ОТК ЗЯ-НС1-093
07.07.2026

Р Е Ц Е Н З И Я

върху дисертационен труд за придобиване на
образователна и научна степен „ДОКТОР"

Автор на дисертационния труд: **маг. Мариан Христов**
Тема на дисертационния труд: „***Изследване на облачно-базирана система за наблюдение и анализ на събития***"
Рецензент: доц. д-р Георги Цочев

1. Актуалност на разработвания в дисертационния труд проблем. Съдържание на дисертационния труд.

Представеният ми за рецензиране дисертационен труд е предназначен за придобиване на образователната и научна степен - Доктор.

Темата е актуална и значима в научно-приложен и приложен аспект, тъй като е насочена към един от най-съществените проблеми на съвременната киберсигурност - наблюдението, анализа и своевременното реагиране на събития в индустриални OT/ICS, IoT и IIoT среди.

Актуалността на изследвания проблем произтича от ускорената дигитализация на индустриалните отрасли, интеграцията между информационни и оперативни технологии, нарастващата свързаност на индустриалните устройства и увеличаването на киберзаплахите към критични инфраструктури. В дисертационния труд убедително е показано, че загубата на видимост, липсата на централизирана телеметрия, недостатъчната сегментация и слабият контрол на отдалечения достъп създават значими рискове за непрекъсваемостта на процесите, безопасността и надеждността на индустриалните системи.

Представената разработка е фокусирана върху изследване и изграждане на облачно-базирана система за наблюдение и анализ на събития, базирана на Microsoft Defender for IoT, Microsoft Sentinel, Azure Logic Apps, Azure Resource Graph, Splunk Enterprise и Zabbix. Изследването има ясно изразена практическа насоченост, тъй като разглежда реални инженерни сценарии за откриване на зловреден софтуер в индустриални мрежи, оперативен мониторинг на системата за мониторинг, разпознаване на понижаване на фърмуерни версии и SIEM-базирана детекция на инциденти и аномалии.

Поставените задачи са формулирани логично: идентифициране на заплахи и основни рискове в OT/ICS; анализ на съществуващите решения; проучване на технологии за мониторинг и анализ; разработване на система за наблюдение; реализация в тестова и реална индустриална среда; оценка на ефективността чрез експерименти; разработване на методология за оценка на риска. Това показва, че трудът разглежда не само теоретична проблематика, но и реална

инженерна необходимост, свързана с практическо повишаване на киберустойчивостта на индустриалните организации.

2. Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал

Дисертационният труд демонстрира много добра степен на познаване на съвременното състояние на изследвания проблем. Авторът разглежда основните понятия и модели в областта на OT/ICS, IACS и IIoT, спецификата на индустриалните комуникационни протоколи, Purdue модела, различията между IT и OT сигурността, както и особеностите на пасивния мониторинг в индустриални среди.

Литературният материал е използван целенасочено и е обвързан с конкретните инженерни решения. Анализирани са стандарти, референтни модели, официална документация на използваните продукти, научни публикации и доклади за актуални OT/ICS заплахи. Особено положително впечатление прави, че авторът не се ограничава с описание на известни средства за защита, а ги поставя в контекста на практически сценарии - работа на SOC, SIEM корелация, автоматизирани уведомления, OSINT проверка, CMDB контекст и наблюдение на работоспособността на самата мониторингова система.

Налице е творческа интерпретация на литературния материал. Тя се изразява в адаптиране и надграждане на известни подходи към специфичните ограничения на OT средите - пасивно наблюдение без агенти, избягване на активно сканиране, минимизиране на риска за производствения процес, намаляване на фалшиво положителните резултати и съобразяване с необходимостта от бърза реакция при инциденти.

3. Съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд с постигнатите приноси:

Избраната методика на изследване е в пълно съответствие с поставените цел и задачи. В труда са използвани теоретико-аналитични, сравнителни, моделиращи и експериментални методи, които позволяват системно изследване на проблема и валидиране на предложените инженерни решения.

Методиката обхваща анализ на заплахите и технологичните решения, проектиране на архитектури за наблюдение и реакция, разработване на конкретни правила и автоматизации чрез KQL, SPL, Azure Logic Apps, Sentinel Automation Rules и Zabbix/SNMP мониторинг, както и практическа проверка чрез контролирани тестови сценарии. Верификацията е направена чрез реални или близки до реалните индустриални постановки - откриване на EICAR тестов файл, комуникация към известен злонамерен IP адрес, контролирано изключване на D4IoT сензор, понижаване на фърмуер на индустриален контролер и възпроизвеждане на Windows/IPS събития в Splunk.

Тази последователност доказва, че дисертантът умее да преминава от анализ на проблема към инженерно решение, оттам към експериментална проверка и накрая към формулиране на научни и научно-приложни приноси. Постигнатите резултати са логично следствие от избраната методика.

4. Кратка аналитична характеристика на естеството и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд.

Дисертационният труд е разработен в обем от 187 страници и е структуриран в увод, четири глави, списъци на фигури и таблици, списък на използвани съкращения и означения и библиографска справка. Структурата е логична и следва естествена последователност - от въвеждане на предметната област и основните заплахи, през технологиите за мониторинг и SIEM, до разработването и експерименталната проверка на конкретни решения.

В увода са мотивирани актуалността, целта и задачите на изследването. Посочена е практическата значимост на разработената система, включително внедряване в голяма автомобилостроителна компания, защита на значителен брой OT, IT, IoT и IIoT устройства, участие в научноизследователски проект и заявка за полезен модел.

В първа глава е представен систематичен обзор на индустриалните мрежи, OT/ICS понятията, спецификите на оборудването, протоколите, референтните модели и Microsoft Defender for IoT. Разработен е механизъм за уведомяване при откриване на зловреден софтуер в индустриална мрежа чрез интеграция D4IoT - Microsoft Sentinel - Azure Logic Apps - SOC. Проведените тестове показват работоспособност както при EICAR тестова детекция, така и при опит за комуникация към известен злонамерен IP адрес.

Втора глава разглежда същността на логовете, SIEM системите и функциите им за събиране, нормализация, разбор, корелация и уведомяване. Основната инженерна разработка в тази глава е оперативният мониторинг на D4IoT имплементация чрез две Sentinel правила, Azure Logic Apps с ARG заявка и локален Zabbix/SNMP мониторинг. Тестовете доказват, че предложената система може да открива различни състояния на деградация или загуба на видимост.

Трета глава е посветена на откриването на атаки, целящи понижаване на версията на фърмуера. Разработеното решение използва алармата „Firmware Change Detected", извличане на версии чрез KQL и регулярни изрази, сравнение на компонентите на версията и генериране на инцидент само при регресия. Валидирането е извършено върху реални индустриални устройства, включително Atlas Copco Power Focus 6000, като системата правилно различава фърмуерно понижаване от последващо легитимно обновяване.

Четвърта глава представя Splunk Enterprise като SIEM решение и разработва референтна архитектура за внедряване на локални, отдалечени Windows и

IDS/IPS логове. Конфигурирани са правила за успешни и неуспешни опити за влизане, CnC комуникация от вътрешна машина, както и изтриване на Windows Security лог. Проведените тестове доказват приложимостта на разработените SPL-базирани правила и механизми за автоматично уведомяване.

Достоверността на материала се основава на реални експериментални постановки, практически внедрявания, конкретни конфигурации, логически адресации, заявки, екранни резултати, таблици и повторяеми тестови сценарии. Използването на стандартни платформи и инструменти, както и сравнението с алтернативни продукти и подходи, допълнително повишават достоверността на получените резултати.

5. Научни, научно-приложни и приложни приноси по дисертационния труд

Приемам дефинираните в дисертационния труд претенции за научни и научно-приложни приноси като отразяващи резултатите, постигнати от докторанта. Приносите могат да бъдат обобщени както следва:

- научни приноси:

✓ Изведен е метод за изграждане на "real-time notification pipeline" за OT/ICS детекции, реализиран чрез последователност D4IoT -> SIEM -> автоматизация -> SOC, като са дефинирани минимални атрибути за оперативно валидно уведомление.

✓ Формулиран е първичен модел за анализ на OT/ICS аларми чрез комбиниране на CMDB контекст, критичност на системата и OSINT репутация на външни дестинации.

✓ Формализирана е концепцията „наблюдение на системата за наблюдение" в OT/ICS контекст чрез индикатори за липса на аларми, прекъсване на облачна свързаност и недостъпност на интерфейс за управление.

✓ Предложен е многослоен модел за надеждност на оперативния мониторинг чрез независими уведомителни механизми - SIEM инцидент, Teams съобщение и имейл.

✓ Въведен е "version-aware" модел за детекция на фърмуерно понижаване в пасивен OT/ICS мониторинг, който трансформира обща аларма за фърмуерна промяна в конкретна индикация за регресия и потенциално повторно въвеждане на уязвимости.

✓ Създаден е SIEM-ориентиран модел за детекция на фази от традиционна кибератака чрез корелация на операционни Windows и мрежови IPS логове в единна система.

- научно-приложни приноси:

- ✓ Създадена и внедрена е автоматизация чрез Azure Logic Apps за незабавно уведомяване при malware детекции от D4IoT в индустриални среди с Microsoft Sentinel интеграция.
- ✓ Разработено е KQL-базирано обогатяване на алармите чрез извличане на SensorId и съпоставяне с физическа локация, което превръща суровата аларма в контекстен сигнал, ориентиран към реакция.
- ✓ Създадени са две Sentinel аналитични правила за откриване на липса на D4IoT аларми - глобално и за конкретен сензор - с цел проследяване на потенциална загуба на видимост.
- ✓ Разработена е Azure Logic Apps автоматизация с Azure Resource Graph заявка за наблюдение на LastConnectivityTime и Teams уведомяване при прекъсната облачна свързаност.
- ✓ Създаден е независим локален мониторинг слой чрез Zabbix, SNMP и ping за наблюдаване на интерфейса за управление на D4IoT сензори, приложим и в среди без Интернет свързаност.
- ✓ Създадено е Sentinel аналитично правило за фърмуерно понижаване чрез разбор на ExtendedProperties, извличане на версии с Regex и "digit-by-digit" сравнение на компонентите на версиите.
- ✓ Разработена е автоматизация за седмични отчети за фърмуерни промени чрез Azure Logic Apps, CSV файл и имейл, подпомагаща управлението на фърмуерния жизнен цикъл и регулаторното съответствие.
- ✓ Реализирана е Splunk Enterprise референтна архитектура с отделни индекси за локални, отдалечени и мрежови логове и набор от SPL-базирани правила за аларми и периодични отчети.

- приложни приноси:
- ✓ Разработени са практически работещи прототипи и технически механизми за наблюдение, уведомяване, корелация и разследване на събития в OT/ICS и IoT среди.
- ✓ Предложените решения са проверени чрез контролирани тестове и реални индустриални сценарии, включително детекция на зловреден софтуер, загуба на свързаност, фърмуерно понижаване и подозрителни SIEM събития.
- ✓ Показана е практическа приложимост на разработената система в мащабна индустриална среда, като е постигнато повишаване на видимостта, съкращаване на времето за реакция и намаляване на риска от пропуснати инциденти.

Докторантът показва знания от различни области и умения при прилагането им в решението на инженерни проблеми, както и да ги свежда до конкретни алгоритми.

6. Оценка за степента на личното участие на дисертанта в приносите.

Представеното съдържание, разработените архитектури, конкретните KQL и SPL правила, автоматизациите, експерименталните сценарии и анализът на резултатите дават основание да се приеме, че приносите са резултат от личната работа на докторанта. Авторът демонстрира висока инженерна компетентност и способност да съчетава знания от киберсигурност, комуникационни мрежи, облачни технологии, SIEM системи и индустриални контролни среди.

Особено съществено е, че дисертантът не се ограничава с теоретично описание на продуктови функционалности, а проектира, реализира и тества практически механизми, които имат пряко отношение към дейността на центрове за информационна сигурност и към защитата на реални индустриални процеси. Това показва висока степен на лично участие и самостоятелност при формулирането и реализирането на приносите.

7. Преценка на публикациите по дисертационния труд.

Представеното съдържание, проведените анализи и разработените примери в рамките на дисертационния труд, показват отличното познаване на изследваната област, в която се фокусира труда. Получените от автора резултати от дисертационното изследване са публикувани в 6 научни труда – 1 в списание и 5 в конференции. Една от статиите е публикувана в международно научно списание с IF 2.2 в Q2 на Web of Science. Всичко това ми дава основание да смятам, че постигнатите резултати в дисертационния труд са направени от докторанта. Всички статии са на английски език, в съавторство с научните ръководители на докторанта.

Няма съмнение, че публикациите са основно дело на докторанта и че чрез тях той е оценен високо от научната и инженерната общност.

8. Използване на резултатите от дисертационния труд в научната и социалната практика. Наличие на постигнат пряк икономически ефект и пр. Документи, на които се основава твърдението.

Резултатите от дисертационния труд имат ясно изразена приложимост в научната, инженерната и социалната практика. Разработената система е насочена към повишаване на сигурността на индустриални мрежи, които поддържат критични процеси в производството, енергетиката, логистиката и други значими отрасли. По този начин резултатите имат не само технологична, но и обществена значимост, тъй като допринасят за ограничаване на риска от оперативни прекъсвания, материални щети и заплахи за безопасността.

В дисертационния труд е посочено, че разработената система е интегрирана в голяма автомобилостроителна компания и защитава значителен брой OT, IT, IoT и IIoT устройства. Посочени са още участие в проект BG-RRP-2.004-0005 „Многовалентна система за защита срещу кибер атаки в комуникационни и

индустриални мрежи с добавена функционалност на невронни мрежи", признание от Microsoft във връзка с принос към функционалностите на Defender for IoT и подаване на заявка за полезен модел.

Към момента не са представени конкретни количествени данни за реализиран пряк икономически ефект. Въпреки това потенциалът за такъв е значителен, тъй като предложените решения могат да намалят времето за откриване и реакция при инциденти, да ограничат непланирани прекъсвания и да подобрят управлението на риска в индустриални организации. Твърденията се основават на представените в дисертационния труд експериментални резултати, описаните внедрявания, проектната дейност и публикационните данни.

9. Оценка на съответствието на автореферата с изискванията за изготвянето му, както и на адекватността на отразяване на основните положения и приносите на дисертационния труд.

Авторефератът е оформен в 32 страници и отговаря на изискванията за изготвянето му, както и за неговото отпечатване. Основните положения на дисертационния труд са отразени точно и ясно в автореферата. Приносите на дисертационния труд са изведени, точно класифицирани и описани.

10. Мнения, препоръки и бележки.

Като цяло мнението, препоръките и бележките ми по представения ми за рецензия труд предадох писмено на докторанта, които са отразени в последната версия на дисертационния труд.

Препоръчвам активна публикационна дейност и в чужбина в бъдещите изследвания на дисертанта.

11. Заключение

В заключение смятам, че работата има завършеност, съдържа оригинални решения и темата е актуална. Направените бележки и препоръки не оспорват приносите на дисертационния труд.

Считам, че изискванията на Закона за развитие на академичния състав в България и Правилника за неговото прилагане са изпълнени в представения дисертационен труд.

Давам положителна оценка за труда и предлагам на уважаемото Научно жури да присъди на маг. инж. Мариан [redacted] Христов образователната и научна степен „**доктор**" по професионално направление 5.3 Комуникационна и компютърна техника, научна специалност „Осигурителна техника и системи".

Дата: 06.07.2026г.

Рецензент: [redacted]
/ доц. д-р Георги Цочев/

ОТК-78-НС/09
07.07.2026

REVIEW

on a dissertation for **"Doctor of Philosophy" degree**

Author of the dissertation: **Marian [redacted]v Hristov**
Dissertation topic: " ***Investigation of a Cloud-based Security Information and Event Management Sistem*** "
Reviewer: Assoc. prof. Georgi Tsochev, PhD

1. Relevance of the problem developed in the dissertation. Content of the dissertation.

The dissertation submitted to me for review is intended for the acquisition of the educational and scientific degree - Doctor.

The topic is topical and significant in scientifically applied and applied aspect, as it is aimed at one of the most significant problems of modern cybersecurity - monitoring, analysis and timely response to events in industrial OT/ICS, IoT and IIoT environments.

The relevance of the problem under study stems from the accelerated digitalization of industrial industries, the integration between information and operational technologies, the growing connectivity of industrial devices and the increase in cyber threats to critical infrastructures. The dissertation convincingly shows that loss of visibility, lack of centralized telemetry, insufficient segmentation and weak remote access control create significant risks for the continuity of processes, safety and reliability of industrial systems.

The presented development is focused on researching and building a cloud-based event monitoring and analysis system based on Microsoft Defender for IoT, Microsoft Sentinel, Azure Logic Apps, Azure Resource Graph, Splunk Enterprise and Zabbix. The study has a clear practical focus, as it considers real engineering scenarios for detecting malware in industrial networks, operational monitoring of the monitoring system, recognition of firmware downgrade and SIEM-based detection of incidents and anomalies.

The tasks set are formulated logically: identification of threats and main risks in OT/ICS; analysis of existing solutions; research on monitoring and analysis technologies; development of a monitoring system; realization in a test and real industrial environment; evaluation of effectiveness through experiments; development of a risk assessment methodology. This shows that the work addresses not only theoretical issues, but also real engineering needs related to the practical increase in cyber resilience of industrial organizations.

2. Degree of knowledge of the state of the problem and creative interpretation of the literary material

The dissertation demonstrates a very good degree of knowledge of the current state of the problem under study. The author examines the basic concepts and models in the field of OT/ICS, IACS and IIoT, the specifics of industrial communication protocols, the Purdue model, the differences between IT and OT security, as well as the peculiarities of passive monitoring in industrial environments.

The literature material is used purposefully and is tied to specific engineering solutions. Standards, reference models, official documentation of the products used, scientific publications and reports on current OT/ICS threats are analyzed. A particularly positive impression is made by the author that the author does not limit himself to a description of known means of protection, but places them in the context of practical scenarios - SOC operation, SIEM correlation, automated notifications, OSINT check, CMDB context and monitoring the performance of the monitoring system itself.

There is a creative interpretation of the literary material. It is expressed in adapting and upgrading certain approaches to the specific limitations of OT environments - passive surveillance without agents, avoiding active scanning, minimizing risk to the production process, reducing false positives and taking into account the need for rapid response to incidents.

3. Compliance of the chosen research methodology with the set goal and objectives of the dissertation with the achieved contributions:

The chosen research methodology is in full compliance with the goals and objectives. Theoretical-analytical, comparative, modeling and experimental methods are used in the work, which allow a systematic study of the problem and validation of the proposed engineering solutions.

The methodology covers threat analysis and technology solutions, design of surveillance and response architectures, development of specific rules and automations through KQL, SPL, Azure Logic Apps, Sentinel Automation Rules, and Zabbix/SNMP monitoring, as well as practical verification through controlled test scenarios. Verification is done through real or close to real industry settings - detection of an EICAR test file, communication to a known malicious IP address, controlled shutdown of a D4IoT sensor, downgrade of industrial controller firmware and playback of Windows/IPS events in Splunk.

This sequence proves that the dissertation student is able to move from problem analysis to engineering solution, from there to experimental verification and finally to the formulation of scientific and applied scientific contributions. The results achieved are a logical consequence of the chosen methodology.

4. A brief analytical description of the nature and assessment of the credibility of the material on which the contributions of the dissertation are built.

The dissertation is developed in a volume of 187 pages and is structured in an introduction, four chapters, lists of figures and tables, a list of abbreviations and notations used and a bibliographic reference. The structure is logical and follows a natural sequence - from the introduction of the subject area and the main threats, through monitoring and SIEM technologies, to the development and experimental verification of specific solutions.

In the introduction, the relevance, purpose and objectives of the study are motivated. The practical significance of the developed system is indicated, including implementation in a large automotive company, protection of a significant number of OT, IT, IoT and IIoT devices, participation in a research project and application for a utility model.

Chapter One presents a systematic overview of industrial networks, OT/ICS concepts, equipment specifics, protocols, reference models, and Microsoft Defender for IoT. A mechanism has been developed for notification when malware is detected in an industrial network through the integration of D4IoT - Microsoft Sentinel - Azure Logic Apps - SOC. The tests conducted show operability both in EICAR test detection and in an attempt to communicate to a known malicious IP address.

Chapter Two examines the nature of logs, SIEM systems and their functions for collecting, normalizing, parsing, correlation, and notification. The main engineering development in this chapter is the operational monitoring of D4IoT implementation through two Sentinel rules, Azure Logic Apps with ARG request, and on-premises Zabbix/SNMP monitoring. Tests prove that the proposed system can detect various states of degradation or loss of vision.

Chapter 3 is devoted to detecting attacks aimed at downgrading the firmware version. The developed solution uses the "Firmware Change Detected" alarm, extracting versions via KQL and regular expressions, comparing version components, and generating an incident only on regression. Validation was performed on real industrial devices, including the Atlas Copco Power Focus 6000, and the system correctly distinguishes a firmware downgrade from a subsequent legitimate upgrade.

Chapter Four introduces Splunk Enterprise as a SIEM solution and develops a reference architecture for deploying on-premises, remote windows, and IDS/IPS logs. Rules for successful and failed login attempts, CnC communication from an internal machine, as well as deletion of the Windows Security log are configured. The tests carried out prove the applicability of the developed SPL-based rules and automatic notification mechanisms.

The credibility of the material is based on real experimental setups, practical implementations, specific configurations, logical addresses, queries, on-screen results, tables, and repeatable test scenarios. The use of standard platforms and tools, as well as comparison with alternative products and approaches, further increase the credibility of the results obtained.

5. Scientific, applied and applied contributions to the dissertation

I accept the claims for scientific and applied scientific contributions defined in the dissertation as reflecting the results achieved by the PhD student. Contributions can be summarised as follows:

- Scientific contributions:

✓ A method for building a "real-time notification pipeline" for OT/ICS detections is derived, implemented through a sequence D4IoT -> SIEM -> automation -> SOC, and minimum attributes for operationally valid notification are defined.

✓ A primary model has been formulated for the analysis of OT/ICS alarms by combining CMDB context, system criticality, and OSINT reputation of external destinations.

✓ The concept of "monitoring the monitoring system" in an OT/ICS context has been formalized through indicators for the absence of alarms, interruption of cloud connectivity and unavailability of the management interface.

✓ A multi-layered model for the reliability of operational monitoring through independent notification mechanisms - SIEM incident, Teams message and email is proposed.

✓ A "version-aware" model has been introduced to detect firmware downgrade in passive OT/ICS monitoring, which transforms a general firmware change alarm into a specific indication of regression and potential reintroduction of vulnerabilities.

✓ A SIEM-oriented model has been created for detecting phases of a traditional cyberattack by correlating Windows operating and network IPS logs in a single system.

- Scientific and applied contributions:

✓ Automation has been created and implemented through Azure Logic Apps for instant notification of malware detections by D4IoT in industrial environments with Microsoft Sentinel integration.

✓ KQL-based alarm enrichment has been developed by extracting the SensorId and matching it to a physical location, which turns the raw alarm into a response-oriented contextual signal.

✓ Two Sentinel analytical rules have been created to detect a lack of D4IoT alarms – globally and for a specific sensor – in order to track potential loss of visibility.

✓ Azure Logic Apps automation has been developed with Azure Resource Graph, a query to monitor LastConnectivityTime, and Teams notification when cloud connectivity is interrupted.

- ✓ An independent local monitoring layer has been created via Zabbix, SNMP and ping to monitor the D4IoT sensor management interface, also applicable in environments without Internet connectivity.
- ✓ A Sentinel analytical rule has been created for firmware downgrade by parsing ExtendedProperties, extracting versions with Regex, and digit-by-digit comparison of version components.
- ✓ Automation has been developed for weekly firmware change reports via Azure Logic Apps, CSV file, and email, supporting firmware lifecycle management and regulatory compliance.
- ✓ A Splunk Enterprise reference architecture with separate indexes for local, remote and network logs and a set of SPL-based rules for alarms and periodic reports has been implemented.

- Applied contributions:
- ✓ Practically working prototypes and technical mechanisms for monitoring, notifying, correlating and investigating events in OT/ICS and IoT environments have been developed.
- ✓ The proposed solutions are verified through controlled tests and real-world industry scenarios, including malware detection, loss of connectivity, firmware downgrade, and suspicious SIEM events.
- ✓ The practical applicability of the developed system in a large-scale industrial environment is shown, achieving an increase in visibility, shortening the response time and reducing the risk of missed incidents.

The PhD student demonstrates knowledge from various fields and skills in applying it to solving engineering problems, as well as reducing them to specific algorithms.

6. Assessment of the degree of personal participation of the dissertation student in the contributions.

The presented content, the developed architectures, the specific KQL and SPL rules, the automations, the experimental scenarios and the analysis of the results give reason to assume that the contributions are the result of the personal work of the PhD student. The author demonstrates high engineering competence and the ability to combine knowledge of cybersecurity, communication networks, cloud technologies, SIEM systems, and industrial control environments.

It is especially important that the dissertation is not limited to a theoretical description of product functionalities, but designs, implements and tests practical mechanisms that are directly related to the activities of information security centers and to the protection of real industrial processes. This shows a high degree of personal participation and autonomy in the formulation and implementation of contributions.

7. Assessment of the publications of the dissertation.

The presented content, the analyzes carried out and the examples developed within the framework of the dissertation show the excellent knowledge of the studied area in which the work is focused. The results of the dissertation research obtained by the author have been published in 6 scientific papers – 1 in a journal and 5 in conferences. One of the papers was published in an international scientific journal with IF 2.2 in Q2 of Web of Science. All this gives me reason to believe that the results achieved in the dissertation were made by the doctoral student. All articles are in English, co-authored with the supervisors of the PhD student.

There is no doubt that the publications are the main work of the PhD student and that through them he is highly appreciated by the scientific and engineering community.

8. Use of the results of the dissertation in scientific and social practice. Presence of a achieved direct economic effect, etc. Documents on which the allegation is based.

The results of the dissertation have a clear applicability in scientific, engineering and social practice. The developed system is aimed at increasing the security of industrial networks that support critical processes in manufacturing, energy, logistics and other significant industries. Thus, the results are not only technological, but also societal significance, as they contribute to limiting the risk of operational interruptions, material damage and safety threats.

In the dissertation, it is stated that the developed system is integrated into a large automotive company and protects a significant number of OT, IT, IoT and IIoT devices. Participation in project BG-RRP-2.004-0005 "Multivalent system for protection against cyber attacks in communication and industrial networks with added functionality of neural networks", recognition by Microsoft in connection with contribution to the functionalities of Defender for IoT and submission of a utility model application are also indicated.

At present, no specific quantitative data on the realized direct economic effect have been presented. However, the potential for such is significant, as the proposed solutions can reduce the time to detect and respond to incidents, limit unplanned outages, and improve risk management in industrial organizations. The statements are based on the experimental results presented in the dissertation, the described implementations, the project activity and the publication data.

9. Assessment of the compliance of the abstract with the requirements for its preparation, as well as the adequacy of the reflection of the main points and contributions of the dissertation.

The abstract is formatted in 32 pages and meets the requirements for its preparation, as well as for its printing. The main provisions of the dissertation are

reflected accurately and clearly in the abstract. The contributions of the dissertation are derived, accurately classified and described.

10. Opinions, recommendations and comments.

In general, I submitted my opinion, recommendations and notes on the work submitted to me for review in writing to the PhD student, which are reflected in the latest version of the dissertation.

I recommend active publication activity abroad in the future research of the dissertation.

11. Conclusion

In conclusion, I believe that the work has completion, contains original solutions and the topic is relevant. The notes and recommendations made do not dispute the contributions of the dissertation.

I believe that the requirements of the Law on the Development of the Academic Staff in Bulgaria and the Regulations for its implementation have been fulfilled in the presented dissertation.

I give a positive assessment of the work and propose to the esteemed Scientific Jury to award to Mag. Eng. Marian Hristov the educational and scientific degree of "**Doctor**" in the professional field 5.3 Communication and Computer Equipment, scientific specialty "Security Equipment and Systems".

Date: 06.07.2026

Reviewer:

/ Assoc. prof. Georgi Tsochev/