FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Mohamed Bettaz, CSc.
Student:	Linda Šindelářová
Název práce:	Detekce bezpečnostních hrozeb v nastrojích pro správu bezpečnostních informací a událostí
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	9. července 2023

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Předložená Závěrečná Práce je v souladu se zadáním a dostatečně plní jeho cíle. Praktická část předložené práce, výslovně nezmiňuje činnost věnovanou programování.
Nástroj Elastic SIEM nabízí celkem šest typů detekčních pravidel a Závěrečná Práce pojednává pouze o čtyřech z nich. Probrané detekční pravidla nezaujímají explicitně všechny typy událostí, které podle pouzité Vyhlášky, je nezbytné zaznamenávat

2. Písemná část práce 90 / 100 (A)

Předložená Závěrečná Práce je dobře strukturovaná a čitelná. Některé části se opakují, i když se záměrem poskytnout více podrobností v některých z nich, viz například sekci 1.2, která pojednává o nástrojích pro řešení kybernetické bezpečnosti, a sekci 2.2, která důkladně vysvětluje funkci SIEM. Obě tyto části se v popisu některých částí SIEM překrývají.
Použitá literatura je důkladně citována. Ke kvalitě předložené práce by však rozhodně přispělo použití vybrané odborné literatury, jelikož Závěrečná Práce má i akademický character.
Doporučuje se sjednotit používanou terminologii. Například, autorka někdy používá výraz "log managment", někdy "správa logů" a někdy "managment logů". Stejná připomínka se týká použití výrazů "machine learning" a "strojové učení".
Pro ilustraci "Podíl SIEM nástrojů na světovém trhu" stačí uvést obrázek 3.1 nebo obrázek 3.2.
Protože akronym SQL je uveden v seznamu zkratek je potřeba také uvést akronym NoSQL v tomto seznamu.

Některé překlepy: Například Operating System místo Operation System, nástroj Sentinel místo nástroj Sentiel, apod.

3. Nepísemná část, přílohy 85 /100 (B)

Praktická část předložené práce, kde je "předvedeno, že je možné pomoci Elastic Stack vyhovět legislativním požadavkům" se skládá ze dvou hlavních částí:
Instalace nástrojů Elastic Stack a návrh pravidel pro vybrané bezpečnostní hrozby.
Autorka výslovně nezmiňuje činnost věnovanou programování a také možné nasazení vyvíjeného softwaru.
Mohlo by být užitečné poskytnout mapování mezi typy událostí určenými Vyhláškou (viz sekci 1.1.2) a typy detekčních pravidel poskytnutých nástrojem Elastic SIEM (viz sekci 4.2.2).
Detekční pravidla nazvané Machine Learning a Indicator Match nejsou probrány, ikdyž v Práci je uvedeno, že Machine Learning je součástí pouze platinum a enterprise edice (viz sekci 4.2.2, která se zabývá tvorbou detekčních pravidel).

4. Hodnocení výsledků, jejich využitelnost 80 /100 (B)

Je důležité zmínit, že většina detekčních pravidel se tyká (přímo nebo nepřímo) události "typu" pokusu o přihlášení (viz 4.2.2.2 Detekční pravidla typu Threshold, 4.2.2.3 Detekční pravidla typu New Terms, 4.2.2.4 Detekční pravidla typu Event Correlation). Bylo by užitečné řešit případy, kde detekční pravidla zaujímají události typu XSS nebo SQL injection, které představují jedny z nejčastějších zranitelností nalezených na Webu.
Praktická využitelnost by také vyžadovala důkladné testování.

Celkové hodnocení 85 /100 (B)

Podle autorky, která cituje použitou literaturu, nástroj Elastic SIEM nabízí celkem šest typů detekčních pravidel a každý je vhodný k uplatnění v jiné situaci. Závěrečná Práce pojednává o čtyřech z nich. Probrané detekční pravidla nezaujímají explicitně typy událostí (počtem osm), které podle Vyhlášky (viz sekci 2.2.1) je nezbytné zaznamenávat. Většina detekčních pravidel se týká (přímo nebo nepřímo) události "typu" pokusu o přihlášení (viz 4.2.2.2 Detekční pravidla typu Threshold, 4.2.2.3 Detekční pravidla typu New Terms, 4.2.2.4 Detekční pravidla typu Event Correlation).

Otázky k obhajobě

Otázka 1: jaký "specifický" protokol používá agent-based metoda pro přenos logů z generujícího zařízení do SIEM serveru? (viz 2.2.1.1).

Otázka 2: Jaký Elastic SIEM detekční pravidlo (viz sekci 4.2.2 Tvorba detekčních pravidel) se uplatňuje k typu události "činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému" ? (viz sekci 2.2.1 Log managment).

Otázka 3: Jaký typ detekčních pravidel (jestli existuje) se uplatňuje na útoky zevnitř?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.