Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2016/2017

Studijní program: Systémové inženýrství a informatika
Forma: Prezenční
Obor/komb.: Informační management (im2-p)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Bc. Nedbal Jan	Zdeňka Fibicha 792, Králíky	I1600310

TÉMA ČESKY:

Uživatelská behaviorální analýza pro systémy SIEM

TÉMA ANGLICKY:

User behavioral analysis for SIEM systems

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je podrobně představit principy behaviorální analýzy v systémech SIEM, provést jeho analýzu s důrazem na její využití pro přizpůsobení systémů SIEM na základě individuálních požadavků klienta a modelové představení.
V teoretické části autor představí principy behaviorální analýzy v systémech SIEM a možností jejich úprav a individuálního nastavení z pohledu koncového klienta.
V praktické části pak autor představí praktické využití BA v SIEM, konkrétní možnosti jeho úprav v rámci optimalizace pro koncového klienta.
Autor se pokusí vytvořit model finanční náročnosti a efektivity nasazení BA v SIEM v porovnání se standardními implementacemi SIEM.

Osnova práce:
Úvod
Rešerše problematiky
Bezpečnost
Principy SIEM
IBM QRadar
AllienVault OSSIM
UBA
Stanovení výchozích hypotéz
Praktické řešení pro IBM QRadar a AllienVault OSSIM
Vyhodnocení hypotéz
Závěr

SEZNAM DOPORUČENÉ LITERATURY:

MILLER, David. Security information and event management (SIEM) implementation. New York: McGraw-Hill, c2011. ISBN 0071701095.
GRIFFOR, Edward. Handbook of system safety and security: cyber risk and risk management, cyber security, threat analysis, functional safety, software systems, and cyber physical systems. Cambridge, MA: Elsevier, 2016. ISBN 9780128037737.
ADAMS, Niall M. a Nicholas. HEARD. Data analysis for network cyber-security. London, UK: Imperial College Press, 2014. ISBN 9781783263745.

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....