

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ
ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія моніторингу та управління інцидентами інформаційної безпеки»

зі спеціальності

125 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної програми

Інформаційна та кібернетична безпека

(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Нікіта БІДНИК

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62

БІДНИК Нікіта

(прізвище, ім'я)

Керівник

д.техніч.н., професор КАЗМІРЧУК

Світлана

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра Систем та технологій кібербезпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ

Завідувач кафедри

Систем та технологій
кібербезпеки

Галина ГАЙДУР
“___” жовтня 2025 року

**З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

БІДНИКУ Нікіті Сергійовичу

(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія моніторингу та управління
інцидентами інформаційної безпеки»

керівник кваліфікаційної роботи

Казмірчук Світлана Володимирівна,
д.техніч.н., професор

(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних
технологій від «___» жовтня 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 25.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи _____

інформаційні ресурси організації;

програмні платформи класу SIEM і SOAR, зокрема Wazuh та Shuffle;

наукова та технічна література, експлуатаційна документація, нормативні
документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно
розробити)

1. Аналіз актуальності проблеми моніторингу та управління інцидентами інформаційної безпеки в інформаційних системах організації.

2. Аналіз технологій автоматизації та оркестрації реагування на інциденти інформаційної безпеки (SOAR).

3. Технологія моніторингу та управління інцидентами інформаційної безпеки на базі інтеграції Wazuh і Shuffle.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми моніторингу та управління інцидентами інформаційної безпеки в інформаційних системах організації.	01.10.2025 р.	
2.	Аналіз наукової, нормативної та технічної літератури з питань моніторингу та управління інцидентами інформаційної безпеки.	15.10.2025 р.	
3.	Порівняльний аналіз SIEM- та SOAR-платформ та обґрунтування вибору Wazuh і Shuffle для побудови технології управління інцидентами.	06.11.2025 р.	
4.	Проектування архітектури технології та визначення її основних компонентів і функцій.	30.11.2025 р.	
5.	Розроблення технології моніторингу та управління інцидентами інформаційної безпеки на базі Wazuh і Shuffle.	17.12.2025 р.	
6.	Оформлення результатів дослідження.	24.12.2025 р.	
7.	Подання роботи на плагіат. Підготовка доповіді до захисту.	25.12.2025 р.	

Здобувач вищої освіти

(підпис)

Нікіта БІДНИК

(ім'я, прізвище)

Керівник кваліфікаційної роботи

(підпис)

Світлана КАЗМІРЧУК

(ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 96 сторінки, 3 рисунків, 4 таблиця, 12 джерел.

Об'єкт дослідження – процеси моніторингу та управління інцидентами інформаційної безпеки в інформаційних системах організації.

Предмет дослідження – технологія моніторингу та управління інцидентами інформаційної безпеки на базі SIEM-платформи Wazuh та SOAR-платформи Shuffle.

Мета роботи – розробити технологію моніторингу та управління інцидентами інформаційної безпеки, а також порядок її застосування з використанням інтеграції SIEM- та SOAR-рішень і надати рекомендації щодо практичної реалізації такої технології.

Методи дослідження – аналіз наукових публікацій та нормативних документів у сфері інформаційної безпеки, вивчення міжнародних стандартів управління інцидентами, аналіз експлуатаційної документації SIEM- і SOAR-платформ, моделювання процесів моніторингу та реагування, порівняльний аналіз технологічних рішень.

Технології класу SIEM забезпечують централізований збір, зберігання та кореляцію подій інформаційної безпеки з різних джерел, що дозволяє своєчасно виявляти інциденти та оцінювати їх критичність. Платформа Wazuh реалізує функції моніторингу журналів, контролю цілісності, аналізу конфігурацій та виявлення аномалій у поведінці систем. Використання агентної архітектури дозволяє здійснювати глибокий аналіз подій на рівні кінцевих вузлів і серверів.

SOAR-платформи доповнюють аналітичні можливості SIEM шляхом автоматизації та оркестрації реагування на інциденти. Платформа Shuffle забезпечує побудову сценаріїв реагування, координацію дій між компонентами інформаційної

інфраструктури та зменшення часу реагування за рахунок автоматизованого виконання типових операцій. Інтеграція Wazuh і Shuffle дозволяє сформувати єдину технологію управління інцидентами, що охоплює повний життєвий цикл інциденту – від виявлення до локалізації, ескалації та контролю виконання дій.

У роботі проаналізовано проблему ефективного моніторингу та управління інцидентами інформаційної безпеки, визначено її мету та основні завдання. Проведено аналіз сучасних підходів і технологій управління інцидентами, досліджено можливості SIEM- і SOAR-рішень та обґрунтовано вибір платформи Wazuh і Shuffle для побудови інтегрованої технології. Визначено призначення, основні функції та складові розробленої технології.

На основі проведених досліджень запропоновано технологію моніторингу та управління інцидентами інформаційної безпеки, розроблено порядок її практичного застосування в тестовому середовищі та сформульовано рекомендації для фахівців з кібербезпеки щодо впровадження й експлуатації інтегрованого SIEM–SOAR рішення.

Галузь використання – кібербезпека інформаційних систем та інформаційних ресурсів організації.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ,
МОНІТОРИНГ, УПРАВЛІННЯ ІНЦИДЕНТАМИ, SIEM, SOAR, WAZUH, SHUFFLE,
ТЕХНОЛОГІЯ МОНІТОРИНГУ ТА РЕАГУВАННЯ

ABSTRACT

Text part of the qualification work: 96 pages, 3 figures, 4 table, 12 sources.

Object of research – processes of monitoring and managing information security incidents in an organization's information systems.

Subject of research – a technology for monitoring and managing information security incidents based on the SIEM platform Wazuh and the SOAR platform Shuffle.

The aim of research – to develop a technology for monitoring and managing information security incidents, define the procedure for its application using SIEM and SOAR integration, and provide recommendations for its practical implementation.

Research methods – analysis of scientific publications in the field of information security, study of international incident management standards, analysis of operational documentation of SIEM and SOAR platforms, modeling of monitoring and response processes, and comparative analysis of technological solutions.

SIEM technologies provide centralized collection, storage, and correlation of security events from multiple sources, enabling timely detection of information security incidents and assessment of their criticality. The Wazuh platform implements log monitoring, file integrity monitoring, configuration assessment, and anomaly detection at the endpoint and server levels. Its agent-based architecture allows in-depth analysis of system activity and supports continuous security monitoring.

SOAR platforms extend SIEM capabilities by automating and orchestrating incident response processes. The Shuffle platform enables the creation of response workflows, coordination of actions across infrastructure components, and reduction of response time through automated execution of routine tasks. The integration of Wazuh and Shuffle makes it possible to build a unified incident management technology that covers the full incident life cycle, from detection and analysis to response, escalation, and control of mitigation actions.

The research analyzes the problem of effective monitoring and management of information security incidents, defines its objectives and tasks, and reviews existing approaches and technologies in this domain. The functional capabilities of SIEM and SOAR solutions are examined, and the choice of Wazuh and Shuffle as the technological basis for an integrated solution is justified. The purpose, main functions, and structure of the proposed technology are defined.

Based on the conducted research, a technology for monitoring and managing information security incidents is proposed, along with a procedure for its practical application in a test environment. Recommendations for cybersecurity specialists regarding the deployment and operation of the integrated SIEM–SOAR solution are developed.

Field of application – cybersecurity of organizational information systems and information resources.

INFORMATION SECURITY, INFORMATION SECURITY INCIDENT,
MONITORING, INCIDENT MANAGEMENT, SIEM, SOAR, WAZUH, SHUFFLE
SECURITY MONITORING AND RESPONSE TECHNOLOGY.

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	12
ВСТУП	13
1 АНАЛІЗ ПРОБЛЕМИ МОНІТОРИНГУ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	16
1.1 Інциденти інформаційної безпеки як об'єкт управління.....	16
1.2 Життєвий цикл інцидентів інформаційної безпеки.....	21
1.3 Моніторинг як технічна основа управління інцидентами	26
1.4 Проблеми управління інцидентами в сучасних організаціях.....	30
2 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ....	32
2.1 Технології класу SIEM у системах управління інцидентами інформаційної безпеки.....	32
2.2 Засоби збору подій та IDS/IPS як елементи моніторингу.....	41
2.3 Порівняльний аналіз SIEM-платформ.....	48
3 РОЗРОБКА ТЕХНОЛОГІЙ МОНІТОРИНГУ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ НА БАЗІ WAZUH + SHUFFLE	60
3.1 Архітектурна модель запропонованої технології	60
3.2 Функціональні компоненти технології та їх призначення.....	68
3.3 Технологічний процес моніторингу та управління інцидентами.....	76
3.4 Практична реалізація технології в тестовому середовищі.....	84
3.5 Оцінювання ефективності запропонованої технології.....	93
3.6 Обмеження запропонованої технології та напрями її подальшого розвитку.....	95
ВИСНОВКИ	97
ПЕРЕЛІК ПОСИЛАНЬ	99
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	100

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface
C2 – Command and Control
CIA – Confidentiality, Integrity, Availability
CVE – Common Vulnerabilities and Exposures
CVSS – Common Vulnerability Scoring System
EDR – Endpoint Detection and Response
FIM – File Integrity Monitoring
IDS – Intrusion Detection System
IPS – Intrusion Prevention System
IR – Incident Response
IT – Information Technology
JSON – JavaScript Object Notation
KPI – Key Performance Indicator
OS – Operating System
RBAC – Role-Based Access Control
SIEM – Security Information and Event Management
SOC – Security Operations Center
SOAR – Security Orchestration, Automation and Response
UEBA – User and Entity Behavior Analytics
WAF – Web Application Firewall
XDR – Extended Detection and Response

ВСТУП

Стрімкий розвиток інформаційних технологій, цифровізація бізнес-процесів і зростання залежності організацій від інформаційних систем супроводжуються постійним збільшенням кількості та складності кіберзагроз. Сучасні інформаційні системи характеризуються високою динамічністю, використанням хмарних сервісів, віддаленого доступу та розподіленої інфраструктури, що суттєво ускладнює забезпечення належного рівня інформаційної безпеки. У таких умовах зростає ймовірність виникнення інцидентів інформаційної безпеки, які можуть призводити до порушення конфіденційності, цілісності та доступності інформаційних ресурсів.

Традиційні підходи до забезпечення інформаційної безпеки, орієнтовані переважно на периметровий захист і ручний аналіз подій, дедалі частіше виявляються недостатньо ефективними. Велика кількість подій безпеки, різноманітність джерел даних і обмежені ресурси персоналу ускладнюють своєчасне виявлення інцидентів і оперативне реагування на них. У результаті інциденти можуть залишатися непоміченими протягом тривалого часу або оброблятися із суттєвою затримкою, що підвищує ризик негативних наслідків для організації.

У відповідь на ці виклики в сучасних системах кіберзахисту все більшого значення набувають технології централізованого моніторингу та управління інцидентами інформаційної безпеки. Системи класу SIEM забезпечують збір, зберігання та кореляцію подій безпеки з різних джерел, дозволяючи формувати цілісне уявлення про стан захищеності інформаційної інфраструктури. Водночас зростання обсягів даних і складності атак зумовлює потребу не лише у виявленні інцидентів, а й у швидкому та керованому реагуванні на них.

У цьому контексті важливу роль відіграють платформи класу SOAR, які забезпечують автоматизацію та оркестрацію процесів реагування на інциденти. Інтеграція SIEM- і SOAR-рішень дозволяє перейти від фрагментарного реагування до цілісної технології управління інцидентами, що охоплює повний життєвий цикл

інциденту — від виявлення та аналізу до локалізації, ескалації та контролю виконання дій. Такий підхід сприяє зменшенню часу реагування, зниженню навантаження на фахівців інформаційної безпеки та підвищенню загального рівня захищеності інформаційних систем.

Особливий інтерес у цьому аспекті становлять відкриті та гнучкі платформи моніторингу та реагування, зокрема SIEM-платформа Wazuh і SOAR-платформа Shuffle. Їх використання дозволяє реалізувати інтегровану технологію управління інцидентами безпеки, адаптовану до потреб організацій різного масштабу та рівня зрілості системи кіберзахисту.

Об'єкт дослідження – процеси моніторингу та управління інцидентами інформаційної безпеки в інформаційних системах організації.

Предмет дослідження – технологія моніторингу та управління інцидентами інформаційної безпеки на базі SIEM-платформи Wazuh та SOAR-платформи Shuffle.

Мета роботи – розробити технологію моніторингу та управління інцидентами інформаційної безпеки, визначити порядок її застосування з використанням інтеграції SIEM- та SOAR-платформ і надати рекомендації щодо її практичної реалізації

Наукові завдання:

дослідити сутність проблеми моніторингу та управління інцидентами інформаційної безпеки;

проаналізувати інциденти інформаційної безпеки як об'єкт управління, їх технічну природу та життєвий цикл;

проаналізувати сучасні підходи та технології моніторингу інцидентів інформаційної безпеки;

дослідити можливості SIEM- і SOAR-платформ у контексті управління інцидентами;

обґрунтувати вибір платформи Wazuh і Shuffle для реалізації інтегрованої технології;

розкрити порядок практичної реалізації технології моніторингу та управління інцидентами інформаційної безпеки;

оцінити ефективність запропонованої технології та визначити напрями її подальшого розвитку.

Методи дослідження – аналіз наукових і навчальних джерел з питань інформаційної безпеки, опрацювання міжнародних стандартів управління інцидентами, аналіз експлуатаційної та технічної документації SIEM- і SOAR-платформ, моделювання процесів моніторингу та реагування, порівняльний аналіз технологічних рішень.

Практичне значення одержаних результатів полягає в розробленні технології моніторингу та управління інцидентами інформаційної безпеки на базі Wazuh і Shuffle, а також у формуванні рекомендацій для фахівців з кібербезпеки щодо її впровадження та використання в інформаційних системах організацій.

1 АНАЛІЗ ПРОБЛЕМИ МОНІТОРИНГУ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інциденти інформаційної безпеки як об'єкт управління

У сучасних інформаційних системах інцидент інформаційної безпеки дедалі частіше розглядається не як одинична подія або ізольований технічний збій, а як повноцінний об'єкт управління, що потребує системного, керованого та формалізованого підходу. Така трансформація підходів зумовлена зростанням складності інфраструктур, обсягів оброблюваних даних і кількості взаємопов'язаних компонентів, у межах яких навіть незначні відхилення можуть мати суттєві наслідки.

Інцидент як об'єкт управління характеризується низкою параметрів, які визначають логіку його обробки. До таких параметрів належать рівень критичності, потенційний вплив на інформаційні активи, джерело виникнення, динаміка розвитку та поточний стан. Наявність цих параметрів дозволяє здійснювати пріоритизацію інцидентів і спрямовувати ресурси системи безпеки на найбільш небезпечні ситуації.

З організаційної точки зору управління інцидентами передбачає чіткий розподіл відповідальності та ролей. Інцидент як об'єкт управління має бути закріплений за певними підрозділами або посадовими особами, які відповідають за його обробку на різних етапах. Відсутність такого розподілу призводить до затримок у реагуванні та знижує загальну ефективність системи інформаційної безпеки.

Важливою особливістю сучасного підходу є інтеграція технічних і організаційних аспектів управління інцидентами. Інцидент не може бути ефективно оброблений лише технічними засобами або лише адміністративними процедурами. Необхідне поєднання автоматизованих інструментів моніторингу, аналітичних механізмів і чітко визначених регламентів дій персоналу.

У контексті автоматизації управління інцидентами особливого значення набуває формалізація процесів. Інцидент повинен бути представлений у вигляді

структури даних, придатної для обробки інформаційними системами. Це створює передумови для використання технологій класу SIEM і SOAR, у межах яких інциденти обробляються як керовані об'єкти з визначеними сценаріями реагування.

Інциденти інформаційної безпеки мають чітко виражену технічну природу, оскільки виникають у результаті функціонування конкретних компонентів інформаційної системи. Сучасні IT-інфраструктури являють собою складні, багаторівневі середовища, що поєднують операційні системи, мережеві компоненти, прикладні сервіси, бази даних і хмарні платформи. У таких умовах інцидент не є випадковою подією, а формується як наслідок взаємодії технічних процесів, конфігурацій і поведінки користувачів.

На рівні операційних систем технічна природа інцидентів проявляється через порушення штатних режимів роботи процесів, зміну системних файлів, несанкціоноване підвищення привілеїв або аномальну активність служб. Наприклад, запуск невідомого процесу з правами адміністратора або неочікувана зміна критичних системних бібліотек може свідчити про компрометацію хоста. Такі інциденти часто не мають миттєвих зовнішніх проявів, проте становлять серйозну загрозу для цілісності системи.

Мережевий рівень є ще одним ключовим джерелом технічних інцидентів. Передача даних між компонентами інформаційної системи супроводжується великою кількістю мережевих подій, серед яких можуть бути як легітимні з'єднання, так і ознаки атак. Аномальна мережева активність, нетипові порти, незвичні напрямки трафіку або різке зростання кількості з'єднань можуть свідчити про спроби несанкціонованого доступу, розвідку мережі або підготовку до атаки. У таких випадках інцидент формується не на основі однієї події, а шляхом аналізу сукупності мережевих характеристик.

Особливу роль у формуванні інцидентів відіграють прикладні сервіси та бізнес-додатки. Помилки в логіці обробки запитів, некоректна обробка введених даних або відсутність належних механізмів автентифікації створюють умови для виникнення

інцидентів, пов'язаних із витоком даних або порушенням доступності сервісів. У сучасних веб-орієнтованих системах такі інциденти можуть розвиватися поступово та маскуватися під звичайну активність користувачів.

Технічна природа інцидентів тісно пов'язана з журналюванням подій. Кожен компонент інформаційної системи генерує журнали, що відображають його стан і виконувані дії. Саме ці журнали є основним джерелом даних для виявлення інцидентів. Проте у реальних умовах журнали мають різний формат, рівень деталізації та якість, що ускладнює їх об'єднання й аналіз. Інцидент у такому середовищі виникає як результат кореляції подій із різних джерел, а не як ізольований запис у журналі.

Хмарні та гібридні інфраструктури значно ускладнюють технічну картину інцидентів. Розподіленість ресурсів, динамічність середовищ і залежність від зовнішніх сервісів створюють нові типи інцидентів, пов'язані з помилками конфігурації доступу, неконтрольованим масштабуванням або витоком облікових даних. У таких умовах інцидент може охоплювати одночасно локальну інфраструктуру та хмарні сервіси, що потребує централізованого технічного підходу до моніторингу.

Класифікація інцидентів інформаційної безпеки є необхідною умовою для побудови ефективної системи автоматизованого управління. В умовах сучасних інформаційних систем кількість подій і потенційних інцидентів є настільки великою, що їх ручна обробка стає практично неможливою. Саме тому інциденти мають бути впорядковані за визначеними ознаками, які дозволяють формалізувати процеси аналізу та реагування.

З точки зору автоматизованого управління інцидентами важливо не лише визначити тип інциденту, а й оцінити можливість його обробки без безпосередньої участі людини. Деякі інциденти мають чітко визначені ознаки, повторюваний характер і стандартні методи реагування, що робить їх придатними для автоматизації. Інші ж інциденти є складними, контекстно залежними та потребують експертної оцінки, що обмежує можливості їх повної автоматизації.

Однією з ключових ознак класифікації є рівень критичності інциденту. Інциденти з низьким рівнем критичності, як правило, не мають значного впливу на функціонування інформаційної системи та можуть оброблятися автоматично з мінімальним ризиком. Інциденти середньої критичності потребують поєднання автоматизованих дій і контролю з боку персоналу. Інциденти високої критичності, навпаки, вимагають залучення фахівців і прийняття управлінських рішень на вищому рівні.

Важливою ознакою класифікації є також джерело виникнення інциденту. Інциденти, що виникають унаслідок зовнішнього впливу, часто мають ознаки атак і потребують швидкої локалізації. Внутрішні інциденти, спричинені помилками персоналу або зловживанням привілеями, можуть бути менш очевидними та потребувати детальнішого аналізу. З точки зору автоматизації такі інциденти складніше формалізувати, оскільки вони часто залежать від поведінкового контексту.

Ще одним критично важливим аспектом є повторюваність інцидентів. Інциденти, що регулярно виникають за однаковим сценарієм, є ідеальними кандидатами для автоматизованої обробки. Натомість унікальні або нетипові інциденти потребують індивідуального підходу та залучення експертів. Таким чином, класифікація дозволяє визначити, які інциденти можуть бути включені до стандартних сценаріїв реагування, а які мають оброблятися вручну.

З урахуванням наведених аспектів доцільно представити узагальнену класифікацію інцидентів інформаційної безпеки з точки зору автоматизованого управління у вигляді таблиці.

Таблиця 1.1.

Класифікація інцидентів інформаційної безпеки з точки зору автоматизованого управління

Ознака класифікації	Тип інциденту	Характеристика	Можливість автоматизації
Рівень критичності	Низький	Мінімальний вплив на систему,	Висока

		відсутність прямих наслідків	
	Середній	Потенційний вплив на окремі компоненти	Часткова
	Високий	Значний вплив на систему або бізнес-процеси	Низька
Джерело виникнення	Зовнішній	Ознаки атаки ззовні, мережеві або сервісні впливи	Середня
	Внутрішній	Помилки або зловживання з боку користувачів	Низька
Повторюваність	Типовий	Регулярно повторювані сценарії	Висока
	Нетиповий	Унікальні або рідкісні випадки	Низька
Рівень формалізації	Формалізований	Чіткі правила виявлення та реагування	Висока
	Контекстний	Потребує аналізу поведінки та середовища	Часткова
Наслідки	Локальні	Обмежені окремим вузлом або сервісом	Висока
	Системні	Впливають на декілька компонентів	Часткова

Представлена класифікація дозволяє структуровано підходити до побудови автоматизованої системи управління інцидентами. Вона створює основу для розробки сценаріїв реагування, визначення рівнів ескалації та оптимального розподілу ресурсів між автоматизованими та ручними процесами. Саме така класифікація є ключовою

для впровадження технологій класу SIEM і SOAR, у межах яких інциденти обробляються як керовані об'єкти з наперед визначеними характеристиками.

1.2. Життєвий цикл інцидентів інформаційної безпеки

Формування інцидентів інформаційної безпеки є складним багатоступеневим процесом, який починається задовго до моменту їх явного прояву. У сучасних інформаційних системах інцидент не виникає раптово, а формується поступово внаслідок накопичення технічних і поведінкових відхилень. Саме тому етап виявлення інцидентів є критично важливим і визначає ефективність усієї системи управління безпекою.

Початковою фазою формування інциденту є поява окремих подій, які фіксуються компонентами інформаційної інфраструктури. До таких подій належать системні повідомлення операційних систем, журнали мережевого обладнання, записи вебсерверів, баз даних, засобів автентифікації та прикладних сервісів. Кожна з цих подій окремо не свідчить про наявність інциденту, проте в сукупності вони можуть утворювати характерний шаблон небезпечної активності.

На етапі формування інциденту ключову роль відіграє контекст. Одна й та сама подія може мати різне значення залежно від середовища, часу виникнення та попередньої історії активності. Наприклад, спроба входу до системи поза робочим часом може бути нормальною для адміністратора, але підозрілою для звичайного користувача. Таким чином, інцидент формується не лише на основі факту події, а через її інтерпретацію в контексті поведінки системи та користувачів.

Виявлення інцидентів у системах моніторингу ґрунтується на аналізі великих обсягів різномірних даних. У реальних умовах інформаційні системи генерують тисячі або мільйони подій на добу, що унеможлиблює їх ручний аналіз. Це зумовлює необхідність використання автоматизованих механізмів фільтрації, нормалізації та

кореляції подій. Саме на цьому етапі системи моніторингу відіграють роль первинного інструмента виявлення потенційних інцидентів.

Важливою особливістю сучасних систем моніторингу є використання різних методів виявлення інцидентів. До них належать порогові методи, сигнатурний аналіз, кореляційні правила та поведінкові підходи. Кожен із цих методів має свої переваги та обмеження. Порогові методи прості в реалізації, але неефективні для складних атак. Сигнатурний аналіз дозволяє виявляти відомі загрози, проте є малоефективним проти нових або модифікованих атак. Поведінкові методи, навпаки, дозволяють виявляти нетипову активність, але потребують більш складної аналітики.

У процесі виявлення інцидентів важливу роль відіграє часовий аспект. Деякі інциденти мають короткочасний характер і потребують негайного реагування, інші ж можуть розвиватися протягом тривалого часу. Системи моніторингу повинні забезпечувати як оперативне виявлення критичних інцидентів, так і можливість аналізу довготривалих тенденцій. Це дозволяє не лише реагувати на вже сформовані інциденти, а й виявляти ознаки потенційних загроз на ранніх етапах.

З точки зору управління інцидентами етап виявлення є перехідною ланкою між технічним моніторингом і процесами реагування. Саме на цьому етапі визначається, чи буде сукупність подій класифікована як інцидент і передана на подальшу обробку. Помилки на цьому етапі можуть призводити як до надмірної кількості хибних інцидентів, так і до пропуску реальних загроз.

Після етапу виявлення інцидентів ключовим елементом життєвого циклу є їх аналіз і підтвердження. На цьому етапі здійснюється перехід від первинної технічної індикації до усвідомленого рішення про наявність або відсутність інциденту інформаційної безпеки. Саме тут визначається, чи є зафіксована активність реальною загрозою, чи вона належить до категорії хибних або малозначущих спрацювань.

Аналіз інциденту передбачає глибоке вивчення сукупності подій, які стали підставою для його формування. Окремі події рідко дають повну картину ситуації, тому аналіз здійснюється з урахуванням часових зв'язків, джерел подій, задіяних

облікових записів, мережевих адрес і контексту функціонування системи. На цьому етапі важливу роль відіграє кореляція подій, яка дозволяє об'єднати розрізнені сигнали в єдину логічну послідовність.

Підтвердження інциденту полягає у визначенні того, чи відповідає зафіксована активність критеріям інциденту інформаційної безпеки. Це рішення базується не лише на технічних ознаках, а й на оцінці потенційного впливу на інформаційні активи. Наприклад, одна й та сама подія може бути класифікована по-різному залежно від того, який саме ресурс було задіяно та яку роль він відіграє в інформаційній системі.

Суттєвим викликом на цьому етапі є велика кількість хибнопозитивних спрацювань. Надмірна кількість таких спрацювань призводить до перевантаження персоналу та зниження уваги до реальних загроз. Саме тому процес підтвердження інцидентів має бути максимально формалізованим і підтримуватись автоматизованими інструментами аналізу.

Після підтвердження інциденту здійснюється його пріоритизація. Пріоритизація визначає черговість обробки інцидентів і є критично важливою в умовах обмежених ресурсів. Неможливо одночасно реагувати на всі інциденти з однаковою інтенсивністю, тому необхідно визначити ті з них, що потребують негайного втручання.

Пріоритизація ґрунтується на поєднанні декількох факторів, серед яких ключовими є рівень критичності інциденту, ймовірність його розвитку та можливі наслідки. Інциденти, що загрожують цілісності або доступності критичних ресурсів, повинні оброблятися в першу чергу. Водночас менш критичні інциденти можуть бути відкладені або оброблені автоматично.

У практичних системах управління інцидентами пріоритизація часто реалізується у вигляді числових або категоріальних оцінок, які дозволяють швидко порівнювати інциденти між собою. Такий підхід спрощує прийняття рішень і створює основу для автоматизації процесів реагування.

Таблиця 1.2.

Критерії аналізу, підтвердження та пріоритизації інцидентів інформаційної безпеки

Критерій	Опис	Вплив на рішення
Джерело подій	Внутрішні або зовнішні джерела активності	Визначення типу інциденту
Кількість подій	Обсяг і частота зафіксованих подій	Виявлення аномалій
Контекст	Час, роль користувача, тип ресурсу	Підтвердження інциденту
Потенційний вплив	Наслідки для інформаційних активів	Визначення критичності
Повторюваність	Типовість або унікальність сценарію	Можливість автоматизації
Стан інциденту	Початковий, активний, локалізований	Визначення пріоритету

Після підтвердження та пріоритизації інциденту інформаційної безпеки ключовим етапом життєвого циклу є реагування. Саме на цьому етапі здійснюється активний вплив на ситуацію з метою обмеження наслідків інциденту, запобігання його подальшому розвитку та мінімізації шкоди для інформаційних активів. Ефективність реагування значною мірою визначає загальний рівень захищеності системи та стійкість організації до інцидентів.

Реагування на інцидент передбачає виконання сукупності технічних і організаційних дій, спрямованих на локалізацію загрози. До таких дій можуть належати ізоляція скомпрометованого вузла, блокування облікового запису, обмеження мережевого доступу або зупинка окремих сервісів. Вибір конкретних заходів залежить від типу інциденту, його критичності та поточного стану розвитку. У цьому контексті важливо забезпечити баланс між швидкістю реагування та ризиком порушення штатного функціонування системи.

Однією з основних проблем реагування є часовий фактор. Чим довше інцидент залишається активним, тим більшими можуть бути його наслідки. Тому сучасні

підходи до управління інцидентами орієнтовані на скорочення часу між виявленням інциденту та виконанням перших дій реагування. Це створює передумови для автоматизації реагування, особливо для типових і повторюваних сценаріїв.

Після локалізації інциденту настає етап відновлення. Його метою є повернення інформаційної системи до штатного режиму роботи та усунення наслідків інциденту. Відновлення може включати відновлення даних із резервних копій, перевірку цілісності системних компонентів, повторну конфігурацію сервісів або оновлення програмного забезпечення. На цьому етапі важливо не лише відновити працездатність, а й переконатися, що першопричини інциденту усунені.

Відновлення є тісно пов'язаним із контролем змін у системі. Некоректно виконані дії відновлення можуть створити нові вразливості або повторно активувати інцидент. Саме тому цей етап потребує чітко визначених процедур і, за можливості, автоматизованих механізмів перевірки стану системи після виконання відновлювальних дій.

Завершальним, але не менш важливим етапом життєвого циклу інциденту є накопичення досвіду та аналіз результатів. Кожен інцидент містить цінну інформацію про слабкі місця системи, ефективність механізмів захисту та адекватність процедур реагування. Аналіз інцидентів після їх завершення дозволяє виявляти системні проблеми та вдосконалювати політики інформаційної безпеки.

Накопичення досвіду передбачає документування інцидентів, збереження журналів, опис виконаних дій та оцінку їх результативності. Ці дані можуть використовуватися для оновлення правил виявлення, кореляційних сценаріїв і процедур реагування. Таким чином, система управління інцидентами поступово адаптується до нових загроз і підвищує свою ефективність.

У контексті автоматизованого управління інцидентами етапи реагування, відновлення та накопичення досвіду є найбільш перспективними для впровадження технологій класу SOAR. Формалізація сценаріїв реагування та інтеграція аналітичних і виконавчих компонентів дозволяють скоротити час реагування,

зменшити навантаження на персонал і підвищити загальну керованість процесів інформаційної безпеки.

1.3. Моніторинг як технічна основа управління інцидентами

Ефективність моніторингу інцидентів інформаційної безпеки безпосередньо залежить від повноти, якості та різноманітності джерел даних, що використовуються для аналізу стану інформаційної системи. Інциденти не виникають у вакуумі, а завжди залишають технічні сліди у вигляді подій, журналів або змін у поведінці системних компонентів. Саме ці сліди формують основу для виявлення, аналізу та подальшого управління інцидентами.

Основними джерелами даних безпеки є журнали операційних систем. Операційна система виступає центральною ланкою будь-якої інформаційної системи, тому більшість критичних подій фіксується саме на цьому рівні. Журнали автентифікації, керування процесами, доступу до файлів і зміни системних налаштувань дозволяють виявляти ознаки несанкціонованого доступу, спроби підвищення привілеїв або виконання нетипових дій. Аналіз таких журналів дає змогу простежити ланцюг подій, що передували інциденту, та визначити його першопричини.

Не менш важливими є журнали мережевих пристроїв і сервісів. Маршрутизатори, комутатори, міжмережеві екрани та системи виявлення вторгнень генерують інформацію про мережеву активність, яка є критичною для виявлення атак і аномалій. Дані про спроби встановлення з'єднань, використання нестандартних портів, зміну маршрутів або блокування трафіку дозволяють виявляти як зовнішні атаки, так і внутрішні порушення політик безпеки.

Прикладні сервіси та бізнес-додатки формують окремий клас джерел даних безпеки. Саме на рівні додатків відбувається безпосередня робота з інформаційними активами, тому журнали вебсерверів, серверів додатків і баз даних є надзвичайно

цінними для виявлення інцидентів, пов'язаних із витоком або модифікацією даних. Аномальна активність користувачів, помилки доступу або нетипові запити можуть свідчити про спроби експлуатації вразливостей або зловмисні дії.

Окрему категорію джерел становлять засоби контролю автентифікації та управління доступом. Системи централізованої автентифікації, такі як служби каталогів або сервіси єдиного входу, надають інформацію про використання облікових записів, спроби входу та зміну прав доступу. Дані з цих систем дозволяють виявляти компрометацію облікових записів, використання викрадених облікових даних і порушення принципу мінімальних привілеїв.

У розподілених і хмарних середовищах додатковими джерелами даних стають журнали хмарних сервісів і платформ управління інфраструктурою. Події, пов'язані зі створенням ресурсів, зміною конфігурацій або доступом до хмарних сервісів, можуть містити ознаки серйозних інцидентів, пов'язаних із помилками налаштування або зловживанням доступом. У таких умовах моніторинг має охоплювати як локальні, так і віддалені компоненти інфраструктури.

Сучасні інформаційні системи дедалі частіше мають розподілену або гібридну архітектуру, що включає локальні сервери, віддалені філії, хмарні сервіси та мобільні робочі станції. У таких умовах моніторинг інформаційної безпеки ускладнюється не лише зростанням кількості компонентів, а й різноманіттям технологій, протоколів і середовищ виконання. Розподіленість інфраструктури безпосередньо впливає на можливість своєчасного виявлення інцидентів і ефективність реагування.

Децентралізований підхід до моніторингу, за якого кожен компонент системи аналізується окремо, не дозволяє сформувати цілісну картину стану безпеки. Події, що виникають у різних сегментах інфраструктури, залишаються ізольованими, а їх взаємозв'язки не враховуються. У результаті складні інциденти, які розвиваються поетапно та охоплюють декілька компонентів, можуть залишатися непоміченими або бути виявленими із запізненням.

Централізований моніторинг покликаний вирішити цю проблему шляхом об'єднання даних з усіх компонентів інфраструктури в єдиному аналітичному просторі. Такий підхід дозволяє здійснювати кореляцію подій, аналізувати поведінкові шаблони та виявляти інциденти, що не можуть бути ідентифіковані на рівні окремих вузлів. Централізація також спрощує управління правилами виявлення та знижує ризик розбіжностей у налаштуваннях безпеки.

У розподілених інфраструктурах особливу складність становить збір даних. Компоненти можуть бути розміщені в різних мережевих сегментах, мати обмежений доступ або працювати в середовищах із підвищеними вимогами до ізоляції. У таких умовах централізований моніторинг потребує використання агентних або безагентних механізмів збору подій, а також забезпечення захищених каналів передачі даних.

Ще одним викликом є різноманітність форматів і структур журналів. Події, що надходять з операційних систем, мережевого обладнання, прикладних сервісів і хмарних платформ, мають різний формат і рівень деталізації. Без нормалізації таких даних централізований аналіз стає малоефективним. Саме тому централізований моніторинг передбачає попередню обробку подій, яка включає приведення їх до уніфікованого вигляду та збагачення контекстною інформацією.

Важливим аспектом централізованого моніторингу є масштабованість. У міру зростання інфраструктури збільшується обсяг подій, що надходять до системи моніторингу. Якщо архітектура не розрахована на таке зростання, це може призвести до втрати подій, затримок у їх обробці або зниження якості аналізу. Тому при побудові централізованого моніторингу необхідно враховувати можливість горизонтального масштабування та оптимізації обробки даних.

Централізований підхід також має організаційні переваги. Наявність єдиного центру моніторингу спрощує координацію дій персоналу, дозволяє стандартизувати процеси реагування та зменшує залежність від окремих фахівців. У межах такого

підходу формується єдине уявлення про стан інформаційної безпеки організації, що є критично важливим для прийняття управлінських рішень.

Разом із тим централізований моніторинг має і певні обмеження. Він може створювати єдину точку відмови, а також вимагати значних ресурсів для зберігання та обробки даних. Крім того, затримки в передачі подій з віддалених сегментів можуть впливати на оперативність виявлення інцидентів. Ці фактори потребують врахування при проєктуванні архітектури моніторингу.

Традиційні системи моніторингу інформаційної безпеки історично орієнтовані на збір і візуалізацію подій, а також на сповіщення персоналу про потенційні порушення. Такий підхід був ефективним на ранніх етапах розвитку інформаційних систем, коли інфраструктури мали обмежену складність, а кількість подій залишалася відносно невеликою. Однак у сучасних умовах цей підхід виявляє суттєві обмеження, які знижують ефективність управління інцидентами.

Обмежені можливості кореляції подій є ще одним недоліком традиційного підходу. Без автоматизованого аналізу складних взаємозв'язків між подіями інциденти, що розвиваються поступово або мають багатоступеневий характер, можуть залишатися непоміченими. У таких випадках моніторинг фіксує лише окремі фрагменти активності, не формуючи цілісної картини загрози.

Ще одним обмеженням є складність масштабування. Зі зростанням інфраструктури та кількості подій традиційні системи моніторингу потребують пропорційного збільшення штату персоналу. Такий підхід є економічно неефективним і не відповідає сучасним вимогам до гнучкості та адаптивності систем інформаційної безпеки.

Важливою проблемою є відсутність зворотного зв'язку між етапами життєвого циклу інциденту. У традиційних системах результати реагування та аналізу інцидентів рідко використовуються для автоматичного вдосконалення механізмів виявлення. Це обмежує можливості самоадаптації системи безпеки та знижує її здатність ефективно протидіяти новим загрозам.

У сукупності наведені обмеження свідчать про те, що традиційний моніторинг без автоматизації реагування не відповідає сучасним вимогам до управління інцидентами інформаційної безпеки. Він забезпечує лише частковий контроль над ситуацією та не дозволяє реалізувати проактивний підхід до захисту інформаційних систем.

1.4. Проблеми управління інцидентами в сучасних організаціях

Однією з ключових перешкод ефективного управління інцидентами інформаційної безпеки в сучасних організаціях є сукупність технічних проблем, що виникають у процесі збору, аналізу та обробки даних безпеки. Зростання складності інформаційних систем, інтеграція різнорідних технологій і постійне збільшення обсягів подій створюють середовище, у якому традиційні підходи до обробки інцидентів стають малоефективними.

Першочерговою технічною проблемою є надмірний обсяг подій, що генеруються компонентами інформаційної інфраструктури. Операційні системи, мережеві пристрої, прикладні сервіси та засоби захисту постійно формують журнали, які можуть містити тисячі записів за короткий проміжок часу. Без відповідних механізмів фільтрації та агрегації такі обсяги даних ускладнюють виявлення інцидентів і призводять до перевантаження аналітичних систем.

Технічні проблеми також виникають у процесі кореляції подій. Побудова ефективних кореляційних правил потребує глибокого розуміння логіки функціонування інформаційної системи та можливих сценаріїв атак. Неправильно налаштовані правила можуть призводити як до пропуску реальних інцидентів, так і до генерації великої кількості хибних спрацювань. Це ускладнює подальшу обробку інцидентів і негативно впливає на довіру до системи моніторингу.

Окрему проблему становить обмежена масштабованість технічних засобів. У міру розвитку інфраструктури зростає кількість джерел даних і обсяг інформації, що

потребує обробки. Якщо архітектура системи управління інцидентами не передбачає масштабування, це може призвести до затримок у аналізі подій або втрати частини даних. Такі ситуації є особливо небезпечними в умовах активних атак, коли своєчасність реагування має критичне значення.

Суттєвим обмеженням є також відсутність єдиного інформаційного простору для управління інцидентами. Дані про події, інциденти та виконані дії часто зберігаються в різних системах і форматах, що ускладнює аналіз ситуації та прийняття обґрунтованих рішень. У таких умовах навіть досвідчені фахівці можуть втрачати цілісне уявлення про розвиток інциденту, що знижує ефективність реагування.

У відповідь на зазначені виклики виникає об'єктивна необхідність переходу до інтегрованих технологій управління інцидентами, які поєднують можливості моніторингу, аналізу та автоматизованого реагування. Саме таку інтеграцію забезпечують технології класу SIEM і SOAR, що доповнюють одна одну та формують єдину керовану систему.

Технології SIEM орієнтовані на централізований збір, нормалізацію та кореляцію подій безпеки з різних джерел. Вони дозволяють формувати інциденти на основі комплексного аналізу даних і забезпечують єдине представлення стану безпеки інформаційної системи. Проте можливості SIEM обмежуються переважно етапами виявлення та аналізу інцидентів і не охоплюють повний цикл реагування.

Технології SOAR, у свою чергу, спрямовані на автоматизацію процесів реагування, оркестрацію дій і підтримку прийняття рішень. Вони дозволяють формалізувати сценарії реагування, зменшити залежність від ручних операцій і забезпечити узгодженість дій персоналу. Без інтеграції з SIEM такі технології не мають достатньої інформаційної бази для ефективного функціонування.

Інтеграція SIEM і SOAR дозволяє усунути розрив між виявленням і реагуванням на інциденти. У межах такої інтегрованої технології інцидент розглядається як керований об'єкт, що проходить усі етапи життєвого циклу в єдиному

інформаційному середовищі. Це забезпечує скорочення часу реагування, підвищення точності рішень і зменшення навантаження на персонал.

Крім того, інтегровані технології створюють умови для накопичення та повторного використання досвіду реагування на інциденти. Дані про попередні інциденти, виконані дії та їх результати можуть використовуватися для вдосконалення правил виявлення, сценаріїв реагування та політик безпеки. Таким чином, система управління інцидентами набуває здатності до самоадаптації та постійного розвитку.

Узагальнюючи наведене, можна зробити висновок, що перехід до інтегрованих технологій SIEM та SOAR є не просто доцільним, а необхідним етапом розвитку систем управління інформаційною безпекою. Такий перехід дозволяє подолати обмеження традиційних підходів, забезпечити цілісність управління інцидентами та створити основу для впровадження ефективної технології моніторингу та автоматизованого реагування.

2 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Технології класу SIEM у системах управління інцидентами інформаційної безпеки

У сучасних умовах функціонування інформаційних систем забезпечення належного рівня інформаційної безпеки неможливе без використання спеціалізованих технологій централізованого моніторингу та аналізу подій. Технології класу SIEM стали відповіддю на зростання складності IT-інфраструктур, збільшення кількості джерел подій і необхідність оперативного управління інцидентами інформаційної безпеки. Їх призначення полягає у створенні єдиного аналітичного середовища, в межах якого здійснюється збір, обробка та інтерпретація даних безпеки.

Роль SIEM у сучасних системах інформаційної безпеки полягає насамперед у подоланні фрагментарності моніторингу. У типовій організації події безпеки генеруються великою кількістю різнорідних компонентів, включаючи сервери, робочі станції, мережеві пристрої, прикладні сервіси та засоби захисту. Без централізованого підходу ці події аналізуються ізольовано, що унеможлиблює виявлення складних інцидентів, які розвиваються поетапно та охоплюють декілька сегментів інфраструктури.

SIEM забезпечує агрегацію подій у єдиному просторі та створює умови для їх подальшого аналізу. Це дозволяє сформувати цілісне уявлення про стан інформаційної безпеки організації в режимі, наближеному до реального часу. Завдяки цьому інциденти можуть бути виявлені на ранніх стадіях, ще до того, як вони призведуть до суттєвих негативних наслідків.

Важливою функцією SIEM є підтримка процесів управління інцидентами. У межах такої технології інцидент формується не як випадковий сигнал, а як результат аналітичної обробки сукупності подій. Це дозволяє перейти від реактивного підходу, заснованого на ручному аналізі окремих повідомлень, до керованого процесу, у якому інциденти мають визначені характеристики, рівні пріоритету та подальші сценарії обробки.

З позиції управління інформаційною безпекою SIEM виконує роль аналітичного ядра, що забезпечує підтримку прийняття рішень. Аналітики безпеки отримують можливість не лише переглядати окремі події, а й аналізувати тенденції, взаємозв'язки та історію розвитку інцидентів. Це особливо важливо для розслідування складних інцидентів і виявлення системних проблем у захисті інформаційних активів.

Роль SIEM також полягає у забезпеченні відповідності вимогам нормативних документів і стандартів інформаційної безпеки. Централізоване зберігання журналів і можливість їх аналізу дозволяють підтверджувати факт виконання вимог щодо моніторингу, аудиту та реагування на інциденти. У цьому контексті SIEM виступає не

лише як технічний засіб, а і як елемент системи управління інформаційною безпекою організації.

Окремої уваги заслуговує роль SIEM у зниженні впливу людського фактора. Автоматизація збору та первинного аналізу подій дозволяє скоротити обсяг ручної роботи та зменшити ризик помилок, пов'язаних із перевантаженням персоналу. Водночас SIEM не замінює фахівців з інформаційної безпеки, а забезпечує їх інструментами для більш ефективної роботи з великими обсягами даних.

Архітектура SIEM-систем визначає їх здатність ефективно обробляти великі обсяги даних безпеки, забезпечувати своєчасне виявлення інцидентів і підтримувати процеси управління інформаційною безпекою в умовах складних і розподілених інфраструктур. Саме архітектурні рішення визначають масштабованість, надійність і функціональні можливості SIEM, а також їх придатність для інтеграції з іншими засобами захисту.

Типова архітектура SIEM складається з декількох логічних рівнів, кожен з яких виконує власну функцію в процесі обробки подій безпеки. До таких рівнів належать рівень збору даних, рівень обробки та нормалізації, аналітичний рівень і рівень зберігання та представлення інформації. Чітке розмежування функцій між цими рівнями дозволяє забезпечити гнучкість і масштабованість системи.

Рівень збору даних є початковою ланкою архітектури SIEM. На цьому рівні здійснюється прийом подій із різноманітних джерел, включаючи операційні системи, мережеве обладнання, прикладні сервіси та засоби захисту. Збір може здійснюватися як за допомогою агентів, встановлених на кінцевих вузлах, так і безагентними методами, наприклад через мережеві протоколи журналювання. Вибір підходу залежить від типу інфраструктури та вимог до деталізації подій.

Наступним елементом архітектури є рівень попередньої обробки та нормалізації даних. Оскільки події надходять у різних форматах і з різним рівнем структурованості, SIEM виконує їх перетворення до уніфікованого вигляду. Нормалізація дозволяє звести події до єдиної моделі даних, що є необхідною умовою для подальшого

кореляційного та поведінкового аналізу. На цьому ж етапі може виконуватися збагачення подій додатковою інформацією, наприклад даними про користувачів або критичність ресурсів.

Аналітичний рівень є центральним елементом архітектури SIEM. Саме тут реалізуються механізми кореляції подій, виявлення аномалій і формування інцидентів інформаційної безпеки. Аналітичні компоненти обробляють як поточні, так і історичні дані, що дозволяє виявляти складні сценарії атак і довготривалі аномальні тенденції. Ефективність цього рівня значною мірою залежить від правильної побудови кореляційних правил і використання контекстної інформації.

Рівень зберігання даних забезпечує довготривале збереження подій і інцидентів. Архітектурні рішення на цьому рівні мають враховувати вимоги до обсягу зберігання, швидкості доступу та надійності. У сучасних SIEM часто використовуються розподілені сховища, які дозволяють масштабувати систему шляхом додавання нових вузлів. Це є критично важливим для обробки великих обсягів даних у реальному часі.

Окрему роль в архітектурі SIEM відіграє рівень представлення інформації та взаємодії з користувачем. Інтерфейси управління, панелі моніторингу та засоби формування звітів дозволяють аналітикам безпеки отримувати узагальнену інформацію про стан системи, переглядати інциденти та аналізувати події. Зручність і інформативність цього рівня безпосередньо впливають на ефективність роботи персоналу.

З точки зору фізичної реалізації архітектура SIEM може бути централізованою або розподіленою. Централізовані архітектури простіші в управлінні, проте мають обмеження щодо масштабованості та відмовостійкості. Розподілені архітектури, навпаки, дозволяють обробляти великі обсяги даних і забезпечують високу надійність, але потребують складнішого адміністрування та налаштування.

Важливим аспектом архітектури SIEM є інтеграція з іншими системами інформаційної безпеки. SIEM повинна мати можливість обмінюватися даними з IDS/IPS, засобами захисту кінцевих точок, системами управління доступом і

платформами автоматизованого реагування. Така інтеграція реалізується через стандартні інтерфейси та протоколи, що дозволяє будувати комплексні технології управління інцидентами.

Архітектурні рішення також визначають здатність SIEM підтримувати автоматизацію процесів. Чітке розмежування компонентів і наявність програмних інтерфейсів створюють умови для подальшої інтеграції з SOAR-платформами та реалізації сценаріїв автоматизованого реагування. У цьому контексті архітектура SIEM є не лише технічним, а й концептуальним елементом системи управління інцидентами.

Збір подій безпеки є базовим технічним процесом, на якому ґрунтується функціонування будь-якої SIEM-системи. Саме на цьому етапі формується первинний масив даних, що в подальшому використовується для аналізу, кореляції та формування інцидентів інформаційної безпеки. Якість і повнота зібраних подій безпосередньо визначають ефективність усіх наступних етапів управління інцидентами.

Події безпеки генеруються практично всіма компонентами інформаційної інфраструктури. До основних джерел належать операційні системи серверів і робочих станцій, мережеві пристрої, системи керування доступом, прикладні сервіси, бази даних, а також спеціалізовані засоби захисту. Кожне з цих джерел формує власні журнали подій, що відрізняються за форматом, рівнем деталізації та семантичним змістом.

У SIEM-системах застосовуються два основних підходи до збору подій: агентний і безагентний. Агентний підхід передбачає встановлення спеціалізованого програмного забезпечення на контрольованих вузлах. Такі агенти забезпечують глибокий доступ до системних журналів, можуть фільтрувати події на локальному рівні та передавати їх у централізоване сховище. Перевагою цього підходу є висока деталізація подій і можливість контролю цілісності даних, однак він потребує додаткових ресурсів і складніший в адмініструванні.

Безагентний підхід базується на використанні стандартних механізмів журналювання та мережевих протоколів передачі подій. У цьому випадку компоненти інфраструктури надсилають журнали безпосередньо до SIEM або проміжних колекторів. Такий підхід спрощує розгортання системи, але може обмежувати глибину аналізу та контроль над якістю зібраних даних. Вибір між агентним і безагентним підходами залежить від архітектури інфраструктури та вимог до моніторингу.

Після збору подій ключовим етапом є їх нормалізація. Нормалізація полягає у приведенні подій із різних джерел до єдиного формату та структури. Оскільки кожне джерело використовує власні поля, назви параметрів і коди подій, без нормалізації автоматизований аналіз був би практично неможливим. SIEM-система виконує перетворення сирих подій у стандартизовані записи, що містять уніфікований набір атрибутів.

Нормалізація також передбачає інтерпретацію значень полів і їх семантичне узгодження. Наприклад, події автентифікації з різних операційних систем можуть містити різні коди помилок або статуси входу. У процесі нормалізації ці значення приводяться до єдиного набору категорій, що дозволяє застосовувати універсальні правила аналізу та кореляції.

Процес збору та нормалізації подій також пов'язаний із питаннями продуктивності та масштабованості. Зі зростанням кількості джерел і обсягу подій навантаження на систему зростає експоненційно. Тому сучасні SIEM реалізують механізми попередньої фільтрації, агрегації та балансування навантаження між компонентами системи. Це дозволяє уникнути перевантаження центральних аналітичних вузлів і забезпечити стабільну роботу системи.

Окрему увагу слід приділити надійності збору подій. Втрата або пошкодження журналів безпеки може призвести до неможливості виявлення інцидентів або відтворення їх хронології. Тому SIEM-системи зазвичай використовують механізми підтвердження доставки, буферизації та резервного зберігання даних. Це забезпечує

цілісність інформації навіть у випадках тимчасових збоїв мережі або окремих компонентів.

Збір і нормалізація подій безпеки формують фундамент для всіх аналітичних функцій SIEM. Саме на основі стандартизованих і збагачених подій стає можливим застосування кореляційних правил, поведінкового аналізу та формування інцидентів інформаційної безпеки. Недостатня увага до цих процесів призводить до зниження ефективності всієї системи управління інцидентами.

Кореляція подій є ключовим аналітичним механізмом SIEM-систем, який дозволяє перейти від обробки ізольованих подій до виявлення цілісних інцидентів інформаційної безпеки. У сучасних інформаційних інфраструктурах окремі події рідко мають самостійне значення, оскільки більшість атак і порушень реалізуються у вигляді послідовності взаємопов'язаних дій. Саме кореляція забезпечує можливість виявлення таких послідовностей і їх інтерпретації як інцидентів.

На базовому рівні кореляція подій полягає у встановленні логічних і часових зв'язків між подіями, що надходять із різних джерел. Наприклад, серія невдалих спроб автентифікації, за якою слідує успішний вхід і нетипова активність користувача, окремо може не викликати підозри, але в сукупності ці події формують характерний сценарій компрометації облікового запису. SIEM-система здатна виявляти такі сценарії на основі заздалегідь визначених правил або моделей поведінки.

Одним із поширених підходів до кореляції є використання правил на основі сигнатур. У цьому випадку інцидент формується при виконанні певної комбінації умов, що відповідають відомим сценаріям атак або порушень. Перевагою цього підходу є його передбачуваність і контрольованість, однак він потребує постійного оновлення правил і не завжди ефективний проти нових або нетипових загроз.

Альтернативним підходом є поведінкова кореляція, яка ґрунтується на аналізі відхилень від нормальної активності. У цьому випадку SIEM формує базові профілі поведінки користувачів, систем або сервісів і виявляє аномалії, що можуть свідчити

про інцидент. Такий підхід дозволяє виявляти раніше невідомі сценарії атак, проте потребує значних обчислювальних ресурсів і якісних даних для побудови коректних моделей.

Важливим аспектом кореляції є врахування часових характеристик подій. Інциденти часто розвиваються протягом певного проміжку часу, і кореляція повинна враховувати не лише факт наявності подій, а й їх послідовність і часові інтервали. Неправильно налаштовані часові вікна можуть призводити до пропуску інцидентів або формування хибних спрацювань.

Контекстна інформація відіграє ключову роль у процесі кореляції. Дані про критичність активів, ролі користувачів, розташування систем і типи сервісів дозволяють значно підвищити точність формування інцидентів. Наприклад, однакова послідовність подій може мати різне значення залежно від того, чи відбувається вона на тестовому сервері або на критично важливому виробничому ресурсі.

Процес формування інцидентів у SIEM передбачає агрегацію корельованих подій у єдиний об'єкт із визначеними характеристиками. Такий об'єкт містить інформацію про тип інциденту, його ймовірну причину, залучені активи та рівень пріоритету. Формування інциденту дозволяє зменшити кількість окремих подій, з якими працює аналітик, і зосередитися на суттєвих загрозах.

Однією з проблем кореляції є баланс між чутливістю та точністю. Надмірно агресивні правила кореляції можуть призводити до великої кількості хибнопозитивних інцидентів, що перевантажує персонал і знижує довіру до системи. З іншого боку, надто консервативні налаштування можуть спричинити пропуск реальних загроз. Тому кореляційні механізми потребують постійного налаштування та оптимізації.

У практичних умовах ефективність кореляції значною мірою залежить від якості попередніх етапів збору та нормалізації подій. Неповні або некоректно нормалізовані дані обмежують можливості кореляції та можуть спотворювати

результати аналізу. Це підкреслює важливість комплексного підходу до побудови SIEM, у якому всі компоненти взаємопов'язані.

Кореляція подій є також основою для подальшої автоматизації реагування. Сформований інцидент може бути переданий до системи автоматизованого реагування для виконання визначених сценаріїв дій. У цьому контексті якість формування інцидентів безпосередньо впливає на ефективність автоматизованих процесів і безпеку всієї системи.

Попри широкі аналітичні можливості, SIEM-системи мають низку обмежень, які проявляються насамперед на етапі реагування на інциденти інформаційної безпеки. Ці обмеження зумовлені як архітектурними особливостями SIEM, так і їх початковим призначенням, орієнтованим переважно на виявлення та аналіз подій, а не на виконання активних дій у відповідь на загрози.

Основним обмеженням SIEM є залежність процесів реагування від ручної участі персоналу. У типовій реалізації SIEM формує інцидент, визначає його пріоритет і генерує сповіщення, після чого подальші дії виконуються аналітиками або адміністраторами вручну. Такий підхід створює часовий розрив між моментом виявлення інциденту та фактичним початком реагування, що може бути критичним у випадках швидкоплинних або автоматизованих атак.

Ще одним суттєвим обмеженням є обмежена підтримка складних сценаріїв реагування. Хоча деякі SIEM дозволяють виконувати прості автоматичні дії, такі як відправлення повідомлень або запуск скриптів, ці можливості зазвичай не охоплюють повний спектр дій, необхідних для комплексного реагування. Реалізація багатокрокових сценаріїв, що потребують взаємодії з різними системами, виходить за межі стандартного функціоналу SIEM.

Проблемою також є відсутність механізмів оркестрації дій. Реагування на інцидент часто потребує послідовного виконання взаємопов'язаних операцій, таких як блокування облікового запису, ізоляція вузла, перевірка стану системи та

повідомлення відповідальних осіб. У межах SIEM ці дії не координуються автоматично, що підвищує ризик помилок і неузгоджених рішень.

SIEM-системи також обмежені у можливостях інтеграції з операційними процесами організації. Реагування на інцидент часто передбачає не лише технічні дії, а й організаційні кроки, включаючи ескалацію, погодження рішень і документування. SIEM зазвичай не підтримує повний цикл таких процесів, що ускладнює управління інцидентами на рівні всієї організації.

Ще одним аспектом обмежень є масштабованість реагування. У ситуаціях, коли одночасно виникає велика кількість інцидентів, ручне реагування стає неефективним. Навіть за високого рівня автоматизації аналізу подій персонал фізично не здатний оперативно обробити всі інциденти. Це створює потребу в механізмах, які дозволяють автоматизувати не лише аналіз, а й виконання стандартних дій реагування.

Важливою проблемою є також відсутність зворотного зв'язку між результатами реагування та аналітичними механізмами SIEM. Дані про виконані дії та їх ефективність зазвичай не використовуються для автоматичного коригування правил виявлення або пріоритизації інцидентів. У результаті система не адаптується до змін у середовищі та зберігає статичний характер.

Обмеження SIEM у процесах реагування не знижують їх значущості як аналітичного інструменту, проте чітко окреслюють межі їх застосування. SIEM ефективно виконує роль центрального елементу моніторингу та аналізу, але не здатна самостійно забезпечити повний цикл управління інцидентами інформаційної безпеки.

2.2. Засоби збору подій та IDS/IPS як елементи моніторингу

Системи виявлення вторгнень є одним із ключових технічних елементів моніторингу інформаційної безпеки, оскільки вони безпосередньо орієнтовані на ідентифікацію спроб несанкціонованого доступу, атак і порушень політик безпеки. На відміну від універсальних механізмів журналювання, IDS та IPS спеціалізуються на

аналізі мережевої та системної активності з позиції безпеки, що робить їх важливим джерелом подій для SIEM-систем.

З функціональної точки зору IDS призначені для виявлення підозрілої або зловмисної активності та генерації відповідних сповіщень. IPS, у свою чергу, доповнюють ці можливості здатністю здійснювати активний вплив на трафік або процеси з метою блокування виявлених загроз. У контексті моніторингу інформаційної безпеки обидва типи систем виконують роль сенсорів, які фіксують ознаки інцидентів на ранніх етапах їх розвитку.

Важливою особливістю IDS/IPS є їх здатність аналізувати події на різних рівнях. Мережеві системи виявлення вторгнень здійснюють контроль трафіку між вузлами, аналізуючи пакети даних і протокольні взаємодії. Це дозволяє виявляти атаки, спрямовані на експлуатацію мережевих вразливостей або порушення політик доступу. Хостові IDS/IPS, у свою чергу, орієнтовані на контроль активності окремих систем, включаючи процеси, файлову систему та системні виклики.

Роль IDS/IPS у моніторингу полягає не лише у виявленні відомих атак, а й у формуванні інформаційної основи для подальшого аналізу інцидентів. Події, що генеруються цими системами, містять технічні деталі про характер загрози, джерело атаки, цільовий ресурс і використані методи. Така інформація є надзвичайно цінною для кореляції подій у SIEM і формування цілісної картини інциденту.

Інтеграція IDS/IPS у загальну систему моніторингу дозволяє компенсувати обмеження інших джерел подій. Наприклад, журнали операційних систем можуть не фіксувати мережеві атаки на ранніх етапах, тоді як IDS здатні виявити підозрілу активність ще до фактичного порушення системи. Це підвищує загальну чутливість моніторингу та зменшує час до виявлення інцидентів.

Разом із тим ефективність IDS/IPS значною мірою залежить від коректності їх налаштувань. Надмірно агресивні правила можуть призводити до великої кількості хибних спрацювань, тоді як надто лояльні налаштування знижують рівень захисту. У

цьому контексті важливою є взаємодія IDS/IPS із SIEM, яка дозволяє фільтрувати та пріоритизувати події з урахуванням контекстної інформації.

Системи виявлення вторгнень також відіграють роль у формуванні бази знань про загрози. Дані про виявлені атаки можуть використовуватися для оновлення правил кореляції, навчання персоналу та вдосконалення політик безпеки. У поєднанні з можливостями централізованого аналізу SIEM це дозволяє підвищувати зрілість системи управління інцидентами.

У сучасних умовах IDS/IPS не можуть розглядатися як автономні засоби захисту. Їх максимальна ефективність досягається лише за умови інтеграції з централізованими платформами моніторингу та реагування. У такій архітектурі IDS/IPS виконують функцію первинних сенсорів, тоді як SIEM і SOAR забезпечують аналіз, координацію та автоматизацію реагування.

Мережеві та хостові джерела подій є базовими складовими інформаційного наповнення систем моніторингу інформаційної безпеки. Саме на основі подій, що генеруються цими джерелами, формується первинне уявлення про стан інфраструктури, характер мережевої взаємодії та поведінку окремих вузлів. Розуміння ролі та можливостей кожної з цих категорій джерел є необхідним для побудови ефективної системи управління інцидентами.

Мережеві джерела подій фіксують інформацію про передавання даних між вузлами інформаційної системи та зовнішнім середовищем. До них належать мережеві маршрутизатори, комутатори, міжмережеві екрани, системи виявлення вторгнень мережевого рівня та інші пристрої, що аналізують трафік. Події, отримані з таких джерел, дозволяють відстежувати спроби несанкціонованого доступу, сканування мережі, аномальні обсяги трафіку та порушення мережевих політик.

Особливістю мережевих джерел є їх здатність виявляти інциденти на ранніх етапах, ще до того, як зломисник отримає доступ до конкретних систем. Аналіз мережевого трафіку дозволяє виявляти підозрілі шаблони взаємодії, характерні для

підготовчих фаз атак. У цьому контексті мережеві події є важливим індикатором потенційних загроз і відіграють значну роль у проактивному моніторингу.

Водночас мережеві події мають певні обмеження. Вони зазвичай не містять детальної інформації про внутрішній стан систем і дії користувачів після встановлення з'єднання. Крім того, у сучасних мережах широке використання шифрування ускладнює аналіз вмісту трафіку, що знижує інформативність деяких мережевих сенсорів. Це обмежує можливості виявлення складних інцидентів, які реалізуються на рівні операційної системи або прикладних сервісів.

Хостові джерела подій, на відміну від мережевих, фокусуються на внутрішньому стані окремих систем. До них належать журнали операційних систем, події прикладних програм, засоби контролю цілісності файлів, системи моніторингу процесів і засоби захисту кінцевих точок. Такі джерела надають детальну інформацію про дії користувачів, виконання програм, зміну конфігурацій і доступ до ресурсів.

Перевагою хостових джерел є їх висока точність і контекстність. Події цього рівня дозволяють визначити, які саме процеси були запущені, які файли змінені та які облікові записи використані. Це є надзвичайно важливим для підтвердження інцидентів і проведення розслідувань. Хостові події також дозволяють виявляти внутрішні загрози та зловживання повноваженнями, які можуть залишатися непоміченими на мережевому рівні.

Разом із тим використання хостових джерел потребує встановлення агентів або налаштування відповідних механізмів журналювання, що може ускладнювати розгортання системи моніторингу. Крім того, велика кількість подій, що генеруються хостами, створює додаткове навантаження на систему аналізу та потребує ефективних механізмів фільтрації й кореляції.

Найбільш ефективний підхід до моніторингу полягає у поєднанні мережевих і хостових джерел подій. Таке поєднання дозволяє компенсувати обмеження кожної категорії та сформувати багатовимірне уявлення про інцидент. Мережеві події можуть

вказувати на початкову фазу атаки, тоді як хостові події підтверджують факт компрометації та дозволяють оцінити її наслідки.

У SIEM-системах мережеві та хостові події обробляються в єдиному аналітичному просторі, що дозволяє здійснювати їх кореляцію та контекстний аналіз. Наприклад, спроба підключення до сервера з підозрілої адреси може бути співставлена з подальшими подіями автентифікації та запуску процесів на цьому сервері. Такий підхід значно підвищує точність виявлення інцидентів і зменшує кількість хибних спрацювань.

Інтеграція систем виявлення та запобігання вторгненням із SIEM-системами є одним із ключових етапів побудови ефективної технології моніторингу інцидентів інформаційної безпеки. Саме на цьому рівні забезпечується перехід від локального виявлення підозрілої активності до централізованого аналізу та управління інцидентами в межах усієї інформаційної інфраструктури.

Практична цінність інтеграції IDS/IPS із SIEM полягає в тому, що події, зафіксовані цими системами, перестають бути ізольованими технічними повідомленнями й набувають контексту в загальній картині безпеки. Події вторгнень співставляються з даними з інших джерел, таких як журнали операційних систем, засоби автентифікації та прикладні сервіси. Це дозволяє не лише зафіксувати факт атаки, а й оцінити її вплив та подальший розвиток.

Інтеграція зазвичай реалізується шляхом передачі подій IDS/IPS у SIEM у стандартизованому форматі. Для цього використовуються механізми журналювання, агентні компоненти або спеціалізовані конектори. На етапі приймання подій SIEM виконує їх нормалізацію, збагачення та класифікацію, що забезпечує уніфіковану обробку незалежно від типу джерела.

Одним із важливих аспектів інтеграції є коректне відображення рівня критичності подій IDS/IPS. Не всі спрацювання мають однакову значущість, і без контекстного аналізу вони можуть створювати надмірну кількість сповіщень. SIEM

дозволяє зіставляти спрацювання IDS/IPS із інформацією про активи, користувачів і поточний стан системи, що зменшує кількість хибнопозитивних інцидентів.

Інтеграція IDS/IPS із SIEM також забезпечує можливість виявлення складних сценаріїв атак. Наприклад, мережеве сканування, зафіксоване IDS, може бути співставлене з подальшими спробами автентифікації та виконанням процесів на хостах. Така кореляція дозволяє ідентифікувати багатоступеневі атаки, які залишилися б непоміченими при ізольованому аналізі подій.

Важливою перевагою інтеграції є підтримка централізованого управління реагуванням. Хоча самі IDS/IPS можуть виконувати окремі дії блокування, їх взаємодія з SIEM дозволяє координувати ці дії з іншими заходами безпеки. Наприклад, спрацювання IDS може ініціювати не лише блокування трафіку, а й подальший аналіз дій користувача або ізоляцію скомпрометованого вузла.

Разом із тим інтеграція IDS/IPS із SIEM пов'язана з низкою технічних викликів. Серед них можна виділити різноманітність форматів подій, обмеження продуктивності та необхідність тонкого налаштування кореляційних правил. Неправильно налаштована інтеграція може призводити до втрати подій або надмірного навантаження на аналітичні компоненти SIEM.

Ще одним аспектом є забезпечення надійності передачі подій. У випадку перевантаження мережі або відмов окремих компонентів важливо зберегти цілісність даних і уникнути втрати інформації про інциденти. Тому інтеграція IDS/IPS із SIEM зазвичай передбачає використання механізмів буферизації та підтвердження доставки подій.

У практичних реалізаціях інтеграція IDS/IPS із SIEM розглядається не як одноразове налаштування, а як постійний процес оптимізації. Зміни в інфраструктурі, оновлення сигнатур і поява нових типів загроз потребують регулярного перегляду правил обробки та кореляції подій. Це дозволяє підтримувати актуальність системи моніторингу та забезпечувати її відповідність реальним умовам експлуатації.

Сигнатурні методи виявлення інцидентів інформаційної безпеки тривалий час залишалися основою роботи систем IDS/IPS та багатьох засобів моніторингу. Їх застосування ґрунтується на порівнянні зафіксованих подій або мережевих шаблонів із наперед визначеними ознаками відомих атак. Такий підхід є ефективним для виявлення добре задокументованих загроз, однак у сучасних умовах його можливості виявляються суттєво обмеженими.

Основною проблемою сигнатурних методів є їх реактивний характер. Система здатна виявити лише ті загрози, для яких уже існує опис або сигнатура. У випадку нових або модифікованих атак, що використовують нетипові техніки, сигнатурний аналіз часто виявляється неефективним. Це створює вікно вразливості між появою нової загрози та моментом оновлення сигнатурної бази.

Ще одним суттєвим обмеженням є чутливість сигнатурних методів до змін середовища. Навіть незначні відхилення у параметрах атаки можуть призвести до того, що сигнатура не спрацює. Зловмисники активно використовують ці особливості, змінюючи послідовності дій, структуру трафіку або параметри запитів, щоб обійти сигнатурні механізми виявлення.

Сигнатурні методи також мають обмежені можливості для аналізу складних багатоступеневих атак. У таких сценаріях кожен окремий етап може виглядати як легітимна активність або малозначуща подія. Лише в сукупності ці дії формують інцидент, проте сигнатурні механізми не завжди здатні встановити такі взаємозв'язки. У результаті інцидент може залишатися непоміченим до моменту завдання значної шкоди.

Окремою проблемою є велика кількість хибнопозитивних спрацювань. Сигнатури часто орієнтовані на загальні шаблони, які можуть відповідати як зловмисній, так і легітимній активності. У таких випадках система генерує значну кількість сповіщень, що перевантажує персонал і ускладнює оперативне реагування. Це особливо критично в умовах великих і динамічних інформаційних інфраструктур.

Зазначені обмеження зумовлюють необхідність доповнення сигнатурних методів поведінковим аналізом. Поведінковий підхід ґрунтується на виявленні відхилень від нормальної роботи системи, користувачів або мережі. Замість пошуку конкретних ознак атак система аналізує шаблони поведінки та ідентифікує аномалії, що можуть свідчити про інцидент.

Поведінковий аналіз дозволяє виявляти раніше невідомі загрози, у тому числі цілеспрямовані атаки та внутрішні порушення. Він не потребує наявності сигнатур і здатний адаптуватися до змін у середовищі. У поєднанні з контекстною інформацією поведінковий підхід значно підвищує точність виявлення інцидентів і зменшує кількість хибнопозитивних спрацювань.

Разом із тим поведінковий аналіз потребує якісних даних і коректного налаштування. Формування базових профілів поведінки є складним процесом, який вимагає часу та обчислювальних ресурсів. Неправильно визначені базові шаблони можуть призводити до помилкових висновків або пропуску реальних загроз. Тому поведінковий аналіз зазвичай використовується у поєднанні з іншими методами виявлення.

У сучасних SIEM-системах сигнатурні та поведінкові методи розглядаються як взаємодоповнювальні. Сигнатурний аналіз забезпечує швидке виявлення відомих загроз, тоді як поведінковий аналіз дозволяє ідентифікувати нетипову активність і нові сценарії атак. Такий комбінований підхід значно підвищує ефективність моніторингу та створює надійну основу для управління інцидентами.

2.3. Порівняльний аналіз SIEM-платформ

Платформа Splunk є одним із найбільш відомих і поширених рішень у сфері аналізу машинних даних та моніторингу інформаційної безпеки. У контексті SIEM Splunk використовується як потужний інструмент централізованого збору, обробки та аналізу подій безпеки з різноманітних джерел. Його популярність зумовлена гнучкою

архітектурою, високою продуктивністю та широкими можливостями розширення функціоналу.

Функціонально Splunk SIEM забезпечує централізований збір подій із мережевих пристроїв, операційних систем, прикладних сервісів і засобів захисту. Платформа підтримує обробку великих обсягів даних у режимі, наближеному до реального часу, що дозволяє оперативно виявляти аномалії та формувати інциденти інформаційної безпеки. Важливою перевагою є потужний механізм індексації, який забезпечує швидкий пошук і аналіз як поточних, так і історичних даних.

Однією з ключових особливостей Splunk є використання власної мови запитів, яка дозволяє аналітикам створювати складні запити для аналізу подій, виявлення закономірностей і побудови кореляційних правил. Це надає значну гнучкість у налаштуванні аналітичних сценаріїв і дозволяє адаптувати систему до специфіки конкретної інфраструктури. У поєднанні з розвинутими засобами візуалізації це спрощує інтерпретацію результатів аналізу та підтримує процеси розслідування інцидентів.

Splunk SIEM також підтримує контекстний аналіз і пріоритизацію інцидентів. Завдяки інтеграції з різними джерелами даних платформа може враховувати інформацію про активи, користувачів і типи ресурсів.



Рис. 1.1. Splunk

Разом із тим використання Splunk як SIEM має низку обмежень. Одним із основних є висока вартість володіння. Ліцензування Splunk зазвичай залежить від обсягу оброблюваних даних, що в умовах великих або швидкозростаючих інфраструктур може призводити до значних фінансових витрат. Це обмежує можливість використання платформи в організаціях із обмеженим бюджетом або у навчальних і дослідницьких середовищах.

Ще одним обмеженням є складність адміністрування та налаштування. Для ефективного використання Splunk потрібні фахівці з відповідним рівнем підготовки, які володіють знаннями внутрішньої архітектури платформи та мови запитів. У разі відсутності таких спеціалістів розгортання та підтримка системи можуть бути ускладненими, що знижує її практичну ефективність.

З точки зору реагування на інциденти Splunk, як і більшість SIEM-рішень, має обмежені можливості автоматизації. Основний акцент платформи зроблено на аналізі та візуалізації даних, тоді як виконання активних дій реагування потребує інтеграції з додатковими рішеннями класу SOAR. Без такої інтеграції процес реагування залишається значною мірою ручним.

Крім того, гнучкість Splunk може бути водночас і перевагою, і недоліком. Високий рівень налаштовуваності потребує значних зусиль на початкову конфігурацію та подальшу оптимізацію. Неправильно налаштовані правила кореляції або візуалізації можуть призводити до неефективного використання платформи та зниження якості виявлення інцидентів.

У контексті побудови практичної технології моніторингу та управління інцидентами інформаційної безпеки Splunk доцільно розглядати як потужне, але ресурсомістке рішення. Його застосування є виправданим у великих організаціях із розвиненою інфраструктурою та достатніми фінансовими й кадровими ресурсами. Водночас для середовищ, де пріоритетом є доступність, відкритість і можливість гнучкої адаптації без значних витрат, можуть бути доцільні альтернативні SIEM-платформи.

ELK Stack є набором відкритих програмних компонентів, який широко використовується для збору, зберігання, аналізу та візуалізації журналів і подій. На відміну від класичних SIEM-платформ, ELK Stack не є завершеним спеціалізованим рішенням для управління інцидентами інформаційної безпеки, однак його гнучка архітектура дозволяє будувати на його основі системи моніторингу, що частково виконують функції SIEM.

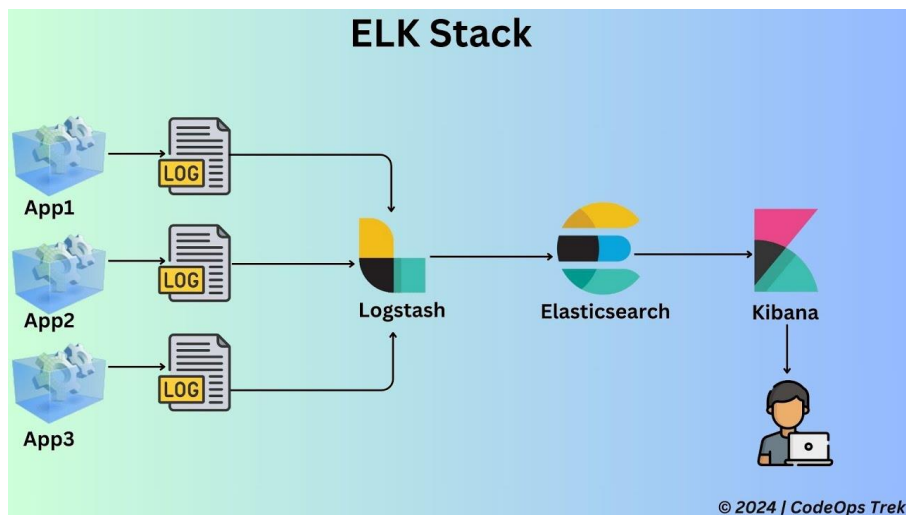


Рис. 1.2. ELK Stack

Архітектурно ELK Stack складається з декількох ключових компонентів, кожен з яких виконує окрему функцію в процесі обробки даних. Компоненти збору подій забезпечують приймання журналів із різноманітних джерел, включаючи сервери, мережеві пристрої та прикладні сервіси. Центральний елемент системи відповідає за індексацію та зберігання даних, що дозволяє ефективно працювати з великими обсягами інформації. Засоби візуалізації забезпечують побудову панелей моніторингу та аналітичних звітів.

Однією з основних переваг ELK Stack є його відкритість і гнучкість. Користувач має можливість самостійно визначати, які джерела подій підключати, як обробляти дані та які аналітичні сценарії реалізовувати. Це дозволяє адаптувати систему до

специфіки конкретної інфраструктури без обмежень, притаманних комерційним рішенням. Такий підхід особливо привабливий для організацій, які прагнуть уникнути залежності від постачальника.

З точки зору моніторингу інформаційної безпеки ELK Stack забезпечує ефективний збір і зберігання подій, а також потужні засоби пошуку й візуалізації. Аналітики можуть швидко аналізувати журнали, виявляти аномальні шаблони та досліджувати інциденти на основі історичних даних. Це робить ELK Stack корисним інструментом для підтримки розслідувань і аналізу подій після їх виникнення.

Разом із тим ELK Stack має суттєві обмеження в контексті повноцінного управління інцидентами. На відміну від спеціалізованих SIEM-платформ, у базовій конфігурації він не містить вбудованих механізмів кореляції подій, класифікації інцидентів і пріоритизації загроз. Реалізація таких можливостей потребує додаткової розробки, використання сторонніх компонентів або створення власних правил і сценаріїв аналізу.

Ще одним важливим аспектом є відсутність нативної підтримки процесів реагування. ELK Stack орієнтований насамперед на аналіз і візуалізацію даних, тоді як виконання активних дій у відповідь на інциденти виходить за межі його функціонального призначення. Для автоматизації реагування необхідна інтеграція з іншими інструментами або розробка власних рішень, що ускладнює побудову цілісної технології управління інцидентами.

Складність впровадження ELK Stack також є чинником, який необхідно враховувати. Хоча компоненти платформи є відкритими, їх розгортання та налаштування потребують значних технічних знань. Забезпечення масштабованості, відмовостійкості та безпеки самої системи вимагає ретельного проєктування архітектури та постійного супроводу. У відсутності відповідної експертизи це може стати серйозною перешкодою для практичного використання.

У контексті побудови технології моніторингу та управління інцидентами інформаційної безпеки ELK Stack доцільно розглядати як гнучку платформу для збору

та аналізу подій, але не як завершене SIEM-рішення. Його використання виправдане в сценаріях, де основний акцент робиться на аналізі журналів і побудові кастомізованих аналітичних інструментів, а не на автоматизованому управлінні інцидентами.

Платформа Wazuh є відкритим SIEM-рішенням, спеціалізованим на завданнях моніторингу інформаційної безпеки, виявлення інцидентів і контролю стану інформаційних систем. На відміну від універсальних платформ аналізу логів або комерційних SIEM-рішень, Wazuh спочатку проєктувалася з фокусом на безпекові сценарії, що визначає її архітектурні та функціональні особливості.

Архітектура Wazuh базується на клієнт-серверній моделі та включає агентні й безагентні механізми збору подій. Агенти Wazuh встановлюються на кінцеві вузли та забезпечують глибокий моніторинг операційних систем, включаючи аналіз журналів, контроль цілісності файлів, виявлення змін конфігурації та моніторинг активності процесів. Такий підхід дозволяє отримувати детальну інформацію про стан систем і дії користувачів, що є критично важливим для управління інцидентами.

Однією з ключових переваг Wazuh є наявність вбудованих правил виявлення загроз. Платформа містить широку базу сигнатур і правил кореляції, орієнтованих на виявлення типових інцидентів інформаційної безпеки, включаючи спроби несанкціонованого доступу, ескалацію привілеїв, підозрілу активність користувачів і порушення політик безпеки. Це дозволяє розгортати систему з мінімальними початковими налаштуваннями та поступово адаптувати її до специфіки конкретної інфраструктури.

Wazuh підтримує нормалізацію та класифікацію подій, що забезпечує уніфіковане представлення інформації незалежно від джерела. Події, зібрані агентами або безагентними методами, проходять обробку на сервері, де їм присвоюються відповідні категорії, рівні важливості та контекстні атрибути. Це створює основу для подальшої кореляції та формування інцидентів інформаційної безпеки.

Важливим аспектом Wazuh є інтеграція з компонентами аналізу та візуалізації. Платформа використовує стек зберігання та візуалізації даних, що дозволяє будувати інформаційні панелі, переглядати події в режимі, наближеному до реального часу, і аналізувати інциденти на основі історичних даних. Це значно спрощує роботу аналітиків і підвищує прозорість процесів моніторингу.

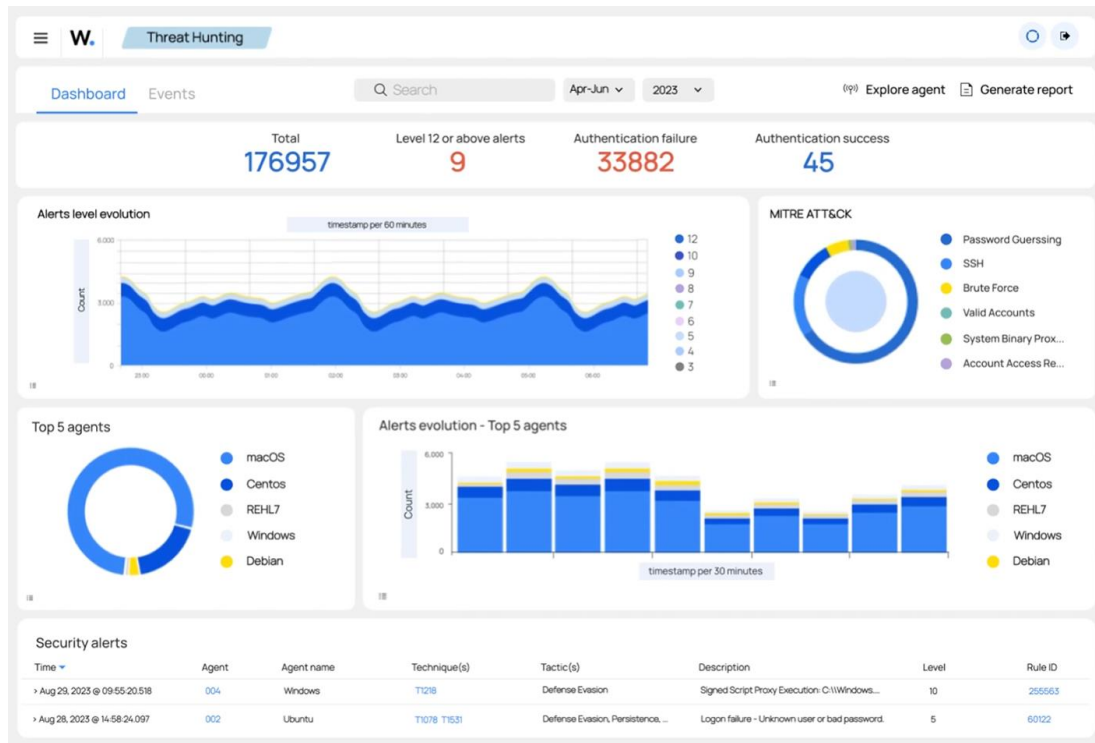


Рис. 1.3. Wazuh

З точки зору управління інцидентами Wazuh дозволяє формувати інциденти на основі кореляції подій і правил виявлення. Інциденти можуть бути класифіковані за типами, пріоритетами та джерелами, що забезпечує структурований підхід до їх обробки. Однак реагування на інциденти в межах самої платформи має обмежений характер і зазвичай зводиться до генерації сповіщень або виконання окремих локальних дій.

Саме ця особливість визначає роль Wazuh у побудові комплексної технології управління інцидентами. Платформа ефективно виконує функції моніторингу, виявлення та первинної класифікації інцидентів, але для реалізації повноцінного циклу реагування потребує інтеграції з додатковими інструментами. Такий підхід відповідає сучасним концепціям розподілу функцій між SIEM і SOAR.

Перевагою Wazuh є її відкритість і доступність. Відсутність ліцензійних обмежень дозволяє використовувати платформу в навчальних, дослідницьких і виробничих середовищах без значних фінансових витрат. Це робить Wazuh особливо привабливою для організацій, які прагнуть впровадити технології моніторингу безпеки з мінімальними ресурсами.

Разом із тим використання Wazuh вимагає відповідного рівня технічної підготовки. Налаштування правил, оптимізація продуктивності та інтеграція з іншими системами потребують глибокого розуміння архітектури платформи та принципів її роботи. У разі недостатньої експертизи ефективність системи може бути знижена.

Таблиця 2.1

Порівняльний аналіз SIEM-платформ Splunk, ELK Stack, Wazuh

Критерій	Splunk (SIEM)	ELK Stack (платформа для побудови SIEM)	Wazuh(відкрита SIEM/SEC платформа)
Тип рішення	Комерційна платформа SIEM високого рівня	Набір компонентів для збору/пошуку/візу алізації логів	Відкрите рішення, орієнтоване на інформаційну безпеку
Орієнтація	Корпоративний моніторинг, масштабні інфраструктури	Гнучка аналітика логів, потребує побудови безпекового шару	Практична безпека, виявлення інцидентів, контроль хостів
Збір подій	Широкі конектори, агенти, інтеграції	Реалізується через Beats/Logstash, залежить від налаштувань	Агенти Wazuh + безагентні джерела, готові модулі

Нормалізація	Розвинуті механізми, залежить від конфігурації	Вимагає ручної нормалізації/пайплайнів	Вбудована класифікація та структурування безпекових подій
Кореляція	Потужні правила та аналітика, але складна настройка	Потрібна розробка кореляції (правила, пайплайни)	Вбудовані правила виявлення + можливість їх розширення
Аномалії / поведінковий аналіз	Можливо, але часто потребує розширень/модулів	Можливо, але потребує додаткових рішень/налаштувань	Частково реалізовано через правила, можливе доповнення
Орієнтація на хост безпеку	Є, але залежить від конфігурації та доп. модулів	Потрібні інструменти збору хост подій	Сильна сторона: FIM, rootcheck, audit, системні журнали
Контроль цілісності файлів (FIM)	Реалізується через додаткові інструменти/інтеграції	Потрібна окрема реалізація	Вбудований механізм FIM
Управління вразливостями	Можливо через інтеграції	Можливо через інтеграції	Є модуль/підхід до оцінки вразливостей (залежить від розгортання)
Масштабованість	Висока, але потребує значних ресурсів і ліцензій	Висока за умови правильного проєктування	Середня/висока, залежить від архітектури й ресурсів
Вартість	Висока, залежить від обсягу даних	Умовно безкоштовно, але «вартість» у складності підтримки	Безкоштовно, основні витрати — адміністрування і ресурси
Складність впровадження	Висока (потрібні фахівці, правильне ліцензування)	Висока (потрібна побудова SIEM-функцій вручну)	Середня/висока, але є готові безпекові модулі
Автоматизація реагування	Обмежена без SOAR	Практично відсутня без додаткових інструментів	Обмежена, потрібна інтеграція з SOAR

Придатність для інтеграції із SOAR	Висока (часто з власними рішеннями)	Потрібні інтеграційні шари	Висока, особливо з відкритими SOAR (Shuffle)
Доцільність для дипломної технології	Висока концептуально, але важко відтворити без ресурсів	Добра гнучкість, але забагато ручної роботи	Найбільш практичний варіант для реалізації технології

Порівняльний аналіз демонструє, що Splunk є потужним комерційним рішенням, яке забезпечує високий рівень аналітики та масштабованості, проте його практичне використання в межах навчального або дослідницького середовища часто обмежується вартістю ліцензування й вимогами до ресурсів. У таких умовах Splunk більше підходить як еталонний приклад корпоративного SIEM-рішення, а не як платформа для відтворення технології в межах дипломної роботи з обмеженими ресурсами.

ELK Stack, навпаки, забезпечує високу гнучкість і можливість побудови власної системи моніторингу, але сам по собі не є SIEM-рішенням у повному розумінні. Для реалізації функцій виявлення інцидентів, кореляції, класифікації та пріоритизації необхідно створювати додатковий рівень логіки та інтеграцій, що суттєво збільшує складність проєкту. У межах технології моніторингу та управління інцидентами це може бути виправдано для великих команд або для організацій із достатніми ресурсами на розробку та супровід, але в межах дипломної роботи створює ризик надмірного технічного обсягу без практичної завершеності.

Wazuh займає проміжну позицію, поєднуючи відкритість із безпековою спеціалізацією. Платформа містить готові механізми, орієнтовані на реальні задачі виявлення інцидентів, включаючи контроль цілісності, виявлення змін конфігурації, аналіз журналів і формування безпекових подій. Це дозволяє реалізувати технологію моніторингу та управління інцидентами з реалістичним рівнем технічної деталізації без необхідності будувати ключові SIEM-механізми «з нуля». Водночас обмеження

Wazuh у частині автоматизованого реагування формують природну потребу інтеграції з SOAR, що ідеально узгоджується з обраною концепцією технології на базі Wazuh + Shuffle.

Вибір базової SIEM-платформи для реалізації технології моніторингу та управління інцидентами інформаційної безпеки має ґрунтуватися не лише на функціональній повноті рішення, але й на його практичній відтворюваності, масштабованості та відповідності реальним умовам експлуатації. У межах цієї роботи основна увага приділяється не створенню теоретичної моделі, а розробці технології, яка може бути реалізована в умовах обмежених ресурсів без втрати функціональної цінності.

Аналіз існуючих SIEM-рішень показав, що комерційні платформи корпоративного рівня забезпечують широкий спектр аналітичних можливостей, проте їх використання супроводжується значними фінансовими витратами та підвищеними вимогами до інфраструктури й персоналу. У таких умовах практична реалізація повного циклу моніторингу та управління інцидентами стає складною або недосяжною, особливо в навчальних або дослідницьких середовищах. Це обмежує доцільність використання подібних рішень як бази для розробки технології в межах дипломної роботи.

Платформи, побудовані на універсальних інструментах аналізу логів, забезпечують високу гнучкість і можливість адаптації, проте не містять вбудованих механізмів управління інцидентами інформаційної безпеки. Реалізація необхідних функцій у таких системах потребує значних зусиль на проєктування, налаштування та підтримку, що ускладнює досягнення завершеного й практично орієнтованого результату. За відсутності спеціалізованих безпекових модулів такі рішення часто залишаються на рівні систем збору та візуалізації подій.

У цьому контексті платформа Wazuh поєднує ключові переваги обох підходів. Вона є відкритим рішенням, що дозволяє використовувати її без ліцензійних обмежень і масштабувати відповідно до наявних ресурсів. Водночас Wazuh спочатку

орієнтована на завдання інформаційної безпеки, що відображається в її архітектурі, вбудованих правилах виявлення та механізмах аналізу подій. Це дозволяє одразу отримати функціональну основу для управління інцидентами без необхідності створення базових механізмів з нуля.

Важливою перевагою Wazuh є її агентна модель, яка забезпечує глибокий моніторинг стану хостів. Контроль цілісності файлів, аналіз змін конфігурації, моніторинг системних журналів і процесів дозволяють виявляти широкий спектр інцидентів, включаючи як зовнішні атаки, так і внутрішні порушення. Такий рівень деталізації є необхідним для повноцінного управління інцидентами та проведення їх аналізу.

Wazuh також підтримує централізовану нормалізацію та класифікацію подій, що спрощує кореляцію та контекстний аналіз. Події, зібрані з різних джерел, обробляються в єдиному аналітичному просторі, що дозволяє формувати інциденти з урахуванням взаємозв'язків між подіями та станом активів. Це створює основу для системного підходу до управління інцидентами, а не лише їх точкового виявлення.

Водночас обмежені можливості автоматизованого реагування в межах Wazuh не слід розглядати як недолік, а як архітектурну особливість, що відповідає сучасним підходам до побудови систем управління інцидентами. Розмежування функцій між SIEM і SOAR дозволяє зберігати гнучкість і масштабованість технології, уникаючи перевантаження одного інструмента надмірною функціональністю. Такий підхід створює чітку основу для інтеграції Wazuh із системами автоматизованого реагування.

Ще одним аргументом на користь вибору Wazuh є активна спільнота та наявність розширеної документації. Це спрощує вивчення платформи, її налаштування та адаптацію до конкретних умов. У межах дипломної роботи це дозволяє зосередитися на розробці технології управління інцидентами, а не на подоланні технічних обмежень або нестачі інформації.

Таким чином, вибір Wazuh як базової SIEM-платформи для реалізації технології моніторингу та управління інцидентами інформаційної безпеки є обґрунтованим з точки зору функціональної доцільності, практичної реалізованості та відповідності сучасним підходам до побудови систем кіберзахисту. Платформа забезпечує необхідний рівень моніторингу та аналітики, водночас створюючи передумови для інтеграції з системами автоматизованого реагування, що дозволяє побудувати цілісну та масштабовану технологію управління інцидентами.

3 РОЗРОБКА ТЕХНОЛОГІЇ МОНІТОРИНГУ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ НА БАЗІ WAZUH + SHUFFLE

3.1. Архітектурна модель запропонованої технології

Побудова ефективної технології моніторингу та управління інцидентами інформаційної безпеки ґрунтується на системному підході до організації процесів виявлення, аналізу та реагування на події безпеки. У сучасних умовах інформаційні інфраструктури характеризуються високою складністю, розподіленістю та динамічністю, що зумовлює необхідність використання технологій, здатних працювати з великими обсягами різномірних даних і забезпечувати оперативну реакцію на потенційні загрози.

Одним із базових принципів побудови такої технології є принцип централізованого моніторингу. Його сутність полягає у зосередженні інформації про події безпеки з усіх елементів інфраструктури в єдиному аналітичному середовищі. Це дозволяє уникнути фрагментарності даних, забезпечити цілісне уявлення про стан безпеки та створити умови для коректної кореляції подій. Централізація є критично важливою для виявлення складних інцидентів, які проявляються не однією подією, а сукупністю взаємопов'язаних дій у різних сегментах системи.

Іншим ключовим принципом є багаторівнева обробка подій інформаційної безпеки. У межах запропонованої технології події проходять кілька етапів обробки — від первинного збору та нормалізації до аналітичного узагальнення й формування інцидентів. Такий підхід дозволяє поступово відфільтровувати незначущі події, концентруючи увагу на тих, що мають потенційний вплив на безпеку системи. Багаторівневність також забезпечує масштабованість технології та можливість її адаптації до зростання обсягів даних.

Важливим принципом є орієнтація на контекстний аналіз подій. Окремі технічні події, розглянуті ізольовано, не завжди дозволяють однозначно визначити наявність інциденту. У зв'язку з цим технологія повинна враховувати контекст, у якому відбувається подія, зокрема роль користувача, критичність ресурсу, часові характеристики та взаємозв'язок з іншими подіями. Контекстний аналіз підвищує точність виявлення інцидентів і зменшує кількість хибнопозитивних спрацювань.

Наступним принципом є розмежування функцій між компонентами технології. Сучасні підходи до управління інцидентами передбачають поділ відповідальності між системами моніторингу та системами реагування. У запропонованій технології цей принцип реалізується шляхом використання окремих компонентів для виявлення та аналізу інцидентів і для автоматизації реагування. Такий розподіл дозволяє спростити архітектуру окремих компонентів, підвищити їх надійність і забезпечити гнучкість у розширенні функціоналу.

Принцип автоматизації реагування є особливо важливим у контексті зростання кількості інцидентів і обмежених ресурсів персоналу. Технологія має забезпечувати можливість автоматичного виконання типових дій у відповідь на інциденти, таких як блокування облікових записів, ізоляція вузлів або сповіщення відповідальних осіб. Автоматизація дозволяє зменшити час реагування та знизити ризик помилок, пов'язаних із людським фактором.

Водночас автоматизація не повинна виключати можливість контролю та втручання з боку фахівців. Тому важливим принципом є керованість і прозорість

процесів реагування. Усі дії, виконані в межах технології, мають бути задокументовані, відтворювані та підконтрольні. Це дозволяє забезпечити відповідність вимогам внутрішніх політик безпеки та створює умови для подальшого аналізу ефективності реагування.

Ще одним принципом побудови технології є її модульність. Модульна архітектура дозволяє змінювати або доповнювати окремі компоненти без необхідності повної перебудови системи. Це особливо актуально в умовах швидкого розвитку засобів кіберзахисту та появи нових загроз. Модульність забезпечує можливість інтеграції додаткових інструментів і адаптації технології до змін у вимогах безпеки.

Не менш важливим є принцип практичної реалізованості. Технологія повинна бути побудована таким чином, щоб її можна було відтворити в реальних умовах із використанням доступних програмних і апаратних засобів. Це передбачає врахування обмежень щодо ресурсів, складності налаштування та підтримки. Практична орієнтованість технології дозволяє використовувати її не лише як концептуальну модель, а й як основу для впровадження в реальних інформаційних системах.

Архітектура запропонованої технології моніторингу та управління інцидентами інформаційної безпеки побудована за багаторівневим принципом, що дозволяє логічно розділити функції збору, аналізу та реагування, а також забезпечити гнучкість і масштабованість системи. Кожен рівень архітектури виконує чітко визначене призначення та взаємодіє з іншими рівнями через стандартизовані потоки даних.

Першим рівнем архітектури є рівень формування подій інформаційної безпеки. На цьому рівні відбувається безпосереднє виникнення первинних подій у середовищі функціонування інформаційної системи. Джерелами таких подій виступають сервери, робочі станції, мережеві пристрої, прикладні сервіси та засоби захисту. Події цього рівня відображають фактичні дії користувачів, процесів і мережевих з'єднань, а також зміни в конфігурації та стані системи. Саме на цьому рівні фіксуються первинні

ознаки потенційних інцидентів, однак вони ще не мають ознак узагальнення або інтерпретації з точки зору безпеки.

Другим рівнем архітектури є рівень збору та первинної обробки подій. Його призначення полягає в централізованому прийманні подій із різних джерел, їх уніфікації та підготовці до подальшого аналізу. У межах запропонованої технології цей рівень реалізується за допомогою агентної інфраструктури та безагентних механізмів збору. Події, що надходять із різних систем, можуть мати різний формат, структуру та ступінь деталізації, тому їх нормалізація є необхідною умовою ефективного аналізу.

На цьому рівні відбувається також попередня фільтрація подій. Малозначущі або технічні повідомлення, які не мають відношення до інформаційної безпеки, можуть бути відсіяні або агреговані. Це дозволяє зменшити навантаження на аналітичні компоненти системи та зосередити ресурси на обробці релевантних подій. Таким чином, рівень збору та первинної обробки виконує роль буферу між сирими даними та аналітичним ядром технології.

Третім рівнем архітектури є аналітичний рівень, на якому здійснюється інтерпретація подій із точки зору інформаційної безпеки. Тут реалізуються механізми кореляції, класифікації та пріоритизації подій. Окремі події об'єднуються в логічні ланцюги, що дозволяє виявляти складні інциденти, які проявляються через послідовність дій або їх взаємозв'язок у часі. На цьому рівні формується поняття інциденту як об'єкта управління, що має визначений тип, рівень критичності та контекст.

Аналітичний рівень також забезпечує збагачення подій додатковою інформацією. До такої інформації можуть належати дані про критичність активів, ролі користувачів, мережеву сегментацію та історію попередніх інцидентів. Це дозволяє оцінювати потенційний вплив інциденту та приймати обґрунтовані рішення щодо подальших дій. У межах архітектури саме цей рівень забезпечує перехід від простого моніторингу до усвідомленого управління інцидентами.

Четвертим рівнем є рівень управління реагуванням. Його призначення полягає в організації та виконанні дій у відповідь на виявлені інциденти. На цьому рівні інциденти, сформовані аналітичним рівнем, використовуються як тригери для запуску сценаріїв реагування. Реалізується оркестрація дій, що може включати автоматизовані та напіваавтоматизовані заходи, а також залучення відповідальних осіб. Рівень управління реагуванням забезпечує скорочення часу між виявленням інциденту та початком протидії.

Важливою характеристикою цього рівня є можливість адаптації сценаріїв реагування до типу та критичності інциденту. Не всі інциденти потребують однакових дій, тому архітектура передбачає гнучке налаштування логіки реагування. Це дозволяє уникнути надмірних або невиннованих дій і зосередити ресурси на найбільш значущих загрозах.

П'ятим рівнем архітектури є рівень контролю та аналізу ефективності. На цьому рівні здійснюється фіксація виконаних дій, оцінка результатів реагування та формування зворотного зв'язку для вдосконалення технології. Аналіз ефективності дозволяє виявляти слабкі місця в архітектурі, правилах виявлення або сценаріях реагування та вносити відповідні коригування. Таким чином, технологія набуває властивостей самовдосконалення.

Розподіл архітектури на зазначені рівні дозволяє забезпечити чітку логіку функціонування технології моніторингу та управління інцидентами інформаційної безпеки. Кожен рівень виконує власне призначення, водночас залишаючись інтегрованим у загальну систему. Такий підхід створює передумови для масштабування, модернізації та практичного впровадження технології в реальних інформаційних середовищах.

Логічна взаємодія між компонентами Wazuh і Shuffle є основою реалізації повного циклу управління інцидентами інформаційної безпеки в межах запропонованої технології. Ця взаємодія забезпечує перехід від етапу виявлення та

аналізу інцидентів до етапу координованого та автоматизованого реагування, що є ключовою вимогою сучасних систем кіберзахисту.

У межах технології Wazuh виконує роль центрального аналітичного компонента, який здійснює безперервний моніторинг середовища, збір подій та формування інцидентів інформаційної безпеки. Shuffle, у свою чергу, виступає як компонент оркестрації та автоматизації реагування, який використовує результати аналітичної обробки для запуску відповідних сценаріїв дій. Такий розподіл ролей дозволяє чітко відокремити функції аналізу та реагування, забезпечуючи гнучкість і керованість технології.

Логічний зв'язок між Wazuh і Shuffle формується на основі подій та інцидентів, які досягають визначеного рівня важливості. Wazuh аналізує потік подій і застосовує правила виявлення для ідентифікації потенційних інцидентів. Коли подія або сукупність подій відповідає критеріям інциденту, формується структуроване повідомлення, що містить ключові атрибути, необхідні для прийняття рішення про реагування. До таких атрибутів належать тип інциденту, джерело, цільовий ресурс, рівень критичності та часові характеристики.

Передача інформації між компонентами здійснюється у вигляді логічних тригерів. Wazuh виступає ініціатором процесу реагування, тоді як Shuffle отримує повідомлення про інцидент і визначає, який сценарій має бути виконаний. Такий підхід дозволяє уникнути жорсткої прив'язки між системами та забезпечує можливість гнучкого налаштування логіки взаємодії без зміни базової архітектури.

У Shuffle логіка реагування реалізується у вигляді послідовності дій, що виконуються відповідно до заданого сценарію. Сценарій може включати перевірку додаткових умов, аналіз супутніх даних або виконання конкретних технічних заходів. Важливою особливістю є можливість комбінування автоматизованих і напіваавтоматизованих дій, що дозволяє адаптувати реагування до складності та критичності інциденту.

Логічна взаємодія між Wazuh і Shuffle також передбачає зворотний зв'язок. Результати виконаних дій можуть бути використані для подальшого аналізу та вдосконалення правил виявлення. Наприклад, інформація про підтверджений або хибний інцидент дозволяє коригувати аналітичні правила, зменшуючи кількість хибнопозитивних спрацювань. Таким чином, технологія набуває адаптивних властивостей.

Ще одним аспектом логічної взаємодії є можливість масштабування сценаріїв реагування. У разі появи нових типів інцидентів або зміни вимог до безпеки можуть бути додані нові сценарії без необхідності модифікації аналітичної частини системи. Це дозволяє розвивати технологію поступово, зберігаючи її цілісність і стабільність.

Взаємодія Wazuh і Shuffle також сприяє стандартизації процесів реагування. Замість індивідуальних рішень, що залежать від досвіду окремих фахівців, технологія забезпечує виконання узгоджених сценаріїв дій. Це підвищує передбачуваність і керованість процесів управління інцидентами, а також полегшує їх документування та аудит.

Потоки даних у межах запропонованої технології визначають послідовність перетворення первинних подій інформаційної безпеки в керовані інциденти та подальші дії реагування. Чітке розуміння цих потоків є необхідним для аналізу ефективності технології, а також для її практичної реалізації та масштабування.

Початковим етапом потоку даних є формування подій у контрольованому середовищі. Події виникають у результаті дій користувачів, виконання процесів, мережевої взаємодії та змін у конфігурації систем. Кожна така подія відображає певний факт функціонування інформаційної системи, проте на цьому етапі вона ще не має визначеного статусу з точки зору інформаційної безпеки. Події є різнорідними за форматом, рівнем деталізації та частотою виникнення.

Наступним етапом є передача подій до системи збору. У межах запропонованої технології цей процес реалізується за допомогою агентної інфраструктури та механізмів безагентного збору. Події передаються до центрального компонента

моніторингу, де відбувається їх приймання та первинна перевірка. На цьому етапі забезпечується цілісність даних і контроль їх доставки, що є важливим для подальшого аналізу інцидентів.

Після приймання подій здійснюється їх нормалізація та попередня обробка. Події приводяться до уніфікованої структури, що дозволяє обробляти їх незалежно від джерела походження. У процесі нормалізації відбувається виділення ключових атрибутів, таких як ідентифікатор джерела, тип події, часові характеристики та додаткові параметри. Це створює єдину інформаційну модель подій безпеки.

Далі події надходять на аналітичний етап, де виконуються правила виявлення та кореляції. Окремі події аналізуються як у ізольованому вигляді, так і в контексті інших подій, що відбулися раніше або відбуваються паралельно. Саме на цьому етапі відбувається перетворення набору технічних подій у логічний інцидент інформаційної безпеки. Інцидент набуває визначених характеристик, зокрема типу, рівня критичності та потенційного впливу на систему.

Сформовані інциденти передаються до рівня управління реагуванням. Передача здійснюється у вигляді структурованих повідомлень, що містять необхідну інформацію для прийняття рішення про подальші дії. Важливим аспектом є те, що не всі інциденти потребують однакового реагування. Тому потік даних на цьому етапі може включати додаткову фільтрацію або пріоритизацію, що дозволяє зосередити ресурси на найбільш значущих загрозах.

На рівні управління реагуванням дані про інцидент використовуються для запуску сценаріїв реагування. Сценарій визначає послідовність дій, які мають бути виконані у відповідь на конкретний тип інциденту. Це можуть бути як технічні дії, так і інформаційні або організаційні заходи. Потік даних у цьому випадку набуває двостороннього характеру, оскільки результати виконаних дій можуть бути передані назад до аналітичного рівня для подальшого аналізу.

Завершальним етапом потоку даних є фіксація результатів реагування та аналіз ефективності виконаних дій. Інформація про інцидент, виконані сценарії та їх

результати зберігається для подальшого використання. Ці дані можуть бути використані для формування звітів, проведення аудитів і вдосконалення правил виявлення та реагування. Таким чином, потоки даних утворюють замкнений цикл, що підтримує безперервне вдосконалення технології.

Описані потоки даних демонструють, що запропонована технологія не обмежується лише виявленням інцидентів, а забезпечує їх повний життєвий цикл — від виникнення первинної події до аналізу результатів реагування. Такий підхід дозволяє інтегрувати моніторинг і управління інцидентами в єдиний технологічний процес, що відповідає сучасним вимогам до систем інформаційної безпеки.

3.2. Функціональні компоненти технології та їх призначення

Платформа Wazuh у межах запропонованої технології виконує роль центрального компонента моніторингу та виявлення інцидентів інформаційної безпеки. Її функціональне призначення полягає у безперервному зборі подій із контрольованого середовища, їх аналітичній обробці та формуванні структурованих інцидентів, які в подальшому використовуються для прийняття рішень щодо реагування. Саме на цьому етапі відбувається перетворення різномірних технічних подій у керовані об'єкти безпеки.

Wazuh забезпечує комплексний підхід до моніторингу, поєднуючи можливості аналізу журналів, контролю цілісності файлів, виявлення змін конфігурації та моніторингу активності системи. Такий підхід дозволяє охопити широкий спектр потенційних інцидентів, включаючи як зовнішні атаки, так і внутрішні порушення політик безпеки. Платформа орієнтована на глибокий аналіз стану хостів, що є критично важливим для сучасних розподілених інформаційних систем.

Однією з ключових функцій Wazuh є централізований збір подій безпеки. Події надходять як від агентів, встановлених на серверах і робочих станціях, так і від зовнішніх джерел, таких як мережеві пристрої та системи виявлення вторгнень. Це

дозволяє сформувати єдиний інформаційний простір, у межах якого здійснюється подальший аналіз. Централізація збору подій є основою для виявлення інцидентів, що охоплюють кілька компонентів інфраструктури.

Аналітичні можливості Wazuh базуються на застосуванні набору правил виявлення, які дозволяють ідентифікувати події, що мають відношення до інформаційної безпеки. Ці правила враховують як окремі ознаки подій, так і їх поєднання в часі. У результаті платформа здатна виявляти типові сценарії інцидентів, такі як спроби несанкціонованого доступу, ескалація привілеїв або порушення цілісності системних файлів.

Важливим аспектом функціонування Wazuh є класифікація та пріоритизація виявлених інцидентів. Кожному інциденту присвоюється певний рівень важливості, що дозволяє диференціювати події за ступенем їх потенційного впливу на інформаційну систему. Така класифікація створює основу для ефективного управління інцидентами та дозволяє зосередити увагу на найбільш критичних загрозах.

Wazuh також забезпечує контекстний аналіз подій, використовуючи інформацію про контрольовані хости, типи систем і їх роль у загальній архітектурі. Завдяки цьому однакові за технічними ознаками події можуть отримувати різну оцінку залежно від середовища, у якому вони виникли. Це підвищує точність виявлення інцидентів і зменшує кількість хибнопозитивних спрацювань.

У межах запропонованої технології Wazuh виконує не лише функцію виявлення, але й підготовку інформації для подальшого реагування. Сформовані інциденти містять структуровані дані, які можуть бути використані системою оркестрації реагування для запуску відповідних сценаріїв. Таким чином, Wazuh виступає як ключовий елемент, що забезпечує зв'язок між моніторингом і управлінням інцидентами.

Окрему увагу слід приділити можливостям масштабування платформи. Wazuh дозволяє поступово розширювати кількість контрольованих вузлів і джерел подій без

необхідності суттєвих змін архітектури. Це робить платформу придатною як для невеликих середовищ, так і для більших інфраструктур, що є важливим з точки зору практичної реалізації технології.

Агентна інфраструктура Wazuh є ключовим елементом запропонованої технології, що забезпечує глибокий і безперервний збір подій інформаційної безпеки безпосередньо з контрольованих хостів. Використання агентів дозволяє отримувати детальну інформацію про внутрішній стан систем, яка недоступна або обмежено доступна при використанні лише мережевих або безагентних методів моніторингу.

Агент Wazuh встановлюється на операційні системи серверів і робочих станцій та функціонує як фоновий процес, що взаємодіє з ядром операційної системи та її службами. Завдяки цьому агент має доступ до системних журналів, інформації про процеси, файлову систему та параметри конфігурації. Такий рівень доступу дозволяє фіксувати події, які безпосередньо відображають дії користувачів і програм, що є критично важливим для виявлення інцидентів внутрішнього характеру.

Однією з основних функцій агентної інфраструктури є збір журналів операційної системи. Агент аналізує системні та прикладні журнали, виділяючи події, що можуть мати відношення до інформаційної безпеки. Це включає події автентифікації, зміни облікових записів, запуск або зупинку сервісів, а також помилки та попередження, що можуть свідчити про аномальну поведінку системи. Такий підхід дозволяє отримувати структуровані дані для подальшого аналізу.

Важливим елементом роботи агентів є контроль цілісності файлів. Агентна інфраструктура забезпечує регулярну перевірку критичних файлів і каталогів на предмет змін, видалення або створення нових об'єктів. Будь-які відхилення від зафіксованого стану розглядаються як потенційні індикатори інциденту. Цей механізм є особливо важливим для виявлення компрометації системи, встановлення шкідливого програмного забезпечення або несанкціонованих змін конфігурації.

Агент Wazuh також виконує моніторинг активності процесів і служб. Він дозволяє відстежувати запуск нових процесів, зміну параметрів виконання та

завершення роботи сервісів. Аналіз такої інформації дає змогу виявляти нетипову поведінку, яка може бути пов'язана з виконанням шкідливого коду або спробами прихованої ескалації привілеїв. У межах запропонованої технології ці дані використовуються для формування контексту інцидентів.

Ще одним аспектом агентної інфраструктури є моніторинг змін конфігурації системи. Агент відстежує модифікації ключових конфігураційних файлів і параметрів, що впливають на безпеку. Зміни такого характеру можуть бути як результатом легітимних адміністративних дій, так і наслідком несанкціонованого втручання. Тому інформація про конфігураційні зміни є важливим джерелом для аналізу інцидентів.

Передача зібраних подій від агентів до центрального сервера здійснюється з використанням захищених каналів зв'язку. Це забезпечує конфіденційність і цілісність даних, що передаються, а також знижує ризик підміни або втрати інформації. Централізований характер обробки дозволяє корелювати події з різних агентів і формувати узагальнену картину безпеки.

Агентна інфраструктура також підтримує механізми управління та оновлення. Конфігурації агентів можуть змінюватися централізовано, що дозволяє адаптувати правила збору подій і рівень деталізації без необхідності ручного втручання на кожному хості. Це підвищує керованість системи та знижує адміністративні витрати.

Серверні компоненти Wazuh виконують центральну роль у запропонованій технології, забезпечуючи приймання, обробку, аналіз і збереження подій інформаційної безпеки, що надходять від агентів і зовнішніх джерел. Саме на серверному рівні відбувається трансформація розрізнених технічних подій у структуровані інциденти, які можуть бути використані для управління реагуванням і прийняття рішень.

Архітектура серверної частини Wazuh побудована за принципом розподілу функцій між кількома логічними компонентами, кожен з яких відповідає за окремий етап обробки подій. Такий підхід дозволяє підвищити продуктивність, забезпечити

масштабованість і спростити супровід системи. Серверна частина виконує роль аналітичного ядра всієї технології моніторингу та управління інцидентами.

Одним із ключових серверних компонентів є модуль приймання подій, який відповідає за отримання інформації від агентів і зовнішніх джерел. Цей компонент забезпечує контроль доставки подій, перевірку їх цілісності та початкову ідентифікацію джерела. На цьому етапі формується первинна структура повідомлень, що дозволяє системі коректно обробляти події незалежно від їх походження.

Після приймання події передаються до модулів декодування та аналізу. Декодування полягає у перетворенні сирих журналів у структурований формат, що містить виділені поля та атрибути. Цей процес є критично важливим, оскільки від якості декодування залежить можливість подальшої кореляції та класифікації подій. У межах Wazuh використовуються заздалегідь визначені шаблони декодування, які можуть бути розширені або модифіковані відповідно до специфіки контрольованого середовища.

Наступним етапом є застосування правил аналізу. Правила визначають логіку виявлення подій, що мають відношення до інформаційної безпеки, і дозволяють класифікувати їх за типами інцидентів. У процесі аналізу враховуються як окремі характеристики події, так і її взаємозв'язок з іншими подіями в часовому або логічному контексті. Це дозволяє виявляти не лише одиничні порушення, а й складні сценарії атак.

Серверні компоненти також забезпечують кореляцію подій, що надходять від різних агентів і джерел. Кореляція дозволяє об'єднувати окремі події в логічні ланцюги, які відображають розвиток інциденту в часі. Наприклад, послідовність невдалих спроб автентифікації, успішний вхід і подальша зміна системних файлів можуть бути об'єднані в єдиний інцидент з високим рівнем критичності. Такий підхід значно підвищує інформативність аналітичних результатів.

Важливою функцією серверної частини є присвоєння інцидентам рівнів важливості. Рівень важливості визначається на основі типу події, її контексту та

потенційного впливу на інформаційну систему. Це дозволяє реалізувати пріоритизацію інцидентів і забезпечити ефективний розподіл ресурсів реагування. У межах технології цей механізм використовується для визначення, які інциденти потребують негайного реагування, а які можуть бути оброблені в плановому режимі.

Серверні компоненти Wazuh також відповідають за збереження подій і інцидентів у централізованому сховищі. Збереження історичних даних є необхідним для проведення ретроспективного аналізу, розслідування інцидентів і підготовки звітів. Наявність структурованих даних дозволяє аналізувати тенденції, виявляти повторювані сценарії атак і оцінювати ефективність заходів безпеки.

Платформа Shuffle у межах запропонованої технології виконує функцію централізованого компонента автоматизованого реагування та оркестрації дій у відповідь на інциденти інформаційної безпеки. Її призначення полягає у формалізації процесів реагування, зменшенні часу між виявленням інциденту та виконанням необхідних заходів, а також у зниженні залежності від ручних дій персоналу.

Shuffle належить до класу SOAR-рішень, які орієнтовані на автоматизацію типових сценаріїв реагування та координацію дій між різними засобами захисту. У межах запропонованої технології платформа використовується як логічне продовження аналітичних можливостей Wazuh. Якщо Wazuh відповідає за виявлення та класифікацію інцидентів, то Shuffle забезпечує практичну реалізацію заходів протидії.

Основною концепцією Shuffle є використання сценаріїв реагування, які формалізують послідовність дій у відповідь на конкретні типи інцидентів. Сценарії створюються у вигляді логічних ланцюгів, що включають умови, перевірки та виконавчі дії. Такий підхід дозволяє структурувати процес реагування та забезпечити його повторюваність незалежно від того, хто саме ініціює обробку інциденту.

Важливою особливістю Shuffle є можливість поєднання автоматизованих і напівавтоматизованих дій. У випадках інцидентів із низьким або середнім рівнем критичності реагування може виконуватися повністю автоматично. Для більш

складних або потенційно небезпечних ситуацій платформа дозволяє включати етапи підтвердження або ухвалення рішення фахівцем. Це забезпечує баланс між швидкістю реагування та контролем з боку персоналу.

Shuffle підтримує інтеграцію з різними зовнішніми системами, що дозволяє використовувати її як центральний елемент координації реагування. У межах запропонованої технології платформа отримує інформацію про інциденти з Wazuh і використовує її для ініціації відповідних сценаріїв. Така інтеграція дозволяє уникнути ручного перенесення інформації між системами та мінімізує ризик помилок.

Значною перевагою Shuffle є її відкритість і модульність. Платформа дозволяє створювати та змінювати сценарії реагування без необхідності модифікації базової архітектури системи. Це дає змогу адаптувати технологію до змін у вимогах безпеки, появи нових типів інцидентів або оновлення політик організації. У контексті практичної реалізації це суттєво спрощує супровід і розвиток системи.

Shuffle також виконує важливу роль у документуванні процесів реагування. Усі дії, виконані в межах сценаріїв, фіксуються та можуть бути використані для подальшого аналізу, аудиту та вдосконалення технології. Це забезпечує прозорість процесів управління інцидентами та створює основу для оцінювання ефективності реагування.

Інтеграція платформи Wazuh із системою автоматизованого реагування Shuffle є ключовим елементом запропонованої технології моніторингу та управління інцидентами інформаційної безпеки. Саме на цьому етапі відбувається поєднання аналітичних можливостей SIEM із механізмами оркестрації та автоматизації реагування, що дозволяє реалізувати повний життєвий цикл інциденту в межах єдиної технологічної моделі.

На логічному рівні інтеграція базується на принципі подієвого тригеру. Wazuh виступає джерелом інформації про інциденти, а Shuffle — виконавчим середовищем, яке реагує на ці інциденти відповідно до визначених сценаріїв. Логічна взаємодія передбачає, що не кожна подія ініціює реагування, а лише ті інциденти, які

відповідають встановленим критеріям важливості та типу загрози. Це дозволяє уникнути надмірної автоматизації та зосередити ресурси на дійсно значущих ситуаціях.

У межах логічної моделі інтеграції визначається відповідність між типами інцидентів і сценаріями реагування. Для кожного класу інцидентів формується набір дій, які мають бути виконані у відповідь. Наприклад, інциденти, пов'язані з несанкціонованою автентифікацією, можуть ініціювати сценарій перевірки облікового запису та тимчасового обмеження доступу, тоді як інциденти, пов'язані зі змінами системних файлів, — сценарій ізоляції вузла та додаткового аналізу. Така логічна відповідність забезпечує структурованість і передбачуваність процесу реагування.

На програмному рівні інтеграція реалізується за допомогою механізмів передачі структурованих повідомлень. Wazuh формує повідомлення про інцидент, яке містить необхідний мінімум даних для ініціації реагування. До таких даних належать ідентифікатор інциденту, тип події, рівень критичності, джерело та часові характеристики. Ця інформація передається до Shuffle через програмні інтерфейси або механізми сповіщень, після чого система реагування інтерпретує отримані дані та запускає відповідний сценарій.

Важливою особливістю програмної інтеграції є незалежність компонентів. Wazuh і Shuffle не є жорстко пов'язаними між собою, що дозволяє змінювати або розширювати логіку реагування без втручання в аналітичну частину системи. Такий підхід відповідає принципам модульності та спрощує подальший розвиток технології. У разі зміни вимог безпеки або появи нових типів інцидентів можуть бути додані нові сценарії реагування без необхідності перебудови всієї архітектури.

Інтеграція також передбачає механізми обробки помилок і виняткових ситуацій. У випадку, якщо сценарій реагування не може бути виконаний автоматично або виникають технічні обмеження, система забезпечує можливість залучення фахівця

для ручного втручання. Це дозволяє зберегти контроль над критичними процесами та запобігти небажаним наслідкам автоматизованих дій.

Ще одним важливим аспектом інтеграції є забезпечення зворотного зв'язку між компонентами. Інформація про виконані дії реагування може бути використана для уточнення статусу інциденту або коригування аналітичних правил. Наприклад, підтвердження реального інциденту дозволяє підвищити пріоритет аналогічних подій у майбутньому, тоді як виявлення хибнопозитивного спрацювання сприяє оптимізації правил виявлення. Такий механізм зворотного зв'язку підвищує адаптивність технології.

Інтеграція Wazuh із Shuffle також сприяє стандартизації процесів управління інцидентами. Сценарії реагування формують єдині підходи до обробки типових інцидентів, що зменшує залежність від суб'єктивних рішень окремих фахівців. Це особливо важливо в умовах, коли реагування здійснюється різними командами або у змінних робочих змінах.

3.3. Технологічний процес моніторингу та управління інцидентами

Формування подій інформаційної безпеки є початковим і фундаментальним етапом технологічного процесу моніторингу та управління інцидентами. Саме на цьому етапі відбувається виникнення первинних сигналів, які в подальшому можуть бути ідентифіковані як інциденти інформаційної безпеки. Якість, повнота та достовірність таких подій безпосередньо впливають на ефективність усієї технології.

Події інформаційної безпеки виникають у результаті функціонування різних компонентів інформаційної інфраструктури. До них належать операційні системи серверів і робочих станцій, мережеві пристрої, прикладні сервіси, системи керування доступом та засоби захисту. Кожен із цих компонентів генерує журнали подій, які відображають як нормальну роботу системи, так і відхилення від штатного режиму.

У контексті запропонованої технології особливу увагу приділено подіям, що мають потенційний вплив на конфіденційність, цілісність і доступність інформаційних ресурсів. Такі події можуть бути пов'язані з автентифікацією користувачів, змінами облікових записів, доступом до критичних файлів, запуском процесів, мережевими з'єднаннями або модифікацією системних параметрів. Кожна з цих подій окремо не завжди є інцидентом, однак у сукупності вони можуть свідчити про реалізацію загрози.

Формування подій відбувається на різних рівнях інфраструктури. На рівні операційної системи це можуть бути події входу в систему, помилки автентифікації, зміни прав доступу або запуск системних служб. На рівні прикладних сервісів фіксуються події, пов'язані з обробкою запитів, доступом до даних, помилками виконання або аномальною поведінкою користувачів. На мережевому рівні формуються події, що відображають встановлення з'єднань, передачу даних і спроби доступу до сервісів.

Важливою особливістю процесу формування подій є їх різноманітність. Події можуть відрізнятися за форматом, структурою та рівнем деталізації залежно від джерела. Це ускладнює їх подальший аналіз і вимагає використання технологій, здатних працювати з різними типами даних. У межах запропонованої технології це враховується шляхом використання агентної інфраструктури та механізмів нормалізації подій.

Окрему категорію складають події, пов'язані з внутрішніми загрозами. Такі події часто не мають яскраво виражених ознак атаки та можуть виглядати як легітимні дії користувачів. Наприклад, послідовні зміни конфігурації, доступ до файлів у незвичний час або запуск нетипових процесів можуть свідчити про зловживання привілеями. Саме тому формування подій має охоплювати не лише очевидні порушення, а й детальну інформацію про поведінку системи.

Етап виявлення та класифікації інцидентів є ключовим у технологічному процесі моніторингу та управління інформаційною безпекою, оскільки саме на цьому

етапі відбувається перехід від набору різнорідних подій до формалізованих інцидентів, які можуть бути об'єктом управління. У межах запропонованої технології цей етап повністю реалізується в аналітичному середовищі платформи Wazuh.

Процес виявлення інцидентів починається з аналізу подій, що надходять від агентів та зовнішніх джерел. Кожна подія порівнюється з набором аналітичних правил, які описують відомі ознаки порушень безпеки або аномальної поведінки. Такі правила формуються на основі практичних сценаріїв атак, вимог безпеки та типових моделей загроз. У результаті події, що відповідають заданим критеріям, виділяються як потенційно небезпечні.

Виявлення інцидентів у Wazuh не обмежується аналізом одиничних подій. Важливу роль відіграє кореляційний аналіз, який дозволяє враховувати взаємозв'язок між подіями в часі та просторі. Наприклад, поєднання декількох невдалих спроб автентифікації з подальшим успішним входом і зміною системних параметрів може бути інтерпретоване як інцидент несанкціонованого доступу, навіть якщо кожна з подій окремо не виглядає критичною. Такий підхід дозволяє виявляти складні багатоступеневі атаки.

Окрему увагу приділено контекстному аналізу подій. У процесі виявлення інцидентів враховується не лише технічний зміст події, а й середовище, у якому вона виникла. До контекстних факторів належать тип хоста, його роль у інфраструктурі, рівень доступу користувача, час виникнення події та історія попередніх інцидентів. Це дозволяє відрізнити легітимні дії від потенційно небезпечних і зменшувати кількість хибнопозитивних спрацювань.

Після виявлення інциденту здійснюється його класифікація. Класифікація передбачає віднесення інциденту до певної категорії залежно від його природи та потенційного впливу. У межах запропонованої технології інциденти можуть бути пов'язані з порушенням конфіденційності, цілісності або доступності інформаційних ресурсів. Такий поділ відповідає класичній моделі інформаційної безпеки та дозволяє структурувати процес реагування.

Важливим аспектом класифікації є визначення рівня критичності інциденту. Рівень критичності відображає ступінь потенційної шкоди, яку інцидент може завдати інформаційній системі. На цьому етапі враховуються такі фактори, як тип активу, що зазнав впливу, можливі наслідки інциденту та швидкість його розвитку. Пріоритизація інцидентів дозволяє ефективно розподіляти ресурси реагування та зосереджувати увагу на найбільш небезпечних ситуаціях.

Класифікація інцидентів також створює основу для подальшої автоматизації реагування. Для кожної категорії та рівня критичності можуть бути визначені відповідні сценарії дій, що реалізуються на наступних етапах технологічного процесу. Таким чином, інцидент набуває не лише описового, а й функціонального значення в системі управління безпекою.

У межах середовища Wazuh результати виявлення та класифікації інцидентів фіксуються у централізованому сховищі. Це дозволяє забезпечити історичну простежуваність, проводити аналіз тенденцій та використовувати накопичені дані для вдосконалення правил виявлення. Наявність структурованої інформації про інциденти також є важливою для підготовки звітності та проведення аудитів.

Після виявлення та класифікації інциденту наступним етапом технологічного процесу є його передача до системи реагування та ініціація відповідних сценаріїв дій. На цьому етапі інцидент переходить зі стану аналітичного об'єкта до стану керованої події, що вимагає практичних заходів протидії. Якість і коректність цього переходу визначають ефективність усього процесу управління інцидентами.

Передача інцидентів до системи реагування здійснюється на основі визначених критеріїв, що враховують тип інциденту, рівень його критичності та контекст виникнення. Не всі інциденти потребують негайного або автоматизованого реагування, тому в межах запропонованої технології передбачено механізм відбору інцидентів, які мають бути передані на наступний рівень обробки. Такий підхід дозволяє уникнути перевантаження системи реагування та зосередити ресурси на найбільш значущих загрозах.

У процесі передачі інциденту формується структурований опис, що містить ключову інформацію, необхідну для ініціації реагування. До такої інформації належать ідентифікатор інциденту, його категорія, рівень критичності, джерело виникнення, цільовий актив та часові параметри. Структурованість даних забезпечує однозначне трактування інциденту та створює умови для автоматизованої обробки на наступному етапі.

Ініціація сценаріїв реагування базується на відповідності між характеристиками інциденту та заздалегідь визначеними сценаріями дій. Для кожної категорії інцидентів у межах технології можуть бути визначені окремі сценарії, які відрізняються за складністю, рівнем автоматизації та набором виконуваних дій. Це дозволяє адаптувати реагування до конкретної ситуації та уникати застосування універсальних, але неефективних заходів.

Сценарії реагування можуть включати як технічні, так і організаційні дії. До технічних дій належать обмеження доступу, ізоляція вузлів, блокування облікових записів або ініціація додаткових перевірок. Організаційні дії можуть передбачати інформування відповідальних осіб, ескалацію інциденту або ініціацію процедур розслідування. Поєднання різних типів дій дозволяє забезпечити комплексний підхід до реагування.

Важливим аспектом ініціації сценаріїв є можливість врахування додаткових умов. Наприклад, сценарій може бути активований лише за умови підтвердження інциденту або при досягненні певного порогу критичності. Це зменшує ризик виконання необґрунтованих дій і підвищує точність реагування. Такий механізм особливо важливий у середовищах із великою кількістю подій і різнорідними джерелами даних.

Передача інцидентів і запуск сценаріїв реагування також передбачають фіксацію стану інциденту. Інцидент переходить у статус обробки, що дозволяє відстежувати його життєвий цикл і контролювати виконання дій. Це створює основу

для подальшого аналізу ефективності реагування та забезпечує прозорість процесів управління.

Етап оркестрації та автоматизації реагування є центральним у практичній реалізації запропонованої технології, оскільки саме на цьому рівні здійснюється виконання конкретних дій у відповідь на виявлені інциденти інформаційної безпеки. Оркестрація дозволяє координувати послідовність дій, задіювати різні компоненти інформаційної інфраструктури та забезпечувати узгодженість реагування незалежно від складності інциденту.

Автоматизація реагування спрямована на скорочення часу між моментом виявлення інциденту та початком активних заходів протидії. У традиційних підходах значна частина часу витрачається на ручний аналіз і прийняття рішень, що може призводити до поглиблення наслідків інциденту. Запропонована технологія передбачає використання заздалегідь визначених сценаріїв, які дозволяють виконувати типові дії без затримок, пов'язаних із людським фактором.

Оркестрація реагування реалізується як керований процес, що складається з кількох логічних етапів. На початковому етапі сценарій реагування отримує інформацію про інцидент, включаючи його тип, критичність і контекст. На основі цієї інформації визначається набір дій, які мають бути виконані. Дії можуть виконуватися послідовно або паралельно залежно від логіки сценарію та вимог до реагування.

Автоматизовані дії можуть охоплювати широкий спектр заходів, спрямованих на локалізацію та мінімізацію наслідків інциденту. До таких заходів належать обмеження доступу до ресурсів, ізоляція скомпрометованих вузлів, призупинення підозрілих процесів або ініціація додаткових перевірок. Вибір конкретних дій визначається характером інциденту та політиками безпеки, що діють у середовищі.

Важливим аспектом автоматизації є можливість умовного виконання дій. Сценарії реагування можуть містити перевірки, які дозволяють уточнити стан системи перед виконанням наступного кроку. Наприклад, перед блокуванням облікового запису може бути перевірено, чи не є активність користувача легітимною. Такий

підхід дозволяє уникнути надмірних або помилкових дій і зберегти стабільність функціонування системи.

Оркестрація також передбачає координацію між різними засобами захисту та елементами інфраструктури. У межах одного сценарію можуть бути задіяні кілька компонентів, кожен з яких виконує свою частину завдання. Координація дій забезпечує цілісність реагування та дозволяє досягти необхідного ефекту з мінімальними витратами ресурсів.

Автоматизація реагування не виключає участі фахівців інформаційної безпеки. Для інцидентів із високим рівнем критичності або складною природою можуть бути передбачені етапи підтвердження або ручного втручання. Це дозволяє поєднати швидкість автоматизованих дій із гнучкістю експертного аналізу та прийняття рішень у нестандартних ситуаціях.

У процесі оркестрації всі виконані дії фіксуються та документуються. Це забезпечує прозорість процесу реагування і створює можливість для подальшого аналізу ефективності дій. Наявність детальної інформації про перебіг реагування є важливою для вдосконалення сценаріїв і підвищення загального рівня зрілості технології.

Ескалація інцидентів і контроль виконання дій реагування є завершальним етапом технологічного процесу моніторингу та управління інцидентами інформаційної безпеки. Цей етап забезпечує перехід від автоматизованих або напівавтоматизованих дій до керованого процесу прийняття рішень на рівні персоналу у випадках, коли інцидент має підвищену складність, критичність або потребує додаткового аналізу.

Ескалація інциденту застосовується у випадках, коли автоматизовані сценарії реагування не можуть повністю усунути загрозу або коли існує ризик значного впливу на інформаційну систему. До таких ситуацій належать інциденти, пов'язані з компрометацією критичних активів, можливим витоків інформації, порушенням доступності ключових сервісів або ознаками цілеспрямованих атак. У таких випадках

залучення фахівців інформаційної безпеки є необхідною умовою ефективного реагування.

Процес ескалації базується на визначених критеріях, які враховують рівень критичності інциденту, його тривалість, масштаб впливу та результати попередніх дій реагування. Якщо інцидент не може бути локалізований у межах стандартного сценарію або його параметри перевищують допустимі порогові значення, він переводиться на вищий рівень обробки. Такий підхід дозволяє систематизувати процес ескалації та уникнути хаотичних рішень.

У межах запропонованої технології ескалація реалізується як керований процес передачі інциденту відповідальним особам або групам. Разом з інцидентом передається повний контекст, включаючи інформацію про джерела подій, виконані дії реагування та поточний стан системи. Це дозволяє фахівцям швидко зорієнтуватися в ситуації та прийняти обґрунтовані рішення без необхідності повторного аналізу всіх даних з нуля.

Контроль виконання дій реагування є невід'ємною частиною управління інцидентами. Навіть у випадках автоматизованого реагування необхідно забезпечити перевірку того, що виконані дії призвели до очікуваного результату. Контроль дозволяє виявляти ситуації, коли застосовані заходи не дали бажаного ефекту або призвели до побічних наслідків, що потребують корекції.

У межах технології контроль виконання дій здійснюється шляхом аналізу подій, що виникають після реагування. Наприклад, після ізоляції вузла або обмеження доступу відстежується, чи припинилася підозріла активність і чи відновився стабільний стан системи. Такий підхід дозволяє оцінювати ефективність реагування на практиці, а не лише формально фіксувати виконання дій.

Ескалація та контроль виконання дій також сприяють накопиченню досвіду реагування на інциденти. Інформація про складні інциденти, прийняті рішення та їх наслідки може бути використана для вдосконалення сценаріїв автоматизованого реагування, уточнення правил виявлення та підвищення загального рівня зрілості

технології. Таким чином, технологія набуває властивостей адаптивності та безперервного вдосконалення.

Важливою складовою цього етапу є документування процесу управління інцидентом. Фіксація етапів ескалації, виконаних дій і отриманих результатів створює основу для подальшого аналізу, звітності та аудиту. Наявність такої інформації є важливою не лише з точки зору внутрішнього управління безпекою, а й для підтвердження відповідності вимогам стандартів та нормативних документів.

3.4. Практична реалізація технології в тестовому середовищі

Практична реалізація технології моніторингу та управління інцидентами інформаційної безпеки потребує попереднього визначення вимог до апаратного та програмного забезпечення. Ці вимоги формуються з урахуванням функціонального навантаження компонентів технології, обсягів оброблюваних даних, а також необхідності забезпечення стабільної та безперервної роботи системи моніторингу і реагування.

Запропонована технологія орієнтована на розгортання в умовах обмежених ресурсів, що є характерним для навчальних, дослідницьких або невеликих корпоративних середовищ. Водночас її архітектура дозволяє масштабування у разі зростання навантаження або кількості контрольованих вузлів. Саме тому вимоги до апаратного забезпечення визначаються з урахуванням базового сценарію використання з можливістю подальшого розширення.

Для розгортання серверної частини технології необхідна окрема обчислювальна система, яка виконуватиме функції центрального вузла моніторингу та аналізу. До мінімальних апаратних вимог такого сервера належать багатоядерний процесор, достатній обсяг оперативної пам'яті та надійна система зберігання даних. Обчислювальні ресурси сервера мають забезпечувати одночасну обробку подій від декількох агентів, виконання аналітичних правил та зберігання історичних даних.

Оперативна пам'ять є критично важливим ресурсом, оскільки значна частина аналітичних операцій виконується в пам'яті. Недостатній обсяг оперативної пам'яті може призводити до затримок у виявленні інцидентів або втрати подій. З урахуванням цього для тестового середовища доцільно передбачати запас оперативної пам'яті, який дозволить стабільно обробляти пікові навантаження.

Система зберігання даних повинна забезпечувати достатній обсяг для накопичення журналів подій і інформації про інциденти. Оскільки технологія передбачає збереження історичних даних для аналізу та аудиту, обсяг сховища визначається не лише поточними потребами, а й перспективою довгострокового зберігання. Для тестового середовища допустиме використання стандартних накопичувачів, однак у разі масштабування доцільно враховувати питання продуктивності дискової підсистеми.

Крім серверної частини, до апаратних вимог належать ресурси контрольованих вузлів, на яких встановлюються агенти моніторингу. Агенти не потребують значних обчислювальних ресурсів і можуть працювати на типових робочих станціях або серверах без істотного впливу на їх продуктивність. Це є важливою перевагою агентної моделі, оскільки вона дозволяє охоплювати широкий спектр систем без необхідності їх модернізації.

З програмної точки зору технологія базується на використанні сучасних операційних систем серверного класу. Вибір операційної системи визначається вимогами сумісності з компонентами платформи моніторингу та реагування, а також зручністю адміністрування. Для тестового середовища доцільним є використання стабільних та поширених дистрибутивів, які забезпечують підтримку необхідних сервісів і механізмів безпеки.

Програмне забезпечення серверної частини включає компоненти моніторингу, аналітичної обробки та зберігання даних. Важливою вимогою є наявність механізмів керування сервісами, моніторингу їх стану та журналювання помилок. Це дозволяє

своєчасно виявляти проблеми у роботі технології та забезпечувати її безперервне функціонування.

Для реалізації автоматизованого реагування необхідне окреме програмне середовище, яке забезпечує виконання сценаріїв, інтеграцію з аналітичною частиною та керування логікою реагування. Програмні вимоги до цього компонента включають підтримку мережових взаємодій, можливість виконання сценаріїв та механізми контролю доступу. Важливою умовою є сумісність із платформою моніторингу, що забезпечує коректний обмін даними між компонентами технології.

Окремо слід враховувати вимоги до мережової інфраструктури. Для коректної роботи технології необхідне стабільне мережеве з'єднання між агентами, сервером моніторингу та компонентом реагування. Мережа має забезпечувати достатню пропускну здатність для передачі подій без значних затримок, а також підтримувати захищені канали обміну даними.

З точки зору безпеки, програмне та апаратне забезпечення повинні відповідати базовим вимогам захисту. Це включає обмеження доступу до серверних компонентів, використання захищених протоколів зв'язку та регулярне оновлення програмних компонентів. Забезпечення базового рівня захисту є необхідною умовою, оскільки система моніторингу сама по собі є критичним елементом інформаційної інфраструктури.

Розгортання платформи Wazuh є базовим етапом практичної реалізації запропонованої технології моніторингу та управління інцидентами інформаційної безпеки. Саме на цьому етапі формується технічне середовище, у межах якого здійснюється збір, аналіз і кореляція подій безпеки з контрольованих вузлів інформаційної інфраструктури.

Процес розгортання доцільно розділити на два логічні етапи: встановлення та налаштування серверної частини Wazuh і розгортання агентної інфраструктури на контрольованих хостах. Такий підхід дозволяє поступово вводити систему в експлуатацію та спрощує усунення можливих проблем на кожному з етапів.

Першим кроком є підготовка серверного середовища. Для цього обирається окрема система, яка виконуватиме роль центрального вузла моніторингу. На сервері встановлюється операційна система серверного класу з мінімальним набором служб, необхідних для стабільної роботи. Перед встановленням платформи моніторингу доцільно виконати базове налаштування системи, зокрема оновлення пакетів, налаштування мережевих інтерфейсів і обмеження доступу до адміністративних сервісів.

Після підготовки операційного середовища здійснюється встановлення серверної частини Wazuh. Серверний компонент виконує функції приймання подій від агентів, аналітичної обробки та зберігання результатів аналізу. Під час встановлення формується базова конфігурація сервісів, визначаються мережеві порти для обміну даними та ініціалізується структура сховища подій. Важливою умовою є коректне налаштування сервісів запуску та моніторингу стану компонентів, що забезпечує автоматичне відновлення роботи у разі збоїв.

На етапі налаштування серверної частини визначаються параметри приймання подій, рівні деталізації журналювання та правила базової обробки даних. Це дозволяє адаптувати систему до особливостей тестового середовища та уникнути надмірного навантаження на серверні ресурси. Також на цьому етапі налаштовуються механізми збереження історичних даних, що є важливим для подальшого аналізу інцидентів.

Наступним кроком є розгортання агентної інфраструктури. Агенти Wazuh встановлюються на сервери та робочі станції, які підлягають моніторингу. Встановлення агентів виконується з урахуванням типу операційної системи та ролі хоста в інфраструктурі. Перед встановленням агентів доцільно визначити перелік контрольованих вузлів і їх пріоритетність, що дозволяє поетапно вводити систему в експлуатацію.

Після встановлення агентів здійснюється їх реєстрація на сервері моніторингу. Реєстрація забезпечує автентифікацію агентів і формування захищеного каналу обміну даними. Це є важливим з точки зору безпеки, оскільки передача подій без

належного захисту може створювати додаткові ризики. Захищений обмін даними гарантує цілісність і достовірність інформації, що надходить до системи аналізу.

Налаштування агентів включає визначення джерел подій, які підлягають збору. До таких джерел належать системні журнали, журнали прикладних сервісів, інформація про зміни у файловій системі та конфігурації. Рівень деталізації збору подій може змінюватися залежно від ролі хоста. Наприклад, для серверів із критичними сервісами доцільно застосовувати більш детальний моніторинг, ніж для робочих станцій користувачів.

Важливою частиною розгортання є перевірка коректності роботи агентної інфраструктури. Після підключення агентів до сервера моніторингу здійснюється тестування передачі подій і перевірка їх відображення в аналітичному середовищі. Це дозволяє переконатися, що система коректно збирає дані та готова до подальшого аналізу інцидентів.

У процесі розгортання можуть виникати типові проблеми, пов'язані з мережевими обмеженнями, некоректними налаштуваннями доступу або несумісністю версій програмного забезпечення. Для їх усунення доцільно використовувати поетапний підхід до введення агентів у роботу та постійно контролювати стан серверних компонентів. Такий підхід дозволяє мінімізувати ризик масових збоїв і забезпечити стабільну роботу системи.

Налаштування правил виявлення інцидентів є ключовим етапом практичної реалізації технології моніторингу та управління інцидентами інформаційної безпеки. Саме на цьому етапі визначається, які події в інформаційній інфраструктурі будуть розглядатися як потенційні інциденти, яким чином вони класифікуватимуться та з яким рівнем критичності передаватимуться на подальшу обробку. Від якості налаштування правил безпосередньо залежить точність виявлення загроз і ефективність реагування.

Правила виявлення інцидентів у середовищі Wazuh ґрунтуються на аналізі подій, що надходять від агентів та зовнішніх джерел. Кожне правило описує умови, за

яких певна подія або сукупність подій інтерпретується як інцидент інформаційної безпеки. Такі умови можуть включати відповідність певним шаблонам журналів, перевищення порогових значень, повторюваність подій у визначений часовий інтервал або поєднання кількох факторів.

На початковому етапі налаштування доцільно використовувати базовий набір правил, який охоплює найбільш поширені сценарії інцидентів. До них належать спроби несанкціонованого доступу, численні помилки автентифікації, зміни системних файлів, запуск підозрілих процесів і порушення конфігурації системи. Такий базовий набір дозволяє забезпечити мінімально необхідний рівень захисту та перевірити коректність роботи всієї технології.

Налаштування правил також передбачає визначення рівнів критичності інцидентів. Рівень критичності відображає ступінь потенційного впливу інциденту на інформаційну систему та використовується для пріоритизації реагування. У межах запропонованої технології доцільно застосовувати багаторівневу шкалу критичності, що дозволяє диференціювати інциденти та уникати однакового підходу до подій різної важливості.

Особливу увагу слід приділити налаштуванню правил кореляції. Кореляційні правила дозволяють об'єднувати окремі події в логічні ланцюги та виявляти складні сценарії атак. Наприклад, поєднання кількох невдалих спроб входу, подальшого успішного доступу та змін у системних файлах може свідчити про компрометацію облікового запису. Без кореляційного аналізу такі події могли б залишитися непоміченими або бути оцінені як несуттєві.

Розгортання платформи Shuffle є наступним етапом практичної реалізації технології моніторингу та управління інцидентами інформаційної безпеки. Цей етап спрямований на створення середовища автоматизованого реагування, яке забезпечує виконання сценаріїв дій у відповідь на інциденти, виявлені аналітичним компонентом технології. Shuffle використовується як центральний елемент оркестрації реагування, що дозволяє координувати дії різних компонентів інформаційної інфраструктури.

Перед розгортанням платформи визначається середовище її встановлення. Для тестового варіанта доцільним є розгортання Shuffle на окремій віртуальній або фізичній системі, що дозволяє ізолювати компонент реагування від аналітичної частини та спростити адміністрування. Такий підхід також відповідає принципу розмежування функцій між компонентами технології, що підвищує її надійність і керованість.

Після підготовки операційного середовища виконується встановлення основних сервісів Shuffle. На цьому етапі формується базова конфігурація платформи, визначаються параметри доступу та налаштовується мережеве з'єднання з іншими компонентами технології. Важливо забезпечити стабільний і захищений обмін даними, оскільки Shuffle отримує інформацію про інциденти та ініціює дії, що можуть впливати на стан системи.

Наступним кроком є налаштування механізмів автентифікації та авторизації в середовищі Shuffle. Оскільки платформа дозволяє створювати та змінювати сценарії реагування, доступ до її функцій повинен бути обмежений відповідно до ролей користувачів. Це дозволяє запобігти несанкціонованим змінам сценаріїв і забезпечити контроль над процесами реагування.

Після завершення базового налаштування платформи здійснюється підготовка середовища для створення сценаріїв реагування. На цьому етапі визначаються логічні категорії інцидентів, які будуть оброблятися в системі, та загальні підходи до реагування. Така підготовка дозволяє структурувати сценарії та уникнути хаотичного накопичення логіки реагування.

Важливою складовою розгортання є налаштування інтеграцій із зовнішніми системами. Shuffle підтримує взаємодію з різними компонентами інформаційної інфраструктури, що дозволяє виконувати дії реагування безпосередньо в середовищі, де виник інцидент. У межах запропонованої технології основна інтеграція здійснюється з аналітичним компонентом, проте архітектура платформи дозволяє розширювати перелік інтеграцій у разі потреби.

Після завершення налаштувань виконується тестування платформи Shuffle. Тестування включає перевірку коректності приймання повідомлень про інциденти, запуск тестових сценаріїв реагування та контроль виконання дій. На цьому етапі важливо переконатися, що сценарії виконуються у правильній послідовності та не призводять до небажаних наслідків для системи.

У процесі розгортання можуть виникати типові проблеми, пов'язані з мережевою взаємодією, помилками конфігурації або некоректною логікою сценаріїв. Для їх усунення доцільно застосовувати поетапний підхід до налаштування та тестування, що дозволяє швидко локалізувати джерело проблеми. Такий підхід підвищує надійність розгортання та зменшує ризик помилок на етапі експлуатації.

Розробка та застосування сценаріїв реагування є завершальним етапом формування практичної частини запропонованої технології. Саме сценарії визначають конкретні дії, які виконуються у відповідь на виявлені інциденти, і перетворюють результати аналітичного моніторингу на практичні заходи протидії. У межах технології сценарії реагування реалізуються в середовищі Shuffle та формуються з урахуванням типу інциденту, рівня його критичності та контексту виникнення.

Одним із типових сценаріїв реагування є обробка інцидентів, пов'язаних із несанкціонованими спробами автентифікації. У цьому випадку аналітичний компонент виявляє серію невдалих спроб входу з подальшим успішним доступом або перевищенням допустимої кількості помилок автентифікації. Сценарій реагування передбачає фіксацію інциденту, перевірку параметрів облікового запису та виконання дій, спрямованих на обмеження потенційної шкоди. До таких дій може належати тимчасове блокування облікового запису, сповіщення відповідальних осіб і ініціація додаткового аналізу активності користувача.

Іншим прикладом є сценарій реагування на порушення цілісності файлів. У разі виявлення несанкціонованих змін у критичних системних або прикладних файлах формується інцидент, що потребує негайного реагування. Сценарій може включати

перевірку характеру змін, визначення джерела модифікації та виконання заходів з локалізації впливу. У разі необхідності може бути ініційована ізоляція відповідного вузла від мережі для запобігання подальшому поширенню загрози.

Сценарії реагування також можуть застосовуватися для обробки інцидентів, пов'язаних із підозрілою активністю процесів. Наприклад, запуск нетипових процесів або зміна параметрів виконання системних служб може свідчити про наявність шкідливого програмного забезпечення. У такому випадку сценарій реагування передбачає аналіз параметрів процесу, перевірку його походження та виконання дій, спрямованих на припинення потенційно небезпечної активності. За необхідності можуть бути зібрані додаткові дані для подальшого розслідування.

Окрему категорію становлять сценарії реагування на інциденти, пов'язані з порушенням конфігурації системи. Зміни критичних параметрів можуть призводити до зниження рівня захисту або створювати умови для подальших атак. Сценарій реагування в цьому випадку може включати фіксацію змін, перевірку їх відповідності встановленим політикам безпеки та відновлення коректних налаштувань. Такий підхід дозволяє оперативно усувати наслідки несанкціонованих або помилкових змін.

Важливою особливістю сценаріїв реагування є можливість поєднання автоматизованих і контрольованих дій. Для інцидентів із низьким або середнім рівнем критичності реагування може виконуватися повністю автоматично, тоді як для більш серйозних інцидентів передбачено залучення фахівців інформаційної безпеки. Це дозволяє забезпечити баланс між швидкістю реагування та необхідністю експертного контролю.

Сценарії реагування формуються з урахуванням можливості повторного використання та адаптації. У разі появи нових типів інцидентів або змін у вимогах безпеки сценарії можуть бути доповнені або модифіковані без необхідності перебудови всієї технології. Такий підхід сприяє гнучкості та довготривалій актуальності запропонованого рішення.

У процесі виконання сценаріїв усі дії фіксуються та можуть бути використані для подальшого аналізу ефективності реагування. Накопичення такої інформації дозволяє виявляти найбільш поширені типи інцидентів, оцінювати доцільність автоматизації окремих дій та вдосконалювати логіку реагування. Це створює передумови для поступового підвищення рівня зрілості технології управління інцидентами.

3.5. Оцінювання ефективності запропонованої технології

Практична оцінка ефективності запропонованої технології спрямована на визначення того, наскільки її застосування дозволяє покращити процеси моніторингу та управління інцидентами інформаційної безпеки порівняно з підходами, що не використовують автоматизовану кореляцію та оркестрацію реагування. Оцінювання здійснюється на основі визначених критеріїв і показників, що відображають ключові аспекти функціонування технології.

Для оцінювання використовується модель умовного тестового середовища, у якому реалізовано моніторинг подій, їх аналітичну обробку та автоматизоване реагування. Як базу для порівняння розглядається варіант ручного або частково автоматизованого управління інцидентами, за якого виявлення і реагування виконуються без використання інтегрованої SIEM–SOAR технології. Такий підхід дозволяє наочно продемонструвати переваги запропонованого рішення.

Одним із ключових показників є час виявлення інциденту. У разі відсутності централізованого моніторингу значна частина інцидентів виявляється із затримкою, що може становити десятки хвилин або навіть години. Запропонована технологія дозволяє скоротити цей час за рахунок безперервного збору подій і автоматизованого аналізу. Це створює умови для оперативного реагування та зменшення потенційного впливу інцидентів.

Не менш важливим показником є точність виявлення інцидентів. Завдяки використанню кореляційних правил і контекстного аналізу зменшується кількість хибнопозитивних спрацювань. Це дозволяє уникнути ситуацій, коли система перевантажена помилковими інцидентами, і забезпечує більш цілеспрямоване реагування на реальні загрози.

Таблиця 3.1

Оцінка ефективності запропонованої технології моніторингу та управління інцидентами

Показник	Без використання технології	З використанням Wazuh + Shuffle	Оцінка результату
Час виявлення інциденту	Високий (десятки хвилин)	Низький (кілька хвилин)	Значне скорочення
Час реагування	Залежить від персоналу	Автоматизований, мінімальний	Підвищення оперативності
Кількість хибнопозитивних інцидентів	Висока	Помірна	Покращення точності
Навантаження на персонал	Високе	Знижене	Оптимізація ресурсів
Рівень автоматизації	Низький	Високий	Підвищення зрілості процесів
Масштабованість	Обмежена	Висока	Підвищення адаптивності

Отримані результати свідчать про те, що застосування запропонованої технології дозволяє суттєво підвищити ефективність управління інцидентами інформаційної безпеки. Особливо помітним є скорочення часу виявлення та реагування, а також зменшення навантаження на персонал за рахунок автоматизації типових процесів.

Практична оцінка також демонструє, що технологія має потенціал для подальшого розвитку та масштабування. За рахунок гнучкої архітектури та

можливості адаптації правил і сценаріїв реагування вона може бути використана як у тестових, так і в реальних інформаційних середовищах різного рівня складності.

3.6. Обмеження запропонованої технології та напрями її подальшого розвитку

Незважаючи на практичну придатність і ефективність запропонованої технології моніторингу та управління інцидентами інформаційної безпеки, її застосування має певні обмеження, які необхідно враховувати під час впровадження та експлуатації. Аналіз таких обмежень дозволяє більш об'єктивно оцінити можливості технології та визначити напрями її подальшого вдосконалення.

Одним із ключових обмежень є залежність ефективності технології від якості початкових налаштувань. Неправильно налаштовані правила виявлення або сценарії реагування можуть призводити до зростання кількості хибнопозитивних або хибнонегативних інцидентів. Це означає, що на початковому етапі впровадження необхідні часові витрати на адаптацію правил і сценаріїв до конкретного середовища, що може ускладнювати швидке введення технології в експлуатацію.

Іншим обмеженням є потреба в обчислювальних ресурсах. Хоча платформа Wazuh та оркестраційне середовище Shuffle можуть бути розгорнуті в умовах обмежених ресурсів, зі зростанням кількості контрольованих вузлів і обсягу подій зростає навантаження на серверну інфраструктуру. У разі недостатніх ресурсів це може призводити до затримок у обробці подій або зниження загальної продуктивності системи.

Також слід враховувати складність розробки та супроводу сценаріїв реагування. Автоматизовані сценарії потребують ретельного тестування, оскільки помилки в логіці можуть призводити до небажаних наслідків, зокрема до порушення доступності сервісів або некоректного обмеження доступу користувачів. Це вимагає наявності

кваліфікованих фахівців, які здатні не лише налаштувати технологію, а й підтримувати її актуальність.

Обмеженням є і залежність від актуальності правил та сценаріїв. Інформаційні загрози постійно змінюються, з'являються нові методи атак і вектори компрометації. Без регулярного оновлення аналітичної бази та сценаріїв реагування ефективність технології з часом знижується. Тому її використання передбачає постійний процес удосконалення та адаптації до нових умов.

Окрему увагу слід приділити людському фактору. Хоча технологія значною мірою автоматизує процеси управління інцидентами, остаточно відповідальність за прийняття рішень у критичних ситуаціях залишається за персоналом. Недостатня підготовка фахівців або відсутність чітко визначених процедур може знижувати ефективність навіть добре налаштованої системи.

Разом із тим виявлені обмеження визначають і напрями подальшого розвитку технології. Одним із перспективних напрямів є поглиблення механізмів автоматичної адаптації правил виявлення інцидентів на основі накопичених даних. Використання статистичних методів або елементів машинного навчання дозволило б підвищити точність виявлення та зменшити кількість хибнопозитивних спрацювань.

Іншим напрямом розвитку є розширення інтеграцій з іншими засобами захисту та управління інформаційною безпекою. Інтеграція з додатковими джерелами даних і системами керування дозволила б забезпечити більш комплексний підхід до управління інцидентами та підвищити рівень ситуаційної обізнаності.

Таким чином, аналіз обмежень і напрямів подальшого розвитку показує, що запропонована технологія є життєздатним і перспективним рішенням у сфері моніторингу та управління інцидентами інформаційної безпеки. Водночас її ефективне застосування потребує системного підходу, постійного вдосконалення та адаптації до змін у середовищі загроз.

ВИСНОВКИ

Сучасний стан розвитку інформаційних технологій і цифровізації організаційних процесів супроводжується зростанням кількості та складності інцидентів інформаційної безпеки. Динамічність загроз, різноманіття векторів атак і високі вимоги до безперервності функціонування інформаційних систем зумовлюють необхідність переходу від фрагментарних і реактивних підходів до системного, технологічно обґрунтованого управління інцидентами. У цьому контексті моніторинг і реагування перестають бути допоміжними процесами та набувають статусу ключових елементів системи кіберзахисту.

У межах роботи було проаналізовано проблему моніторингу та управління інцидентами інформаційної безпеки як комплексну задачу, що поєднує технічні, організаційні та процесні аспекти. Показано, що інцидент інформаційної безпеки слід розглядати не лише як окрему подію, а як об'єкт управління, що має власний життєвий цикл, характеристики впливу та контекст виникнення. Такий підхід створює передумови для формалізації процесів реагування та підвищення їх керованості.

У результаті аналізу теоретичних засад встановлено, що традиційні підходи до управління інцидентами часто не забезпечують необхідної оперативності та масштабованості, особливо в умовах великої кількості подій і обмежених ресурсів персоналу. Обґрунтовано доцільність використання централізованих платформ моніторингу та оркестрації реагування як основи для побудови сучасних технологій управління інцидентами. Окрему увагу приділено ролі кореляції подій, автоматизації рутинних дій та формалізації сценаріїв реагування.

Проведений огляд сучасних технологій моніторингу показав, що SIEM-платформи забезпечують ефективний збір і аналіз подій, однак без інтеграції з механізмами автоматизованого реагування їх можливості залишаються обмеженими. Використання SOAR-платформ дозволяє доповнити аналітичні можливості практичними діями, забезпечуючи скорочення часу реагування та зменшення

навантаження на фахівців інформаційної безпеки. На цій основі обґрунтовано вибір комбінації Wazuh як SIEM-рішення та Shuffle як платформи оркестрації реагування.

Практична реалізація технології в тестовому середовищі підтвердила можливість її впровадження без використання спеціалізованого дорогого обладнання, що є важливою перевагою для навчальних і невеликих корпоративних середовищ. Наведені приклади сценаріїв реагування демонструють здатність технології адаптуватися до різних типів інцидентів і забезпечувати баланс між автоматизацією та контролем з боку персоналу.

Оцінювання ефективності запропонованої технології показало суттєве скорочення часу виявлення та реагування на інциденти, зменшення кількості хибнопозитивних спрацювань і зниження навантаження на фахівців інформаційної безпеки. Порівняльний аналіз підтвердив, що інтеграція SIEM і SOAR у межах єдиної технології підвищує зрілість процесів управління інцидентами та створює умови для їх подальшого розвитку.

Разом із тим визначено низку обмежень, пов'язаних із необхідністю якісного початкового налаштування, потребою в регулярному оновленні правил і сценаріїв, а також залежністю від кваліфікації персоналу. Виявлені обмеження розглянуто як напрями подальшого розвитку технології, зокрема в частині підвищення адаптивності, розширення інтеграцій і використання інтелектуальних методів аналізу.

Загалом результати дослідження свідчать про те, що запропонована технологія моніторингу та управління інцидентами інформаційної безпеки є обґрунтованим, практично придатним і перспективним рішенням. Вона може бути використана як основа для побудови систем управління інцидентами в організаціях різного масштабу, а також як навчальна модель для підготовки фахівців у сфері кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Автоматизація реагування на інциденти (рішення SOAR). *Seeton*. URL: <https://www.seeton.pro/cybersecurity/soar/> (дата звернення: 21.11.2025).
2. АНАЛІЗ ТЕХНОЛОГІЇ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ | Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/699> (дата звернення: 22.12.2025).
3. Головна - Репозитарій Вінницького Національного Технічного Університету. URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/27130/7460.pdf?sequence=3&isAllowed=y> (дата звернення: 18.10.2025).
4. Головна - Факультет інформаційних і прикладних технологій. URL: https://phys.donnu.edu.ua/wp-content/uploads/sites/10/2020/02/125_kiberbezpeka_vk-9-dv-4_monitoryng-ta-upravlinnya-incydydentamy-kiberbezpeky.pdf (дата звернення: 09.12.2025).
5. НУБіП | Національний університет біоресурсів і природокористування України. URL: https://www.nubip.edu.ua/sites/default/files/u34/vk7.2_audit_incident_15042014.pdf (дата звернення: 17.11.2025).
6. Рішення / ІБ / SIEM. *Softlist - смарт рішення у сфері інформаційної безпеки та ІТ*. URL: <https://softlist.ua/services/siem> (дата звернення: 04.12.2025).
7. УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ | Herald of Khmelnytskyi National University. Technical sciences. *Herald of Khmelnytskyi National University. Technical*

sciences. URL: <https://heraldts.khmnua.edu.ua/index.php/heraldts/article/view/1987> (дата звернення: 19.12.2025).

8. Учасники проектів Вікімедіа. Система виявлення вторгнень – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень (дата звернення: 23.11.2025).

9. Що таке IPS/IDS і де застосовується - Блог - HostZealot. *HostZealot*. URL: <https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya> (дата звернення: 03.10.2025).

10. Що таке SIEM? | Захисний комплекс Microsoft. *Your request has been blocked. This could be due to several reasons*. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem> (дата звернення: 02.12.2025).

11. Що таке SOAR? Технології та рішення | Захисний комплекс Microsoft. *Microsoft – AI, Cloud, Produktivität, Computing, Gaming und Apps*. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-soar> (дата звернення: 24.10.2025).

12. vkarova7. Що таке управління інцидентами та які його переваги?. *ISSP Training*. URL: <https://www.issp.training/post/shcho-take-upravlinnya-intsydentamy-ta-yaki-yoho-perevahy> (дата звернення: 04.11.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)