КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 26.08.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Богдан Радосављевић под насловом ,,Имплементација и евалуација SIEM/XDR решења у симулираном пословном окружењу". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Основне студије завршио је на Електротехничком факултету Универзитета у Београду, на смеру Софтверско инжењерство, а након тога је уписао мастер академске студије на истом модулу. Током студија био је активан у студентским организацијама EESTEC и Google Developer Student Club, где је учествовао у организацији радионица, такмичења и пројеката из области ИТ-а. У оквиру програма студентске размене, провео је четири месеца (март–јун 2025) у Бечу, где се усавршавао у области сајбер безбедности. Последњих годину дана активно се бави облашћу сајбер безбедности где практично искуство стиче тренутно на стручној пракси у компанији PULSEC, где се сусрео са реалним пословним изазовима у ИТ сектору.

2. Извештај о студијском истраживачком раду

Кандидат Богдан Радосављевић је у оквиру припреме за израду мастер рада анализирао SIEM и XDR системе за централизовање прикупљање догађаја и њихову корелацију, са посебним освртом на детекцију малициозних активности. Истраживање је обухватило свеобухватну анализу различитих SIEM и XDR алата, са посебним освртом на платформу Wazuh, која представља интегрисано SIEM и XDR решење отвореног кода са великим бројем модула и могућности за интеграције, чиме је приказана његова практична примена у симулираној пословној организацији.

3. Опис мастер рада

Мастер рад под насловом „Имплементација и евалуација SIEM/XDR решења у симулираном пословном окружењу“ обухвата 47 страна без насловне стране, са укупно 46 слика, 3 табеле и 8 референци. Рад садржи шест поглавља, спискове референци, скраћеница, слика и табела.

У првом поглављу дефинисани су предмет рада, мотиви и циљеви, као и значај система за детекцију, корелацију и одговоре на безбедоносне инциденте у савременом дигиталном свету који је све више изложен сајбер нападима. Друго поглавље даје преглед основних појмова и Wazuh платформе, као и напада који су симулирани у раду.

У трећем поглављу детаљно је представљено окружење које је развијено за симулацију рада платформе у оквиру пословног система. Приказани су главни аспекти дизајна и имплементације, са циљем да се прикаже како се поставља и конфигурише интегрисамо SIEM/XDR решење.

У четвртом поглављу приказан је рад различитих модула у оквиру Wazuh платформе, а такође су дефинисана и правила чији је циљ детекција претходно дефинисаних напада. У оквиру политике компаније приказани су модули за скенирање рањивости на крајњим уређајима и за аутоматизовану контролу усклађености са дефнисаним безбедоносним политикама. У каснијим нападима су уведени модули за праћење промена у фајл систему и за аутоматски одговор на неки догађај у систему.

У петом поглављу су симулирани напади на инфраструктуру са циљем да се процени способност Wazuh платформе да правовремено детектује и адекватно реагује на различите врсте безбедносних инцидената. Напади који су симулирани су: кршење правила политике компаније, напад грубом силом на SSH, ескалација привилегија и скидање малициозног фајла на рачунар. Након комплетне анализе резултата, дат је предлог о могућим унапређењима система.

У шестом поглављу сумирани су резултати спроведеног истраживања, анализирани кључни увиди добијени током имплементације система за детекцију и изнети главни закључци рада.

4. Анализа са кључним резултатима

Мастер рад кандидата Богдана Радосављевића бави се анализом и применом система за детекцију, корелацију и одговор на безбедоносне инциденте. Успешно је креиран контролисани лабораторијски

сценарио који симулира рад једне компаније. Током рада приказано је како Wazuh може да пружи кључне функционалности SIEM и XDR система, укључујући прикупљање логова, детекцију претњи, креирање правила политике безбедности, као и аутоматизовани одговор на инциденте.
Основни доприноси рада су: 1) демонстрација практичне примене једног SIEM/XDR решења у реалном сценарију; 2) рад не остаје само на теоријском приказу архитектуре, већ уводи и експерименте са стварним нападима; 3) могућност проширења оваквог система са већим скупом правила и додатним интеграцијама; 4) водич за изградњу сопственог лабораторијског окружења и тестирање механизама за детекцију.

5. Закључак и предлог

Кандидат Богдан Радосављевић је у свом мастер раду успешно имплементирао систем за детекцију, корелацију и одговор на безбедоносне инциденте у оквиру симулираног пословног окружења. Кроз примену Wazuh платформе приказао је рад различитих модула и правила у циљу повећања безбедности система и детекције различитих врста претњи. Рад је показао висок ниво разумевања принципа сајбер безбедности и практичну примену SIEM и XDR концепата. Кандидат је током израде рада исказао самосталност, аналитичност и систематичност у приступу, као и способност интеграције теоријских и практичних аспеката сајбер безбедности.

На основу наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Богдана Радосављевића, под насловом „Имплементација и евалуација SIEM/XDR решења у симулираном пословном окружењу“, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 19.10.2025. године

Чланови комисије:

др Павле Вулетић Редовни професор
сагласан, 19.10.2025.

др Жарко Станисављевић Ванредни професор
сагласан, 19.10.2025.