УДК 004.056.53:681.5
DOI https://doi.org/10.15589/znp2025.4(502).25

ARCHITECTURAL PRINCIPLES OF SECURITY EVENT MONITORING SYSTEM DEVELOPMENT IN COMPUTER-INTEGRATED SYSTEMS BASED ON WAZUH PLATFORM

АРХІТЕКТУРНІ ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ПОДІЙ БЕЗПЕКИ В КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ СИСТЕМАХ НА БАЗІ ПЛАТФОРМИ WAZUH

Halina A. Bogdan
bohdan.halyna@lll.kpi.ua
ORCID: 0000-0001-6745-1509

Dzhamil V. Trokhymchuk
trokhymchuk.jamil@lll.kpi.ua
ORCID: 0009-0003-1059-9483

Г. А. Богдан,
канд. техн. наук, доцент

Д. В. Трохимчук,
здобувач вищої освіти

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Abstract. *Purpose*. The purpose of the article is to analyze the principles of building security monitoring systems in computer-integrated systems, define specific requirements for such systems, and substantiate a hybrid monitoring architecture based on the Wazuh platform as an effective means of threat detection in heterogeneous environments.
Methodology. The current issues of ensuring information security of modern computer-integrated systems characterized by deep convergence of information and operational technologies are analyzed. A detailed analysis of the threat landscape resulting from connecting previously isolated industrial networks to corporate infrastructure and the global Internet is conducted. It is determined that traditional monitoring approaches, focused primarily on data confidentiality, are insufficient and sometimes dangerous for computer-integrated systems, where the priorities are service availability, technological process integrity, and physical safety of personnel and equipment. The features of applying Security Information and Event Management (SIEM) systems under conditions of limited computing resources and specific requirements of industrial data transmission protocols are investigated. It is revealed that existing commercial solutions often have excessive licensing costs dependent on data volume and closed architecture, complicating their adaptation to heterogeneous industrial environments. Special attention is paid to analyzing vulnerabilities of legacy equipment that cannot be updated and the need for compensatory protection measures.
Results. Based on a comparative analysis of functional capabilities, the feasibility of using the open-source platform Wazuh as a base component of the monitoring system is justified. An architectural approach combining agent-based monitoring of critical nodes, such as operator stations and engineering servers, with passive network traffic analysis at the level of industrial controllers is proposed. Recommendations for configuring event correlation rules and active response scenarios considering the "Human-in-the-Loop" principle to avoid emergency shutdown of technological processes due to false positives are developed and described. The research results confirm that using the proposed architecture allows creating a cost-effective, scalable, and flexible intrusion detection system capable of identifying complex targeted attacks at early implementation stages.
Scientific novelty. The approach to building monitoring systems for industrial environments has been further developed. It is based on combining active file integrity monitoring (FIM) and passive analysis of industrial protocols, which allows eliminating "blind spots" in the protection of computer-integrated systems.
Practical importance. The practical value of the work lies in the development of a typical architecture and recommendations that can be implemented at critical infrastructure enterprises with minimal financial costs due to the use of open-source software.
Key words: computer-integrated systems, operational technologies, information security, Wazuh, incident monitoring, intrusion detection system, SCADA, Purdue model.

Анотація. *Мета*. Аналіз принципів побудови систем моніторингу безпеки в комп'ютерно-інтегрованих системах, визначення специфічних вимог до таких систем та обґрунтування гібридної архітектури моніторингу на базі платформи Wazuh як ефективного засобу виявлення загроз у гетерогенних середовищах.
Методика. Проаналізовано актуальну проблематику забезпечення інформаційної безпеки сучасних комп'ютерно-інтегрованих систем, які характеризуються глибокою конвергенцією інформаційних та операційних технологій. Проведено детальний аналіз ландшафту загроз, що виникають внаслідок підключення раніше ізольованих промислових мереж до корпоративної інфраструктури та глобальної мережі Інтернет. Визначено, що традиційні підходи до моніторингу, орієнтовані насамперед на забезпечення конфіденційності даних, є недостатніми та подекуди небезпечними для комп'ютерно-інтегрованих систем, де пріоритетами виступають доступність сервісів, цілісність технологічного процесу та фізична безпека персоналу і обладнання. Досліджено особливості застосування систем управління інформацією про безпеку та подіями (SIEM) в умовах обмежених обчислювальних ресурсів та специфічних вимог промислових протоколів передачі даних. Виявлено, що наявні комерційні рішення часто мають надмірну вартість ліцензування, яка залежить від обсягу даних, та закриту архітектуру, що ускладнює їх адаптацію до гетерогенних середовищ промислових підприємств. Особливу увагу приділено аналізу вразливостей застарілого обладнання, яке не підлягає оновленню, та необхідності застосування компенсаційних заходів захисту.
Результати. На основі проведеного порівняльного аналізу функціональних можливостей обґрунтовано доцільність використання платформи з відкритим кодом Wazuh як базового компонента системи моніторингу. Запропоновано архітектурний підхід, що поєднує агентський моніторинг критичних вузлів, таких як станції оператора та інженерні сервери, з пасивним аналізом мережевого трафіку на рівні промислових контролерів. Розроблено та описано рекомендації щодо налаштування правил кореляції подій та сценаріїв активного реагування, які враховують принцип участі людини в контурі управління (Human-in-the-Loop) для уникнення аварійного зупинення технологічних процесів через помилкові спрацьовування системи захисту. Результати дослідження підтверджують, що використання запропонованої архітектури дозволяє створити економічно ефективну, масштабовану та гнучку систему виявлення вторгнень, здатну ідентифікувати складні цільові атаки на ранніх етапах їх реалізації.
Наукова новизна. У роботі набув подальшого розвитку підхід до побудови систем моніторингу для промислових середовищ, який базується на поєднанні активного моніторингу цілісності файлів (FIM) та пасивного аналізу промислових протоколів, що дозволяє усунути «сліпі зони» в захисті комп'ютерно-інтегрованих систем.
Практична значимість роботи полягає у розробці типової архітектури та рекомендацій, які можуть бути імплементовані на підприємствах критичної інфраструктури з мінімальними фінансовими витратами завдяки використанню відкритого програмного забезпечення.
Ключові слова: комп'ютерно-інтегровані системи, операційні технології, інформаційна безпека, Wazuh, моніторинг інцидентів, система виявлення вторгнень, SCADA, модель Пердью.

ПОСТАНОВКА ЗАДАЧІ

Сучасний етап розвитку промисловості, відомий як концепція Індустрії 4.0, характеризується безпрецедентною інтеграцією фізичних виробничих процесів з цифровими технологіями. Комп'ютерно-інтегровані системи (КІС) стають основою критичної інфраструктури держави, забезпечуючи керування енергетикою, транспортом, водопостачанням та автоматизованим виробництвом. Однак, конвергенція інформаційних (IT) та операційних (OT) технологій, що надає значні переваги в ефективності, гнучкості та керованості, водночас руйнує традиційний периметр безпеки, який десятиліттями базувався на фізичній ізоляції або так званому «повітряному проміжку» (air gap).

Відкриття промислових мереж для зовнішнього світу призвело до появи нових векторів атак, спрямованих не на викрадення інформації, а на порушення технологічних процесів, фізичне пошкодження дороговартісного обладнання та створення екологічних загроз. В умовах зростання кількості та складності кібератак питання побудови ефективної, всеосяжної та економічно доступної системи моніторингу подій безпеки в КІС набуває критичної актуальності. Існуючі комерційні рішення класу SIEM (Security Information and Event Management) часто є фінансово недоступними для багатьох підприємств або надто складними в адаптації до специфічних промислових протоколів (Modbus, DNP3, IEC 61850). Тому виникає науково-практична задача пошуку та обґрунтування архітектурних рішень на базі відкритого програмного забезпечення, які б забезпечували необхідний рівень захисту без надмірних витрат.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Фундаментальні відмінності між безпекою традиційних IT-систем та промислових систем управління (ICS) були детально досліджені в роботі К. Стоуффера та співавторів [1]. У їхньому керівництві NIST SP 800-82 визначено, що в той час як в IT пріоритетом є конфіденційність, в OT на першому місці стоять доступність та цілісність. Це твердження

підкріплюється міжнародними стандартами серії IEC 62443 [2], які закладають основу для зонування мереж та оцінки ризиків у промисловому середовищі.

Проблематика вразливості протоколів SCADA та необхідність перегляду підходів до їх захисту глибоко проаналізована Е.Дж. Байерсом [3], який вказує на відсутність вбудованих механізмів автентифікації у застарілих протоколах. Загальні принципи обробки інцидентів інформаційної безпеки викладені у керівництві П. Чіхонскі [4], однак Р.М. Лі [5] адаптував ці підходи, запропонувавши модель Cyber Kill Chain саме для промислових систем, що дозволяє розуміти етапність атак на КІС.

Питання важливості логування та аудиту подій розкрито К. Кентом [6], а специфічні огляди кібербезпеки промислових систем надані у працях К. Хемслі [7]. Структуру промислових мереж та вектори атак на них досліджували Б. Гелловей та Г.П. Ханке [8].

Окрему увагу дослідників привертають резонансні атаки на КІС. Технічний аналіз хробака Stuxnet, який змінив парадигму кібервійни, проведено Р. Лангнером [9] та Д. Кушнером [12]. Аналіз атаки на енергосистему України (Industroyer) представлено у звітах ESET [10], а специфіку промислових програм-вимагачів, таких як LockerGoga, досліджено Check Point Research [11].

Ринок сучасних SIEM-систем та тенденції його розвитку висвітлені у звітах Gartner [13]. Порівняльний аналіз інструментів SIEM наведено у роботі С.А. Басета [14]. Технічна документація платформи Wazuh [15] надає детальну інформацію про архітектуру та можливості цього рішення з відкритим кодом, проте в науковій літературі питання комплексної побудови системи захисту КІС саме на базі Wazuh висвітлено недостатньо.

Метою статті є аналіз принципів побудови систем моніторингу безпеки в комп'ютерно-інтегрованих системах, визначення специфічних вимог до таких систем та обґрунтування гібридної архітектури моніторингу на базі платформи Wazuh як ефективного засобу виявлення загроз у гетерогенних середовищах.

ОСНОВНИЙ МАТЕРІАЛ.

1. Специфіка об'єкта захисту та модель Пердью

Комп'ютерно-інтегровані системи функціонують на перетині цифрового та фізичного світів. Для їх структурного опису та побудови системи захисту традиційно використовується ієрархічна модель Пердью (Purdue Enterprise Reference Architecture), яка розділяє інфраструктуру підприємства на логічні рівні. Розуміння цієї моделі є критичним для правильного розміщення сенсорів моніторингу.

- Рівень 0 (Фізичний процес): включає датчики, приводи, мотори, турбіни та інше обладнання, що безпосередньо виконує фізичну роботу. Моніторинг тут ускладнений через відсутність цифрових інтерфейсів.
- Рівень 1 (Базове управління): тут розміщуються програмовані логічні контролери (PLC) та віддалені термінальні пристрої (RTU), які зчитують дані з сенсорів та керують приводами за закладеною логікою. Це критичний рівень, атака на який (як у випадку Stuxnet) призводить до фізичних наслідків.
- Рівень 2 (Локальне управління): включає людино-машинні інтерфейси (HMI) та інженерні станції, що дозволяють операторам взаємодіяти з процесом в межах одного цеху чи установки. Це найчастіша точка входу для атак через USB або скомпрометовані ноутбуки підрядників.
- Рівень 3 (Управління виробництвом): системи SCADA, сервери баз даних історичних подій (Historian), системи управління виробничими процесами (MES). Цей рівень є мостом між OT та IT.
- Рівень 4 та 5 (Корпоративна мережа): бізнес-системи (ERP), поштові сервери, доступ до Інтернету.

Згідно з дослідженнями Б. Гелловея [8], конвергенція IT/OT призводить до розмивання меж між рівнями 3 та 4, що створює прямі маршрути для зловмисників від Інтернету до фізичного обладнання. Тому система моніторингу повинна охоплювати всі рівні, починаючи з Рівня 1.

Ключовою відмінністю КІС від класичних IT-систем є інверсія тріади безпеки. Як зазначається в роботі К. Стоуффера [1], якщо в IT головним є конфіденційність, то в КІС пріоритети розподіляються наступним чином:

1) Доступність, адже простій системи може призвести до зупинки конвеєра, відключення електроенергії або аварії.

2) Цілісність, адже дані телеметрії та керуючі команди повинні бути точними (наприклад, модифікація уставки тиску або температури може спричинити вибух)

3) Безпека – це специфічний для КІС пріоритет, що означає захист життя та здоров'я людей.

2. Аналіз актуальних загроз

Ландшафт загроз для КІС суттєво змінився за останнє десятиліття. Адаптована Р. М. Лі [5] модель «Cyber Kill Chain» показує, що атака на промисловий об'єкт зазвичай складається з двох фаз: перша – компрометація корпоративної мережі та закріплення, друга – перехід в OT-мережу та маніпуляція технологічним процесом.

Аналіз відомих інцидентів дозволяє виділити основні класи загроз:

- Складні цільові атаки (APT). Яскравим прикладом є Stuxnet, детально проаналізований Р. Лангнером [9] та Д. Кушнером [12]. Цей шкідливий код використовував вразливості «нульового дня» та розповсюджувався через USB-носії, щоб обійти повітряний проміжок, цілеспрямовано модифікуючи логіку роботи контролерів Siemens.
- Атаки на протоколи управління. Дослідження ESET [10] щодо атаки Industroyer показали, що

зловмисники можуть використовувати нативні команди промислових протоколів (IEC 104, IEC 61850) для відключення підстанцій, не використовуючи експлойти, а лише легітимний функціонал управління. Це робить такі атаки невидимими для стандартних антивірусів.

• Промислові програми-вимагачі. Згідно зі звітом Check Point [11], такі загрози як LockerGoga або EKANS цілеспрямовано шукають та зупиняють процеси SCADA-систем перед шифруванням даних, що призводить до повної втрати видимості та контролю над процесом.

3. Вибір інструментарію моніторингу

Для побудови системи моніторингу, що відповідає вимогам стандартів та враховує наведені загрози, було проведено порівняння провідних SIEM-рішень. Аналіз ринку, проведений Gartner [13], виділяє лідерів, таких як Splunk та IBM QRadar. Огляд інструментів С. А. Басета [14] також вказує на їхні широкі можливості. Однак, для українських реалій та специфіки КІС, платформа Wazuh має низку переваг (таблиця 1)

Як зазначено в документації [15], Wazuh поєднує в собі функції XDR (Extended Detection and Response) та SIEM. Ключовою перевагою для КІС є наявність потужного хостового агента (HIDS). Оскільки багато атак (як Stuxnet) починаються з компрометації робочої станції оператора або інженера, моніторинг цілісності файлів (FIM) на цих вузлах є критично важливим. Wazuh дозволяє виявляти зміни в конфігураційних файлах SCADA, проектах PLC та системних бібліотеках в реальному часі, навіть якщо комп'ютер не підключений до Інтернету (при наступному підключенні агент передасть дані).

4. Запропонована архітектура системи

Враховуючи рекомендації NIST SP 800-82 [1] щодо необхідності ешелонованого захисту, пропонується гібридна архітектура системи моніторингу. Вона поєднує активний збір даних з хостів та пасивний аналіз мережі.

Архітектура складається з трьох рівнів:

1) Рівень збору даних:

– на рівнях 2, 3 та 4 моделі Пердью (сервери SCADA, HMI, інженерні станції, сервери баз даних) встановлюються легковісні Wazuh Agents. Вони збирають системні логи, інформацію про запущені процеси, мережеві з'єднання та контролюють цілісність файлів.

– на рівні 1 (контролери PLC), де встановлення агентів неможливе, використовується пасивний моніторинг. Мережевий трафік дзеркалюється через SPAN-порти комутаторів на сенсори (наприклад, Suricata або Zeek). Ці сенсори аналізують промислові протоколи (Modbus, DNP3, S7comm) та передають логи на сервер Wazuh.

2. Рівень обробки та аналізу:

– Wazuh Server – центральний компонент, який отримує дані від агентів та мережевих сенсорів. Він виконує декодування логів, їх нормалізацію та кореляцію на основі попередньо заданих правил. Сервер розгортається в захищеному сегменті (DMZ).

– Wazuh Indexer – база даних на основі OpenSearch, що забезпечує швидке індексування та зберігання великих обсягів подій безпеки.

3) Рівень візуалізації та реагування:

– Wazuh Dashboard – веб-інтерфейс для аналітиків SOC (Security Operations Center), що надає інструменти для візуалізації атак, пошуку загроз та формування звітів.

5. Виявлення та реагування

Ефективність системи залежить від якості правил кореляції. Базовий набір правил Wazuh орієнтований на IT-загрози. Для захисту КІС необхідно розробити специфічні правила.

Наприклад, для виявлення атаки типу «Man-in-the-Middle» на протокол Modbus TCP, правило кореляції має аналізувати логи мережевого сенсора і спрацьовувати, якщо фіксується команда «Write Single Coil» (код функції 05) з IP-адреси, яка не належить авторизованій SCADA-системі або інженерній станції.

Особливу увагу слід приділити автоматизації реагування. Керівництво NIST SP 800-61 [4] описує загальний цикл обробки інцидентів. Wazuh реалізує цей цикл через механізм Active Response. Однак, в контексті КІС, застосування автоматичного блокування (наприклад, розрив з'єднання або блокування порту на комутаторі) несе високі ризики. Як зазначають К. Хемслі та Е. Фішер [7], помилкове спрацьовування системи захисту може призвести до втрати керування процесом, що є недопустимим.

Тому запропоновано диференційовану стратегію реагування:

• Зона IT (Рівень 4–5) – Дозволена повна автоматизація. Наприклад, при виявленні шкідливого ПЗ

Таблиця 1. Порівняльний аналіз засобів моніторингу

Характеристика	Splunk Enterprise	IBM QRadar	Wazuh
Ліцензування	Комерційне (за обсяг/EPS)	Комерційне (за EPS)	Безкоштовне (GPLv2)
Архітектура	Закрита	Закрита	Відкрита
HIDS функціонал	Потребує додаткових агентів	Обмежений	Ядро системи
FIM (Цілісність файлів)	Додатковий модуль	Додатковий модуль	Вбудовано (Real-time)
SCA (Оцінка конфігурації)	Окремий додаток	Окремий модуль	Вбудовано
Active Response	Через SOAR (Phantom)	Через SOAR	Вбудовано

на поштовому сервері, Wazuh може автоматично ізолювати хост або видалити файл.

• Зона ОТ (Рівень 1–3) – Застосовується принцип Human-in-the-Loop (Людина в контурі). При виявленні підозрілої активності на HMI-станції (наприклад, зміна системного файлу), Wazuh не блокує станцію, а виконує скрипт оповіщення оператора та інженера безпеки, а також може підвищити рівень логування для збору доказів. Блокування можливе лише після підтвердження людиною.

ВИСНОВКИ

У даному дослідженні проаналізовано проблематику захисту сучасних комп'ютерно-інтегрованих систем в умовах конвергенції технологій. На основі аналізу джерел підтверджено, що традиційні підходи до безпеки потребують адаптації.

Обґрунтовано вибір платформи Wazuh як оптимального рішення для побудови системи моніторингу. Запропонована гібридна архітектура, що поєднує агентський HIDS-моніторинг та пасивний мережевий аналіз, дозволяє усунути «сліпі зони» в захисті КІС. Реалізація принципу Human-in-the-Loop в сценаріях реагування забезпечує баланс між безпекою та безперервністю технологічних процесів.

Подальші дослідження можуть бути спрямовані на розробку спеціалізованих декодерів Wazuh для пропрієтарних промислових протоколів та інтеграцію системи з засобами машинного навчання для виявлення аномалій у технологічних даних.

REFERENCES

[1] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

[2] International Electrotechnical Commission. (2018). Security for industrial automation and control systems – Part 1–1: Terminology, concepts and models (IEC 62443-1-1).

[3] Byres, E. J. (2012). SCADA Security: What's Broken and How to Fix It. British Columbia Institute of Technology.

[4] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

[5] Lee, R. M. (2017). The Industrial Control System Cyber Kill Chain. SANS Institute.

[6] Kent, K., & Grance, T. (2006). Guide to Computer Security Log Management (NIST Special Publication 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

[7] Hemsley, K., & Fisher, E. (2018). A Review of Industrial Control System Cyber Security. International Conference on Cyber Warfare and Security.

[8] Galloway, B., & Hancke, G. P. (2013). Introduction to Industrial Control Networks. IEEE Communications Surveys & Tutorials, 15(2), 860–880. https://doi.org/10.1109/SURV.2012.071812.00124

[9] Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy, 9(3), 49–51. https://doi.org/10.1109/MSP.2011.67

[10] ESET. (2017). Industroyer: A new threat for industrial control systems [White Paper].

[11] Check Point Research. (2020). LockerGoga: A New Targeted Ransomware Attack [Technical Report].

[12] Kushner, D. (2013). The Real Story of Stuxnet. IEEE Spectrum, 50(3), 48–53. https://doi.org/10.1109/MSPEC.2013.6471059

[13] Gartner. (2021). Magic Quadrant for Security Information and Event Management.

[14] Baset, S. A., & Bith, H. (2014). A Survey of SIEM Tools and Their Application in Detecting Attacks. International Conference on Cyber Security and Protection of Digital Services. https://www.google.com/search?q=https://doi.org/10.1109/CyberSecPODS.2014.6851979

[15] Wazuh. (2025). Architecture. Wazuh Documentation. Retrieved from https://documentation.wazuh.com/current/architecture/index.html

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

[2] International Electrotechnical Commission. (2018). Security for industrial automation and control systems – Part 1–1: Terminology, concepts and models (IEC 62443-1-1).

[3] Byres, E. J. (2012). SCADA Security: What's Broken and How to Fix It. British Columbia Institute of Technology.

[4] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

[5] Lee, R. M. (2017). The Industrial Control System Cyber Kill Chain. SANS Institute.

[6] Kent, K., & Grance, T. (2006). Guide to Computer Security Log Management (NIST Special Publication 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

[7] Hemsley, K., & Fisher, E. (2018). A Review of Industrial Control System Cyber Security. International Conference on Cyber Warfare and Security.

[8] Galloway, B., & Hancke, G. P. (2013). Introduction to Industrial Control Networks. IEEE Communications Surveys & Tutorials, 15(2), 860–880. https://doi.org/10.1109/SURV.2012.071812.00124

[9] Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy, 9(3), 49–51. https://doi.org/10.1109/MSP.2011.67

[10] ESET. (2017). Industroyer: A new threat for industrial control systems [White Paper].

[11] Check Point Research. (2020). LockerGoga: A New Targeted Ransomware Attack [Technical Report].

[12] Kushner, D. (2013). The Real Story of Stuxnet. IEEE Spectrum, 50(3), 48–53. https://doi.org/10.1109/MSPEC.2013.6471059

[13] Gartner. (2021). Magic Quadrant for Security Information and Event Management.

[14] Baset, S. A., & Bith, H. (2014). A Survey of SIEM Tools and Their Application in Detecting Attacks. International Conference on Cyber Security and Protection of Digital Services. https://www.google.com/search?q=https://doi.org/10.1109/CyberSecPODS.2014.6851979

[15] Wazuh. (2025). Architecture. Wazuh Documentation. Retrieved from https://documentation.wazuh.com/current/architecture/index.html

Дата надходження статті до редакції: 08.11.2025
Дата затвердження статті до друку: 27.11.2025
Опубліковано: 30.12.2025