

Špecialista pre analýzu digitálnych stôp

Rola:	Špecialista pre analýzu digitálnych stôp	
Vedomosti:	<p>Riadenie bezpečnosti</p> <ol style="list-style-type: none"> 1) zásady organizácie informačnej a kybernetickej bezpečnosti 2) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti 3) princípy riadenia IT služieb, správy systémov a správy počítačových sietí 4) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.) 5) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) 6) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby 7) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) 8) charakteristiky fyzických a virtuálnych nosičov údajov 9) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu, digitálne fotoaparáty, digitálne skenery, pevné disky, pamäťové karty, modemy, sieťové komponenty, sieťové zariadenia, sieťové domáce ovládacie zariadenia, tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.) 10) elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér) 11) koncepcia a mechanizmy zálohovania a obnovy dát 12) kryptografické algoritmy 13) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia) 14) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov 15) metódy a politiky správy a štandardizácie údajov 16) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti 17) princípy dolovania a ukladania údajov 18) princípy elektronickej pošty, vyhľadávacích/analytických techník, nástrojov a používania súborov cookie 19) princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML) 	<p>BL4</p> <p>BL4</p> <p>BL4</p> <p>BL5</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL5</p> <p>BL5</p> <p>BL5</p> <p>BL5</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL6</p>

20) princípy zálohovania a obnovy dát	BL6
21) programovacie rozhrania pre prístup k databázam	BL5
22) šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN)	BL5
23) systémy riadenia bázy dát a ich správa, dopytovacie jazyky, tabuľkové vzťahy	BL5
24) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL5
25) technológie filtrovania webového obsahu	BL5
26) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL6
27) typy sieťovej komunikácie (napr. LAN, WAN, MAN, WLAN, WWAN)	BL6
28) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL5
29) XML schémy (Extensible Markup Language)	BL5
30) koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky	BL6
31) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér, aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	BL6
32) 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	BL5
3) zásady aplikačnej bezpečnosti	BL5
4) teória, koncepty a metódy systémového inžinierstva	BL5
5) bezpečnostné koncepty v operačných systémoch	BL5
6) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)	BL5
7) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL6
8) nástroje na posudzovanie zraniteľností	BL6
9) sieťové protokoly a adresárové služby	BL6
10) architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL6

11) prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL6
12) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL5*
13) posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL6
14) princípy a techniky etického hackingu	BL5
15) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny)	BL6
16) triedy a vektory útokov	BL6
Aplikácia bezpečnostných opatrení	
1) bezpečnostné mechanizmy a spôsoby ich implementácie	BL6
2) opatrenia týkajúce sa používania, spracovania, uchovávanía a prenosu údajov	BL6
3) zásady a princípy riadenia identít a prístupov	BL6
4) koncepcie a technológie vzdialeného prístupu	BL6
5) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL6
6) zabezpečenie virtuálnych privátnych sietí (VPN)	BL6
7) 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, zahľadanie 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	BL5
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	BL6
23) zásady riadenia bezpečnosti prostredia cloudu	BL6
24) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií	BL6
25) princípy zraniteľností bezdrôtových sietí	BL5
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) štandardy bezpečnosti platobných kariet (PCI)	BL5*
8) metódy testovania a vyhodnocovania bezpečnosti systémov	BL5

Zručnosti:	<p>Riadenie bezpečnosti</p> <ul style="list-style-type: none"> • podpora riadenia informačnej a kybernetickej bezpečnosti organizácie <p>Riadenie hrozieb a rizík</p> <ol style="list-style-type: none"> a) posudzovanie hrozieb a rizík b) hodnotenie technických zraniteľností systémov c) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov <p>Aplikácia bezpečnostných opatrení</p> <ul style="list-style-type: none"> • predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie <p>Výkon operatívnych bezpečnostných činností</p> <ul style="list-style-type: none"> • výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe <p>Riadenie súladu</p> <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a) schopnosť myslieť a konať v súvislostiach b) analytické myslenie c) tvorivosť (kreativita) d) prezentačná zručnosť

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