ADAPTIVE CYBER INCIDENT RESPONSE METHOD FOR ENSURING DEPENDABILITY OF INFORMATION SYSTEMS IN SITUATION CENTERS

The paper develops an adaptive cyber incident response method aimed at ensuring the dependability of information systems used in situation centers under conditions of increasing cyber threats, growing complexity of information system architectures, and higher requirements for the continuity of critical services. The relevance of the study is determined by the need for timely detection of cyber incidents, assessment of their impact on the state of information systems, and automated generation of decisions to maintain the required level of dependability. The purpose of the research is to develop an adaptive cyber incident response method based on intelligent security event analysis, risk assessment, and dynamic selection of countermeasures. A review of current approaches to ensuring the dependability of information systems in situation centers, cyber incident response methods, and decision support technologies is conducted. A mathematical model for assessing the impact of cyber incidents on dependability indicators is proposed, and the adaptive response process is formalized. The developed method includes security event monitoring, incident classification, criticality assessment, threat evolution forecasting, and selection of an optimal response strategy. In addition, an architecture of an intelligent decision support system for ensuring the dependability of information systems in situation centers is proposed. Simulation results confirmed the effectiveness of the approach in increasing the level of dependability, reducing cyber incident response time, decreasing the risk of disruption of information resources, and improving system resilience to destructive impacts. The obtained results can be applied in the design, modernization, and operation of information systems in situation centers, as well as in the development of intelligent cybersecurity management tools and mechanisms for ensuring operational continuity.

Keywords: situation center, dependability, cyber incident, adaptive response, information system, intelligent system, decision support, mathematical model, risk management, cybersecurity.

Надійшла до редакції (Received): 25.08.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

УДК 004.056.53:004.89 DOI: 10.31673/2409-7292.2026.037206

Лозова Ірина Леонідівна
кандидат технічних наук, доцент кафедри Управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-7224-4763
E-mail: illozovaya@gmail.com

Скулиш Євген Деонізійович
доктор юридичних наук, професор, керівник наукового центру національної безпеки і права
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», Київ, Україна
ORCID: https://orcid.org/0000-0001-9646-8473
E-mail: us5519mail@gmail.com

ПІДХІД ДО АВТОМАТИЗАЦІЇ ПЕРВИННОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В SOC НА ОСНОВІ ІНТЕГРАЦІЇ SIEM ТА МЕХАНІЗМІВ АВТОМАТИЗОВАНОЇ ОБРОБКИ

У статті запропоновано підхід до автоматизації первинного реагування на кіберінциденти в центрі моніторингу безпеки (SOC) на основі інтеграції системи SIEM із програмним модулем автоматизованої обробки та зовнішніми джерелами даних. Запропонований підхід передбачає автоматизоване отримання та структурування інформації про інциденти з IBM QRadar через REST API, її збагачення результатами перевірки IP-адрес, характеристиками активів і даними про вразливості з Nessus Vulnerability Management. На основі сформованого контексту здійснюється визначення пріоритетності інцидентів, формування заявок, надсилання сповіщень аналітику та оновлення відповідної інформації в SIEM. Особливістю запропонованого підходу є автоматизація стандартизованих процедур первинного опрацювання без необхідності впровадження повноцінної SOAR-платформи, із збереженням контролю аналітика SOC над критичними діями реагування.

© Гречанінов В.Ф. Метод адаптивного реагування на кіберінциденти для забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Сучасний захист інформації, 3(67), 217–232.
https://doi.org/10.31673/2409-7292.2026.038701

Експериментальне дослідження на типових сценаріях кіберінцидентів продемонструвало скорочення часу їх первинного опрацювання та зменшення кількості операцій, що потребують безпосередньої участі аналітика. Отримані результати підтверджують доцільність використання запропонованого підходу як додаткового рівня автоматизації між SIEM та аналітиком SOC. Перспективними напрямами подальших досліджень є розширення переліку сценаріїв, інтеграція додаткових джерел кіберрозвідки та вдосконалення механізмів визначення пріоритетності кіберінцидентів.

Ключові слова: кіберінцидент, кібербезпека, SIEM, SOC, автоматизація.

Вступ та постановка проблеми

Стрімка цифровізація інформаційних систем і зростання обсягів обробки даних супроводжуються ускладненням кіберзагроз та збільшенням кількості кіберінцидентів. За таких умов своєчасне виявлення, аналіз і реагування на інциденти є важливою складовою забезпечення кібербезпеки організації [1]. Значну роль у цьому процесі відіграють центри моніторингу безпеки (Security Operations Center, SOC), які забезпечують централізований моніторинг подій, виявлення підозрілої активності та координацію реагування.

Одним із основних технологічних компонентів SOC є системи класу SIEM (Security Information and Event Management), призначені для централізованого збору, агрегації та аналізу подій безпеки, їх кореляції та виявлення потенційних інцидентів [2]. Водночас виявлення інциденту SIEM не охоплює всіх операцій первинного реагування. Після його формування аналітику необхідно додатково перевіряти індикатори компрометації, аналізувати пов’язані події, отримувати інформацію про активи та вразливості, збагачувати контекст інциденту і формувати результати для подальшого прийняття рішення.

За значної кількості одночасно оброблюваних інцидентів виконання таких операцій у ручному режимі збільшує навантаження на аналітиків SOC, час первинного опрацювання та класифікації інцидентів та ризик помилок. Відповідно, актуальним є підвищення рівня автоматизації процесів первинного опрацювання інцидентів шляхом інтеграції SIEM із зовнішніми джерелами даних та механізмами автоматизованої обробки. Автоматизація типових операцій дає змогу скоротити час збирання й аналізу контексту інциденту, залишаючи за аналітиком SOC прийняття остаточного рішення щодо подальших дій.

Таким чином, науково-практична проблема полягає у розробленні підходу до автоматизації первинного реагування на кіберінциденти, який забезпечує автоматичне отримання, структуризацію та збагачення інформації про інцидент на основі даних SIEM і зовнішніх джерел. Метою такого підходу є зменшення часових витрат на виконання рутинних операцій та підвищення оперативності роботи SOC без необхідності впровадження повноцінної SOAR-платформи.

Аналіз останніх досліджень і публікацій

Сучасні дослідження автоматизації процесів кібербезпеки зосереджені переважно на оркестрації дій, автоматизованому виконанні сценаріїв реагування та підтримці аналітика під час розслідування інцидентів. Одним із основних технологічних напрямів у цій сфері є використання платформ Security Orchestration, Automation and Response (SOAR), які забезпечують інтеграцію різних засобів кіберзахисту та виконання визначених послідовностей операцій відповідно до заданих сценаріїв. У роботі [3] запропоновано підхід до формування playbook-сценаріїв, за якого контекст сповіщення та поточний стан сценарію використовуються для визначення подальших дій аналітика. Автори зазначають, що традиційне створення та налаштування playbook потребує значних ручних зусиль, що може обмежувати масштабування автоматизації.

Практичну ефективність засобів автоматизації досліджено у роботі [4], де проведено експериментальне порівняння SOAR-рішень. Отримані результати свідчать про можливість скорочення кількості перемикань між різними джерелами інформації та підвищення ефективності виконання окремих операцій під час аналізу інцидентів. Водночас дослідження підкреслює важливість збереження участі аналітика у процесах, де автоматизовані дії можуть впливати на результати розслідування. Це підтверджує доцільність використання

© Лозова І.Л., Скулиш Є.Д. Підхід до автоматизації первинного реагування на кіберінциденти в SOC на основі інтеграції SIEM та механізмів автоматизованої обробки. Сучасний захист інформації, 3(67), 232–239. https://doi.org/10.31673/2409-7292.2026.037206

автоматизації насамперед для виконання стандартизованих операцій, результати яких можуть бути передані фахівцю для подальшого прийняття рішення.

Окрему групу досліджень становлять підходи до інтеграції SIEM із зовнішніми сервісами та засобами автоматизованої обробки. Зокрема, можливості інтеграції SIEM і SOAR реалізовані в IBM QRadar, де передбачено автоматизований обмін інформацією про виявлені інциденти, пов'язані події та артефакти. Використання програмних інтерфейсів API дає змогу отримувати дані про інциденти та передавати їх до зовнішніх компонентів для подальшої обробки [5, 6]. Такий підхід демонструє можливість побудови інтегрованого процесу обробки інцидентів без необхідності виконання кожної операції безпосередньо в інтерфейсі SIEM.

Ще одним напрямом є використання методів машинного навчання для класифікації подій та підтримки прийняття рішень. У дослідженні [7] запропоновано використання алгоритмів Random Forest і XGBoost для аналізу подій безпеки та зменшення кількості хибнопозитивних сповіщень SIEM. Для досліджуваного набору даних авторами отримано точність класифікації до 99,6%. Однак такі результати значною мірою залежать від характеристик набору даних і обраних ознак, тому застосування машинного навчання не усуває потреби в контекстному аналізі конкретного інциденту та перевірці отриманих результатів аналітиком.

Отже, проведений аналіз свідчить, що сучасні дослідження охоплюють автоматизацію сценаріїв реагування, інтеграцію SIEM із зовнішніми системами та використання методів машинного навчання. Водночас значна частина запропонованих рішень орієнтована на повноцінну оркестрацію процесів реагування або автоматичне прийняття окремих рішень. Менш дослідженим залишається підхід, за якого автоматизація обмежується первинним етапом опрацювання інциденту та виконує функцію підготовки контексту для аналітика на основі вже наявної SIEM-інфраструктури. Це формує напрям подальшого дослідження, спрямованого на визначення складу операцій первинного опрацювання, які доцільно автоматизувати, та експериментальне оцінювання отриманого ефекту.

Мета та завдання дослідження

Метою статті є розроблення та експериментальне дослідження підходу до автоматизації первинного реагування на кіберінциденти в SOC на основі інтеграції SIEM із механізмами автоматизованої обробки та збагачення даних.

Для досягнення поставленої мети визначено такі завдання: проаналізувати процес первинного опрацювання кіберінцидентів у SOC та визначити операції, доцільні для автоматизації; розробити архітектуру інтеграції SIEM із механізмами автоматизованої обробки інцидентів; розробити алгоритм автоматизованого отримання, аналізу та збагачення інформації про кіберінциденти; реалізувати механізми перевірки IP-адрес, аналізу результатів сканування вразливостей, створення записів про інциденти та формування сповіщень; експериментально оцінити ефективність запропонованого підходу за часовими та організаційними показниками первинного реагування.

Виклад основного матеріалу дослідження

Запропонований підхід до автоматизації первинного реагування на кіберінциденти базується на інтеграції SIEM-платформи IBM QRadar із програмним модулем автоматизованої обробки інцидентів та системою аналізу вразливостей Nessus Vulnerability Management. Основною ідеєю підходу є винесення повторюваних операцій первинного аналізу з ручного процесу опрацювання аналітиком у автоматизований workflow, у межах якого здійснюється отримання даних про інцидент, їх збагачення, визначення пріоритетності, формування службової інформації та інформування відповідального фахівця. Така організація процесу дає змогу скоротити кількість ручних операцій без повної передачі процесу прийняття рішень автоматизованій системі.

Архітектурно рішення складається з джерел подій безпеки, SIEM-платформи IBM QRadar, модуля автоматизованої підтримки реагування, системи Nessus Vulnerability Management, механізму створення заявок про інциденти та засобів взаємодії з аналітиком SOC.

Події надходять до QRadar із серверів, мережевого обладнання, міжмережевих екранів, кінцевих пристроїв та інших засобів захисту інформації. Після нормалізації та кореляції подій QRadar формує інцидент типу offense, який містить відомості про характер підозрілої активності, джерело події, задіяні активи та базовий рівень серйозності.

Для автоматизованої передачі сформованого інциденту до модуля підтримки реагування використовується програмний інтерфейс REST API IBM QRadar. Така взаємодія забезпечує програмне отримання активних інцидентів, їх параметрів та пов'язаних подій без необхідності ручного перенесення інформації між компонентами системи. У результаті модуль функціонує як додатковий рівень автоматизації поверх наявної SIEM-інфраструктури.

Після отримання інформації про інцидент виконується збагачення даних, призначене для розширення початкового контексту. Воно включає перевірку IP-адрес, аналіз репутації мережевих індикаторів, перевірку активів на наявність відомих вразливостей та визначення критичності активу. Для отримання відомостей про вразливості використовується Nessus Vulnerability Management, результати сканування якого дають змогу визначати критичні або високоризикові вразливості CVE, пов'язані з активами, залученими до інциденту [8].

На основі отриманого контексту виконується автоматизована пріоритезація інциденту. Для цього враховуються значення severity у QRadar, наявність критичних CVE, тип і критичність активу, характер мережевої активності та результати перевірки IP-адрес. Виявлення критичних вразливостей може бути підставою для підвищення пріоритету інциденту, оскільки наявність відомої вразливості на активі потенційно збільшує наслідки реалізації загрози. Принциповою особливістю запропонованої архітектури є реалізація функцій автоматизації та оркестрації без обов'язкового розгортання окремої повноцінної SOAR-платформи. Відповідні функції реалізуються в окремому модулі, який взаємодіє з QRadar та іншими компонентами через програмні інтерфейси. Це дозволяє використовувати наявну SIEM-інфраструктуру як основу для поступового впровадження автоматизованих процедур реагування.

Процес автоматизованого опрацювання інциденту представлено як послідовність взаємопов'язаних етапів: отримання та аналіз даних про інцидент, збагачення даних, визначення пріоритетності, виконання визначених автоматизованих процедур, створення заявки про інцидент та інформування аналітика SOC (рис. 1).

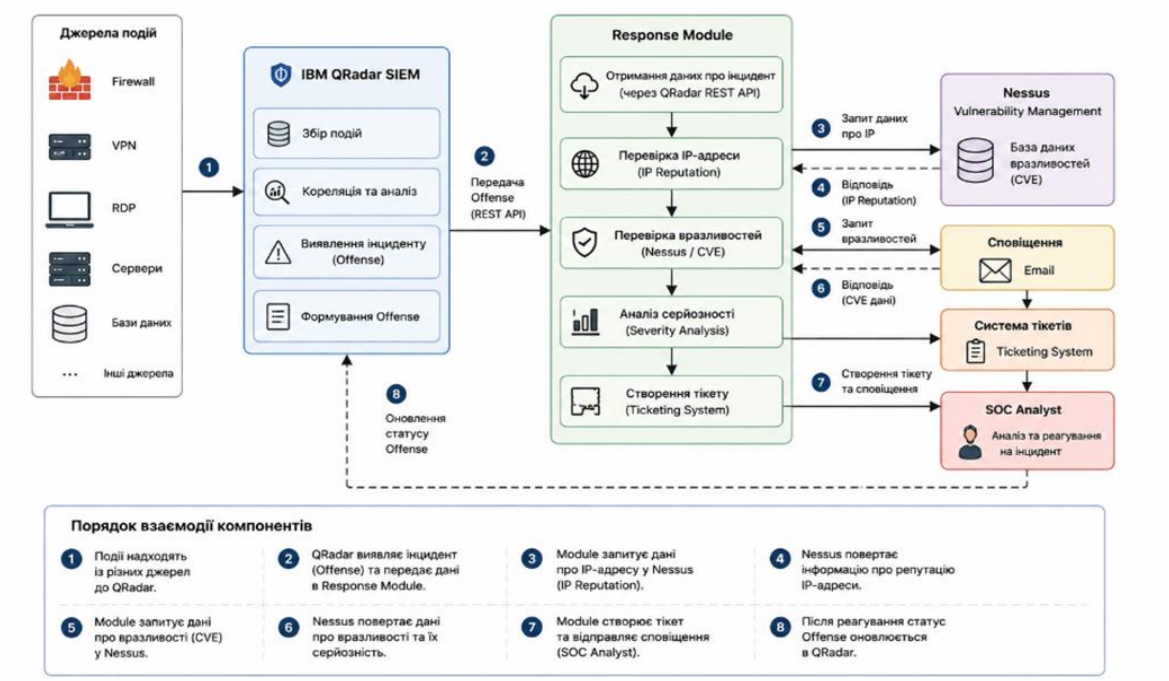

Рис. 1. Архітектура запропонованого підходу

© Лозова І.Л., Скулиш Є.Д. Підхід до автоматизації первинного реагування на кіберінциденти в SOC на основі інтеграції SIEM та механізмів автоматизованої обробки. Сучасний захист інформації, 3(67), 232–239. https://doi.org/10.31673/2409-7292.2026.037206

На початковому етапі QRadar здійснює збір і кореляцію подій та формує інцидент. Модуль автоматизованої обробки отримує відповідні дані через REST API та виконує перевірку категорії інциденту, типу мережевої активності, джерела події, значення severity та переліку задіяних активів. На основі цих даних визначається можливість подальшої автоматизованої обробки.

На наступному етапі здійснюється збагачення інформації про інцидент. Автоматично перевіряється репутація IP-адрес, аналізуються характеристики активів, опрацьовуються результати сканування Nessus та визначаються критичні CVE. Якщо актив, пов'язаний із підозрілою активністю, містить критичні або високоризикові вразливості, ця інформація враховується під час визначення пріоритетності реагування.

Для управління подальшою обробкою використовується триступенева градація пріоритетів: низький, середній та високий. Інциденти низького пріоритету можуть залишатися на етапі моніторингу або додаткової перевірки, інциденти середнього пріоритету передаються аналітику для детального аналізу, а для високопріоритетних інцидентів виконуються визначені автоматизовані процедури та формується відповідна заявка.

Після завершення автоматизованої обробки формується структурований результат, що містить ідентифікатор інциденту, його опис, встановлений рівень критичності, результати збагачення інформації та рекомендації щодо подальших дій. Ці відомості використовуються для створення заявки про інцидент та електронного сповіщення аналітика SOC. Результати проведених операцій також записуються безпосередньо до відповідного інциденту в QRadar у вигляді примітки. Це забезпечує централізоване зберігання результатів первинного аналізу.

Практична реалізація запропонованого підходу здійснюється на основі сценаріїв автоматизованої обробки (playbooks). Вони визначають послідовність операцій, які необхідно виконати після надходження певного типу інциденту до модуля. Розроблені сценарії орієнтовані на типові події інформаційної безпеки, зокрема підозрілу мережеву активність, спроби несанкціонованого доступу, аномальну поведінку користувачів, спрацювання правил кореляції SIEM та виявлення потенційно скомпрометованих активів (рис. 2).

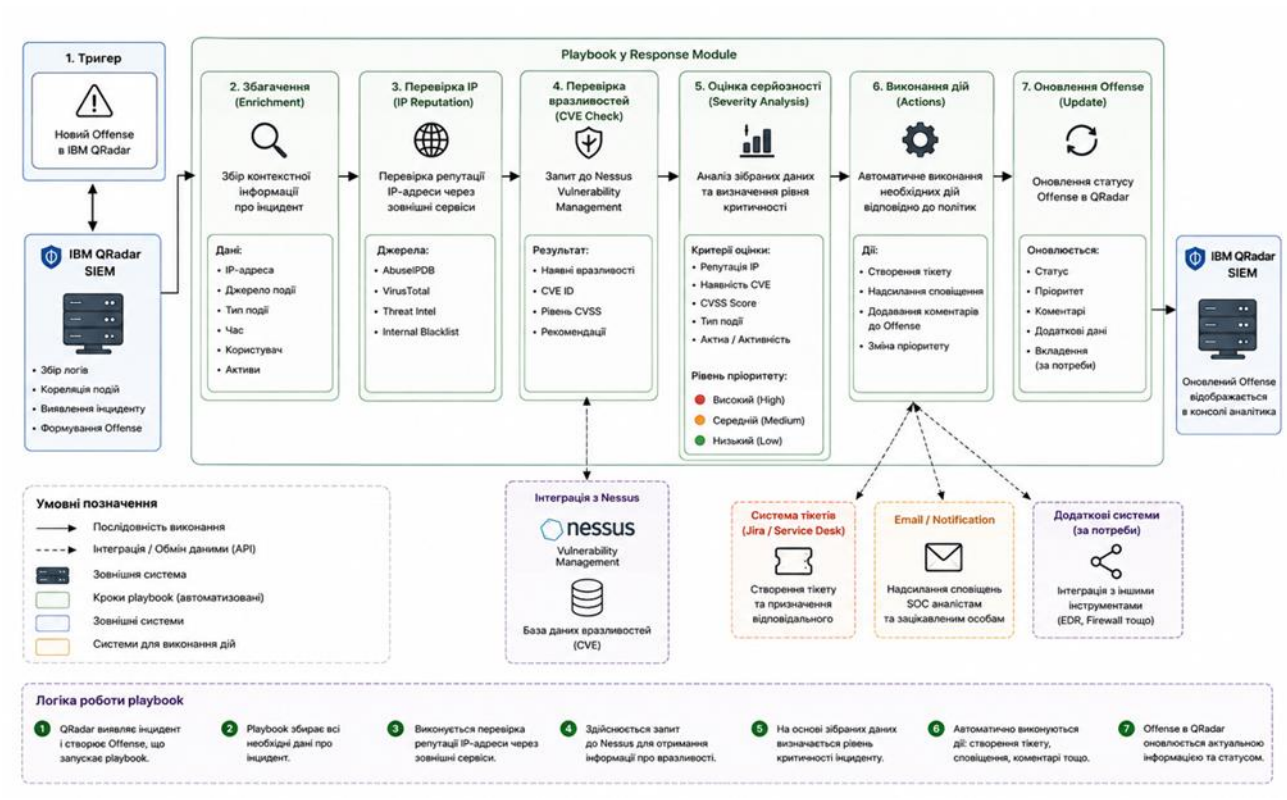

Рис. 2. Логіка сценаріїв автоматизованої обробки

У загальному випадку playbook передбачає отримання інциденту з QRadar, перевірку його параметрів, збагачення інформації, визначення пріоритетності, створення заявки, надсилання сповіщення аналітику та оновлення інформації в QRadar. Дані, що надходять через програмний інтерфейс, містять ідентифікатор інциденту, опис, значення severity, IP-адреси джерела та призначення, категорію, перелік задіяних активів і параметри правила кореляції.

Важливою особливістю реалізованих сценаріїв є обмеження автоматизації на етапі первинного аналізу. Модуль не виконує безпосереднього блокування облікових записів або ізоляції хостів без підтвердження аналітика SOC. Автоматизованими залишаються операції збагачення інформації, створення заявок, надсилання повідомлень та оновлення інформації про інцидент. Такий принцип реалізації дає змогу знизити ризик небажаних автоматичних дій і водночас скоротити обсяг рутинної роботи аналітика.

Програмний модуль реалізовано як окремий компонент SOC, інтегрований із IBM QRadar через REST API. Його функціональна структура включає модуль отримання інцидентів, модуль модуль збагачення даних, модуль аналізу вразливостей, модуль пріоритезації, модуль створення заявок та модуль сповіщень. Такий поділ забезпечує модульність програмного рішення і створює можливість подальшого розширення його функціональності.

Послідовність реалізації починається з отримання переліку активних інцидентів через REST API QRadar. Для кожного запису виділяються основні параметри: ідентифікатор інциденту, опис, значення severity, IP-адреси джерела та призначення, категорія та задіяні активи. Після перевірки відповідності встановленим умовам модуль переходить до до етапу збагачення даних.

В процесі збагачення здійснюється перевірка IP-адрес, аналіз інформації про активи, опрацювання результатів сканування вразливостей та визначення критичності активу. Взаємодія з Nessus Vulnerability Management дає змогу встановити наявність критичних або високоризикових CVE, після чого відповідна інформація враховується під час визначення пріоритету інциденту.

Завершальним етапом є формування заявки про інцидент, надсилання email-сповіщення та оновлення відповідного запису в QRadar. У заявці зберігаються ідентифікатор інциденту, його опис, результати збагачення, перелік CVE, рівень серйозності та рекомендації щодо подальшого опрацювання. Одночасно результати аналізу записуються до QRadar, що дає змогу зберігати контекст проведених операцій безпосередньо в SIEM-системі.

Модуль реалізовано за принципом, що забезпечує можливість додавання нових playbook-сценаріїв, інтеграції додаткових джерел Threat Intelligence, зміни логіки обробки інцидентів та розширення набору автоматизованих дій реагування. Отже, запропоноване рішення може розглядатися не лише як засіб автоматизації окремих операцій, а і як базовий рівень для подальшого розвитку більш складної системи оркестрації та автоматизованого реагування. Для оцінювання ефективності запропонованого підходу проведено порівняння традиційного ручного та автоматизованого опрацювання трьох типових кіберінцидентів у SOC: підозрілої активності входу, brute force активності та несанкціонованої ескалації привілеїв. Основними критеріями оцінювання визначено час первинного опрацювання та класифікації інциденту, кількість ручних операцій, швидкість формування заявки та час інформування аналітика SOC. Експериментальне порівняння проводилося за однакових умов для ручного та автоматизованого способів опрацювання. Для кожного сценарію фіксувався час від моменту надходження інциденту до завершення первинного опрацювання та формування результату для аналітика SOC. Додатково враховувалася кількість операцій, які потребували безпосередньої участі аналітика.

Результати експерименту засвідчили суттєве скорочення часу первинного опрацювання для всіх досліджуваних сценаріїв. Для підозрілої активності входу час зменшився з 12 до 1,5 хв, для brute force активності – з 16 до 1,92 хв, а для несанкціонованої ескалації привілеїв – з 20 до 2,25 хв. Отже, відносне скорочення часу становило відповідно 87,5 %, 88,0 % та 88,75 %,

© Лозова І.Л., Скулиш Є.Д. Підхід до автоматизації первинного реагування на кіберінциденти в SOC на основі інтеграції SIEM та механізмів автоматизованої обробки. Сучасний захист інформації, 3(67), 232–239. https://doi.org/10.31673/2409-7292.2026.037206

а середнє значення – близько 88,1 %. Найбільший ефект спостерігався під час виконання операцій перевірки IP-адрес, аналізу активів і вразливостей, створення заявки та інформування аналітика.

Додатково встановлено зменшення кількості ручних операцій під час опрацювання інциденту: з 6–8 операцій у традиційному процесі до 2–3 при використанні запропонованого модуля. Автоматизовано формування заявки, надсилання сповіщень, доповнення контексту інциденту та оновлення інформації в QRadar. Особливо суттєвим є ефект використання даних Nessus Vulnerability Management, оскільки автоматичне виявлення критичних CVE дає змогу оперативніше визначати пріоритетність інциденту.

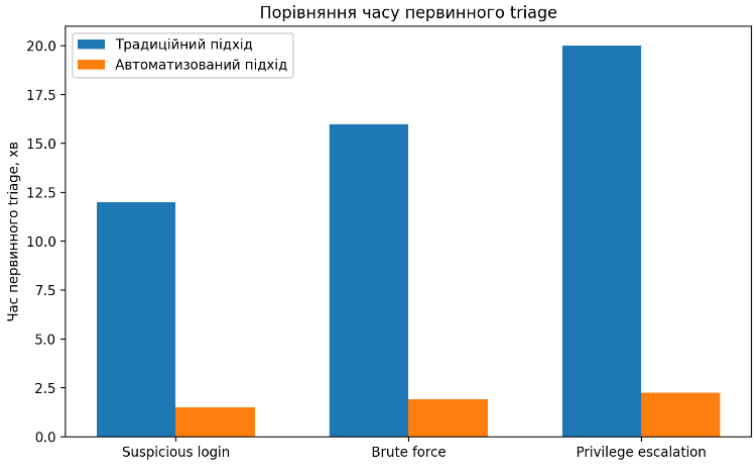

Рис. 3. Порівняння часу первинного опрацювання кіберінцидентів за досліджуваними сценаріями

Експериментальні результати свідчать про доцільність використання запропонованого підходу як додаткового рівня автоматизації між SIEM та аналітиком SOC. Його застосування дає змогу скоротити час первинного опрацювання та класифікації інцидентів, зменшити кількість ручних операцій і стандартизувати виконання типових процедур. При цьому остаточне рішення щодо критичних дій реагування залишається за аналітиком SOC, що забезпечує поєднання автоматизованої обробки з контролем фахівця.

Висновки та перспективи подальших досліджень

У роботі запропоновано підхід до автоматизації первинного реагування на кіберінциденти в SOC на основі інтеграції SIEM із програмним модулем автоматизованої обробки та зовнішніми джерелами даних. Підхід передбачає автоматизацію отримання й структурування інформації про інцидент, збагачення контексту, аналізу вразливостей, визначення пріоритетності, формування заявки та інформування аналітика. Експериментальне дослідження трьох типових сценаріїв показало скорочення часу первинного опрацювання на 87,5–88,75 %, а кількість ручних операцій зменшилася з 6–8 до 2–3. Отримані результати свідчать про доцільність використання запропонованого підходу як додаткового рівня автоматизації між SIEM та аналітиком SOC без обов'язкового впровадження повноцінної SOAR-платформи. Перспективи подальших досліджень полягають у розширенні набору сценаріїв автоматизованої обробки, інтеграції додаткових джерел кіберрозвідки та вдосконаленні алгоритмів визначення пріоритетності з урахуванням критичності активів і контексту загрози. Доцільним також є проведення масштабніших експериментів за різної інтенсивності надходження інцидентів та дослідження можливості часткової автоматизації окремих дій реагування із збереженням контролю та остаточного рішення за аналітиком SOC.

Перелік посилань

1. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile: NIST SP 800-61 Rev. 3 [Електронний ресурс]. Gaithersburg: National Institute of Standards and Technology, 2025. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final.

© Лозова І.Л., Скулиш Є.Д. Підхід до автоматизації первинного реагування на кіберінциденти в SOC на основі інтеграції SIEM та механізмів автоматизованої обробки. Сучасний захист інформації, 3(67), 232–239. https://doi.org/10.31673/2409-7292.2026.037206

2. Kent K., Souppaya M. Guide to Computer Security Log Management: NIST SP 800-92 [Електронний ресурс]. Gaithersburg: National Institute of Standards and Technology, 2006. URL: https://csrc.nist.gov/pubs/sp/800/92/final.

3. Kremer R., Wudali P. N., Momiyama S., Araki T., Furukawa J., Elovici Y., Shabtai A. IC-SECURE: Intelligent System for Assisting Security Experts in Generating Playbooks for Automated Incident Response [Електронний ресурс]. arXiv, 2023. DOI: 10.48550/arXiv.2311.03825.

4. Bridges R. A., Rice A. E., Oesch T. S., Nichols J. A., Watson C. L., Spakes K. D., Norem S. A., Huettel M. R., Jewell B. C., Weber B., Gannon C. M., Bizovi O. M., Hollifield S. C., Erwin S. H. Testing SOAR tools in use. Computers & Security. 2023. Vol. 129. Article 103201. DOI: 10.1016/j.cose.2023.103201.

5. IBM. Ingesting QRadar offense alerts by creating an ingestion data source [Електронний ресурс]: IBM Documentation. URL: https://www.ibm.com/docs/en/security-qradar/security-qradar-siem/saas?topic=suqof-ingesting-qradar-offense-alerts-by-creating-ingestion-data-source.

6. IBM. QRadar SOAR Integration Guide [Електронний ресурс]: IBM Security QRadar SOAR Documentation. URL: https://www.ibm.com/docs/en/sqsp/51.0.0?topic=platform-soar-documentation-communities.

7. Ali G., Shah S., Elaffendi M. Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection. Results in Engineering. 2025. Vol. 25. Article 104078. DOI: 10.1016/j.rineng.2025.104078.

8. Johnson C. S., Badger M. L., Waltermire D. A., Snyder J., Skorupka C. Guide to Cyber Threat Information Sharing: NIST SP 800-150 [Електронний ресурс]. Gaithersburg: National Institute of Standards and Technology, 2016. DOI: 10.6028/NIST.SP.800-150. URL: https://csrc.nist.gov/pubs/sp/800/150/final.

Iryna Lozova
Candidate of Technical Sciences, Associate Professor, Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-7224-4763
E-mail: illozovaya@gmail.com

Yevhenii Skulysh
Doctor of Law, Professor, Head of the Research Centre for National Security and Law
State Research Institution Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-9646-8473
E-mail: us5519mail@gmail.com

AN APPROACH TO AUTOMATING INITIAL RESPONSE TO CYBER INCIDENTS IN SOC BASED ON THE INTEGRATION OF SIEM AND AUTOMATED PROCESSING MECHANISMS

The paper proposes an approach to automating the initial response to cyber incidents in a SOC based on the integration of a SIEM system with an automated processing module and external data sources. The proposed approach involves the automated retrieval and structuring of incident information from IBM QRadar via the REST API, followed by data enrichment using IP address verification results, asset characteristics, and vulnerability data obtained from Nessus Vulnerability Management. Based on the resulting context, incident prioritization, ticket creation, analyst notification, and updating of the relevant information in the SIEM system are performed. A distinctive feature of the proposed approach is the automation of standardized initial incident processing procedures without requiring the deployment of a full-scale SOAR platform, while maintaining SOC analyst control over critical response actions. Experimental evaluation using typical cyber incident scenarios demonstrated a reduction in the time required for initial incident processing and a decrease in the number of operations requiring direct analyst involvement. The results indicate the feasibility of using the proposed approach as an additional automation layer between the SIEM system and SOC analysts. Future research will focus on expanding the range of incident scenarios, integrating additional cyber threat intelligence sources, and improving mechanisms for cyber incident prioritization.

Keywords: cyber incident, cybersecurity, SIEM, SOC, automation.

Надійшла до редакції (Received): 29.08.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

© Лозова І.Л., Скулиш Є.Д. Підхід до автоматизації первинного реагування на кіберінциденти в SOC на основі інтеграції SIEM та механізмів автоматизованої обробки. Сучасний захист інформації, 3(67), 232–239. https://doi.org/10.31673/2409-7292.2026.037206