Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Jméno studenta: Jan Nedbal

Název práce: Uživatelská behaviorální analýza pro systémy SIEM

Autor posudku: Vladimír Soběslav

Cíl práce: Definovat použití principů uživatelské behaviorální analýzy a aplikovat teoretické poznatky na vybraných SIEM sytémech.

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

Dle anti-plagiátorské kontroly je zde minimální shoda v počtu jednotek procent.

Dílčí připomínky a náměty:

V diplomové práci bylo možné hlouběji analyzovat teoretické aspekty standardů v oblasti informační a kybernetické bezpečnosti, toto rozšíření by zvýšilo úroveň diplomové práce.
Diplomová práce mohla dále srovnat či uvést přehled širšího množství SIEM systémů, respektive zdůvodnění pro výběr dvou využitých systémů.
V některých částech práce by bylo vhodné lépe formátovat obrázky a stylovat text.

Celkové posouzení práce a zdůvodnění výsledné známky:

Diplomová práce je zaměřena na problematiku SIEM systémů a behaviorální analýzy chování uživatelů. Jedná se o aktuální téma se zajímavým aplikační potenciálem.

Závěrečnou práci je možné rozdělit do dvou logických celků, teoretickou analýzu problematiky informační a kybernetické bezpečnosti s důrazem na sběr a vyhodnocování událostí v síti a praktické nasazení SIEM technologií, které bylo anonymizováno.

Teoretickou část reprezentuje druhá až sedmá kapitola. Autor v této části jednoznačně vymezil své cíle, strukturaci práce, vhodně abstrahoval a zvolil klíčové technologie pro následnou

implementaci praktických ukázek. Tato část je sepsána na slušné odborné úrovni, autor zde mohl analyzovat širší množství technologií.

V následující části závěrečné práce autor implementoval teoretické poznatky do dvou klíčových systémů, kterými jsou IBM Security QRadar a AlienVault OSSIM. V obou systémech se autor pokusil analyzovat a zhodnotit možnost pro behaviorální analýzu, toto se bohužel podařilo pouze v jednom ze systémů – IBM QRadar. Výstupy z provedené analýzy poskytují zajímavý vhled do možností strojového učení a reportingu chování uživatelů. Jedná se spíše o praktický pohled na možné nastavení v QRadar systému.

Návrhem nového řešení promítl autor získané zkušenosti ve společnosti Autocont a v neposlední řadě také na stážích a zejména pak v organizaci IHMC v USA na Floridě, kde působil v týmu zaměřujícím se na kybernetickou bezpečnost.

Celkově se jedná a pěkně zpracovanou závěrečnou práci s praktickým řešením analyzovaného problému.

Otázky k obhajobě:

1) Pokuste se představit základní principy strojového učení a jak je využíváno v SIEM systému.
2) Jaké jsou bezpečnostní hrozby/útoky na SIEM systémy a jak je možné jim předcházet?

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové**, dne 3. ledna 2019**

podpis