



## POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

**Jméno studenta:** Ondřej Daniš

**Název práce:** Využití MITRE ATT&CK pro efektivní řízení kybernetické bezpečnosti

**Autor posudku:** Vladimír Soběslav

**Cíl práce:** Na základě analýzy znalostní báze MITRE ATT&CK a bližšího průzkumu problematiky definovat relevantní taktiky a techniky cílící na základní funkcionalitu platform Windows a Linux.

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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" 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

Dle anti-plagiátorské kontroly je zde shoda 3 procenta. Analyzované shody se jeví jako minimální.

### **Dílčí připomínky a náměty:**

Práce místy obsahuje překlepy či drobné stylistické nesrovnalosti. Nejvíce viditelný je překlep MITER ATT&CK místo MITRE ATT&CK, pravděpodobně by vícekrát kopírován viz např. strana 4.

### **Celkové posouzení práce a zdůvodnění výsledné známky:**

Diplomová práce je zaměřena na problematiku kybernetické bezpečnosti se zaměřením na operační systémy Windows s Linux. Jedná se o etablované téma s dostatečným množstvím zdrojů.

Závěrečnou práci je možné rozdělit do dvou logických celků, teoretickou analýzu problematiky kybernetické bezpečnosti související s danou oblastí a část praktickou, která si klade za cíl analyzovat a pro-mapovat tzv. mitigační, respektive zmírňující opatření ze znalostní báze Mitre. Teoretickou část reprezentuje první až pátá kapitola. Tato část práce je sepsána přehledně a na slušné odborné úrovni. Autor neopomenul provést základní rešerši v dané oblasti.

V praktické části práce autor vhodně dekomponoval jednotlivé části a procesy v operačních systémech Windows a Linux a vhodně navrhl odpovídající opatření.

Celkově se jedná o pěkně zpracovanou diplomovou práci, ke které nemám zásadních výhrad. Autor jednoznačně prokázal svoji odbornou erudici a schopnost analyzovat problematiku kybernetické bezpečnosti v dané oblasti a realizovat konkrétní opatření na úrovni OS Windows a Linux.

### **Otázky k obhajobě:**

- 1) Zdůvodněte výběr daných mitigačních opatření pro operační systémy a případně jaké další byly ve vašem výběru?

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: A**

**V Hradci Králové, dne 13. května 2022**



---

**podpis**