	weryfikować, czy zainstalowane lub zmodyfikowane urządzenie, oprogramowanie lub system działają zgodnie z założeniami podstawowymi grup funkcyjnych oraz systemów (OQ)	**P6SCB_UVII2**	weryfikować, czy połączone grupy funkcyjne w określonym czasie i miejscu obiektu właściwie tworzą określony proces generacji oraz dostarczają określony produkt lub półprodukt (PQ)	**P7SCB_UVII2**	dopasować działania audytowe do specjalistycznych wymagań konkretnych organizacji		

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
Potrafi:														
UMIEJĘTNOŚCI:	Audyt cyberbezpieczeństwa w ramach zarządzania bezpieczeństwem	Przeprowadzenie audytu	P3SCB_UVII3	rozróżniać czynności dla trybu audytu, kontroli i oceny	P4SCB_UVII3	przeprowadzać zadania audytowe zgodnie z programem zabezpieczać materiał dowodowy	P5SCB_UVII3	analizować wnioski z przeprowadzonego audytu oraz proponować rozwiązania używać narzędzia do audytu cyberbezpieczeństwa zgodnie z ich przeznaczeniem przygotować raport z audytu bezpieczeństwa przygotować protokół z kontroli	P6SCB_UVII3	opracować raport z audytu bezpieczeństwa wraz z rekomendacjami dotyczącymi niezgodności i obszarów do optymalizacji określać zakres poszczególnych działań wynikających z audytu i przydzielać działania do realizacji poszczególnym komórkom organizacji	P7SCB_UVII3	przeprowadzić transfer wiedzy po dokonaniu audytu cyberbezpieczeństwa w trakcie audytu elastycznie stosować nowe, niezbędne czynności audytowe, w tym dobierać adekwatny zakres próby	P8SCB_UVII3	projektować nowe czynności audytowe
		Działania po audycie cyberbezpieczeństwa					P5SCB_UVII4	oceniać wdrożenie zaleceń przez jednostkę audytowaną po przeprowadzonym zadaniu audytowym	P6SCB_UVII4	wdrażać wnioski i rekomendacje z audytu cyberbezpieczeństwa	P7SCB_UVII4	implementować i nadzorować wdrażanie zasadniczych zmian wynikających z audytu cyberbezpieczeństwa	P8SCB_UVII4	projektować rozwiązania po przeprowadzeniu audytu cyberbezpieczeństwa
Jest gotów do:														
KOMPETENCJE SPOŁECZNE:	Standardy pracy	Kształtowanie postaw w obszarze cyberbezpieczeństwa	P3SCB_KSVIII1	przyjmowania odpowiedzialności za sposób użytkowania produktów i usług	P4SCB_KSVIII1	postępowania zgodnie z zasadami i procedurami cyberbezpieczeństwa produktów, usług i organizacji	P5SCB_KSVIII1	prowadzenia działań informacyjnych w celu podniesienia poziomu cyberodporności w użytkowaniu produktów i usług	P6SCB_KSVIII1	promowania i komunikowania działań na rzecz podnoszenia poziomu cyberodporności	P7SCB_KSVIII1	promowania i kształtowania właściwych postaw w obszarze cyberbezpieczeństwa	P8SCB_KSVIII1	tworzenia wzorców postaw w obszarze cyberbezpieczeństwa
		Normy etyczne					P5SCB_KSVIII2	postępowania zgodnie z zasadami etyki zawodowej w cyberprzestrzeni promowania zasad etycznych w cyberprzestrzeni	P6SCB_KSVIII2	rozstrzygania dylematów etycznych związanych z zapewnieniem cyberbezpieczeństwa				

	WYZNACZNIK SEKTOROWY	WIĄZKA KOMPETENCJI	SRK CB	POZIOM 3	SRK CB	POZIOM 4	SRK CB	POZIOM 5	SRK CB	POZIOM 6	SRK CB	POZIOM 7	SRK CB	POZIOM 8
		Jest gotów do:												
KOMPETENCJE SPOŁECZNE:	**Komunikacja i współpraca**	Odpowiedzialność			**P4SCB_KSVIII3**	świadomego przestrzegania zasad i procedur cyberbezpieczeństwa, z uwzględnieniem ewentualnych konsekwencji nierzetelnego wykonywania zadań	**P5SCB_KSVIII3**	ponoszenia konsekwencji za nierzetelne wykonywanie zadań lub nieprzestrzeganie zasad i procedur cyberbezpieczeństwa	**P6SCB_KSVIII3**	promowania postawy odpowiedzialności za procesy zapewniania cyberbezpieczestwa	**P7SCB_KSVIII3**	współtworzenia norm/ standardów zachowań projakościowych w obszarze cyberbezpieczeństwa promowania kultury projakościowej w obszarze cyberbezpieczeństwa	**P8SCB_KSVIII3**	kształtowania kultury projakościowej w obszarze cyberbezpieczeństwa
		Komunikacja			**P4SCB_KSIX1**	komunikowania się z różnymi interesariuszami, w tym nieznającymi terminologii sektorowej, w sposób dla nich zrozumiały	**P5SCB_KSIX1**	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	**P6SCB_KSIX1**	przedstawiania i uzasadniania zasad funkcjonowania systemu cyberbezpieczeństwa osobom zarządzającym z uwzględnieniem zakresu ich odpowiedzialności	**P7SCB_KSIX1**	komunikowania się w międzynarodowym środowisku, z uwzględnieniem różnic kulturowych		
		Relacje, zachowania, reakcje			**P4SCB_KSIX2**	ścisłej i efektywnej współpracy z interesariuszami w zadaniach związanych z zapewnieniem cyberbezpieczeństwa właściwego działania w warunkach stresowych	**P5SCB_KSIX2**	zmian rozwiązań technicznych i organizacyjnych w systemie cyberbezpieczeństwa adaptacji w zmieniających się uwarunkowaniach sektora cyberbezpieczeństwa	**P6SCB_KSIX2**	podejmowania decyzji w zmiennych, nietypowych warunkach w sytuacji wystąpienia incydentu bezpieczeństwa, w warunkach niepełnej informacji, wysokiego ryzyka				
		Prywatność i anonimowość w internecie			**P4SCB_KSIX3**	korzystania z portali społecznościowych w sposób pozwalający na zachowanie anonimowości i prywatności	**P5SCB_KSIX3**	zarządzania informacjami na swój temat w internecie						

Słownik pojęć stosowanych w Sektorowej Ramie Kwalifikacji dla Cyberbezpieczeństwa

POJĘCIE	DEFINICJA
Adres IP	Adresy IP umożliwiają urządzeniom, które znajdują się w tych samych lub różnych sieciach, komunikowanie się ze sobą. Adresy IPv4 to adresy 32-bitowe, reprezentowane w notacji dziesiętnej z kropkami, np. 192.168.1.0. Adresy IPv6 są adresami 128-bitowymi, reprezentowanymi w notacji szesnastkowej z dwukropkami, np. 2a01:612f:1047:9710:e9e0:ca9a:586b:dd04. Istnieją dwie metody przydzielania adresów IP w interfejsie sieciowym: dynamiczne i statyczne. Dynamiczne adresy są przydzielane przez serwer DHCP z dostępnej puli adresów, a statyczne adresy IP są przypisywane ręcznie.
Anomalia	Zachowanie (zdarzenie) niezgodne z procedurami, standardami przyjętymi w organizacji.
API	Application Programming Interface – interfejs programowania, czyli zestaw reguł, protokołów i narzędzi używanych do budowy i interakcji z oprogramowaniem i aplikacjami. Definiuje on sposób, w jaki aplikacje lub moduły systemów powinny się ze sobą komunikować, określa dostępne do użycia funkcje, zasady ich działania oraz wskazuje dane niezbędne do ich wykonania. Określa również reguły umożliwiające bezpieczne przesyłanie danych np. poprzez wdrażanie uwierzytelniania (weryfikację tożsamości użytkownika) oraz autoryzację (nadanie uprawnień).
Aplikacje desktopowe	Programy, które instalowane są i uruchamiane bezpośrednio na urządzeniu, np. komputerze stacjonarnym, laptopie, tablecie, smartfonie. Do ich działania nie jest konieczny dostęp do internetu.
Aplikacje mobilne	Programy instalowane i uruchamiane na urządzeniach przenośnych (mobilnych), np. smartfonach, tabletach. Jest to publicznie dostępne oprogramowanie z interfejsem dotykowym, zaprojektowane do wykorzystania na urządzeniach mobilnych.

Aplikacje webowe (internetowe)	Programy uruchamiane w przeglądarce, które przez zaprojektowany interfejs mają dostarczać użytkownikowi konkretną usługę udostępnianą przez serwer.
Autoryzacja	Proces weryfikacji uprawnień użytkownika lub systemu, aby określić, czy dana osoba, aplikacja lub urządzenie ma prawo dostępu do określonych zasobów lub funkcji systemu informatycznego. Autoryzacja jest jednym z kluczowych elementów kontroli dostępu i ma na celu zapewnienie, że tylko uprawnione osoby lub systemy uzyskują dostęp do zasobów lub danych, które są im przydzielone.
Bazy CMDB	Baza danych zarządzania konfiguracją (ang. Configuration Management Database) – baza danych zawierająca informacje o aktywach oraz relacjach pomiędzy nimi.
Bezpieczeństwo informacji danych	Zestaw narzędzi i procedur zabezpieczeń, które szeroko chronią poufne informacje przed nadużyciami, nieautoryzowanym dostępem, ujawnieniem, modyfikacją, kontrolą, zakłóceniami lub zniszczeniem.
Biblioteka DQL, DML, DCL	Biblioteki zawierające definicję składni języka SQL: DQL (Data Query Language), DML (Data Manipulation Language), DCL (Data Control Language).
Blueteaming	Zespół zajmujący się działaniami defensywnymi. Jego rolą jest reagowanie na ataki, zagrożenia, monitorowanie ruchu sieciowego oraz podejmowanie działań w przypadku wykrycia próby ataku.
Branża	Jeden z obszarów dla poszczególnych sektorów, np. branża ciepłownicza (sektor energetyczny), branża suplementów (sektor farmeceutyczny) etc.
Buffer overflow	Podatność polegająca na próbie zapisu większej ilości danych do bufora pamięci, przekraczająca jego rozmiar.
Cyberbezpieczeństwo	Działania, polityki i procedury mające na celu utrzymanie ciągłości działania organizacji poprzez ochronę systemów, sieci oraz danych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem oraz zdolność do odzyskiwania ciągłości działania po incydencie.

Cybezagrożenia	Cyberzagrożenia to sytuacje lub działania, które stanowią potencjalne ryzyko dla ciągłości działania i realizacji podstawowych funkcji systemów komputerowych, sieci, urządzeń związanych z technologią informacyjną, w tym kontroli dostępu, integralności i poufności danych.
Dane	Zarejestrowane, przetwarzane i przesyłane przez nadawcę w formie komunikatu fakty, które nie są uporządkowane, przetworzone ani połączone zgodnie z celem i zadaniami odbiorcy.
Dekompilacja	Proces tłumaczenia pliku wykonywalnego do wyższego rzędu (kod źródłowy).
DQ	Kwalifikacja dokumentów (ang. Design Qualification) – weryfikacja dokumentacji projektowej, podwykonawczej oraz instrukcji eksploatacyjnych obiektu pod kątem zgodności zawartych w nich wymagań ze stanem faktycznym.
Etap identyfikacji	Przygotowanie i wdrożenie odpowiednich działań w celu zidentyfikowania i oceny wystąpienia ryzyk wpływających na cyberbezpieczeństwo.
Etap ochrony	Przygotowanie i wdrożenie odpowiednich zabezpieczeń w celu zapewnienia poprawnego świadczenia usług i działania produktów.
Etap odbudowy	Analiza zdarzenia, przygotowanie i wdrożenie odpowiednich działań mających na celu realizację planów na wypadek sytuacji kryzysowych oraz przywrócenie funkcji lub usług, które zostały zakłócone w wyniku zdarzenia związanego z cyberbezpieczeństwem.
Etap reakcji	Przygotowanie i wdrożenie odpowiednich działań mających na celu reakcję i odpowiedź na wykryte zdarzenie związane z cyberbezpieczeństwem. Jest to działanie krótkoterminowe i doraźne.
Etap wykrywania	Przygotowanie i wdrożenie odpowiednich działań w celu zidentyfikowania wystąpienia zdarzeń wpływających na cyberbezpieczeństwo.

Exploit	Gotowe narzędzie, udostępniane zazwyczaj w formie skryptu lub kodu źródłowego, służące do wykorzystania określonej podatności.
Format string	Działania polegające na wykorzystaniu błędnego sposobu przekazywania argumentów do funkcji operujących na ciągach znaków. Ich celem jest napisanie i zastosowanie takiego programu, który poprzez wykorzystanie błędnego sposobu przekazywania argumentów umożliwia wklejenie łańcucha znaków w odpowiednim polu tak, aby przemycić niebezpieczny kod do źle zabezpieczonej aplikacji.
Haszować, haszowanie	Proces polegający na utworzeniu skrótu (hash) za pomocą jednokierunkowej funkcji skrótu. Przykładowy hash wygenerowany z użyciem funkcji skrótu MD5 dla wyrażenia „SRK CYBER" – „e9ea2a5425f062c8c5b003c525a2dc2d"
IaaS	Infrastruktura jako usługa (ang. Infrastructure as a Service) – jeden z modeli, obok SaaS (ang. Software as a Service) i PaaS (ang. Platforma as a Service), usługi przetwarzania w chmurze, w którym zasoby obliczeniowe są hostowane w chmurze. Dostawca usługi hostuje fizyczną infrastrukturę, oprogramowanie oraz sieć o określonej przepustowości.
Incydent	Zdarzenie lub zespół niepożądanych lub/i niespodziewanych zdarzeń związanych z cybezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłóceń działań biznesowych.
IoT	IoT (ang. Internet of Things) – koncepcja wykorzystywania urządzeń niebędących typowymi komputerami (na przykład elektroniki użytkowej w gospodarstwach domowych) do budowy sieci urządzeń gromadzących i przetwarzających dane oraz komunikujących się ze sobą za pomocą sieci komputerowej lub innej.

IQ	Kwalifikacja Instalacyjna (IQ ang. Installation Qualification) – udokumentowane sprawdzenie i potwierdzenie, że zainstalowane lub zmodyfikowane urządzenie, oprogramowanie lub system jest zgodne z zatwierdzonym projektem, zaleceniami producenta lub wymaganiami użytkownika.
Klasy ataków SQL Injection	Ataki typu SQL Injection polegają na wykorzystaniu błędów programistycznych, głównie w językach skryptowych (PHP, ASP itd.). Błędy te polegają na braku filtrowania danych wejściowych, które wykorzystywane są do dynamicznie generowanych zapytań SQL i przez co możliwa jest zmiana całości lub fragmentu zapytania do systemu bazodanowego. Wykorzystanie podatności aplikacji na ataki wstrzyknięcia kodu SQL może doprowadzić do ujawnienia zawartości bazy danych lub jej modyfikacji.
Klasy ataków XSS	Atak XSS (ang. Cross Site Scripting) polega na wstrzyknięciu do przeglądarki użytkownika fragmentu kodu JavaScript bądź innego języka skryptowego, który może być uruchomiony w przeglądarce. W efekcie atakujący ma możliwość wykonania dowolnego kodu skryptowego w przeglądarce, co pozwala na wykradzenie ciasteczek sesyjnych użytkownika, a w konsekwencji przechwycenie całej jego sesji.
Klasy ataków XXE	Ataki XXE (ang. XML External Entities) są przeprowadzane w momencie parsowania dokumentu XML dostarczonego z zewnętrznego źródła. Jest to atak podobny do SQL Injection, ponieważ ma miejsce w momencie przetwarzania XML zawierającego referencje do zewnętrznych źródeł, które zostaną załadowane do treści XML.
Kod źródłowy	Szczegółowe instrukcje pisane przez programistę i zrozumiałe dla programisty przy wykorzystaniu danego języka programowania, których wykonanie przez komputer prowadzi do prezentacji wyników operacji na dostępnych danych.
Kopia bezpieczeństwa	Zestaw danych, które w przypadku ich utracenia (np. ataku wirusa, przypadkowego usunięcia) pozwolą na odtworzenie oryginalnych danych.

Kryptoanaliza	Dziedzina wiedzy dotycząca przekształcania informacji tajnej (zaszyfrowanej) w informację jawną (niezaszyfrowaną) bez konieczności posiadania klucza deszyfrującego.
Kryptografia	Dziedzina wiedzy obejmująca metody szyfrowania, czyli przekształcania informacji jawnej w informację tajną (szyfrogram). Szyfrogram jest niezrozumiały dla odbiorcy bez operacji deszyfrowania, która wymaga posiadania dodatkowej, zwykle tajnej informacji, czyli klucza deszyfrującego.
Łańcuch dostaw	Sieć podmiotów zaangażowanych w tworzenie, dystrybucję i sprzedaż produktów lub usług. Obejmuje wszystkie etapy procesu, począwszy od pozyskania surowców, poprzez produkcję, magazynowanie, transport i sprzedaż, aż do dostarczenia produktu do ostatecznego odbiorcy.
MAC adres	Każda karta sieciowa ma unikalny 48-bitowy adres MAC zakodowany w karcie, reprezentowany w notacji szesnastkowej. Znany również jako adres fizyczny. Adres MAC Ethernet ma dwie części. Pierwsze 24 bity adresu reprezentują unikatowy identyfikator organizacji. Jest to część dostawcy lub producenta adresu, np. 00-60-2F. Drugie 24 bity są przypisane przez dostawcę i unikalne w ramach jego identyfikatora, np. 3A-07-BC. Pełny zapis adresu składający się z obu częsci to 00-60-2F-3A-07-BC. Adresy mogą, oprócz identyfikacji urządzeń, służyć do komunikacji pomiędzy interfejsami sieciowymi w tej samej sieci.

Materiał dowodowy (ulotny/nieulotny)	Materiały dowodowe mogą pomóc w rekonstrukcji ataków, identyfikacji luk w zabezpieczeniach i świadczeniu dowodów w celu identyfikacji sprawców lub dowiedzenia popełnionych działań nieautoryzowanych. Materiał dowodowy ulotny w obszarze cyberbezpieczeństwa odnosi się do informacji lub śladów, które mogą istnieć tylko przez krótki czas. Przykładem są tymczasowe pliki logów, sesje połączeń sieciowych, dane w pamięci podręcznej, które mogą zawierać ważne informacje na temat ataków lub działań nieautoryzowanych. Ze względu na swoją nietrwałość, zbieranie i analiza tych materiałów ulotnych są kluczowe dla zrozumienia ataków i podejmowania odpowiednich działań naprawczych. Materiał dowodowy nieulotny w obszarze cyberbezpieczeństwa to taki, który jest trwały i może istnieć przez dłuższy czas. Obejmuje to np. kopie zapasowe danych, zrzuty stanu systemów, archiwalne pliki logów oraz nagrania zdarzeń związanych z bezpieczeństwem.
Model IACS	(ang. Industrial Automation and Control Systems) – model odnoszący się do urządzeń automatyki przemysłowej i systemów sterowania.
Model OSI	Pełna nazwa ISO OSI RM (ang. International Organization for Standardization Open Systems Interconnection Reference Model) – standard opisujący strukturę komunikacji w sieci teleinformatycznej w podziale na siedem warstw abstrakcji, takich jak: fizyczna, łącze danych, sieć, transport, sesja, prezentacja i aplikacja.
Nośnik danych	Urządzenie wykorzystywane do gromadzenia, przechowywania, przetwarzania i transmisji danych. Nośniki mogą być wewnętrzne (np. dyski twarde) oraz zewnętrzne/przenośne (np. pendrive, karta pamięci, dysk zewnętrzny czy płyta CD).

Obiekt	W kontekście cyberbezpieczeństwa termin „obiekt" może odnosić się do różnych koncepcji i aspektów. W zależności od kontekstu, obiekt w cyberbezpieczeństwie może mieć następujące znaczenia: **Obiekt danych:** W kontekście ochrony danych i prywatności obiektem może być zbiór informacji, dokument lub plik, który zawiera wrażliwe dane, takie jak dane osobowe klientów lub tajemnice handlowe. Obiekty danych są ważnym celem ochrony przed cyberatakami i naruszeniami danych. **Obiekt ataku:** W dziedzinie cyberbezpieczeństwa obiekt ataku oznacza cel, na którym atakujący próbuje przeprowadzić atak lub naruszenie. To może być konkretny system komputerowy, sieć, aplikacja lub urządzenie. **Obiekt monitoringu:** W kontekście monitoringu bezpieczeństwa obiektami monitoringu mogą być konkretne zasoby lub aktywności w systemie informatycznym, które są śledzone w celu wykrycia nieprawidłowości lub podejrzanej aktywności. Na przykład obiektem monitoringu może być ruch sieciowy, logi zdarzeń czy zmiany w konfiguracji systemu. **Obiekt kontroli dostępu:** W zarządzaniu dostępem i kontroli dostępu do zasobów informatycznych obiektem może być użytkownik, aplikacja lub urządzenie, które próbuje uzyskać dostęp do określonych zasobów. Systemy bezpieczeństwa mogą oceniać, czy dany obiekt ma uprawnienia do dostępu do określonych zasobów i czy jest to autoryzowane. **Obiekt analizy:** W analizie zagrożeń i reagowaniu na incydenty obiektem analizy mogą być dane, logi lub ślady, które są badane w celu zrozumienia natury ataku lub incydentu. To może obejmować analizę kodu złośliwego, wykrywanie anomalii w ruchu sieciowym itp. **Obiekt zarządzania ryzykiem:** W zarządzaniu ryzykiem w dziedzinie cyberbezpieczeństwa obiektami są czynniki ryzyka, które mogą wpływać na bezpieczeństwo organizacji. To mogą być systemy, aplikacje, osoby, procesy czy technologie, które są oceniane pod kątem potencjalnych zagrożeń i skutków incydentów.

OQ	Kwalifikacja Operacyjna (OQ ang. Operational Qualification): udokumentowane sprawdzenie i potwierdzenie, że zainstalowane lub zmodyfikowane urządzenie, oprogramowanie lub system działają poprawnie w całym zakresie zakładanych warunków operacyjnych.
OWASP top10	Dokument organizacji OWASP zawierający 10 najistotniejszych podatności dla aplikacji webowych. Dokument jest regularnie aktualizowany.
PaaS	Platforma jako usługa (ang. Platform as a Service) – jeden z modeli, obok IaaS i SaaS, usługi przetwarzania w chmurze, w którym dostawca udostępnia platformę programistyczną lub developerską.
Phishing	Forma cyberataków, które polegają na próbie oszukania lub wyłudzenia poufnych informacji od użytkowników internetu, takich jak hasła, numery kart kredytowych, dane osobowe czy inne wrażliwe dane. Atak phishingowy jest zazwyczaj przeprowadzany przez cyberprzestępców, którzy udają inne, godne zaufania źródło, aby wprowadzić swoje ofiary w błąd i skłonić je do ujawnienia swoich poufnych informacji.
Podatność	Słabość aktywów lub zabezpieczenia, która może być wykorzystana przez zagrożenia rozumiane jako potencjalna przyczyna niepożądanego incydentu mogącego wywołać szkodę w systemie lub organizacji.
PQ	Kwalifikacja Procesu (Działania) (PQ ang. Performance Qualification): udokumentowane sprawdzenia i potwierdzenia, że urządzenia i instalacje pomocnicze, połączone w jedną funkcjonalną całość, mogą pracować efektywnie i powtarzalnie zgodnie z zatwierdzoną metodą prowadzenia procesu i specyfikacjami.
Programowanie	Proces tworzenia i rozwijania programów komputerowych poprzez formułowanie instrukcji, które komputer może zrozumieć i wykonywać. Programowanie jest fundamentalnym elementem informatyki i polega na tworzeniu algorytmów, czyli sekwencji logicznych kroków, które określają, jakie działania ma wykonać komputer.

Redteaming	Ogół działań podejmowanych przez zespół (ang. red team), którego celem jest zasymulowanie ataku na określoną organizację lub część jej struktury. Red teaming ma na celu sprawdzenie poziomu bezpieczeństwa organizacji i prawidłowego działania jej systemów zabezpieczeń, zarówno informatycznych (np. systemy antywirusowe, zapobiegania wyciekom danych, zapory sieciowe itd.), technicznych (systemy kontroli dostępu, monitoringu wizyjnego), jak i organizacyjnych (odpowiednio przygotowane, wdrożone i przestrzegane polityki i procedury bezpieczeństwa). Red teaming wykorzystuje metody znane z testów penetracyjnych, testów bezpieczeństwa fizycznego i testów socjotechnicznych, ale nie ogranicza się do ich zakresu, będąc zazwyczaj działaniem bardziej rozciągniętym w czasie, zakresie i wykorzystywanych technikach od testów penetracyjnych. Zazwyczaj celem red teamingu jest uzyskanie dostępu do określonego zasobu (np. wykradnięcie jakichś informacji) lub dotarcie do miejsca objętego kontrolą dostępu.
Reverse Engineering	Inżynieria odwrotna/inżynieria wsteczna (ang. reverse engineering) – ogół czynności prowadzących do odzyskania ze skompilowanego kodu maszynowego (dostępnego zazwyczaj w formie plików wykonywalnych analizowanych programów) instrukcji stanowiących kod źródłowy. Inżynieria wsteczna pozwala także na odtworzenie i ustalenie wymagań oraz przyjętych rozwiązań projektowych badanego oprogramowania, wykonywanych operacji, wykorzystywanych protokołów komunikacyjnych i zastosowanych algorytmów. Inżynieria wsteczna może być prowadzona w celu audytu bezpieczeństwa analizowanych aplikacji, wyeliminowania zabezpieczeń zastosowanych przez twórców oprogramowania (np. blokady kopiowania, sprawdzania aktywacji systemu) lub próbie stworzenia własnego rozwiązania na podstawie cudzej pracy. Inżynieria wsteczna może dotyczyć też urządzeń (np. sprzętu komputerowego) i protokołów komunikacyjnych.

Rozwiązania chmurowe	Nowoczesne usługi polegające na udostępnianiu przez podmioty wyspecjalizowane (dostawcę) swojej mocy obliczeniowej, przestrzeni dyskowej czy środowiska programistycznego lub gotowych aplikacji. Użytkownik nie musi posiadać licencji na używanie aplikacji czy inwestować w przestrzeń dyskową, a dzięki tej odpłatnej usłudze może w pełni wykorzystywać ich funkcjonalność. Do największych zalet rozwiązań chmurowych należą: redukcja kosztów, stała dostępność do zasobów, możliwość pracy zespołów rozproszonych oraz standaryzowanie, uelastycznienie i dopasowywanie usług do bieżących potrzeb.
SaaS	Oprogramowanie jako usługa (ang. Software as a Service) – jeden z modeli, obok IaaS i PaaS, usługi przetwarzania w chmurze. Dostawca usługi hostuje oprogramowanie klienta.
Sektor	Jeden z działów gospodarki, np. sektor: energetyczny, farmeceutyczny etc. Sektor dzieli się na branże.
Sieci	Połączenie urządzeń w celu wymiany danych między nimi. Urządzenia komunikują się ze sobą za pomocą mediów transmisyjnych, wykorzystując odpowiednie protokoły komunikacyjne.
Sieci AIM	Część systemów zautomatyzowanego zarządzania infrastrukturą AIM, czyli rozwiązania udostępniającego funkcje ilustrowania, zarządzania, analizy i planowania.
Skanowanie	Działanie, które po zbadaniu portów, adresów IP, hostów oraz sieci pozwala zidentyfikować aktywne urządzenia, rozpoznać uruchomione serwisy oraz systemy operacyjne i dostarczyć informacji o zaistniałych zdarzeniach, np. powstałych lukach w zabezpieczeniach czy potencjalnych zagrożeniach. Skanowanie pomaga również rozpoznać topologię sieci i konfigurację urządzeń dostępowych oraz wskazać otwarte porty.
Skrypt	Krótki program komputerowy lub zestaw instrukcji, które są używane do wykonywania określonych działań lub zadań w środowisku informatycznym. Skrypty mogą być używane zarówno w celach bezpieczeństwa, jak i w innych aspektach zarządzania systemem lub automatyzacji procesów. Co do zasady skrypty nie są kompilowane i nie wymagają jej do działania.

Sniffing	Czynności polegające na monitorowaniu przepływu informacji w sieci oraz analizowaniu tych informacji.
SOC	Security Operations Center – całodobowa usługa (24/7/365) składająca się z pracy systemów teleinformatycznych oraz ekspertów ds. bezpieczeństwa. Pozwala ona wynajętym specjalistom na analizowanie zasobów teleinformatycznych pod kątem ich bezpieczeństwa oraz reagowanie na ewentualnie pojawiające się incydenty.
Socjotechnika	Socjotechnika (inżynieria społeczna) – czynności wywierania wpływu na ludzi, praktyczne zastosowanie podstępu poprzez stosowanie środków psychologicznych i metod manipulacji mających na celu wyłudzenie określonych informacji bądź nakłonienie do realizacji określonych działań. Celem takiego działania jest nieautoryzowane pozyskanie poufnych lub niedostępnych w inny sposób informacji. Podstawowe metody socjotechniki to np. perswazja, manipulacja, intensyfikacja lęku.
Środowisko	Ogół warunków funkcjonowania danego podmiotu w przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami, scharakteryzowany przez wyzwania (szanse i ryzyka) oraz zagrożenia dla osiągania przyjętych celów.
SSRF	Podatności SSRF (ang. Server-Side Request Forgery) występują, gdy aplikacja internetowa pobiera dane z zewnętrznych zasobów bez walidacji adresu URL podanego przez użytkownika. Pozwala to wymusić na aplikacji wysłanie spreparowanego requestu (żądania) do nieoczekiwanego miejsca docelowego, nawet gdy znajduje się ono w sieci lokalnej lub jest zabezpieczone VPN, firewallem lub ma aktywną listę ACL.
SSTI	Server-Side Template Injection – podatność umożliwiająca zdalne wykonanie kodu poprzez przygotowanie odpowiednio spreparowanego wejścia (payload) z wykorzystaniem natywnej składni specyficznej dla wykorzystanego silnika szablonów.

System	Układ współpracujących ze sobą dwóch składowych: sprzętu komputerowego (hardware) oraz oprogramowania (software) w celu osiągnięcia założonego celu. Na system składa się kilka warstw: sprzętowa, system operacyjny, programy narzędziowe, programy użytkowe oraz wykorzystujący go użytkownicy.
Systemy DLP	Data Loss/Leakage Prevention – system do wykrywania i zapobiegania wyciekowi danych.
Systemy IT	Information Technology – systemy komputerowe, sieci i oprogramowania służące do przetwarzania informacji. Składają się one zazwyczaj z komputera lub komputerów połączonych siecią, oprogramowania oraz urządzeń peryferyjnych: drukarek, skanerów, myszki, klawiatury itp.
Systemy OT	Operational Technology – wszelkie urządzenia i systemy (software) służące do zarządzania i monitorowania pracy w środowiskach produkcyjnych i przemysłowych. Ich głównym zadaniem jest wspomaganie mające na celu poprawę wydajności produkcji i bezpieczeństwa operacyjnego.
Systemy SOAR	Security Orchestration, Automation, and Response – trzy elementy (orkiestracja, automatyzacja i reagowanie na zdarzenia) współdziałające w celu znalezienia i powstrzymania ataków. Orkiestracja to połączenie w jednym centralnym miejscu różnych narzędzi wewnętrznych i zewnętrznych, co pozwala na skonsolidowanie danych i usprawnienie procesów pod automatyzację. Automatyzacja to zaprogramowanie zadań za pomocą odpowiednich procedur w taki sposób, aby były wykonywane automatycznie. Reagowanie na zdarzenia to podejmowanie właściwych reakcji na ewentualne zagrożenia i incydenty. Systemy SOAR umożliwiają szybsze i dokładniejsze reagowanie na ewentualne incydenty oraz zmniejszają liczbę ewentualnych problemów z bezpieczeństwem pracy.

Szkodliwe oprogramowanie	Szkodliwe oprogramowanie, znane również jako malware – rodzaj oprogramowania stworzonego z zamiarem wyrządzenia szkód, kradzieży informacji lub przeprowadzenia innych nielegalnych działań na komputerze, sieci lub urządzeniach. Szkodliwe oprogramowanie jest tworzone przez cyberprzestępców w celu osiągnięcia korzyści finansowych, szkodzenia innym lub pozyskiwania poufnych danych.
Ślad cyfrowy	Ślad cyfrowy (ang. Forensic Artifact) – każda informacja pozostawiona w systemach teleinformatycznych przez użytkownika (w tym urządzeniach końcowych, na serwerach, w sieci komputerowej itd.), którego działania są przedmiotem badania analizy śledczej. Zebrane ślady cyfrowe stanowią cyfrowy materiał dowodowy.
Test penetracyjny	Test penetracyjny (ang. penetration test, pentest) – test bezpieczeństwa systemu informatycznego, którego celem jest wykrycie podatności (słabości) tego systemu poprzez próbę odzworowania działań, które mogą być wykonywane przez atakującego podczas rzeczywistego ataku komputerowego. Testy penetracyjne mogą być prowadzone manualnie przez testera lub w sposób częściowo zautomatyzowany i wykorzystują gotowe lub specjalnie przygotowane exploity, tj. metody wykorzystania podatności obecnych w systemach komputerowych celem wykonania pożądanego przez atakującego działania, najczęściej wykonania programu przygotowanego przez atakującego lub zwiększenia jego uprawnień. Cechą charakterystyczną testów penetracyjnych jest nie tylko poprzestanie na wyszukiwaniu podatności, ale próba ich wykorzystania (sprawdzenia, czy da się „włamać" do systemu). Testy penetracyjne mogą obejmować działania w postaci testów bezpieczeństwa fizycznego (dostania się przez testującego do obszaru chronionego kontrolą dostępu, np. chronionego budynku), a także działań socjotechnicznych.

Umowy OLA i SLA	Umowa SLA (ang. Service Level Agreement) – umowa o gwarantowanym poziomie świadczenia usług, określająca, na jakim minimalnym poziomie dostawca świadczyć będzie określone usługi klientowi. Umowa OLA (ang. Operational Level Agreement) określa zobowiązania wewnętrzne pomiędzy operacyjnymi jednostkami zapewniającymi poziom świadczenia usług. Celem tego kontraktu jest zagwarantowanie poziomu usług ustalonego w OLA, głównie utrzymania i rozwoju.
Usługi katalogowe	Usługa katalogowa (ang. Directory Service) – usługa będąca specjalizowaną bazą danych, pozwalająca na przechowywanie, przetwarzanie i odwzorowywanie relacji pomiędzy obiektami obecnymi w usłudze katalogowej, którymi typowo są użytkownicy, aplikacje, komputery, serwery i inne urządzenia komputerowe. Usługi katalogowe pozwalają na budowanie hierarchicznych grup obiektów, ułatwiają zarządzanie nimi (np. zarządzanie uprawnieniami poszczególnych grup). Jednym z najpopularniejszych standardów usług katalogowych jest ITU-T X.500, implementowany jako protokół LDAP (ang. Lightweight Directory Access Protocol). Jednym z najpopularniejszych komercyjnych rozwiązań usługi katalogowej jest Active Directory.
Uwierzytelnianie	Weryfikacja tożsamości osoby, aplikacji lub systemu. Jest to sprawdzenie, czy podmiot, który próbuje uzyskać dostęp, jest tym, za kogo się podaje. Proces uwierzytelniania może obejmować używanie haseł, certyfikatów, biometrycznych danych (takich jak odciski palców lub rozpoznawanie twarzy) albo innych metod.
Zdarzenie	Zachowanie w systemach informatycznych, np. logowanie do komputera. Może mieć charakter zgodny z procedurami, standardami lub niezgodny. W drugim wypadku mówimy o anomalii.