КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.19.176196
УДК 004.056.5

Гнатюк Сергій Олександрович
д.т.н., проф., декан факультету комп'ютерних наук та технологій
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua

Бердибаєв Рат Шиндалійович
PhD, керівник науково-технічного центру проблем інформаційної безпеки імені Турганбека Омара
Алматинський університет енергетики та зв'язку, Алмати, Казахстан
ORCID ID: 0000-0002-8341-9645
r.berdybaev@aues.kz

Сидоренко Вікторія Миколаївна
к.т.н., доц., доцент кафедри безпеки інформаційних технологій
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Жигаревич Оксана Костянтинівна
старший викладач кафедри комп'ютерних наук та кібербезпеки
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID ID: 0000-0002-7154-9733
zhyharevych.oksana@vnu.edu.ua

Смірнова Тетяна Віталіївна
к.т.н., доцент, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0001-5093-1581
sm.tetyana@gmail.com

СИСТЕМА КОРЕЛЮВАННЯ ПОДІЙ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Сучасна інформаційна інфраструктура складається з великої кількості систем та компонентів, що потребують постійного моніторингу та контролю. Для виявлення аналізу та усунення можливих кіберзагроз рекомендовано використовувати єдине спільне рішення – так звані SIEM-системи. SIEM збирає дані журналів подій, визначає нетипові дії за допомогою аналізу в реальному часі, визначає загрози, генерує сповіщення та пропонує вжити відповідні сценарії заходів. Сьогодні кількість та якість SIEM систем значно виросла, а для забезпечення швидкого та ефективного виявлення загроз використовуються новітні технології штучного інтелекту, інтернету речей та хмарних технологій. Таким чином, в роботі проведено дослідження сучасних SIEM систем, їхньої функціональності, основних принципів роботи, а також представлено порівняльний аналіз їх можливостей та відмінностей, переваг та недоліків використання. Крім того, розроблена та експериментально досліджена універсальна система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури. Розроблено моделі функціонування гібридного сховища даних безпеки, які дозволяють сервісу індексації отримувати доступ до зовнішніх сховищ даних, провести масштабування при зростанні обсягу даних, забезпечити високу швидкість пошуку тощо. Розроблено моделі, методики та алгоритми функціонування розподіленої шини даних, які дозволяють забезпечити високу швидкість обробки великих потоків інформації, мінімальні затримки на обробку даних, високу стійкість до відмов, гнучкість і розширюваність сховища. Запропонована система призначена для вирішення низки актуальних задач кібербезпеки та відповідає основним вимогам міжнародних стандартів та найкращих світових практик щодо створення систем управління кіберінциденти.

Ключові слова: SIEM-система, кіберзагроза, кібербезпека, інцидент кібербезпеки, критична інфраструктура, об'єкти критичної інфраструктури, система корелювання подій та управління інцидентами кібербезпеки.

ВСТУП

Сьогодні управління інформацією та подіями інформаційної безпеки (SIEM, Security Information and Events Management) є важливим напрямком, що бурхливо розвивається та має велику ефективність для виявлення загроз і розробки контрзаходів щодо забезпечення необхідного рівня захисту інформаційної інфраструктури.

Функціонування SIEM-системи полягає в оперативному збиранні, збереженні та аналітичній обробці даних про події безпеки, які першочергово формуються та фіксуються в системних журналах різних апаратних і програмних елементів, а також формують інформаційні інфраструктури: сервери, робочі станції, маршрутизатори, мережеві екрани, системи управління базами даних, системи виявлення атак, антивірусні засоби тощо [1-2]. Основною метою побудови та функціонування SIEM-систем є значне підвищення рівня інформаційної безпеки (ІБ) в інформаційно-телекомунікаційній інфраструктурі за рахунок забезпечення можливості в режимі, близькому до реального часу, маніпулювати інформацією про безпеку та здійснювати проактивне управління інцидентами та подіями безпеки. «Проактивне» означає «діюче до того, як ситуація стане критичною». Передбачається, що проактивне управління інцидентами та подіями безпеки ґрунтується на автоматичних механізмах, які використовують інформацію про «історію» аналізованих мережевих подій та прогноз майбутніх подій, а також на автоматичному налаштовуванні параметрів моніторингу подій до поточного стану системи, що захищається. Для досягнення цієї мети SIEM-система для критичних інфраструктур (КІ) повинна успішного вирішувати такі завдання:

- збирання, обробки та аналізу подій безпеки, що надходять у систему з безлічі гетерогенних джерел;
- виявлення, в режимі реального часу, атак та порушень політик безпеки;
- оперативної оцінки захищеності інформаційних, телекомунікаційних та інших критично важливих ресурсів (КВР);
- аналізу та управління ризиками безпеки КІ;
- проведення розслідувань інцидентів;
- виявлення розбіжностей КВР та бізнес-процесів з внутрішніми політиками безпеки та приведення їх у відповідність один з одним;
- прийняття ефективних рішень щодо захисту інформації;
- формування звітних документів.

Основними вихідними даними, які використовуються SIEM-системою для вирішення зазначених завдань, є записи різних журналів (logs), що протоколюють події для КІ, які називають «подіями безпеки». Ці події відображають такі дії користувачів та програм, які можуть вплинути на безпеку. Із загальної множини подій безпеки SIEM-система повинна знаходити такі, які свідчать про атаки або інші небажані дії для КІ, причому традиційні методи пошуку подібної інформації є досить трудомісткими.

Постановка проблеми. Як правило, SIEM-система має архітектуру «агенти» – «сховище даних» – «сервер додатків», яка розгортається поверх інформаційної інфраструктури, що захищається. Агенти виконують збір подій безпеки, їхню початкову обробку та фільтрацію. Зібрана та відфільтрована інформація про події безпеки надходить до сховища даних або репозиторій, де вона зберігається у внутрішньому

форматі з метою подальшого використання та аналізу сервером додатків. Сервер додатків реалізує основні функції захисту інформації. Він аналізує інформацію, яка зберігається в репозиторії, і перетворює її для розробки попереджень чи управлінських рішень щодо захисту інформації. Таким чином, у SIEM-системі можна виділити такі три архітектурні рівні її побудови, як збирання даних, управління даними та аналіз даних.

На першому рівні *збирання даних* здійснюється від джерел різних типів. До них належать: файлові сервери, сервери баз даних, Windows-сервери, мережеві екрани (MCE), робочі станції, системи протидії атакам (IPS, Intrusion Prevention Systems), антивірусні програми тощо.

На другому рівні здійснюється *управління даними* про події безпеки, які зберігаються у репозиторії. Дані, які містяться у репозиторії, видаються за запитами моделей *аналізу даних*.

Результатами обробки інформації в SIEM-системі, одержуваними на третьому рівні, є звіти в визначеній та довільній формі, оперативна (online) кореляція даних про події, а також попередження, що розробляються в режимі online та (або) передаються електронною поштою.

Функціонування системи SIEM. SIEM-система поєднує у собі функції двох різноманітних класів, що належать до систем моніторингу та управління безпекою інформації – SIM (Security Information Management) та SEM (Security Event Management). До групи функцій SIM-системи належать збирання, зберігання та аналіз записів журналів, а також формування необхідної звітності. До групи функцій SEM-систем належить моніторинг подій безпеки в реальному часі, а також виявлення та реагування на інциденти безпеки. Реалізація зазначених вище функцій у SIEM-системі складає основу виконання комплексу різних механізмів функціонування. У SIEM-системах до таких механізмів, як правило, відносяться нормалізація, фільтрація, класифікація, агрегація, кореляція та пріоритезація подій, а також генерація звітів та попереджень. У SIEM-системах нового покоління до них слід додати також аналіз подій, інцидентів та їх наслідків, а також прийняття рішень та візуалізація [3]. Розглянемо їх більш детально:

- *нормалізація* означає приведення форматів записів журналів, зібраних із різних джерел, до єдиного внутрішнього формату, який потім буде використовуватись для їх зберігання та подальшої обробки;
- *фільтрація подій безпеки* полягає у видаленні надлишкових подій з потоків, що надходять в систему;
- *класифікація* дозволяє атрибутам подій безпеки визначити їхню належність до певного класу;
- *агрегація* поєднує події, схожі за певними ознаками;
- *кореляція* виявляє взаємозв'язки між різнорідними подіями, що дозволяє виявляти атаки на КІ, а також порушення критеріїв та політик безпеки;
- *пріоритезація* визначає значимість та критичність подій безпеки на підставі правил, визначених у системі;
- *аналіз подій, інцидентів та їх наслідків* включає процедури моделювання подій, атак та їх наслідків, аналізу уразливостей та захищеності системи, визначення параметрів порушників, оцінки ризику, прогнозування подій та інцидентів;
- *генерація звітів та попереджень* означає формування, передачу, відображення та (або) друк результатів функціонування;
- *прийняття рішень* визначає вироблення заходів щодо реконфігурування засобів захисту з метою запобігання атакам або відновлення безпеки інфраструктури;

- *візуалізація* передбачає подання у графічному вигляді даних, що характеризують результати аналізу подій безпеки та стан КІ, та її елементів.

Взаємозв'язок механізмів функціонування SIEM-системи нового покоління наочно демонструє функціональна модель, де виділено п'ять основних функціональних підсистем: збору даних; обробки; зберігання; аналізу; представлення.

Причому перші дві функціонують у режимі online, решта – у близькому до нього. Розглянемо коротку характеристику цих підсистем:

1) Підсистема збирання даних. Для отримання інформації від джерел використовуються два основні методи: Push та Pull. Суть методу Push полягає в тому, що джерело саме надсилає дані записів своїх журналів у SIEM-систему. У методі Pull система сама здійснює процес отримання даних із журналів. Збір даних здійснюється від джерел різних типів.

2) Підсистема опрацювання. Обробка інформації включає нормалізацію, фільтрацію, кореляцію, агрегацію і класифікацію.

3) Підсистема зберігання. Відфільтровані дані в нормалізованому вигляді розміщуються для зберігання у репозиторій. Репозиторій може бути створений на основі реляційної СУБД (найбільш поширене рішення), XML-орієнтованої СУБД та / або сховища триплетів. Сховище триплетів – спеціально створена база даних, оптимізована для зберігання та пошуку триплетів, тобто тверджень типу «суб'єкт – предикат – об'єкт».

4) Підсистема аналізу. Аналіз даних включає наступні функції: кореляцію даних, класифікацію, агрегацію, пріоритезацію та аналіз подій, інцидентів та їх наслідків, а також підтримку ухвалення рішень. Аналіз даних може ґрунтуватися на якісних та кількісних оцінках. Кількісна оцінка є точнішою, але потребує помітно більшого часу, що не завжди допустимо. Найчастіше буває досить швидкого якісного аналізу, завдання якого полягає у розподілі факторів ризику за групами. Шкала якісного аналізу може відрізнятися в різних методах оцінки, але все зводиться до того, щоб виявити найсерйозніші загрози.

5) Підсистема представлення. Представлення включає кілька функцій: візуалізацію, генерацію звітів і генерацію попереджень

Зазначені твердження свідчать про наявність важливого наукового завдання щодо аналізу існуючих SIEM-систем та розробки універсальної системи корелювання подіями та управління інцидентами кібербезпеки на об’єктах КІ.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Для сертифікації всі SIEM-системи повинні відповідати міжнародній групі стандартів з ІБ: ISO/IEC 27000 PCI-DSS, HIPAA, NIST 800-171, DoD, RMF, GDPR. Для вирішення завдань пов'язаних з безпекою та фіксацію подій SIEM-системи у [4-5] були розглянуті основні характеристики функціонування існуючих SIEM-систем та проведено їх порівняльний аналіз. Розглянемо деякі з них більш детально.

1. IBM QRadar Security Intelligence Platform [6] складається з низки інтегрованих систем збору подій, моніторингу, аналізу захищеності та розслідування інцидентів: 1) Log Manager; 2) SIEM; 3) Flow Processor; 4) Vulnerability Manager; 5) Risk Manager; Network Insights; 6) Watson Advisor for Cyber Security; 7) Packet Capture and Incidents Forensics.

QRadar дозволяє збирати та обробляти дані про події ІБ з журналів аудиту безпеки, аналізувати мережеву статистику (NetFlow та ін.), здійснювати самостійний аналіз мережного трафіку та інформації, що передається, будувати топологію мережі та емулювати зміни в конфігураційних файлах мережного обладнання, виявляти

уразливості та небезпечні систем, повністю захоплювати трафік та відтворювати ланцюжок комунікацій між вузлами мережі. Переваги IBM QRadar:

- єдина платформа для планомірного створення SOC: збирання та аналіз подій ІБ, виявлення аномальної мережевої активності, сканування уразливостей та виявлення небезпечних конфігурацій, інтеграція зі штучним інтелектом IBM Watson, мережевою форензикою та перехід до процесів реагування на інциденти в IBM Resilient;
- гнучка архітектура QRadar Platform, що дозволяє перевизначати ролі та функції модулів платформи та не обмежує клієнтів жорсткими рамками обраної схеми;
- велика кількість безкоштовних програм, контенту та інтеграційних модулів.

2. LogRhythm [7] – платформа, що пропонує інтелектуальне безпекове рішення, яке використовує для аналізу журналів і трафіку в операційних системах Windows і Linux штучний інтелект. Переваги системи:

- володіє сховищем даних, що розширюється;
- підходить для систем, де відсутні структуровані дані, централізація чи автоматизація;
- підходить для малих та середніх організацій;
- дозволяє відсіювати марну інформацію або інші журнали та звузити аналіз до мережного рівня;
- сумісний із широким спектром журналів та пристроїв, а також для розширення можливостей реагування на загрози та інциденти легко інтегрується з Varonis.

3. Splunk інструмент, який використовує можливості штучного інтелекту та машинного навчання для надання практичних, ефективних та прогнозуючих відомостей. Splunk [7-8] підходить для всіх типів організацій для локального розгортання, так і для розгортання у вигляді SaaS. Ключові переваги:

- швидке виявлення загрози;
- визначення та оцінка ризиків;
- керування оповіщеннями;
- упорядкування подій;
- швидке та ефективне реагування;
- працює з даними як у локальному середовищі, так і в хмарній інфраструктурі.

4. McAfee Enterprise Security Manager (ESM) [7] постачається в якості фізичного та віртуального пристрою та програмного забезпечення. До його основного складу входять такі три компоненти – ESM, Event Receiver та Enterprise Log Manager, які можуть бути розгорнуті разом як одна система або окремо для розподілених чи великомасштабних середовищ. Переваги McAfee ESM:

- ESM має гарне охоплення промислових систем управління (ICS) і пристроїв диспетчерського управління та збору даних (SCADA);
- McAfee Data Exchange Layer (DXL) від Intel Security забезпечує інтеграцію зі сторонніми технологіями без використання API. Цей підхід дає можливість використовувати ESM як платформу SIEM;
- McAfee Global Threat Intelligence дозволяє розширити можливості SIEM-системи Enterprise Security Manager, додавши джерело безперервно оновлюваної інформації про загрози, що дає можливість швидко виявляти події, що включають сеанси зв'язку з підозрілими або шкідливими IP-адресами.

5. AlientVault USM – багатофункціональна платформа управління ІБ, яка централізує та спрощує виявлення загроз, реагування на інциденти та управління дотриманням стандартів у хмарних та локальних середовищах. Ключові можливості [9]:

- видобувати та аналізувати дані безпеки сторонніх додатків;
- візуалізувати зовнішні дані в графічних інформаційних панелях USM Anywhere з багатьма функціями;
- керувати діями сторонніх рішень безпеки на основі даних про загрози, проаналізовані в USM Anywhere;
- використовувати прогресивні функції безпеки при додаванні нових модулів AlienApps до USM Anywhere.

6. FortiSIEM – комплексний, масштабований інструментальний засіб управління безпекою, продуктивністю та забезпеченням відповідності вимогам усіх компонентів інфраструктури, здатний працювати як з хмарами, так і з Інтернетом речей (IoT) [10-12]. Рішення [7] спрямоване на зниження складності виявлення загроз при підвищенні ефективності системи безпеки та можливості обмінюватися з продуктом інформацією, у тому числі і про виявлені уразливості. Основні переваги FortiSIEM:

- масштабований та гнучкий збір журналів;
- повідомлення та управління інцидентами;
- надання користувачеві налаштовуваних функціональних панелей моніторингу;
- інтеграція зовнішніх даних про загрози;
- надання масштабованої функції аналізу;
- завдання базових показників та виявлення статистичних аномалій поведінки кінцевої точки/сервера/користувача;
- інтеграція зовнішніх технологій.

7. Ixia ThreatARMOR забезпечує виконання таких можливостей:

- забезпечення повної пропускної спроможності;
- усунення загроз шляхом блокування всього трафіку з відомих шкідливих сайтів та недовірених країн;
- виключення можливості помилкових спрацьовувань – наочне підтвердження шкідливих дій для всіх заблокованих сайтів;
- покращення ефективності за рахунок зменшення кількості попереджень безпеки;
- оновлення даних про загрози кожні 5 хвилин за допомогою хмарної підписки на оновлення (ATI);
- швидке визначення скомпрометованих внутрішніх систем;
- блокування з'єднання із захопленими IP-адресами;
- подвійне резервування живлення та вбудована можливість режиму by pass для максимальної надійності;
- просте 30-хвилинне налаштування без необхідності подальших коригувань, а також централізоване керування з хмари;
- підвищує рентабельність інвестицій та продуктивність інфраструктури мережевої безпеки.

8. MozDef Mozilla SIEM-система [8, 13], що використовується для автоматизації процесів обробки інцидентів безпеки. Система розроблена з нуля для отримання максимальної швидкодії, масштабованості та стійкості до відмов, з мікросервісною архітектурою – кожен сервіс працює в контейнері Docker. Перевагами системи є:

- не використовує агентів – працює зі стандартними логами JSON;
- легко масштабується завдяки мікросервісній архітектурі;
- підтримує джерела даних хмарних сервісів, включаючи AWS CLOUDTRAIL та GUARDDUTY.

9. Wazuh. Основні переваги системи:

- заснована та сумісна з популярною SIEM OSSEC;
- підтримує різноманітні варіанти установки: DOCKER, PUPPET, CHEF, ANSIBLE;
- підтримує моніторинг хмарних сервісів, включаючи AWS та AZURE;
- включає комплексний набір правил для виявлення безлічі типів атак і дозволяє зіставляти їх у відповідність до PCI DSS V3.1 і CIS.
- інтегрується із системою зберігання та аналізу логів SPLUNK візуалізації подій та підтримки API [14].

10. Prelude OSS це рішення є гнучкою модульною SIEM-системою, що підтримує безліч форматів логів, інтеграцію зі сторонніми інструментами такими як OSSEC, Snort і мережеву систему виявлення Suricata. Переваги сервісу, відповідно до [14-15]:

- випробувана часом система, що розробляється і використовується з 1998 року;
- підтримує багато різних форматів логів;
- нормалізує дані до формату IMDEF, що дозволяє легко передавати дані до інших систем безпеки.

11. Sagan. Має такі переваги:

- повністю сумісна з базою даних SNORT, правилами і інтерфейсом користувача;
- багатопотокова архітектура забезпечує високу продуктивність [14].

12. SolarWinds має широкі можливості з управління журналами та звітністю, реагуванням на інциденти в режимі реального часу [7, 16]. Основні можливості системи:

- швидке виявлення підозрілих дій та загроз;
- безперервний контроль за станом безпеки;
- визначення часу події;
- відповідність стандартам DSS, HIPAA, SOX, PCI, STIG, DISA та ін.;
- рішення Solarwinds підходить для малого та великого бізнесу. він має як локальні, так і хмарні варіанти розгортання та працює під керуванням Windows та Linux.

13. ManateEngine – це SIEM рішення, яке фокусується на аналізі різних журналів і витягує з них різні відомості про продуктивність та безпеку.

Цільові області включають такі ключові вузли та програми, як веб-сервери, сервери DHCP, бази даних, сервери друку, поштові служби, тощо.

Крім того, аналізатор ManageEngine, що працює в системах Windows і Linux, корисний для приведення систем у відповідність до стандартів захисту даних, таких як PCI, HIPPA, DSS, ISO 27001 та ін. [12, 17].

14. EventTracker. Ключові особливості платформи SIEM EventTracker:

- оповіщення в режимі реального часу та реагування на інциденти. EventTracker генерує оповіщення на основі правил з оновленнями панелі керування та рекомендаціями щодо виправлення;
- пошук та криміналістичний аналіз. Журнали індексуються в Elastic Search з використанням моделі загального індексування, що розширюється;
- складання звітів. Модуль звітів включає понад 1500 визначених звітів про безпеку та відповідність. Повна підтримка включена для PCI-DSS, HIPAA, ISO 27001, NIST 800-171, DoD, RMF, GDPR та інших;
- аналіз поведінки та кореляція. EventTracker швидко виявляє та враховує зміни в системах та поведінці користувачів. Обробка та кореляція в реальному часі дає повну картину того, що нового та незвичного відбувається;
- аналіз небезпек. EventTracker інтегрується з цінними потоками даних про загрози від партнерів у екосистемі та постачальників з відкритим вихідним кодом, щоб забезпечити швидке та точне виявлення загроз для вашої мережі [18].

15. Trustwave SIEM Enterprise. Переваги Trustwave:

- користувачі інших продуктів безпеки Trustwave отримають переваги від покращення двонаправленої інтеграції з технологіями у своєму портфелі, які підтримують можливості автоматичного реагування, такі як ізоляція скомпрометованих кінцевих точок або блокування облікових записів користувачів;
- Trustwave SIEM Enterprise має одну з найпростіших архітектур, яка знижує навантаження на клієнтів під час розгортання та подальшого розширення [16].

16. BlackStratus SIEM Storm. Пристрій BlackStratus SIEM Storm надає гнучкі інструменти візуалізації загроз та пом'якшення їх наслідків у розподілених мережах. SIEM Storm інтегрується з існуючим мережним обладнанням та обладнанням для забезпечення безпеки, надаючи такі розширені функції [16, 19]:

- розширена архітектура. BlackStratus SIEM Storm забезпечує повне аварійне перемикання та багаторівневе резервування для задоволення складних нормативних вимог, забезпечення безперервності бізнесу та управління ризиками;
- візуалізація атаки у реальному часі. Виявлення атак нульового дня з використанням складних метрик на основі правил, уразливості, статистичних та історичних кореляцій;
- кореляція вразливості. Інтеграція даних із CVE-сумісних систем виявлення вторгнень, усунення хибних спрацьовувань та звільнення вашої команди, щоб зосередитися на реальних загрозах;
- прозорість. Отримання безпрецедентної видимості у розподілених мережах для кореляції активності в окремих мережевих середовищах, виявлення прихованих загроз, підозрілих тенденцій та іншої потенційно небезпечної поведінки;
- складання звітів. BlackStratus SIEM Storm забезпечує просту звітність відповідно до ISO, PCI, HIPAA, SOX та інших стандартів ІБ.

У Табл. 1, відповідно до [4-5], систематизовано та представлено детальний аналіз SIEM-систем за такими 18 критеріями (запропоновані авторами):

1. Аудит та перевірка на відповідність стандартам;
2. Повноцінність системи (повноцінна – «+», є лише обробка логів – «-»);
3. Оцінка захищеності ресурсів системи, що контролюється (у т.ч. КВР);
4. Перевірка відповідності системи управління ІБ;
5. Управління ризиками ІБ;
6. Збір та зберігання подій, які надходять до системи;
7. Обробка та аналіз зареєстрованих подій;
8. Виявлення атак та порушень політик безпеки;
9. Виявлення та розбір інцидентів безпеки;
10. Можливість розслідувань;
11. Пошук уразливостей;
12. Формування звітів;
13. Підтримка роботи з хмарними середовищами;
14. Підтримка роботи з Big Data платформами;
15. Можливість інтеграції з новими системами у майбутньому;
16. Розширені можливості пошуку;
17. User Friendly інтерфейс;
18. Можливість безкоштовного використання.

Таблиця 1

Порівняльний аналіз SIEM-систем

№	Назва	Критерії																	
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
1.	IBM QRadar	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
2.	LogRhythm	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
3.	Splunk	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
4.	McAfee (ESM)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
5.	AlienVault USM	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
6.	FortiSIEM	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
7.	Ixia ThreatARMOR	+	+	+	+	+	+	+	+	+	+	+	+	-	-	+	+	+	-
8.	MozDef	+	+	-	+	-	+	+	+	+	+	-	+	+	+	+	+	+	+
9.	Wazuh	+	+	-	+	-	+	+	+	+	+	+	+	+	+	+	+	+	+
10.	Prelude OSS	+	+	-	+	+	+	+	+	+	+	+	+	-	-	-	+	+	+
11.	Sagan	-	-	-	-	-	+	+	+	+	+	-	+	-	-	-	+	-	+
12.	SolarWinds	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
13.	ManateEngine	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
14.	EventTracker	+	+	-	+	-	+	+	+	+	+	+	+	+	+	-	+	+	-
15.	Trustwave SIEM Enterprise	+	+	-	+	+	+	+	-	+	+	+	+	+	+	-	+	+	-
16.	Black Stratus SIEM Storm	+	+	-	+	-	+	+	+	+	+	+	+	-	-	-	+	+	-

У табл. 1 відображено огляд сучасних SIEM-систем та інших систем ІБ, що виконують їх функції. Зокрема відображено їх функціональність, основний принцип роботи, а також проведено порівняльний аналіз їх можливостей та відмінностей, переваг та недоліків використання. Також проведено аналіз на відповідність до міжнародних специфікацій та стандартів. Проведений аналіз показав, що найбільш оптимальними є системи *IBM QRadar, LogRhythm, Splunk, McAfee (ESM), AlienVault USM, FortiSIEM, SolarWinds* та *ManateEngine* (виділені у табл. 1 сірим кольором), адже вони відповідають найбільшій кількості критеріїв, проте відрізняються вартістю. З урахуванням зазначеного, вбачається за доцільне розробити універсальну SIEM-систему, у якій будуть враховані всі перелічені функціональні особливості та переваги.

Метою статті є розроблення, програмна реалізація та експериментальне дослідження системи корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури. Система повинна відповідати визначеним критеріям і забезпечувати як ефективне корелювання подій кібербезпеки, так і управління інцидентами, які виникають в КІ і мають вплив на КВР.

ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ СИСТЕМИ КОРЕЛЮВАННЯ ПОДІЙ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ

У процесі дослідження було визначено, що сьогодні доцільно використовувати Open Source системи з погляду витрат та можливості доповнення функціоналу для потреб конкретного підприємства (об'єкта КІ). З позицій безпеки, найкращим варіантом є розробка власної системи корелювання подій та управління інцидентами кібербезпеки (СКУІК) на об'єктах КІ, яка володітиме широким функціоналом з ІБ, буде гнучкою та масштабованою, а також захищеною від можливих уразливостей та бекдорів.

Авторами було запропоновано універсальне рішення, що базується на використанні хмарної SIEM-системи для галузі КІ [5] та розроблено концепцію архітектури СКУІК. Рис. 1 відображає архітектуру запропонованої системи, яка орієнтована на використання в різних секторах КІ з підтримкою хмарних технологій.

Запропонована схема може бути інтегрована в реальні інфраструктури з різними SIEM-системами або іншими інструментами управління інцидентами, що функціонують.

Основними структурними одиницями СКУІК є:

- горизонтальні бази даних (Horizontal Databases);
- блок аналітики (Analytics);
- блок моніторингу (Monitoring);
- хмарне сховище (Cloud Storage);
- шифратор даних (Encryptor);
- брокер повідомлень (Message Broker);
- джерела (System 1 – System *N*).

Для СКУІК розроблено моделі функціонування гібридного сховища даних безпеки, які відрізняються від аналогів тим, що поєднують два різні типи БД – зокрема для швидкої обробки журналів використовується масштабований повнотекстовий пошуковий двигун з відкритим вихідним кодом Elasticsearch (який використовує бібліотеку Lucene, написаний на Java, формат документів JSON), а також відкрита документоорієнтована СУБД MongoDB (використовує JSON-подібні документи та схему БД, написана на C++). Такий підхід дозволяє сервісу індексації отримувати доступ до зовнішніх сховищ даних (при цьому дані коректно індексуються та виводяться при пошуку), провести масштабування (кластеризацію) при зростанні обсягу даних, підтримує роботу з різними запитами (прості, складні, структуровані) та з різними типами даних, дозволяє робити агрегацію, проводити аналіз, збирати закономірності, спростити пошук та забезпечити високу швидкість пошуку. Крім того, SIEM-система на базі запропонованих моделей може працювати з набором реплік (тобто містити дві або більше копії даних на різних вузлах), масштабується горизонтально, використовуючи техніку сегментування об'єктів БД і може бути використана як файлове сховище з балансуванням навантаження та реплікацією даних (функція Grid File System).

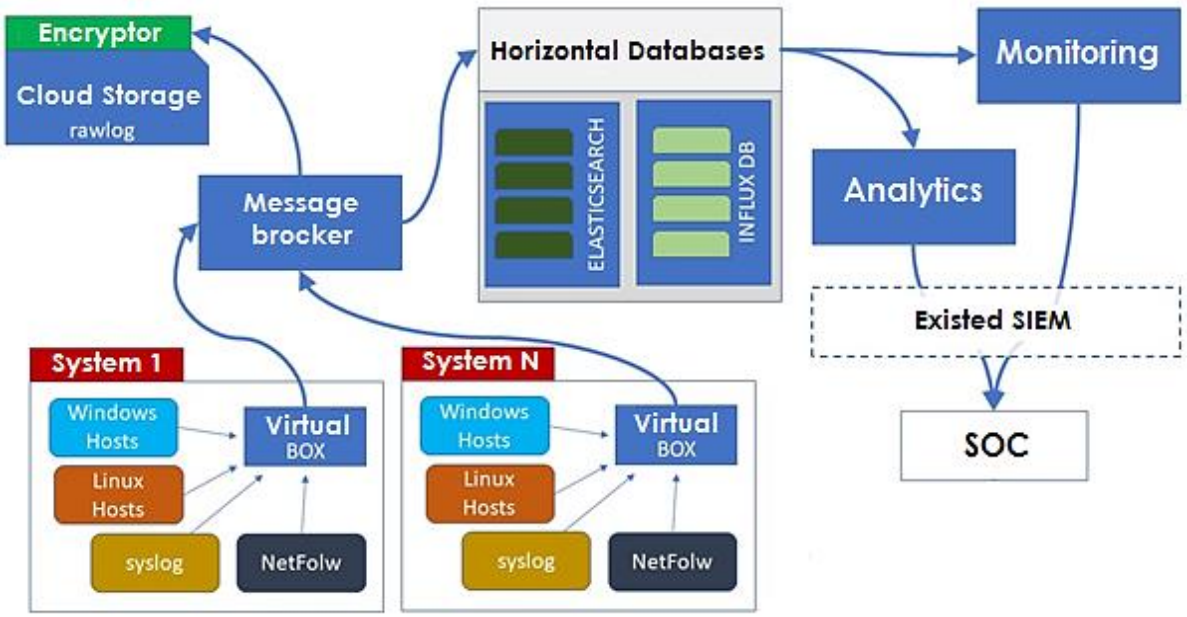

Рис. 1 Архітектура розробленої СКУІК

Розроблено моделі, методики та алгоритми функціонування розподіленої шини даних (ШД), які відрізняються від аналогів тим, що для збору інформації (подій) використовують власні агенти, які встановлюються в контрольовані системи, а також стандартні існуючі механізми збору подій (syslog, snmp тощо) використовують сценарії інтеграції з можливістю модифікації з мінімальним втручанням розробників; ШД для контролю мережі може використовуватися як колектор NetFlow статистики, одержуваних з мережного обладнання, а також для аналізу мережевого трафіку як з використанням або дзеркального трафіку з мережевого обладнання, або пропускаючи трафік через себе. Такий підхід дозволить забезпечити високу швидкість обробки великих потоків інформації, мінімальні затримки на обробку даних, мінімальні затримки для побудови аналітичних звітів і запитів, високу стійкість до відмов, гнучкість і розширюваність сховища шляхом простого додавання вузлів без простою бази.

З погляду ІБ, важливу роль у цій системі відіграє шифратор даних (Encryptor), який фактично є єдиним блоком з хмарним сховищем (Cloud Storage), забезпечуючи таким чином конфіденційність необроблених записів після збору агентами syslog, NetFlow і т.д. Крім цього, віртуальна машина (Virtual BOX) відправляє зібрані дані у зашифрованому вигляді через брокер повідомлень (Message Broker) у горизонтальні бази даних (Horizontal Databases). У разі відсутності зв'язку з брокером повідомлень забезпечується тимчасове зберігання даних у хмарному сховищі, як уже зазначалося.

Далі, зазначена система СКУІК була реалізована програмно, наступним етапом є експериментальне дослідження програмного рішення як інструменту ІБ (у контексті відповідності визначеним критеріям і забезпечення ефективного корелювання подій кібербезпеки та управління інцидентами, які виникають в КІ і мають вплив на КВР).

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ РОЗРОБЛЕНОЇ СИСТЕМИ

Розроблена СКУІК автоматизує визначення пріоритетів загроз безпеці та порушень вимоги ІБ на основі аналізу та кореляції подій ІБ. СКУІК аналізує кожен вхід у систему та вихід із неї, доступ до ресурсів (у т.ч. КВР), запити до бази та транзакції тощо.

Система забезпечує:

- збирання, зберігання та аналіз подій з будь-якого джерела та у необхідний час;
- аналізу подій та виявлення незвичайних чи несанкціонованих дій;
- графічні панелі моніторингу подій, що настроюються;
- API для інтеграції зі сторонніми системами та сервісами.

Архітектура системи

Система має високу гнучкість і горизонтальну масштабованість. Для зберігання подій використовується NoSQL СУБД Elasticsearch, для зберігання всієї інформації про конфігурацію та правила використовується NoSQL СУБД mongoDB.

Система, залежно від вимог до продуктивності та надійності, може бути розгорнута у різних варіантах. Приклад архітектури системи СКУІК наведено на рис. 2.

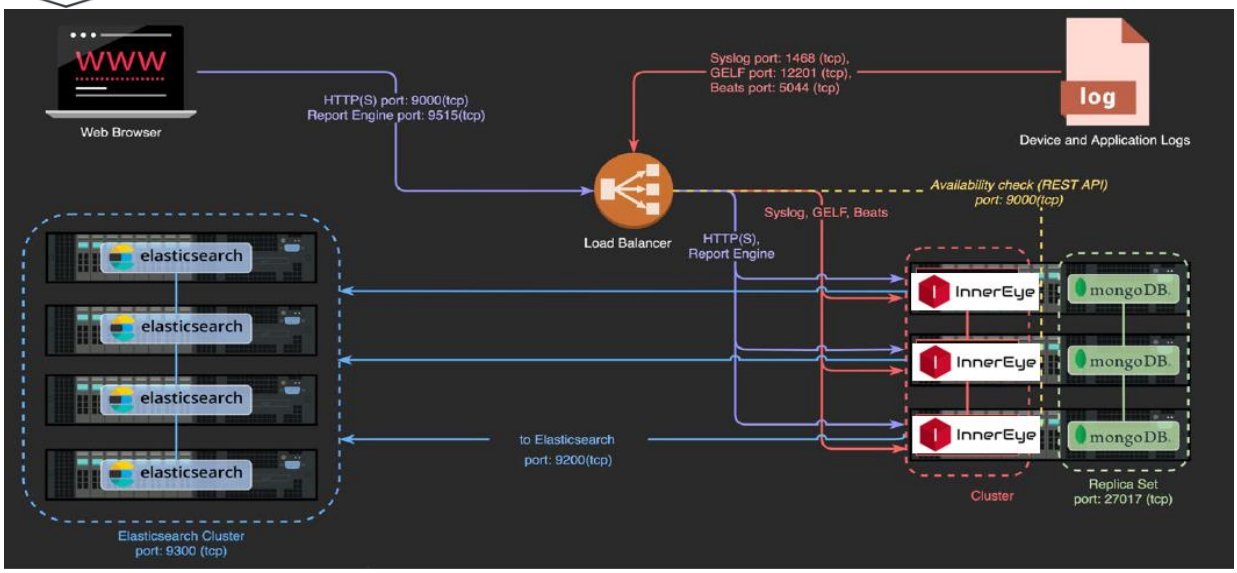

Рис. 2 Приклад архітектури СКУІК з продуктивністю до 300 Гб подій на добу

Використання кластерів у СКУІК забезпечує високу продуктивність та надійність системи в цілому та дозволяє гнучко адаптувати систему до конкретних умов.

Функціональні можливості системи

Джерела подій та робота з ними

Система підтримує стандартні методи збирання журналів подій (див. Рис. 3), які складаються з таких компонентів:

- Syslog (TCP, UDP, AMQP, Kafka);
- GELF (TCP, UDP, AMQP, Kafka, HTTP);
- AWS (AWS Logs, FlowLogs, CloudTrail);
- Beats/Logstash;
- CEF (TCP, UDP, AMQP, Kafka);
- JSON Path from HTTP API;
- Netflow/IPFIX (UDP);
- Plain/Raw Text (TCP, UDP, AMQP, Kafka).

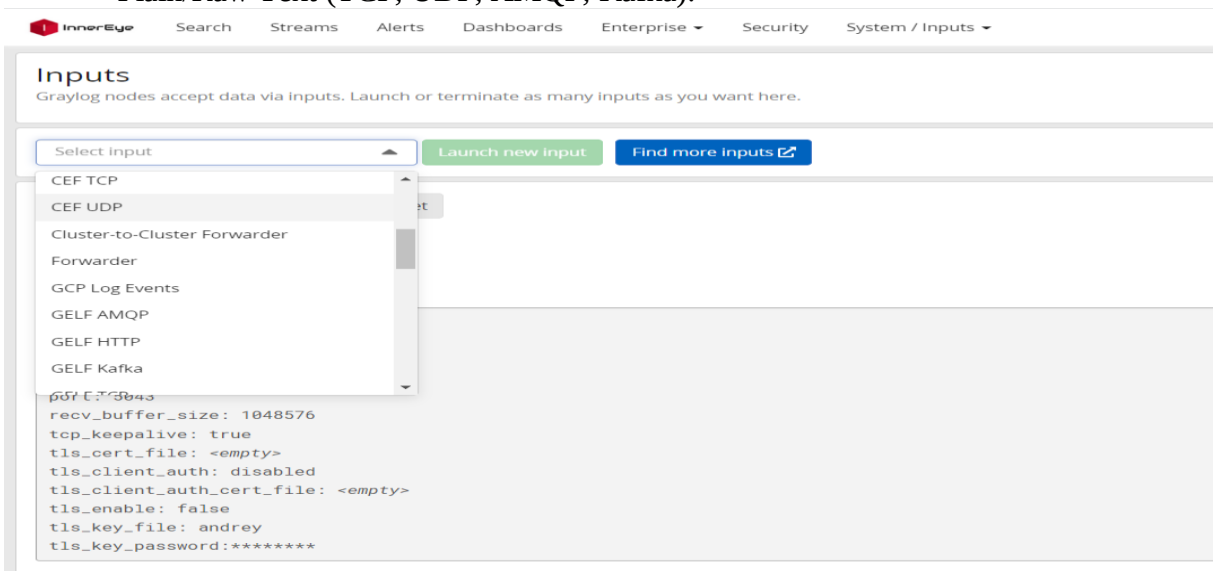

Рис. 3 Меню вибору типу джерела подій

До кожного типу джерела подій можливе створення індивідуального приймача (далі – Input) з індивідуальними параметрами. За кожним джерелом подій можна переглянути загальну інформацію, а також перейти до перегляду подій від цього джерела. Крім того, для протоколів, що підтримують безпечне передавання даних (TLS), можливе налаштування відповідних параметрів.

Збереження подій у базі даних

СКУІК зберігає події в NoSQL СУБД Elasticsearch. Можливе створення довільної (в рамках обмежень самої СУБД Elasticsearch) кількості баз даних (індексів) (Рис. 4).

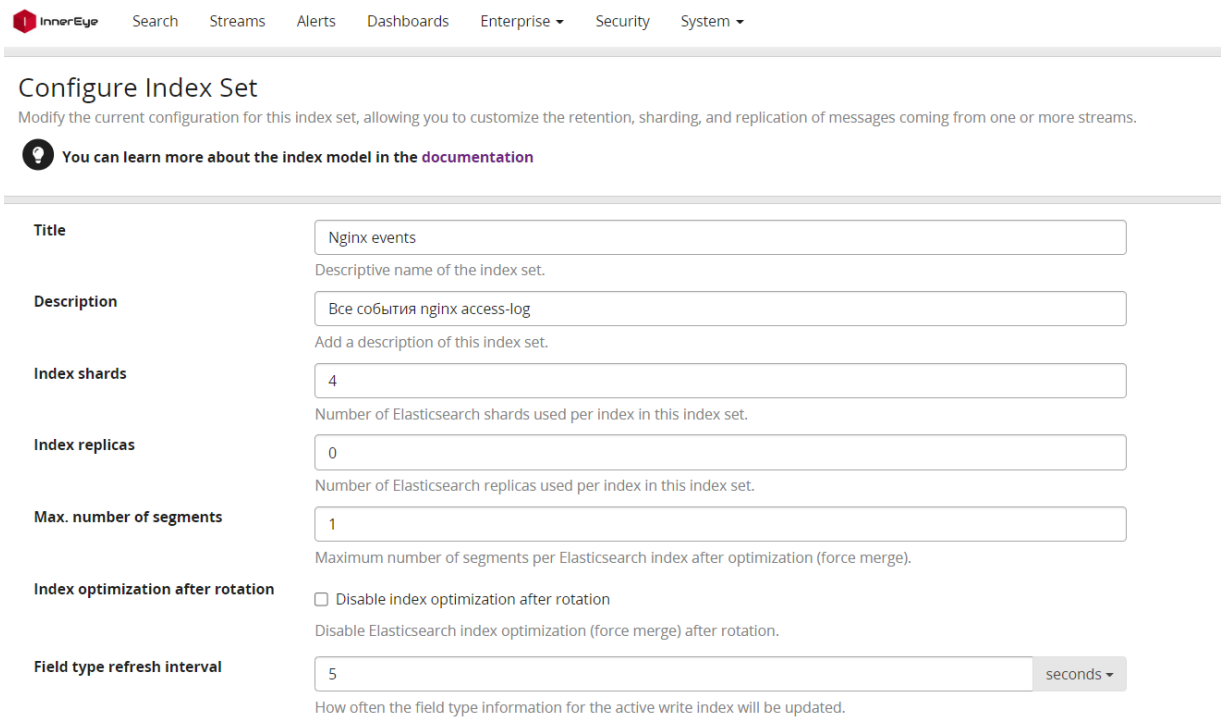

Рис. 4 Налаштування параметрів бази даних (індексу)

Обробка подій – потоки

Потоки – це механізм, який розподіляє події за категоріями реального часу під час їх обробки (Рис. 5). Можливе створення довільної (в рамках фізичних обмежень серверного обладнання та обмежень СУБД mongoDB) кількості потоків.

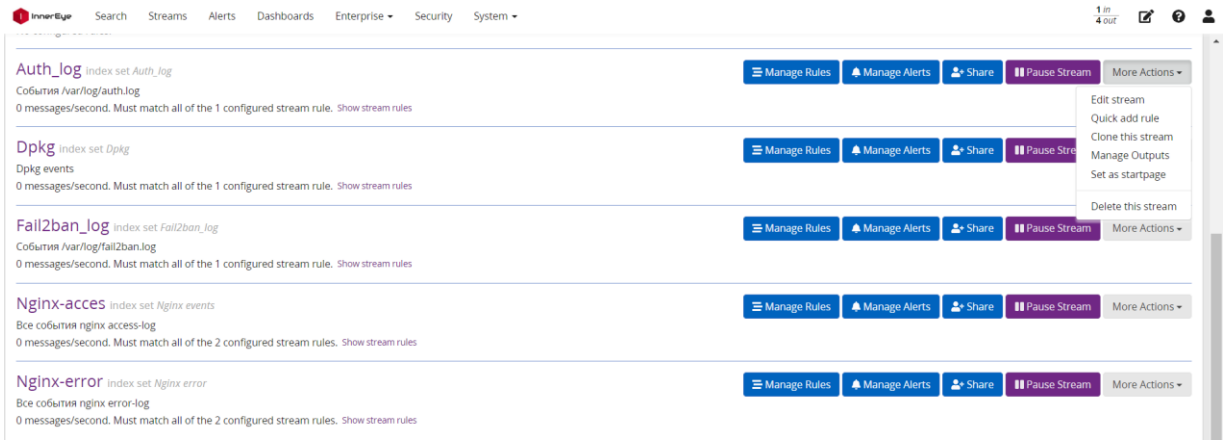

Рис. 5 Загальна інформація про потоки та можливі дії з ними

Розподіл подій за потоками складає основу правил. Система передбачає створення (редагування) правил розподілу подій за потоками. Використання потоків дозволяє в реальному часі обробляти, сповіщати та пересилати події в інші системи, наприклад, відправляти інформацію про помилки бази даних в іншу систему.

Обробка подій – конвеєри (pipelines) та правила обробки

Конвеєри – це центральна концепція, що поєднує етапи обробки, що застосовуються до подій. Конвеєри містять правила і можуть бути підключені до одного або кількох потоків, що дозволяють точно контролювати обробку, що застосовується до подій (Рис. 6).

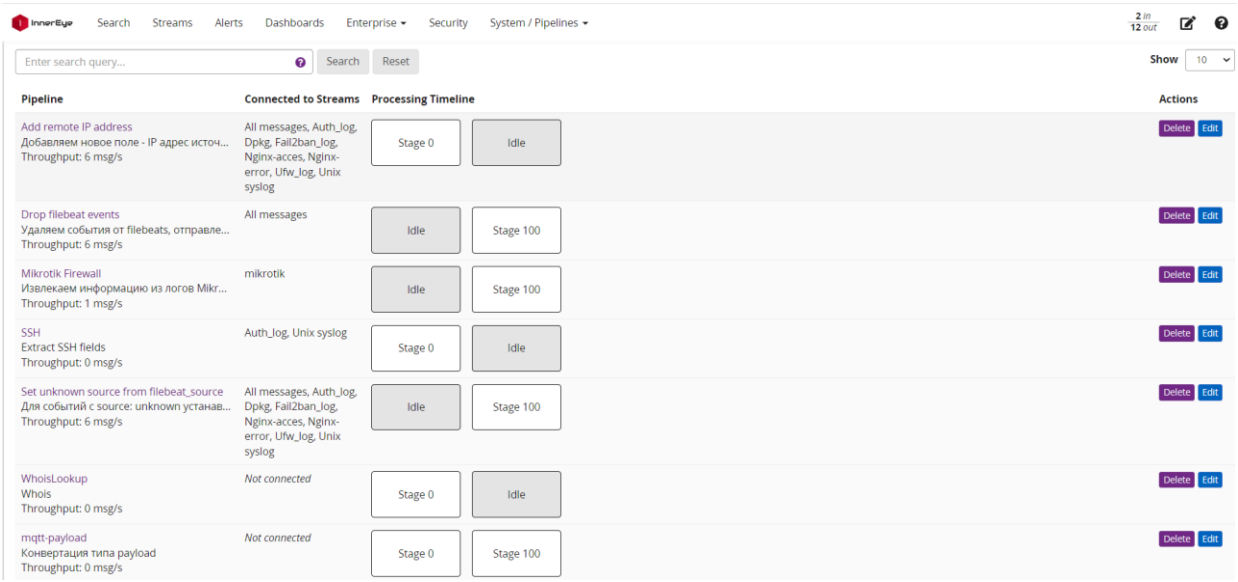

Рис. 6 Загальна інформація про конвеєри

Правила обробки – це умови, за якими слідує список дій, і самі по собі вони не мають потоку управління. Тому конвеєри мають ще одне поняття – етапи, які є групами умов та дій, що повинні виконуватися за порядком. Усі етапи з однаковим пріоритетом виконуються одночасно у всіх підключених конвеєрах. Етапи забезпечують необхідний потік управління для прийняття рішення про те, чи слід запускати етапи, що залишилися, в конвеєрі. Етапи виконуються в порядку їхнього пріоритету і не мають інших назв. Пріоритети етапів можуть бути будь-якими цілими числами, позитивними чи негативними. Порядок, що ґрунтується на пріоритеті етапу, дає можливість запускати певні правила до або після інших, які можуть існувати в інших підключених конвеєрах, без зміни цих інших підключених конвеєрів (Рис. 7).

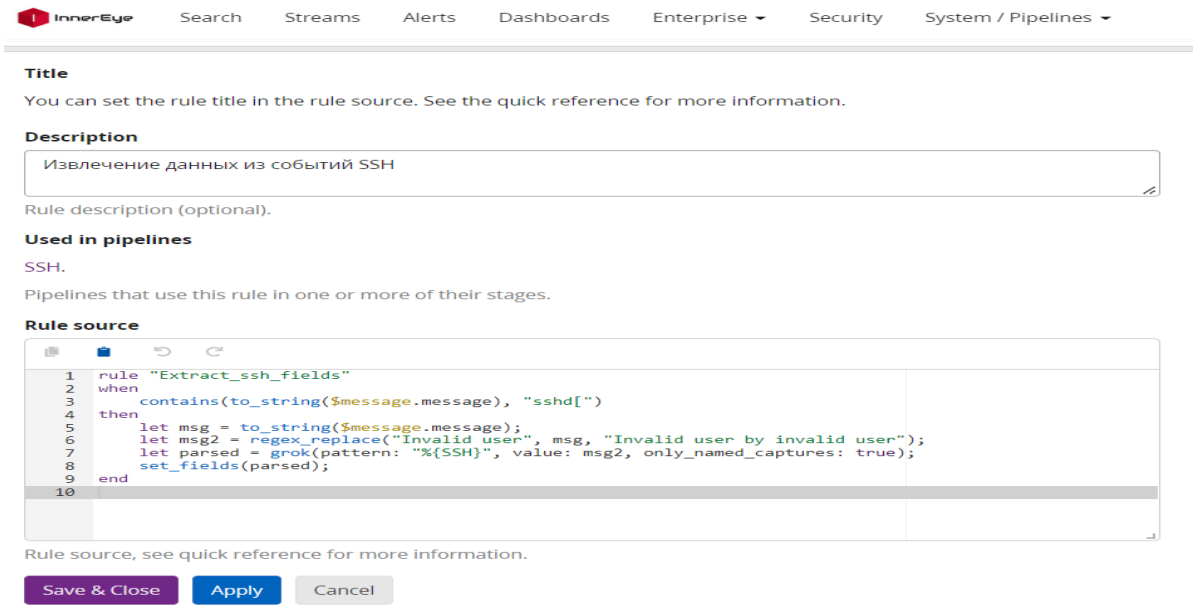

Рис. 7 Створення та редагування правил обробки

Правила є основою конвеєрів обробки. Вони містять логіку про те, як змінювати, доповнювати, маршрутизувати та видаляти повідомлення. Обробка повідомлень виконується у функціях. СКУІК містить велику кількість вбудованих функцій, що забезпечують перетворення даних, маніпулювання рядками, вилучення даних за допомогою таблиць пошуку, синтаксичний аналіз JSON, тощо. Правила посилаються на імена і тому вони можуть спільно використовуватися багатьма різними конвеєрами. Мета полягає в тому, щоб уможливити створення повторно використовуваних стандартних блоків, спрощуючи обробку даних, характерних для конкретного варіанту використання.

Події та оповіщення

Подія – це умова, яка зіставляє повідомлення, що надходять від джерел (у потоці повідомлень) з періодом часу або агрегацією. Події можна використовувати для угруповання схожих полів, зміни вмісту поля або створення нового вмісту поля для використання з попередженнями та правилами кореляції.

Створення (редагування) події складається з кількох етапів. На першому етапі визначаються загальні властивості події. На другому етапі можна конкретно описати критерії виявлення події на основі фільтра та агрегації. Фільтр визначається за допомогою пошуку. Для обмеження області пошуку можна вибрати потік, у якому потрібно знайти повідомлення. Можна визначити період часу, протягом якого фільтр шукатиме повідомлення у зворотному напрямку. Пошук буде виконуватись із заданим інтервалом. На наступному етапі виконується створення полів, що налаштовуються (Рис. 8), що дозволяє заповнювати дані з вихідного журналу в індекс подій. Це позбавляє оператора необхідності виконувати наступні пошуки для отримання важливої інформації, і також дають можливість використовувати їх для обмеження обсягу даних, що надсилаються в ціль повідомлень. Подія буде записана в потік «Всі події» і міститиме поле користувача, а також результат агрегування, що викликало подію.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

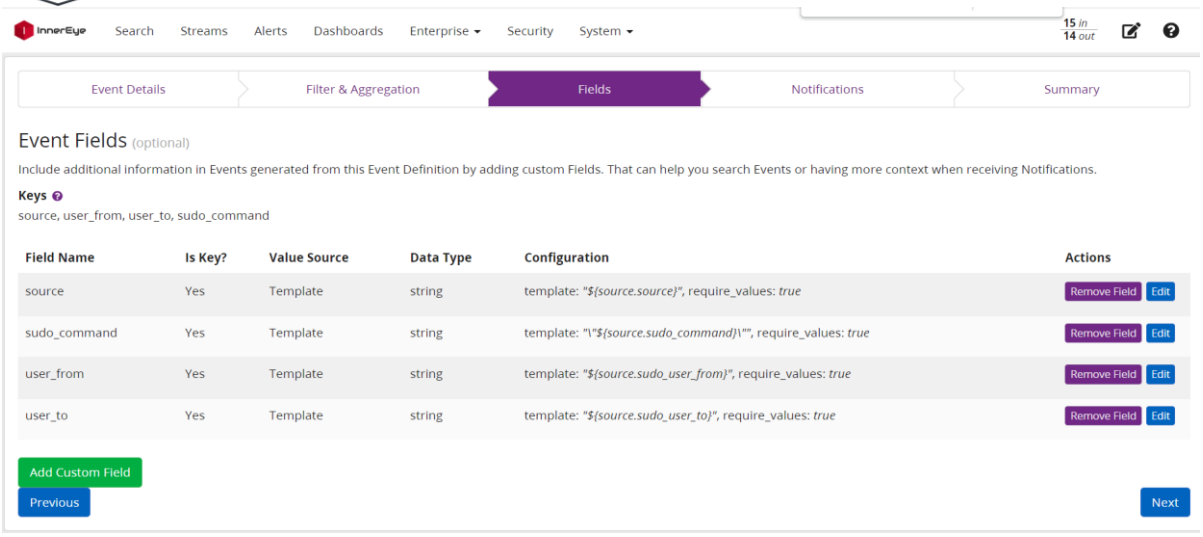

Рис. 8 Редагування (створення) події – поля, що налаштовується

На наступному етапі можливе підключення до події сповіщення, при цьому статус події підвищується до оповіщення (Рис. 9). На останньому етапі здійснюється контроль параметрів та збереження конфігурації події. На сторінці Alerts&Events є повна інформація про всі події та всі оповіщення.

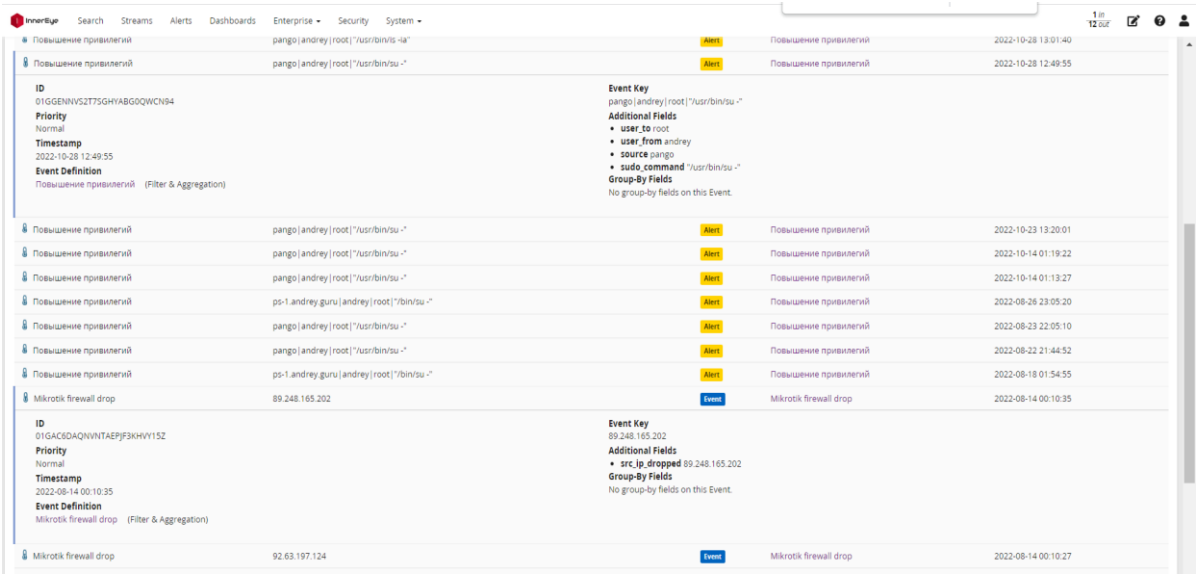

Рис.9 Інформація про події та оповіщення

Інформаційні панелі (dashboards)

Використання інформаційних панелей дозволяє створювати наперед визначені (зумовлені) пошуки за даними. Це дозволяє отримати доступ до важливої інформації в один клік. Інформаційні панелі дозволяють визначити конкретні критерії пошуку, такі як запит або часовий діапазон. Інформаційні панелі (Рис. 10) також дозволяють створювати кілька вкладок для різних варіантів використання, відображати результат у повноекранному режимі.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

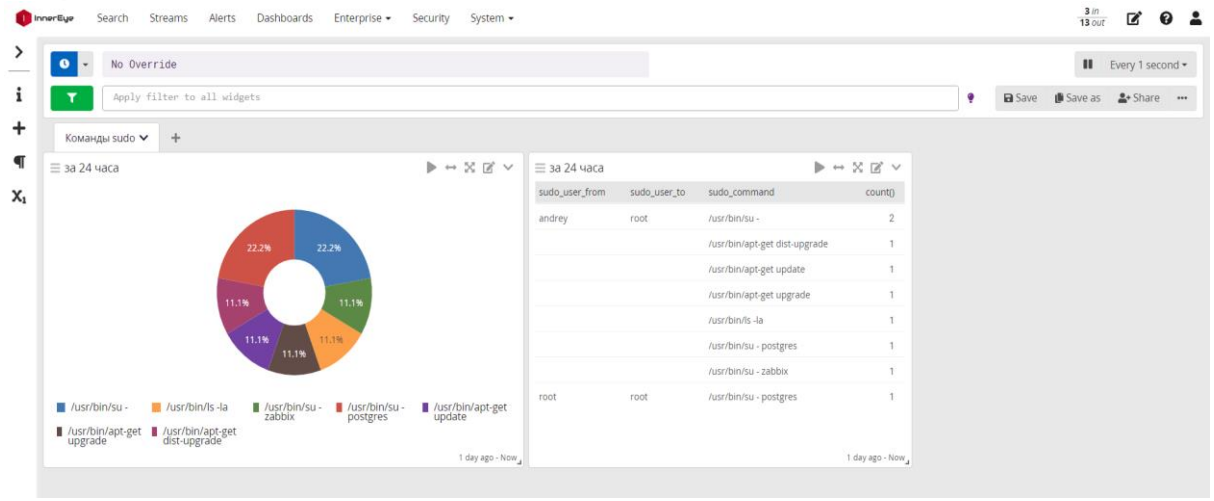

Рис. 10 Інформаційна панель – стандартне відображення

Пошук

Сторінка пошуку – це «серце» використання СКУІК. На вкладці (Рис. 11) можна виконати пошук (запит) та візуалізувати результат за допомогою різних віджетів. Будь-який пошук можна зберегти або експортувати до інформаційної панелі. Збережені пошуки дають змогу легко повторно використовувати певні конфігурації пошуку. Інформаційні панелі дозволяють виконувати пошукові запити, специфічні для віджетів, і можуть використовуватись спільно, щоб інші користувачі могли використовувати їх у своїх процесах.

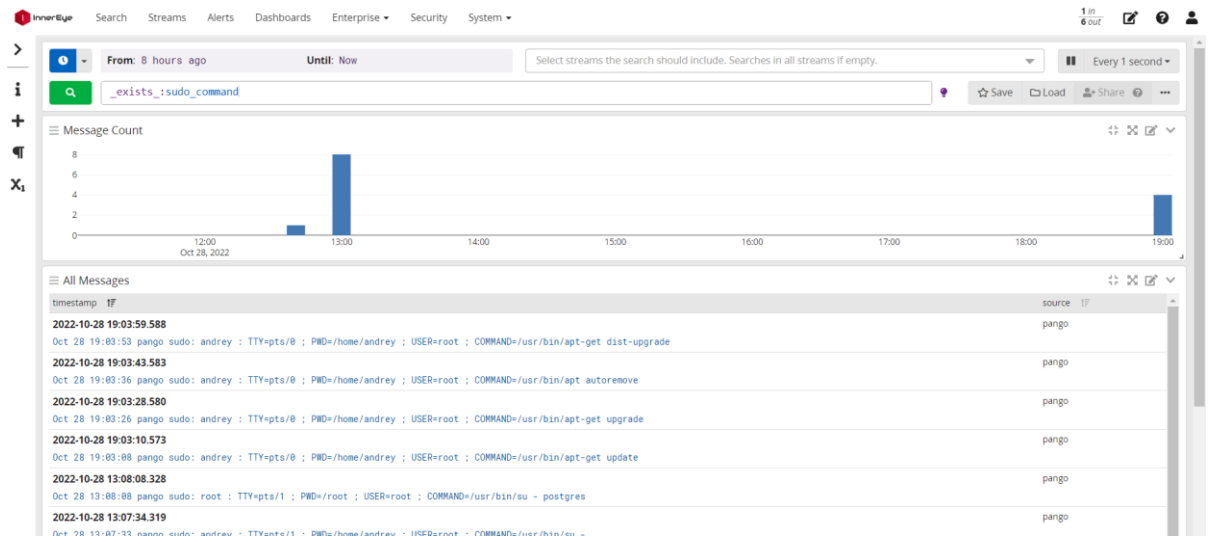

Рис. 11 Вікно пошуку – загальний вигляд

Після завершення роботи з експериментального дослідження системи згідно з розробленою концепцією архітектури проведено навантажувальне випробування макета, яке підтвердило високу ефективність рішень (модулів), що використовуються в розробленій СКУІК. Крім цього, за допомогою спеціалізованих засобів проведено перевірку вихідного коду на наявність уразливостей, внаслідок якої критичних уразливостей не було виявлено. Таким чином, розроблена система дозволяє

забезпечувати ефективне корелювання подій кібербезпеки та управління інцидентами, які виникають в КІ і мають вплив на КВР.

ВИСНОВКИ

У роботі проведено аналіз існуючих SIEM-систем, визначено їх функціональність, основний принцип роботи, а також проведено аналіз на відповідність до міжнародних специфікацій та стандартів. Проведений аналіз показав, що найбільш оптимальними є системи IBM QRadar, LogRhythm, Splunk, McAfee (ESM), AlienVault USM, FortiSIEM, SolarWinds та ManateEngine, адже вони відповідають найбільшій кількості критеріїв, проте відрізняються вартістю. З урахуванням результатів аналізу, на базі відкритих модулів, було розроблено універсальну СКУІК на об’єктах КІ, в якій враховані всі перелічені функціональні особливості та переваги.

Розроблено моделі функціонування гібридного сховища даних безпеки, які дозволяють сервісу індексації отримувати доступ до зовнішніх сховищ даних, провести масштабування при зростанні обсягу даних, підтримують роботу з різними запитами та з різними типами даних; дозволяють робити агрегацію, проводити аналіз, збирати закономірності, спростити пошук та забезпечити високу швидкість пошуку.

Розроблено моделі, методики та алгоритми функціонування розподіленої ШД, які дозволяють забезпечити високу швидкість обробки великих потоків інформації, мінімальні затримки на обробку даних, мінімальні затримки для побудови аналітичних звітів і запитів, високу стійкість до відмов, гнучкість і розширюваність сховища шляхом простого додавання вузлів без простою бази.

Система СКУІК призначена для розв’язання низки актуальних у кібербезпеці задач, таких як: реєстрація дій користувачів під час використання інформаційних ресурсів (у т.ч. КВР) організації у системних журналах; періодичний контроль коректності дій користувачів системи шляхом аналізу вмісту системних журналів; контроль цілісності (забезпечення незмінності) середовища виконання програм та її відновлення у разі порушення; захист інформації від несанкціонованої модифікації; контроль цілісності програмних засобів, що використовуються, а також захист системи від впровадження шкідливих кодів, включаючи комп'ютерні віруси; своєчасне виявлення загроз, причин та умов, що сприяють завданню шкоди; створення механізму оперативного реагування на загрози ІБ та негативні тенденції; створення умов для мінімізації та локалізації завданих збитків неправомірними діями фізичних та юридичних осіб, послаблення негативного впливу та ліквідація наслідків порушення ІБ.

Крім того, проведено експериментальне дослідження СКУІК і доведено, що розроблена система відповідає вимогам, поставленим на основі аналізу міжнародних стандартів та найкращих світових практик щодо створення систем управління кіберінцидентами, які стосуються: цільового призначення системи; централізованого управління компонентами та функціоналом системи; візуалізації даних через відповідні інтерфейси; підтримки відкритого програмного інтерфейсу API; підтримки аутентифікації та авторизації; можливості автоматичного та/або ручного оновлення; відмовостійкості; масштабування; збору та фільтрації подій; управління обліковими записами. Система СКУІК може використовуватись для управління інцидентами, які виникають в КІ і мають вплив на КВР.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Buriachok, V., Sokolov, V., Skladannyi, P. (2019). Security rating metrics for distributed wireless systems. У *Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science* (с. 222–233).

2 Kipchuk, F., Sokolov, V., Buriachok, V., Kuzmenko, L. (2019). Investigation of Availability of Wireless Access Points based on Embedded Systems. У *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/picst47496.2019.9061551.

3 Bogachuk, I., Sokolov, V., & Buriachok, V. (2018). Monitoring Subsystem for Wireless Systems Based on Miniature Spectrum Analyzers. У *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/infocommst.2018.8632151.

4 Gnatyuk, S., Berdibayev, R., Fesenko, A., Kyryliuk, O., & Bessalov, A. (2021). Modern SIEM Analysis and Critical Requirements Definition in the Context of Information Warfare. У *Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems* (с. 149–166).

5 Berdibayev, R., Gnatyuk, S., Tynymbayev, S., Sydorenko, V. (2022). *Advanced Technologies of Cyber Incident Management in Critical Infrastructure: Monograph*. “Pro Format” Publishing House.

6 Ariel Query Language Guide, IBM QRadar 7.3.3 (2013 and 2019). https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_aql.pdf.

7 Vielberth, M., Pernul, G. (2018). A Security Information and Event Management Pattern. У *12th Latin American Conference on Pattern Languages of Programs (SugarLoafPLoP 2018).*

8 Karlzén, H. (2009). *An Analysis of Security Information and Event Management Systems*. University of Gothenburg, Göteborg. http://publications.lib.chalmers.se/records/fulltext/89572.pdf.

9 Agrawal, K., Makwana, H. (2015). A Study on Critical Capabilities for Security Information and Event Management. *International Journal of Science and Research (IJSR)*, 4(7), 1893-1896.

10 Berdibayev, R., Gnatyuk, S., Yevchenko, Yu., Kishchenko, V. (2021). A concept of the architecture and creation for SIEM system in critical infrastructure. *Studies in Systems, Decision and Control, 346*, 2021, 221-242.

11 Gnatyuk, S., Berdibayev, R., Avkurova, Z., Verkhovets, O., Bauyrzhan, M. (2021). Studies on cloud-based cyber incidents detection and identification in critical infrastructure. *CEUR Workshop Proceedings, 2923*, 68-80.

12 Lee, J.-H., Kim, Y. S., Kim, J. H., & Kim, I. K. (2017). Toward the SIEM architecture for cloud-based security services. У *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE. https://doi.org/10.1109/cns.2017.8228696.

13 Miller, D., Harris, Sh., Harper, A., VanDyke, S., Blask, C. (2010). Security Information and Event Management (SIEM) Implementation. McGraw-Hill Osborne Media.

14 SIEM Analytics. http://www.siem.su/compare_SIEM_systems.php.

15 Lee, J.-H., Kim, Y. S., Kim, J. H., & Kim, I. K. (2017). Toward the SIEM architecture for cloud-based security services. У *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE. https://doi.org/10.1109/cns.2017.8228696

16 Bachane, I., Adsi, Y. I. K., & Adsi, H. C. (2016). Real time monitoring of security events for forensic purposes in Cloud environments using SIEM. У *2016 Third International Conference on Systems of Collaboration (SysCo)*. IEEE. https://doi.org/10.1109/sysco.2016.7831327

17 AlSabbagh, B., & Kowalski, S. (2016). A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM). У *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE. https://doi.org/10.1109/eisic.2016.049.

18 Serckumecka, A., Medeiros, I., & Bessani, A. (2019). Low-Cost Serverless SIEM in the Cloud. У *2019 38th Symposium on Reliable Distributed Systems (SRDS)*. IEEE. https://doi.org/10.1109/srds47363.2019.00057.

19 R Mahmoud, R.-V., Kidmose, E., Turkmen, A., Pilawka, O., & Pedersen, J. M. (2021). DefAtt - Architecture of Virtual Cyber Labs for Research and Education. У *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE. https://doi.org/10.1109/cybersa52016.2021.9478236.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

Sergiy Gnatyuk
DSc, Professor, Dean of the Faculty of Computer Sciences and Technologies
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua

Rat Berdibayev
PhD, Chair of Scientific and Technical Center of Information Security Problems n.a. Turganbek Omar
Almaty University of Power Energy and Telecommunication, Almaty, Kazakhstan
ORCID ID: 0000-0002-8341-9645
r.berdybaev@aues.kz

Viktoriia Sydorenko
PhD, Associate Professor, Associate Professor of IT-Security Academic Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Oksana Zhyharevych
Senior lecturer of the Department of Computer Science and Cyber Security
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID ID: 0000-0002-7154-9733
zhyharevych.oksana@vnu.edu.ua

Tetiana Smirnova
PhD, Associate Professor, Associate Professor of Academic Department of Cybersecurity and Software
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-5093-1581
sm.tetyana@gmail.com

SYSTEM FOR CYBER SECURITY EVENTS CORRELATION AND INCIDENT MANAGEMENT IN CRITICAL INFRASTRUCTURE OBJECTS

Abstract. Modern information infrastructure consists of a large number of systems and components that require constant monitoring and control. To identify, analyze and eliminate possible cyber threats, it is recommended to use a single common solution - the so-called SIEM systems. SIEM technology collects event log data, detects unusual activity through real-time analysis, identifies threats, generates alerts, and suggests appropriate action scenarios. Today, the number and quality of SIEM systems has grown significantly, and the latest technologies of artificial intelligence, the Internet of Things, and cloud technologies are used to ensure fast and effective detection of threats. Thus, the work carried out a study of modern SIEM systems, their functionality, basic principles of operation, as well as a comparative analysis of their capabilities and differences, advantages and disadvantages of use. In addition, a universal system of event correlation and management of cyber security incidents at critical infrastructure facilities was developed and experimentally investigated. Models of the operation of the hybrid security data storage have been developed, which allow the indexing service to access external data storages, to perform scaling when the volume of data increases, to ensure high search speed, etc. Models, methods and algorithms for the operation of a distributed data bus have been developed, which allow for high speed processing of large flows of information, minimal delays in data processing, high resistance to failures, flexibility and expandability of storage. The proposed system is designed to solve a number of current cyber security problems and meets the main requirements of international standards and best global practices regarding the creation of cyber incident management systems.

Keywords: SIEM system, cyber threat, cyber security, cyber security incident, critical infrastructure, critical infrastructure objects, event correlation system and cyber security incident management.

REFERENCES

1. Buriachok, V., Sokolov, V., Skladannyi, P. (2019). Security rating metrics for distributed wireless systems. In *Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science* (p. 222–233).
2. Kipchuk, F., Sokolov, V., Buriachok, V., Kuzmenko, L. (2019). Investigation of Availability of Wireless Access Points based on Embedded Systems. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/picst47496.2019.9061551.
3. Bogachuk, I., Sokolov, V., Buriachok, V. (2018). Monitoring Subsystem for Wireless Systems Based on Miniature Spectrum Analyzers. У *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/infocommst.2018.8632151.
4. Gnatyuk, S., Berdibayev, R., Fesenko, A., Kyryliuk, O., Bessalov, A. (2021). Modern SIEM Analysis and Critical Requirements Definition in the Context of Information Warfare. In *Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems* (c. 149–166).
5. Berdibayev, R., Gnatyuk, S., Tynymbayev, S., Sydorenko, V. (2022). *Advanced Technologies of Cyber Incident Management in Critical Infrastructure: Monograph.* "Pro Format" Publishing House.
6. Ariel Query Language Guide, IBM QRadar 7.3.3 (2013 and 2019). https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_aql.pdf.
7. Vielberth, M., Pernul, G. (2018). A Security Information and Event Management Pattern. In *12th Latin American Conference on Pattern Languages of Programs (SugarLoafPLoP 2018).*
8. Karlzén, H. (2009). *An Analysis of Security Information and Event Management Systems*. University of Gothenburg, Göteborg. http://publications.lib.chalmers.se/records/fulltext/89572.pdf.
9. Agrawal, K., Makwana, H. (2015). A Study on Critical Capabilities for Security Information and Event Management. *International Journal of Science and Research (IJSR)*, 4(7), 1893-1896.
10. Berdibayev, R., Gnatyuk, S., Yevchenko, Yu., Kishchenko, V. (2021). A concept of the architecture and creation for SIEM system in critical infrastructure. *Studies in Systems, Decision and Control, 346*, 2021, 221-242.
11. Gnatyuk, S., Berdibayev, R., Avkurova, Z., Verkhovets, O., Bauyrzhan, M. (2021). Studies on cloud-based cyber incidents detection and identification in critical infrastructure. *CEUR Workshop Proceedings, 2923*, 68-80.
12. Lee, J.-H., Kim, Y. S., Kim, J. H., Kim, I. K. (2017). Toward the SIEM architecture for cloud-based security services. In *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE. https://doi.org/10.1109/cns.2017.8228696.
13. Miller, D., Harris, Sh., Harper, A., VanDyke, S., Blask, C. (2010). Security Information and Event Management (SIEM) Implementation. McGraw-Hill Osborne Media.
14. SIEM Analytics. http://www.siem.su/compare_SIEM_systems.php.
15. Lee, J.-H., Kim, Y. S., Kim, J. H., Kim, I. K. (2017). Toward the SIEM architecture for cloud-based security services. In *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE. https://doi.org/10.1109/cns.2017.8228696
16. Bachane, I., Adsi, Y. I. K., Adsi, H. C. (2016). Real time monitoring of security events for forensic purposes in Cloud environments using SIEM. In *2016 Third International Conference on Systems of Collaboration (SysCo)*. IEEE. https://doi.org/10.1109/sysco.2016.7831327
17. AlSabbagh, B., Kowalski, S. (2016). A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM). In *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE. https://doi.org/10.1109/eisic.2016.049.
18. Serckumecka, A., Medeiros, I., Bessani, A. (2019). Low-Cost Serverless SIEM in the Cloud. У *2019 38th Symposium on Reliable Distributed Systems (SRDS)*. IEEE. https://doi.org/10.1109/srds47363.2019.00057.
19. R Mahmoud, R.-V., Kidmose, E., Turkmen, A., Pilawka, O., Pedersen, J. M. (2021). DefAtt - Architecture of Virtual Cyber Labs for Research and Education. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE. https://doi.org/10.1109/cybersa52016.2021.9478236.