



## POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

**Jméno studenta:** Bc. Ondřej Daniš  
**Název práce:** Využití MITRE ATT&CK pro efektivní řízení kybernetické bezpečnosti  
**Autor posudku:** Mgr. Josef Horálek, Ph.D.  
**Cíl práce:** Cílem práce je podrobně popsat projekt MITRE ATT&CK, jeho strukturu a možnosti využití pro efektivní řízení kybernetické bezpečnosti.

Povinná kritéria hodnocení práce	Stupeň hodnocení (známka)					
	A	B	C	D	E	F
Práce svým zaměřením odpovídá studovanému oboru	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vymezení cíle a jeho naplnění	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování teoretických aspektů tématu	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování praktických aspektů tématu	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adekvátnost použitých metod, způsob jejich použití	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hloubka a správnost provedené analýzy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Práce s literaturou	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logická stavba a členění práce	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jazyková a terminologická úroveň	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Formální úprava a náležitosti práce	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vlastní přínos studenta	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Využitelnost výsledků práce v teorii (v praxi)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Vyjádření k výsledku anti-plagiátorské kontroly

Anti-plagiátorská kontrola eVSKP identifikovala celkovou podobnost: 3,9 %. U jednotlivých identifikovaných zdrojů, není shoda vyšší než 1%. Převážně se jedná o obecná konstatování a popis všeobecně známých faktů.

### Dílní připomínky a náměty:

Vedoucí nemá připomínky k předložené práci.

### Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce je rozdělena do devíti kapitol včetně úvodu a závěru. Práce je zpracována systematicky a autor postupně plní vytyčené cíle ze zadání práce. Po úvodní rešerši zaměřené na vývoj rámce MITER ATT&CK následuje představení základních přístupů kybernetické bezpečnosti založeného na modelu CIA (confidentiality, integrity, availability), definování životního cyklu a pojmů KB a pohled na KB v ČR.

Obsáhlá pátá kapitola popisuje principy a rámce MITER ATT&CK s důrazem na nástroje rámce MITER ATT&CK, využití matice MITER ATT&CK. Následuje přehled definovaných taktik a technik. V sedmé kapitole je pak podrobně představeno řešení vybraných technik, jejich mitigací a ověření implementace mitigačních opatření. Na základě přiřazení zvolených technik k doporučeným

mitigacím z pohledu znalostní báze ATT&CK, autor realizoval jejich rozdělení na kategorie směřující na konkrétní oblast z pohledu nastavení systémů v rámci platforem Windows a Linux. Autor práce naplnil všechny vytyčené cíle. Práce je zpracována systematicky a na vysoké odborné úrovni. Práci doporučuji k obhajobě.

**Otázky k obhajobě:**

Nejsou

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: A**

**V Hradci Králové, dne 11. května 2022**

---

**podpis**