

## Analytik/analytička kybernetické bezpečnosti (kód: 18-016-T)

<b>Autorizující orgán:</b>	Národní úřad pro kybernetickou a informační bezpečnost
<b>Skupina oborů:</b>	Informatické obory (kód: 18)
<b>Týká se povolání:</b>	Analytik kybernetické bezpečnosti
<b>Kvalifikační úroveň NSK - EQF:</b>	7

### Odborná způsobilost

Název	Úroveň
Aplikace právních základů kybernetické bezpečnosti při analýze incidentů	5
Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti	5
Identifikace kybernetické hrozby a typu útoku pro potřeby analýzy kybernetické bezpečnosti	7
Analýza kybernetických hrozeb při využití technických prostředků kybernetické bezpečnosti (security devices)	7
Využití informací o kybernetických hrozbách - cyber threat intelligence	7

### Platnost standardu

Standard je platný od: 20.05.2025

## Kritéria a způsoby hodnocení

### Aplikace právních základů kybernetické bezpečnosti při analýze incidentů

Kritéria hodnocení	Způsoby ověření
a) Orientovat se v obsahu jednotlivých částí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, které jsou zaměřeny na analýzu incidentů	Ústní ověření
b) Vysvětlit části prováděcích předpisů vztahujících se k zákonu č. 181/2014 Sb. (vyhláška č. 82/2018 Sb. a nařízení vlády č. 432/2010 včetně jeho pozdějších příloh a změn), ve znění pozdějších předpisů, které jsou zaměřeny na analýzu incidentů	Ústní ověření
c) Vyplnit hlášení kybernetického bezpečnostního incidentu	Praktické předvedení

**Je třeba splnit všechna kritéria.**

### Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Definovat metody sběru dat v kybernetické bezpečnosti a jejich zpracování	Ústní ověření
b) Provést analýzu údajů a sběru dat pro kybernetickou bezpečnost	Praktické předvedení a ústní ověření
c) Vysvětlit postup při zpracování zpráv a výkazů pro dohledové centrum, požadavky rozlišení adresátů v souladu se zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy	Ústní ověření
d) Charakterizovat základní pojmy a procesy CSIRT týmů (ve smyslu RFC 2350)	Ústní ověření
e) Vysvětlit pojem threat hunting s uvedením příkladů nad různými druhy dat	Ústní ověření
f) Popsat a vysvětlit hlavní funkce SIEM	Ústní ověření
g) Prezentovat metody sběru dat v kybernetické bezpečnosti a jejich zpracování	Praktické předvedení a ústní ověření

**Je třeba splnit všechna kritéria.**

### Identifikace kybernetické hrozby a typu útoku pro potřeby analýzy kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Uvést jednotlivé kategorie útoků – síťové útoky, útoky na uživatele, útoky na koncové stanice	Ústní ověření
b) Popsat DDoS a uvést typově podobné hrozby	Ústní ověření
c) Vysvětlit pojem malware a specifikovat další typy škodlivého kódu	Ústní ověření
d) Vysvětlit phishing a uvést typově podobné hrozby	Ústní ověření
e) Vysvětlit sniffing a uvést typově podobné hrozby	Ústní ověření
f) Vysvětlit pojem drive-by download a uvést typově podobné hrozby	Ústní ověření
g) Popsat známý rozsáhlý kybernetický útok dle výběru uchazeče a vysvětlit jeho části	Ústní ověření

**Je třeba splnit všechna kritéria.**

**Analýza kybernetických hrozeb při využití technických prostředků kybernetické bezpečnosti (security devices)**

Kritéria hodnocení	Způsoby ověření
a) Specifikovat nástroje pro ochranu integrity komunikačních sítí	Ústní ověření
b) Specifikovat nástroje pro ověřování identity uživatelů a řízení přístupových oprávnění	Ústní ověření
c) Specifikovat nástroje pro ochranu před škodlivým kódem	Ústní ověření
d) Specifikovat nástroje pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů	Ústní ověření
e) Specifikovat nástroje pro detekci kybernetických bezpečnostních událostí a nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	Ústní ověření
f) Předvést možnosti nastavení zaznamenávání činností (logování) OS Windows nebo Linux	Praktické předvedení

**Je třeba splnit všechna kritéria.**

**Využití informací o kybernetických hrozbách - cyber threat intelligence**

Kritéria hodnocení	Způsoby ověření
a) Popsat fáze kybernetického útoku - cyber kill chain	Ústní ověření
b) Vysvětlit pojem indikátory kompromitace systému (IoCs)	Ústní ověření
c) Vysvětlit pojem TTP - taktiky, techniky a postupy	Ústní ověření
d) Popsat MITRE ATT&CK framework	Ústní ověření
e) Namapovat TTP známé skupiny útočníků dle výběru uchazeče na MITRE ATT&CK framework	Praktické předvedení a ústní ověření

**Je třeba splnit všechna kritéria.**

## Organizační a metodické pokyny

### Pokyny k realizaci zkoušky

#### 1. Vstupní předpoklady pro účast na zkoušce

Uchazečem o zkoušku může být každá fyzická osoba starší 18 let, která získala alespoň základy vzdělání, nebo účastník rekvalifikace podle zákona č. 435/2004 Sb., zákon o zaměstnanosti.

Zdravotní způsobilost není vyžadována.

Autorizovaná osoba zároveň s odesláním pozvánky ke zkoušce písemnou formou sdělí, kde a jakým způsobem se uchazeč může informovat o svých povinnostech a průběhu zkoušky a které doklady/dokumenty musí uchazeč předložit bezprostředně před započítáním zkoušky.

Autorizovaná osoba informuje žadatele písemnou formou v předstihu minimálně 7 dní o vybraných technologiích (HW a SW) a platformách zvolených pro vykonání zkoušky.

#### 2. Průběh zkoušky

Před zahájením zkoušky uchazeč předloží zkoušejícímu průkaz totožnosti a případně další dokumenty opravňující k připuštění ke zkoušce uvedené v části 1. Vstupní předpoklady pro účast na zkoušce.

Bezprostředně před zahájením zkoušky autorizovaná osoba seznámí uchazeče s pracovištěm, s organizací zkoušky, s jeho právy a povinnostmi v rámci zkoušky dle zákona č. 179/2006 Sb. a s požadavky bezpečnosti a ochrany zdraví při práci (BOZP) a požární ochrany (PO), o čemž bude autorizovanou osobou vyhotoven a uchazečem podepsán písemný záznam.

Zkoušející uzná, a tedy nemusí ověřovat, ty odborné způsobilosti, které byly již dříve u uchazeče ověřeny v rámci zkoušky z jiné profesní kvalifikace (nutno doložit osvědčením o získání profesní kvalifikace), a které jsou shodné svým rozsahem i obsahem. Rozsah a obsah odborné způsobilosti určují její jednotlivá kritéria a pokyny k realizaci zkoušky popsané v hodnoticím standardu. Zkoušející tyto odborné způsobilosti neuzná jako již ověřené, pokud by tím nebylo zajištěno řádné ověření ostatních požadavků stanovených tímto hodnoticím standardem (například při nutnosti dodržení technologických postupů a časové souslednosti různých činností).

Zkouška se koná v českém jazyce.

Zkouška je veřejná. Praktická část zkoušky a praktická zkouška není veřejná v případech, kdy to je nutné z hygienických důvodů nebo z důvodu ochrany zdraví a bezpečnosti práce.

#### Pokyny k jednotlivým způsobům ověřování:

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „ústní ověření“:

- jsou ověřována formou individuálního pohovoru obou členů zkušební komise s uchazečem, tj. s vyloučením možnosti, že by odpovědi aktuálně zkoušeného uchazeče slyšel jiný uchazeč / ostatní uchazeči,
- tato kritéria se ověřují například v odděleném samostatném prostoru (místnosti) nebo takovým způsobem, kdy je zaručeno individuální zkoušení uchazeče,
- přítomnost obou členů zkušební komise po celou dobu ústního ověřování je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „praktické předvedení a ústní ověření“:

- jsou ověřována tak, že uchazeč nejprve prakticky předvede požadovanou činnost a poté (nikoliv však nutně bezprostředně) na pokyn zkušební komise svou činnost obhájí, odpoví na otázky,
- přítomnost obou členů zkušební komise po celou dobu ověřování formou praktického předvedení a ústního ověření je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „praktické předvedení“:

- přítomnost obou členů zkušební komise po celou dobu ověřování formou praktického předvedení je vyžadována.

#### Specifické pokyny k vybraným odborným způsobilostem a kritériím:

K ověření odborné způsobilosti *Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti*, kritérium b) autorizovaná

osoba vytvoří 3 případové studie, z nichž si uchazeč při zkoušce vylosuje jednu. Výsledek řešení případové studie zpracuje uchazeč písemně na místě a následně postoupí k ústnímu ověření.

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby, je oprávněna předčasně ukončit zkoušku, pokud vyhodnotí, že v důsledku činnosti uchazeče bezprostředně došlo k ohrožení nebo bezprostředně hrozí nebezpečí ohrožení zdraví, života a majetku či životního prostředí. Zdůvodnění předčasného ukončení zkoušky uvede autorizovaná osoba do záznamu o průběhu a výsledku zkoušky. Uchazeč může ukončit zkoušku kdykoliv v jejím průběhu, a to na vlastní žádost.

## Výsledné hodnocení

Zkoušející hodnotí uchazeče zvlášť pro každou odbornou způsobilost a výsledek zapisuje do záznamu o průběhu a výsledku zkoušky.

Výsledné hodnocení pro danou odbornou způsobilost musí znít:

- „splnil“, nebo
- „nesplnil“ v závislosti na stanovení závaznosti, resp. nezávaznosti jednotlivých kritérií u každé odborné způsobilosti.

Výsledné hodnocení zkoušky zní buď:

- „vyhověl“, pokud uchazeč splnil všechny odborné způsobilosti, nebo
- „nevyhověl“, pokud uchazeč některou odbornou způsobilost nesplnil. Při hodnocení „nevyhověl“ uvádí autorizovaná osoba vždy zdůvodnění, které uchazeč svým podpisem bere na vědomí.

## Počet zkoušejících

Zkouška probíhá před zkušební komisí složenou ze dvou členů. Všichni členové komise musí být přítomni u zkoušky po celou dobu trvání zkoušky.

Zkoušející je povinen provádět ověřování odborných způsobilostí při zkoušce přesně podle všech ustanovení tohoto hodnotícího standardu.

## Požadavky na odbornou způsobilost autorizované osoby, resp. autorizovaného zástupce autorizované osoby

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby musí splňovat alespoň jednu z následujících variant požadavků:

- a) Vysokoškolské vzdělání magisterského stupně v oblasti informačních a komunikačních technologií a nejméně 5 let prokázané odborné praxe v činnostech analytika kybernetické bezpečnosti.
- b) Profesionální kvalifikace Analytik/analytička kybernetické bezpečnosti (18-016-T), vysokoškolské vzdělání magisterského stupně a nejméně 5 let prokázané odborné praxe v činnostech analytika kybernetické bezpečnosti.

Žadatel o udělení autorizace prokazuje splnění požadavků na odbornou způsobilost a praxi v povolání autorizujícím orgánem, a to předložením dokladu nebo dokladů o získání odborné způsobilosti a praxe v povolání v souladu s hodnotícím standardem této profesní kvalifikace, nebo takovým postupem, který je v souladu s požadavky uvedenými v hodnotícím standardu této profesní kvalifikace autorizujícím orgánem stanoven.

Žádost o udělení autorizace naleznete na internetových stránkách autorizujícího orgánu: Národní úřad pro kybernetickou a informační bezpečnost, [www.nukib.gov.cz](http://www.nukib.gov.cz).

### Nezbytné materiální a technické předpoklady pro provedení zkoušky

- Učebna odpovídající bezpečnostním a hygienickým předpisům, stoly, židle,
- psací potřeby, papír,
- soubor 3 případových studií,
- stolní počítač nebo notebook (dostatečně výkonný natolik, aby zajistil plynulý provoz aplikací) s aktuálním operačním systémem, kancelářský software, internetové připojení,
- mobilní telefon (dostatečně výkonný, aby zajistil plynulý provoz vyžadovaných aplikací) pro ověřování kritéria b) odborné způsobilosti *Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti*,
- dataprojektor, plátno, flip-chart.

K žádosti o udělení autorizace žadatel přiloží seznam materiálně-technického vybavení dokládající soulad s požadavky uvedenými v hodnotícím standardu pro účely zkoušky. Zajištění vhodných prostor pro provádění zkoušky prokazuje žadatel odpovídajícím dokladem (např. výpis z katastru nemovitostí, nájemní smlouva, dohoda).

### Doba přípravy na zkoušku

Uchazeč má nárok na celkovou dobu přípravy na zkoušku v trvání 10 minut. Do doby přípravy na zkoušku se nezapočítává doba na seznámení uchazeče s pracovištěm, s organizací zkoušky, s požadavky BOZP a PO a s právy a povinnostmi uchazeče v rámci zkoušky dle zákona č. 179/2006 Sb.

### Doba pro vykonání zkoušky

Celková doba trvání vlastní zkoušky jednoho uchazeče (bez času na přestávky a na přípravu) je 5 až 7 hodin (hodinou se rozumí 60 minut).

## **Autoři standardu**

### **Autoři hodnotícího standardu**

Hodnotící standard profesní kvalifikace připravila SR pro informační technologie a elektronické komunikace, ustavená a licencovaná pro tuto činnost HK ČR a SP ČR.

Na tvorbě se dále podílely subjekty zastoupené v pracovní skupině:

- Network Security Monitoring Cluster, družstvo
- AXENTA, a. s.
- Jihomoravský kraj