



POSUDEK VEDOUcíHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Denis Šabacký
Název práce: Procesní a technologické řešení zajištění dat pro zpětné vyšetřování
Autor posudku: doc. Mgr. Josef Horálek, Ph.D.
Cíl práce: Cílem práce je analyzovat a navrhnout procesní a technologické postupy pro zajištění digitálních stop z bezpečnostního dohledu L1 a L2 pro zpětné vyšetřování a modelování incidentů.

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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Využitelnost výsledků práce v teorii (v praxi)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 4%. Jedná se shodu v obecných a citovaných deklaracích a pojmech, zejména při citování norem a standardů.

Dílní připomínky a náměty:

Vedoucí práce nemá žádné závažné připomínky k předložené práci.

Celkové posouzení práce a zdůvodnění výsledné známky:

Cílem práce tedy bylo identifikovat možné nedostatky ve známých standardech, ze kterých mohou společnosti vycházet při implementaci procesů sběru a zpracování digitálních stop. Dále navrhnout procesní a technologické postupy pro zajištění digitálních stop a vytvořit table-top cvičení, které by nastavení těchto procesů demonstrovalo. Autor realizoval SWOT analýzu nejvýznamnějších standardů a norem, ze které plyne, že jednotlivé standardy obsahují užitečné informace, návody a doporučení pro zpracování digitálních stop, avšak častou jsou zaměřeny na omezený sektor či užití, a hlavně některé dílní korky nedostatečně popisují. Tyto nedostatky se autor pokouší odstranit v kapitolách 6, 7 a 8, které obsahují návrh technologických, resp. procesních postupů pro zajištění digitálních stop a využití rámce MITRE ATT&CK pro modelování incidentů. V poslední části práce se autor zaměřil na

návrh table-top cvičení, jehož úkolem je simulovat možné bezpečnostní incidenty a ověřit relevantnost a vhodnost reakcí na ně. Autor splnil všechny vytyčené cíle a bakalářská práce splňuje všechny požadavky.

Otázky k obhajobě:

Nejsou

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové, dne 6. května 2024

podpis