КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 28.5.2024. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Оливере Крњајић под насловом „Имплементација технологија и процеса у безбедносно-оперативном центру". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Оливера Крњајић је рођена 24. 12. 1998. године у Београду. Завршила је основну школу „Борислав Пекић" у Београду као вуковац и ђак генерације. Уписала је Девету гимназију „Михаило Петровић Алас" у Београду и коју је завршила као вуковац. Електротехнички факултет уписала је 2017. године. Дипломирала је на одсеку за Рачунарску технику и информатику 2022. године са просечном оценом 8,17. Дипломски рад „Детекција инцидената и аномалија у раду система *SIEM* алатима" одбранила је у марту 2022. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за рачунарску технику и информатику уписала је у октобру 2022. године. Положила је све испите са просечном оценом 9,40.

2. Извештај о студијском истраживачком раду

Кандидат Оливера Крњајић је анализирала имплементиране процесе и технологије и урадила истраживање релевантне литературе која се односи на област безбедносно-оперативних центара (енг. *Security Operations Centre*). Имплементирани су и анализирани процеси који се одвијају у реалном безбедносно-оперативном центру и упоређени са индустријским стандардима. Истраживањем је утврђено које технологије представљају водећа решења у области информационе безбедности, и који су најефективнији начини њихове оркестрације и аутоматизације процеса у безбедносно-оперативном центру. Такође, установљено је који све фактори највише штете информационој безбедности организације, каква упозорења представљају уско грло приликом адресирања инцидената, као и које су се методе показале као ефективне у пракси.

3. Опис мастер рада

Мастер рад обухвата 56 страна, са укупно 51 сликом, 12 табела и 24 референце. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљен је значај информационе безбедности у савременом свету, као и безбедносно-оперативних центара. Додатно, описани су изазови са којима се организације и појединци сусрећу у дигиталном окружењу.

У другом поглављу је описан појам безбедносних операција, безбедносно-оперативних центара, као и њихове еволуције. Представљене су технологије и процеси који су се деценијама уназад развијали и описана је архитектура SOC центара

У трећем поглављу су детаљно анализирани процеси савременог безбедносно-оперативног центра, као што су надзор система и детекција инцидената, дигитална форензика и одговор на инциденте, управљање рањивостима и обавештајним подацима о претњама, и други. Затим су анализирани алати који чине саставни део сваког безбедносно-оперативног центра, који се користе у сврху спровођења претходно описаних процеса –

алати за надзор и детекцију, анализу софтвера, филтрирање саобраћаја, оркестрацију и аутоматизацију процеса, и други.

Четврто поглавље детаљно описује систем имплементиран у реалном безбедносно-оперативном центру. То подразумева коришћене технологије, њихову међусобну интеграцију, успостављене процесе, као и целокупну имплементацију која је спроведена у циљу оптималног искоришћења доступних ресурса – технолошких, људских и временских.

У оквиру петог поглавља су представљени примери реалних безбедносних случајева са различитим исходом, као и процедуре њиховог решавања. На тај начин је демонстрирана стварна употреба имплементираног система и успостављених процеса.

Шесто поглавље је закључак у оквиру кога су резимирани резултати рада, као и његови доприноси. Описан је значај безбедносно-оперативних центара и уопштено информационе безбедности, као и предвиђања даљег развоја ове области под утицајем савремених технологија.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Оливере Крњајић се бави значајем безбедносно-оперативних центара у заштити дигиталног простора од хакерских напада, технологијама и процесима савремених центара, као и имплементацијом истих у реалном окружењу. Кључни део рада представља опис реалног безбедносно-оперативног центра који је кандидат успоставила, начин имплементације технологија и процеса у оквиру њега уз све предузете кораке, као и примери безбедносних случајева и начини њиховог адресирања. Основни доприноси рада су: приказ добре праксе и начина пројектовања технологија и процеса у савременим безбедносно-оперативним центрима; анализа реалних ситуација и метода за максимално искоришћење доступних ресурса, са акцентом на аутоматизацију процеса и паметну обраду података; анализа могућности даљег развоја метода заштите од претњи по организације и појединце у дигиталном окружењу.

5. Закључак и предлог

Кандидат Оливера Крњајић је у свом мастер раду успешно представила начин имплементације процеса и технологија у савременим безбедносно-оперативним центрима на примеру реалног окружења и ситуација. Предложено решење може значајно да унапреди методе заштите система и корисника од хакерских напада, омогућавајући правовремени одговор на инциденте у дигиталном окружењу.

Кандидат Оливера Крњајић је исказала самосталност и систематичност у своме поступку, као и иновативне елементе у решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Оливере Крњајић прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 08.07.2024. године

Чланови комисије:

_____

др Павле Вулетић, в. проф.

_____

Др Жарко Станисављевић, в. проф.