Špecialista pre riešenie kybernetických incidentov

Rola:	**Špecialista pre riešenie kybernetických incidentov**	
Vedomosti:	**Riadenie bezpečnosti**	
	1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti	BL2
	2) zásady organizácie informačnej a kybernetickej bezpečnosti	BL2
	3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti	BL6
	4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí	BL5
	5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.)	BL5
	6) zdroje, charakteristiky a použitie informačných aktív organizácie	BL6
	7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami	BL6
	8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI)	BL5
	9) procesy riadenia kontinuity činností a plánovania havarijnej obnovy prevádzky	BL5
	10) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.)	BL4
	11) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.)	BL5
	12) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby	BL5
	13) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.)	BL6
	14) zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku	BL5
	15) charakteristiky fyzických a virtuálnych nosičov údajov	BL5
	16) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu,	BL6

	digitálne fotoaparáty, digitálne skenery, pevné disky, pamäťové karty, modemy, sieťové komponenty, sieťové zariadenia, sieťové domáce ovládacie zariadenia, tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.)	
	17) elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér)	BL5
	18) koncepcia a mechanizmy zálohovania a obnovy dát	BL6
	19) kryptografické algoritmy	BL5
	20) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia)	BL5
	21) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov	BL5
	22) metódy a politiky správy a štandardizácie údajov	BL6
	23) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti	BL6
	24) princípy dolovania a ukladania údajov	BL6
	25) princípy elektronickej pošty, vyhľadávacích/analytických techník, nástrojov a používania súborov cookie	BL6
	26) princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML)	BL6
	27) princípy zálohovania a obnovy dát	BL6
	28) programovacie rozhrania pre prístup k databázam	BL5
	29) šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN)	BL5
	30) systémy riadenia bázy dát a ich správa, dopytovacie jazyky, tabulkové vzťahy	BL5
	31) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL4
	32) technológie filtrovania webového obsahu	BL5
	33) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL6
	34) typy sieťovej komunikácie (napr LAN, WAN, MAN, WLAN, WWAN)	BL6
	35) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL5
	36) XML schémy (Extensible Markup Language)	BL5
	37) koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky	BL6
	38) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér,	BL6

	aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	
	39) princípy zraniteľností bezdrôtových sietí	BL6
	Riadenie hrozieb a rizík	
	1) procesy riadenia rizík, postupy a metodiky analýzy rizík	BL5
	2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie	BL6
	3) zásady aplikačnej bezpečnosti	BL6
	4) teória, koncepty a metódy systémového inžinierstva	BL5
	5) metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru	BL4
	6) bezpečnostné koncepty v operačných systémoch	BL6
	7) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)	BL5
	8) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL6
	9) nástroje na posudzovanie zraniteľností	BL6
	10) sieťové protokoly a adresárové služby	BL6
	11) architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL6
	12) prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL6
	13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL6*
	14) posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL6
	15) princípy a techniky etického hackingu	BL6
	16) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny)	BL6
	17) triedy a vektory útokov	BL6
	Aplikácia bezpečnostných opatrení	
	1) navrhovanie opatrení na ošetrenie bezpečnostných rizík	BL6
	2) bezpečnostné mechanizmy a spôsob ich implementácie	BL6
	3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti	BL6

	4) nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL5
	5) zásady personálnej bezpečnosti	BL6
	6) opatrenia týkajúce sa používania, spracovania, uchovávania a prenosu údajov	BL6
	7) zásady a princípy riadenia identít a prístupov	BL6
	8) kryptografické bezpečnostné mechanizmy	BL5
	9) koncepcie a technológie vzdialeného prístupu	BL5
	10) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL6
	11) zabezpečenie virtuálnych privátnych sietí (VPN)	BL6
	12) techniky a metódy správy systémov a hardeningu systémov	BL6
	Výkon operatívnych bezpečnostných činností	
	1) procesy riešenia kybernetických bezpečnostných incidentov	BL6
	2) znalosti o štádiách kybernetického útoku (napr. prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahladenie stôp)	BL6
	3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL6
	4) princípy logovania a bezpečnostného monitorovania	BL6
	5) princípy korelácie bezpečnostných udalostí	BL6
	6) identifikácia digitálnych stôp a postupy pri ich spracúvaní	BL6
	7) princípy, nástroje a techniky testovania prieniku	BL6
	8) analýza sieťového prenosu (nástroje, metodiky, procesy)	BL6
	9) bezdrôtové technológie (napr. celulárne, satelitné, GSM) zahŕňajúce základnú štruktúru, architektúru a dizajn moderných bezdrôtových komunikačných systémov	BL6
	10) charakteristiky komunikačných sietí (napr. kapacita, funkčnosť, trasy, kritické uzly)	BL6
	11) forenzné súvislosti štruktúry a procesov operačného systému	BL6
	12) koncepcia architektúry sietí vrátane topológie, protokolov, komponentov a bezpečnostných princípov	BL6
	13) konfigurácia forenzných laboratórií a podporných aplikácií (napr VMWare, Wireshark)	BL6
	14) mechanizmy zabezpečenia siete (napr. Host based IDS, IPS, ACL) vrátane ich funkcií a umiestnenia v sieti	BL6
	15) metódy a nástroje analýzy sieťového prenosu	BL6
	16) porty a služby Windows/Unix	BL6

	17) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL6
	18) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti	BL6
	19) princípy sieťových demilitarizovaných zón	BL6
	20) princípy súborových systémov (napr. NTFS, FAT a iné)	BL6
	21) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL6
	22) bezpečnostné zásady správy a údržby databázových systémov	BL5
	23) zásady riadenia bezpečnosti prostredia cloudu	BL6
	24) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií	BL6
	25) zásady riadenia sieťových systémov, modely, metódy (napr. monitorovanie výkonnosti systémov end-to-end)	BL5
	26) princípy zraniteľností bezdrôtových sietí	BL6
	Riadenie súladu	
	1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť	BL3
	2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na ochranu osobných údajov	BL3
	3) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií	BL3
	4) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky	BL3
	5) princípy posudzovania kybernetickej bezpečnosti	BL5
	6) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii	BL4
	7) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín	BL4
	8) štandardy bezpečnosti platobných kariet (PCI)	BL5*
	9) štandardy a procesy riadenia rizík v dodávateľskom reťazci	BL5
	10) metódy testovania a vyhodnocovania bezpečnosti systémov	BL5
Zručnosti:	**Riadenie bezpečnosti**	
	a) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie	
	b) správa bezpečnosti informačných aktív organizácie	

	Riadenie hrozieb a rizík a) implementácia procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík b) posudzovanie hrozieb a rizík c) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí d) hodnotenie technických zraniteľností systémov e) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov f) koordinácia procesov obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning) **Aplikácia bezpečnostných opatrení** a) zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení b) návrhy zmien a integrácie bezpečnostných technológií a riešení c) podpora riadenia bezpečnostnej architektúry **Výkon operatívnych bezpečnostných činností** a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) prevádzka technických bezpečnostných opatrení **Riadenie súladu** a) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti b) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) analytické myslenie d) tvorivosť (kreativita) e) schopnosť organizovania a plánovania práce

Požiadavky označené * sú odvetvovo závislé. Pre príslušnú rolu sú posudzované v kontexte kompetencií, potrebných na vykonávanie určitej pracovnej činnosti v konkrétnom odvetví.