ОТЗ-ИС1-093
07.04.2026

СТАНОВИЩЕ

върху дисертационен труд за придобиване на образователна и научна степен **„доктор“**

Автор на дисертационния труд: **маг. инж. Мариан Христов**

Тема на дисертационния труд: **Изследване на облачно-базирана система за наблюдение и анализ на събития**

Член на научното жури: **доц. д-р инж. Кирил Късев**

1. Актуалност на разработвания в дисертационния труд проблем в научно и научноприложно отношение.

Дисертационният труд акцентира върху актуален научно-приложен проблем, произтичащ от задълбочаващата се конвергенция между информационни (IT) и оперативни технологии (OT), в контекста на масовото навлизане на IoT/IIoT устройства в индустриалните системи. Компрометирането на този вид инфраструктура носи значими рискове. Това придава на изследваната проблематика особена значимост.

Авторът коректно идентифицира следните системни предизвикателства, които обуславят необходимостта от нов подход: техническа невъзможност за инсталиране на агенти и ограничения пред активното сканиране в OT среда; хетерогенност на източниците на телеметрия, която затруднява корелацията и трансформиране на детекцията в оперативни действия; липса на бърза и надеждна връзка между детекция и реакция; нарастваща тенденция за прикриване на злонамерени действия зад легитимни процеси, което изисква контекстно-ориентирана аналитична логика.

Върху тази основа е обоснован избора на облачно-базиран подход за наблюдение и анализ на събития, като адекватно решение, съчетаващо централизация, мащабируемост и аналитични процедури в реално време, съобразно специфичните изисквания за индустриални среди.

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

Докторантът демонстрира задълбочено познаване на състоянието на проблема. В дисертацията са използвани 240 източника. Преобладаваща част са под формата на онлайн съдържание. Извършен е анализ на методи, алгоритми и протоколи, свързани с наблюдение и анализ на събития в индустриални мрежи. Всичко това показва, че докторантът е запознат със състоянието на проблема. На базата на представения литературен обзор, коректно са дефинирани задачите за постигане на поставената цел.

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

Поставените задачи в дисертационния труд са решени в необходимия обем. Изследванията са подчинени на подход, който обхваща: анализ на облачно-базирана система за събиране и обработване на събития; оценка на различните видове събития, обогатяване на контекст и механизми за алармиране; създаване на процедури за автоматизация и канали за уведомяване, с които се подпомагат оперативните дейности; процедури за валидиране, чрез проведени тестове в реална индустриална среда.

4. Приноси на дисертационния труд

Приносите в дисертационния труд имат научно-приложен и приложен характер. Представляват подобряване на известни подходи, модели и методи. Могат да бъдат оценени като релевантни, приложими и полезни за повишаване на ефективността на системи за киберзащита в индустриални среди. Приносите могат да бъдат обобщени, както следва: предложени и валидирани механизми за уведомяване в реално време, обогатяване на алармите с оперативен контекст и първоначална оценка на риска чрез CMDB и OSINT проверки; разработен и валидиран подход за трудно различими въздействия, имитиращи легитимни процеси (version-aware детекция на firmware-downgrade); предложена SIEM-ориентирана рамка за детекция на различни фази на кибератака, чрез корелация на операционни и мрежови логове; създадени и внедрени правила, автоматизации и механизми за уведомяване в утвърдени среди за наблюдение и анализ на потенциално опасни събития.

5. Преценка на публикациите по дисертационния труд.

Броят на авторските публикации, отразяващи постиженията в дисертационния труд, са 6. В четири от тях маг. инж. Мариан Христов е основен автор, а в останалите 2 е в съавторство.

Всички представени публикации са на английски език и са в актуална и развиваща се област, с акцент върху наблюдение и анализ на събития в индустриални мрежи. Публикувани са в международни конференции и в национални конференции с международно участие. Една от научните разработки е публикувана в международно списание със SJR 0.424 (2025), попадащо в квартил Q2. Допълнителен атестат за качеството на публикационната дейност е индексирането на всички публикации в базата данни Scopus. Забелязват се и цитирания на авторските публикации – за индексираните в базата данни Scopus са налични 30 цитирания.

Публикационната дейност на кандидата показва, че дисертационния труд е получил публичност пред специалистите в областта. В количествено и качествено отношение напълно удовлетворяват минималните национални изисквания, както и минималните изисквания на Технически университет – София за придобиване на образователна и научна степен „доктор".

6. Мнения, препоръки и бележки.

Докторантът в голяма степен е отчел направените препоръки и забележки, следствие от процедурата за предварително обсъждане. Нямам съществени критични забележки, а по-скоро следните препоръки:

- Приносите на автора към отделните глави на дисертационния труд биха могли да се формулират по-добре;
- Дисертационният труд би спечелил от по-задълбочен сравнителен анализ, спрямо утвърдени решения, извън системата на Microsoft Defender for IoT.

Въпреки гореизложеното, посочените препоръки не омаловажават постигнатите научно-приложни и приложни резултати.

7. Заключение с ясна положителна или отрицателна оценка на дисертационния труд.

Темата на дисертационния труд е актуална. Получените резултати са следствие от проведени изследвания, които са станали достояние на научната общност. Подходите и методите, използвани за решаване на поставените задачи, се отличават с адекватност и имат научно-приложен и приложен характер.

Взимайки под внимание приносите на докторанта, считам че са удовлетворени изискванията на ЗРАСРБ и Правилника за условията и реда за придобиване на научни степени в Технически университет – София. Давам положителна оценка на дисертационния труд и предлагам на уважаемото Научно жури да присъди образователната и научна степен „доктор" на маг. инж. Мариан Христов, по докторска програма „Осигурителна техника и системи", в област 5. Технически науки, професионално направление 5.3 „Комуникационна и компютърна техника".

Дата: 07.07.2026 г. ЧЛЕН НА ЖУРИТО: [redacted]

(доц. д-р инж. Кирил Кърсев)

ОПС 78-НС1-023
07.07.20[redacted]

EVALUATION STATEMENT

on a dissertation submitted for the award of the „**Ph.D.**" degree

Thesis Author:	**Marian Hristov**, MSc. Eng.
Thesis Title:	**Investigation of a Cloud-based Security Information and Event Management System**
Scientific Jury Member:	**Dr. Kiril Kassev**, Assoc. Prof.

1. Relevance of the problem addressed in the dissertation in scientific and applied-scientific terms.

The thesis focusses on a relevant scientific and applied problem arising from the deep convergence between information technologies (IT) and operational technologies (OT), in the context of the widespread introduction of IoT/IIoT devices into industrial systems. Compromising this infrastructure type entails significant risks. This gives the research topic particular importance.

The author correctly identifies a set of challenges paving the way for new approaches: both technical impossibility of installing agents and the limitations on active monitoring in an OT environment; the heterogeneity of telemetry sources, which complicates correlation and the transformation of detection into operational actions; the lack of a rapid and reliable link between detection and response; and the growing tendency to mask malicious actions behind legitimate processes, which requires context-oriented analytical logic.

On this basis, the choice of a cloud-based approach for event monitoring and analysis is justified as an adequate solution combining centralization, scalability and real-time analytical procedures, in line with the specific requirements of industrial environments.

2. Degree of familiarity with the state of the problem and the references creative interpretation.

The doctoral candidate demonstrates an in-depth knowledge of the state of the problem. The dissertation draws on 240 references, the predominant part of which consists of online content. An analysis has been carried out of methods, algorithms and protocols related to the monitoring and analysis of events in industrial networks. All this shows that the doctoral candidate is well acquainted with the state of the problem. On the basis of the literature review presented, the tasks for achieving the stated aim have been correctly defined.

3. Compliance of the selected research methodology as well as the stated aim and objectives of the dissertation with the contributions achieved.

The tasks set in the dissertation have been solved to the required extent. The research follows an approach that encompasses analysis of a cloud-based system for collecting and processing events; assessment of different types of events, context enrichment and alerting mechanisms; development of automation procedures and notification channels supporting operational activities; and validation procedures through tests conducted in a real industrial environment.

4. Dissertation contributions

The contributions of the dissertation are of a scientific-applied and applied nature. They represent improvements to known approaches, models and methods. They can be assessed as relevant, applicable and useful for increasing the effectiveness of cybersecurity systems in industrial environments. The contributions can be summarized as follows: proposed and validated mechanisms for real-time notification, enrichment of alerts with operational context, and initial risk assessment through CMDB and OSINT checks; a developed and validated approach for hard-to-distinguish impacts that mimic legitimate processes (version-aware detection of firmware-downgrade attacks); a proposed SIEM-oriented framework for detecting different phases of a cyberattack through correlation of operational and network logs; and rules, automations and notification mechanisms created and implemented within established monitoring and analysis environments for potentially dangerous events.

5. Assessment of the publications related to the dissertation.

The number of author's publications reflecting the achievements of the dissertation is 6. In four of them, Marian Hristov, MSc Eng., is the principal author, while in the remaining 2 he is a co-author.

All submitted publications are in English and fall within a current and developing field, with an emphasis on event monitoring and analysis in industrial networks. They have been published at international conferences and at national conferences with international participation. A scientific paper has been published in an international journal with an SJR of 0.424 (2025), falling within quartile Q2. A further testament to the quality of the publication activity is the fact that all publications are indexed in the Scopus database. Citations of the author's publications are also observed — 30 citations are recorded for those indexed in Scopus.

The candidate's publication activity shows that the dissertation has gained visibility among specialists in the field. In quantitative and qualitative terms, it fully satisfies the minimum national requirements, as well as the minimum requirements of the Technical University of Sofia for the acquisition of the "PhD" degree.

6. Opinions, recommendations and remarks.

The doctoral candidate has largely considered the recommendations and remarks made following the preliminary discussion procedure. I have no substantial critical remarks, but rather the following recommendations:

- The author's contributions to the individual chapters of the dissertation may be formulated more clearly.
- The dissertation would benefit from a more in-depth comparative analysis against established solutions outside the Microsoft Defender for IoT system.

Notwithstanding the above, these recommendations do not diminish both the scientific-applied and applied results achieved.

7. Conclusion with a clear positive or negative assessment of the dissertation.

The topic of the dissertation is relevant. The results obtained are a consequence of research that has become known to the scientific community. The approaches and methods used to solve the stated tasks are characterized by adequacy and have a scientific-applied and applied nature.

Taking into account the doctoral candidate's contributions, I consider that the requirements of both the Act for the Development of the Academic Staff in the Republic of Bulgaria and the Regulations on the Terms and Procedure for the Acquisition of Scientific Degrees at the Technical University of Sofia have been satisfied. I give a positive assessment of the dissertation and propose to the respected Scientific Jury that the educational and scientific degree "Doctor" be awarded to Marian Hristov, MSc. Eng., in the doctoral programme "Safety and Security Systems Engineering", in Area 5. Technical Sciences, professional field 5.3 "Communication and Computer Engineering".

07 July 2026 SCIENTIFIC JURY MEMBER: ...

(Dr. Kiril Kassev, Assoc. Prof.)