ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «SOC-конвеєр моніторингу та тріажу інцидентів із застосуванням SIEM та endpoint-телеметрії»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

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

_____	*Андрій КОЖУШКО*
(підпис)	*Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Андрій КОЖУШКО
Ім'я, ПРІЗВИЩЕ
Керівник: Кирило СОКОЛОВ, PhD
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2026р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кожушко Андрій Олександрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: SOC-конвеєр моніторингу та тріажу інцидентів із застосуванням SIEM та endpoint-телеметрії
керівник кваліфікаційної роботи Кирило СОКОЛОВ, PhD,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» лютого 2026р. № 51
2. Строк подання кваліфікаційної роботи «5» червня 2026р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література; документація NIST, Microsoft, Splunk, Velociraptor та MITRE ATT&CK; лабораторна мережа 192.168.100.0/24; домен corp.kozhushko.internal; вузли DC01, WS01, WS02, SPLUNK01, Ubuntu-IR, KALI01; Windows Server 2022, Windows 11, Ubuntu, Kali Linux; Splunk Enterprise, Splunk Universal Forwarder, Sysmon, Velociraptor; події Windows Security та Sysmon.
Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні основи побудови SOC-конвеєра моніторингу та тріажу інцидентів.
2. Проєктування та розгортання лабораторного стенда SOC-конвеєра.
3. Експериментальне дослідження сценаріїв виявлення та тріажу інцидентів у розробленому SOC-конвеєрі.
4. Перелік ілюстративного матеріалу: презентація; структурно-мережеві схеми; скріншоти Active Directory, Splunk, Sysmon, Splunk Universal Forwarder, Kali Linux та Velociraptor.
4. Дата видачі завдання «24»' лютого 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	01.03–10.03.2026	Виконано
2	Формування плану роботи та теоретичної частини	11.03–25.03.2026	Виконано
3	Проєктування архітектури лабораторного SOC-стенда	26.03–01.04.2026	Виконано
4	Розгортання доменної інфраструктури, Splunk, Sysmon та Velociraptor	02.04–09.04.2026	Виконано
5	Моделювання контрольованих атак та збір експериментальних даних	11.04–15.04.2026	Виконано
6	Аналіз результатів експериментів і формування висновків	16.04–17.04.2026	Виконано
7	Оформлення пояснювальної записки	19.04–20.04.2026	Виконано
8	Розробка презентації	01.05–03.05.2026	Виконано
9	Передзахист	04.05-07.05.2026	Виконано
10	Здача в деканат	08.05.2026	Виконано

Здобувач вищої освіти _____ Андрій КОЖУШКО

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Кирило СОКОЛОВ, PhD

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 69 стор., 30 рис., 15 табл., 30 джерел, 4 додатки.

Мета роботи – розробити та експериментально перевірити лабораторний SOC-конвеєр моніторингу та triage інцидентів із застосуванням SIEM та endpoint-телеметрії.

Об'єкт дослідження – процес моніторингу, виявлення та первинного triage подій безпеки в корпоративній інфраструктурі.

Предмет дослідження – методи та засоби побудови лабораторного SOC-конвеєра на основі Splunk Enterprise, Windows Event Logs, Sysmon, Splunk Universal Forwarder, Velociraptor та контрольованої атакувальної активності з KALI01.

Короткий зміст роботи: у кваліфікаційній роботі розглянуто теоретичні та практичні аспекти побудови SOC-конвеєра моніторингу та triage інцидентів. У теоретичній частині проаналізовано функції SOC, роль SIEM у централізованому зборі подій, значення endpoint-телеметрії, Windows Security Events, Sysmon і IR-платформ. У практичній частині спроєктовано та розгорнуто лабораторний стенд з доменною інфраструктурою, робочими станціями, SIEM-вузлом Splunk, IR-вузлом Velociraptor та тестовим вузлом KALI01. Експериментальна частина містить сценарії мережевого сканування, невдалих SMB-автентифікацій і аналізу події ANONYMOUS LOGON. На основі отриманих результатів оцінено можливості та обмеження розробленого SOC-конвеєра.

КЛЮЧОВІ СЛОВА: SOC, SIEM, ENDPOINT-ТЕЛЕМЕТРІЯ, SPLUNK, SYSMON, WINDOWS EVENT LOGS, VELOCIRAPTOR, INCIDENT RESPONSE, TRIAGE, KALI LINUX, SMB, ANONYMOUS LOGON, WINDOWS SECURITY EVENTS.

ABSTRACT

The text part of the qualification work for obtaining a bachelor's degree: 69 pages, 30 figures, 15 tables, 30 sources, 4 appendices.

The purpose of the work is to develop and experimentally verify a laboratory SOC pipeline for monitoring and incident triage using SIEM and endpoint telemetry.

The object of the research is the process of monitoring, detecting, and performing primary triage of security events in a corporate infrastructure.

The subject of the research is the methods and tools for building a laboratory SOC pipeline based on Splunk Enterprise, Windows Event Logs, Sysmon, Splunk Universal Forwarder, Velociraptor, and controlled attack activity from KALI01.

Summary of the work: the qualification work examines the theoretical and practical aspects of building a SOC pipeline for monitoring and incident triage. The theoretical part analyzes SOC functions, the role of SIEM in centralized event collection, the importance of endpoint telemetry, Windows Security Events, Sysmon, and IR platforms. In the practical part, a laboratory stand with domain infrastructure, workstations, the Splunk SIEM node, the Velociraptor IR node, and the KALI01 test node was designed and deployed. The experimental part includes scenarios of network scanning, failed SMB authentications, and analysis of the ANONYMOUS LOGON event. Based on the obtained results, the capabilities and limitations of the developed SOC pipeline were evaluated.

KEY WORDS: SOC, SIEM, ENDPOINT TELEMETRY, SPLUNK, SYSMON, WINDOWS EVENT LOGS, VELOCIRAPTOR, INCIDENT RESPONSE, TRIAGE, KALI LINUX, SMB, ANONYMOUS LOGON, WINDOWS SECURITY EVENTS.

ЗМІСТ

ВСТУП 9
1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ SOC-КОНВЕЄРА МОНІТОРИНГУ ТА ТРІАЖУ ІНЦИДЕНТІВ 11
1.1 Поняття та функції SOC у сучасній корпоративній інфраструктурі 11
1.2 SIEM як основа централізованого збору та аналізу подій безпеки 13
1.3 Endpoint-телеметрія як джерело даних для виявлення інцидентів 15
1.4 Тріаж інцидентів у процесі моніторингу безпеки 18
1.5 Роль Windows Security Events і Sysmon у побудові сценаріїв виявлення 20
1.6 IR-платформи у SOC-конвеєрі та місце Velociraptor 22
Висновки до розділу 1 24
2. ПРОЄКТУВАННЯ ТА РОЗГОРТАННЯ ЛАБОРАТОРНОГО СТЕНДА SOC-КОНВЕЄРА 26
2.1 Архітектура лабораторного стенда 26
2.2 Мережева схема та взаємодія вузлів 28
2.3 Розгортання доменної інфраструктури 29
2.4 Розгортання та налаштування Splunk Enterprise 32
2.5 Налаштування Splunk Universal Forwarder на Windows-вузлах 34
2.6 Налаштування збору endpoint-телеметрії 36
2.7 Розгортання IR-вузла на базі Velociraptor 38
Висновки до розділу 2 40
3. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СЦЕНАРІЇВ ВИЯВЛЕННЯ ТА ТРІАЖУ ІНЦИДЕНТІВ У РОЗРОБЛЕНОМУ SOC-КОНВЕЄРІ 41
3.1 Мета та логіка експериментальної перевірки 41
3.2 Перевірка повноти телеметрії перед сценаріями атак 42
3.3 Сценарій 1: виявлення мережевого сканування з KALI01 44
3.4 Сценарій 2: виявлення невдалих SMB-автентифікацій з KALI01 46
3.5 Сценарій 3: аналіз ANONYMOUS LOGON як неоднозначної події 4624 48
3.6 Додаткова endpoint-телеметрія: процеси, DNS, реєстр і файли 51
3.7 Побудова detection-to-triage ланцюга 55
3.8 Оцінювання результатів і обмежень експерименту 57

Висновки до розділу 3 59
ВИСНОВКИ 60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 63
Додаток А 66
Додаток Б 67
Додаток В 68
Додаток Г 69

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SOC – Security Operations Center, центр моніторингу та реагування на події безпеки

SIEM – Security Information and Event Management, система централізованого збору та аналізу подій безпеки

IR – Incident Response, реагування на інциденти

DFIR – Digital Forensics and Incident Response, цифрова криміналістика та реагування на інциденти

EDR – Endpoint Detection and Response, виявлення та реагування на кінцевих точках

UF – Splunk Universal Forwarder

AD – Active Directory

DC – Domain Controller, контролер домену

DNS – Domain Name System

SMB – Server Message Block

NTLM – NT LAN Manager

WFP – Windows Filtering Platform

Sysmon – System Monitor, компонент Microsoft Sysinternals для розширеного журналювання подій Windows

Event ID – ідентифікатор події в журналі Windows або Sysmon

GUI – Graphical User Interface, графічний інтерфейс користувача

API – Application Programming Interface

ОС – операційна система

ПЗ – програмне забезпечення

IP – Internet Protocol

TCP – Transmission Control Protocol

VM – Virtual Machine, віртуальна машина

ВСТУП

У сучасних корпоративних інформаційних системах безпека вже не може спиратися лише на окремі засоби захисту або ручний перегляд журналів. Робочі станції, сервери, доменні служби, мережеві підключення та прикладні сервіси щодня формують велику кількість подій. Частина з них є штатною технічною активністю, однак серед них можуть бути ознаки сканування, невдалих спроб автентифікації, підозрілого запуску процесів або змін на кінцевих точках. Через це для організації важливо мати не тільки засоби захисту, а й зрозумілий процес централізованого моніторингу, аналізу та первинного triage інцидентів.

Актуальність теми кваліфікаційної роботи зумовлена тим, що SOC-підхід дозволяє поєднати різні джерела телеметрії в єдиний процес: збір подій, їх централізований аналіз у SIEM, виявлення підозрілої активності та уточнення стану конкретного endpoint-вузла. У межах цієї роботи такий підхід досліджується на прикладі лабораторного стенда, де Splunk Enterprise використовується як SIEM-рівень, Windows Event Logs і Sysmon виступають джерелами endpoint-телеметрії, а Velociraptor застосовується для первинного triage робочих станцій.

Мета роботи – розробити та експериментально перевірити лабораторний SOC-конвеєр моніторингу та triage інцидентів із застосуванням SIEM та endpoint-телеметрії.

Для досягнення поставленої мети необхідно розв’язати такі завдання: проаналізувати теоретичні основи побудови SOC-конвеєра; визначити роль SIEM і endpoint-телеметрії в процесі виявлення інцидентів; спроєктувати лабораторну інфраструктуру з доменом, робочими станціями, SIEM-вузлом, IR-вузлом і атакувальним тестовим вузлом; налаштувати збирання Windows Event Logs і Sysmon через Splunk Universal Forwarder; розгорнути Velociraptor для endpoint-triage; змоделювати контрольовані сценарії атакувальної активності з KALI01; проаналізувати отримані події у Splunk; оцінити практичну придатність і обмеження побудованого стенда.

Об’єктом дослідження є процес моніторингу, виявлення та первинного triage подій безпеки в корпоративній інфраструктурі.

Предметом дослідження є методи та засоби побудови лабораторного SOC-конвеєра з використанням Splunk Enterprise, Windows Event Logs, Sysmon, Splunk Universal Forwarder, Velociraptor і контрольованої активності з KALI01.

Практичне значення роботи полягає в тому, що розроблений стенд може використовуватися як навчальне середовище для демонстрації базових етапів роботи SOC: централізованого збору подій, виявлення ознак мережевого сканування та невдалих спроб автентифікації, аналізу неоднозначних подій на зразок ANONYMOUS LOGON і переходу від SIEM-події до endpoint-triage у Velociraptor.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. У першому розділі розглянуто теоретичні основи SOC, SIEM, endpoint-телеметрії та triage. У другому розділі описано проєктування й розгортання лабораторного стенда. У третьому розділі наведено експериментальну перевірку сценаріїв виявлення та triage інцидентів у побудованому SOC-конвеєрі.

1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ SOC-КОНВЕЄРА МОНІТОРИНГУ ТА ТРІАЖУ ІНЦИДЕНТІВ

1.1 Поняття та функції SOC у сучасній корпоративній інфраструктурі

У сучасній корпоративній інфраструктурі кількість подій безпеки, журналів, системних повідомлень і технічних сповіщень настільки велика, що їхній ручний перегляд перестає бути реалістичним. Саме тому в практиці захисту інформації формується окрема функція безперервного спостереження за станом середовища, виявлення відхилень і первинного реагування на інциденти. У документах NIST така діяльність розглядається як складова безперервного моніторингу та процесів incident response, а в організаційному вимірі найчастіше реалізується через Security Operations Center, або SOC [1, 3].

Під SOC доцільно розуміти не окреме приміщення і не конкретний програмний продукт, а поєднання процесів, ролей, інструментів і джерел даних, що забезпечують систематичний контроль подій безпеки. Такий підхід важливий для коректного розуміння теми дипломної роботи: навіть якщо у стенді використовується обмежена кількість машин і програмних компонентів, логіка SOC зберігається, якщо є централізований збір телеметрії, її аналіз, пріоритизація і подальший triage [1–3].

З практичного погляду SOC виконує кілька взаємопов’язаних функцій. По-перше, він забезпечує постійне отримання та консолідацію подій із різних джерел: операційних систем, засобів мережевого контролю, серверів, робочих станцій, хмарних сервісів та спеціалізованих засобів захисту. По-друге, він дозволяє відокремлювати звичайну технічну активність від подій, які можуть свідчити про помилку конфігурації, порушення політик або реальний інцидент. По-третє, SOC створює основу для маршрутизації інцидентів: від первинного виявлення до triage, ескалації та подальшого реагування [1–3].

Для корпоративного середовища особливе значення має те, що SOC працює не з окремими подіями у відриві одна від одної, а з контекстом. Одна й та сама дія

може мати різне значення залежно від вузла, облікового запису, часу доби, типу процесу або пов’язаних журналів. Через це ефективність SOC визначається не тільки кількістю зібраних подій, а й тим, наскільки швидко та послідовно вони можуть бути інтерпретовані в межах єдиного процесу моніторингу [1 - 3].

У сучасних роботах українських авторів, присвячених SIEM та побудові ситуаційних центрів з кібербезпеки, також підкреслюється, що ядром такого центру є не окремий інструмент, а зв’язок між джерелами телеметрії, механізмами аналізу та процедурою прийняття рішень. Це добре узгоджується з практикою побудови навчального стенда: навіть спрощена лабораторна інфраструктура може відтворювати реальний SOC-конвеєр, якщо в ній є джерела подій, засіб централізованого збору та інструмент первинного triage [29, 30].

У межах цієї роботи SOC розглядається як логічний конвеєр, у якому інформація проходить кілька послідовних етапів: збір подій, централізація, первинний аналіз, уточнення пріоритету, triage кінцевої точки та прийняття рішення про подальші дії. Така інтерпретація є зручною для дипломного дослідження, оскільки дозволяє не абстрактно описувати функції центру безпеки, а прив’язати їх до конкретних компонентів лабораторного стенда, які розглядатимуться в наступних розділах [1–3].

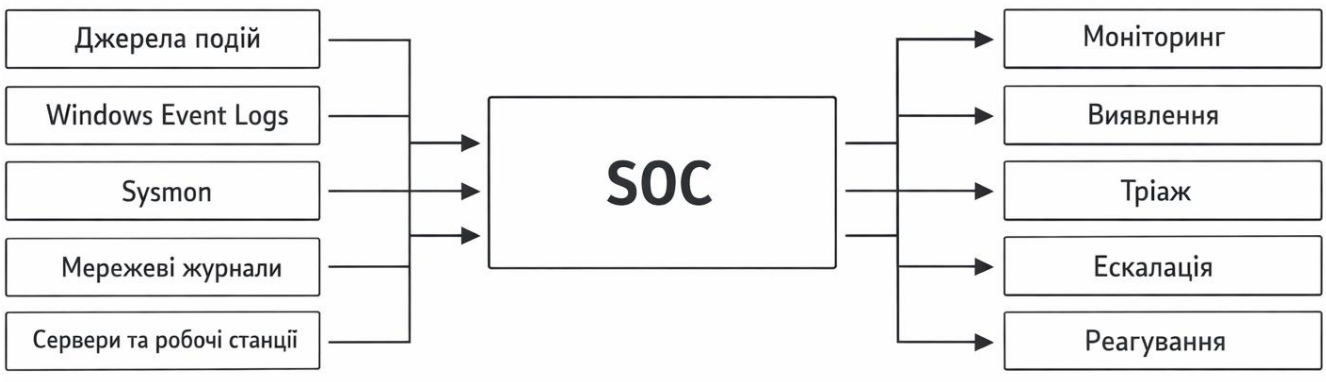


Рисунок 1.1 — Узагальнена схема функцій SOC у сучасній корпоративній інфраструктурі

Для деталізації основних функцій SOC у контексті моніторингу подій безпеки доцільно подати їх у табличному вигляді.

Таблиця 1.1 — Основні функції SOC у контексті моніторингу подій безпеки

Функція	**Зміст**	**Практичне значення**
Збір подій	Отримання журналів і телеметрії з різних джерел	Формує базу даних для подальшого аналізу
Централізація	Об’єднання подій в одному аналітичному середовищі	Дає цілісне уявлення про стан інфраструктури
Виявлення	Пошук аномалій, підозрілих дій і відхилень	Дозволяє швидко помітити потенційний інцидент
Тріаж	Первинна оцінка важливості та контексту події	Зменшує кількість хибних ескалацій
Ескалація	Передавання інциденту на наступний рівень обробки	Дозволяє розподіляти навантаження між ролями
Реагування	Дії після підтвердження інциденту	Спрямоване на локалізацію та усунення наслідків

1.2 SIEM як основа централізованого збору та аналізу подій безпеки

Практична реалізація функцій SOC майже завжди спирається на платформу, яка приймає події з різних джерел, зберігає їх у централізованому вигляді та надає аналітику засоби пошуку, фільтрації та кореляції. У такій ролі виступає SIEM – Security Information and Event Management. У документах NIST з лог-менеджменту акцент зроблено на тому, що ефективне ведення журналів є не лише технічною вимогою, а й умовою подальшого аналізу, розслідування та реагування на інциденти [2].

Важливо, що SIEM не створює події самостійно. Його роль полягає в тому, щоб прийняти інформацію від джерел, перетворити її на придатний для аналізу масив даних і зробити доступною для аналітика. Це означає, що якість роботи SIEM напряму залежить від того, які журнали надходять, наскільки правильно їх зібрано та наскільки послідовно організовано їхню доставку. Саме через це питання SIEM у дипломній роботі тісно пов’язане не лише з аналітикою, а й з архітектурою стенда, зокрема з forwarder-компонентами та конфігурацією джерел даних [2, 17–19].

Сильна сторона SIEM полягає в централізації. Без такого рівня зведення кожен вузол залишався б окремою точкою перегляду, а аналіз подій перетворювався б на послідовний ручний обхід серверів і робочих станцій. Централізована модель дає змогу бачити події від різних хостів в одному середовищі, виконувати однакові запити до всіх вузлів і порівнювати їхню активність за часом, джерелом або типом журналу [2, 17].

У практиці SOC це особливо важливо тоді, коли одна підозріла дія залишає сліди в кількох місцях. Наприклад, логон користувача може бути зафіксований у журналі безпеки, запуск процесу – в Security або Sysmon, а подальший DNS-запит – в endpoint-телеметрії. Без централізованого середовища такі дані важко співвіднести між собою. SIEM дозволяє виконувати саме цю задачу: не просто зберігати записи, а працювати з ними як з узгодженим потоком подій [2–5, 17]. Роль SIEM у такому централізованому зборі та аналізі подій показано на рисунку 1.2.

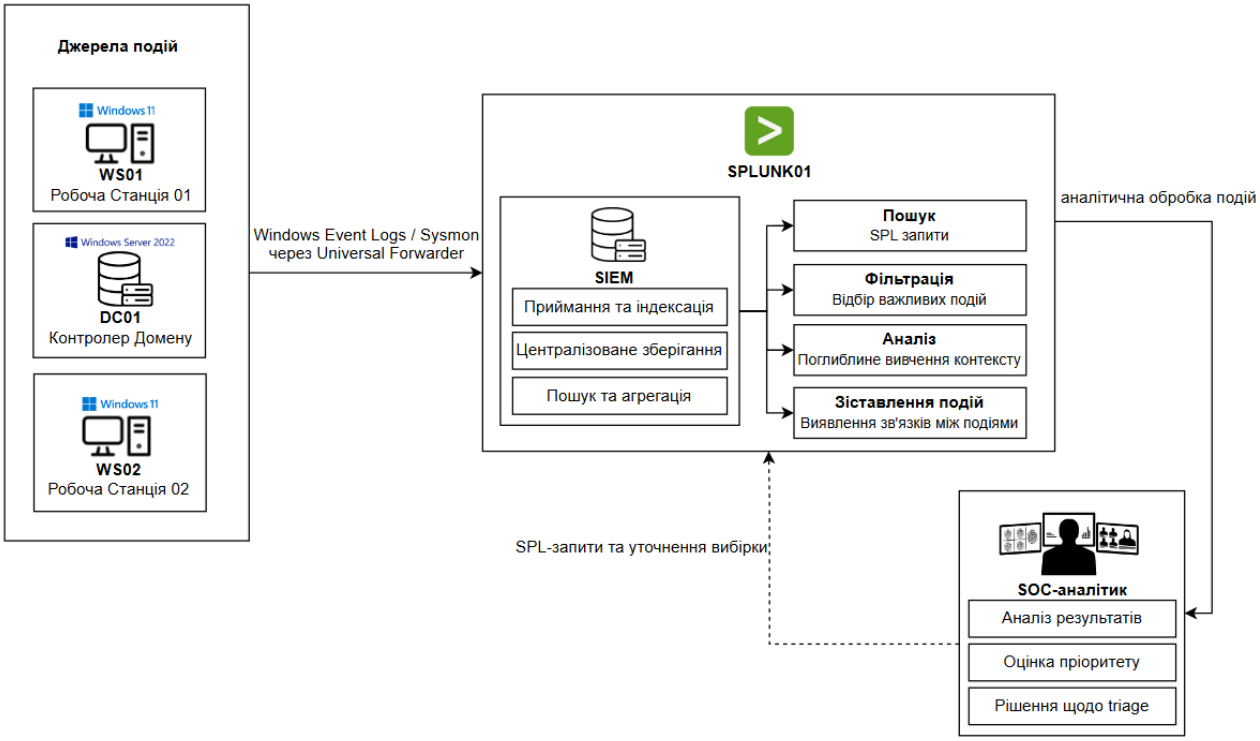


Рисунок 1.2 — Роль SIEM у централізованому зборі та аналізі подій безпеки

Для цієї дипломної роботи роль SIEM виконує Splunk Enterprise. У його документації модель приймання та пересилання даних описується через взаємодію receiving instance і forwarder-компонентів. Така архітектура добре підходить для лабораторного стенда: одна система централізовано приймає події, а окремі вузли

пересилають їх у визначений індекс. У результаті SIEM стає не просто сховищем, а центральною точкою доступу до телеметрії всього середовища [17–19, 21].

Водночас SIEM не слід розглядати як повний замінник triage або incident response. Він ефективний для первинного виявлення, вибірки, кореляції та побудови часової картини, але якщо потрібно уточнити контекст безпосередньо на кінцевій точці, часто виникає потреба звернутися до окремого IR-інструмента. Саме тому в подальших підрозділах SIEM розглядається як базовий рівень SOC-конвеєра, але не як єдиний його компонент [1, 17, 22, 23]. Основні можливості SIEM, які використовуються в межах цієї роботи, узагальнено в таблиці 1.2.

Таблиця 1.2 — Можливості SIEM у моніторингу та первинному аналізі

Можливість	**Що дає аналітику**	**Приклад застосування**
Централізований збір	Доступ до подій з усіх вузлів в одному інтерфейсі	Перегляд журналів DC01, WS01 і WS02 в одному індексі
Пошук та фільтрація	Швидке виділення потрібних подій	Пошук за host, source, Event ID
Агрегація даних	Порівняння подій між різними хостами	Оцінка активності за період або вузлом
Побудова контексту	Об’єднання окремих подій у послідовність	Логон → запуск процесу → DNS-запит
Аналітика	Підготовка даних до triage	Виділення підозрілих сценаріїв для подальшої перевірки

1.3 Endpoint-телеметрія як джерело даних для виявлення інцидентів

Під endpoint-телеметрією доцільно розуміти журнали та події, які формуються безпосередньо на кінцевих точках: робочих станціях, серверах та інших вузлах, де виконується операційна система, запускаються процеси та взаємодіють користувачі. На відміну від мережевих журналів, endpoint-телеметрія показує події ближче до джерела дії: який обліковий запис виконав вхід, який процес було створено, який об’єкт змінено, який DNS-запит ініційовано [4, 5].

Узагальнену роль endpoint-телеметрії у процесі виявлення інцидентів наведено на рисунку 1.3.



Рисунок 1.3 — Endpoint-телеметрія як джерело даних для виявлення інцидентів

Для Windows-середовища базовими джерелами такої телеметрії є журнали Security, System і Application. Журнал Security містить події автентифікації, змін привілеїв і створення процесів за умови належного аудиту. System фіксує роботу служб, драйверів і системних компонентів. Application відображає події прикладного рівня. Самі по собі ці журнали вже становлять значну аналітичну цінність, однак для задач більш детального моніторингу їх часто доповнюють Sysmon [4, 6]. Приклад основних журналів Windows у Event Viewer наведено на рисунку 1.4.

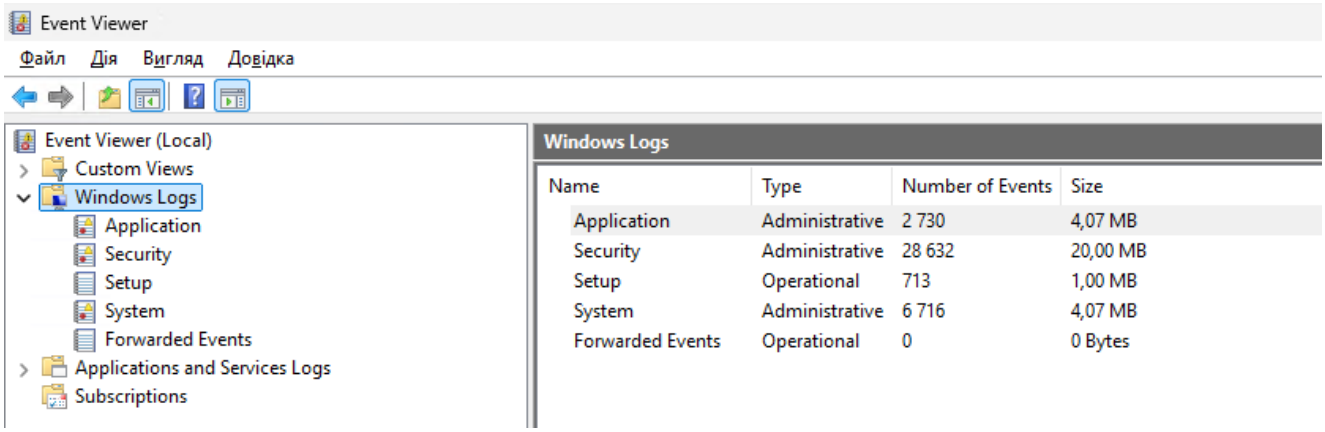


Рисунок 1.4 — Основні журнали Windows у Event Viewer

Основні джерела endpoint-телеметрії, використані в роботі, узагальнено в таблиці 1.3.

Таблиця 1.3 — Основні джерела endpoint-телеметрії у Windows-середовищі

Джерело	**Тип даних**	**Аналітична цінність**
Security	Логони, привілеї, створення процесів	Дає змогу відстежувати користувачів і дії доступу
System	Служби, драйвери, системні зміни	Допомагає бачити фоновий стан вузла
Application	Події прикладного рівня	Фіксує активність програм і служб користувача
Sysmon	Розширені поведінкові події	Надає деталізований контекст для виявлення сценаріїв

У документації Microsoft Sysmon визначається як засіб, що після встановлення залишається активним між перезавантаженнями та записує детальну інформацію про процеси, мережеві з'єднання та зміни, пов'язані з файлами. Для SOC це важливо тому, що Sysmon дає набагато більше контексту, ніж стандартні журнали: повний шлях до процесу, командний рядок, ідентифікатори процесів, дані про батьківський процес та інші поля, які корисні для побудови поведінкових сценаріїв [4, 5].

Endpoint-телеметрія стає особливо цінною тоді, коли подія безпеки не виглядає небезпечною у відриві від контексту. Наприклад, сам по собі запуск PowerShell або командного рядка може бути законною адміністративною дією. Але якщо такий запуск відбувається від незвичного користувача, у нетиповий час і супроводжується DNS-запитами чи змінами у реєстрі, сукупність подій уже заслуговує на увагу. Саме для таких ситуацій endpoint-телеметрія має вирішальне значення [5, 6, 27, 28].

Українські автори, які досліджують засоби SIEM у сучасних комп'ютерних мережах, також підкреслюють, що ефективний моніторинг не обмежується одним типом журналів. Навпаки, найбільшу практичну цінність має поєднання централізованої аналітики SIEM із даними, які надходять із кінцевих точок. У статті про метод та засіб моніторингу безпеки на основі SIEM це прямо розглядається як зв'язок між SIEM, EDR і NDR-компонентами, де endpoint-рівень виступає одним із ключових джерел контексту [29].

Для дипломного стенда endpoint-телеметрія є одним із центральних елементів, оскільки саме вона дозволяє перейти від загальних міркувань про моніторинг до конкретних подій, які можна дослідити у Splunk і потім уточнити за допомогою IR-інструмента. У подальших розділах це буде показано на прикладах Security Events, Sysmon Event ID та первинного triage на кінцевих точках [4, 5, 17, 22].

1.4 Тріаж інцидентів у процесі моніторингу безпеки

Після виявлення підозрілої події аналітик не переходить одразу до повного розслідування. Між моментом первинного спрацювання та рішенням про ескалацію існує проміжний етап, який у практиці incident response називають triage. Його завдання полягає в тому, щоб швидко оцінити наявний контекст, визначити пріоритет, відокремити очевидні хибнопозитивні випадки від дійсно важливих і вирішити, чи потрібне подальше поглиблене реагування [1].

У документах NIST triage прямо пов’язаний із загальною логікою incident response: організація має не просто збирати сигнали, а й мати процес, який дозволяє послідовно їх оцінювати. Інакше моніторинг швидко перетворюється на накопичення подій без зрозумілого механізму прийняття рішень. Для SOC це критично, оскільки навіть у відносно невеликому середовищі кількість технічних подій перевищує той обсяг, який можна осмислено обробляти без пріоритизації [1–3]. Місце triage у загальній логіці SOC-конвеєра показано на рисунку 1.5.

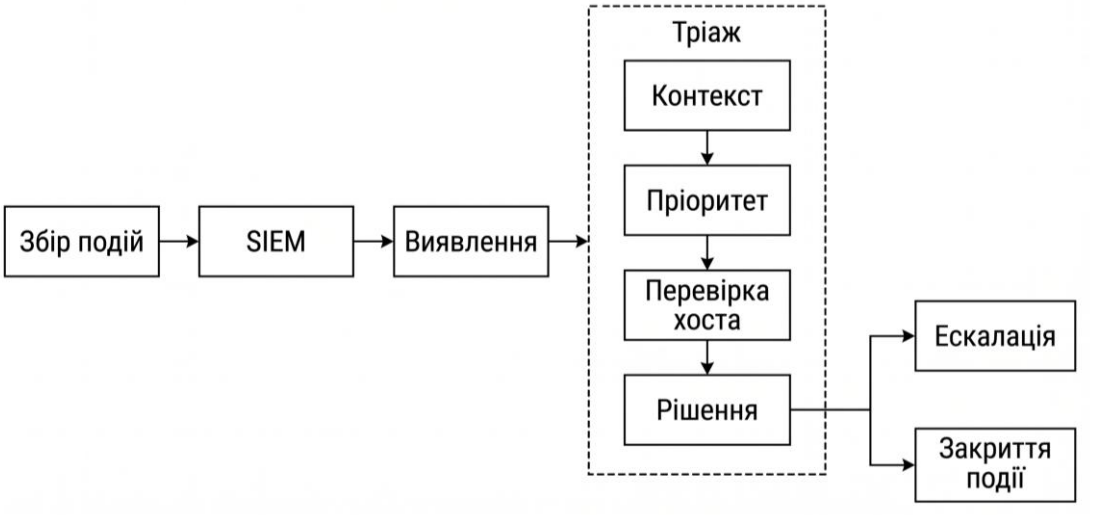


Рисунок 1.5 — Місце triage у SOC-конвеєрі моніторингу та реагування

На етапі triage аналітик зазвичай уточнює кілька базових питань: де саме сталася подія, який користувач із нею пов’язаний, чи є ознаки привілейованого доступу, який процес або механізм її породив, чи є суміжні події в тому самому часовому вікні та чи впливає вона на критичний актив. Частина такої перевірки виконується безпосередньо в SIEM, але якщо наявної телеметрії недостатньо, виникає потреба звернутися до інструментів endpoint-triage [1, 5, 22–24]. Основні етапи первинного triage подій безпеки наведено в таблиці 1.4.

Таблиця 1.4 — Основні етапи первинного triage подій безпеки

Етап	**Що перевіряється**	**Результат**
Первинний перегляд	Час, вузол, користувач, тип події	Розуміння базового контексту
Оцінка важливості	Критичність активу та привілеї	Попередній пріоритет події
Кореляція	Наявність суміжних подій у тому самому часовому вікні	Формування послідовності дій
Уточнення	Потреба в endpoint-перевірці або додаткових артефактах	Рішення щодо наступного кроку
Ескалація або закриття	Підтвердження або спростування ризику	Передавання інциденту далі або завершення розгляду

Для лабораторного стенда важливо, що triage розглядається не як абстрактна управлінська процедура, а як конкретний технічний крок між виявленням і поглибленою перевіркою. Наприклад, подія успішного логону сама по собі не є інцидентом. Але якщо вона поєднується з привілейованим входом, нетиповим запуском PowerShell і додатковими змінами на хості, пріоритет такої активності вже змінюється. Саме вміння побачити цю різницю і становить зміст первинного triage [1, 10, 13, 14, 28].

Огляд документації Velociraptor також добре показує місце triage в загальному DFIR-процесі. Платформа орієнтована не лише на повну збірку даних, а й на швидке виявлення відхилень за допомогою triaging artifacts та targeted queries. Це узгоджується з сучасною практикою: замість того щоб одразу копіювати великі масиви даних з усіх вузлів, аналітик спочатку намагається локалізувати підозрілий актив і звузити коло перевірки [22–24].

У межах дипломної роботи triage розглядається як ключова ланка між SIEM і IR-рівнем. Це дозволяє уникнути крайнощів: з одного боку, не зупинятися лише на поверхневому перегляді журналів, а з іншого – не запускати поглиблений збір артефактів без достатніх підстав. Така логіка буде використана в експериментальній частині роботи, де після виявлення подій у Splunk здійснюватиметься первинна перевірка кінцевих точок у Velociraptor [1, 17, 22–24].

1.5 Роль Windows Security Events і Sysmon у побудові сценаріїв виявлення

Для побудови практичних сценаріїв виявлення недостатньо лише загального уявлення про наявність журналів. Потрібно розуміти, які саме події дають аналітично корисний сигнал і як вони поєднуються між собою. У Windows-середовищі важливу роль відіграють як Security Events, так і Sysmon-події, оскільки вони доповнюють одна одну: перші фіксують безпекові факти, другі надають деталізований поведінковий контекст [4–6].

До найбільш корисних Security Events у контексті дипломного стенда належать подія 4624, що відображає успішний логон, подія 4625 про невдалий вхід до системи, подія 4672 про надання спеціальних привілеїв новому входу, а також подія 4688 про створення нового процесу. Для контролера домену додаткову цінність становлять події 4768 і 4769, пов’язані з Kerberos-квитками. Разом вони дозволяють побудувати базову картину того, хто увійшов у систему, з якими правами та які дії виконував далі [11–16].

Sysmon у цій логіці виступає як розширювач контексту. Наприклад, Sysmon Event ID 1 дозволяє бачити процес, командний рядок і батьківський процес. Інші події Sysmon можуть відображати файлові зміни, реєстрову активність або DNS-запити. Коли такі записи аналізуються разом із Security Events, аналітик отримує не один ізольований сигнал, а послідовність дій, придатну для побудови сценарію виявлення [4, 5].

Це особливо добре узгоджується з підходом MITRE ATT&CK, де увага зосереджується не на назві конкретної утиліти, а на типі поведінки. Якщо в

середовищі спостерігається використання командних інтерпретаторів або PowerShell для виконання команд, така активність може бути співвіднесена з технікою T1059 і підтехнікою T1059.001. Для дипломної роботи це корисно не тому, що кожна дія в лабораторії є шкідливою, а тому, що це дозволяє описувати події мовою загальновизнаної матриці поведінки [26–28]. Приклад прив'язки процесної активності до техніки MITRE ATT&CK наведено в Додатку А.

Важливий момент полягає в тому, що жодна окрема подія не повинна тлумачитися як доказ інциденту без контексту. Успішний логон може бути звичайною робочою дією, привілейований логон – штатною адміністративною операцією, а запуск PowerShell – цілком легітимним інструментом. Аналітична цінність виникає тоді, коли події розглядаються у зв'язку одна з одною: наприклад, після логону фіксується привілейований доступ, потім створення процесу, а далі додаткові зміни на хості [1, 5, 7, 9]. Приклад такого ланцюга подій наведено на рисунку 1.6.



Рисунок 1.6 — Приклад ланцюга подій для сценарію виявлення на основі Security Events і Sysmon.

Саме тому в цій роботі Security Events і Sysmon розглядаються як основа для побудови контрольованих сценаріїв виявлення. Вони достатньо стандартні, добре документовані та водночас придатні для демонстрації того, як формується логіка від окремої події до послідовності, яка вже потребує triage. Це робить їх особливо зручними для навчального SOC-стенда [4–6, 17]. Події Windows Security та Sysmon, які використовуються як основа сценаріїв виявлення, наведено в таблиці 1.5.

Таблиця 1.5 — Події Windows і Sysmon, які доцільно використовувати у сценаріях виявлення

Подія	Опис	Аналітичне значення
4624	Успішний вхід до системи	Дозволяє встановити факт логону та пов’язаний обліковий запис
4625	Невдалий вхід до системи	Дозволяє виявляти спроби автентифікації з помилковими обліковими даними
4672	Привілеї нового входу	Показує появу адміністративного або системного контексту
4688	Створення нового процесу	Дає змогу бачити запуск інструментів та команд
4768 / 4769	Kerberos-квитки	Корисні для аналізу доменної автентифікації
Sysmon Event ID 1	Створення процесу	Надає деталізований контекст виконання процесу
Інші Sysmon-події	Файли, реєстр, DNS та інше	Дозволяють розширити сценарій поведінковими ознаками

1.6 IR-платформи у SOC-конвеєрі та місце Velociraptor

Навіть добре налаштований SIEM не закриває всіх потреб аналітика. Центральна платформа дозволяє знайти підозрілий вузол, вибрати часовий проміжок, побачити події та зв’язки між ними. Однак коли виникає потреба уточнити фактичний стан конкретної кінцевої точки – наприклад, отримати додаткові відомості про вузол, запустити артефакт збору інформації або звузити перевірку до конкретного хоста – зручніше використовувати окрему IR-платформу [1, 22, 23].

У документації Velociraptor платформа описується як засіб для endpoint monitoring, digital forensics і cyber response. Для дипломної теми це особливо важливо, оскільки вона добре вкладається у роль інструмента первинного triage. SIEM у такій моделі виконує функцію централізованого виявлення та агрегації

подій, тоді як IR-платформа допомагає перейти від загального сигналу до перевірки конкретного вузла [22, 23].

Окреме місце в цій логіці посідають артефакти Velociraptor. Саме вони визначають, які дані збираються, як вони обробляються і для якої задачі призначені. У практиці DFIR це означає, що перевірка хоста може бути не хаотичною, а цілеспрямованою: аналітик запускає не довільний набір команд, а конкретний артефакт, розрахований на певний тип triage або збору інформації [24].

Порівняння ролей SIEM та IR-платформи є важливим для уникнення плутанини. SIEM зручно використовувати для пошуку, кореляції, побудови часової послідовності й оцінки того, чи є подія підозрілою. IR-платформа корисна тоді, коли потрібно уточнити стан endpoint-вузла, виконати адресний збір даних або підтвердити гіпотезу, яка виникла на основі журналів. У такій моделі ці інструменти не дублюють один одного, а працюють як послідовні частини одного конвеєра [1, 17, 22–24]. Співвідношення SIEM та IR-платформи у SOC-конвеєрі наведено на рисунку 1.7.

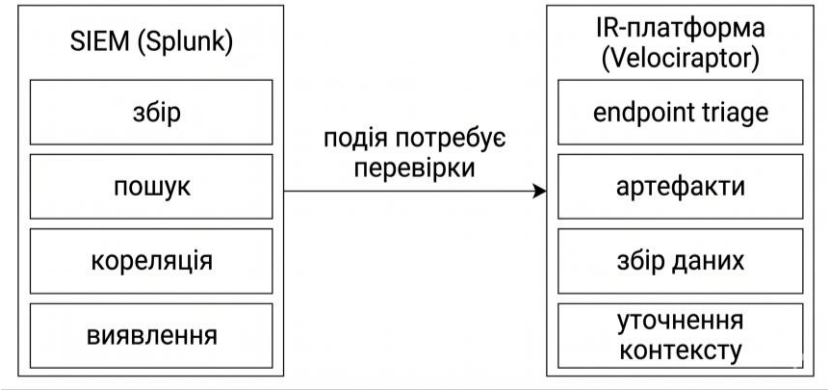


Рисунок 1.7 — Співвідношення SIEM та IR-платформи у SOC-конвеєрі

Для лабораторного стенда це означає наступне: Splunk використовується як SIEM-рівень, а Velociraptor – як засіб endpoint-triage на окремому IR-вузлі. Така зв’язка є достатньою, щоб продемонструвати повний мінімальний цикл: подія потрапляє у централізоване середовище, аналітик оцінює її в контексті інших журналів, після чого за потреби переходить до перевірки конкретного хоста [17, 22–24]. Основні відмінності між SIEM та IR-платформою наведено в таблиці 1.6.

Таблиця 1.6 — Порівняння ролей SIEM та IR-платформи у SOC-конвеєрі

Критерій	**SIEM**	**IR-платформа**
Основне призначення	Централізований збір і аналіз подій	Перевірка конкретних endpoint-вузлів
Тип роботи	Пошук, агрегація, кореляція	Адресний triage та збір артефактів
Рівень контексту	Міжвузловий і часовий	Локальний контекст хоста
Тип рішення	Виявити та пріоритизувати	Підтвердити або спростувати підозру
Місце в конвеєрі	Початкове виявлення	Подальше уточнення та triage

У результаті місце Velociraptor у цій роботі визначається не як універсальна заміна SIEM, а як логічне доповнення до нього. Саме це дозволяє побудувати SOC-конвеєр, у якому виявлення і triage розведені по різних рівнях, але зберігають спільну послідовність дій. Такий підхід є достатньо реалістичним для навчальної інфраструктури і водночас зрозумілим для подальшого практичного використання [1, 17, 22–24].

Висновки до розділу 1

У першому розділі було розглянуто теоретичні основи побудови SOC-конвеєра моніторингу та тріажу інцидентів. Встановлено, що SOC доцільно розглядати не як окремий програмний продукт, а як поєднання процесів, ролей, інструментів і джерел телеметрії, які забезпечують централізований контроль подій безпеки, їх аналіз і подальше реагування.

Окремо визначено роль SIEM у такому конвеєрі. SIEM-платформа забезпечує централізоване приймання, зберігання, пошук і аналітичну обробку подій, однак не замінює повноцінний процес triage або incident response. Її основне призначення полягає в тому, щоб надати SOC-аналітику єдину точку доступу до подій з різних джерел та дозволити швидко виділяти підозрілу активність.

Також було показано значення endpoint-телеметрії у Windows-середовищі. Журнали Security, System, Application та події Sysmon дають змогу аналізувати не лише факт входу користувача або запуску процесу, а й ширший

поведінковий контекст: командний рядок, DNS-запити, зміни у реєстрі та файлову активність. Саме така телеметрія є основою для побудови практичних сценаріїв виявлення.

У розділі також розглянуто місце triage у процесі моніторингу безпеки. Визначено, що triage є проміжним етапом між первинним виявленням події в SIEM та подальшим реагуванням. Його завдання полягає в уточненні контексту, оцінці пріоритету та прийнятті рішення щодо необхідності подальшої перевірки endpoint-вузла.

Таким чином, теоретична частина сформувала основу для практичного розгортання лабораторного стенда. У наступному розділі ці положення застосовуються для проєктування середовища, у якому Splunk Enterprise виконує роль SIEM-рівня, Windows Event Logs і Sysmon виступають джерелами endpoint-телеметрії, а Velociraptor використовується як інструмент первинного endpoint-triage.

2. ПРОЄКТУВАННЯ ТА РОЗГОРТАННЯ ЛАБОРАТОРНОГО СТЕНДА SOC-КОНВЕЄРА

2.1 Архітектура лабораторного стенда

Проєктування лабораторного стенда виконувалося з урахуванням двох вимог: по-перше, середовище мало відтворювати базову корпоративну інфраструктуру з доменом, робочими станціями, централізованим моніторингом і окремим вузлом triage; по-друге, його потрібно було розгорнути так, щоб кожен елемент стенда можна було окремо налаштувати, перевірити та показати у кваліфікаційній роботі. Такий підхід відповідає логіці побудови навчального SOC-середовища, де важливим є не лише кінцевий результат, а й прозорість усіх етапів розгортання [2].

У межах стенда було використано п’ять основних вузлів SOC-конвеєра та окремий вузол KALI01 для моделювання контрольованої атакувальної активності, для яких під час підготовки практичної частини було зафіксовано ролі, операційні системи та мережеві параметри. Контролер домену DC01 виконує функції централізованої автентифікації та є джерелом доменних журналів безпеки. Робочі станції WS01 та WS02 виступають кінцевими точками, на яких формується основна endpoint-телеметрія. Сервер SPLUNK01 призначений для приймання та індексації журналів, а вузол Ubuntu-IR із сервісом Velociraptor виконує функції первинного triage і перевірки кінцевих точок.

Архітектурно стенд побудовано за принципом розділення ролей. Це означає, що доменні функції, збирання подій і endpoint-triage не поєднуються на одній системі, а винесені на окремі вузли. Така побудова не копіює повністю велику виробничу інфраструктуру, але наближає лабораторне середовище до реальної логіки роботи SOC, де дані надходять із різних джерел, агрегуються в SIEM і за потреби перевіряються на рівні конкретного хоста [1].

Як базову платформу віртуалізації доцільно використовувати середовище, у якому можна одночасно підтримувати кілька Windows- і Linux-вузлів, швидко керувати їхнім станом, а також робити знімки, повторювати конфігурації та

відновлювати окремі машини після тестів. У практичній частині таким середовищем виступає Hyper-V, що дозволяє централізовано адмініструвати лабораторний стенд і зберігати контроль над усією структурою в межах одного хостового сервера. Перелік віртуальних машин, використаних для розгортання лабораторного SOC-стенда у Hyper-V, наведено в додатку Г.

Для подальшого опису доцільно зафіксувати склад стенда в окремій таблиці. Така подача зручна не лише для читання, а й для перевірки конфігурації під час демонстрації або повторного розгортання лабораторії. Склад основних вузлів лабораторного стенда наведено в таблиці 2.1.

Таблиця 2.1 — Склад лабораторного стенда

Вузол	**Роль у стенді**	**ОС**	**IP адреса**
DC01	Контролер домену, джерело доменних і безпекових подій	Windows Server 2022	192.168.100.10
WS01	Робоча станція, джерело endpoint-телеметрії	Windows 11 Pro	192.168.100.20
WS02	Робоча станція, джерело endpoint-телеметрії	Windows 11 Pro	192.168.100.21
SPLUNK01	SIEM-вузол, receiving та search	Windows Server 2022	192.168.100.30
Ubuntu-IR	IR-вузол з Velociraptor	Ubuntu 24.04 LTS	192.168.100.40
KALI01	Вузол моделювання контрольованої атакувальної активності	Kali Linux	192.168.100.50

Таким чином, уже на етапі архітектурного проєктування було сформовано достатню основу для подальшого розгортання стенда: окремий доменний вузол, окремий SIEM-сервер, дві робочі станції як джерела подій та окремий вузол triage. Саме така структура надалі дозволяє не лише збирати події, а й демонструвати повний ланцюг «джерело події – централізований аналіз – перевірка кінцевої точки» [1, 2, 17, 22].

2.2 Мережева схема та взаємодія вузлів

Після визначення ролей вузлів наступним кроком стало проєктування мережевої схеми. Для лабораторного середовища було обрано єдину локальну підмережу 192.168.100.0/24, у межах якої кожен основний вузол отримав статично визначену IPv4-адресу. Таке рішення спрощує маршрутизацію подій, налаштування forwarder-ів, перевірку доступності сервісів і документування конфігурації в тексті дипломної роботи.

Для коректної роботи доменної інфраструктури особливу увагу приділено параметрам DNS. Контролер домену DC01 виконує не лише роль централізованого вузла автентифікації, а й виступає DNS-сервером для доменних систем. Саме тому робочі станції WS01 і WS02, а також сервер SPLUNK01 використовують адресу 192.168.100.10 як DNS-сервер. Це дозволяє їм коректно розпізнавати доменні імена типу WS01.corp.kozhushko.internal або DC01.corp.kozhushko.internal.

З погляду потоку даних взаємодія вузлів організована у двох основних площинах. Перша площина — доменна: робочі станції взаємодіють із контролером домену, проходять автентифікацію, отримують політики та генерують відповідні події Security. Друга площина — моніторингова: Windows-вузли через Splunk Universal Forwarder передають журнали подій до SPLUNK01, де вони приймаються, індексуються та аналізуються [17–19, 21]. Структурно-мережеву схему лабораторного SOC-стенда наведено на рисунку 2.1.

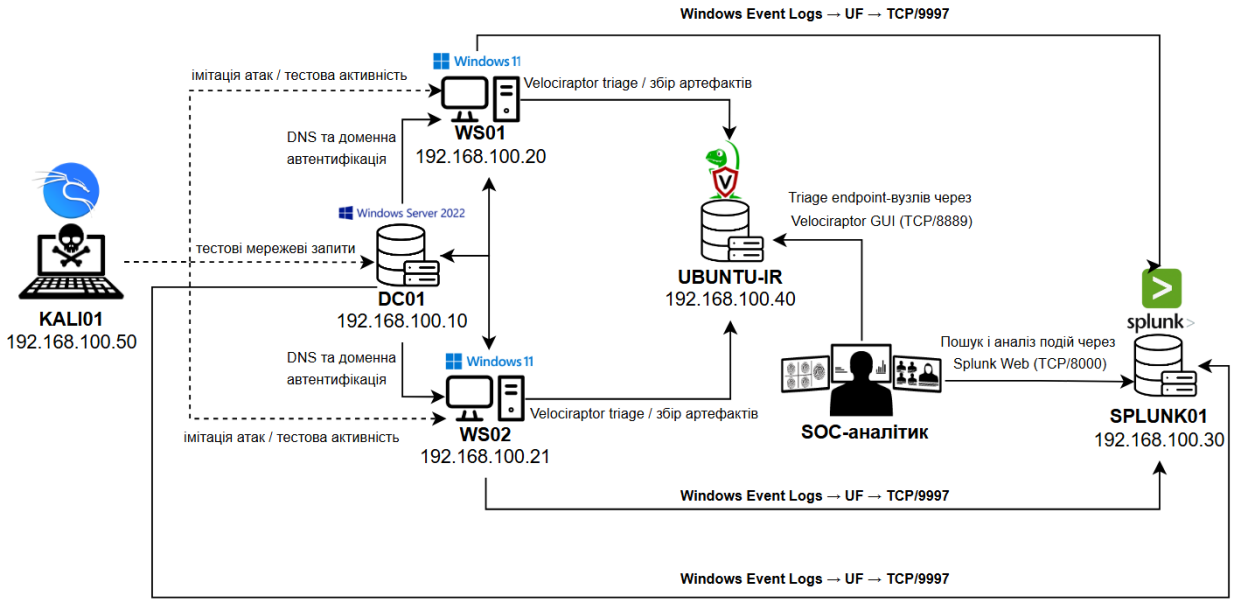


Рисунок 2.1 – Структурно-мережева схема лабораторного SOC-стенда

Адресацію та мережеві параметри вузлів стенда наведено в таблиці 2.2.

Таблиця 2.2 — Адресація та мережеві параметри основних вузлів

Вузол	**IPv4**	**Основна функція в мережі**	**DNS**
DC01	192.168.100.10	Контролер домену, DNS	127.0.0.1 / ::1
WS01	192.168.100.20	Клієнт домену, джерело логів	192.168.100.10
WS02	192.168.100.21	Клієнт домену, джерело логів	192.168.100.10
SPLUNK01	192.168.100.30	Приймання та індексація подій	192.168.100.10
Ubuntu-IR	192.168.100.40	GUI та frontend Velociraptor	системна Ubuntu
KALI01	192.168.100.50	Вузол моделювання атак	192.168.100.10

Зафіксована схема адресації важлива ще й тому, що вона напряму відображається в конфігураційних файлах. Наприклад, саме адреса 192.168.100.30 використовується як receiving-ціль у файлі outputs.conf на Windows-вузлах, тоді як адреса 192.168.100.10 використовується як доменний орієнтир і DNS-сервер. Тому таблиця мережевих параметрів у цьому розділі виконує не лише довідкову, а й верифікаційну функцію.

2.3 Розгортання доменної інфраструктури

Функціонування лабораторного SOC-конвеєра потребує середовища, у якому події користувацького входу, призначення привілеїв та Kerberos-активність формуються не штучно, а в межах реально працюючого домену. Саме тому окремим етапом було розгорнуто домен corp.kozhushko.internal на базі контролера DC01. Структуру домену в оснастці Active Directory Users and Computers наведено на рисунку 2.2.

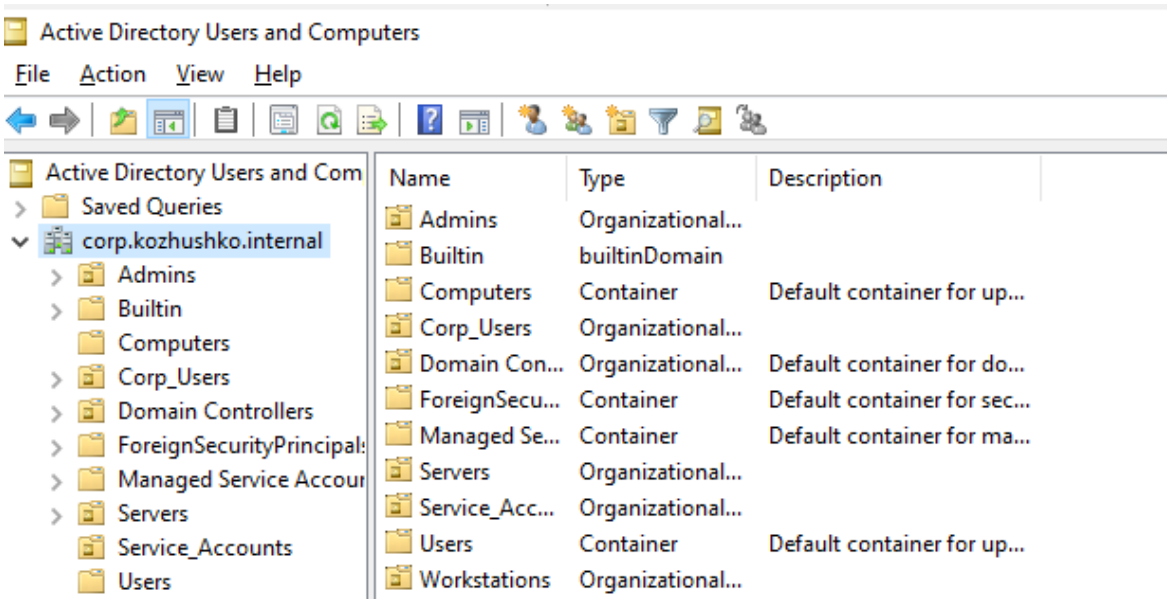


Рисунок 2.2 — Оснастка Active Directory Users and Computers із доменною структурою corp.kozhushko.internal

Така конфігурація дозволяє одразу отримати той тип подій, який типовий для корпоративної інфраструктури: журнали логону, події облікових записів, запити TGT і сервісних квитків [9, 15, 16].

У практичній частині підтверджено наявність доменних користувачів Administrator, socadmin, akozhushko, а також доменних комп'ютерів DC01, WS01, WS02 і SPLUNK01. Перелік доменних користувачів, отриманий за допомогою PowerShell, наведено на рисунку 2.3.

```
PS C:\Windows\system32> Get-ADUser -Filter * | Select Name, SamAccountName, Enabled

Name              SamAccountName Enabled
----              -------------- -------
Administrator     Administrator     True
Guest             Guest            False
krbtgt            krbtgt           False
Andrii Kozhushko akozhushko         True
SOC Admin         socadmin          True
```

Рисунок 2.3 – Перелік доменних користувачів, отриманий засобами PowerShell

Додатково виведено склад групи Domain Admins, до якої входять Administrator та socadmin. Це важливо для подальшого аналізу, оскільки події привілейованого входу та дії адміністративних облікових записів у третьому розділі розглядаються вже не абстрактно, а в контексті реальної доменної конфігурації. Склад групи Domain Admins наведено на рисунку 2.4.

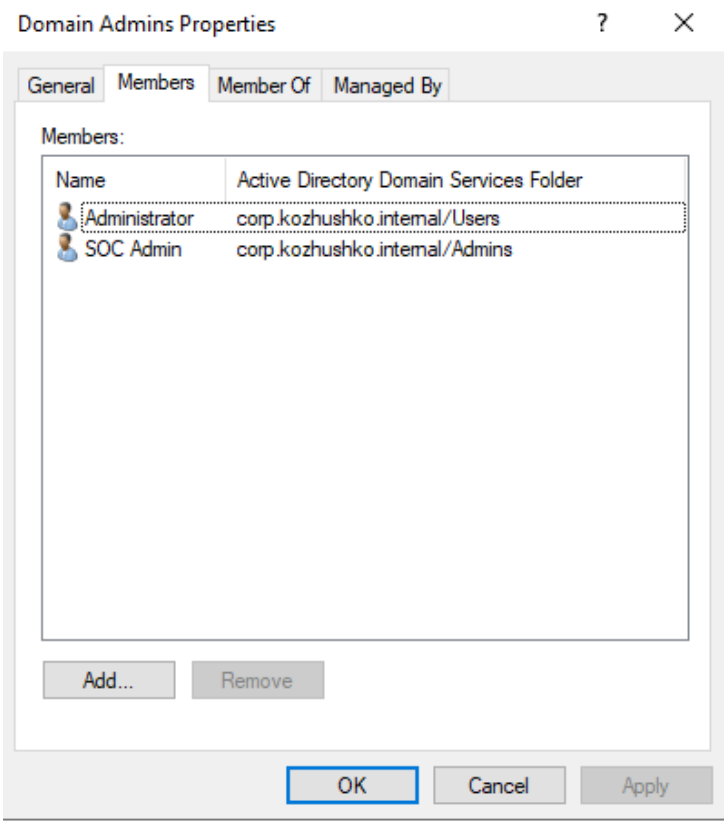


Рисунок 2.4 — Склад групи Domain Admins у домені corp.kozhushko.internal

Основні доменні об’єкти, зафіксовані у стенді, узагальнено в таблиці 2.3.

Таблиця 2.3 — Основні доменні об’єкти, зафіксовані у стенді

Тип об’єкта	**Назва**	**Призначення у стенді**
Користувач	Administrator	Базовий адміністративний обліковий запис домену
Користувач	socadmin	Основний робочий обліковий запис адміністратора
Користувач	akozhushko	Доменний користувач для перевірки сценаріїв
Комп’ютер	WS01	Клієнт домену, джерело endpoint-подій
Комп’ютер	WS02	Клієнт домену, джерело endpoint-подій
Комп’ютер	SPLUNK01	Член домену, SIEM-вузол

Ще один практичний аспект полягає в тому, що доменна інфраструктура дозволяє коректно відтворювати різні типи подій Windows Security. Якщо в локальному недоменному середовищі частина сценаріїв мала б спрощений

характер, то в домені з’являються Kerberos-події, прив’язка до доменних SID, груп, комп’ютерних об’єктів і журналювання автентифікації на контролері домену. З огляду на тему дипломної роботи це є принципово важливим.

Отже, доменна інфраструктура в межах стенда не є другорядним елементом. Вона задає той контекст, у якому з’являються події Security, що використовуються надалі для аналізу входів у систему, привілеїв і доменної активності. Без такого шару практична частина роботи втратила б значну частину наближеності до реального корпоративного середовища [1, 9].

2.4 Розгортання та налаштування Splunk Enterprise

Центральним елементом моніторингової частини стенда став сервер SPLUNK01, на якому розгорнуто Splunk Enterprise. Саме цей вузол відповідає за приймання подій від forwarder-ів, їх індексацію та подальший пошук через веб-інтерфейс. У контексті роботи Splunk використовується не просто як сховище логів, а як SIEM-компонент, у якому можна централізовано переглядати події з різних джерел, групувати їх за host, source, sourcetype і формувати початкові аналітичні вибірки [17, 21]. Приклад веб-інтерфейсу Splunk Enterprise наведено на рисунку 2.5.

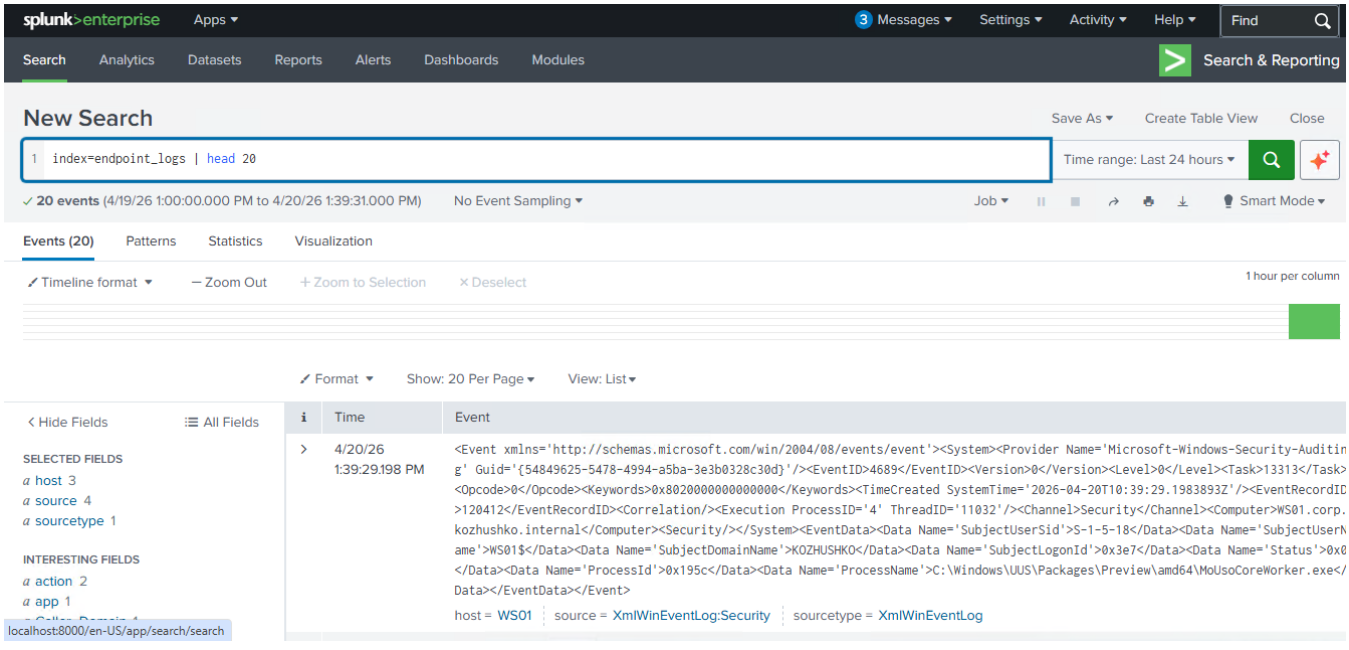


Рисунок 2.5 — Веб-інтерфейс Splunk Enterprise

Практична перевірка конфігурації показала, що на SPLUNK01 відкрито три ключові порти: 8000 для веб-інтерфейсу, 8089 для керування сервісом Splunkd і 9997 для приймання даних від forwarder-ів. Така конфігурація повністю відповідає документації Splunk, у якій receiving-instance та management-layer розглядаються як окремі функціональні площини [17, 18, 20, 21]. Результат перевірки відкритих портів Splunk на SPLUNK01 наведено на рисунку 2.6.

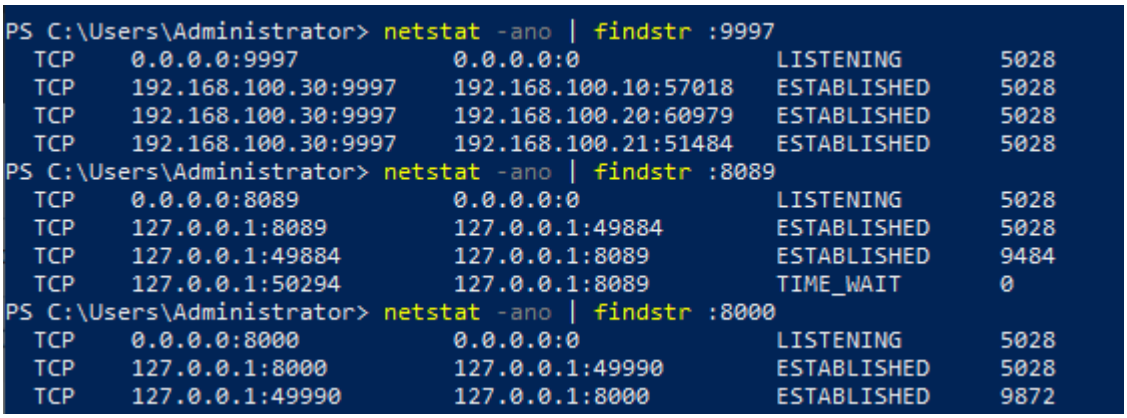


Рисунок 2.6 — Перевірка відкритих портів 8000, 8089, 9997 на SPLUNK01

Важливим етапом було також підтвердження того, що сервіс Splunkd працює коректно, а receiving-порт дійсно приймає TCP-з’єднання від Windows-вузлів. Це видно як за результатами команди netstat, так і з факту появи подій у пошуковому індексі endpoint_logs. Тобто зв’язок між описаною архітектурою та реальною телеметрією підтверджено не теоретично, а безпосередньо в лабораторному середовищі. Основні сервіси та порти Splunk у лабораторному стенді наведено в таблиці 2.4.

Таблиця 2.4 — Основні сервіси та порти Splunk у лабораторному стенді

Елемент	**Призначення**	**Підтверджене значення**
Splunk Web	Веб-інтерфейс аналітика	TCP/8000
Splunkd	Керування службою та API	TCP/8089
Receiving port	Приймання подій від forwarder-ів	TCP/9997
Служба	Фоновий сервіс Splunk	Splunkd – Running

Таким чином, SIEM-рівень стенда можна вважати налаштованим коректно: сервер SPLUNK01 приймає журнали, надає веб-інтерфейс для пошуку та підтримує керуючі функції через Splunkd. Це створює практичну основу для наступного етапу — розгортання Universal Forwarder та передавання подій з Windows-вузлів [17–19, 21].

2.5 Налаштування Splunk Universal Forwarder на Windows-вузлах

Щоб події з Windows-вузлів надходили до централізованого індексу, на DC01, WS01 та WS02 було встановлено Splunk Universal Forwarder. Вибір саме цього компонента є логічним для лабораторного стенда, оскільки Splunk прямо позиціонує Universal Forwarder як легкий агент для пересилання даних із кінцевих систем до receiving instance [18].

На всіх трьох Windows-вузлах у файлі outputs.conf було вказано адресу receiving-сервера 192.168.100.30:9997. Це означає, що вся телеметрія, яку forwarder отримує з локальних журналів Windows, пересилається до SPLUNK01. З технічного погляду саме цей файл визначає мережевий напрямок передавання подій і є одним із ключових елементів практичної конфігурації [20]. Приклад налаштування файлу outputs.conf наведено на рисунку 2.7.

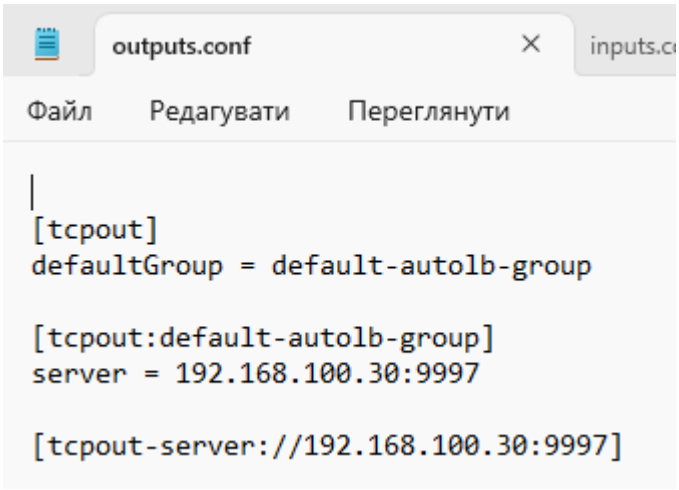


Рисунок 2.7 — Файл outputs.conf на Windows-вузлі

Другим критично важливим файлом є inputs.conf, де задається, які саме журнали слід збирати. На DC01 активовано збір Application, Security та System. Фрагмент файлу inputs.conf на DC01 наведено на рисунку 2.8.

inputs - Notepad

File Edit Format View Help

```
[WinEventLog://Application]
disabled = 0
index = endpoint_logs
renderXml = true
sourcetype = XmlWinEventLog:Application

[WinEventLog://Security]
disabled = 0
index = endpoint_logs
renderXml = true
sourcetype = XmlWinEventLog:Security

[WinEventLog://System]
disabled = 0
index = endpoint_logs
renderXml = true
sourcetype = XmlWinEventLog:System
```

Рисунок 2.8 – Файл inputs.conf на DC01

На WS01 і WS02 додатково активовано Microsoft-Windows-Sysmon/Operational. Приклад файлу inputs.conf на робочій станції WS01 наведено на рисунку 2.9.

inputs.conf

Файл Редагувати Переглянути

```
[WinEventLog://Application]
disabled = 0
index = endpoint_logs
renderXml = true
sourcetype = XmlWinEventLog:Application

[WinEventLog://Security]
disabled = 0
index = endpoint_logs
renderXml = true
sourcetype = XmlWinEventLog:Security

[WinEventLog://System]
disabled = 0
index = endpoint_logs
renderXml = true
sourcetype = XmlWinEventLog:System

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = 0
index = endpoint_logs
renderXml = true
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

Рисунок 2.9 — Файл inputs.conf на WS01

Узагальнення налаштувань Universal Forwarder наведено в таблиці 2.5.

Таблиця 2.5 — Налаштування Universal Forwarder на основних Windows-вузлах

Вузол	**Наявність UF**	**Основні журнали**	**Ціль пересилання**
DC01	Так	Application, Security, System	192.168.100.30:9997
WS01	Так	Application, Security, System, Sysmon	192.168.100.30:9997
WS02	Так	Application, Security, System, Sysmon	192.168.100.30:9997

Така відмінність між контролером домену та робочими станціями повністю відповідає ролям вузлів у стенді: сервер домену є насамперед джерелом доменних і безпекових подій, тоді як робочі станції виступають джерелом розширеної endpoint-телеметрії.

Після застосування конфігурації було перевірено запуск і стан служби SplunkForwarder на кожному вузлі. Факт роботи сервісу важливий не сам по собі, а як підтвердження того, що журнали не лише зазначені в конфігурації, а й реально пересилаються до SIEM. Саме ця перевірка з’єднує текстову конфігурацію з практичним результатом у Splunk Search.

Отже, рівень централізованого збору подій у стенді побудовано на єдиній і зрозумілій схемі: кожен Windows-вузол має локально визначений набір журналів, а далі через Universal Forwarder передає їх до receiving-instance на SPLUNK01. Така схема легко документується, перевіряється й повторно відтворюється [17–21].

2.6 Налаштування збору endpoint-телеметрії

Окремим етапом розгортання стало налаштування саме endpoint-телеметрії, тобто тих даних, які безпосередньо описують поведінку системи на кінцевій точці. У лабораторному стенді цей рівень базується на двох джерелах: стандартних журналах Windows Security/System/Application та журналі Sysmon. Поєднання цих джерел є виправданим, оскільки стандартний аудит дає базові події доступу й

процесів, а Sysmon забезпечує більш деталізоване спостереження за локальною активністю [4, 5].

На робочих станціях WS01 і WS02 було підтверджено, що служба Sysmon64 працює. Результат перевірки служби наведено на рисунку 2.10.

```
PS C:\WINDOWS\system32> Get-Service Sysmon*

Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           Sysmon64
```

Рисунок 2.10 — Перевірка служби Sysmon64

Також було перевірено, що журнал Microsoft-Windows-Sysmon/Operational існує та містить події. Приклад локального журналу Sysmon наведено на рисунку 2.11.

```
PS C:\WINDOWS\system32> Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 10


   ProviderName: Microsoft-Windows-Sysmon

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
20.04.2026 14:29:59             13 Information      Registry value set:...
20.04.2026 14:29:59             13 Information      Registry value set:...
20.04.2026 14:29:59             13 Information      Registry value set:...
20.04.2026 14:29:59             13 Information      Registry value set:...
20.04.2026 14:29:57              3 Information      Network connection detected:...
20.04.2026 14:29:57              3 Information      Network connection detected:...
20.04.2026 14:29:57              3 Information      Network connection detected:...
20.04.2026 14:29:56              3 Information      Network connection detected:...
20.04.2026 14:29:54              1 Information      Process Create:...
20.04.2026 14:29:51              1 Information      Process Create:...
```

Рисунок 2.11 — Локальний журнал Sysmon на робочій станції

У контексті дипломної роботи це має принципове значення: саме Sysmon дає змогу надалі аналізувати події створення процесів, DNS-запити, зміни в реєстрі та створення файлів, які є ключовими для третього розділу [4–6, 8].

Для коректного наповнення журналу Security також було перевірено налаштування аудиту. Зокрема, важливими є підкатегорії Process Creation, Process Termination, Logon, Credential Validation, User Account Management та низка інших параметрів Advanced Audit Policy. Їх наявність або відсутність прямо впливає на те, які події реально з’являються в Splunk. Тому в цьому розділі доцільно зафіксувати не лише факт встановлення Sysmon, а й увімкнення потрібного аудиту в Windows [9, 10]. Повний вивід параметрів аудиту Windows наведено в додатку Б.

Джерела endpoint-телеметрії, використані у стенді, наведено в таблиці 2.6.

Таблиця 2.6 — Джерела endpoint-телеметрії у стенді

Джерело	Приклади подій	Призначення в роботі
Security	4624, 4625, 4672, 4688	Логон, привілеї, створення процесів
System	Системні служби та події ОС	Контекст стану вузла
Application	Прикладні події	Додатковий контекст активності
Sysmon	1, 11, 13, 22	Поведінкова endpoint-телеметрія

Після налаштування аудиту й Sysmon стенд отримує не тільки базову доменну видимість, а й деталізований endpoint-рівень. Це дозволяє переходити від простого факту входу в систему до аналізу того, які саме дії виконувалися на хості, у якій послідовності та з якими наслідками.

2.7 Розгортання IR-вузла на базі Velociraptor

Щоб лабораторний стенд не обмежувався лише централізованим збиранням і пошуком подій, до його складу було включено окремий IR-вузол на базі Ubuntu 24.04 LTS із розгорнутим Velociraptor. Таке рішення дозволяє перевести аналіз із рівня «подія в SIEM» до рівня «перевірка конкретної кінцевої точки», тобто реалізувати базовий triage у межах одного навчального конвеєра [1, 22–24].

Практична перевірка показала, що на вузлі Ubuntu-IR активний сервіс Velociraptor. Результат перевірки статусу сервісу наведено на рисунку 2.12.

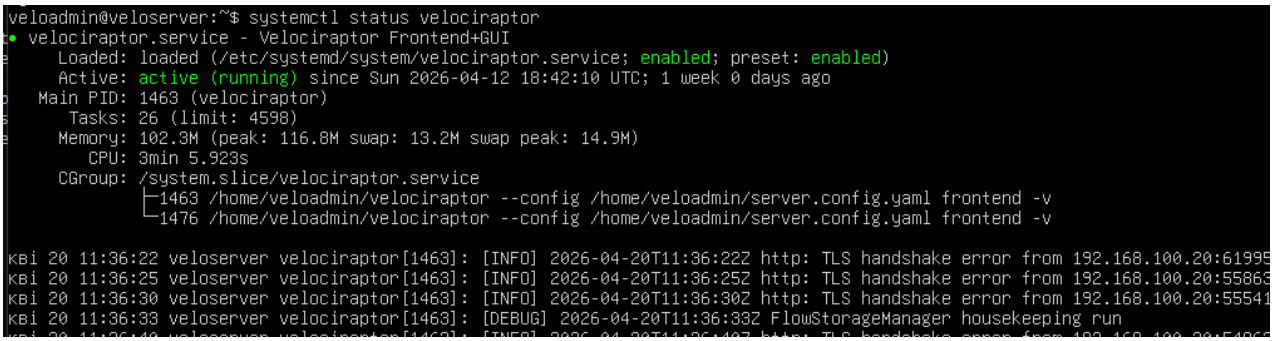


Рисунок 2.12 — Статус сервісу Velociraptor на Ubuntu-IR

Додатково було перевірено відкриті порти Velociraptor. GUI працює на адресі 192.168.100.40:8889, а frontend приймає клієнтські підключення на порту 8000. Результат перевірки портів наведено на рисунку 2.13.

```
veloadmin@veloserver:~$ ss -tulpn
Netid       State        Recv-Q       Send-Q             Local Address:Port              Peer Address:Port       Process
udp         UNCONN       0            0                     127.0.0.54:53                   0.0.0.0:*
udp         UNCONN       0            0                  127.0.0.53%lo:53                   0.0.0.0:*
tcp         LISTEN       0            4096                     0.0.0.0:22                   0.0.0.0:*
tcp         LISTEN       0            4096                 127.0.0.1:8003                   0.0.0.0:*
tcp         LISTEN       0            4096                 127.0.0.1:8001                   0.0.0.0:*
tcp         LISTEN       0            4096                 127.0.0.54:53                    0.0.0.0:*
tcp         LISTEN       0            4096              127.0.0.53%lo:53                    0.0.0.0:*
tcp         LISTEN       0            4096                        [::]:22                      [::]:*
tcp         LISTEN       0            4096                           *:8889                       *:*
tcp         LISTEN       0            4096                           *:8000                       *:*
```

Рисунок 2.13 — Перелік відкритих портів Velociraptor

Така конфігурація узгоджується з документацією платформи, у якій frontend, GUI та артефакти розглядаються як окремі, але взаємопов’язані елементи IR-робочого процесу [22–24].

У GUI Velociraptor було підтверджено наявність клієнтів WS01 і WS02.



Рисунок 2.14 — Список клієнтів у Velociraptor

Основні елементи IR-рівня у складі стенда наведено в таблиці 2.7.

Таблиця 2.7 — Основні елементи IR-рівня у складі стенда

Елемент	Функція	Підтвердження у практиці
Velociraptor GUI	Робота аналітика з клієнтами та артефактами	https://192.168.100.40:8889/
Velociraptor frontend	Приймання підключень від клієнтів	порт 8000
Clients	Представлення кінцевих точок	WS01, WS02 у списку клієнтів
Artifacts	Збирання відомостей для triage	Generic.Client.Info та пов’язані результати

Це має не лише демонстраційну, а й методичну цінність: якщо в Splunk з’являється підозріла активність з одного з цих хостів, аналітик може перейти до Velociraptor і виконати базову перевірку клієнта, переглянути його overview або результати

артефакту Generic.Client.Info. Таким чином, у стенді формується завершеніший цикл моніторингу та первинного triage, а не просто окремий збір логів.

Включення Velociraptor до складу стенда дозволяє обґрунтовано називати розгорнуте середовище саме SOC-конвеєром, а не просто SIEM-лабораторією. У ньому вже є не тільки централізоване виявлення подій, а й окремий інструмент для переходу до endpoint-перевірки, що цілком відповідає логіці первинного triage [1, 22–24].

Висновки до розділу 2

У другому розділі було розглянуто проєктування та практичне розгортання лабораторного стенда, призначеного для дослідження SOC-конвеєра моніторингу та triage інцидентів. У межах стенда реалізовано доменну інфраструктуру на базі DC01, дві робочі станції як джерела endpoint-телеметрії, SIEM-вузол SPLUNK01 і окремий IR-вузол на базі Ubuntu з Velociraptor.

На етапі розгортання було зафіксовано мережеву схему, підтверджено ролі вузлів, налаштовано Splunk Enterprise як receiving-instance, а на Windows-вузлах розгорнуто Splunk Universal Forwarder із конфігурацією inputs.conf та outputs.conf. Окремо підтверджено збір журналів Security, System, Application і Sysmon, що формує достатню основу для подальшого експериментального дослідження [4, 5, 8, 9].

Крім централізованого моніторингу, до складу стенда включено Velociraptor, який забезпечує базовий рівень endpoint-triage. У результаті створено цілісне навчальне середовище, у якому можна послідовно відстежувати шлях від джерела події до її аналізу в SIEM і подальшої перевірки на конкретному вузлі. Саме цей результат створює основу для третього розділу, де розглядатимуться сценарії виявлення та triage на основі реально зібраної телеметрії [1, 22–24].

3. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СЦЕНАРІЇВ ВИЯВЛЕННЯ ТА ТРІАЖУ ІНЦИДЕНТІВ У РОЗРОБЛЕНОМУ SOC-КОНВЕЄРІ

3.1 Мета та логіка експериментальної перевірки

Після розгортання лабораторного стенда потрібно було перевірити не тільки факт надходження журналів до Splunk, а й те, чи здатне побудоване середовище виявляти контрольовану активність атакувального вузла та переводити її в процедуру первинного triage. Експериментальна частина виконувалася на основі структурно-мережевої схеми лабораторного SOC-стенда, наведеної на рисунку 2.1. У цьому розділі та сама інфраструктура розглядається вже не як об’єкт проєктування, а як середовище перевірки detection-to-triage сценаріїв: KALI01 використовується як вузол моделювання атак, SPLUNK01 — як SIEM-рівень централізованого виявлення, а Ubuntu-IR з Velociraptor — як IR-рівень для уточнення стану атакованого endpoint-вузла [1–3].

Такий підхід дозволяє відійти від формальної перевірки окремих Event ID і перейти до більш реалістичної логіки SOC-конвеєра. У практиці моніторингу події не мають цінності лише як ізольовані записи. Їх потрібно розглядати в контексті джерела, часу, вузла, облікового запису, типу активності та подальших дій аналітика. Саме тому в цьому розділі окремо описуються сценарії мережевого сканування, невдалих SMB-автентифікацій та неоднозначної події ANONYMOUS LOGON [1, 2, 29, 30].

Лабораторний вузол KALI01 має адресу 192.168.100.50 і не є джерелом телеметрії для SIEM. Його роль полягає у створенні контрольованої атакувальної активності щодо Windows-вузлів. Події при цьому формуються не на Kali, а на цільових системах: DC01, WS01 або WS02. Саме ці події передаються через Splunk Universal Forwarder до SPLUNK01 і далі аналізуються у Splunk Search. Такий розподіл ролей відповідає схемі, наведеної на рисунку 2.1, де KALI01 показано як допоміжний атакувальний вузол, а основними джерелами телеметрії для SIEM залишаються Windows-системи стенда [17–19, 21].

Для експериментальної частини було обрано безпечні сценарії, які не передбачають використання шкідливого програмного забезпечення, експлуатації вразливостей або руйнування системи. Їхнє призначення — створити контрольовані ознаки, типові для початкових етапів атакувальної активності: мережеву розвідку, невдалі спроби автентифікації та перевірку того, як Windows фіксує SMB-взаємодію. Цього достатньо для демонстрації принципу detection-to-triage без ризику пошкодження лабораторного середовища.

Окрему увагу приділено тому, що не всі події слід інтерпретувати як підтверджений інцидент. Наприклад, подія 4624 з обліковим записом ANONYMOUS LOGON не є доказом успішного входу доменного користувача. У межах дослідження вона розглядається як приклад того, чому SOC-аналітик має перевіряти контекст події, а не реагувати лише на сам факт появи Event ID [11, 12]. Ролі компонентів у сценаріях експериментальної перевірки наведено в таблиці 3.1.

Таблиця 3.1 — Ролі компонентів у сценаріях експериментальної перевірки

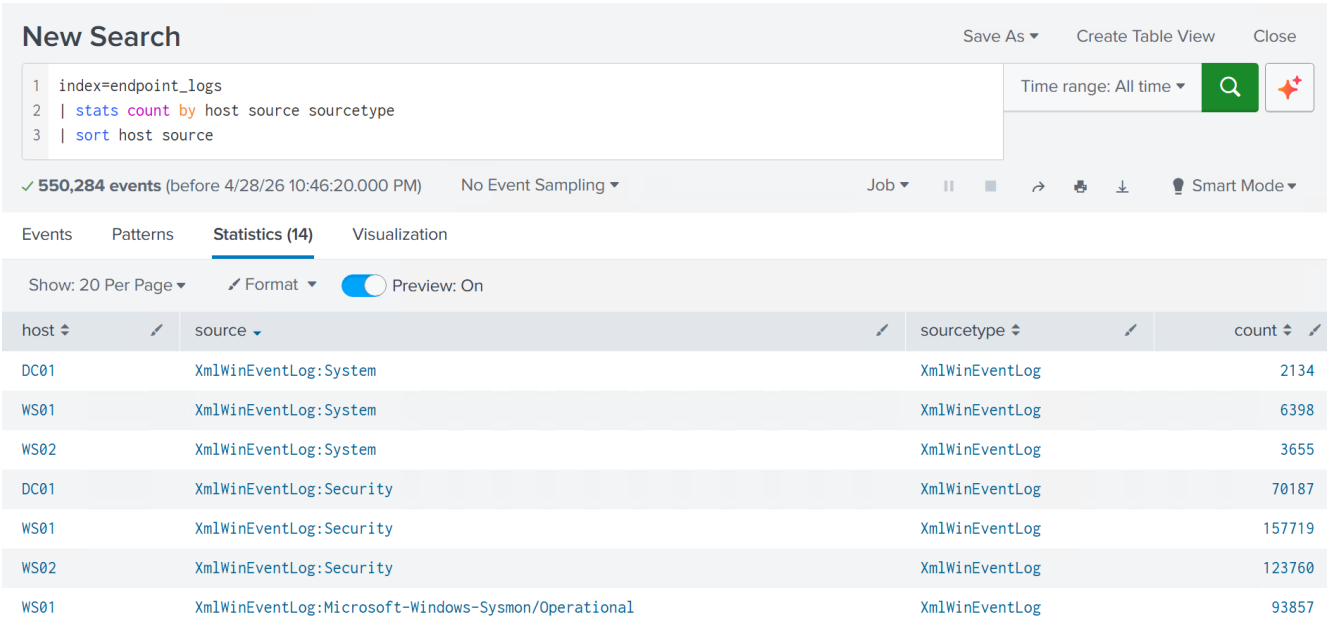
Компонент	**Роль у розділі 3**	**Практичне значення**
KALI01	Вузол моделювання атак	Створює контрольовану мережеву активність щодо Windows-вузлів
WS01 / WS02	Цільові endpoint-вузли	Формують Security- та Sysmon-події, що передаються до Splunk
DC01	Контролер домену	Формує доменний контекст, події автентифікації та Kerberos-активності
SPLUNK01	SIEM-рівень	Централізовано приймає, індексує та відображає події
Ubuntu-IR	IR-рівень з Velociraptor	Дає змогу перейти від події в SIEM до triage конкретного endpoint-вузла
SOC-аналітик	Логічна роль користувача	Виконує пошук у Splunk та перевірку endpoint у Velociraptor

3.2 Перевірка повноти телеметрії перед сценаріями атак

Перед виконанням контрольованих атакувальних дій було перевірено, чи всі потрібні джерела журналів надходять до індексу endpoint_logs. Цей крок є

обов’язковим, оскільки відсутність одного з журналів може зробити подальший сценарій неповним: атака може відбутися, але SIEM не покаже потрібної події. Така перевірка відповідає загальній логіці лог-менеджменту, де важлива не тільки наявність журналів, а й їхня повнота, стабільність і придатність до аналізу [2, 3].

У Splunk було виконано агрегований пошук за host, source та sourcetype. Очікуваним результатом було надходження Security, System і Application з DC01, WS01 та WS02, а також Microsoft-Windows-Sysmon/Operational з робочих станцій WS01 і WS02. Саме така конфігурація відповідає ролям вузлів: DC01 формує доменні події, а WS01 і WS02 додатково дають поведінкову endpoint-телеметрію через Sysmon [4, 5, 8].



host	source	sourcetype	count
DC01	XmlWinEventLog:System	XmlWinEventLog	2134
WS01	XmlWinEventLog:System	XmlWinEventLog	6398
WS02	XmlWinEventLog:System	XmlWinEventLog	3655
DC01	XmlWinEventLog:Security	XmlWinEventLog	70187
WS01	XmlWinEventLog:Security	XmlWinEventLog	157719
WS02	XmlWinEventLog:Security	XmlWinEventLog	123760
WS01	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	XmlWinEventLog	93857

Рисунок 3.1 — Перевірка надходження подій у Splunk за host, source та sourcetype

Отриманий результат підтверджує, що перед виконанням сценаріїв у Splunk уже надходили події з основних Windows-вузлів, а отже стенд був готовий до експериментальної перевірки. Очікувані джерела телеметрії перед виконанням сценаріїв наведено в таблиці 3.2.

Таблиця 3.2 — Очікувані джерела телеметрії перед виконанням сценаріїв

Вузол	Очікувані журнали	Значення для експериментів
DC01	Security, System, Application	Доменні події, автентифікація, Kerberos, події доступу
WS01	Security, System, Application, Sysmon	Endpoint-події, ціль для атакувальних сценаріїв і triage
WS02	Security, System, Application, Sysmon	Друга endpoint-ціль для порівняння і повторення сценаріїв
SPLUNK01	Індекс endpoint_logs	Єдина точка пошуку та аналізу подій

Наявність Sysmon має окреме значення для цього розділу. Стандартний журнал Security дозволяє бачити події входу, невдалої автентифікації, привілеїв і створення процесів, але він не завжди дає достатній поведінковий контекст. Sysmon розширює спостереження за процесами, файлами, DNS-запитами та змінами у реєстрі, а його конфігурація визначає, які саме події будуть записані у журнал [4–7].

На рівні Splunk також було важливо підтвердити, що forwarder-логіка працює коректно. У розгорнутому стенді Universal Forwarder на Windows-вузлах надсилає події до receiving instance на SPLUNK01. Це відповідає моделі Splunk, у якій легкий агент на endpoint-вузлі передає дані до централізованої системи приймання й індексації [17–21].

3.3 Сценарій 1: виявлення мережевого сканування з KALI01

Перший практичний сценарій був спрямований на перевірку того, чи може SIEM зафіксувати ознаки мережевої розвідки з боку KALI01. У цьому сценарії Kali не передає події до Splunk напряму. Він лише ініціює мережеві з’єднання до Windows-вузлів, а фактичні записи формуються на цільових системах і передаються до Splunk через Universal Forwarder [17–19].

Мережева розвідка є логічним початковим етапом багатьох атакувальних сценаріїв. У лабораторному середовищі вона була змодельована обмеженим nmap-скануванням лише потрібних службових портів. Такий формат дозволяє отримати

достатній набір подій для демонстрації detection-логіки, але не створює надмірного шуму в журналах і не перевантажує стенд.

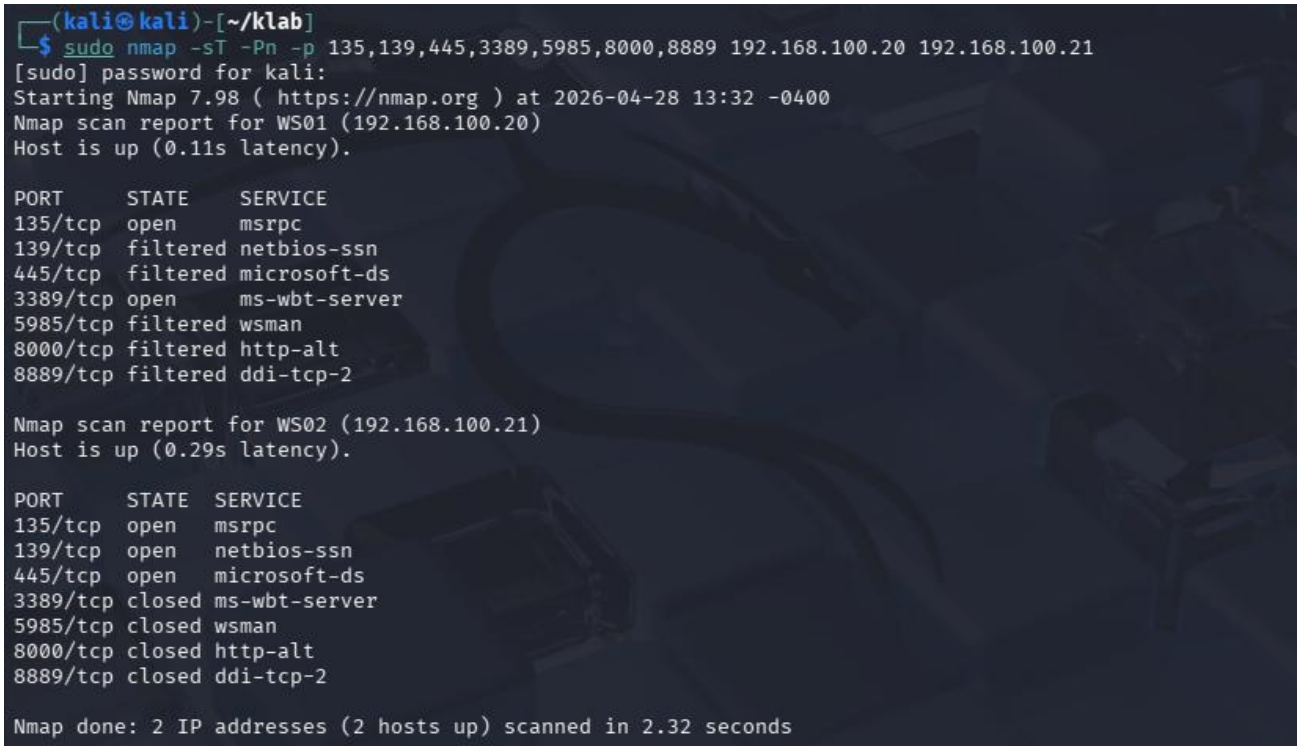


Рисунок 3.2 — Імітація сканування портів з KALI01 до WS01 та WS02

Таким чином, KALI01 створює контрольовану мережеву активність, але не є джерелом журналів для Splunk.

Для фіксації мережевих з’єднань у Windows використовувалися події Windows Filtering Platform. Зокрема, Event ID 5156 означає, що Windows Filtering Platform дозволила з’єднання. У поєднанні з IP-адресою KALI01 це дає можливість побачити, що мережеві запити надходили саме з атакувального вузла 192.168.100.50 [25].

У Splunk основний пошук виконувався за Event ID 5156 та IP-адресою KALI01. Якщо Splunk не витягує поля SourceAddress або DestPort як окремі атрибути, подію можна аналізувати через сирий текст _raw. Такий варіант не є ідеальним з погляду нормалізації, але він є допустимим для лабораторного стенда і добре показує зв’язок між мережевою активністю та відповідними Windows-подіями [2, 25].

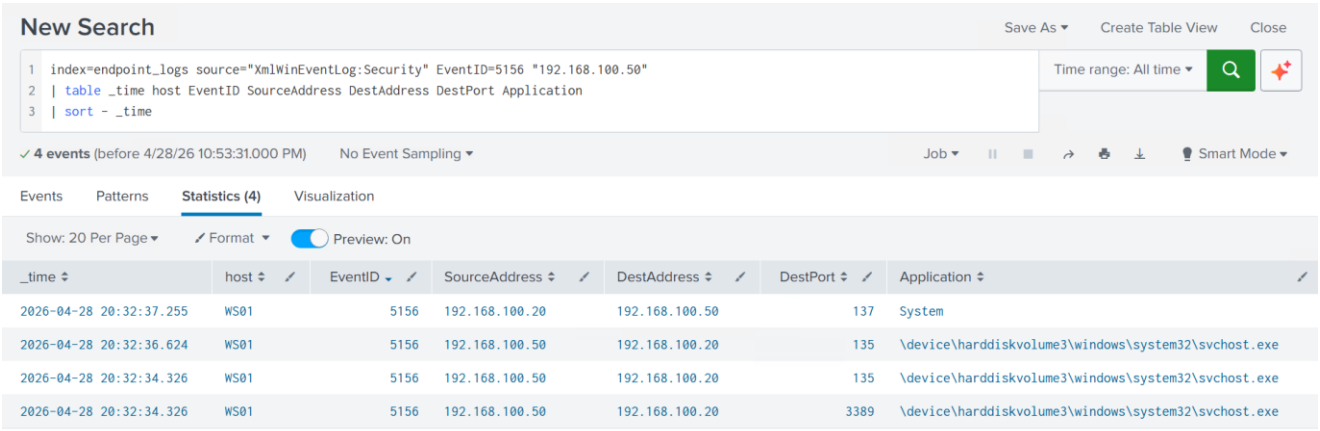


Рисунок 3.3 — Виявлення мережевого сканування з KALI01 у Splunk

Наявність IP-адреси 192.168.100.50 у результатах пошуку дозволяє пов’язати події з дією, виконаною на KALI01.

Основні ознаки мережевого сканування в межах сценарію 1 наведено в таблиці 3.3.

Таблиця 3.3 — Ознаки мережевого сканування в межах сценарію 1

Ознака	Джерело	Інтерпретація
IP 192.168.100.50	Security / WFP 5156	Джерело контрольованої активності - KALI01
Звернення до кількох портів	WFP-події або _raw	Ознака мережевої розвідки
Події на кількох Windows-вузлах	host у Splunk	Підтвердження того, що активність спрямована на кілька цілей
Відсутність прямого логування Kali у Splunk	Архітектура стенда	Splunk бачить наслідки активності на Windows-вузлах, а не Kali як джерело логів

3.4 Сценарій 2: виявлення невдалих SMB-автентифікацій з KALI01

Другий сценарій є більш показовим для SOC-аналізу, оскільки він створює події безпеки, які безпосередньо пов’язані з автентифікацією. З KALI01 було виконано кілька контрольованих невдалих спроб SMB-входу до Windows-вузла. Мета полягала не в отриманні доступу, а в перевірці того, чи будуть спроби помітні в журналі Security та чи можна буде виділити їх у Splunk як послідовність невдалих автентифікацій.

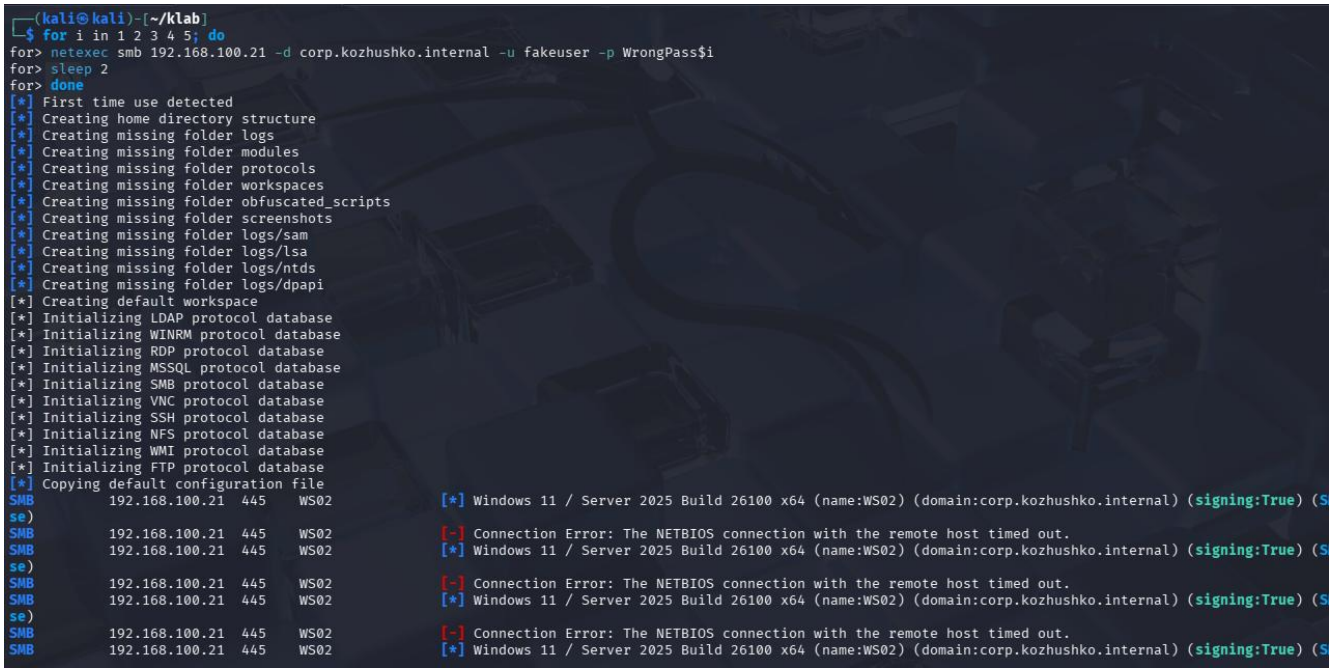


Рисунок 3.4 — Виконання контрольованих SMB-спроб з KALI01

Для такого сценарію ключовим є Event ID 4625. У документації Microsoft ця подія відповідає невдалому входу в систему. У ній можуть бути корисні поля TargetUserName, WorkstationName, IpAddress, LogonType, Status і FailureReason. Навіть якщо частина цих полів у Splunk не витягнута як окремі атрибути, наявність IP-адреси KALI01 у сирому XML-представленні події вже дозволяє пов’язати спробу входу з атакувальним вузлом [12].

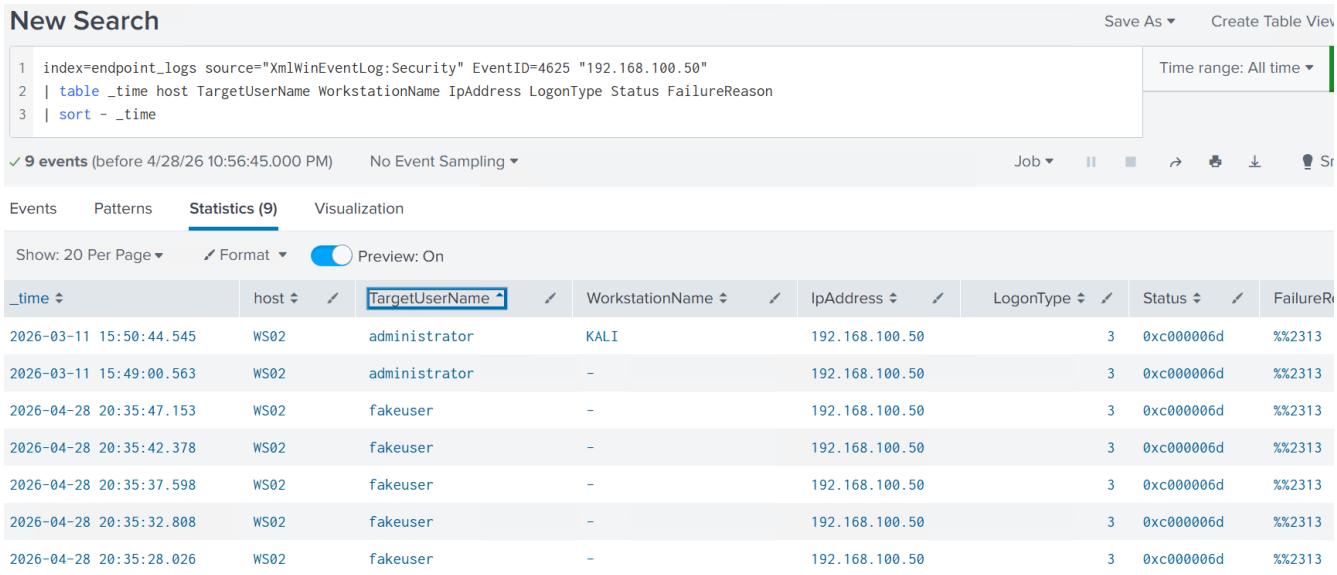


Рисунок 3.5 — Невдалі SMB-автентифікації з KALI01 за даними Event ID 4625

Інтерпретацію ключових полів подій 4625 наведено в таблиці 3.4.

Таблиця 3.4 — Інтерпретація подій 4625 у сценарії невдалих SMB-автентифікацій

Поле / ознака	Очікуване значення	Значення для triage
EventID	4625	Факт невдалої автентифікації
IpAddress	192.168.100.50	Зв’язок події з KALI01
TargetUserName	fakeuser	Обліковий запис, щодо якого виконувалася спроба входу
host	WS01 або WS02	Вузол, на який була спрямована активність
FailureReason / Status	Помилка автентифікації	Причина відмови, корисна для первинної оцінки

Сценарій було виконано обмеженою кількістю спроб. Це важливо, оскільки метою дипломної роботи є демонстрація detection-логіки, а не створення великого обсягу шуму або блокування облікових записів. У реальному SOC велика кількість подій 4625 з однієї адреси могла б бути індикатором password guessing, brute force або іншої активності, пов’язаної з підбором облікових даних [1, 12].

У межах стенда події 4625 мають особливу цінність, оскільки вони утворюють зрозумілий ланцюг: KALI01 ініціює спроби доступу, Windows-ціль фіксує невдалі входи, Universal Forwarder передає ці події до Splunk, а SOC-аналітик бачить їх централізовано. Саме така послідовність найбільш чітко демонструє ідею SOC-конвеєра [1, 2, 17].

3.5 Сценарій 3: аналіз ANONYMOUS LOGON як неоднозначної події 4624

Під час перевірки третього сценарію, пов’язаного з SMB-взаємодією, з вузла KALI01 було виконано запит до робочої станції WS02 за допомогою інструмента netexec. Команда була спрямована на адресу 192.168.100.21, що відповідає WS02, із використанням домену CORP, облікового запису socadmin та параметра --shares. Метою цієї перевірки було з’ясувати, як Windows і Splunk відобразять спробу SMB-доступу з атакувального вузла.

Результат виконання команди на KALI01 показав, що SMB-служба на WS02 доступна на порту 445, а цільовий вузол ідентифікується як WS02 у домені corp.kozhushko.internal. Також у виводі видно, що для SMB увімкнено підписування з’єднань. Водночас успішна автентифікація користувача socadmin не була

підтверджена: команда завершилася повідомленням “The NETBIOS connection with the remote host timed out”. Отже, цей етап не можна описувати як успішний вхід доменного користувача або компрометацію облікового запису.

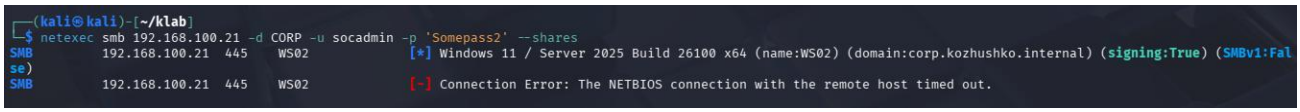
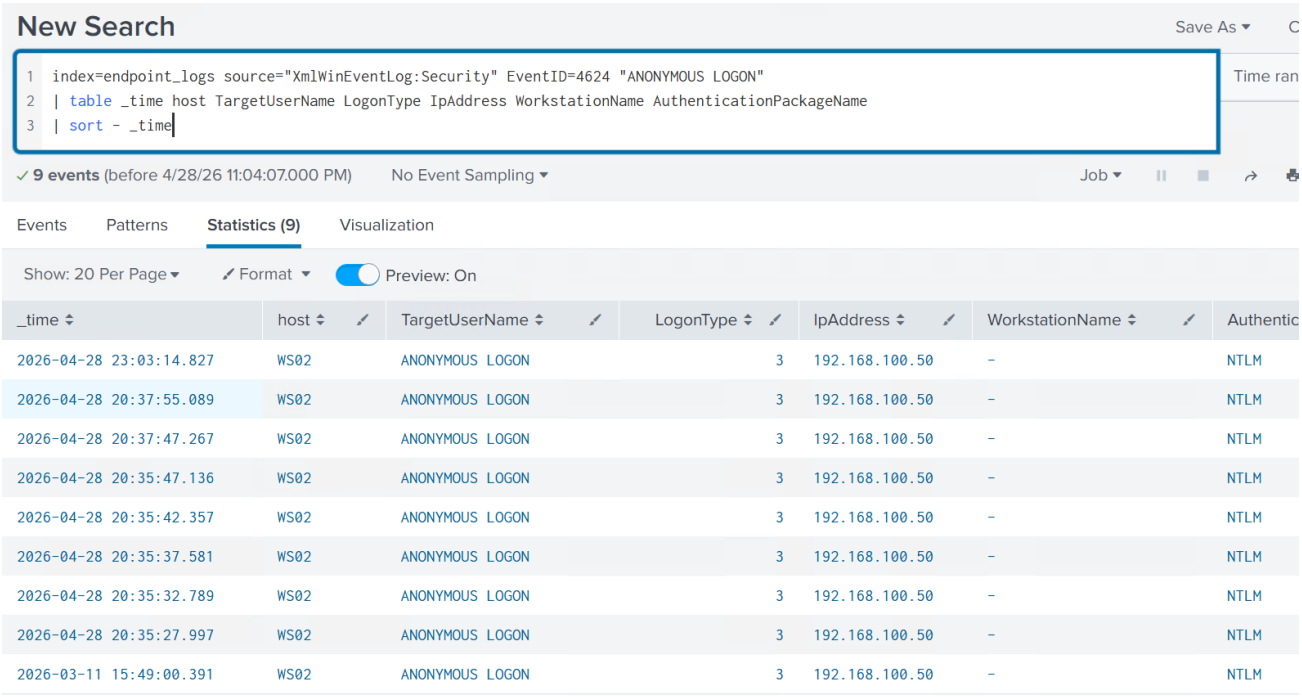


Рисунок 3.6 — Виконання SMB-запиту з KALI01 до WS02 за допомогою netexec

Результат команди підтверджує доступність SMB-служби, але не підтверджує успішну автентифікацію користувача socadmin.

Після виконання SMB-запиту в Splunk було перевірено події журналу Security на цільовому вузлі. У результаті було зафіксовано події Event ID 4624 з обліковим записом ANONYMOUS LOGON. Подія 4624 формально відповідає успішному логону, однак її реальне значення залежить від полів події: TargetUserName, LogonType, IpAddress, WorkstationName, AuthenticationPackageName та інших атрибутів [11].



_time	host	TargetUserName	LogonType	IpAddress	WorkstationName	Authentic
2026-04-28 23:03:14.827	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-04-28 20:37:55.089	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-04-28 20:37:47.267	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-04-28 20:35:47.136	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-04-28 20:35:42.357	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-04-28 20:35:37.581	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-04-28 20:35:32.789	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-04-28 20:35:27.997	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM
2026-03-11 15:49:00.391	WS02	ANONYMOUS LOGON	3	192.168.100.50	-	NTLM

Рисунок 3.7 — Подія ANONYMOUS LOGON у Splunk під час SMB-взаємодії з KALI01

На рисунку 3.7 видно, що події сформувалися на вузлі WS02, а в полі IpAddress вказано адресу 192.168.100.50, яка відповідає KALI01. Значення TargetUserName = ANONYMOUS LOGON показує, що подію не можна трактувати

як успішну автентифікацію доменного користувача socadmin. Поле LogonType = 3 вказує на мережевий тип входу, що є типовим для SMB-взаємодії, а AuthenticationPackageName = NTLM додатково підтверджує зв'язок події з Windows/SMB-механізмом автентифікації [11]. Оцінку події ANONYMOUS LOGON у межах сценарію 3 наведено в таблиці 3.5.

Таблиця 3.5 — Оцінка події ANONYMOUS LOGON у межах сценарію 3

Ознака	**Що показує**	**Як інтерпретувати**
EventID 4624	Формально успішний логон	Потребує перевірки полів події
TargetUserName = ANONYMOUS LOGON	Анонімний або службовий мережевий контекст	Не є підтвердженням успішного входу доменного користувача
IpAddress = 192.168.100.50	Зв'язок із KALI01	Показує джерело SMB-взаємодії
Відсутність очікуваного доменного користувача	Сценарій не підтвердив успішну авторизацію	Не слід описувати як компрометацію
Наявність супутніх 4625 або 5156	Додатковий контекст	Допомагає зрозуміти характер активності

Таким чином, у межах сценарію було зафіксовано не успішну атаку, а неоднозначну подію мережевого логону, пов'язану з SMB-запитом із KALI01. Вона є корисною для SOC-аналізу, оскільки показує активність атакувального вузла щодо Windows-системи, але сама по собі не підтверджує успішний вхід очікуваного доменного користувача. Коректна інтерпретація полягає в тому, що KALI01 ініціював SMB-взаємодію з WS02, а Windows зафіксувала це як мережевий логон у контексті ANONYMOUS LOGON.

Для SOC-аналітика цей сценарій є показовим, оскільки він демонструє небезпеку поверхневого аналізу подій. Якщо орієнтуватися лише на Event ID 4624, можна помилково зробити висновок про успішну автентифікацію. Якщо ж проаналізувати поля події та зіставити їх із результатом команди на KALI01, стає зрозуміло, що успішний вхід socadmin не підтверджено. Саме тому події 4624 у SMB-сценаріях потрібно перевіряти разом із подіями невдалих входів 4625, мережевими подіями Windows Filtering Platform 5156 та іншими суміжними записами [12, 25].

З практичного погляду цей результат є цінним для дипломної роботи, оскільки він показує, що SOC-конвеєр не повинен працювати як механічний перелік спрацювань. Спочатку Splunk виявляє подію, після цього аналітик перевіряє її поля, порівнює її з дією на атакувальному вузлі та лише потім робить висновок щодо реального ризику. У цьому випадку правильний висновок полягає не в підтвердженні компрометації, а в тому, що SMB-взаємодія з KALI01 створила події ANONYMOUS LOGON, які потребують додаткового контекстного аналізу [1, 2, 11].

3.6 Додаткова endpoint-телеметрія: процеси, DNS, реєстр і файли

Після аналізу мережевих і автентифікаційних сценаріїв було перевірено, яку додаткову картину дає endpoint-телеметрія. Для цього використовувалися події Security 4688 та Sysmon Event ID 1, 11, 13 і 22. Ці події не обов'язково є прямими наслідками SMB-сценаріїв, але вони демонструють здатність стенда бачити локальну поведінку на робочих станціях [4, 5, 14].

Подія 4688 у журналі Security показує факт створення нового процесу. За наявності command line process auditing вона також дозволяє бачити командний рядок, що істотно підвищує цінність події для SOC-аналітика. У межах стенда це було використано для відображення запусків whoami, hostname, ipconfig та інших контрольованих команд [10, 14].

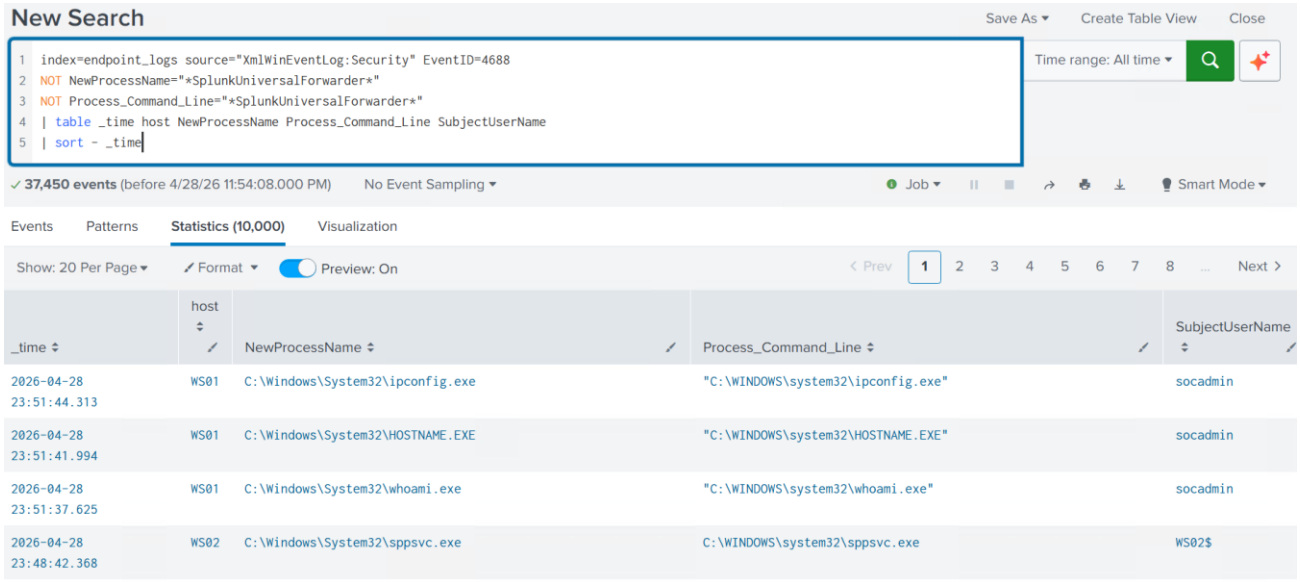


Рисунок 3.8 — Процесна активність у журналі Security (Event ID 4688)

На рисунку видно, що журнал Security може використовуватися для базового контролю запуску команд і процесів на робочій станції.

Sysmon Event ID 1 дублює частину процесної картини, але додає більше поведінкового контексту: Image, CommandLine, ParentImage, User та інші поля. Саме такі дані важливі тоді, коли потрібно перейти від факту запуску процесу до розуміння його ролі в послідовності дій на хості [4–6].

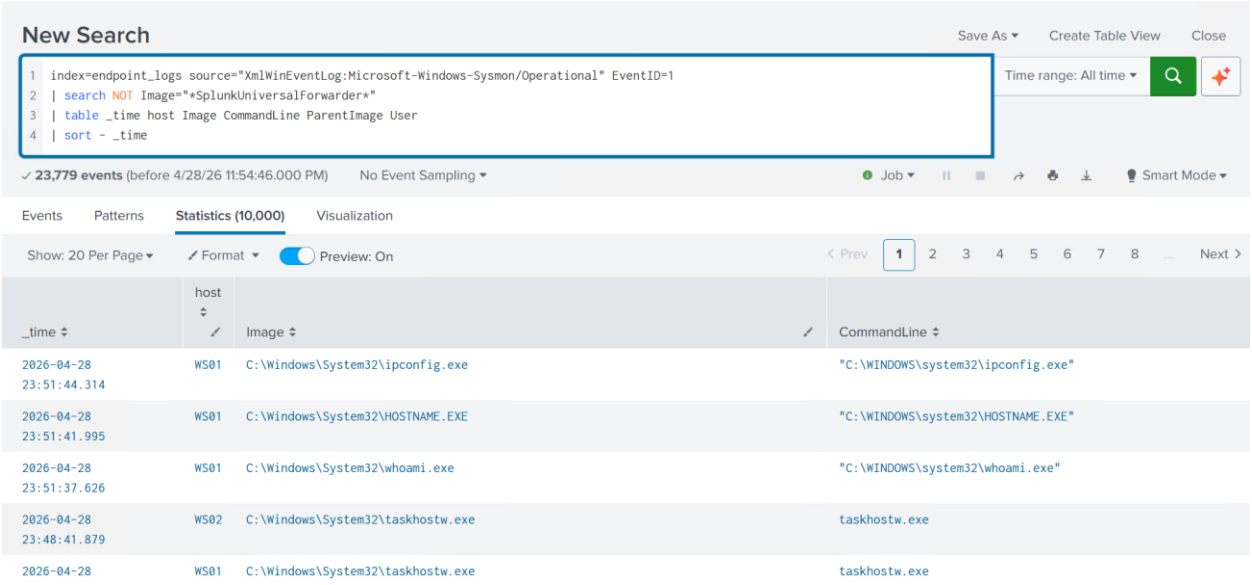


Рисунок 3.9 — Створення процесу за даними Sysmon (Event ID 1)

На відміну від Security 4688, Sysmon Event ID 1 надає розширений контекст запуску процесу, зокрема Image, CommandLine, ParentImage та User.

Події Sysmon Event ID 22, 13 і 11 відповідають DNS-запитам, змінам у реєстрі та створенню файлів. У межах дипломного стенда вони використовуються як додаткові шари видимості. DNS-події дозволяють побачити, який процес ініціював звернення до мережевого імені. Приклад таких подій наведено на рисунку 3.10.

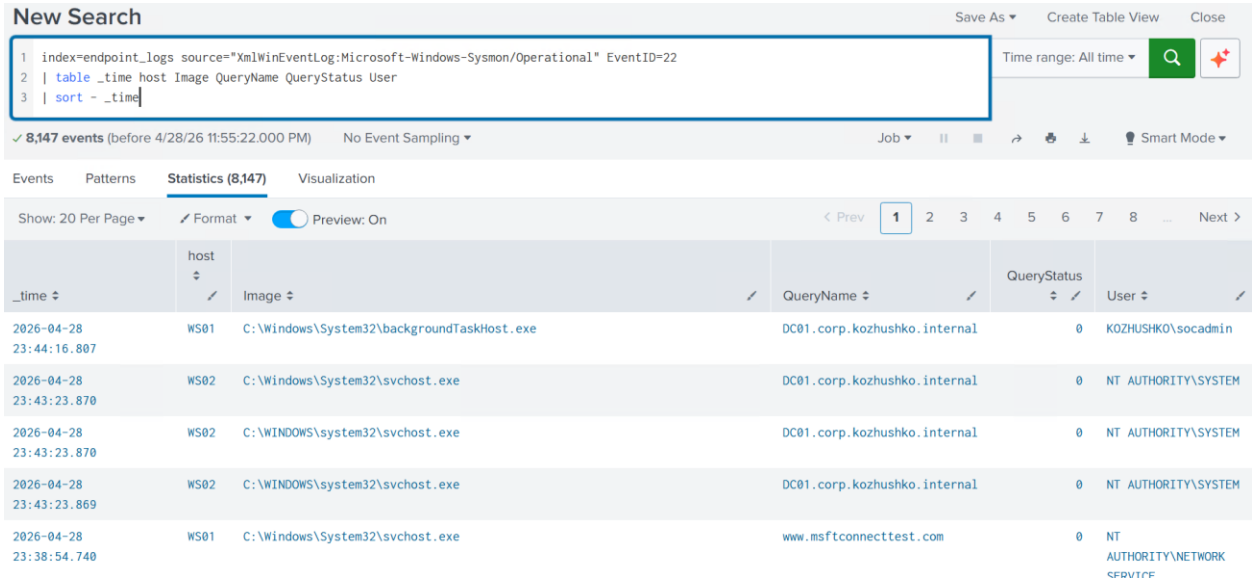


Рисунок 3.10 — DNS-активність процесів за даними Sysmon (Event ID 22)

Цей результат показує, що endpoint-телеметрія може пов’язувати DNS-запити з конкретними процесами. Події реєстру показують локальні зміни конфігурації на endpoint-вузлі. Приклад таких подій наведено на рисунку 3.11.

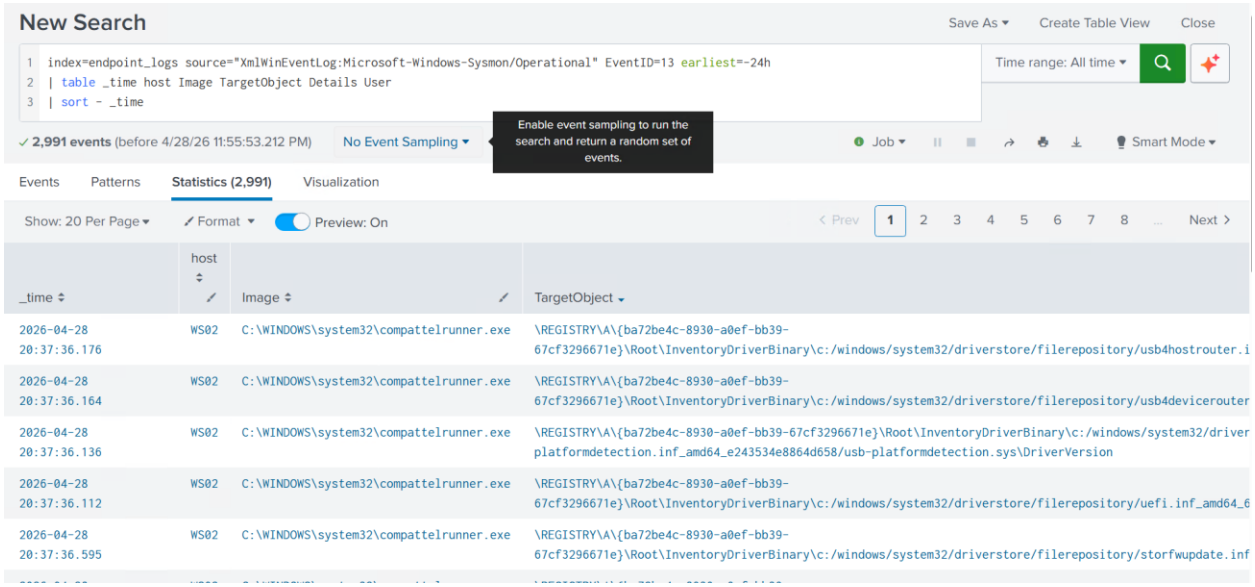


Рисунок 3.11 — Зміни у реєстрі за даними Sysmon (Event ID 13)

Такі події корисні для виявлення локальних змін конфігурації, які можуть супроводжувати підозрілу активність.

Файлові події дають змогу зафіксувати появу артефактів на диску. Приклад створення файлів за даними Sysmon наведено на рисунку 3.12.

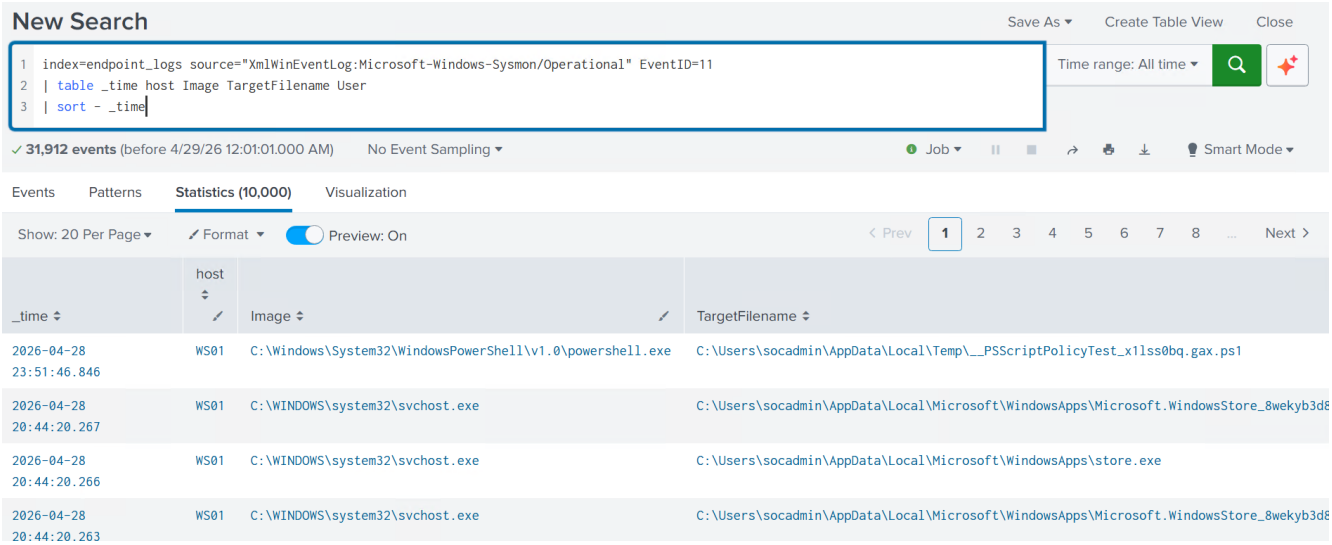


Рисунок 3.12 — Створення файлів за даними Sysmon (Event ID 11)

Події створення файлів доповнюють процесну та мережеву телеметрію, оскільки показують локальні наслідки активності на endpoint-вузлі.

Таблиця 3.6 — Endpoint-події, використані для додаткового аналізу

Джерело	Event ID	Що показує	Значення для SOC-конвеєра
Security	4688	Створення процесу	Базовий контроль запусків програм і команд
Sysmon	1	Детальний Process Create	Контекст Image, CommandLine, ParentImage, User
Sysmon	22	DNS Query	Зв’язок мережевих імен із процесами
Sysmon	13	Registry Value Set	Фіксація змін у локальній конфігурації
Sysmon	11	File Create	Виявлення створення файлів як наслідку активності

З точки зору ATT&CK, процесна активність, пов’язана з командними інтерпретаторами і PowerShell, може бути співвіднесена з технікою T1059 і підтехнікою T1059.001. У цій роботі така прив’язка використовується не для доведення шкідливості кожного запуску, а як спосіб нормалізовано описати поведінку, яку SOC може спостерігати на endpoint-рівні [26–28].

3.7 Побудова detection-to-triage ланцюга

Після виконання сценаріїв мережевого сканування та невдалих SMB-автентифікацій можна сформувати завершений detection-to-triage ланцюг. Його практичний зміст полягає в тому, що SOC-аналітик спочатку виявляє подію в Splunk, а потім переходить до Velociraptor для уточнення стану конкретного endpoint-вузла. У цьому випадку основним кандидатом для triage є WS01 або WS02 - залежно від того, на який вузол були спрямовані події 5156 або 4625 [1, 12, 25].

У такому ланцюгу Splunk виконує роль централізованої системи виявлення. Він показує факт мережевої активності з 192.168.100.50, невдалі спроби входу або неоднозначні події ANONYMOUS LOGON. Проте сам Splunk не відповідає на всі питання про фактичний стан endpoint-вузла. Для цього використовується Velociraptor, який дає можливість перевірити клієнт, його онлайн-статус, основну інформацію про ОС і результати базових артефактів [22–24].

Важливо підкреслити, що в цьому стенді Velociraptor не повинен дублювати Splunk. Його функція полягає в уточненні endpoint-контексту після того, як SIEM уже виділив вузол, що потребує уваги. Це відповідає логіці incident response: спочатку подія виявляється та пріоритизується, після чого аналітик переходить до адресної перевірки конкретної системи [1, 22, 24].

У поточній інфраструктурі клієнтами Velociraptor виступають WS01 і WS02. Відсутність DC01 серед клієнтів Velociraptor не є помилкою, оскільки контролер домену в межах стенда виконує роль джерела доменних подій для Splunk, тоді як Velociraptor використовується саме для triage робочих станцій. Такий розподіл ролей є логічним для навчального стенда і не суперечить темі роботи.

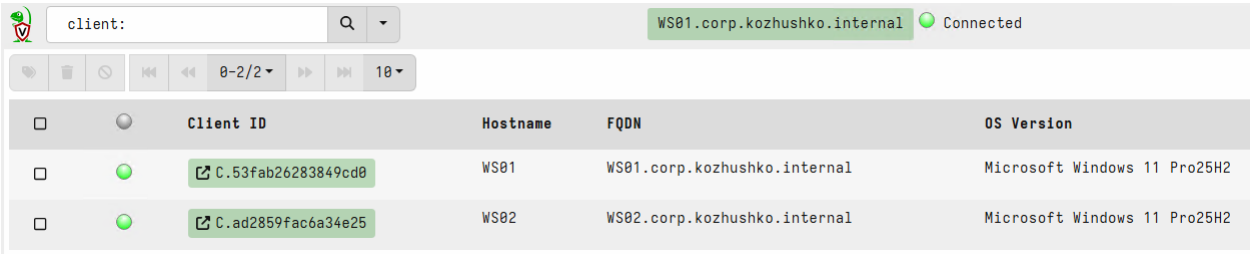


Рисунок 3.13 - Список клієнтів у Velociraptor після виявлення активності в Splunk

Наявність WS01 і WS02 у списку клієнтів підтверджує можливість переходу від події в Splunk до endpoint-перевірки в Velociraptor.

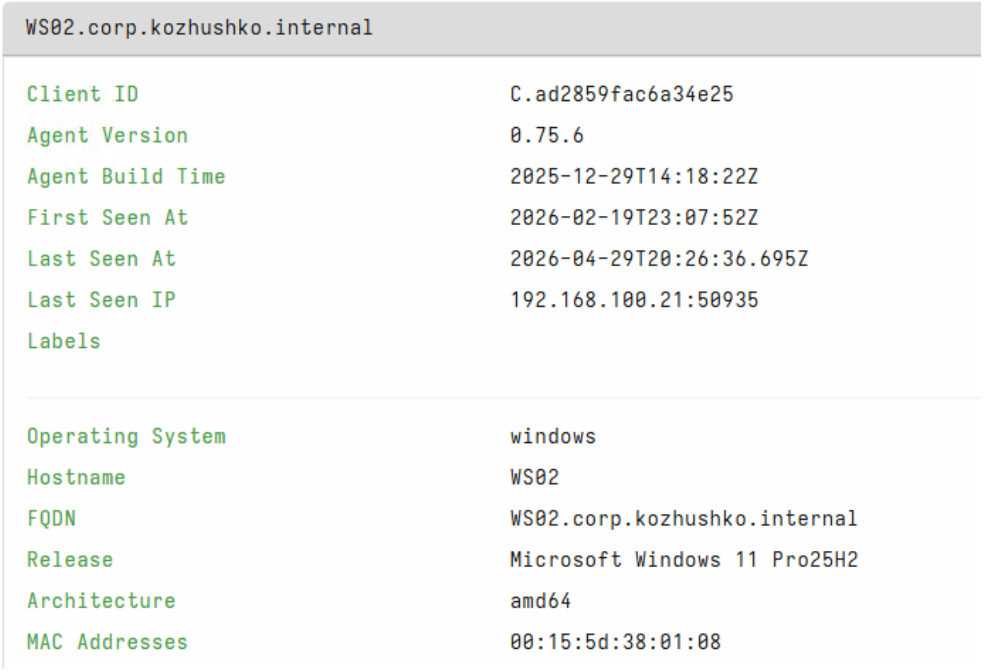


Рисунок 3.14 — Overview атакованого endpoint-вузла у Velociraptor

Overview endpoint-вузла дозволяє швидко перевірити його статус, ім’я, доменну належність та базові параметри перед запуском артефактів.

Практичний triage у цьому розділі не розглядається як повна комп’ютерна форензика. Його завдання обмежене первинною перевіркою: вибрати атакований endpoint, підтвердити його статус, переглянути базову інформацію через Generic.Client.Info і зафіксувати, що IR-рівень дійсно може бути використаний після SIEM-виявлення. Це достатньо для демонстрації SOC-конвеєра в межах бакалаврської роботи [1, 23, 24].

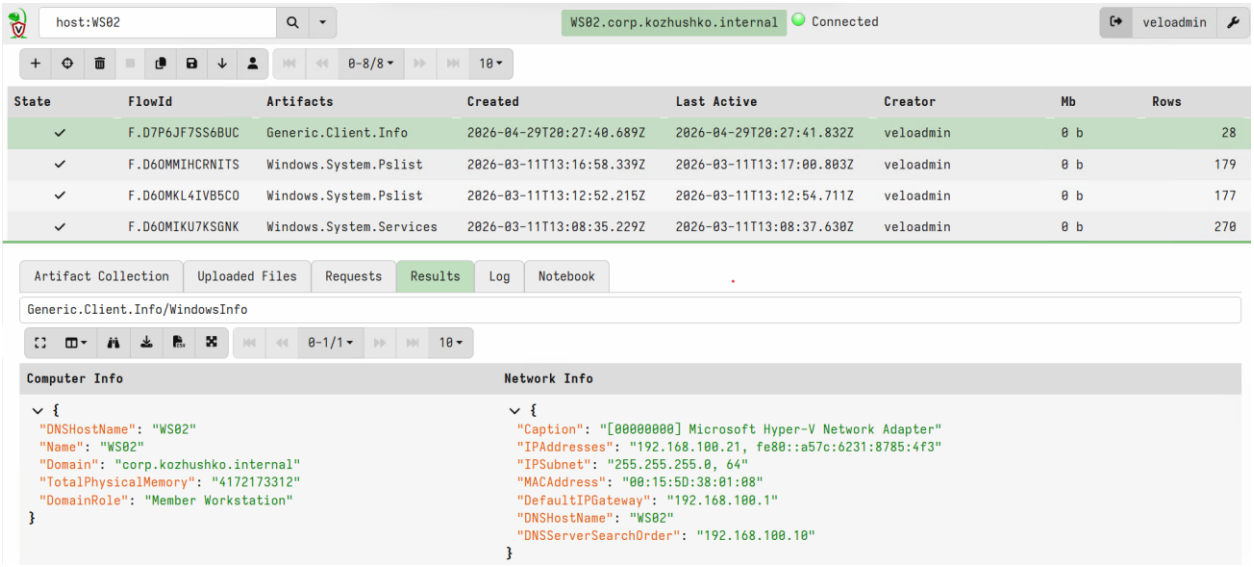


Рисунок 3.15 — Результат артефакту Generic.Client.Info для endpoint-triage

Додатковий результат артефакту Generic.Client.Info з переліком локальних профілів користувачів на вузлі WS02 наведено в додатку В.

Результат артефакту Generic.Client.Info підтверджує IP-адресу, домен, роль вузла та інші параметри, необхідні для первинного endpoint-triage.

Ланцюг detection-to-triage у межах розробленого стенда наведено в таблиці 3.7.

Таблиця 3.7 — Ланцюг detection-to-triage у межах розробленого стенда

Етап	Інструмент	Що підтверджується
Моделювання активності	KALI01	Мережеве сканування або SMB-спроби з 192.168.100.50
Виявлення події	Splunk	Події 5156, 4625 або 4624 ANONYMOUS LOGON у Security-журналі
Відбір цільового вузла	Splunk Search	Визначення host, на який була спрямована активність
Endpoint-triage	Velociraptor	Перевірка стану WS01 або WS02 як endpoint-клієнта
Фіксація результату	Документування	Підтвердження зв’язку між атакувальною активністю, SIEM і IR-рівнем

3.8 Оцінювання результатів і обмежень експерименту

Експериментальна перевірка показала, що розроблений стенд здатний фіксувати контрольовану атакувальну активність з KALI01. Сценарій мережевого сканування підтвердив, що події Windows Filtering Platform можуть бути використані для виявлення мережевих з’єднань з конкретної IP-адреси. Сценарій невдалих SMB-автентифікацій підтвердив, що Event ID 4625 є придатним джерелом для виявлення спроб доступу з неправильними обліковими даними [12, 25].

Водночас третій сценарій продемонстрував важливе обмеження: не кожна подія 4624 означає успішний вхід очікуваного користувача. Поява ANONYMOUS LOGON показує, що SIEM-аналітика потребує уважного читання полів події. У цьому сенсі сценарій 3 є не невдачею, а корисним прикладом коректного triage:

подія була зафіксована, але її не було інтерпретовано як успішну компрометацію [1, 11].

Стенд також продемонстрував корисність поєднання Security-журналу і Sysmon. Security Events добре підходять для автентифікації, привілеїв і процесної активності, тоді як Sysmon дає більш детальний endpoint-контекст. Саме разом ці джерела дозволяють переходити від простої фіксації події до поведінкового аналізу на рівні процесів, файлів, DNS і реєстру [4, 5, 9, 10, 14].

Основним обмеженням стенда є його лабораторний масштаб. Він не містить великої кількості користувачів, серверів, сегментів мережі або складних правил автоматичної кореляції. Також у роботі не використовується повноцінний EDR або комерційний SOC-пакет. Проте для цілей дипломної роботи це не є критичним недоліком, оскільки завдання полягає не в побудові production-SOC, а в демонстрації керованого SOC-конвеєра на зрозумілій інфраструктурі [1, 2, 29, 30].

Ще одне обмеження пов’язане з тим, що частина полів у Splunk може не витягуватися як окремі поля. У таких випадках аналіз виконувався через _raw або через ті атрибути, які були доступні в поточній конфігурації. Це типова особливість лабораторних SIEM-стендів і водночас корисний навчальний момент: коректна нормалізація даних є окремою задачею, яку можна розвивати в подальших версіях проєкту [2, 17].

Загалом результати експерименту підтверджують основну ідею роботи: KALI01 генерує контрольовану атакувальну активність, Windows-вузли створюють події, Splunk централізовано їх виявляє, а Velociraptor дає можливість перейти до первинного triage endpoint-вузла. Саме така послідовність і становить практичну реалізацію SOC-конвеєра в межах лабораторного стенда [1, 22, 24].

Узагальнене оцінювання результатів експериментальних сценаріїв наведено в таблиці 3.8.

Таблиця 3.8 — Оцінювання результатів експериментальних сценаріїв

Сценарій	Результат у Splunk	Висновок
Мережеве сканування з KALI01	Події WFP 5156 із IP 192.168.100.50	SIEM бачить мережеву активність атакувального вузла через журнали Windows
Невдалі SMB-автентифікації	Події 4625 із контекстом джерела	Сценарій придатний для демонстрації detection failed logons
SMB-взаємодія з ANONYMOUS LOGON	Подія 4624 з ANONYMOUS LOGON	Не підтверджує успішний доменний вхід; потребує обережної інтерпретації
Endpoint-triage	WS01/WS02 у Velociraptor	IR-рівень дозволяє перейти від SIEM-події до перевірки endpoint
Sysmon-телеметрія	Події 1, 11, 13, 22	Додає поведінковий контекст до Security-журналів

Висновки до розділу 3

У третьому розділі було проведено експериментальну перевірку розробленого SOC-конвеєра з урахуванням реальної ролі KALI01 як вузла моделювання атак. На відміну від початкового варіанту, де основний акцент робився лише на перевірці наявності журналів, оновлена логіка розділу демонструє повний шлях: атакувальна активність з Kali, фіксація подій на Windows-вузлах, централізоване виявлення у Splunk і подальший triage через Velociraptor.

Перший сценарій підтвердив, що мережеве сканування з KALI01 може бути відображене через події Windows Filtering Platform, зокрема Event ID 5156. Другий сценарій підтвердив виявлення невдалих SMB-автентифікацій за Event ID 4625. Обидва сценарії є безпечними для лабораторного середовища, але достатньо показовими для демонстрації логіки SOC-виявлення [12, 25].

Третій сценарій показав, що подія 4624 з ANONYMOUS LOGON не повинна трактуватися як успішна компрометація. Це важливий результат, оскільки він демонструє необхідність контекстного аналізу, перевірки полів події та співставлення з іншими журналами. Саме такий підхід відрізняє реальний triage від механічного реагування на номер Event ID [1, 11, 12].

Додатково було показано, що Security Events і Sysmon-події доповнюють одна одну. Події 4688 і Sysmon Event ID 1 описують процесну активність, а Event ID 22, 13 і 11 додають DNS-, registry- та file-контекст. Завдяки цьому стенд дозволяє аналізувати не лише факт мережевої або автентифікаційної активності, а й локальні дії на endpoint-рівні [4, 5, 14].

Завершальним елементом перевірки стало використання Velociraptor для первинного triage WS01 або WS02 після того, як Splunk виявив активність з боку KALI01. Таким чином, у межах роботи вдалося показати не окремий SIEM-стенд, а саме SOC-конвеєр: від моделювання атаки до централізованого виявлення та переходу до endpoint-перевірки [1, 22–24].

ВИСНОВКИ

У кваліфікаційній роботі було розроблено та експериментально перевірено лабораторний SOC-конвеєр моніторингу та тріажу інцидентів із застосуванням SIEM та endpoint-телеметрії. У межах роботи було показано, що базову логіку SOC можна реалізувати не лише у великій виробничій інфраструктурі, а й у керованому лабораторному середовищі, якщо в ньому наявні джерела подій, централізований збір журналів, інструмент аналітичного пошуку та засіб первинної перевірки endpoint-вузлів.

У теоретичній частині роботи було розглянуто поняття SOC, роль SIEM у централізованому зборі та аналізі подій безпеки, значення endpoint-телеметрії, а також місце triage у процесі моніторингу та реагування на інциденти. Встановлено, що SIEM не слід розглядати як повну заміну incident response, оскільки його основне призначення полягає у виявленні, пошуку, фільтрації та зіставленні подій. Для уточнення стану конкретного вузла після виявлення підозрілої активності доцільно використовувати окремий IR-рівень.

У практичній частині було спроєктовано лабораторний стенд, що включає контролер домену DC01, робочі станції WS01 і WS02, SIEM-вузол SPLUNK01, IR-вузол Ubuntu-IR із Velociraptor та вузол KALI01 для моделювання контрольованої атакувальної активності. Такий розподіл ролей дозволив відтворити базову

корпоративну інфраструктуру, у якій Windows-вузли формують події, Splunk Enterprise централізовано їх приймає та індексує, а Velociraptor забезпечує можливість переходу до endpoint-triage.

Під час розгортання стенда було налаштовано домен corp.kozhushko.internal, збір журналів Windows Security, System, Application та Sysmon, а також пересилання подій через Splunk Universal Forwarder до індексу endpoint_logs. Окремо було перевірено роботу Sysmon, параметри auditpol, відкриті порти Splunk і доступність клієнтів Velociraptor. Це підтвердило, що побудоване середовище придатне для подальшої експериментальної перевірки detection-to-triage сценаріїв.

В експериментальній частині було змодельовано кілька безпечних сценаріїв активності з KALI01. Сценарій мережевого сканування показав, що Windows Filtering Platform Event ID 5156 може використовуватися для виявлення мережевих з'єднань з конкретної IP-адреси. Сценарій невдалих SMB-автентифікацій підтвердив, що Event ID 4625 є придатним джерелом для виявлення спроб доступу з помилковими обліковими даними. Сценарій з ANONYMOUS LOGON продемонстрував важливість контекстного аналізу, оскільки подія 4624 не завжди означає успішний вхід очікуваного доменного користувача.

Додатково було показано практичну цінність Sysmon як джерела розширеної endpoint-телеметрії. Події Sysmon Event ID 1, 11, 13 і 22 дозволяють аналізувати створення процесів, файлову активність, зміни у реєстрі та DNS-запити. У поєднанні з Windows Security Events така телеметрія дає змогу перейти від аналізу окремих Event ID до побудови більш повної поведінкової картини на рівні кінцевої точки.

Завершальним елементом роботи стало використання Velociraptor для первинного endpoint-triage після виявлення подій у Splunk. Це дозволило продемонструвати зв'язок між SIEM-рівнем і IR-рівнем: спочатку аналітик визначає підозрілий вузол за подіями у Splunk, після чого уточнює його стан через Velociraptor. Таким чином, у роботі було реалізовано не просто збір логів, а саме SOC-конвеєр: від контрольованої активності до централізованого виявлення, аналізу та первинної перевірки endpoint-вузла.

Практичне значення роботи полягає в тому, що розроблений стенд може використовуватися як навчальна платформа для відпрацювання базових сценаріїв SOC-моніторингу, аналізу Windows-подій, роботи зі Splunk-запитами та первинного triage за допомогою Velociraptor. Обмеженням роботи є лабораторний масштаб середовища, відсутність повноцінного EDR-рішення та складних автоматизованих правил кореляції. Водночас для бакалаврської кваліфікаційної роботи побудований стенд достатньо повно демонструє принципи роботи SOC-конвеєра та може бути розширений у майбутньому за рахунок додавання нових сценаріїв, правил виявлення, дашбордів і більш складної автоматизації реагування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cyber Risk Management URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

2. Kent K., Souppaya M. Guide to Computer Security Log Management URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf.

3. Dempsey K., Chawla N., Johnson R. et al. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf.

4. Microsoft. Sysmon Overview URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/overview.

5. Microsoft. Understanding Sysmon events URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/sysmon-events.

6. Microsoft. Read and tune Sysmon events URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/read-tune-sysmon-events.

7. Microsoft. Understanding Sysmon configuration files URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/sysmon-configuration-files.

8. Microsoft. Sysmon in Windows URL: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/sysmon.

9. Microsoft. Advanced Audit Policy Configuration settings URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/advanced-audit-policy-configuration.

10. Microsoft. Command line process auditing URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing.

11. Microsoft. 4624(S): An account was successfully logged on URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624.

12. Microsoft. 4625(F): An account failed to log on URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4625.

13. Microsoft. 4672(S): Special privileges assigned to new logon URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4672.

14. Microsoft. 4688(S): A new process has been created URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4688.

15. Microsoft. 4768(S, F): A Kerberos authentication ticket (TGT) was requested. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4768.

16. Microsoft. 4769(S, F): A Kerberos service ticket was requested URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4769.

17. Splunk Inc. About forwarding and receiving URL: https://help.splunk.com/en/splunk-enterprise/forward-and-process-data/forwarding-and-receiving-data.

18. Splunk Inc. The universal forwarder URL: https://help.splunk.com/en/data-management/transform-and-route-data/perform-basic-data-processing/process-data-with-forwarders/the-universal-forwarder.

19. Splunk Inc. Configure the universal forwarder using configuration files URL: https://help.splunk.com/en/splunk-enterprise/forward-and-process-data/forwarding-and-receiving-data/9.4/configure-forwarders/configure-the-universal-forwarder-using-configuration-files.

20. Splunk Inc. outputs.conf URL: https://help.splunk.com/en/data-management/splunk-enterprise-admin-manual/9.4/configuration-file-reference/9.4.1-configuration-file-reference/outputs.conf.

21. Splunk Inc. Enable a receiver URL: https://help.splunk.com/en/splunk-enterprise/forward-and-process-data/forwarding-and-receiving-data/9.1/deploy-heavy-and-light-forwarders/enable-a-receiver (дата звернення: 19.04.2026).

22. Velocidex. Welcome URL: https://docs.velociraptor.app/.

23. Velocidex. Overview URL: https://docs.velociraptor.app/docs/overview/.

24. Velocidex. Velociraptor Artifacts URL: https://docs.velociraptor.app/docs/artifacts/.

25. Microsoft. 5156(S): The Windows Filtering Platform has permitted a connection URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5156.

26. MITRE Corporation. Enterprise Matrix URL: https://attack.mitre.org/matrices/.

27. MITRE Corporation. Command and Scripting Interpreter (T1059) URL: https://attack.mitre.org/techniques/T1059/.

28. MITRE Corporation. PowerShell (T1059.001) URL: https://attack.mitre.org/techniques/T1059/001/.

29. Савицька Л. А., Коробейнікова Т. І., Волос О. П., Тарновський М. Г. Метод та засіб моніторингу безпеки в комп’ютерній мережі засобами SIEM URL: https://itce.vntu.edu.ua/index.php/itce/article/view/968.

30. Субач І., Кубрак В. Лексографічний метод рішення багатокритеріальної задачі вибору SIEM-системи для побудови ситуаційного центру з кібербезпеки, URL: https://its.iszzi.kpi.ua/article/download/283535/278322/655300.

Додаток А

Відповідність сценаріїв роботи елементам MITRE ATT&CK



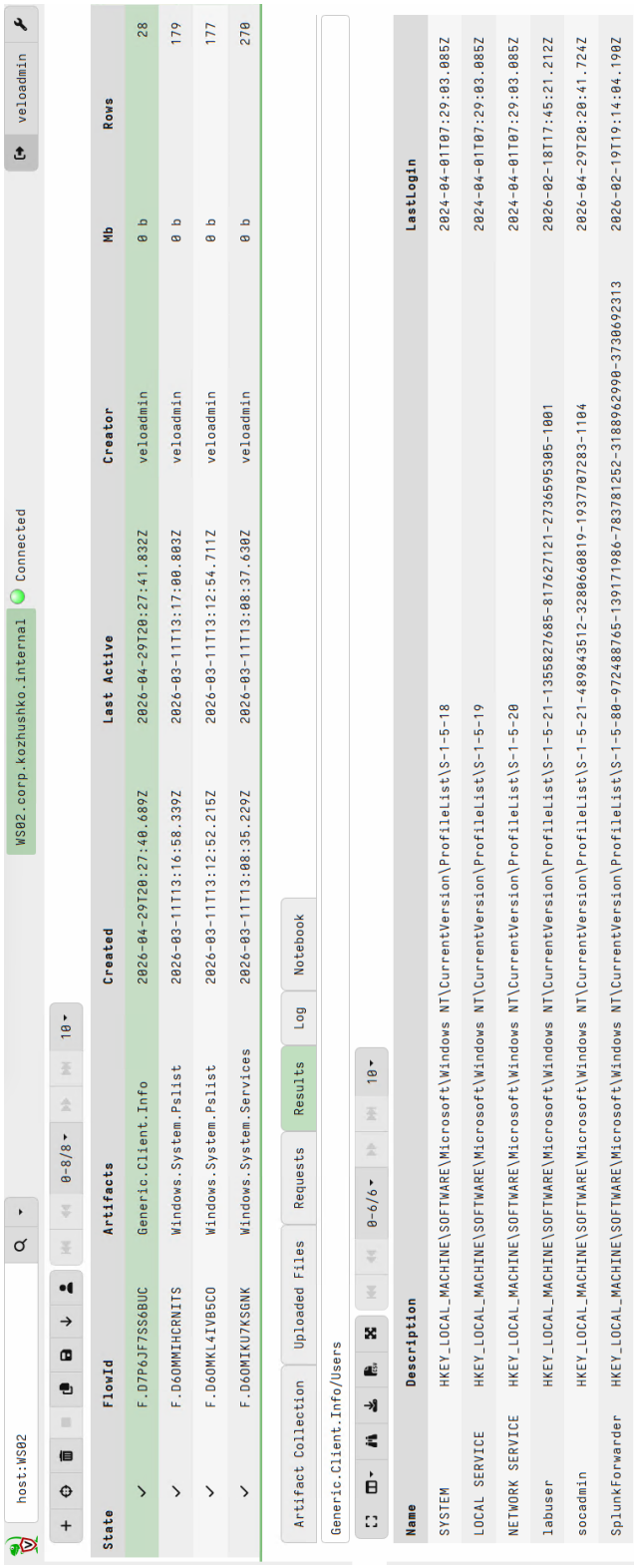
Додаток Б

Повний вивід налаштувань auditpol на робочій станції

```
PS C:\WINDOWS\system32> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
  Access Rights                           No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        Success
  Process Termination                     Success
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
  Token Right Adjusted Events             No Auditing
Policy Change
  Audit Policy Change                     No Auditing
  Authentication Policy Change            No Auditing
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             No Auditing
  Security Group Management               No Auditing
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         No Auditing
  User Account Management                 Success
DS Access
  Directory Service Access                No Auditing
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   Success and Failure
```

Додаток В

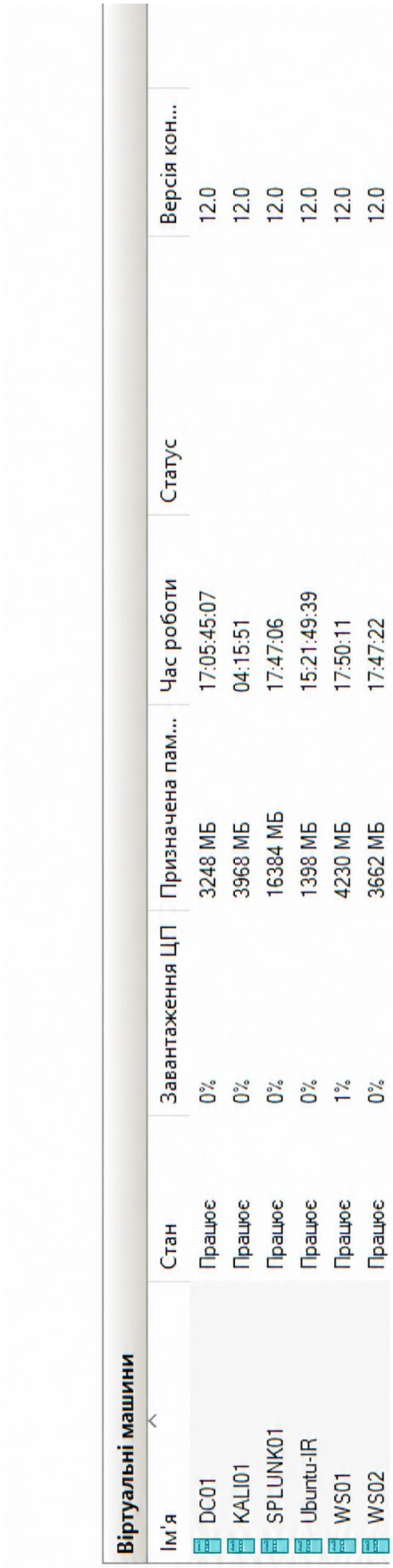
Результат Generic.Client.Info/Users для вузла WS02 у Velociraptor



На додатку В наведено додатковий результат артефакту Generic.Client.Info, який відображає локальні профілі користувачів на endpoint-вузлі WS02. Ці дані можуть використовуватися як допоміжний контекст під час endpoint-triage.

Додаток Г

Перелік віртуальних машин лабораторного SOC-стенда у Hyper-V



Додаток Ґ

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)



ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

на тему:

«SOC-конвеєр моніторингу та тріажу інцидентів із застосуванням SIEM та endpoint-телеметрії»

Виконав студент групи КІД-41
Андрій КОЖУШКО

Керівник кваліфікаційної роботи:
Кирило СОКОЛОВ, PhD

Київ – 2026

1

ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Мета, об'єкт і предмет дослідження

Мета роботи

розробити та експериментально перевірити лабораторний SOC-конвеєр моніторингу та triage інцидентів із застосуванням SIEM та endpoint-телеметрії.

Об'єкт дослідження

процес моніторингу, виявлення та первинного triage подій безпеки в корпоративній інфраструктурі.

Предмет дослідження

методи та засоби побудови лабораторного SOC-конвеєра на основі Splunk Enterprise, Windows Event Logs, Sysmon, Splunk Universal Forwarder, Velociraptor та контрольованої активності з KALI01.

2

ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Актуальність теми

Проблема не у відсутності логів, а в їх централізованій інтерпретації

корпоративні вузли щодня формують велику кількість подій Security, System, Application та Sysmon;
ручний перегляд журналів на кожному вузлі не масштабується і не дає повної картини;
SIEM централізує події, але не замінює endpoint-triage та incident response;
зв'язка Splunk + Velociraptor дозволяє перейти від події в SIEM до перевірки конкретного endpoint-вузла.

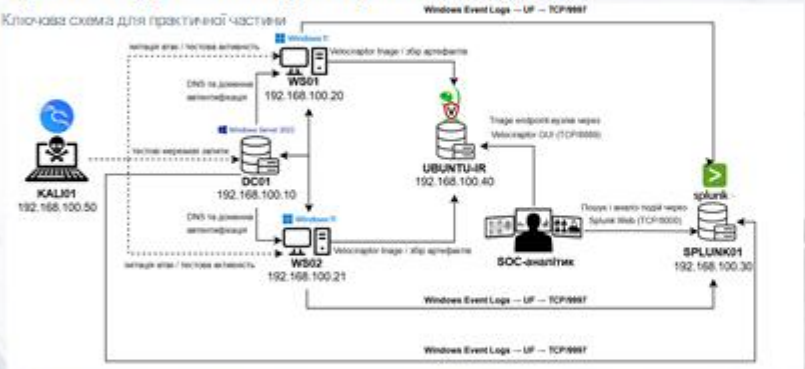
SIEM-рівень	endpoint telemetry	IR-рівень	моделювання
Splunk	Windows + Sysmon	Velociraptor	KALI01

3

ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Архітектура лабораторного стенда

Ключова схема для практичної частини



DC01 — домен, DNS, доменні події;
WS01/WS02 — endpoint-вузли з Windows Event Logs та Sysmon;
SPLUNK01 — централізоване приймання та пошук подій;
Ubuntu-IR — Velociraptor для endpoint-triage;
KALI01 — контрольована атакувальна активність.

4


ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ
Збір endpoint-телеметрії
Перед сценаріями перевірено повноту надходження подій до Splunk
index=endpoint_logs
| stats count by host source sourcetype
| sort host source
DC01: Security / System / Application;
WS01, WS02: Security / System / Application / Sysmon;
передача через Splunk Universal Forwarder;
цільовий індекс: endpoint_logs.
host source sourcetype count
DC01 XmlWinEventLog:System XmlWinEventLog 2134
WS01 XmlWinEventLog:System XmlWinEventLog 6398
WS02 XmlWinEventLog:System XmlWinEventLog 3655
DC01 XmlWinEventLog:Security XmlWinEventLog 70187
WS01 XmlWinEventLog:Security XmlWinEventLog 157719
WS02 XmlWinEventLog:Security XmlWinEventLog 123760
WS01 XmlWinEventLog:Microsoft-Windows-Sysmon/Operational XmlWinEventLog 93857
Висновок: телеметрія з основних Windows-вузлів надходить до Splunk і придатна для сценаріїв виявлення.
5


ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ
Сценарії експериментальної перевірки
На цьому слайді лише логіка сценаріїв; повні результати винесені на окремі слайди
Сценарій 1
Мережеве сканування з KALI01
джерело: 192.168.100.50
цілі: WS01 / WS02
очікуваний сигнал: WFP 5156
Сценарій 2
Невдалі SMB-автентифікації
джерело: KALI01
ціль: WS02
очікуваний сигнал: Event ID 4625
Сценарій 3
SMB та ANONYMOUS LOGON
джерело: KALI01
ціль: WS02
сигнал: 4624 ANONYMOUS LOGON
Принцип: Kali створює активність, Windows-вузли формують події, Splunk їх виявляє, Velociraptor використовується для уточнення endpoint-контексту.
6

ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Результат 1: виявлення мережевого сканування

Event ID 5156 показує дозволені мережеві з'єднання

```
index=endpoint_logs source="XmlWinEventLog:Security" EventID=5156 "192.168.100.50"
| table _time host EventID SourceAddress DestAddress DestPort Application
```

_time	host	EventID	SourceAddress	DestAddress	DestPort	Application
2026-04-28 20:32:37.255	WS01	5156	192.168.100.20	192.168.100.50	137	System
2026-04-28 20:32:36.624	WS01	5156	192.168.100.50	192.168.100.20	135	\device\harddiskvolume3\windows\system32\svchost.exe
2026-04-28 20:32:34.326	WS01	5156	192.168.100.50	192.168.100.20	135	\device\harddiskvolume3\windows\system32\svchost.exe
2026-04-28 20:32:34.326	WS01	5156	192.168.100.50	192.168.100.20	3389	\device\harddiskvolume3\windows\system32\svchost.exe

у результатах видно IP-адресу KALI01 — 192.168.100.50;
події сформовані на Windows-вузлі, а не на Kali;
Splunk дозволяє пов'язати мережеву активність із конкретним джерелом.

7

ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Результат 2: невдалі SMB-автентифікації

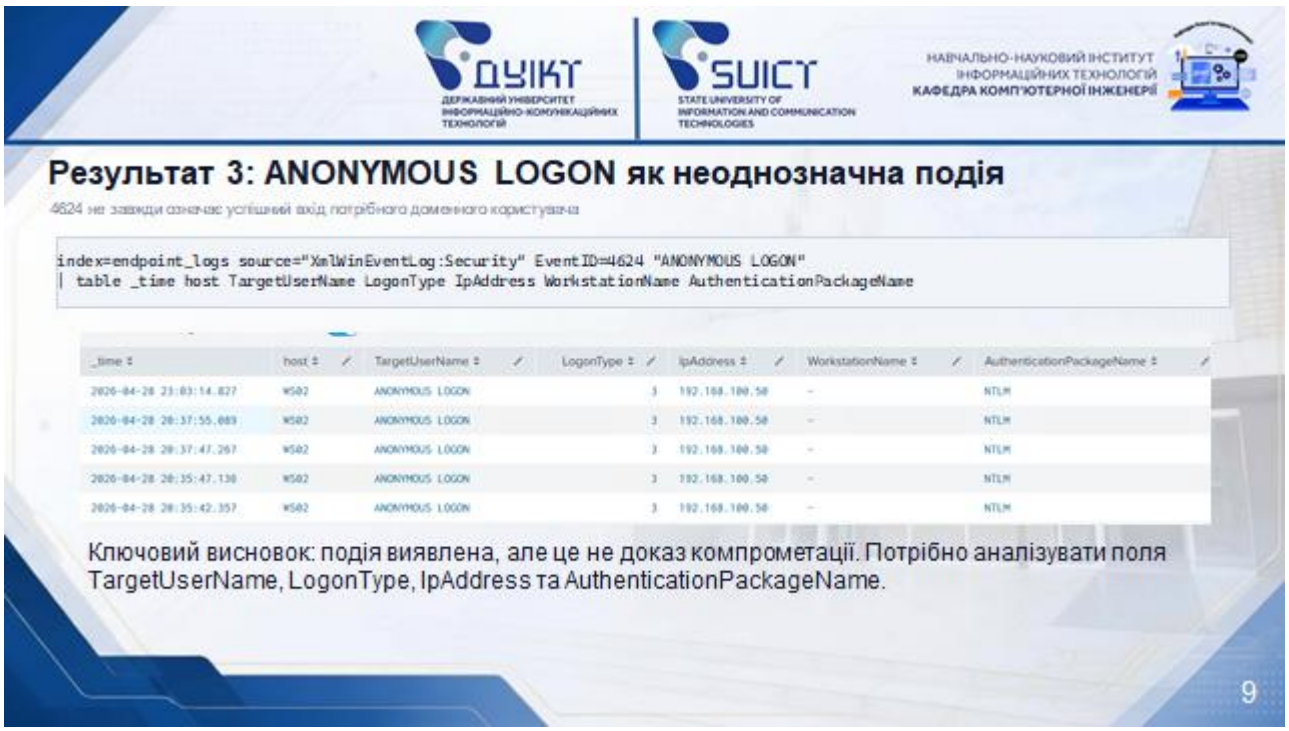
Event ID 4625 використано як сигнал failed logon

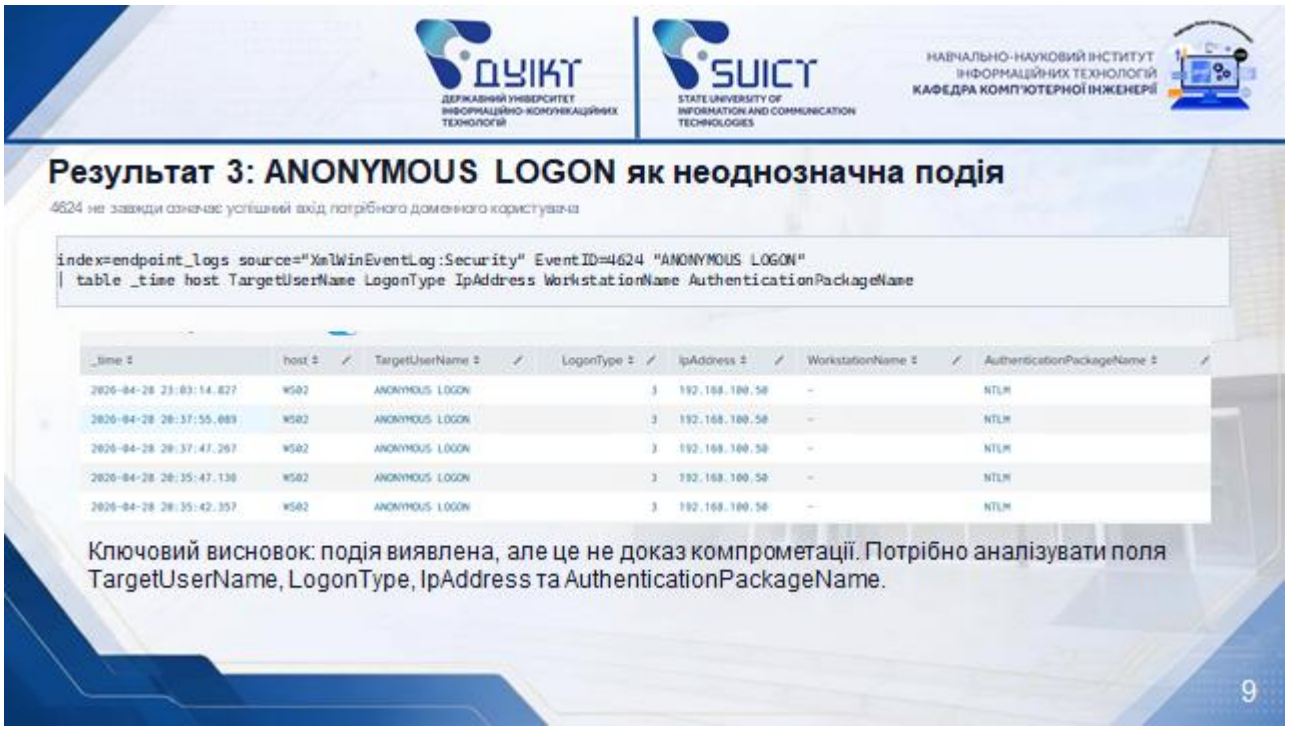
```
index=endpoint_logs source="XmlWinEventLog:Security" EventID=4625 "192.168.100.50"
| table _time host TargetUserName WorkstationName IpAddress LogonType Status FailureReason
```

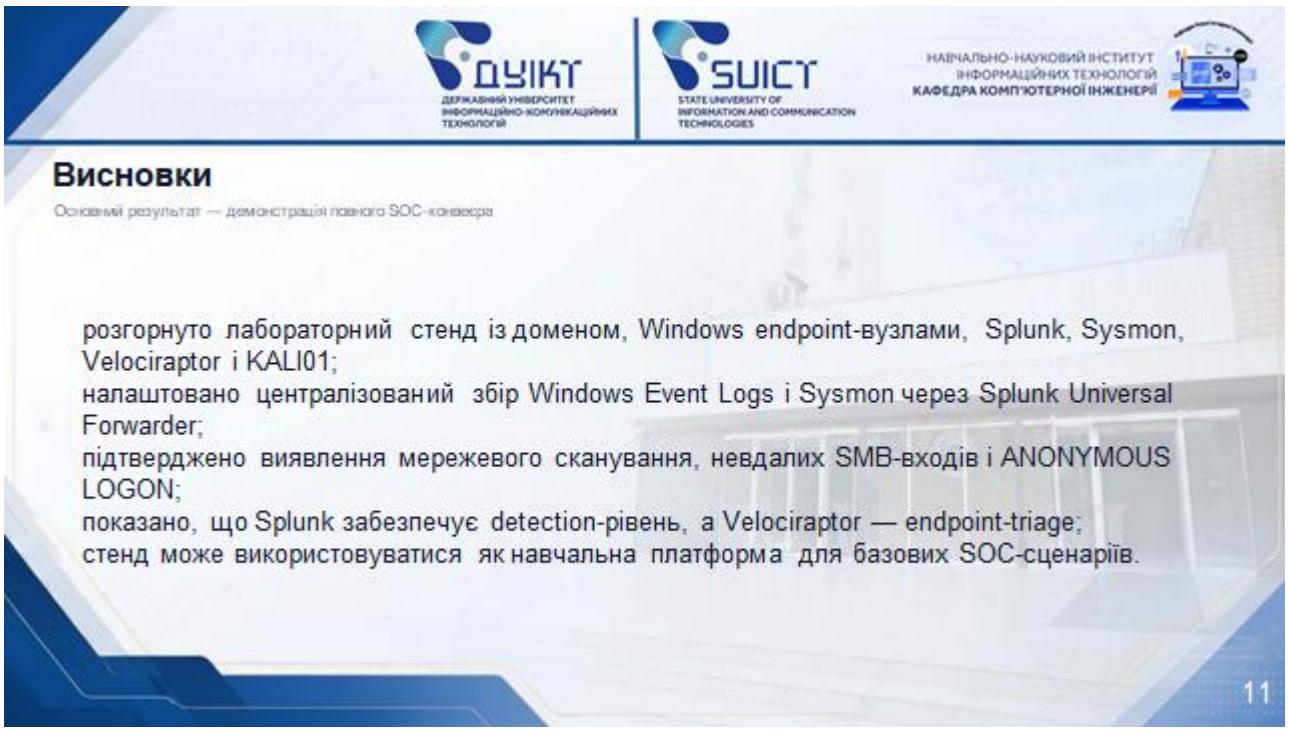
_time	host	TargetUserName	WorkstationName	IpAddress	LogonType	Status	FailureReason
2026-03-11 15:50:46.545	WS02	administrator	KALI	192.168.100.50	3	0xc000006d	%%2313
2026-03-11 15:49:00.563	WS02	administrator	-	192.168.100.50	3	0xc000006d	%%2313
2026-04-28 20:35:47.153	WS02	fakeuser	-	192.168.100.50	3	0xc000006d	%%2313
2026-04-28 20:35:42.378	WS02	fakeuser	-	192.168.100.50	3	0xc000006d	%%2313
2026-04-28 20:35:37.598	WS02	fakeuser	-	192.168.100.50	3	0xc000006d	%%2313
2026-04-28 20:35:32.808	WS02	fakeuser	-	192.168.100.50	3	0xc000006d	%%2313
2026-04-28 20:35:28.026	WS02	fakeuser	-	192.168.100.50	3	0xc000006d	%%2313

TargetUserName показує обліковий запис, щодо якого виконувалась спроба входу;
IpAddress = 192.168.100.50 пов'язує подію з KALI01;
LogonType = 3 вказує на мережевий тип входу.

8


ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ
Результат 3: ANONYMOUS LOGON як неоднозначна подія
4624 не завжди означає успішний вхід потрібного доменного користувача
index=endpoint_logs source="XmlWinEventLog:Security" EventID=4624 "ANONYMOUS LOGON"
| table _time host TargetUserName LogonType IpAddress WorkstationName AuthenticationPackageName
_time host TargetUserName LogonType IpAddress WorkstationName AuthenticationPackageName
2026-04-28 23:03:14.827 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:37:55.089 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:37:47.267 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:35:47.130 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:35:42.357 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
Ключовий висновок: подія виявлена, але це не доказ компрометації. Потрібно аналізувати поля TargetUserName, LogonType, IpAddress та AuthenticationPackageName.
9


ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ
Результат 3: ANONYMOUS LOGON як неоднозначна подія
4624 не завжди означає успішний вхід потрібного доменного користувача
index=endpoint_logs source="XmlWinEventLog:Security" EventID=4624 "ANONYMOUS LOGON"
| table _time host TargetUserName LogonType IpAddress WorkstationName AuthenticationPackageName
_time host TargetUserName LogonType IpAddress WorkstationName AuthenticationPackageName
2026-04-28 23:03:14.827 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:37:55.089 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:37:47.267 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:35:47.130 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
2026-04-28 20:35:42.357 WS02 ANONYMOUS LOGON 3 192.168.100.50 - NTLM
Ключовий висновок: подія виявлена, але це не доказ компрометації. Потрібно аналізувати поля TargetUserName, LogonType, IpAddress та AuthenticationPackageName.
9


ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
SUICT
STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ
Висновки
Основний результат — демонстрація повного SOC-конвеєра
розгорнуто лабораторний стенд із доменом, Windows endpoint-вузлами, Splunk, Sysmon, Velociraptor і KALI01;
налаштовано централізований збір Windows Event Logs і Sysmon через Splunk Universal Forwarder;
підтверджено виявлення мережевого сканування, невдалих SMB-входів і ANONYMOUS LOGON;
показано, що Splunk забезпечує detection-рівень, а Velociraptor — endpoint-triage;
стенд може використовуватися як навчальна платформа для базових SOC-сценаріїв.
11