



## POSUDEK VEDOUcíHO BAKALÁŘSKÉ PRÁCE

**Jméno studenta:** Jan Nedbal  
**Název práce:** Analýza a návrh nasazení SIEM řešení v prostředí středního podniku  
**Autor posudku:** Josef Horálek  
**Cíl práce:** Cílem práce je provést podrobnou analýzu požadavků a dostupných řešení SIEM s přihlédnutím k požadavkům zákona o kybernetické bezpečnosti. V praktické části autor vypracuje případovou studii nasazení SIEM ve firemním prostředí.

Povinná kritéria hodnocení práce	Stupeň hodnocení (známka)			
	A	C	E	F
Práce svým zaměřením odpovídá studovanému oboru	<input checked="" 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"/>
Zpracování teoretických aspektů tématu	<input checked="" 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"/>
Adekvátnost použitých metod, způsob jejich použití	<input checked="" 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"/>
Práce s literaturou	<input checked="" 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"/>
Jazyková a terminologická úroveň	<input checked="" 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"/>
Vlastní přínos studenta	<input checked="" 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"/>

### Dílní připomínky a náměty:

Vedoucí práce nemá připomínky.

### Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená bakalářská práce se zabývá problematikou nasazení a využívání Security Information and Event Management. Autor nejprve podrobně představuje ISO standardy a zákon o kybernetické bezpečnosti, jehož implementace vyžaduje nasazení SIEM řešení. V následující části autor představuje obecné principy SIEM, jeho architekturu a na závěr se zabývá vybraným produktem IBM Security QRadar.

V praktické části pak představuje návrh řešení nasazení SIEM do podniku z oblasti bankovníctví a zdravotnického sektoru. V rámci případové studie předkládá ucelený návrh řešení, včetně technických a ekonomických požadavků. Předložená řešení vycházejí z reálných projektů, na kterých se autor v rámci své praxe podílel a představují modelové příklady nasazení SIEM řešení v oblastech, ve kterých jsou vysoké bezpečnostní standardy podstatnou součástí IT infrastruktury.

Autor práce splnil všechny vytyčené cíle a práce splňuje požadavky kladené na bakalářskou práci.

**Otázky k obhajobě:**

Jaké existují alternativní SIEM řešení k IBM Security QRadar?

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: A - výborně**

**V Hradci Králové, dne 6. května 2016**

---

podpis