Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Jméno studenta: Bc. Jan Nedbal

Název práce: Uživatelská behaviorální analýza pro systémy SIEM

Autor posudku: Mgr. Josef Horálek, Ph.D.

Cíl práce: Tato diplomová práce má jako hlavní cíl představení principů a možností užití uživatelské behaviorální analýzy v systémech SIEM.

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

Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP vykazuje shodu ve 2% textu, která se výhradně týká názvů a definic ISO a citací doporučení z NÚKIB.

Dílčí připomínky a náměty:

Vedoucí práce nemá závažné připomínky k předložené práci

Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce volně navazuje a vychází z autorovi bakalářské práce Analýza a návrh nasazení SIEM řešení v prostředí středního podniku.
V předložené práci autor prokazuje hlubokou míru znalostí dané problematiky, kde využívá nejen znalostí získaných při studiu, ale také v rámci své odborné praxe.
V samotné práci autor nejprve přestavuje normativní a legislativní rámec z oblasti kybernetické a informační bezpečnosti s důrazem na Security Information and Event management.
Dále autor představuje dva významné nástroje využitelné právě pro behaviorální analýzu a to komplexní a robustní řešení IBM Security QRadar SIEM a vedle open-source SIEM řešení AlienVault OSSIM. Následně oba nástroje porovnává a vyhodnocuje. Následně autor představuje přístupy k uživatelské behaviorální analýze na obou výše zmíněných nástrojích. Autor zabývá užitím modulu

uživatelské behaviorální analýzy na vestavěném Use case, kde prakticky ukazuje možnosti a postupy pro využití uživatelské behaviorální analýzy. V závěru práce pak shrnuje možnosti obou porovnávaných řešení.
Autor tak zcela splnil zadání práce.

Otázky k obhajobě:

Jaký shledáváte přínosy při využití behaviorální analýza pro systémy SIEM s dopadem na zvýšení zabezpečení informačních systémů?

Práci doporučuji k obhajobě.

Navržená výsledná známka: A

V Hradci Králové**, dne 2. ledna 2019**

podpis