

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технології автоматизації процесів виявлення та реагування на інциденти
безпеки в корпоративній мережі на базі FortiSOAR»**

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*

Ярослав ВАСИЛЕНКО

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61

ВАСИЛЕНКО Ярослав

(прізвище, ім'я)

Керівник

к.військ.н., доцент ГАХОВ Сергій

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

Рецензент

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

Київ 2025

2. Аналіз методів та засобів автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі на базі fortisoar

3. Технологія автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі на базі fortisoar

4. 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 автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі.	01.10.2025 р.	
2.	Аналіз наукової та технічної літератури з питань управління інцидентами кібербезпеки та концепції SOAR.	12.10.2025 р.	
3.	Аналіз методів і засобів автоматизації та оркестрації операцій безпеки на базі платформи FortiSOAR.	27.10.2025 р.	
4.	Розробка технології та практичних сценаріїв (плейбуків) для автоматизованого реагування на інциденти (наприклад, фішинг, шкідливе ПЗ).	03.11.2025 р.	
5.	Розроблення рекомендацій щодо впровадження та оцінки ефективності створених технологій в корпоративній мережі.	15.11.2025 р.	
6.	Оформлення результатів дослідження.	26.11.2025 р.	
7.	Підготовка доповіді до захисту.	15.12.2025 р.	

Здобувач вищої освіти

(підпис)

Ярослав ВАСИЛЕНКО

(ім'я, прізвище)

Керівник кваліфікаційної роботи

(підпис)

Сергій ГАХОВ

(ім'я, прізвище)

ВІДГУК РЕЦЕНЗЕНТА на кваліфікаційну роботу

здобувача ВАСИЛЕНКА Ярослава

на тему: «Технології автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі на базі FortiSOAR»

Актуальність: У сучасних умовах корпоративні мережі постійно стикаються з ескалацією кількості кіберзагроз, а рівень їхньої складності продовжує зростати. Аналітики безпеки перебувають під постійним тиском через надмірну кількість сповіщень, що призводить до виснаження та зниження точності ручних дій. На цьому фоні автоматизація процесів виявлення та реагування постає не лише бажаним, а й критично необхідним напрямом розвитку систем безпеки. Робота, присвячена дослідженню можливостей FortiSOAR в автоматизації SOC-процесів, є надзвичайно актуальною, оскільки відповідає світовим тенденціям переходу до інтелектуальних платформ оркестрації та автоматизації.

Позитивні сторони:

1. На основі проведеного аналізу в роботі встановлено зміст проблеми автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі та визначено мету і завдання автоматизації, а також її основні складові.
2. Досліджено методи та засоби автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі на базі FortiSOAR.
3. Розглянуто зміст технології автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі на базі FortiSOAR та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно та послідовно. Сформульовано чіткі й змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз умов застосування корпоративних додатків та забезпечення безпечного доступу гібридних працівників на прикладі конкретної організації.
2. Запропонований порядок застосування технології забезпечення безпечної роботи гібридних працівників бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“відмінно”**, а здобувач(ка) **ВАСИЛЕНКО Ярослав** – присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь,
вчене звання)

(підпис)

(ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 70 сторінки, 32 рисунків, 2 таблиці, 25 джерел.

Об'єкт дослідження – виявлення та реагування на інциденти безпеки в корпоративній мережі.

Предмет дослідження – технологія автоматизації виявлення та реагування на інциденти на базі платформи FortiSOAR з інтеграцією суміжних засобів моніторингу та захисту.

Мета роботи – сформувати практичний порядок впровадження та використання FortiSOAR для підвищення швидкості і якості реагування на інциденти, а також розробити рекомендації щодо його експлуатації в корпоративній мережі.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Технологія Security Orchestration, Automation and Response (SOAR) узгоджує роботу засобів безпеки та автоматизує типові кроки реагування. В одному середовищі поєднано збір і кореляцію подій, оркестрацію дій та керування інцидентами для захисту користувачів, застосунків і даних у корпоративній мережі та поза нею. FortiSOAR надає централізовану консоль, широку бібліотеку конекторів до SIEM, EDR, NGFW, хмарних сервісів і каталогів, конструктор плейбуків, кейс-менеджмент та панелі метрик для контролю MTTA і MTTR.

В роботі проаналізовано проблему автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі, визначено мету та завдання дослідження. Проведено аналіз підходів та існуючих рішень для автоматизації виявлення й реагування на інциденти. Досліджено методи та засоби автоматизації на базі платформи FortiSOAR. Визначено призначення, основні функції та склад платформи FortiSOAR у корпоративній системі кіберзахисту.

На основі досліджень, проведених у роботі, запропоновано порядок застосування FortiSOAR для автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі. Розроблено практичні рекомендації для фахівців з кібербезпеки щодо впровадження та використання FortiSOAR.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНЦИДЕНТИ, SOAR, SIEM, АВТОМАТИЗАЦІЯ, ОРКЕСТРАЦІЯ, ПЛЕЙБУКИ, FORTISOAR, КОРПОРАТИВНА МЕРЕЖА, ЗАХИСТ ДАНИХ

ABSTRACT

Text part of the qualification work: 70 pages, 32 figures, 2 tables, 25 sources.

Object of research – detecting and responding to security incidents in a corporate network.

Subject of research – the technology for automating incident detection and response based on the FortiSOAR platform with integration of related monitoring and protection tools.

The aim of research – to develop a procedure for applying technology to ensure the secure work of hybrid employees of the organization and recommendations for its implementation.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards and their comparison.

Security Orchestration, Automation and Response (SOAR) streamlines the operation of security controls and automates routine response steps. A single environment combines event collection and correlation, action orchestration, and incident management to protect users, applications, and data within and beyond the corporate network. FortiSOAR provides a centralized console, an extensive library of connectors to SIEM, EDR, NGFW, cloud services, and directories, a playbook builder, case management, and metric dashboards to track MTTA and MTTR.

The study examines problem of automating the processes of detecting and responding to security incidents in a corporate network is analyzed, and the aim and objectives of the study are defined. Approaches and existing solutions for automating incident detection and response are reviewed. Methods and tools for automation based on the FortiSOAR platform are investigated. The purpose, key functions, and components of the FortiSOAR platform within a corporate cybersecurity system are identified.

Based on the research conducted in this thesis, a procedure for applying FortiSOAR to automate the detection and response to security incidents in a corporate network is proposed. Practical recommendations for cybersecurity specialists on implementing and using FortiSOAR are developed.

Field of application – cybersecurity of information resources of the organization.

INCIDENTS, SOAR, SIEM, AUTOMATION, ORCHESTRATION,
PLAYBOOKS, FORTISOAR, CORPORATE NETWORK, DATA PROTECTION

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	8
ВСТУП	9
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КОРПОРАТИВНІЙ МЕРЕЖІ	12
1.1 Дослідження проблеми автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі	12
1.2 Аналіз підходів до автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі	19
1.3 Аналіз існуючих рішень для автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі	24
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ FORTISOAR	35
2.1 Призначення та функціональні можливості платформи FortiSOAR .	35
2.2 Основні компоненти та архітектура FortiSOAR. Інтеграція з корпоративною інфраструктурою і Fortinet Security Fabric	40
2.3 Порядок функціонування платформи FortiSOAR	47
3 ТЕХНОЛОГІЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ FORTISOAR.....	56
3.1 Технологія застосування плейбука перевірки підозрілих фішингових листів у FortiSOAR	56
3.2 Рекомендації щодо автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі	70
ВИСНОВКИ	77
ПЕРЕЛІК ПОСИЛАНЬ	79
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	82

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

CSPM – Cloud Security Posture Management

CVE – Common Vulnerabilities and Exposures

EDR – Endpoint Detection and Response

IoC – Indicator of Compromise

IoT – Internet of Things

IPS – Intrusion Prevention System

MTTD – Mean Time to Detect

MTTR – Mean Time to Respond

NGFW – Next-Generation Firewall

SIEM – Security Information and Event Management

SOAR – Security Orchestration, Automation and Response

ВСТУП

Актуальність дослідження. Цифрова трансформація, активне використання хмарних сервісів, розподілені робочі місця та зростання залежності бізнес-процесів від мережевої інфраструктури суттєво розширили поверхню атаки корпоративних мереж. Паралельно ускладнюються ланцюжки атак і зростає частка інцидентів, пов'язаних із соціальною інженерією, компрометацією облікових записів, шкідливим ПЗ та атаками на ланцюги постачання. За цих умов організаціям недостатньо лише виявляти підозрілі події – критично важливо забезпечити швидке, кероване та документоване реагування з мінімальним впливом на доступність сервісів і безперервність діяльності.

Практика реагування, що переважно спирається на ручні дії аналітиків SOC, має системні обмеження: тривалий час на збагачення подій контекстом, нерівномірна якість рішень залежно від досвіду виконавця, складність координації між засобами захисту та ІТ-службами, а також ризик пропуску критичних сигналів через надмірний “шум” сповіщень. Навіть за наявності SIEM, EDR/NGFW та інших компонентів захисту часто бракує єдиного механізму, який забезпечує узгоджене виконання процедур реагування, контроль етапів інцидент-менеджменту та накопичення доказової бази. Це призводить до зростання MTTA/MTTR і, як наслідок, до більших збитків і простоїв.

Перспективним напрямом вирішення зазначених проблем є впровадження технологій класу SOAR (Security Orchestration, Automation and Response), які дозволяють стандартизувати процес реагування через плейбуки, оркеструвати взаємодію між різними засобами безпеки та автоматизувати рутинні кроки (тріаж, enrichment, containment) із повним аудитом дій. Водночас для практичного застосування в корпоративному середовищі ключовими залишаються питання порядку інтеграції SOAR із суміжними системами, побудови плейбуків під типові сценарії (зокрема фішинг) та оцінювання ефективності автоматизації за процесними метриками.

З огляду на інтенсивність і тривалість кіберзагроз в Україні, а також обмеженість ресурсів і кадровий дефіцит, актуальність теми посилюється потребою масштабувати можливості SOC без пропорційного збільшення штату, підвищити відтворюваність процесів реагування та зменшити час простоїв критичних сервісів. Таким чином, робота спрямована на розв'язання практичної частини проблеми автоматизації реагування шляхом формування порядку застосування FortiSOAR у корпоративній мережі та розроблення прикладного сценарію реагування на фішингові інциденти.

Об'єкт дослідження – виявлення та реагування на інциденти безпеки в корпоративній мережі.

Предмет дослідження – технологія автоматизації виявлення та реагування на інциденти на базі платформи FortiSOAR з інтеграцією суміжних засобів моніторингу та захисту.

Мета роботи – сформувати практичний порядок впровадження та використання FortiSOAR для підвищення швидкості і якості реагування на інциденти, а також розробити рекомендації щодо його експлуатації в корпоративній мережі.

Наукові завдання:

дослідити сутність проблеми автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі;

проаналізувати підходи до автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі;

проаналізувати існуючі рішення для автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі;

проаналізувати методи та засоби автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі на базі FortiSOAR;

розкрити порядок застосування технології автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі на базі FortiSOAR та надати рекомендації щодо її використання.

Практичне значення одержаних результатів: запропоновано порядок

застосування FortiSOAR для автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі. Розроблено практичні рекомендації для фахівців з кібербезпеки щодо впровадження та використання FortiSOAR.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КОРПОРАТИВНІЙ МЕРЕЖІ

1.1 Дослідження проблеми автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі

Аналізуючи сучасний стан інформаційної безпеки, доцільно першочергово розглянути динаміку еволюції кіберзагроз. Світова статистика свідчить про стрімке зростання впливу кіберзлочинності на економіку. Згідно з прогнозами, загальна вартість шкоди від кібератак може зрости з приблизно 9,22 трлн доларів у 2024 р. до 13,82 трлн доларів у 2028 р. [1]. Такий масштаб потенційних фінансових втрат підкреслює неспроможність виключно ручних методів моніторингу та потребує переходу до високоавтоматизованих систем управління інцидентами. Спеціалісти ІВМ, аналізуючи інциденти 2024 р., зазначають, що промисловість четвертий рік поспіль залишається головною ціллю, на частку якої припадає найбільша кількість випадків вимагання та крадіжки даних [2]. Динаміка зростання світових збитків від діяльності кіберзлочинців відображена на рис. 1.1.

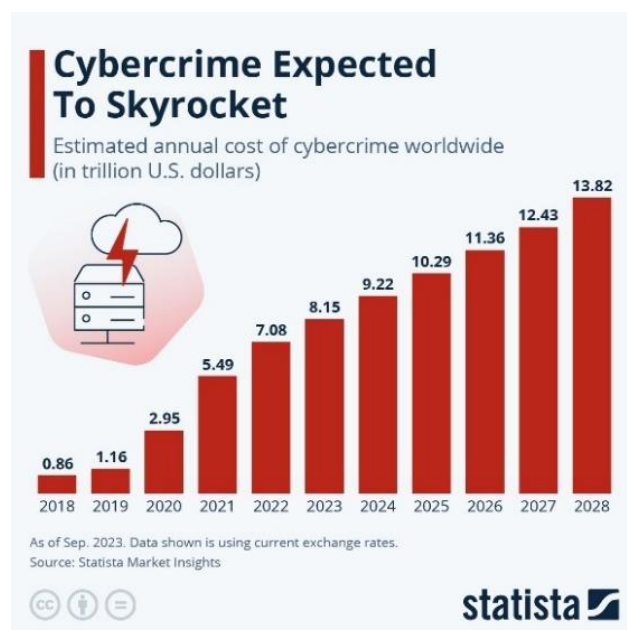


Рис. 1.1. Прогноз зростання світових збитків від кіберзлочинності до 2028 року

Зміни в організації роботи також впливають на рівень ризику. Популярність віддаленої роботи, використання хмарних сервісів та кількість підключених пристроїв розширили поверхню атаки, що робить традиційні «периметрові» підходи недостатніми. Українські експерти підкреслюють, що в епоху безпрецедентного зв'язку виклики та загрози цифровій безпеці продовжують зростати [3]. Поширення мобільних і IoT-пристроїв, розподілених серед користувачів, робить питання керування кінцевими точками ключовим завданням, адже ці пристрої часто мають слабкі механізми захисту [3].

У цих умовах пріоритетною стає задача своєчасного виявлення та коректного реагування на інциденти безпеки. Однак у практичній площині організація стикається з протиріччям: з одного боку, кількість подій безпеки та телеметрії зростає (SIEM/EDR/NDR, поштові шлюзи, проксі, IDS/IPS, хмарні журнали тощо), з іншого – можливості людського ресурсу в SOC залишаються обмеженими. Як наслідок, збільшення обсягу сигналів без належного збагачення та пріоритезації породжує перевантаження аналітиків і зниження ефективності тріажу.

Для систематизації контексту доцільно виділити групи загроз, які найбільш характерні для корпоративних мереж у період 2024–2025 рр. та створюють підвищене навантаження на процеси моніторингу й реагування (табл. 1.1).

Таблиця 1.1.

Класифікація та аналіз домінуючих кіберзагроз для корпоративних мереж

Категорія загрози	Характер впливу на корпоративну мережу	Ключовий показник (2024–2025 рр.)
Атаки з використанням ШІ	Автоматизація створення шкідливого ПЗ та масових фішингових кампаній.	Зростання ШІ-фішингу на 202%.
Програми-вимагачі (Ransomware)	Шифрування критичних даних з метою отримання викупу та загрозою оприлюднення конфіденційної інформації.	Складають 28% усіх випадків використання шкідливого ПЗ.
Компрометація облікових даних	Використання легітимних акаунтів для тривалого прихованого перебування в мережі.	30% усіх успішних вторгнень відбуваються через вкрадені облікові дані.
Вразливості IoT та периферії	Експлуатація слабких механізмів захисту підключених пристроїв для проникнення у внутрішній периметр.	Промисловість залишається ціллю №1 через інтеграцію застарілих ОТ-систем.
Атаки на ланцюги постачання	Проникнення через мережі партнерів та постачальників послуг для доступу до цільової організації.	54% великих організацій вважають ризики третіх сторін критичним викликом.

Надалі у роботі буде проведено детальний аналіз кожного виду виділених загроз.

В контексті сучасних методів злочинної діяльності слід приділити окрему увагу використанню алгоритмів штучного інтелекту (ШІ) та інструментам соціальної інженерії. З одного боку, штучний інтелект (ШІ) допомагає захисникам швидко аналізувати великі обсяги даних. З іншого - кіберзлочинці застосовують його для створення масових фішингових кампаній та підроблених повідомлень. Наприклад, дослідження показують, що 202 % зростання кількості фішингових листів у другій половині 2024 р. пов'язують із використанням ШІ [1]. За даними IBM, зловмисники активніше використовують генеративні моделі для створення фішингових електронних листів і шкідливого коду [2], що ускладнює виявлення атак традиційними засобами. У корпоративних мережах це призводить до збільшення кількості компрометованих облікових даних; 30 % усіх вторгнень у 2024 р. здійснювались з використанням легітимних акаунтів [2]. Використання зловмисниками ШІ-моделей для генерації шкідливого контенту вимагає від засобів захисту аналогічного рівня швидкодії, що може бути реалізовано лише через механізми автоматичного пріоритезування та реагування.

Додатково в межах окреслення проблеми доцільно підкреслити роль соціальної інженерії та фішинг, оскільки саме вона часто запускає ланцюжок подій, який потім перетворюється на “повноцінний” інцидент у корпоративній мережі. За даними аналітичних звітів, “людський фактор” залишається системним компонентом значної частки порушень безпеки, а в межах соціальної інженерії суттєву частину інцидентів становлять саме фішингові сценарії та пре-текстинг. Для корпоративного середовища це означає, що навіть при наявності сучасних технічних засобів захисту організація стабільно отримує потік звернень від користувачів щодо підозрілих листів, вкладень і посилань, а також потік автоматичних спрацювань поштових шлюзів і EDR-агентів. У результаті саме “поштова” тематика перетворюється на один із найчастіших об'єктів тріажу в SOC.

Одним із різновидів соціальної інженерії стали атаки типу BEC (business email compromise), коли шахраї видають себе за керівників або партнерів

організації. У 2024 р. таких атак зазнали 64 % компаній, середня сума збитку від одного інциденту – 150 тис. доларів [1]. Крім того, зростає використання вішингу та підроблених відеодзвінків (deepfake), що потребує підвищення обізнаності персоналу та впровадження двофакторної автентифікації.

Продовжуючи аналіз шкідливого програмного забезпечення, варто відзначити домінуючу роль програм-вимагачів (ransomware) у структурі сучасних інцидентів. Програми-вимагачі і надалі домінує серед шкідливих програм. За оцінками аналітиків IBM X-Force, рансомвар становив 28% випадків використання шкідливого ПЗ у 2024 р. [2]. Співвідношення основних типів шкідливого програмного забезпечення, що використовувалося під час атак у 2024 році, представлено на рис. 1.2.

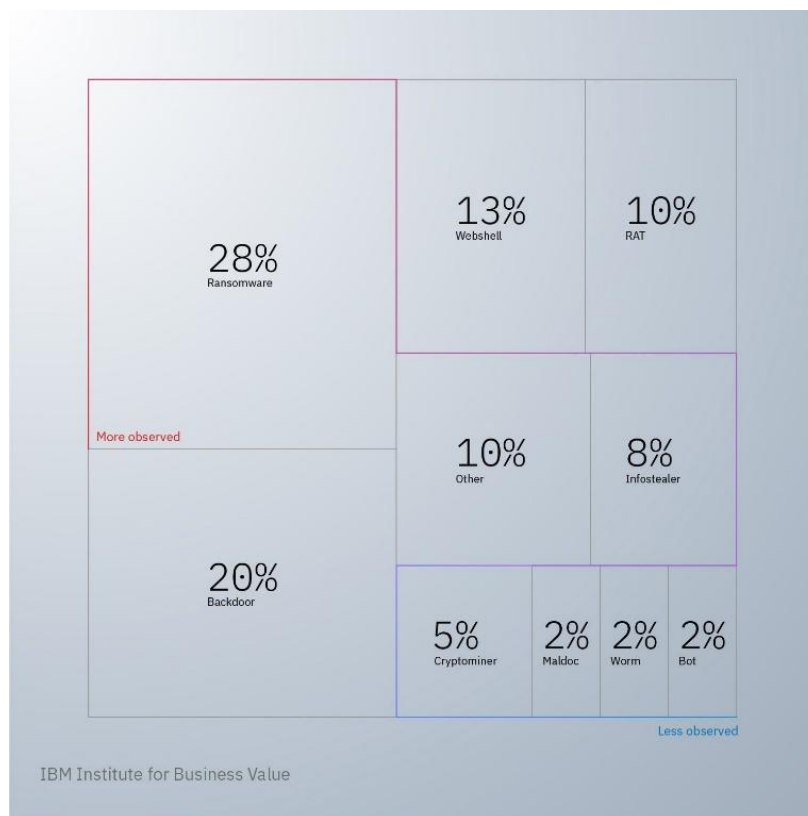


Рис. 1.2. Розподіл інцидентів за типами шкідливого програмного забезпечення

Хоча кількість інцидентів дещо зменшується завдяки відмові компаній платити викуп та міжнародним операціям проти злочинних груп, атаки стають складнішими: зловмисники поєднують шифрування даних з їх викраденням і погрожують оприлюднити конфіденційні відомості. Боротьбу ускладнює «як-

послуга» модель RaaS, яка надає готові інструменти для непрофесійних злочинців [1].

Іншою загрозою є інфостилери – шкідливі програми, що викрадають облікові дані та іншу конфіденційну інформацію. IBM повідомляє, що кількість інфостилерів, які поширюються через фішингові листи, зросла на 84 % за рік [2]. Викрадення паролів дає змогу зловмисникам здійснювати довготривалі атаки, залишаючись непомітними, що особливо небезпечно для підприємств із розгалуженою інфраструктурою.

Окремим критичним вектором атак, що зумовлений глибокою інтеграцією сучасних компаній у глобальні бізнес-екосистеми, є компрометація ланцюгів постачання та експлуатація вразливостей хмарних сервісів з ростом взаємозалежності компаній зростає частка атак на ланцюги постачання. Нападники проникають у мережі постачальників, щоб отримати доступ до систем більших клієнтів. Дослідження свідчать, що 54 % великих організацій розглядають керування ризиками третіх сторін як головний виклик [1]. Атаки на ланцюг постачання можуть призвести до зупинки виробництва, збитків і втрати репутації. В умовах України, де багато компаній інтегровані у глобальні ланцюги постачання, такі загрози стають критичними.

Хмарні сервіси, що забезпечують гнучкість і масштабованість, створюють новий клас ризиків. Основними проблемами є неправильне налаштування хмарних ресурсів, недостатній контроль доступу та нерозуміння моделі розподіленої відповідальності. Тому компанії впроваджують засоби CSPM (Cloud Security Posture Management) і регулярно проводять аудит налаштувань [3]. Надійне шифрування, багатофакторна автентифікація та сегментація мережі залишаються базовими заходами захисту.

Значну небезпеку для стійкості корпоративних мереж становлять таргетовані атаки типу АРТ, які часто базуються на використанні раніше невідомих уразливостей (0-day). Такі уразливості та атаки, що використовують їх, становлять серйозну загрозу. Їх активно експлуатують не лише кіберзлочинці, а й державні хакерські угруповання. Атаки типу АРТ характеризуються тривалим перебуванням

у мережі та шпигунською активністю. Для ефективного захисту необхідні системи виявлення аномалій, сегментування мережі та постійне оновлення програмного забезпечення. У глобальному рейтингу найбільш популярних вразливостей чотири з десяти мають публічно доступний експлойт або були активно використані впродовж двох тижнів від оприлюднення [2].

Динаміка зростання кількості виявлених вразливостей та створення на їх основі готових експлойтів, що значно скорочує час на підготовку атаки, наведена на рис. 1.3.

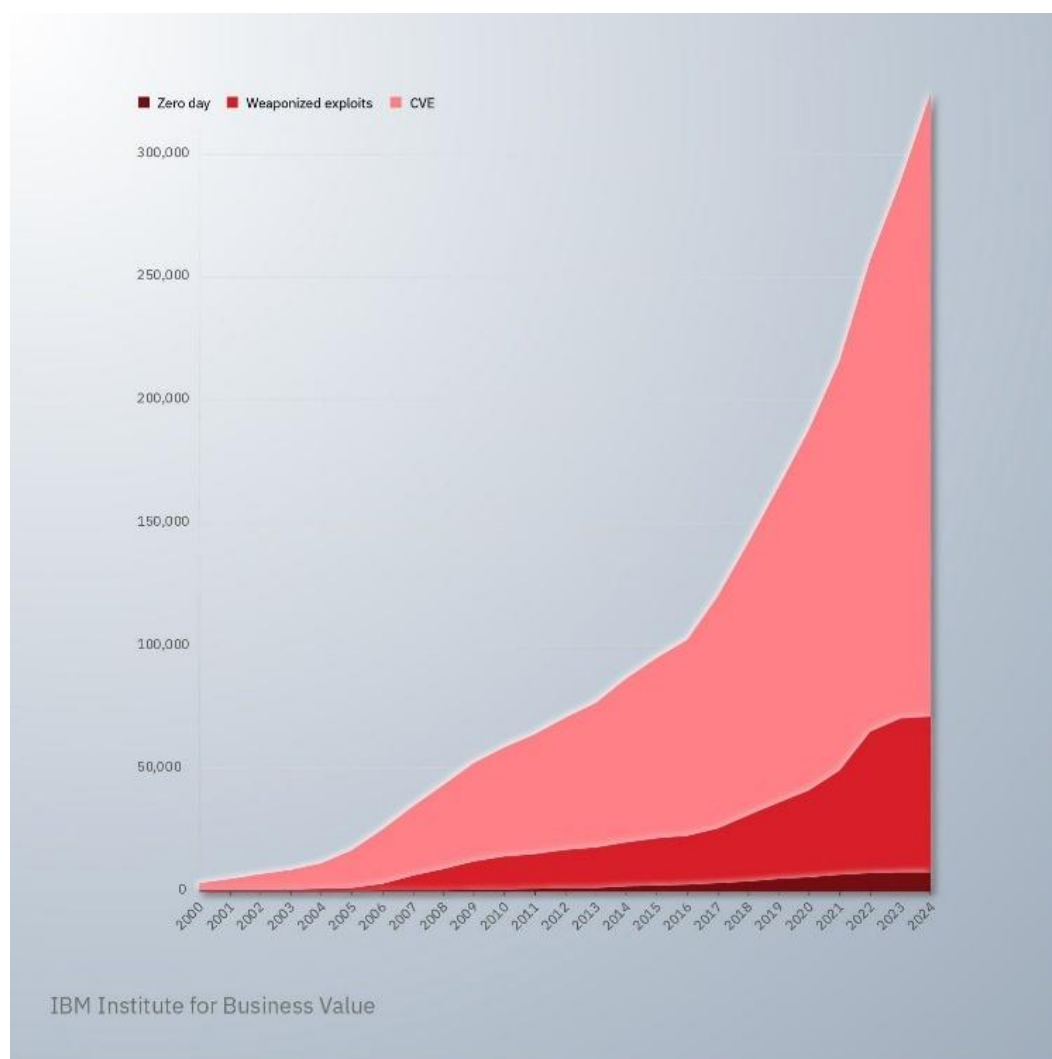


Рис. 1.3. Статистика виявлення вразливостей та динаміка розробки експлойтів (2000–2024 pp.)

Аналіз рис. 1.3 дозволяє зробити висновок про критичне скорочення часового вікна між оприлюдненням вразливості (CVE) та появою експлойту. Це створює

ситуацію, за якої стандартні цикли оновлень ПЗ не встигають за темпами зловмисників, що підтверджує необхідність впровадження систем реагування в реальному часі.

Додатковим фактором розширення поверхні атаки є масове впровадження пристроїв інтернету речей (IoT), які зазвичай позбавлені розвинених вбудованих механізмів автентифікації та захисту. IoT розширює корпоративний периметр, однак більшість пристроїв постачаються без належних механізмів безпеки. Зловмисники використовують слабкі паролі або відкриті порти для створення ботнетів та проникнення у внутрішню мережу. Експерти радять підтримувати інвентаризацію всіх під'єднаних пристроїв, сегментувати мережу та впроваджувати політики оновлення прошивок [3]. Усвідомлення цих ризиків особливо важливе для промислових підприємств і критичної інфраструктури.

У сукупності наведені фактори (зростання кількості атак, ускладнення інфраструктури, розширення периметра за рахунок хмарних сервісів, віддалених користувачів та IoT) призводять не лише до підвищення загального рівня ризику, але й до суттєвого ускладнення щоденної операційної роботи з подіями безпеки.

Ключова операційна проблема, що виникає на перетині зазначених факторів, проявляється як перевантаження SOC сповіщеннями та інцидентами і, як наслідок, alert fatigue (втома від алертів). У науково-практичних дослідженнях втома від алертів описують як явище, коли SOC змушений обробляти надмірну кількість повторюваних або хибнопозитивних алертів, через що аналітики витрачають значну частину часу на рутинну перевірку «шуму», ризикують пропустити критичні сигнали та швидше виснажуються. Фактично йдеться не лише про незручність, а про пряме погіршення якості виявлення: якщо пріоритезація слабка, а кореляція подій недостатня, то швидкість і точність тріажу падають саме тоді, коли організації потрібно реагувати швидше.

Підтвердженням актуальності цього виклику є результати профільних опитувань SOC-практиків: серед типових бар'єрів називають і надлишок алертів, які неможливо якісно опрацювати, і нестачу процесів/плейбуків, і брак автоматизації та оркестрації як фактор, що безпосередньо обмежує здатність SOC

масштабуватися. Таким чином, проблема автоматизації виявлення та реагування виходить за рамки «оптимізації»: вона стає необхідною умовою підтримання прийнятного рівня кіберстійкості в корпоративній мережі.

Отже, у межах даного підрозділу проблему автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі можна узагальнити так: зростання різномірних кіберзагроз і розширення поверхні атаки збільшують потік подій та інцидентів, а обмежені ресурси SOC та ручні процедури тріажу призводять до alert fatigue, що погіршує якість реагування, підвищує ризик пропуску критичних атак і збільшує час від виявлення до локалізації. Особливо показовим для корпоративної практики є потік фішингових звернень від користувачів, який потребує швидкої перевірки, збагачення контекстом та стандартизованих дій. Саме тому подальше дослідження має бути спрямоване на обґрунтування підходів до автоматизації та на вибір інструментів, здатних зменшити операційне навантаження на SOC без втрати якості контролю.

1.2 Аналіз підходів до автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі

Реагування на інциденти в корпоративних мережах супроводжується безперервним потоком телеметрії від десятків різномірних засобів захисту. Аналітики SOC стикаються з втомою від сповіщень (alert fatigue) - станом виснаження через надмірну кількість хибних або неінформативних сигналів [2]. Відсутність консолідації подій від мережевих пристроїв, хмарних сервісів та систем ідентифікації призводить до фрагментації та дублювання інцидентів. Автоматизація скорочує час реагування та стандартизує процеси, зберігаючи можливість аудиту дій. Проте стійкий ефект досягається лише за умови поєднання автоматизації з чіткою методологією на основі стандарту NIST SP 800-61r3 [4]. Такий підхід інтегрує обробку інцидентів у загальну стратегію управління ризиками, узгоджену з фреймворком NIST CSF 2.0 [5].

Класична логіка NIST, яку зручно використовувати для проектування автоматизації в SOC, охоплює (рис. 1.4) [4]:

1. підготовку (політики, ролі, інструменти, журналювання, готовність до збору доказів);
2. виявлення та аналіз (ідентифікація події, тріаж, підтвердження інциденту, визначення масштабу та впливу);
3. стримування, ліквідацію та відновлення (containment, eradication, recovery з урахуванням збереження доказової бази);
4. післяінцидентні активності (уроки, коригування контролів, вдосконалення детекцій та процедур).

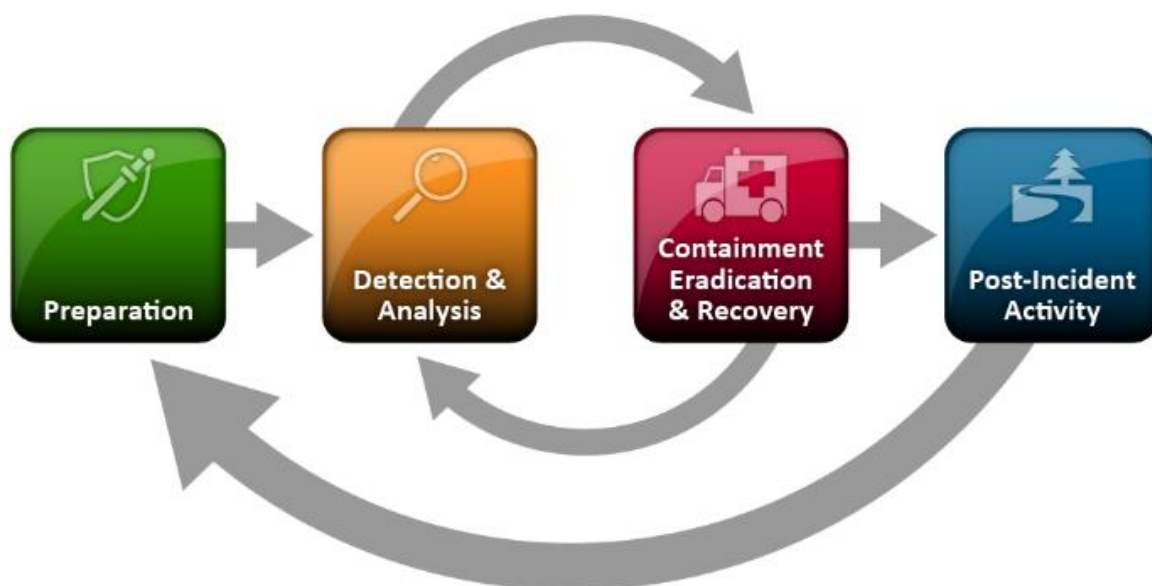


Рис. 1.4. Класична модель життєвого циклу реагування на інциденти

Паралельно NIST CSF 2.0 [5] задає «мову» очікуваних результатів без прив'язки до конкретних технологій: Govern, Identify, Protect, Detect, Respond, Recover (рис. 1.5). Це корисно саме для автоматизації, бо дозволяє формувати профіль цілей (outcomes) і вимірювати, які елементи процесу реально підсилені автоматизованими механізмами, а які залишилися ручними або неформалізованими.

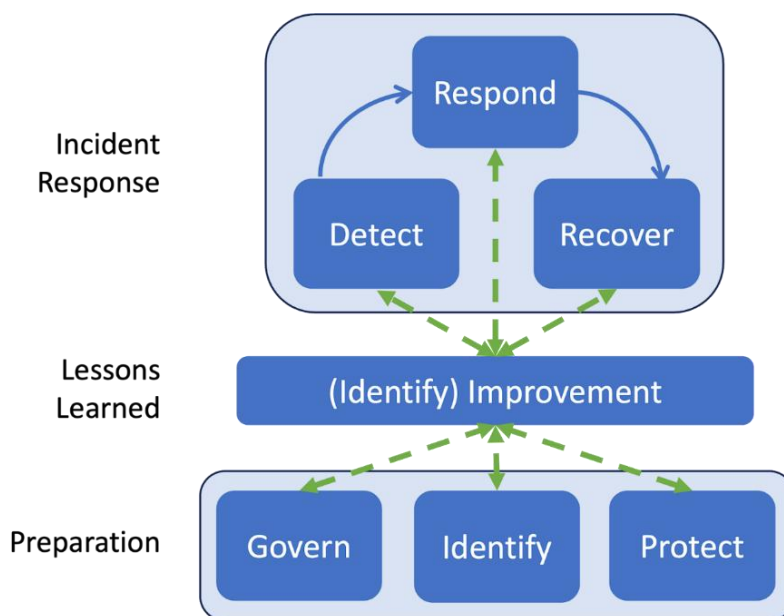


Рис. 1.5. Модель життєвого циклу реагування на інциденти (CSF 2.0)

У практичному сенсі підхід виглядає так: NIST задає послідовність робіт та контрольні точки якості, а автоматизація «підставляється» в ті місця, де (1) повторюваність висока, (2) ризик помилки людини суттєвий, (3) час критичний, (4) рішення можна прийняти за правилами або за наперед узгодженими умовами.

Ключова причина втоми від алертів полягає не лише у кількості сповіщень, а у структурі роботи: коли SOC вимушений обробляти події поштучно, без швидкого групування та контексту, навіть помірний обсяг даних перетворюється на нескінченний тріаж. Тому перший базовий підхід до автоматизації полягає у переході від «alert-driven» до «case-driven» моделі:

1. сирі події та алерти збираються і нормалізуються;
2. далі автоматично корелюються і агрегуються;
3. формується інцидент або кейс із мінімально достатнім контекстом;
4. аналітик отримує не сотні «одинакових» алертів, а обмежену кількість пріоритизованих кейсів із поясненням, чому вони важливі.

Цей підхід узгоджується з ідеєю NIST про систематизацію виявлення та аналізу інцидентів, коли підтвердження інциденту відбувається через збирання свідчень, визначення масштабу, впливу і подальшу маршрутизацію реагування.

Автоматизація в SOC має підсилювати роботу аналітика: рутинні кроки тріажу, збирання артефактів і запуск типових дій виконуються автоматично, тоді як високовпливові рішення (ізоляція, блокування доступу, зміни політик) доцільно залишати в режимі людської валідації через механізми погодження та ескалації [6].

Окремий практичний підхід для корпоративної мережі полягає у введенні risk-based triage, коли пріоритет визначається не «важкістю алерта» від одного інструмента, а комбінацією:

1. критичність активу (сервер з фінансовими даними проти тестового середовища);
2. рівень привілеїв користувача;
3. наявність ознак латерального руху або ексфільтрації;
4. повторюваність сигналу;
5. підтвердження кількома незалежними джерелами.

Це дозволяє скоротити кількість «high severity» кейсів до тих, що мають реальний бізнес-ваговий сенс, і тим самим адресно зменшити втому від алертів.

На етапі Respond головне завдання автоматизації полягає у скороченні часу між рішенням і дією, а також у стабільності виконання. Microsoft Cloud Security Benchmark прямо вказує, що ручні дії створюють затримки, які дають зловмиснику час для розвитку атаки, тоді як автоматизовані плейбуки можуть виконувати стримування та інші кроки значно швидше і послідовніше [6].

Для корпоративної мережі практичні підходи до автоматизації реагування зазвичай групуються так:

1. Автоматизація комунікацій і ескалації. Автоматичні сповіщення потрібних ролей, створення задач у тикет-системі, запуск процедури інформування керівництва або комплаєнсу за критеріями інциденту. Це зменшує «розрив координації», коли кілька команд працюють без спільної картини.

2. Автоматизація стримування (containment) з правилами безпеки. Типові дії включають ізоляцію хоста, блокування ІоС на мережевому периметрі, відключення сесій, тимчасове блокування облікового запису, переведення користувача на примусову зміну пароля, перевірка MFA, заборона доступу з

ризикових геолокацій. Підхід «pre-authorized containment» (наперед узгоджене стримування) дозволяє прибрати часову затримку на погодження у критичні хвилини, але потребує чітких умов запуску, журналювання і механізму відкату.

3. Напіваавтоматичне реагування (human-in-the-loop). Для ризикових дій корисний режим, коли система готує план дій, збирає артефакти і пропонує рішення, але остаточне підтвердження робить відповідальний спеціаліст. Це знижує ймовірність «самострілу» автоматизації та підтримує контрольованість.

4. Створення циклу постійного покращення. Четвертий підхід до автоматизації полягає у формуванні процесів, що дозволяють SOC розвиватися:

- автоматичне формування звітів за інцидентами, таймлайнів, переліку артефактів;
- контроль повноти виконання процедур (чи зібрані логи, чи зафіксовано рішення, чи проведено аналіз кореневих причин);
- оновлення правил кореляції та зменшення фальшивих спрацювань за результатами розбору;
- поповнення бази знань SOC, щоб повторні інциденти оброблялися швидше.

Microsoft окремо підкреслює значення систематичних lessons learned процесів і збереження доказів як частини зрілої реакції [6].

У таблиці 1.2 систематизовано співвідношення типових симптомів операційного перевантаження SOC та відповідних функціональних механізмів автоматизації процесів реагування.

Таблиця 1.2

Роль автоматизації у зменшенні втоми від алертів у корпоративній мережі

Джерело проблеми	Як проявляється в SOC	Автоматизований підхід (без прив'язки до конкретного вендора)
Надмірний потік алертів	Аналітики витрачають час на однотипні події, знижується увага, зростає ризик пропусків	Дедуплікація, агрегація, кореляція, перехід від алертів до інцидентів/кейсів
Висока частка false positive	Постійні «порожні» розслідування, демотивація, втрачений час	Автоматичне збагачення, базові перевірки, правила відсіву, тюнінг детекцій за результатами інцидентів
Фрагментація інструментів	Різні команди бачать різні «шматки» картини, дублювання, неузгоджені дії	Оркестрація інтеграцій, централізований кейс-менеджмент, єдині маршрути ескалації

Продовження таблиці 1.2

Джерело проблеми	Як проявляється в SOC	Автоматизований підхід (без прив'язки до конкретного вендора)
Ручний збір контексту	Тріаж «з'їдає» більшість часу, а не аналіз	Автоматизовані запити до CMDB/AD/EDR/пошти/мережі, збагачення TI-контекстом, автозбір артефактів
Повільна ескалація і комунікації	Затримки на узгодження, «загублені» інциденти	Автоматичні сповіщення, створення тикетів, правила ескалації за критичністю і бізнес-впливом
Непослідовні дії реагування	Результат залежить від досвіду аналітика, можливі пропуски кроків	Плейбуки/ранбуки, чек-листи, контроль виконання, approval workflows для ризикових дій
Відсутність системного покращення	Однакові інциденти повторюються, правила не покращуються	Автозвіти, lessons learned, контроль метрик (MTTA/MTTR), замикання «фідбек-петлі» в детекції та плейбуки

Отже, у корпоративній мережі автоматизація процесів виявлення та реагування є цілеспрямованою відповіддю на наслідки зростання кількості атак і «шуму» телеметрії. Методологічно автоматизацію доцільно проєктувати через NIST-орієнтований процес [4, 5], а практично реалізовувати як набір механізмів, що зменшують ручний тріаж (агрегація, збагачення, пріоритизація), пришвидшують і стандартизують реагування (оркестрація та плейбуки), підтримують контроль і безпечність автоматичних дій (approval, аудит, rollback), формують цикл постійного покращення, який поступово знижує частку false positive і стабілізує навантаження SOC.

1.3 Аналіз існуючих рішень для автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі

Сучасна корпоративна мережа функціонує в умовах постійного тиску з боку загроз, що швидко еволюціонують, а також в умовах дефіциту часу і людського ресурсу в центрі моніторингу та реагування (SOC). У практичній експлуатації визначальним є не лише факт виявлення інциденту, а здатність організації відтворено, керовано та контролювано проходити повний цикл реагування: від тріажу й збагачення події контекстом до стримування, усунення наслідків, відновлення сервісів і фіксації доказів для подальшого аудиту. Саме на цьому етапі

часто формується вузьке місце, зумовлене людським фактором: аналітик змушений повторювати однотипні дії в різних консолях, перемикатися між інструментами, збирати артефакти вручну та паралельно підтримувати комунікацію з ІТ-експлуатацією, власниками сервісів і керівництвом. У таких умовах автоматизація не може розглядатися як факультативна опція, оскільки вона є механізмом зниження когнітивного навантаження й стабілізації якості реагування, щоб управлінські та технічні рішення не залежали від втоми, зміни та конкретного виконавця.

Клас SOAR (Security Orchestration, Automation and Response) сформувався як відповідь на зазначену проблему. У профільних аналітичних матеріалах QKS Group SOAR описується як клас платформ, що поєднують інтеграцію інструментів безпеки, автоматизацію повторюваних задач і керовану координацію дій реагування в межах інцидентного процесу.

Важливо, що для корпоративної мережі SOAR є не лише виконавчим механізмом плейбуків (формалізованих сценаріїв реагування), а й операційною основою для SOC: платформа об'єднує оркестрацію дій між системами, керування кейсами та SLA, журналювання, контроль доступу, аудит, а також підтримку доказової бази. Відповідно, під час вибору доцільно оцінювати не окрему функцію, а комплекс можливостей і обмежень з урахуванням архітектури підприємства, наявного стеку захисту та зрілості процесів реагування.

Огляди ринку SOAR демонструють стійку тенденцію зростання сегмента та розширення сценаріїв застосування, включно з автоматизацією тріажу, збагачення, узгодження рішень і формуванням звітності. Аналітичні матеріали також підкреслюють вплив дефіциту кадрів у кібербезпеці, через який організації вимушені скорочувати ручну працю та формалізувати процеси реагування за допомогою автоматизації [7, 8].

Паралельно змінюється технологічна модель: функції оркестрації та автоматизації дедалі частіше інтегруються в ширші екосистеми SIEM та XDR, а також доповнюються low-code підходами і генеративними інструментами для пришвидшення створення сценаріїв [9].

У профільних оглядах SOAR-платформ підкреслюється, що базові групи вимог до корпоративної експлуатації зазвичай охоплюють: централізоване керування інцидентами (кейс-менеджмент) і SLA, механізми побудови плейбуків із умовними переходами, циклічними конструкціями та обробкою помилок, широку мережу інтеграцій (конектори, API, підтримка SIEM/EDR/пошти/IAM), засоби захисту (рольова модель, аудит, керування секретами), а також експлуатаційну стійкість (оновлення, резервування, підтримка відмовостійких сценаріїв) і прийнятну сукупну вартість володіння [10]. Саме ці критерії доцільно застосовувати для порівняння Cortex XSOAR, FortiSOAR та Splunk SOAR у контексті задач магістерської роботи.

На практиці «найкраща SOAR-платформа» визначається не загальною впізнаваністю, а тим, наскільки вона знімає операційні проблеми конкретного SOC і забезпечує керованість процесу реагування. Тому коректний підхід до порівняння полягає у переході від формального переліку функцій до перевірки того, як ці функції працюють у типовому циклі реагування на інцидент і як вони підтримують процеси кейс-менеджменту, оркестрації та автоматизації в експлуатаційних умовах. Для отримання більш об'єктивної оцінки доцільно поєднувати аналітичні матеріали постачальників і дослідницьких компаній із незалежними користувацькими джерелами, зокрема оглядами Gartner Peer Insights (Peer Reviews), а також методологіями квадрантів і матриць, які базуються на структурованому опитуванні та оцінюванні користувачами, зокрема Data Quadrant (рис. 1.6) від SoftwareReviews і SPARK Matrix/квадрантними (рис. 1.7) поданнями від QKS Group [11].



Рис. 1.6. Data Quadrant / SoftwareReviews 2025

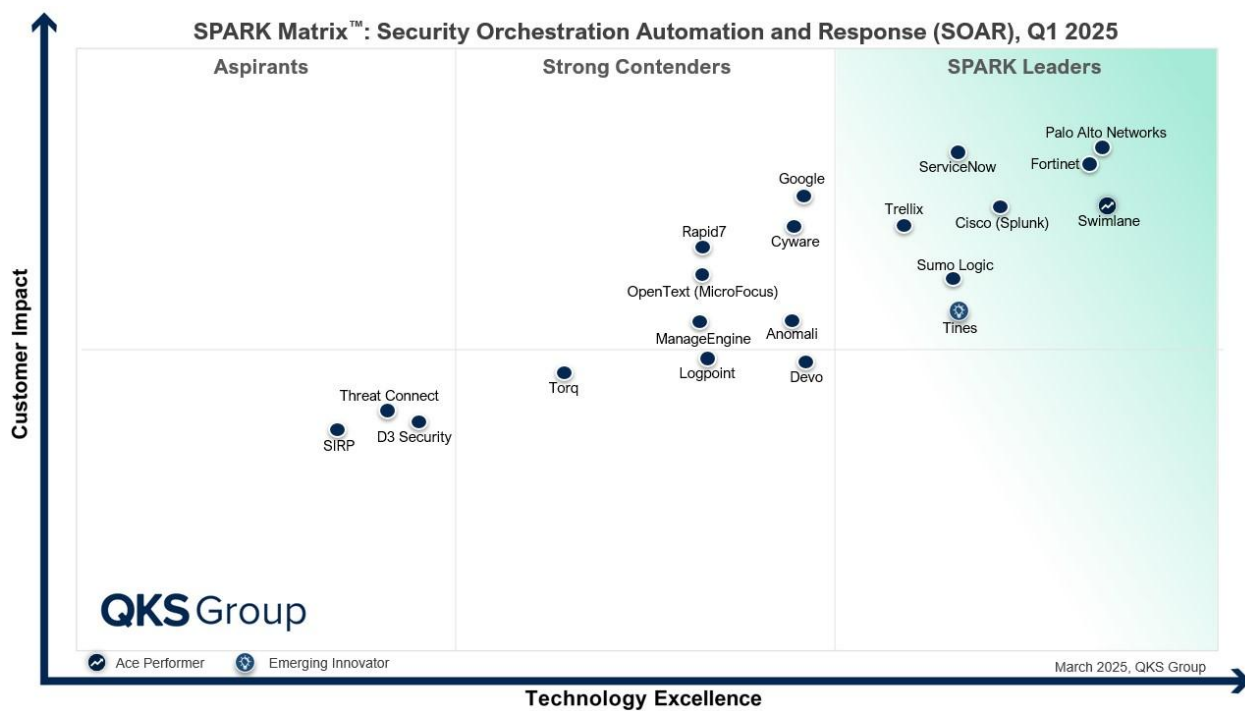


Рис. 1.7. SPARK Matrix від QKS Group 2025Q1

У межах даного підрозділу порівняння побудовано навколо таких ключових запитань.

Наскільки платформа підтримує керування інцидентами як процесом, а не лише запуск окремих автоматизованих дій: чи є зрілий кейс-менеджмент, етапи опрацювання, SLA, рольова модель, контроль виконання, відтворюваність рішень, фіксація доказів.

Наскільки потужні та безпечні плейбуки: чи підтримуються умовні гілки, цикли, обробка помилок, повторні спроби, керування винятками, а також безпечне зберігання секретів.

Наскільки практичною є оркестрація: скільки інтеграцій доступно, як швидко підключаються SIEM/EDR/пошта/IAM, чи можна збагачувати алерти контекстом і виконувати керуючі дії (ізоляція хоста, блокування облікового запису, оновлення правил NGFW, карантин електронного листа).

Експлуатаційна придатність: моделі розгортання, відмовостійкість, оновлення, журналювання, адміністрування, масштабування під навантаження та життєвий цикл платформи.

Економіка і результат: не лише вартість ліцензії, а й витрати на впровадження, підтримку інтеграцій, розробку плейбуків, навчання команди та подальше масштабування.

Цей набір критеріїв важливий ще й тому, що автоматизація в SOC не може бути “чорною скринькою”. Якщо платформа є непрозорою або недостатньо керованою, з часом вона може породжувати додаткові ризики: помилкові автоматичні дії, втрату контексту, проблеми аудиту. Тому рішення має забезпечувати баланс між швидкістю та контрольованістю.

Cortex XSOAR (Palo Alto Networks) позиціонується як платформа, що поєднує оркестрацію, автоматизацію та керування інцидентами, а також сильний блок Threat Intelligence Management [12]. В аналітичних оглядах QKS Group [13] підкреслюється, що користувачі відзначають ефективність автоматизації операцій і суттєве зменшення потреби в ручній праці.

Для корпоративного SOC це безпосередньо конвертується у швидший тріаж, зниження “рутинних” задач та більш швидко збагачення алертів.

Окремо варто виділити роботу з Threat Intelligence. За оцінками QKS Group [13], сильна сторона Cortex XSOAR полягає в автоматизованому підключенні TI-стрічок, збагаченні та кореляції, що допомагає швидше перетворювати “сирий” індикатор на зрозумілий контекст загрози.

У типовому сценарії реагування це означає, що SOC може швидше визначити, чи є IOC релевантним для конкретної мережі, які активи зачеплені, які супутні артефакти потрібно зібрати, і які дії будуть пропорційними ризику.

Разом з тим, для нашої задачі важливо врахувати аспект керування кейсами і гнучкості процесу. В QKS Group зазначається, що хоча XSOAR має вбудований кейс-менеджмент, частина користувачів оцінює його як менш гнучкий у порівнянні з альтернативами.

У корпоративній мережі, де узгодження дій між SOC, IT-експлуатацією, власниками сервісів і керівництвом часто визначає фактичний час реагування, “жорсткість” кейс-менеджменту може зменшувати практичну ефективність платформи, навіть за наявності сильного движка автоматизації.

Отже, Cortex XSOAR є потужним варіантом у середовищах, де критично важлива розвинена робота з Threat Intelligence та інтеграція з екосистемою Palo Alto Networks [12]. Проте для нашого випадку, де ключовим є баланс між автоматизацією, зрілим кейс-менеджментом і простотою промислового розгортання, доцільно порівнювати XSOAR з альтернативами через призму експлуатаційної практики, а не лише функцій TI.

Splunk SOAR (історично відомий як Phantom) є одним із найпоширеніших рішень у сегменті автоматизації SOC, особливо в організаціях, де Splunk використовується як центральний SIEM [14]. Платформа акцентує увагу на оркестрації між системами, побудові playbook-логіки та керуванні інцидентами, забезпечуючи інтеграційний міст між детекцією (SIEM/EDR) і діями реагування [15]. За даними порівняльних матеріалів (вибірка верифікованих оглядів), користувачі Splunk SOAR відзначають гнучкість налаштувань та широку

інтеграцію з інструментами безпеки, а також зменшення ручного навантаження аналітиків через автоматизацію.

Також у відгуках фігурує сильний кейс-менеджмент та простота створення плейбуків, що є важливим фактором для організацій з великою кількістю повторюваних сценаріїв реагування. Водночас, у корпоративному контексті важливо врахувати не лише “що платформа може”, а “скільки зусиль коштує, щоб вона робила це стабільно”. У порівняльних матеріалах серед зон розвитку Splunk SOAR згадуються потреба у кращих візуальних навчальних матеріалах та посиленні автоматизації щодо створення плейбуків [13].

Ці, на перший погляд, “нефункціональні” аспекти безпосередньо впливають на швидкість адаптації команди, зниження помилок на етапі розробки сценаріїв та підтримку платформи в довгому циклі експлуатації.

Таким чином, Splunk SOAR виглядає особливо логічним у середовищах із домінуючим стеком Splunk, де інтеграція “SIEM плюс SOAR” дає найкоротший шлях до операційного ефекту. Однак для нашої роботи важливо оцінити, чи відповідає Splunk SOAR вимозі low-code/зручної інженерії плейбуків і чи не створює зайвий експлуатаційний тягар, якщо корпоративний стек не є Splunk-центрованим [9].

FortiSOAR (Fortinet) позиціонується як платформа, що об’єднує оркестрацію, автоматизацію та керування інцидентами, з вираженою орієнтацією на практичні потреби SOC і на інтеграцію в екосистему Fortinet Security Fabric [16]. У порівнянні QKS Group підкреслюється, що *FortiSOAR* автоматизує тріаж алертів, збагачення інцидентів та дії з remediation на основі prebuilt playbooks, а також має зрілий візуальний конструктор плейбуків і розвинені інструменти кейс-менеджменту “з коробки” [13].

Для корпоративної мережі це є критично важливим: сильний playbook-движок без зрілого кейс-менеджменту часто перетворюється на набір “скриптів”, тоді як SOC потребує керованого процесу із відповідальностями, SLA, маршрутизацією і аудитом.

Ще один практичний аспект FortiSOAR полягає у збагаченні контекстом загроз. За даними QKS Group, FortiSOAR інтегрує FortiGuard та інші стрічки загроз для надання контексту та enrichment IOC у реальному часі безпосередньо в процесі розслідування [13].

У корпоративній експлуатації це зменшує затримки, коли аналітик вимушений “вручну” перевіряти індикатори в різних джерелах. Коли контекст підтягується автоматично і стандартизовано, підвищується якість рішень і спрощується перевірка правильності дій, особливо в умовах зміни змін і ротації персоналу.

Окремо потрібно підкреслити фактор інтеграційної екосистеми. FortiSOAR у межах Security Fabric має природну сумісність із продуктами Fortinet (мережевий захист, endpoint, пошта, sandboxing, threat intelligence), а також підтримує інтеграції з зовнішніми системами. У матеріалах QKS Group наголошується на “безшовній взаємодії” саме в межах Security Fabric [13], що практично означає менший час на підключення конекторів, менше “клеювого” коду і більш прогнозовану підтримку інтеграцій на оновленнях.

З точки зору корпоративної мережі це часто вирішальний аргумент: інтеграції є “кровоносною системою” SOAR, і будь-які збої в інтеграціях одразу знижують цінність автоматизації. Важливим для вибору є також питання розгортання і експлуатаційної придатності. У нашому випадку доцільно мати платформу, яка підтримує промислове розгортання, оновлення, керування компонентами та сценарії НА/резервування, щоб простаї SOAR не паралізували процес реагування.

Документація Fortinet (User Guide та Deployment Guide) дозволяє розглядати FortiSOAR саме як промисловий продукт із формалізованим життєвим циклом розгортання [17].

Отже, FortiSOAR формує сильну позицію тоді, коли організація прагне максимально “приземлити” автоматизацію під SOC-процеси, отримати зрілий playbook-конструктор і кейс-менеджмент, а також скористатися перевагами інтегрованої екосистеми Fortinet.

Для обґрунтованого вибору важливо поєднати технічне порівняння з емпіричними даними від користувачів, оскільки саме вони відображають реальні витрати на впровадження та підтримку, стабільність інтеграцій і практичну придатність до операційної роботи SOC. У матеріалах порівняння продуктів на основі верифікованих оглядів Gartner Peer Insights [18] (категорія рішень оркестрації, автоматизації та реагування) наведено узагальнені показники: FortiSOAR має оцінку 4.9/5 при 115 відгуках і 97% готовності рекомендувати, Cortex XSOAR 4.5/5 при 67 відгуках і 85% готовності рекомендувати, Splunk SOAR 4.3/5 при 86 відгуках і 78% готовності рекомендувати. Важливо, що в цих самих матеріалах наведено агрегований показник Overall Capability Score, який дозволяє порівнювати не лише «враження», а й узагальнену оцінку можливостей платформи: FortiSOAR демонструє найвищий рівень (4.8), далі йде Splunk SOAR (4.5), тоді як Cortex XSOAR має нижче значення (4.3) [18]. За деталізованими підкритеріями FortiSOAR також зберігає перевагу саме в тих компонентах, які найчастіше формують сумарну «вартість впровадження» у SOC: інтеграції (4.7), налаштовуваність (4.7) та масштабованість (4.7). Для порівняння, у Splunk SOAR показники інтеграцій (4.4) та налаштовуваності (4.3) нижчі, хоча масштабованість залишається порівнянною (4.5), тоді як Cortex XSOAR вирізняється високою оцінкою інтеграцій (4.6), але поступається за налаштовуваністю (4.1) [18]. Таким чином, у зрізі Gartner Peer Insights FortiSOAR виглядає найбільш збалансованим рішенням з погляду «корисності в експлуатації» та стабільності ключових функцій, що напряду пов'язано зі зменшенням трудомісткості підтримки плейбуків і конекторів у довгому циклі використання.

Додатковий незалежний зріз забезпечує підхід Data Quadrant / SoftwareReviews, який спирається на опитування користувачів і деталізує оцінки за групами можливостей та параметрами постачальника. У цій системі Splunk SOAR [14] має вищі агреговані значення (Composite Score 83/100; Customer Experience 87/100), а також дуже високі наміри продовження використання (plan to renew 95%) і готовність рекомендувати (88%). Це корелює з сильними сторонами Splunk SOAR у площині «інженерії автоматизації» та операційної організації: високі оцінки

отримують розроблення сценаріїв використання, оркестрація й автоматизація, побудова плейбуків, інформаційні панелі та взаємодія команди під час інцидентів.

Водночас у FortiSOAR у цьому ж зрізі агреговані показники нижчі (Composite Score 72/100; Customer Experience 76/100; готовність рекомендувати 84%) [19], а серед зон, що потребують посилення, фіксуються аспекти, пов'язані з упровадженням та сервісною складовою постачальника, що потенційно збільшує організаційні витрати на старті. Разом із тим, навіть у межах SoftwareReviews FortiSOAR демонструє конкурентні оцінки в процесно критичних елементах, зокрема у керуванні кейсами та зворотному зв'язку (case management; feedback loop), а також у виконанні сценаріїв реагування через плейбуки (playbooks / runbooks), тобто в частині «керованого процесу» SOC [19]. Практично це означає, що Splunk SOAR може виглядати сильнішим у зрізі «зручності та загальної задоволеності платформою», однак FortiSOAR зберігає фокус на процесних і контрольних механізмах, які важливі для відтворюваності рішень та аудиту.

Ще один допоміжний інструмент зіставлення, придатний для ілюстрацій у роботі (квадрант/матриця), надає SPARK Plus (QKS Group). У ньому наведено загальні користувацькі оцінки за невеликою вибіркою: Cortex XSOAR має 8.9, FortiSOAR 8.1, Splunk SOAR 8.0 (кожне значення сформовано на основі 1–2 оцінок), тому ці дані методологічно коректно трактувати як орієнтовні. [25] Водночас аналітичні коментарі QKS Group [13] дозволяють порівняти акценти платформ у розрізі функціональних блоків: FortiSOAR описується як рішення, що автоматизує тріаж, збагачення інцидентів контекстом та усунення наслідків через попередньо підготовлені плейбуки, а також орієнтоване на узгоджену оркестрацію в інтегрованому середовищі. Для Splunk SOAR у практичному вимірі типовою перевагою виступає сильна інтеграція у Splunk-центрований SOC та зрілий інструментарій плейбуків і оркестрації, тоді як Cortex XSOAR часто обирають у сценаріях, де вагому роль відіграють інтеграції та компоненти, пов'язані з контекстом загроз і розширеною аналітикою [13]. Таким чином, SPARK Plus доцільно використати як ілюстративний «квадрантний» зріз позиціонування, а

визначальні висновки робити на основі більш репрезентативних джерел на кшталт Gartner Peer Insights та детальних метрик SoftwareReviews.

Таким чином, узгодження трьох незалежних зрізів дозволяє сформуванати практично орієнтований висновок. По-перше, за результатами верифікованих оглядів Gartner Peer Insights FortiSOAR має найвищу загальну оцінку, найбільшу готовність рекомендувати та найвищий Overall Capability Score, а також сильні значення за інтеграціями, налаштуваністю і масштабованістю, тобто за тими параметрами, які безпосередньо визначають витрати на підтримку автоматизації у корпоративній мережі. По-друге, SoftwareReviews показує, що Splunk SOAR може мати перевагу за інтегральними показниками задоволеності та досвіду користувача, однак у задачі даної роботи пріоритетом є не «зручність як самоціль», а керованість процесу реагування, відтворюваність сценаріїв та практична інтеграційна придатність, де FortiSOAR утримує сильні позиції і водночас отримує найбільш переконливу підтримку за даними Gartner Peer Insights [18]. Отже, з урахуванням сукупності критеріїв корпоративної експлуатації та підтвердження незалежними метриками, FortiSOAR є найбільш доцільним вибором для реалізації технологій автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі в межах теми даної роботи.

Отже, в даному розділі досліджено проблему автоматизації процесів виявлення та реагування на інциденти безпеки в корпоративній мережі в умовах зростання кіберзагроз, розширення поверхні атаки та перевантаження SOC подіями. Обґрунтовано необхідність переходу від переважно ручного реагування до процесно керованої моделі з формалізованими етапами тріажу, збагачення контекстом, стримування, усунення наслідків і відновлення, а також із забезпеченням контролю, аудиту й стандартизованих сценаріїв реагування. Виконано порівняльний аналіз SOAR-платформ Cortex XSOAR, Splunk SOAR і FortiSOAR за критеріями експлуатаційної придатності, інтеграційних можливостей та керованості процесу реагування, за результатами якого обґрунтовано вибір FortiSOAR як найбільш доцільної платформи для корпоративного середовища.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ FORTISOAR

2.1 Призначення та функціональні можливості платформи FortiSOAR

SOAR-платформи у корпоративній мережі застосовуються для оркестрації дій між різними засобами безпеки та ІТ, автоматизації повторюваних процедур реагування, а також централізації процесів обробки інцидентів у межах SOC [20]. У цій логіці FortiSOAR розглядається як модульне середовище, яке поєднує управління інцидентами з механізмами інтеграції та автоматизованих дій, забезпечуючи виконання узгоджених сценаріїв реагування через єдиний операційний контур у складі SOC (рис. 2.1) [21].

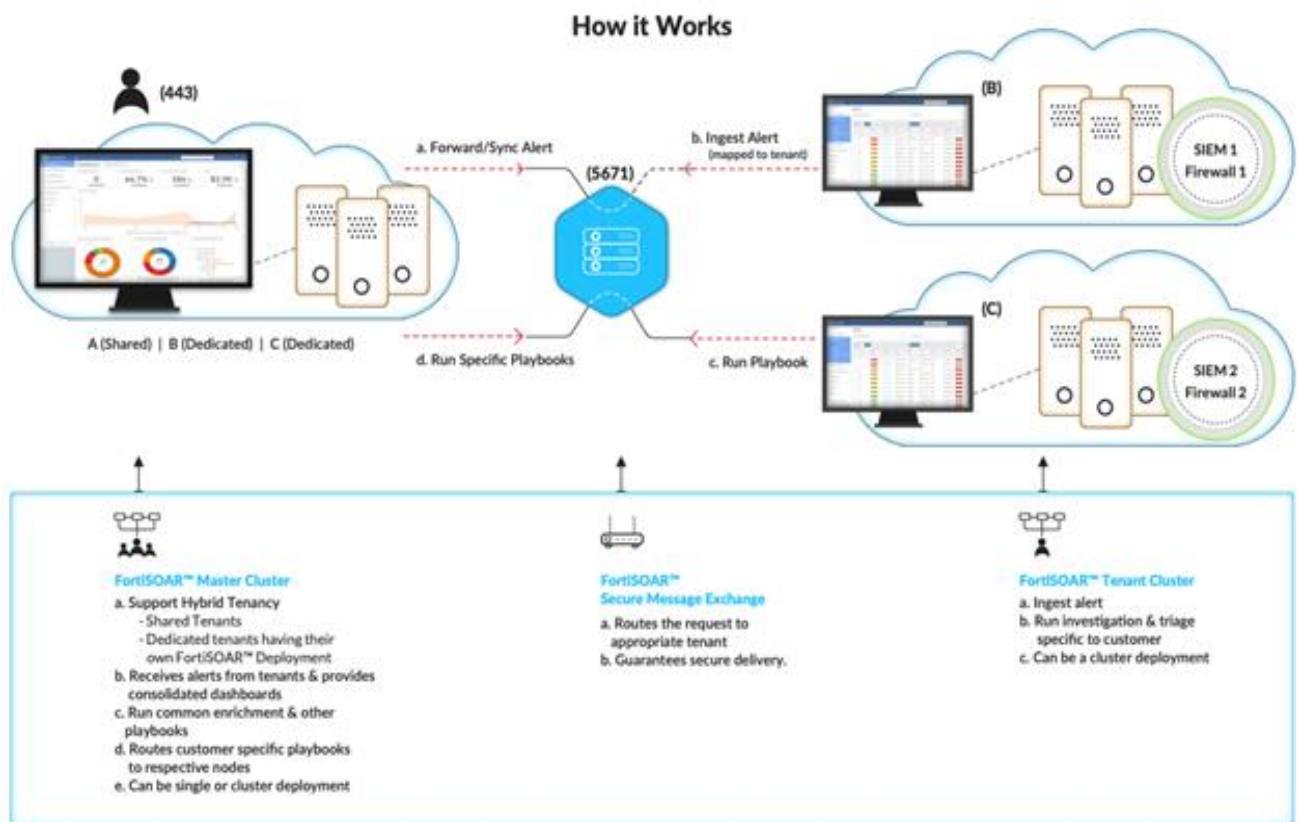


Рис. 2.1. Узагальнена схема взаємодії FortiSOAR із джерелами подій SOC

На практичному рівні призначення платформи проявляється у скороченні частки ручних операцій (тріаж, збагачення, передача задач), уніфікації процедур за рахунок стандартизованих сценаріїв та підвищенні керованості реагування через формалізацію робочих процесів SOC [21]. Додатково платформа підтримує різні моделі розміщення (локальні та хмарні середовища, у т.ч. контейнеризовані підходи), що важливо для узгодження вимог безпеки й експлуатаційних обмежень корпоративної інфраструктури [21].

Базовою складовою FortiSOAR у контексті SOC є кейс-менеджмент: платформа структурує обробку подій через типові сутності (Alerts > Incidents > Tasks > Indicators > Attachments), що дозволяє переводити «сирі» повідомлення засобів моніторингу у керований процес розслідування та реагування [22]. Зокрема, модуль Alerts забезпечує агрегацію повідомлень, вилучення метаданих та ініціацію подальших дій, включно зі створенням пов'язаних індикаторів [22]. Модуль Incidents призначений для консолідації матеріалів розслідування та підтримує групування інцидентів у кампанії, що спрощує відстеження довготривалих або серійних атак і пов'язування їх із типовими ланцюжками активності [22]. У межах Tasks фіксуються дії аналітиків і автоматизованих процедур; додатково зазначається можливість синхронізації із зовнішніми системами керування зверненнями/тикетами, що забезпечує зв'язність між процесами SOC та IT-сервіс-менеджментом [22]. Окреме місце займають Indicators (рис. 2.2) як централізоване сховище ІоС (наприклад, IP, URL, хеш-суми) з атрибутами статусу/типу, що використовується для кореляції та прискорення повторного аналізу подібних подій [3]. Підтримка вкладень (Attachments) дає змогу пов'язувати з кейсами артефакти розслідування (логи, зразки шкідливого ПЗ тощо), тим самим підвищуючи відтворюваність аналізу й якість доказової бази в рамках інциденту [22].

The screenshot shows the 'Indicators' section of the FortiSOAR interface. It features a header with 'Malicious Indicators' and a dropdown for 'Indicators By Type By Rep'. Below the header is a toolbar with buttons for '+ Add', 'Execute', 'Hunt Indicators', and 'Import Bulk Indicators'. The main area contains a table with 453 items. The table has columns for ID, Reputation, Type, Value, Country, and Status. Each row represents an indicator with its specific details.

ID	Reputation	Type	Value	Country	Status
903	No Reputation Available	User	СИСТЕМА		TBD
808	No Reputation Available	User	yuliia.truba		TBD
634	Malicious	Domain	youtube.com		TBD
790	No Reputation Available	User	yaroslav.vasylenko@kyivcity.gov.ua		TBD
789	No Reputation Available	Email Address	yaroslav.vasylenko@kyivcity.gov.ua		TBD
628	Good	Domain	www.youtube.com		TBD
665	Good	Domain	www.wikipedia.org		TBD
600	No Reputation Available	Domain	www.virustotal.com		TBD
691	Good	Domain	www.synevo.ua		TBD

Рис. 2.2. Вкладка Індикаторів в FortiSOAR

Для командної взаємодії під час критичних подій у FortiSOAR передбачено колаборативний формат War Room, який у межах опрацьованих джерел описано як середовище спільного розслідування з інтеграціями з комунікаційними засобами (зокрема MS Teams, Slack, Zoom) [21, 23].

Автоматизація в FortiSOAR реалізується насамперед через плейбуки (Playbooks) – сценарії реагування, які будуються у візуальному конструкторі (no-code/low-code) з підтримкою керуючих конструкцій (рис. 2.3), обробки помилок і виконання Python-коду для розширення логіки [21]. Такий підхід дозволяє переносити типові процедури (первинний тріаж, збагачення, ескалація, запуск дій у суміжних системах) у відтворювані сценарії, зменшуючи залежність від ручного виконання однотипних кроків [21].

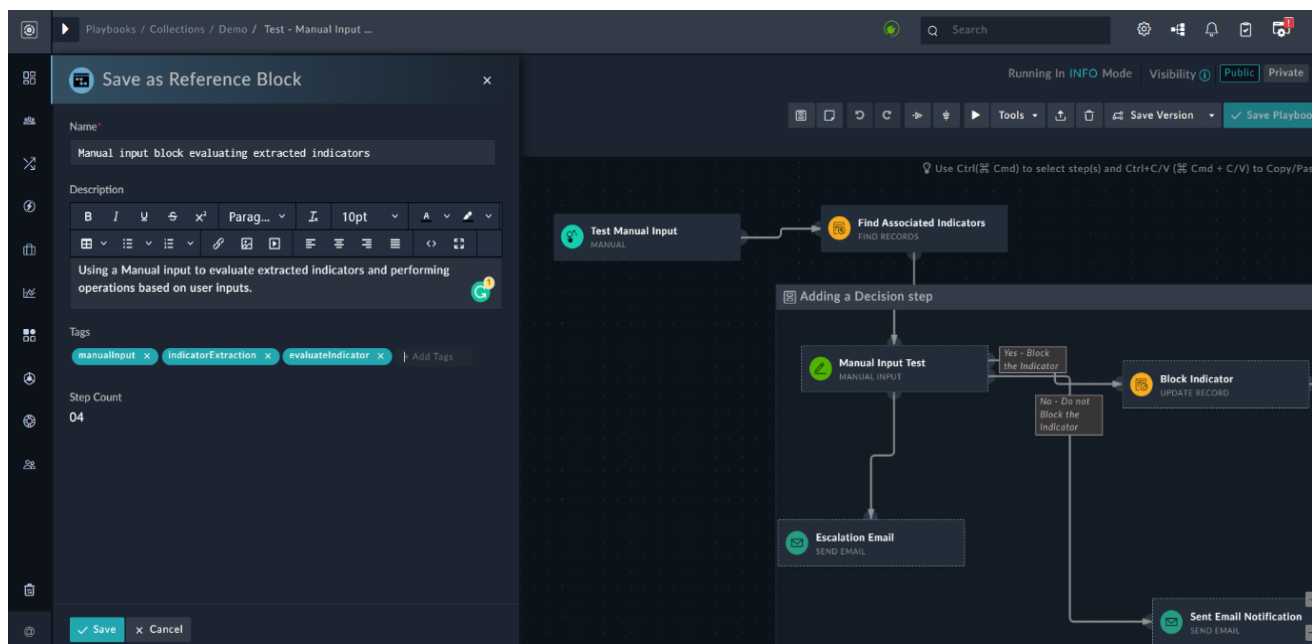


Рис. 2.3. Playbook Designer у FortiSOAR

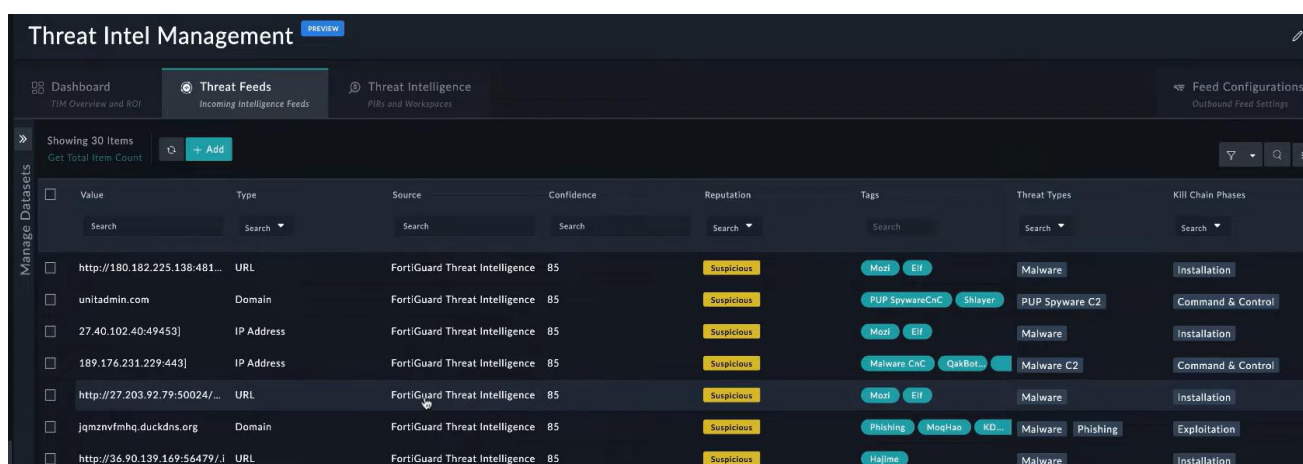
Конектори (Connectors) описані як механізм двосторонньої взаємодії з інструментами безпеки та ІТ, зокрема класів SIEM/EDR/IPS, що дає можливість не лише отримувати дані, а й виконувати керовані дії реагування у зовнішніх системах [21]. У наданих матеріалах фіксуються показники масштабу інтеграцій: зазначено «понад 350 готових інтеграцій» та «3000 автоматизованих дій» [21], а також окремо згадується «понад 500 вбудованих конекторів», що, імовірно, відображає інший підхід до підрахунку/категоризації інтеграцій у межах екосистеми продукту [23].

Операційну дисципліну автоматизації доповнюють можливості запуску сценаріїв за розкладом та керування термінами виконання через SLA-шаблони, що дозволяє формалізувати очікувані часові межі реагування і контролювати дотримання регламентів у процесі обробки інцидентів [3]. Для стандартизації обміну інформацією у SOC окремо виокремлюються шаблони електронних повідомлень, які спрощують уніфіковані внутрішні та зовнішні комунікації під час інцидентів [22].

Для взаємодії з ізольованими сегментами мережі та забезпечення виконання дій без прямого «виходу» у публічну мережу в матеріалах описано використання агентного підходу (FSR-агенти) та механізму Secure Message Exchange (SME), який

гарантує доставку запитів шляхом чергування повідомлень навіть за умов тимчасових розривів зв'язку [22]. У функціональному вимірі це дає змогу реалізовувати окремі сценарії (наприклад, ізоляцію кінцевих точок або локальне збагачення даних) безпосередньо в середовищі організації та з урахуванням локальних облікових даних [22].

У межах FortiSOAR виділяється функціональність Threat Intelligence Management (TIM), призначена для автоматизованого збору та нормалізації розвідувальних даних про загрози з зовнішніх джерел (рис. 2.4). У межах розглянутих документів як приклади таких джерел наведено FortiGuard Labs та Cisco Talos [23]. З погляду задач SOC це забезпечує швидше збагачення кейсів релевантними ІоС та контекстом щодо кампаній і відомих вразливостей, що безпосередньо впливає на якість тріажу та обґрунтованість рішень під час реагування [22].



The screenshot displays the Threat Intel Management (TIM) interface. It features a sidebar with 'Manage Datasets' and a main table showing threat intelligence data. The table has columns for Value, Type, Source, Confidence, Reputation, Tags, Threat Types, and Kill Chain Phases. The data is sourced from FortiGuard Threat Intelligence and includes various threat types like Malware, PUP Spyware C2, and Shlayer.

Value	Type	Source	Confidence	Reputation	Tags	Threat Types	Kill Chain Phases
http://180.182.225.138:481...	URL	FortiGuard Threat Intelligence	85	Suspicious	Most	Malware	Installation
unitadmin.com	Domain	FortiGuard Threat Intelligence	85	Suspicious	PUP Spyware C2, Shlayer	PUP Spyware C2	Command & Control
27.40.102.40:49453]	IP Address	FortiGuard Threat Intelligence	85	Suspicious	Most	Malware	Installation
189.176.231.229:443]	IP Address	FortiGuard Threat Intelligence	85	Suspicious	Malware CnC, QakBot	Malware C2	Command & Control
http://27.203.92.79:50024/...	URL	FortiGuard Threat Intelligence	85	Suspicious	Most	Malware	Installation
jqmznvmhq.duckdns.org	Domain	FortiGuard Threat Intelligence	85	Suspicious	Phishing, MoqHao, KD...	Malware, Phishing	Exploitation
http://36.90.139.169:56479/...	URL	FortiGuard Threat Intelligence	85	Suspicious	Hajime	Malware	Installation

Рис. 2.4. Інтерфейс модуля TIM

Окремо підкреслено підтримку глобального пошуку по ТІ (Threat Intel Search), організацію робочих просторів для пріоритетних запитів (PIR), а також обмін даними за стандартами STIX/TAXII [22]. Це важливо для інтеграції ТІ-процесів із зовнішніми платформами та для забезпечення інтероперабельності даних у гетерогенній екосистемі SOC [22]. Також у матеріалах згадується інтегрований конектор MITRE ATT&CK і модуль Hunts, які орієнтовані на

підтримку сценаріїв «полювання» на приховані загрози та зіставлення активності з тактиками/техніками противника [22, 23].

Для управління ефективністю процесів реагування FortiSOAR передбачає рольові інформаційні панелі та звітність, орієнтовані на кількісні показники діяльності SOC [21]. У матеріалах зазначено наявність готових шаблонів звітів (зокрема щодо закриття інцидентів, тижневого прогресу, зведень ІоС) та інструментів побудови власних віджетів, які дозволяють формувати графіки й таблиці під потреби конкретних ролей (керівництво, менеджмент, аналітики) [21].

Отже, FortiSOAR у межах корпоративного SOC позиціонується як платформа класу SOAR, яка поєднує керований кейс-менеджмент із механізмами інтеграції та автоматизації, забезпечуючи формалізований життєвий цикл обробки інцидентів [20, 22]. Функціональні можливості автоматизації, інтеграції, регламентного керування і командної взаємодії утворюють основу для стандартизації реагування та зниження частки ручної роботи в SOC [21, 23]. Додаткові модулі збагачення ТІ та аналітики/звітності забезпечують підвищення обґрунтованості рішень і контроль результативності через метрики на кшталт MTTD/MTTR, що є важливим для управління операційною ефективністю служби безпеки [21, 22].

2.2 Основні компоненти та архітектура FortiSOAR. Інтеграція з корпоративною інфраструктурою і Fortinet Security Fabric

У SOC-ландшафті FortiSOAR доцільно розглядати як центральний вузол оркестрації між джерелами подій безпеки та виконавчими системами, які здатні реалізувати дію у мережі, на кінцевих точках або в хмарних сервісах. Такий підхід відповідає загальній логіці SOAR, де цінність формується не в ізольованому аналізі телеметрії, а у керованому перетворенні даних на відтворювані рішення та дії [10, 20].

Архітектурно це зручно описується концептом “data-in / action-out”. платформа приймає вхідні події, алерти та артефакти, виконує їхню первинну обробку й нормалізацію, далі ініціює узгоджені реакції у підключених системах та

фіксує результати (стани, коментарі, докази, часові мітки) у централізованій моделі інциденту (рис. 2.5). Саме цей цикл, повторюваний сотні разів на добу, знімає з аналітика частину рутинного навантаження, але водночас зберігає прозорість, без якої автоматизації просто не довіряють [16].

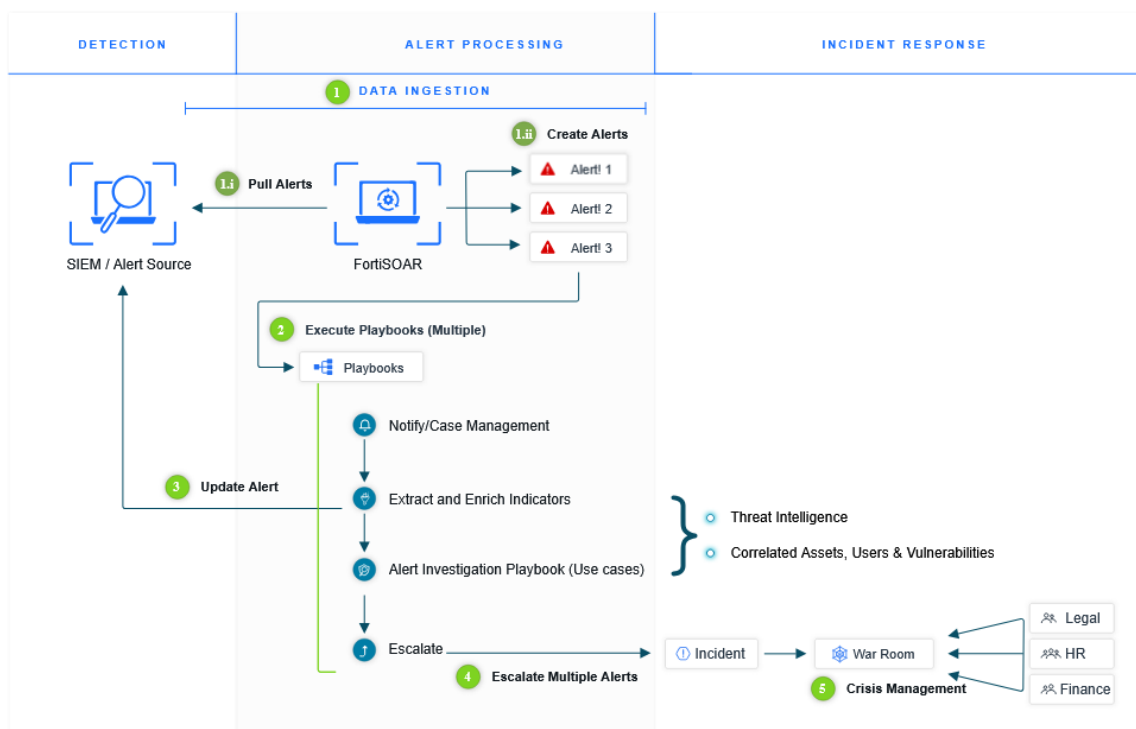


Рис. 2.5. Концептуальний потік обробки алертів у FortiSOAR

Водночас важливо окреслити межі відповідальності FortiSOAR. Платформа не замінює SIEM як шар централізованого збору та кореляції логів і не є EDR як механізм детекції та контролю кінцевих точок. Її роль полягає у надбудові оркестрації та автоматизації: під'єднати різні джерела та виконавців, уніфікувати дані інциденту, забезпечити керовані сценарії реагування і контроль виконання [16, 20].

На логічному рівні FortiSOAR доцільно описувати як сукупність взаємопов'язаних підсистем, кожна з яких забезпечує окрему частину “data-in / action-out” циклу. Центральним елементом виступає ядро керування інцидентами (рис. 2.6), де записи про алерти, інциденти (кейси) та задачі формують структурований контекст розслідування, а також задають відповідальність і хід робіт [22, 23].

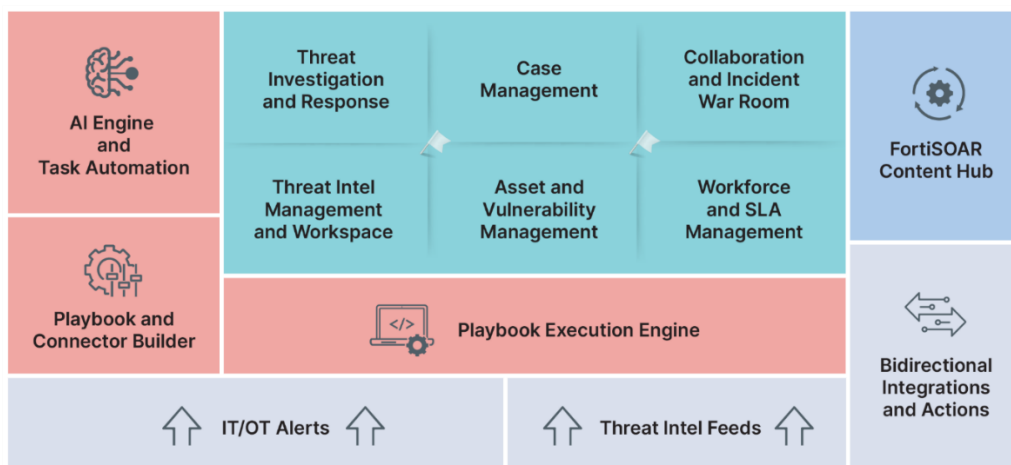


Рис. 2.6. Логічна архітектура FortiSOAR

Другим компонентом є підсистема автоматизації, яка реалізує виконання сценаріїв реагування на основі подій, правил і керованих workflow. Важливо підкреслити саме її роль як механізму виконання, не переходячи до покрокового конструювання сценаріїв: автоматизація тут є “двигуном”, що запускає узгоджені дії у відповідь на тригери та стан інциденту [10, 22].

Третій компонент, критичний саме для корпоративного середовища, це підсистема інтеграції. Вона визначає транспорт взаємодії з зовнішніми системами, включно з готовими конекторами, програмними інтерфейсами та подієвими механізмами, які дозволяють як отримувати дані, так і ініціювати дії у сторонніх продуктах [17, 24].

Окрему роль відіграють сутності знань інциденту: артефакти, індикатори компрометації, вкладення, коментарі та довідникові дані. Вони забезпечують накопичення доказової бази, збереження контексту та повторне використання інформації між етапами розслідування [22].

Нарешті, для керованості та відповідності вимогам безпеки необхідним є шар журналювання та аудиту: фіксація змін у записах, відстеження дій користувачів і результатів автоматизації, а також збереження причинно-наслідкових зв’язків між рішенням і його виконанням. Навіть якісна автоматизація втрачає практичну цінність, якщо її результати неможливо перевірити або відтворити під час внутрішнього розбору інциденту [22].

Інтеграційно-орієнтована архітектура FortiSOAR спирається на те, що різні джерела подій генерують різні формати й структури даних. Тому платформа акумулює декілька базових типів інформації: події та алерти, артефакти й індикатори (наприклад, IP-адреси, URL, хеші), вкладення (файли, журнали), коментарі, метадані та пов'язані задачі, які утворюють цілісний “паспорт” інциденту [22].

Функціонально така уніфікація даних потрібна не лише для зручності відображення. Її ключова роль полягає у нормалізації: приведенні різномірних вхідних повідомлень до спільної моделі, що робить сценарії реагування більш універсальними та переносними між різними джерелами телеметрії. Це узгоджується з підходом, коли процеси реагування мають бути стандартизованими й відтворюваними, а не залежати від випадкових особливостей одного конкретного лог-джерела [10].

З погляду архітектури даних важливими є зв'язки між сутностями. Логіка розслідування зазвичай формується як граф взаємопов'язаних об'єктів, наприклад case пов'язується з артефактами, індикаторами та задачами, а також із вкладеннями та коментарями, які документують перебіг аналізу. Саме ці зв'язки перетворюють “набір алертів” у керований процес реагування, де кожна дія має контекст і наслідок [22].

Інтеграційна модель FortiSOAR включає декілька практичних шляхів підключення корпоративних систем. На концептуальному рівні це можна подати як поєднання: готових конекторів для типових продуктів, програмних інтерфейсів (API) для кастомної взаємодії, подієвих механізмів (зокрема webhooks), а також каналів інжесту для окремих класів даних, наприклад інцидентів із SIEM або повідомлень електронної пошти як частини сценаріїв реагування на фішинг [17, 22].

В архітектурі інтеграцій принципово важливим є розмежування двох типів взаємодії: “читання/збагачення” та “виконання дій”. У першому випадку FortiSOAR агрегує контекст (деталі події, атрибути активу, репутаційну інформацію, пов'язані індикатори), у другому ініціює керовану реакцію у

виконавчих системах (наприклад, блокування, ізоляцію, карантин або створення задач у сервіс-деску). Саме баланс між цими режимами визначає якість автоматизації: без повноцінного контексту реакція стає ризикованою, а без здатності виконувати дію оркестрація втрачає сенс [10].

Питання доступів в інтеграціях мають розглядатися як частина архітектури, а не як “технічна деталь налаштування”. Для інтеграцій характерні ключі й токени, службові облікові записи, ролі та розмежування прав, а також потреба у безпечному зберіганні секретів і контролі їх ротації. В корпоративній мережі особливо важливо, щоб права інтеграцій відповідали принципу найменших привілеїв і були прив’язані до конкретних бізнес-функцій реагування.

Окремо слід відзначити, що інтеграції безпосередньо впливають на стабільність автоматизації. Неповні дані, нестабільні API або некеровані помилки (таймаути, ліміти, тимчасова недоступність сервісу) транслуються у “розриви” сценаріїв. Тому інтеграційна архітектура повинна передбачати контроль стану підключень і узгоджену обробку відмов, щоб автоматизація залишалась передбачуваною навіть у реальних, неідеальних умовах [17].

Масштабування інтеграцій у FortiSOAR логічно пов’язане з механізмом контенту: використанням готових пакунків, які постачають не лише інтеграційні модулі, а й супутні елементи процесу. У загальному вигляді роль пакунків контенту полягає у тому, щоб поєднати конектори, заготовки сценаріїв (workflow), а також шаблони об’єктів і полів, необхідні для уніфікованого ведення інцидентів [22, 24].

Переваги такого підходу полягають у прискоренні впровадження, стандартизації процесів і повторному використанні напрацювань, які вже були “упаковані” у підтримуваний формат. Для SOC це зменшує часовий розрив між потребою (наприклад, підключити нове джерело подій) та фактичним переходом до керованого реагування, що в людському вимірі часто означає зниження виснаження команди від нескінченних ручних перевірок і переключень між консолями [10, 22].

Разом із тим Content Hub і solution packs створюють і специфічні обмеження. До них належать версійні залежності, можливі зміни в структурах полів або

конфігураціях, а також потреба тестування перед розгортанням у продуктивному середовищі. На архітектурному рівні це означає, що організація має мати хоча б мінімальний контур валідації змін: перевірку сумісності, контроль впливу на поточні процеси та план відкату [17, 22].

У межах екосистеми Fortinet Security Fabric FortiSOAR доцільно трактувати як оркестратор, який допомагає перетворити розрізнені засоби захисту на узгоджену систему реакцій. Концептуальна логіка Fabric полягає в узгодженості телеметрії та реакцій: події з різних компонентів формують спільний контекст, а відповіді на інцидент можуть ініціюватися так, щоб підсилювати одна одну на різних рівнях інфраструктури [16, 25].

Типові точки інтеграції в цій моделі охоплюють мережеві та прикладні засоби захисту, аналітичні компоненти та платформи моніторингу. Без прив'язки до конкретного стенду організації, у ролі таких інтегрованих елементів можуть виступати, зокрема, FortiGate, FortiMail, FortiEDR, FortiAnalyzer та FortiSIEM (рис. 2.7). Архітектурна цінність полягає у тому, що FortiSOAR не лише приймає сигнали від цих компонентів, а й може повертати результати аналізу та ініціювати дії у відповідь, підтримуючи замкнений цикл “виявлення – реагування – фіксація” [16, 25].

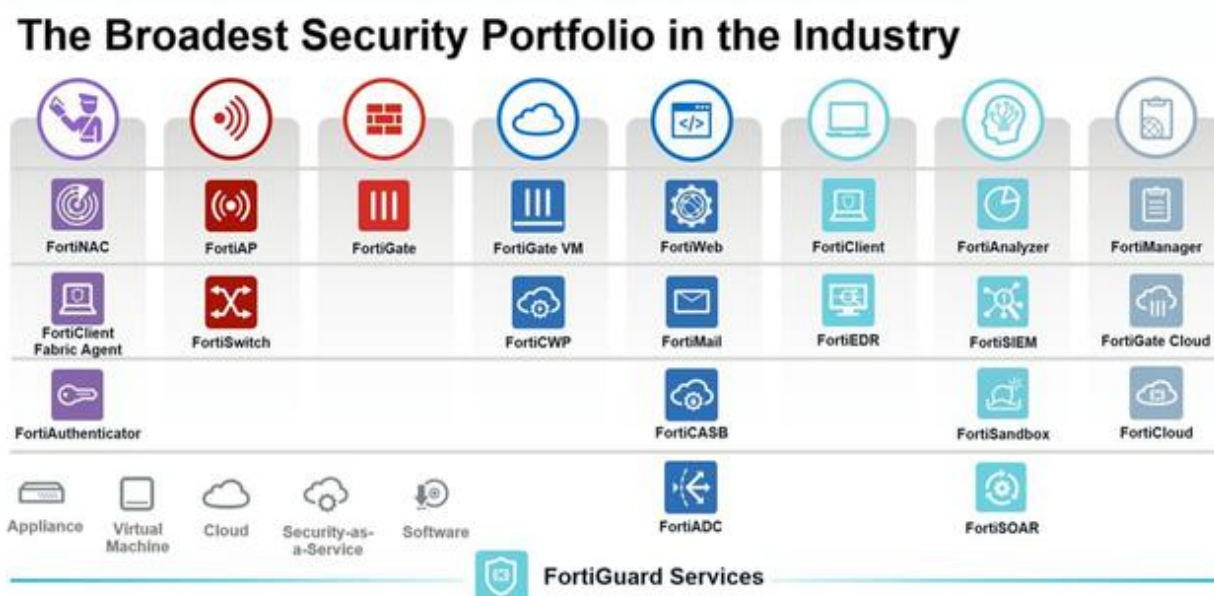


Рис. 2.7. FortiSOAR як частина екосистеми Security Fabric

Сценарії взаємодії з Security Fabric у загальному вигляді зводяться до трьох категорій: збагачення контексту (наприклад, отримання додаткових атрибутів події або активу), передача індикаторів компрометації як елементу колективного захисту та виконання дій (блокування, ізоляція, карантин) у виконавчих системах. Важливо, що в SOC-практиці саме “керованість” цих дій (хто ініціював, на якій підставі, з яким результатом) часто є вирішальною для прийняття автоматизації командою, а не лише сама наявність технічної можливості [16].

Архітектурні вимоги інтеграції починаються з мережевого рівня: доступність зовнішніх сервісів, коректна маршрутизація, використання захищених каналів обміну (типово HTTPS), а також урахування корпоративних проксі та сегментації. У реальному середовищі саме мережеві обмеження часто визначають, які інтеграції можливі напряму, а де потрібні проміжні вузли або окремі канали для обміну даними. [17].

На рівні надійності інтеграції критичними є передбачувана обробка помилок, таймаути, повторні спроби, а також керування чергами задач і “поганими” повідомленнями, які не можуть бути оброблені з першого разу. Для SOC це не теоретичне питання: якщо платформа не витримує деградацію зовнішніх сервісів, автоматизація починає створювати додатковий шум замість того, щоб його зменшувати [10].

Вимоги до безпеки інтеграції охоплюють принцип найменших привілеїв, аудит інтеграційних дій, контроль змін і розмежування ролей (хто може підключати системи, хто може змінювати облікові дані, хто може запускати ті чи інші класи реакцій). У термінах практик кібербезпеки це означає, що інтеграція має бути не тільки функціональною, але й керованою: з чітко визначеними межами доступу та з можливістю перевірки історії рішень під час інцидент-розборів і внутрішніх аудитів.

Таким чином, FortiSOAR у корпоративній мережі доцільно розглядати як інтеграційно-орієнтовану платформу, що забезпечує перехід від “потоків подій” до керованих дій, з фіксацією результатів у спільній моделі інциденту [16, 20]. Її логічна архітектура спирається на ядро керування інцидентами, механізми

автоматизації та підсистему інтеграції, які разом формують цілісний цикл “data-in / action-out” [17, 22]. Важливим фактором масштабування виступають контентні пакунки та каталог інтеграцій, що дозволяють стандартизувати підключення та повторно використовувати напрацювання [22, 24]. На концептуальному рівні взаємодія з Fortinet Security Fabric підсилює узгодженість телеметрії та реакцій, даючи можливість будувати замкнений цикл реагування між компонентами екосистеми [16, 25]. Водночас практична цінність інтеграції визначається не лише функціональністю, а й дотриманням вимог безпеки доступів, стабільності обробки та аудитованості дій, що є критичним для довіри SOC-команди до автоматизації.

2.3 Порядок функціонування платформи FortiSOAR

У контурі SOC платформа класу SOAR зазвичай виконує роль “операційного ядра”, яке поєднує керування інцидентами, оркестрацію інтеграцій та автоматизацію повторюваних дій, щоб перевести реакцію на події з режиму хаотичних ручних кроків у керований процес із фіксацією результатів. Саме ця ідея простежується в загальному визначенні SOAR, де автоматизація не замінює аналітика, а масштабує його можливості та зменшує рутинне навантаження [10, 20].

Логіка роботи у FortiSOAR у типових впровадженнях вибудовується як послідовність: подія або алерт > перетворення у керований робочий об’єкт інциденту (case) > запуск автоматизації через плейбук > виконання дій та/або збагачення > документування фактичних результатів > закриття з видимою історією рішень. Такий підхід узгоджується з практикою організації incident handling як життєвого циклу з етапами підготовки (рис. 2.8), обробки, відновлення та подальшого вдосконалення, де важлива не тільки реакція, але й контрольоване завершення з уроками та артефактами [5].



Рис. 2.8. Узагальнені фази реагування на інцидент у SOC

Межі застосування платформи в SOC залежать від зрілості процесів та ризик-профілю. FortiSOAR може керувати процесом “від старту до закриття”, коли вхідні сигнали надійно нормалізовані, інтеграції стабільні, а правила автоматизації узгоджені з політиками доступу. У більш стриманих сценаріях платформа зосереджується на агрегації даних, узгодженні командних дій і централізованому веденні кейса, залишаючи частину кроків у ручному режимі, щоб зберегти контроль над ризиковими операціями. Така варіативність відповідає загальній логіці SOAR: автоматизується те, що повторюється і добре формалізується, а “нестандартні” ситуації залишають простір для експертного рішення [10, 20].

Порядок функціонування FortiSOAR починається з надходження вхідних сигналів. Типові канали включають інтеграційні конектори, webhooks, API-взаємодію, поштовий ingest, імпорт даних та планові запити до зовнішніх систем. З погляду SOAR це не просто “доставка повідомлення”, а механізм, який має забезпечити достатній контекст для подальшої автоматизації, тобто зробити подію придатною до машинної обробки [10, 22].

Первинна нормалізація у вхідному потоці спрямована на те, щоб зберегти мінімально необхідні атрибути для старту обробки: час події, джерело та тип, пріоритет або критичність, а також ключові артефакти, навколо яких і буде будуватися збагачення та реагування (наприклад, адреси, хеші, URL, ідентифікатори сутностей). Якщо на вході цих полів немає, автоматизація швидко перетворюється на набір припущень, тому якість вхідного “каркасу” прямо впливає на надійність плейбуків [5, 22].

Далі інформація прив’язується до об’єктної моделі платформи, де алерт слугує пусковим сигналом, а інцидент (case) стає центральним об’єктом керування роботою. Початкове наповнення кейса зазвичай включає базові поля інциденту, посилання на джерело, первинні артефакти та технічні деталі, які згодом можуть доповнюватися в результаті збагачення. Така прив’язка потрібна, щоб подальші дії не “розпорошувалися” між різними каналами, а фіксувалися у єдиному керованому контексті [22].

Після створення або оновлення кейса запускається етап ініціалізації, коли кейс набуває ознак керованого робочого процесу: визначається стан життєвого циклу, уточнюється пріоритет, формуються задачі та відповідальні, задаються очікувані терміни або SLA-параметри, якщо вони використані у процесі. У практиці SOC цей крок важливий ще й психологічно: він переводить “шум подій” у зрозумілий список відповідальностей, де видно, хто що робить і на якому етапі перебуває інцидент. [5, 22].

План каркасу підрозділу передбачає обговорення дедуплікації, кореляції та ескалації як правил створення або оновлення кейса. У наданих матеріалах кореляція та ескалація описані як типові механізми перетворення алертів у керовані інциденти, тоді як деталізація окремого механізму дедуплікації у FortiSOAR не розкрита, тому цей аспект варто розглядати як практичну вимогу процесу, але без прив’язки до конкретної реалізації в платформі [22].

Документування на етапі ініціалізації формує основу прозорості. У межах кейса накопичуються коментарі, результати дій, артефакти та матеріали розслідування, а також відомості про зміни, що підтримують аудит і відтворюваність розгляду інциденту. Такий підхід підсилює довіру до автоматизації: аналітик бачить не тільки “що спрацювало”, але й “чому саме так” та “хто ініціював зміни”, що є критичним для керування ризиком і якості процесу [5, 22].

Після того як кейс створено і потрапив у робочий контур, настає момент запуску автоматизації. У FortiSOAR використовується кілька моделей запуску плейбуків: подієві тригери (on create, on update), ручний запуск аналітиком, запуск за розкладом (schedule), а також умовні запуски за ознаками об’єкта, тегами чи рівнем критичності. Практичне значення цієї багатомодальності в тому, що SOC може поєднувати “швидкі” реакції для стандартних кейсів і більш обережні режими там, де потрібна додаткова перевірка [22]

Центральним механізмом “коли і який playbook” виступають automation rules, які дозволяють зіставити подію з відповідним сценарієм реагування (рис. 2.9). Логіка правил у межах наявної документації описується як побудова умов для

запуску, де важливі фільтри за об'єктами та атрибутами, а також керування тим, які саме плейбуки дозволено запускати у певному контексті. Такий шар правил є містком між об'єктною моделлю (alerts, cases) та оркестрацією дій, і фактично задає політику автоматизації для SOC [22].



Рис. 2.9. Узагальнена логіка SOAR-обробки

Окремо слід підкреслити узгодження автоматизації з ролями та правами доступу (RBAC). Плейбук може бути технічно готовий, але його запуск і виконання повинні відповідати політикам доступу, щоб автоматизація не “перескочила” через контрольні бар’єри. У наданих матеріалах акцентовано, що для роботи з плейбуками та інтеграціями важливі права читання, створення, оновлення та виконання, а також практика обмеження привілеїв інтеграційних облікових записів за принципом мінімально необхідних прав. Це створює основу безпечної автоматизації, коли платформа виконує лише те, що їй дозволено у межах ролей і політик [6, 22].

Виконання плейбука у FortiSOAR можна описати як керовану послідовність кроків, де кожен крок або збирає дані, або приймає рішення, або виконує дію, а результати повертаються у контекст кейса. Типова структура сценарію виглядає як: збір даних > збагачення > логічне рішення > виконання дій реагування > фіксація результату. Ця структура зручна тим, що дозволяє відокремити етап “зрозуміти

ситуацію” від етапу “вплинути на ситуацію”, а також забезпечити відтворюваність рішень у схожих інцидентах [10, 22].

Логіка плейбуків у наданих матеріалах підтримує умовні гілки (вибір), що дозволяє відрізняти обробку за типом артефактів або за рівнем критичності. Окремо важливими є цикли для роботи з множинними артефактами, коли один кейс може містити кілька URL, кілька хешів, кілька адрес чи інші множинні сутності. Саме тут автоматизація демонструє найбільшу “економію часу”: замість повторення однакових кроків вручну, платформа відпрацьовує їх у стандартизованому циклі та акуратно складає результати у кейс [10, 22].

Стійкість автоматизації визначається не лише “успішними” шляхами, а й тим, як обробляються збої інтеграцій. В межах опрацьованих джерел згадано використання таймаутів, повторних спроб (retry), fallback-логіки та фіксації помилок інтеграцій. Ці механізми дозволяють відокремлювати тимчасові відмови зовнішніх сервісів від реальних ознак компрометації, а також зменшують ризик ситуації, коли плейбук “обривається” без зрозумілого пояснення [21, 22, 23].

Концепт “human-in-the-loop” у контексті плейбуків означає, що для критичних дій можуть бути передбачені точки підтвердження. В межах розглянутих документів ця ідея підтримується через поєднання автоматичних та ручних механізмів запуску, а також через організацію задач і ролей у кейсі: автоматизація може підготувати контекст і рекомендації, а остаточне виконання ризикового кроку залишити аналітику. Це дає баланс між швидкістю та відповідальністю, що особливо важливо для дій, які здатні вплинути на бізнес-процеси [6, 22].

Оркестрація інтеграцій у FortiSOAR практично проявляється як взаємодія з зовнішніми джерелами для збагачення (enrichment) і як виконання керованих дій (action). Збагачення орієнтується на отримання додаткового контексту з репутаційних сервісів, sandbox, джерел Threat Intelligence або інших систем, які можуть допомогти класифікувати подію. Дії реагування, навпаки, спрямовані на зміну стану середовища: блокування, карантин, створення тикета, ініціація комунікації та інші операції, що знижують ризик або фіксують результат у

суміжних системах. Такий поділ “спочатку зрозуміти, потім вплинути” є характерним для практик SOAR і підтримує керованість процесу [10, 20].

В статті підкреслено що результати інтеграцій повертаються у кейс у різних формах: як оновлені поля інциденту, як артефакти та індикатори, як вкладення або як коментарі з технічними деталями виконання. Завдяки цьому SOC отримує не лише “факт виконання”, але й доказову базу: що саме було перевірено, які відповіді повернули зовнішні сервіси, які рішення були прийняті на основі цих відповідей. Така фіксація підсилює якість розслідувань і спрощує подальший аудит [22].

Стандартизація результатів потрібна, щоб один раз сформовані шаблони даних і підходи до збагачення можна було повторно використовувати в інших сценаріях. У FortiSOAR це підтримується концепцією уніфікованих дій конекторів та спільних підходів до наповнення об’єктів, а також можливістю підключати та оновлювати інтеграції через каталоги конекторів і типові пакети контенту. Це зменшує “ручну творчість” у кожному плейбуку й робить процес більш передбачуваним для команди [22, 24].

Окремий практичний аспект оркестрації стосується виконання кроків у відокремлених сегментах мережі. За наявними джерелами описано використання агентів (FSR-agent) та механізму Secure Message Exchange, що дозволяє виконувати дії через проміжний вузол із контрольованими службами. Такий підхід важливий для корпоративних мереж, де прямий доступ із платформи до внутрішніх ресурсів обмежений, а реагування все одно має бути технічно здійсненим і керованим [22].

Комунікаційний шар у FortiSOAR включає використання шаблонів повідомлень (email templates), що дозволяють стандартизувати розсилки та зменшити кількість помилок у взаємодії з користувачами й стейкхолдерами. Цінність шаблонів у SOC часто недооцінюють, хоча саме вони допомагають підтримувати єдиний стиль комунікації та не втрачати критичні деталі під час інцидентів, коли команда працює під тиском часу [22].

План каркасу також згадує сповіщення та ескалації. У наданих матеріалах ці аспекти напряду не деталізовані як окремі механізми, однак логіка стандартизованих повідомлень та керування життєвим циклом кейса створює

основу для керованої ескалації у процесі: зміни статусу, призначення відповідальних, формування задач і подальші комунікації можуть узгоджуватися у межах кейса, без розпорошення по сторонніх каналах [22].

Для колаборації й прозорості роботи команди за наявними джерелами описано концепцію War Rooms та інтеграцію з популярними інструментами командної взаємодії. Ідея полягає в тому, щоб обговорення кейса, ключові рішення та контекст не зникали в приватних чатах, а були доступні учасникам процесу та пов'язані з інцидентом. Це знижує ризик “втрати пам'яті” під час зміни чергувань та робить розслідування відтворюваним [21, 23].

Відтворюваність комунікацій означає, що SOC може відповісти на питання: що було повідомлено, кому, коли і за якими умовами. У межах кейса це підтримується через фіксацію результатів плейбуків, коментарі та історію змін, а також через використання стандартних шаблонів повідомлень. У підсумку комунікація стає частиною керованого процесу, а не “паралельним світом”, що існує окремо від інциденту [22].

Контроль виконання автоматизації передбачає видимість того, що відбувається під час роботи плейбука: статуси, трасування кроків і фіксація помилок. У наданих матеріалах це описано як поєднання механізмів виконання сценарію та збереження результатів у кейсі, що дає можливість аналізувати як технічні наслідки, так і управлінські рішення. Для SOC це критично, бо автоматизація без пояснюваності швидко втрачає довіру, особливо після першого збою у виробничому середовищі [6, 22].

Метрики SOC у межах розглянутих документів згадуються в узагальненому вигляді як показники, що дозволяють оцінювати ефективність обробки інцидентів (зокрема MTTR та MTTD), а також навантаження на команду та частку автоматизованих дій. Така аналітика важлива не як “красиві графіки”, а як інструмент управління: вона показує, де процеси справді прискорилися, а де автоматизація створила нові вузькі місця чи ризики [21, 23].

Звіти та дашборди у FortiSOAR можуть виступати механізмом керування ефективністю, коли керівник SOC бачить картину по типах інцидентів,

дотриманню термінів, завантаженню груп і результативності автоматизації. Важливо, що такі звіти мають спиратися на якісні первинні дані у кейсах, тому дисципліна документування та коректна побудова плейбуків прямо впливають на якість управлінських висновків [21, 22, 23].

Експлуатація FortiSOAR у корпоративному середовищі неможлива без керування змінами контенту автоматизації. В межах опрацьованих джерел описано підходи до організації плейбуків як керованих об'єктів: іменування, опис, теги, власники, коментарі та налаштування видимості (public або private). На практиці це знижує “хаос сценаріїв”, коли в SOC накопичуються десятки плейбуків, і без стандартизації стає складно зрозуміти, який сценарій актуальний і хто відповідає за його підтримку [22].

Версійність, тестування перед впровадженням та контроль змін логічно пов'язані з безпекою експлуатації. У межах розглянутих документів акцентовано RBAC та необхідність коректного розмежування прав для виконання плейбуків і дій інтеграцій, а також практику мінімізації привілеїв інтеграційних облікових записів. У підсумку керування змінами має бути не лише “технічним”, але й організаційним процесом: хто може змінювати, хто може запускати, хто може виконувати критичні дії [6, 22].

Окремим джерелом змін є інтеграції та Solution Packs. У наданих матеріалах описано використання контентних пакетів і залежностей між ними, а також необхідність враховувати версії та сумісність під час оновлень. Це підводить до потреби регламенту оновлень: планування, оцінювання впливу, перевірка залежностей, а також контрольований перехід у продуктивне середовище, щоб оновлення конектора або пакета не зламало критичний плейбук у момент реального інциденту [22, 24].

Таким чином, FortiSOAR у контурі SOC підтримує керований життєвий цикл інцидентів, де кейс виступає центральним контекстом для автоматизації, комунікацій та фіксації результатів [20, 22]. Платформа дозволяє поєднувати різні моделі запуску плейбуків, що дає змогу балансувати між швидкістю реагування і контролем ризикових дій через ролі, права та ручні точки участі аналітика [6, 22].

Оркестрація інтеграцій розділяє збагачення та виконання дій, а результати повертаються у кейс у формах, придатних для подальшого аналізу та аудиту [10, 22]. Комунікаційні механізми, зокрема шаблони повідомлень і колабораційні підходи, допомагають зробити взаємодію повторюваною та прив'язаною до інциденту, а не до розрізнених каналів [21, 22]. Контроль виконання, звітність і метрики створюють підґрунтя для управління ефективністю процесів SOC, якщо автоматизація спирається на якісно структуровані дані та дисципліну документування [21, 23]. Експлуатація FortiSOAR потребує керування змінами плейбуків та інтеграцій, включно з обмеженням прав, контролем оновлень і врахуванням залежностей контенту, щоб автоматизація залишалася надійною у виробничому контурі [22, 24].

Отже, у розділі 2 проаналізовано застосування FortiSOAR як платформи класу SOAR у корпоративному SOC для централізації обробки інцидентів та оркестрації дій між засобами безпеки й ІТ. Показано, що керований кейс-менеджмент із типовими сутностями алертів, інцидентів, задач, індикаторів і вкладень формує єдиний контекст розслідування та накопичує доказову базу. Обґрунтовано роль плейбуків як механізму автоматизації повторюваних процедур тріажу, збагачення та виконання реакцій, з можливістю розширення логіки через Python і керування помилками. Охарактеризовано інтеграційно-орієнтовану архітектуру за принципом data-in/action-out, у якій нормалізовані дані перетворюються на керовані дії у підключених системах із фіксацією результатів, журналюванням і аудитом. Розглянуто інтеграції через конектори, контентні пакунки та взаємодію з Fortinet Security Fabric, що підтримує замкнений цикл виявлення, реагування і документування. Визначено порядок функціонування як послідовність від події до case, запуску плейбуків за тригерами, вручну або за розкладом, виконання кроків і контрольованого закриття інциденту. Підкреслено значення RBAC, шаблонів комунікацій, колаборації War Room та керування змінами плейбуків і інтеграцій для надійності автоматизації та вимірювання ефективності через метрики SOC

3 ТЕХНОЛОГІЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Технологія застосування плейбука перевірки підозрілих фішингових листів у FortiSOAR

Підрозділ описує технологію застосування плейбука перевірки підозрілих фішингових листів у FortiSOAR у сценарії, коли ініціатором звернення виступає користувач. Метою є автоматизація первинної перевірки листа та підготовка матеріалів для подальшого експертного аналізу в SOC. Практичний сенс такого підходу полягає в тому, щоб перетворити розрізнені дані електронного листа на структурований набір артефактів, виділених індикаторів компрометації (IoC) та результатів їх збагачення, придатних для відтворюваного розбору інциденту. Очікуваним результатом виконання сценарію є сформований запис інцидентного об'єкта в FortiSOAR із прив'язкою оригінального повідомлення, виділеними IoC (URL, хеші файлів) та збереженими відповідями зовнішніх сервісів збагачення, які підсилюють доказову базу. Межі сценарію принципові: платформа не виконує блокувань і не завершує процес автоматичним вердиктом, а зосереджується на прискоренні та стандартизації збору й верифікації даних.

Узагальнена схема процесу має вигляд: «користувач > пошта > FortiSOAR ingest > парсинг > збір IoC > enrichment > проміжна відповідь > аналіз аналітика > закриття». Користувач ініціює перевірку, пересилаючи підозрілий лист у визначений канал, що дозволяє мінімізувати затримку між виявленням підозри та стартом обробки. Поштова система виконує роль контрольованого середовища доставки повідомлення до заданої папки, де створюються умови для запуску автоматизації без додаткових ручних дій. FortiSOAR ingest приймає подію надходження листа і підхоплює первинні дані, забезпечуючи цілісність «ланцюжка доказів» через збереження оригіналу та службових атрибутів повідомлення. Далі

виконується парсинг: вилучаються заголовки, вміст і вкладення, а також виділяються потенційні IoC, які становлять основу подальшої перевірки. На етапі збору IoC артефакти нормалізуються і готуються до збагачення, щоб результати зовнішніх перевірок були зіставними та придатними для кореляції. Етап enrichment забезпечує верифікацію IoC через зовнішні сервіси, формуючи технічні свідчення, які згодом використовуються аналітиком як аргументи під час прийняття рішення. Паралельно користувач отримує проміжну автовідповідь, яка знижує невизначеність, фіксує факт прийому звернення та задає базову безпечну поведінку до отримання фінального висновку. Завершальним етапом є аналіз аналітика, який інтерпретує зібрані докази в контексті організації та після цього закриває кейс вручну.

Сценарій може функціонувати в середовищах електронної пошти Microsoft 365 або у варіанті on-prem, оскільки логіка запуску спирається на подієвий факт потрапляння листа в задану папку, а не на специфічну модель розгортання поштового сервісу. Ключова умова ініціації визначена однозначно: у темі листа має міститися ключове слово “TEST-fortiSOAR”, після чого лист потрапляє у папку “testfortisoar”. Тригер запуску є подієвим і спрацьовує в момент потрапляння листа до папки, що забезпечує передбачувану точку старту та відділяє «вхідні» повідомлення від загального потоку пошти. Практично це означає, що до FortiSOAR надходять лише ті звернення, які пройшли первинний організаційний фільтр, а сам механізм запуску мінімізує ризик випадкового опрацювання нерелевантних листів. Якщо лист не відповідає умовам маршрутизації (немає ключового слова або він не потрапив до цільової папки), автоматизація не ініціюється, а подальші дії перебувають поза межами цього сценарію. Додатковою умовою працездатності технічного розбору є наявність оригінального повідомлення у форматі, придатному для вилучення метаданих, тому в разі відсутності вкладеного файлу з оригінальним листом (.msg або .eml) процес передбачає відмову в автоматичній обробці з поверненням користувачу повідомлення про необхідність додати оригінал; приклад такої комунікації ілюструє рис. 3.1.

Re: [DANGER!] TEST-fortiSOAR Перевірка листа на ШПЗ - Security Review

Підсумувати



soar

Кому: Василенко Ярослав Олександрович



Відповісти

Відповісти всім

Переслати

...

ср 24.12.2025 20:05

Дякуємо за відправлений лист. Ми спробуємо проаналізувати його якомога швидше та повернемося до Вас зі зворотною відповіддю.

Поки що **попередьте колег** про підозрілий лист та **не відкривайте** його та посилання в ньому.

З повагою,
SOC Team

Рис. 3.1. Автоматизована відповідь користувачу про прийняття звернення

Після запуску сценарію відбувається формування об'єкта для подальшої роботи SOC, який використовується як контейнер доказів і робочий простір для аналітика. У реалізованій логіці створюється запис алерту з описовими атрибутами, що відображають походження повідомлення, первинні дані та службовий контекст, зокрема дані про ініціатора звернення, оригінального відправника, тему, час, а також технічні заголовки, необхідні для аналізу маршруту доставки та можливих аномалій. До алерту прив'язується вкладення з оригінальним листом як доказовий об'єкт, що підтримує трасованість і дозволяє виконувати повторний аналіз без втрати вихідних даних; у термінах візуального подання це узгоджується з прикладом картки алерту на рис. 3.2.



Рис. 3.2. Картка алерту фішингового інциденту у FortiSOAR

Документування результатів відбувається не як одноразовий підсумок, а як накопичення структурованих елементів: окремі ІоС фіксуються у вигляді

індикаторів, результати enrichment додаються до описів індикаторів та/або коментарів, а звіти sandbox можуть зберігатися як вкладені або приєднані описи артефактів. Такий підхід створює «доказовий пакет», у якому технічні факти відокремлені від інтерпретації, але залишаються доступними для перевірки та аудиту.

Первинне вилучення даних починається з приймання та обробки повідомлень у межах ланцюжка плейбуків, де для інжесту та отримання листів застосовується плейбук “TEST - Exchange Ingest & Fetch”, а для розбору конкретного звернення - “TEST - Exchange Process Email”. Логіка інжесту полягає у вибірці повідомлень з контрольованого джерела та передаванні їх у внутрішню обробку; цей фрагмент процесу відображено на рис. 3.3.

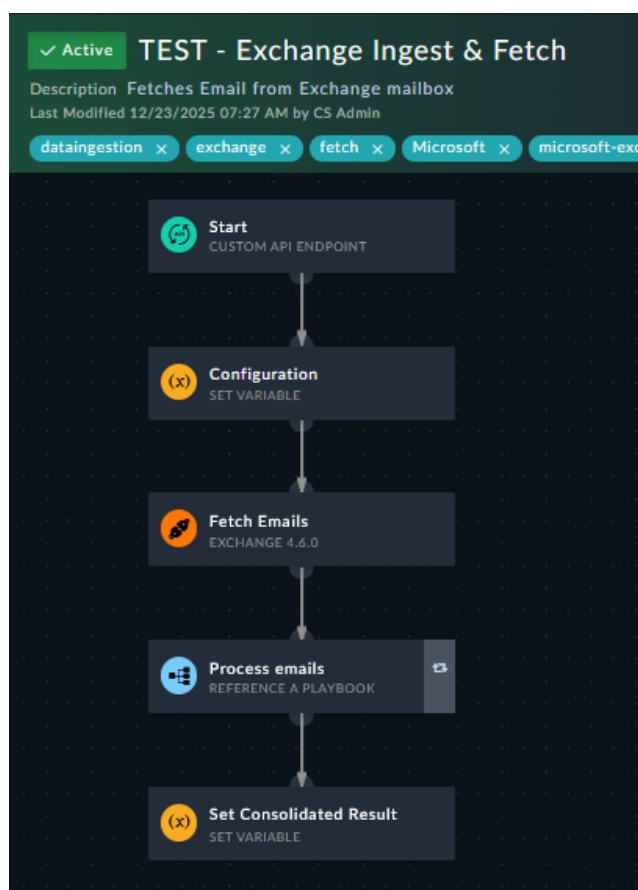


Рис. 3.3. Плейбук інжесту фішингових листів з Exchange у FortiSOAR

На етапі первинної обробки виконується виокремлення службового контексту звернення, зокрема визначається адреса ініціатора та тема листа, а також перевіряється, чи не є повідомлення відповіддю в уже створеному ланцюжку

комунікації. Якщо у темі присутній маркер, що вказує на належність листа до існуючого алерту, звернення може бути маршрутизоване на окрему обробку відповіді без повторного створення інцидентного об'єкта; деталізацію внутрішньої логіки цього відгалуження не описано. Базовими первинними даними є заголовки листа, тіло повідомлення та виділені URL, а базовим “attachment” розглядається сам лист від користувача як доказ факту звернення. Для глибшого технічного розбору сценарій спирається на вкладений оригінал листа у форматі .eml або .msg, з якого вилучаються заголовки, текстова або HTML-частина, а також вкладення з їх метаданими. Вилучення headers використовується як технічний контекст, який дозволяє аналізувати ланцюжок доставки, ознаки підміни та нетипові атрибути повідомлення, тоді як тіло листа є основним носієм соціальної інженерії, текстових «гачків» і посилань; приклад представлення вмісту листа як джерела ІоС і ознак соціальної інженерії наведено на рис. 3.4.

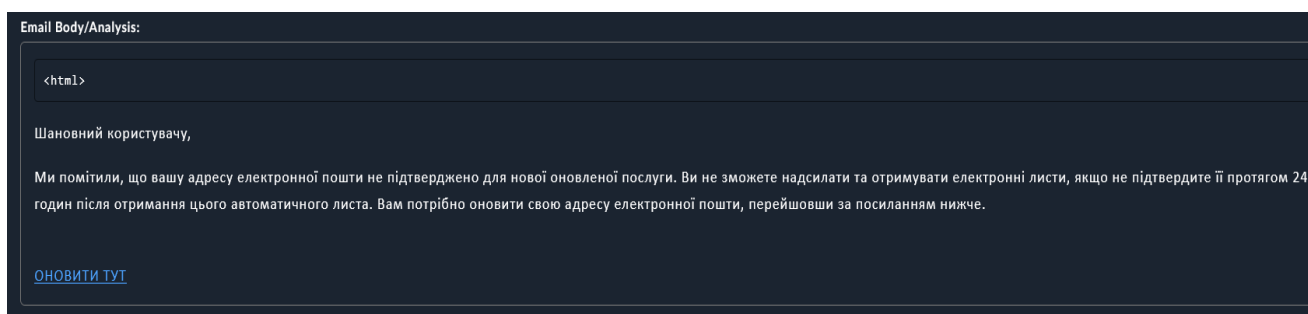


Рис. 3.4. Вміст підозрілого листа як джерело ІоС та ознак соціальної інженерії

Виділення URL виконується як критично важлива частина підготовки ІоС, оскільки саме посилання часто виступає первинним механізмом доставки шкідливого контенту або збору облікових даних. Окремо трактуються вкладення: за наявності прикріплених файлів з них обчислюється SHA-256, який використовується як стійкий ідентифікатор для подальшої перевірки репутації та кореляції між подіями. Підготовка артефактів включає початкову нормалізацію, зокрема усунення дублікатів у переліках URL і доменів, щоб зменшити шум і зробити результати enrichment більш керованими. Узагальнена логіка первинної обробки та переходу до збагачення ілюструється на рис. 3.5 і рис. 3.6 а етап виділення індикаторів узагальнено на рис. 3.7.

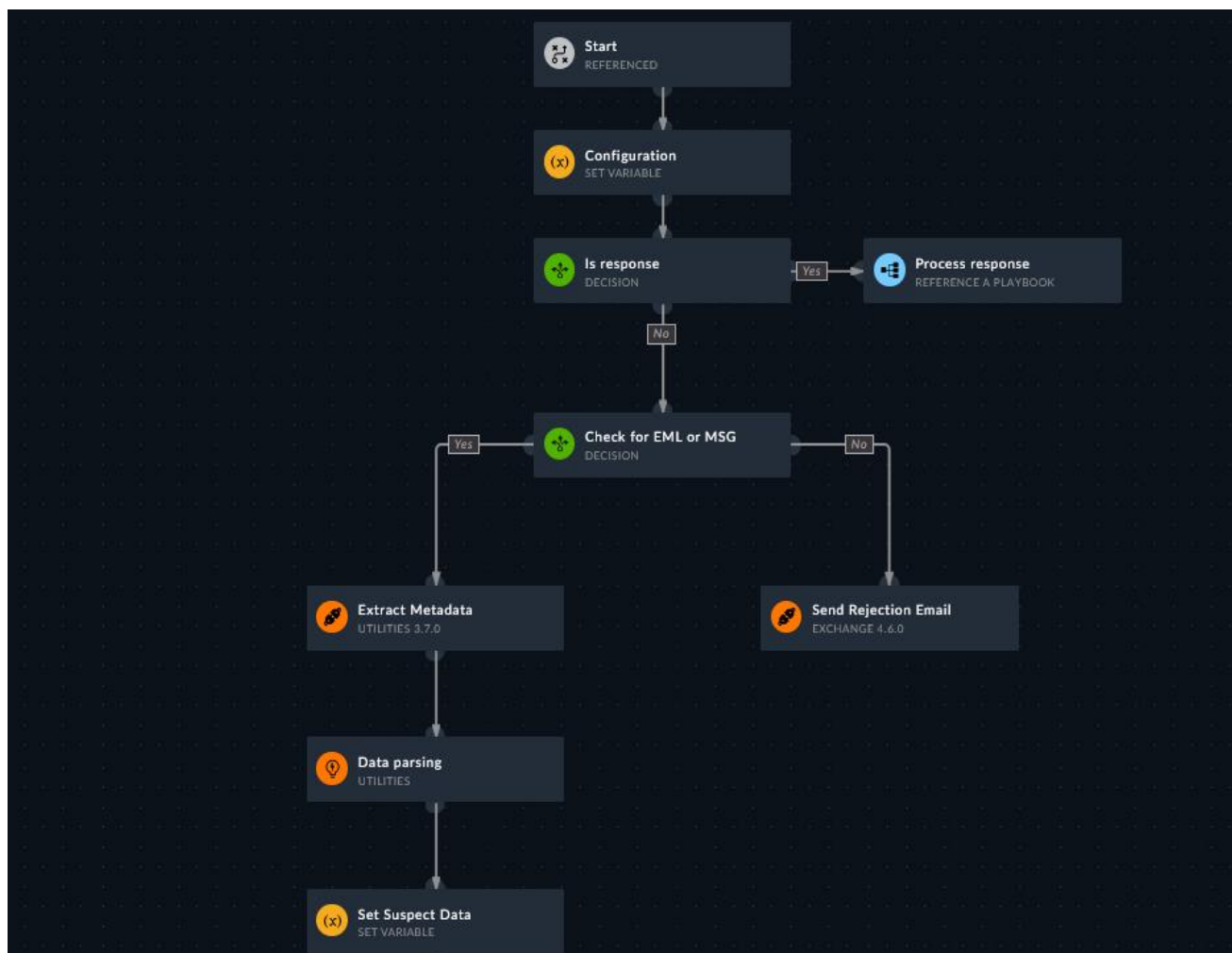


Рис. 3.5. Плейбук первинної обробки фішингового листа



Рис. 3.6. Плейбук розширеної обробки фішингового листа

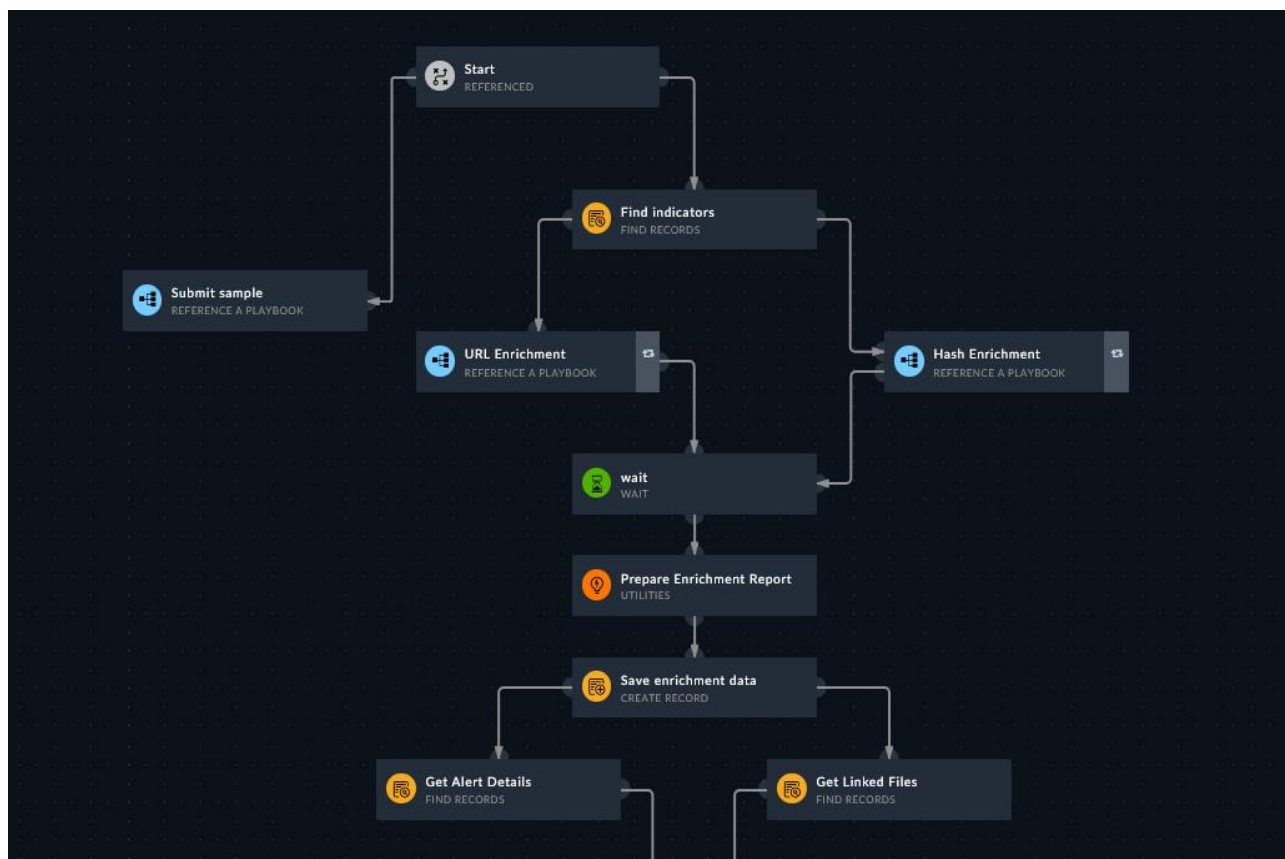


Рис. 3.7. Збір IoC з фішингового листа

Автоматизоване збагачення у цьому сценарії розглядається як етап верифікації IoC та накопичення доказів, а не як механізм постановки «діагнозу» листу. Його мета полягає у тому, щоб перевірити індикатори компрометації (URL і хеші) у зовнішніх джерелах, зібрати додатковий контекст і зафіксувати результати у формі, зручній для подальшої інтерпретації аналітиком. Збагачення виконується через набір сервісів, до яких віднесено VirusTotal (VT), AlienVault OTX, URLscan, Recorded Future та sandbox. Технічно запуск збагачення організовано через плейбук “TEST - PhishEmail IOC Enrichment”, який знаходить індикатори, пов’язані з алертом, і запускає підпроцеси для окремих типів IoC.

Для URL застосовується перевірка через сервіс URLscan, де формується підсумок щодо характеристик вебресурсу, інфраструктурних ознак та наявних сигналів шкідливості; відповідний фрагмент збагачення відображено на рис. 3.8.

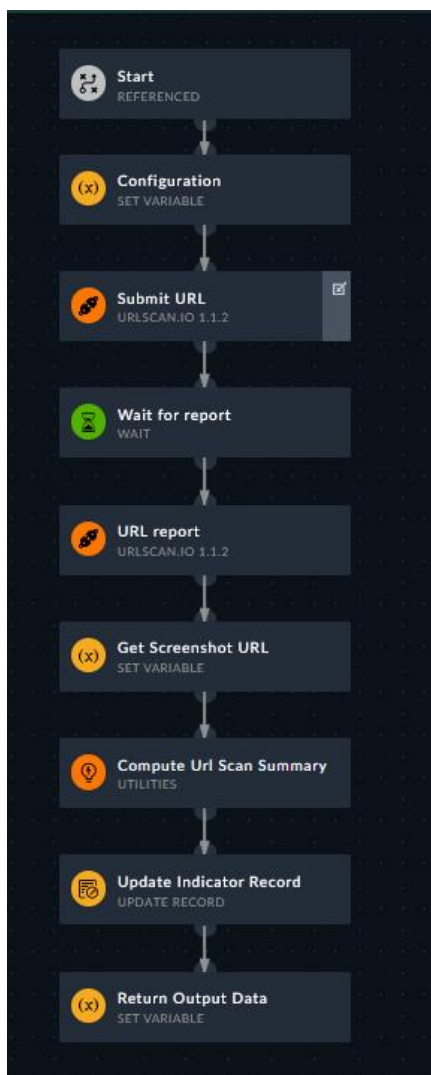


Рис. 3.8. Плейбук перевірки URL у сервісі URLScan

Для хешів файлів застосовується збагачення репутації через VT та OTX, що дозволяє встановити, чи відомий зразок у публічних базах, і які сигнали щодо нього накопичені спільнотою або аналітичними двигунами; ці перевірки узагальнюються на рис. 3.9 і рис. 3.10. Якщо у зверненні присутні вкладення, додатково може застосовуватися поведінковий або динамічний аналіз у sandbox, який дає спостережувані ознаки виконання та взаємодії файлу із середовищем, не підміняючи при цьому рішення аналітика; приклад такого етапу наведено на рис. 3.11. Підхід до інтерпретації результатів enrichment принципово доказовий: сигнали зовнішніх сервісів розглядаються як свідчення, що підсилюють або послаблюють підозру, але не знімають потреби у перевірці контексту, зіставленні з політиками організації та аналізі первинного змісту листа.

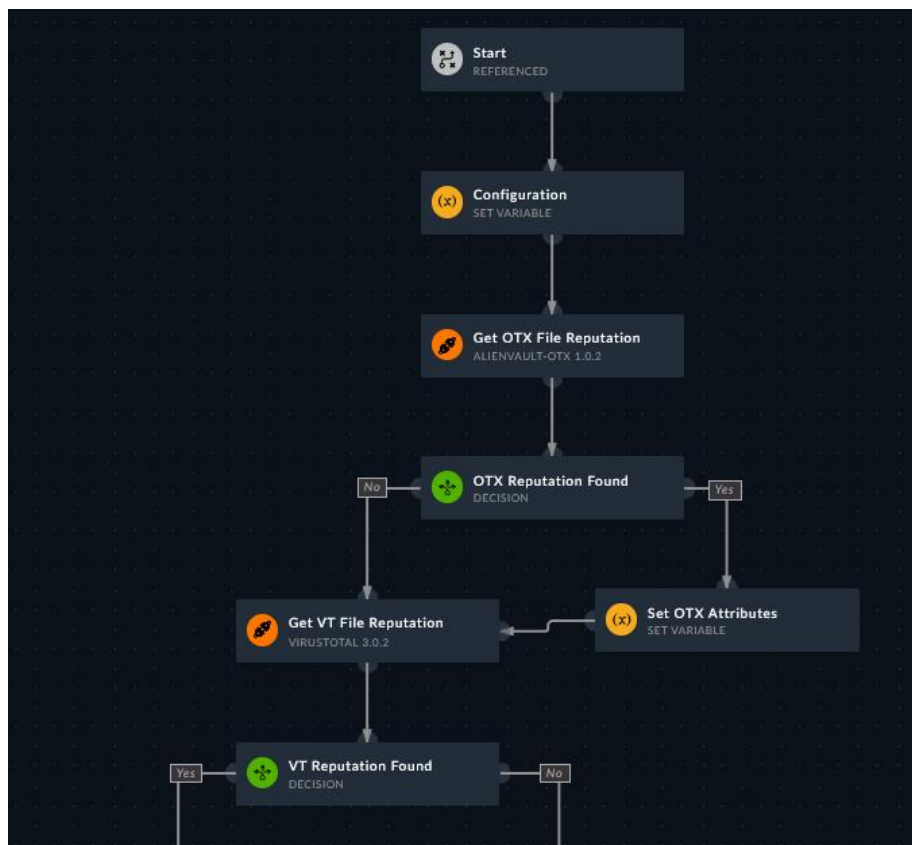


Рис. 3.9. Збагачення хеш-індикаторів VT



Рис. 3.10. Збагачення хеш-індикаторів OTX



Рис. 3.11. Плейбук аналізу вкладень у пісочниці

Результати enrichment з різних джерел агрегуються у межах інцидентного об'єкта як доказовий пакет, що поєднує структурований перелік IoC з прив'язкою до алерту та контекстом їх перевірок. Практично агрегація означає, що окремі результати перевірки URL, хешів і вкладень не залишаються розрізненими відповідями інтеграцій, а перетворюються на збережені артефакти: індикатори отримують описи з підсумками перевірок, у картці алерту додаються коментарі зі зведеною інформацією, а дані sandbox можуть фіксуватися у вкладеннях або описах пов'язаних файлів. Саме така фіксація важлива для відтворюваності: аналітик може спиратися на збережені технічні факти, пояснити підстави висновку та повернутися до них ретроспективно, наприклад під час аудиту або повторної перевірки схожих інцидентів. Ілюстративно підсумкові результати відпрацювання процесу показані на рис. 3.12, а приклади збереження артефактів і результатів аналізу представлено на рис. 3.13, рис. 3.14 та рис. 3.15. Такий спосіб агрегації підсилює доказову базу не кількістю перевірок, а тим, що кожна перевірка завершується документованим і

прив'язаним до кейса результатом, який можна перевірити, порівняти та інтерпретувати в єдиному робочому просторі.

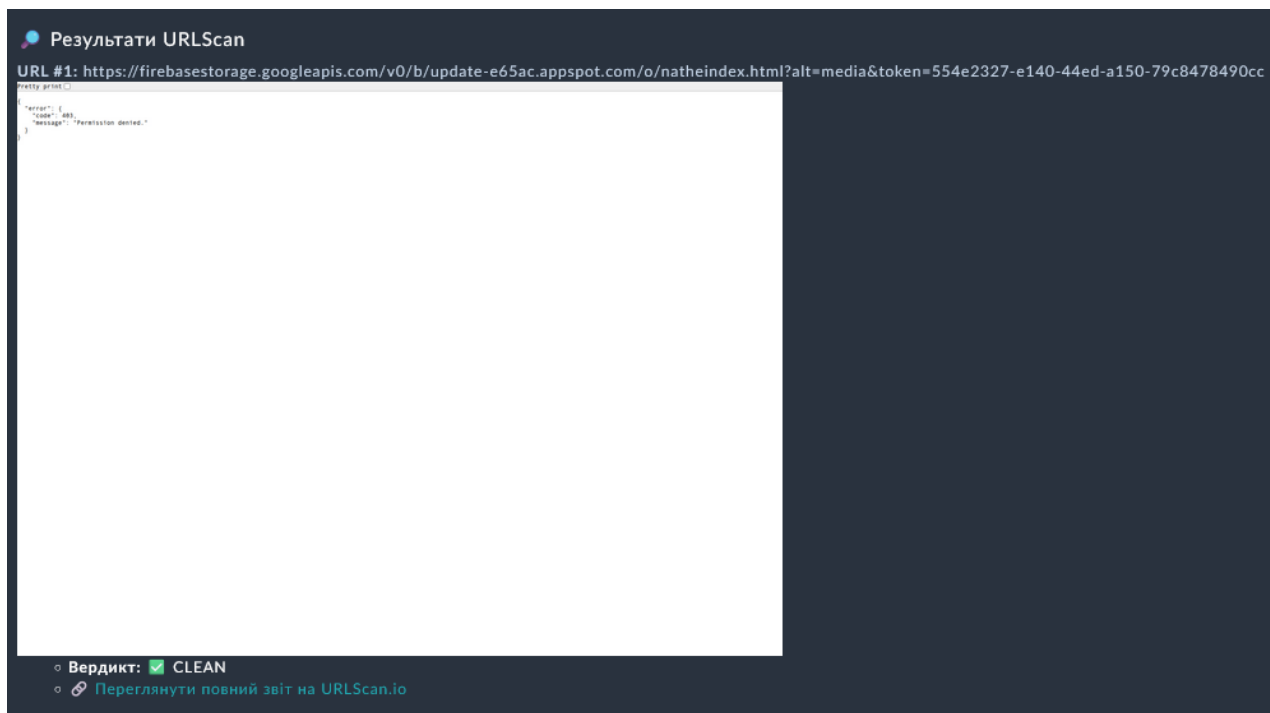


Рис. 3.12. Підсумкові результати виконання плейбука реагування на фішинг

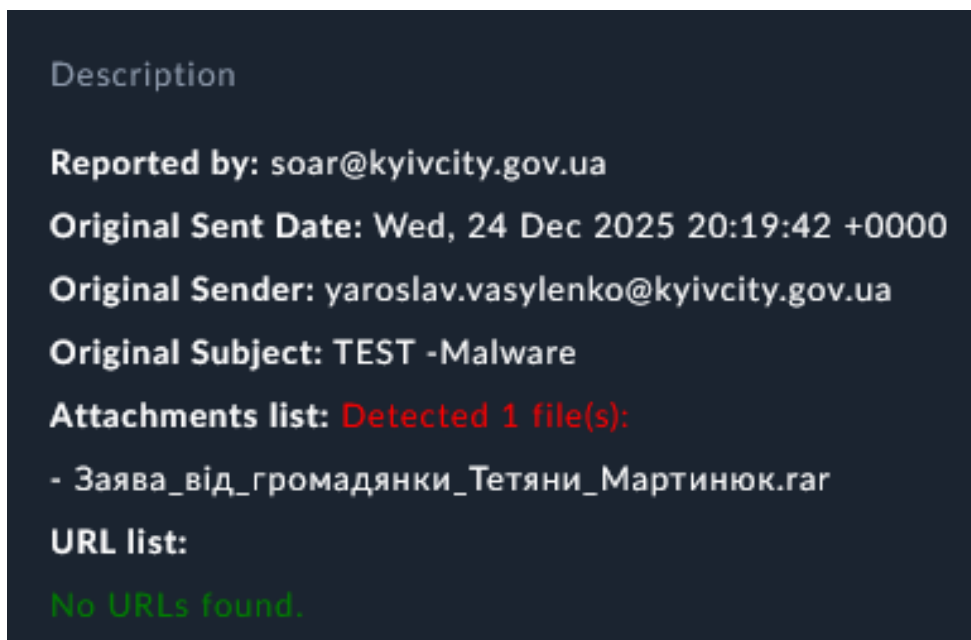


Рис. 3.13. Опис артефакту/вкладення з доданими результатами аналізу

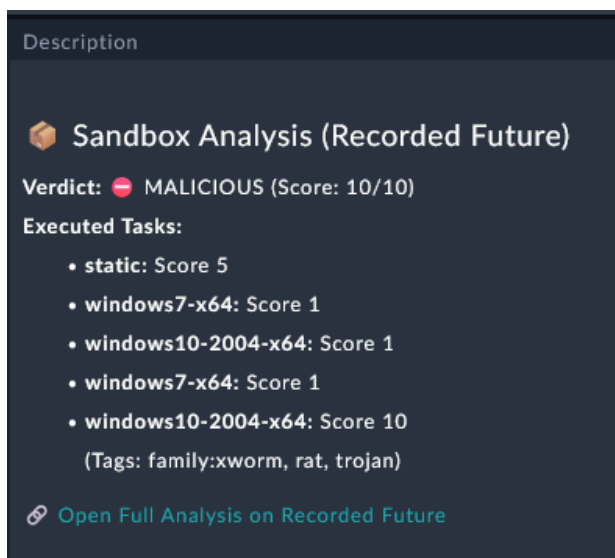


Рис. 3.14. Звіт пісочниці (sandbox report) щодо аналізу вкладки



Рис. 3.15. Результати збагачення індикатора за хеш-значенням

Комунікація з користувачем вбудована в процес як механізм зниження ризику на ранній стадії та як спосіб керування очікуваннями. Після прийняття звернення надсилається проміжна автовідповідь, що підтверджує факт отримання листа, містить попередження не відкривати підозріле повідомлення чи посилання та заклик проінформувати колег, якщо існує ризик розсилки в межах організації. Паралельно з цим матеріали передаються аналітику у вигляді сформованого алерту з прив'язаним оригіналом листа, виділеними ІоС та збагаченими результатами перевірок, що дає змогу швидко перейти від «сирого» звернення до предметного аналізу. Фінальна відповідь користувачу формується аналітиком після оцінювання доказів, оскільки саме на цьому етапі стає можливим коректно врахувати контекст

організації та дати змістовний зворотний зв'язок без ризику передчасних висновків.

Фінальний висновок у сценарії навмисно залишено за аналітиком, оскільки автоматизація, навіть за наявності багатьох інтеграцій, не усуває потреби в експертній інтерпретації. По-перше, зовнішні сервіси enrichment можуть повертати неповні або суперечливі сигнали: для одного й того самого ІоС можливі різні оцінки, а для нових або цільових атак репутаційні бази можуть взагалі не містити інформації. По-друге, автоматичне формування вердикту підвищує ризик хибнопозитивних і хибнонегативних оцінок, що в корпоративному середовищі має прямі наслідки як для безпеки, так і для доступності бізнес-процесів. По-третє, суттєвим є організаційний контекст: корпоративні домени, типові патерни комунікації, легітимні сервіси та специфіка внутрішніх процесів можуть робити «підозрілий» з точки зору зовнішнього сервісу сигнал цілком пояснюваним, або навпаки - нейтральний сигнал може набувати критичного значення в конкретній ситуації. У підсумку автоматизація в цьому сценарії виконує роль інструмента підготовки та накопичення доказів, стандартизуючи збір і верифікацію ІоС та зменшуючи ручне навантаження на ранніх етапах, тоді як відповідальність за висновок, комунікацію і закриття кейса зберігається за людиною.

Контроль виконання процесу забезпечується спостережуваністю станів виконання, фіксацією результатів кроків та збереженням проміжних даних у картці алерту. Для інтеграцій характерні типові виняткові ситуації, такі як таймаути, тимчасова недоступність сервісу або часткові результати, коли відповідь повертається не для всіх ІоС. У логіці enrichment застосовуються паузи очікування для отримання звітів зовнішніх систем, що дозволяє асинхронно завершувати перевірки без блокування основного процесу. Водночас зберігається принцип достатності: навіть якщо частина enrichment не завершилась або повернула неповні дані, кейс усе одно містить базові артефакти (оригінальний лист, заголовки, тіло, виділені URL, хеші), які дають аналітику основу для ручного аналізу та прийняття рішення. Практичний аспект моніторингу виконання, включно з відстеженням прогресу плейбука, ілюструє рис. 3.16.

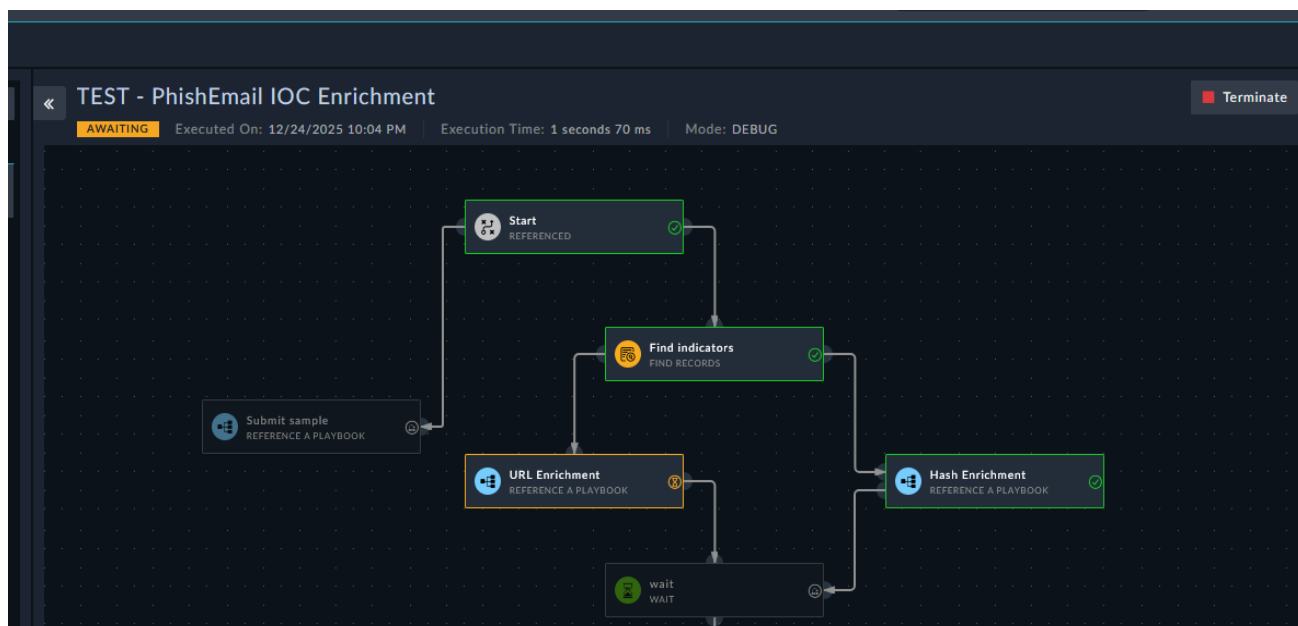


Рис. 3.16. Моніторинг статусу виконання плейбука у FortiSOAR

Завершення процесу передбачає оформлення підсумку аналітиком на основі зібраної доказової бази. Ручне закриття кейса виконує функцію контролю якості та підтвердження рішення, оскільки дозволяє переконатися, що результати enrichment інтерпретовано коректно, а контекст організації враховано. Після завершення кейса зберігаються артефакти та результати перевірок, що підтримує можливість подальших ретроспективних перевірок, повторної кореляції з новими даними та аудиту реагування у разі інцидентного розслідування.

Описана технологія застосування плейбука формує відтворюваний регламент перевірки фішингових звернень, де ключовими є стандартизований інжест, структурований збір IoC та їх верифікація через enrichment з подальшим документуванням результатів у межах кейса. Ефект від такого підходу проявляється у скороченні ручних операцій на етапах збору й збагачення, підвищенні якості первинної верифікації та уніфікації представлення доказів для аналітика. Водночас зберігається принципова межа: остаточний висновок і закриття кейса залишаються за аналітиком, що узгоджується з моделлю human-in-the-loop і відповідає природі фішингових інцидентів, де технічні сигнали потребують контекстного тлумачення.

3.2 Рекомендації щодо автоматизації процесів виявлення та реагування на інциденти безпеки корпоративної мережі

Рекомендації спрямовані на практичне впровадження автоматизації в корпоративному SOC так, щоб вона підсилювала керований життєвий цикл реагування, зменшувала частку рутинних операцій і водночас не руйнувала контрольованість рішень. Методично доцільно спиратися на поєднання логіки incident response як процесу управління кіберризиками та моделі цільових результатів CSF 2.0, оскільки це дозволяє одночасно формалізувати послідовність робіт і вимірювати, які етапи реально посилюються автоматизацією [9, 10].

Межі рекомендацій визначаються тим, що автоматизація не має перетворюватися на автономне “винесення вердиктів”. Для корпоративної мережі ефективнішим є підхід, коли платформа стандартизує приймання подій, агрегує контекст, забезпечує збирання та збереження доказів, а критичні рішення залишаються у відповідальності фахівця. Така постановка узгоджується з практикою використання SOAR як операційного ядра, яке масштабує роботу аналітика, а не замінює її [14, 21].

Додатковою підставою для фокусування на автоматизації є тенденції еволюції загроз і зростання навантаження на команди захисту, що підсилює потребу в стандартизації та зменшенні ручної праці в тріажі, збагаченні та координації реагування. Це важливо розглядати не як технологічну моду, а як організаційну відповідь на дефіцит ресурсу в SOC [3, 4, 8].

Першим принципом є “процес перед автоматизацією”: сценарії мають бути прив’язані до контрольних точок якості в життєвому циклі реагування, а не до випадкового набору інтеграцій. Практично це означає, що автоматизація проектується під підготовку, виявлення та аналіз, стримування, відновлення і післяінцидентні активності, із явним визначенням, які артефакти та рішення мають бути зафіксовані на кожному етапі. [9, 10]

Другий принцип полягає у переході від “alert-driven” до “case-driven” логіки, коли сирі події нормалізуються, корелюються, агрегуються та оформлюються як

керований кейс з мінімально достатнім контекстом. У такій моделі автоматизація працює з об'єктом, який має структуру, відповідальних і історію змін, що знижує ризик втрати контексту та підтримує відтворюваність розслідувань [14, 22].

Третій принцип - ризик-орієнтований тріаж і модульність сценаріїв. Пріоритет має визначатися поєднанням критичності активів, рівня привілеїв, повторюваності сигналів і наявності незалежних підтверджень, а модулі автоматизації мають давати змогу замінювати або доповнювати окремі кроки без руйнування всього процесу. Такий підхід зменшує залежність якості реагування від конкретного виконавця і підтримує поступове дозрівання практик SOC [9, 11].

Четвертий принцип - контроль ризикових дій через точки погодження, аудит і можливість відкату. Навіть за наявності автоматизованого збору контексту та виконання типових кроків, дії з потенційним впливом на доступність сервісів або права користувачів доцільно виносити в режим підтвердження відповідальним спеціалістом. Це підтримує практичну реальність впровадження у корпоративній мережі, де помилкова автоматична дія часто дорожча за затримку на валідацію [9, 11].

Рекомендовано починати з формалізації керованих каналів надходження подій, де кожен канал має чіткі правила ініціації, ідентифікації та мінімального набору атрибутів для тріажу. У практичному кейсі з фішинговими листами така керованість забезпечується подієвим фактом надходження повідомлення у визначену папку і додатковою умовою для запуску обробки, що зменшує шум і дозволяє відпрацьовувати сценарій у контрольованому контурі [9, 22].

Для корпоративної мережі доцільно уніфікувати структуру первинних даних і забезпечити нормалізацію перед кореляцією та збагаченням. Це знижує ризик того, що результати зовнішніх перевірок будуть незіставними між інцидентами, а також підсилює якість подальшої аналітики та звітності. На рівні процесу важливо заздалегідь визначити, які атрибути є обов'язковими для запуску плейбука, а які можуть бути порожніми без блокування кейса [10, 22].

Окремо доцільно закласти дедуплікацію і базову агрегацію на вході, щоб SOC працював з обмеженою кількістю кейсів, а не з потоком однотипних алертів.

У поєднанні з ризик-орієнтованою маршрутизацією це дозволяє стабілізувати навантаження і підтримати цільову ефективність автоматизації без вимоги одразу змінювати весь інструментальний стек [9, 14].

Кейс доцільно розглядати як центральний контекст, який пов'язує алерти, задачі, артефакти, індикатори, коментарі, вкладення та історію дій. Така “хабова” організація підтримує прозорість розслідування і дозволяє відокремити технічні факти від інтерпретації, що особливо важливо під час аудиту або повторної перевірки інцидентів. Практична реалізація цієї ідеї відображена у структурі обробки фішингового інциденту, де акцент робиться на накопиченні доказів у межах одного об'єкта (див. рис. 3.2) [9, 22].

Рекомендовано забезпечити збереження оригіналу та службових атрибутів об'єкта розслідування як елемента “ланцюжка доказів”, після чого виконувати парсинг, виділення ІоС і подальшу фіксацію результатів перевірок у формах, придатних для ретроспективного аналізу. У такому підході доказовий пакет формується не підсумковим текстом, а сукупністю структурованих елементів: індикатори отримують описи, результати збагачення додаються як контекст до індикаторів і коментарів, звіти із середовищ аналізу можуть зберігатися як вкладення [9, 11].

Для підвищення відтворюваності доцільно встановити мінімальний стандарт “повноти кейса”: збережений первинний об'єкт, виділені ІоС, контекст перевірок і зафіксовані рішення аналітика. Цей стандарт варто узгодити з очікуваними результатами Respond і Recover у CSF 2.0, щоб документування підтримувало не лише технічну роботу SOC, а й управлінську придатність матеріалів інциденту [10, 11].

Плейбуки доцільно проєктувати як послідовність етапів, що відповідають логіці NIST: приймання події, первинний аналіз, формування доказів, підготовка варіантів реагування і контрольоване завершення. У практичному сценарії фішингових листів це виражається у розділенні первинної обробки та розширеної обробки, що дозволяє швидко отримати базовий контекст і, за потреби, поглибити перевірки (див. рис. 3.5 та рис. 3.6) [9, 22].

Для корпоративної мережі важливо визначати межі автоматизації через тип рішень. Дії, що впливають на доступність або права, варто виконувати лише за наперед узгодженими умовами або через механізми підтвердження, тоді як збір артефактів, нормалізація даних, заповнення картки кейса та підготовка підсумків можуть бути максимально автоматизованими. Така схема підтримує оптимальність, оскільки мінімізує ручні операції там, де ризик помилки людини високий, і зберігає ручний контроль там, де помилка автоматизації є критичною [9, 11].

Рекомендовано закладати в плейбуки обробку винятків як нормальний режим, а не як аварійну ситуацію: таймаути інтеграцій, часткові результати, тимчасова недоступність сервісів мають приводити до збереження мінімально достатньої доказової бази, а не до втрати кейса. Практично це означає, що навіть за неповного збагачення інцидент має містити базові артефакти для ручного аналізу і прийняття рішення. [9, 22].

Enrichment доцільно трактувати як етап верифікації індикаторів і накопичення технічних свідчень, а не як автоматичне встановлення “діагнозу”. У кейсі фішингових листів перевірки URL і хешів виконуються через набір зовнішніх сервісів і оформлюються так, щоб аналітик міг інтерпретувати зібраний контекст у політиках організації, а не підміняти рішення “репутаційною оцінкою” одного джерела (див. рис. 3.7-3.11) [9, 22].

Під час підбору джерел enrichment рекомендовано застосовувати критерії надійності, повноти, швидкості й відтворюваності результатів, а також використовувати узгоджений підхід до перевірки типових об’єктів, зокрема URL, хешів та вкладень. Для підвищення якості тріажу доречним є багатоджерельне підтвердження, оскільки воно знижує ризик хибних висновків у разі неповноти або упередженості окремих баз [3, 9].

Важливо заздалегідь визначити політику обробки неповних відповідей: таймаути, часткове збагачення та асинхронне завершення окремих перевірок мають бути передбачені процедурно, щоб основний процес не блокувався і не втрачав керованості. Для корпоративного застосування корисним є принцип

достатності, коли рішення може бути прийняте на основі мінімального набору артефактів, а enrichment підсилює доказовість і зменшує час на ручні перевірки, не будучи єдиною підставою [9, 14].

Документування результатів enrichment має бути спрямоване на формування доказової бази: результати варто зберігати у прив'язці до індикаторів і кейса так, щоб їх можна було перевірити ретроспективно. Такий підхід підтримує післяінцидентні активності, повторну кореляцію з новими даними та аудит дій SOC, що узгоджується з практиками накопичення знань і lessons learned [10, 11].

Комунікаційний контур доцільно будувати як частину інцидентного процесу, а не як паралельний обмін повідомленнями поза кейсом. Для типових звернень корисно впроваджувати стандартні шаблони повідомлень, зокрема підтвердження прийому і короткі інструкції безпечної поведінки до завершення перевірки, що знижує невизначеність і ризик неконтрольованих дій користувача [9, 22].

Ефективною є модель двоетапного зворотного зв'язку: проміжна відповідь формується автоматично одразу після ініціації кейса, а підсумкова надається відповідальним фахівцем після інтерпретації доказової бази. Така схема одночасно зменшує навантаження на SOC від повторних звернень і зберігає якість висновку, оскільки фінальне рішення залишається керованим і контекстним [9, 11].

У корпоративній мережі важливо запобігати паніці та помилковим діям користувачів через чіткі короткі інструкції, пов'язані з інцидентом: що не робити, які артефакти надати, як діяти з підозрілим вкладенням або посиланням. Це також підтримує збір доказів, оскільки дисциплінує передачу вихідних даних у форматі, придатному для подальшої перевірки [9, 10].

Контроль виконання плейбуків має включати журналювання, статуси кроків і явне відображення виняткових ситуацій, щоб аналітик бачив реальний прогрес, точки зупинки та причини часткових результатів. Практична доцільність такого підходу проявляється тоді, коли збагачення організовано асинхронно і потребує очікування результатів, а інцидент при цьому залишається керованим і не “зависає” у невизначеному стані (див. рис. 3.16) [9, 22]

Показники ефективності автоматизації рекомендовано формувати без прив'язки до наперед заданих чисел і без спокуси “оптимізувати статистику”. Для корпоративної мережі показовими є скорочення ручних операцій у тріажі, стабільність збору артефактів, час первинної перевірки, частка кейсів із повним мінімальним пакетом доказів і частка сценаріїв, що завершуються без помилок інтеграцій. Усі ці метрики мають бути пов'язані з цільовими результатами процесу, а не з кількістю виконаних дій [9, 10].

Зворотний зв'язок для покращення плейбуків доцільно будувати на основі даних, що вже накопичуються в кейсах: які поля найчастіше лишаються порожніми, де виникають таймаути, які інтеграції дають часткові відповіді, на яких етапах аналітик змушений повторювати ручні перевірки. Такий цикл підтримує поступове зниження частки рутинної праці та підвищує відтворюваність реагування [10, 11].

Експлуатаційна стійкість автоматизації вимагає керування змінами плейбуків та інтеграцій через версійність, тестування перед внесенням змін і контроль залежностей. Для корпоративної мережі практично значущими є розділення тестового і робочого контурів, регламент оновлень, а також перевірка того, як зміна конектора або структури даних вплине на існуючі сценарії й доказову базу [19, 22].

Управління доступами і секретами має бути організоване через розмежування ролей і мінімально необхідні права, оскільки автоматизація фактично стає виконавчим механізмом дій у різних системах. Доцільно забезпечити, щоб права на модифікацію плейбуків, налаштування інтеграцій і запуск високоризикових дій були відокремлені, а всі зміни підлягали аудиту та могли бути відтворені під час перевірки інцидентів [9, 22].

Окремої уваги потребує аудит і відповідальність: має бути визначено, хто має право змінювати сценарії та конектори, як фіксуються підстави змін, і як перевіряється коректність після оновлення. Для практичної реальності важливо мати простий механізм контрольованого повернення до стабільного стану у разі

регресії, з акцентом на збереження працездатності ключових ланцюжків приймання та документування інцидентів [10, 22, 24].

Запропоновані рекомендації поєднують методичний каркас реагування та практичні вимоги корпоративної експлуатації: автоматизація прив'язується до контрольних точок процесу, переходить до кейс-орієнтованої моделі, формує доказову базу та підтримує відтворюваність рішень. Це забезпечує оптимальність через зменшення рутинних операцій, цільову ефективність через фокус на якості тріажу, верифікації та контрольованому завершенні кейсів, а також практичну реальність через точки погодження, аудит, обробку винятків і керування змінами [9, 10].

Отже, у розділі 3 розкрито технологію автоматизації перевірки підозрілих фішингових листів у FortiSOAR за сценарієм ініціації користувачем, де метою є прискорення первинного тріажу та підготовка доказової бази для подальшого аналізу SOC. Описано керований ланцюжок обробки від інжесту листа й парсингу до виділення IoC, нормалізації артефактів і збагачення індикаторів через зовнішні сервіси з фіксацією результатів у межах інцидентного об'єкта. Показано, що ключовим результатом є формування структурованого «пакета доказів» із прив'язкою оригіналу листа, URL і хешів, а також звітів перевірок і sandbox-аналізу, придатних для аудиту та повторної верифікації. Обґрунтовано принцип human-in-the-loop, за якого платформа не виносить остаточний вердикт і не виконує блокувань, а залишає фінальне рішення та закриття кейса за аналітиком. Наведено підхід до комунікації з користувачем через проміжну автовідповідь і організацію контролю виконання плейбуків із врахуванням типових винятків інтеграцій. Сформульовано практичні рекомендації щодо впровадження автоматизації в SOC, з акцентом на процесну прив'язку сценаріїв, кейс-орієнтовану модель, керування ризиковими діями та відтворюваність реагування.

ВИСНОВОК

Проведено оцінку стану автоматизації виявлення та реагування на інциденти в корпоративних мережах в Україні за умов зростання загроз. Встановлено, що ручні процедури тріажу й координації уповільнюють реакцію та погіршують керованість процесу під час інцидентів.

Досліджено сутність проблеми автоматизації як потребу у відтворюваних діях у SOC, єдиному контексті та прозорому контролі рішень. Визначено ключові вузькі місця, пов'язані зі збагаченням подій, пріоритизацією та передачею задач між ролями чергової зміни. Узагальнено вимоги до фіксації артефактів і доказів для подальшого аналізу, а також до журналювання змін у кейсах.

Проаналізовано підходи до автоматизації на основі процесного керування інцидентами та стандартизації етапів реагування в корпоративній мережі. Описано застосування оркестрації, плейбуків і контрольних точок погодження для зменшення помилок, ризиків та повторюваності ручних дій. Показано доцільність використання процесних метрик, зокрема MTTA та MTTR, для оцінювання результативності й своєчасності реагування.

Проаналізовано існуючі рішення класу SOAR для автоматизації реагування в корпоративному SOC та їх функціональні можливості в експлуатації. Розглянуто Cortex XSOAR, Splunk SOAR і FortiSOAR за критеріями інтеграцій, керування кейсами, підтримки плейбуків та масштабування автоматизації. Обґрунтовано вибір FortiSOAR як платформи з розвиненою оркестрацією і фокусом на керованості інцидентів та аудиті дій.

Розкрито методи та засоби автоматизації на базі FortiSOAR через конектори, інтеграції та оброблення алертів у єдиному просторі кейса. Охарактеризовано механізми плейбуків, задач, War Room, RBAC і аудит як основу контрольованого виконання дій та взаємодії команди. Висвітлено використання збагачення даних, Threat Intel та взаємодії із SIEM, EDR, поштовими системами й sandbox.

Запропоновано порядок застосування FortiSOAR від приймання сигналів до закриття інциденту з фіксацією рішень, дій та артефактів у кейсі. Описано прикладний сценарій реагування на фішингові повідомлення зі збором ІоС, збагаченням, класифікацією та ініціюванням стримування. Сформовано рекомендації щодо керування плейбуками, розподілу ролей, тестування змін, контролю доступів та моніторингу показників SOC.

ПЕРЕЛІК ПОСИЛАНЬ

1. Top 10 Emerging Cyber Threats and How to Prepare for Them. BCS365 : веб-сайт. URL: <https://bcs365.com/insights/top-10-emerging-cyber-threats-and-how-to-prepare-for-them> (дата звернення: 02.10.2025).
2. X-Force Threat Intelligence Index 2025. IBM Research : веб-сайт. URL: <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index> (дата звернення: 03.10.2025).
3. Технологічні тренди в кібербезпеці 2023. Інститут проблем реєстрації інформації НАН України. URL: <https://ippi.org.ua/sites/default/files/2023-11.pdf> (дата звернення: 04.10.2025).
4. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61r3. National Institute of Standards and Technology. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf> (дата звернення: 12.10.2025).
5. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. National Institute of Standards and Technology. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> (дата звернення: 11.10.2025).
6. Microsoft Cloud Security Benchmark. Microsoft Learn : веб-сайт. URL: <https://learn.microsoft.com/en-us/security/benchmark/azure/introduction> (дата звернення: 05.10.2025).
7. SOAR Statistics 2025: Trends, Growth & Market Share. Expert Insights : веб-сайт. URL: <https://expertinsights.com/network-security/soar-statistics-2025> (дата звернення: 14.10.2025).
8. Security Orchestration Automation and Response (SOAR) Market Size & Share Analysis. Mordor Intelligence : веб-сайт. URL: <https://www.mordorintelligence.com/industry-reports/security-orchestration->

[automation-and-response-market](#) (дата звернення: 15.10.2025).

9. Gartner Says Goodbye to SOAR: What's Next for Security Operations?. Blink Ops : веб-сайт. URL: <https://www.blinkops.com/blog/gartner-says-goodbye-to-soar> (дата звернення: 16.10.2025).

10. How SOAR Works: Pros, Cons, and Choosing the Right Platform. Exabeam : веб-сайт. URL: <https://www.exabeam.com/explainers/soar/how-soar-works-pros-cons-and-choosing-the-right-platform> (дата звернення: 17.10.2025).

11. About Data Quadrants. SoftwareReviews : веб-сайт. URL: <https://www.softwarereviews.com/about-data-quadrants> (дата звернення: 18.10.2025).

12. Cortex XSOAR Customer Reviews 2025 (SOAR category). SoftwareReviews : веб-сайт. URL: https://www.softwarereviews.com/products/cortex-xsoar?c_id=218 (дата звернення: 19.10.2025).

13. FortiSOAR Vs Splunk SOAR Vs Cortex XSOAR | SPARK Plus by QKS Group. QKS Group : веб-сайт. URL: <https://qksgroup.com/sparkplus/compare-products?market-id=243&pid1=988&pid2=5197&pid3=994> (дата звернення: 20.10.2025).

14. Splunk SOAR Customer Reviews 2025 (SOAR category). SoftwareReviews : веб-сайт. URL: https://www.softwarereviews.com/products/splunk-soar?c_id=218 (дата звернення: 21.10.2025).

15. Splunk SOAR: Modernize and Automate your SOC. Splunk : веб-сайт. URL: https://www.splunk.com/en_us/products/soar.html (дата звернення: 22.10.2025).

16. FortiSOAR. Fortinet : веб-сайт. URL: <https://www.fortinet.com/products/fortisoar> (дата звернення: 27.10.2025).

17. FortiSOAR 7.6 Documentation (Installation and Deployment Guides). Fortinet. URL: <https://docs.fortinet.com/product/fortisoar/7.6> (дата звернення: 30.10.2025).

18. Security Orchestration, Automation and Response Solutions. Gartner Peer Insights : веб-сайт. URL: <https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions> (дата звернення: 24.10.2025).

19. FortiSOAR Customer Reviews 2025 (SOAR category). SoftwareReviews : веб-сайт. URL: https://www.softwarereviews.com/products/fortisoar?c_id=218 (дата

звернення: 25.10.2025).

20. What Is SOAR (Security Orchestration, Automation and Response)? (Cyberpedia). Palo Alto Networks : веб-сайт. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-soar> (дата звернення: 10.10.2025).

21. FortiSOAR™: Security Orchestration, Automation and Response : Datasheet. Acora & Fortinet. 2022. URL: <https://static.acora.com/app/uploads/2023/11/acora-fortinet-fortisoar-datasheet-2022.pdf> (дата звернення: 26.10.2025).

22. FortiSOAR 7.0.1 User Guide. Fortinet. URL: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a2452001-dbf1f-11eb-97f7-00505692583a/FortiSOAR-7.0.1-User_Guide.pdf (дата звернення: 01.11.2025).

23. FortiSOAR: Security Orchestration, Automation and Response : Datasheet. Fortinet. URL: https://www.boll.ch/at_fr/datasheets/FortiSOAR.pdf (дата звернення: 23.10.2025).

24. FortiSOAR Content Hub: Connectors. Fortinet : веб-сайт. URL: <https://fortisoar.contenthub.fortinet.com/list.html?contentType=connector> (дата звернення: 03.11.2025).

25. FortiSIEM and FortiSOAR Offer Essential SOC Capabilities : Solution Guide. Fortinet. URL: <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortisiem-fortisoar.pdf> (дата звернення: 15.11.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)