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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі Splunk»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Євген ГАВРИЛОВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-44
ГАВРИЛОВ Євген
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 65 сторінок, 16 рисунків, 8 таблиць, 37 джерел.

Об'єкт дослідження – виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі Splunk.

Предмет дослідження – методи та засоби виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі Splunk.

Мета роботи визначити оптимальні підходи та методи виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі платформи Splunk.

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

Система Splunk розглядається як комплексне рішення для збору, аналізу та кореляції подій безпеки в режимі реального часу. Вона дозволяє централізовано моніторити активність кінцевих точок, що сприяє швидкому виявленню та реагуванню на інциденти безпеки, зокрема пов’язані із шкідливим програмним забезпеченням.

В роботі досліджено проблему виявлення шкідливого програмного забезпечення на кінцевих точок організації, визначено її мету та завдання. Проведено аналіз існуючих методів та засобів виявлення шкідливого програмного забезпечення кінцевих точок організації. Досліджено методи та засоби виявлення шкідливого програмного забезпечення на кінцевих точок організації на базі Splunk. Визначено призначення, основні функції та склад рішення Splunk.

На основі досліджень проведених в роботі запропоновано варіант системи на базі Splunk. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів виявлення та реагування на шкідливе програмне забезпечення на кінцевих точках організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, КІНЦЕВІ ТОЧКИ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APT — Advanced Persistent Threat

CIM — Common Information Model

COPE — Corporate-Owned, Personally-Enabled

CPU — Central Processing Unit

CVSS — Common Vulnerability Scoring System

DLP — Data Loss Prevention

EPP — Endpoint Protection Platform

ES — Enterprise Security

FIM — File Integrity Monitoring

HF — Heavy Forwarder

HIDS — Host-based Intrusion Detection System

IDS — Intrusion Detection System

IOC — Indicator of Compromise

IoT — Internet of Things

IPS — Intrusion Prevention System

ISAC — Information Sharing and Analysis Center

LF — Lightweight Forwarder

MDM — Mobile Device Management

OT — Operational Technology

RAM — Random Access Memory

SIEM — Security Information and Event Management

SOAR — Security Orchestration, Automation, and Response

SPL — Search Processing Language

SVM — Support Vector Machine

TTP — Tactics, Techniques, and Procedures

UF — Universal Forwarder

XDR — Extended Detection and Response

ВСТУП

Актуальність дослідження. У сучасних умовах глобальної цифровізації та стрімкого розвитку інформаційних технологій питання захисту кінцевих точок організації від шкідливого програмного забезпечення набуває особливої актуальності. Кінцеві точки, такі як робочі станції, сервери та мобільні пристрої, стали основною мішенню для кібератак, оскільки саме через них відбувається безпосередній доступ до інформаційних ресурсів організації. Згідно з дослідженням Cybersecurity Insiders, зовнішня площина атак постійно зростає через впровадження хмарних сервісів, інтеграцій з третіми сторонами, гібридної моделі праці та ускладнень у ланцюгах постачання. Це зумовлює необхідність глибокого розуміння як операційного, так і фінансового впливу таких вразливостей. Дослідження показує, що протягом останнього року в кібератаках на ресурси організацій використовувались: malware та ransomware (54%), скомпрометовані облікові дані (50%) і фішинг (49%). Також суттєвий вплив мають атаки через ланцюги постачання (40%) та інциденти, пов’язані з активами, доступними з Інтернету, і хмарною інфраструктурою (36%).

Актуальність даної роботи зумовлена декількома чинниками. По-перше, традиційні методи захисту, засновані на сигнатурному аналізі, демонструють недостатню ефективність проти сучасних загроз, які постійно еволюціонують та використовують різноманітні техніки обходу стандартних механізмів захисту. По-друге, зростаюча складність IT-інфраструктури сучасних організацій, поширення концепцій віддаленої роботи та BYOD (Bring Your Own Device) створюють додаткові виклики для забезпечення однорідного захисту всіх кінцевих точок. По-третє, відсутність централізованих систем моніторингу та аналізу даних безпеки з кінцевих точок обмежує можливості для своєчасного виявлення та реагування на інциденти.

Впровадження сучасних підходів до виявлення шкідливого програмного забезпечення на базі платформи Splunk дозволяє вирішити ці проблеми шляхом централізованого збору, аналізу та візуалізації даних безпеки з усіх кінцевих точок організації. Це забезпечує повну видимість подій безпеки, оперативне

виявлення загроз та швидке реагування на інциденти, що має особливе значення для захисту інформаційних ресурсів українських підприємств та установ в умовах зростаючої кількості цільових кібератак.

Об'єкт дослідження – виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі Splunk.

Предмет дослідження – методи та засоби виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі Splunk.

Мета роботи розробити варіант системи на базі рішення Splunk та рекомендації щодо застосування методів та засобів виявлення шкідливого програмного забезпечення на кінцевих точках організації.

Наукові завдання:

дослідити сутність проблеми виявлення шкідливого програмного забезпечення на кінцевих точках організації;

проаналізувати основні підходи до виявлення шкідливого програмного забезпечення на кінцевих точках організації;

проаналізувати існуючі рішення із виявлення шкідливого програмного забезпечення на кінцевих точках організації;

проаналізувати методи та засоби виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі Splunk;

запропонувати варіант системи виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі Splunk;

розробити рекомендацій щодо застосування методів та засобів виявлення шкідливого програмного забезпечення на кінцевих точках організації.

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

Практичне значення одержаних результатів: розроблено порядок виявлення та реагування на шкідливе програмне забезпечення на кінцевих точках організації, а також рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми виявлення шкідливого програмного забезпечення на кінцевих точок організації

Сучасний кіберпростір характеризується постійним зростанням числа та складності кібератак, спрямованих на кінцеві точки корпоративних мереж. Кінцеві точки, до яких належать робочі станції, ноутбуки, сервери та мобільні пристрої, формують периметр організації та представляють привабливу ціль для зловмисників. Компрометація цих пристроїв може призвести до несанкціонованого доступу до конфіденційної інформації, розповсюдження шкідливого програмного забезпечення всередині мережі та порушення цілісності роботи всієї інформаційної інфраструктури організації.

Шкідливе програмне забезпечення (malware) визначається як програмний код або програмне забезпечення, спеціально розроблене для пошкодження, порушення нормальної роботи, крадіжки даних або отримання несанкціонованого доступу до комп'ютерних систем. Сучасні зразки шкідливого програмного забезпечення використовують різноманітні техніки обходу традиційних захисних механізмів, включаючи поліморфізм, обфускацію коду та використання легітимних системних утиліт для здійснення зловмисних дій.

Результати дослідження Cybersecurity Insiders демонструють, що зовнішня площина атак постійно зростає через впровадження хмарних сервісів, інтеграцій з третіми сторонами, гібридної моделі праці та ускладнень у ланцюгах постачання. Це зумовлює необхідність глибокого розуміння як операційного, так і фінансового впливу таких вразливостей. Дослідження показує, що протягом останнього року в кібератаках на ресурси організацій використовувались: malware та ransomware (54%), скомпрометовані облікові дані (50%) і фішинг

(49%). Також суттєвий вплив мають атаки через ланцюги постачання (40%) та інциденти, пов’язані з активами, доступними з Інтернету, і хмарною інфраструктурою (36%) [2].

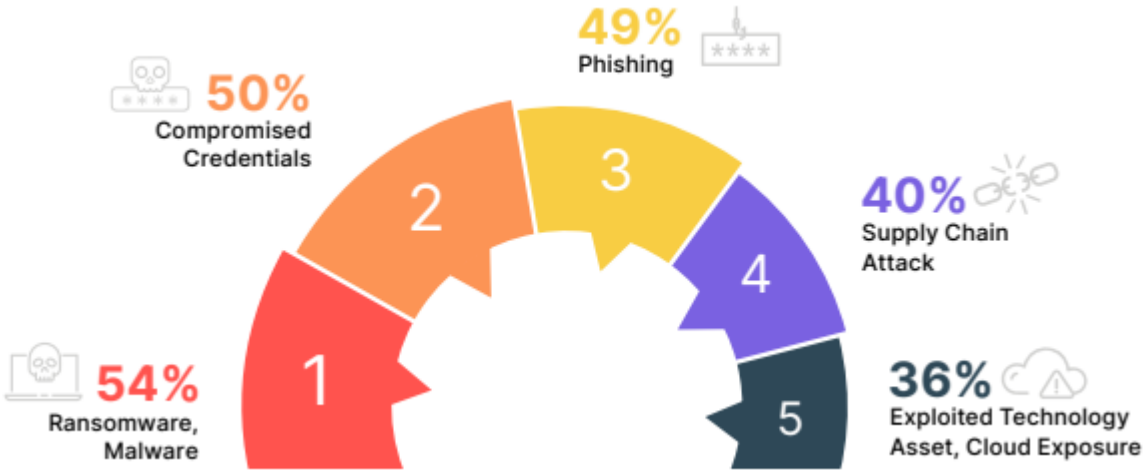

Рис. 1.1. Вектори кібератак протягом останніх 12 місяців [2]

Атаки на кінцеві точки стають більш цілеспрямованими та персоналізованими, використовуючи методи соціальної інженерії для отримання первинного доступу до цільової системи. Традиційні антивірусні рішення, засновані на сигнатурному аналізі, демонструють недостатню ефективність проти сучасних загроз, що вимагає впровадження комплексних технологій виявлення та реагування.

Кіберзлочинці постійно вдосконалюють методи зараження кінцевих пристроїв, включаючи використання фішингових повідомлень з шкідливими вкладеннями, експлуатацію вразливостей програмного забезпечення та компрометацію легітимних веб-ресурсів. Згідно з дослідженнями, середній час перебування зловмисника в мережі до виявлення (dwell time) становить близько 21 дня, що надає достатньо часу для досягнення зловмисних цілей.

Рис. 1.2. Діаграма прецедентів процесу виявлення шкідливого програмного забезпечення на кінцевих точках

Одним із факторів, що ускладнює виявлення шкідливого програмного забезпечення, є використання технік безфайлових атак (fileless malware), які функціонують виключно в оперативній пам'яті системи та не залишають слідів на жорсткому диску. Такі атаки складно виявити традиційними методами захисту, оскільки вони маскуються під легітимні системні процеси та використовують довірені операційні компоненти для виконання зловмисних дій.

Додатковою проблемою є зростаюча складність IT-інфраструктури сучасних організацій, яка включає широкий спектр пристроїв з різними операційними системами, програмним забезпеченням та рівнями захисту [2]. Гетерогенність середовища створює додаткові ускладнення для забезпечення однорідного захисту та моніторингу всіх кінцевих точок, що збільшує ризик виникнення "сліпих зон" у системі безпеки.

Проблема виявлення шкідливого програмного забезпечення посилюється тенденцією до віддаленої роботи та впровадження концепції BYOD (Bring Your Own Device), коли співробітники використовують особисті пристрої для робочих

цілей. Ці пристрої часто знаходяться поза корпоративним периметром безпеки, що ускладнює застосування централізованих політик захисту та моніторингу.

Необхідно врахувати зростаючу загрозу програм-вимагачів (ransomware), які шифрують дані на кінцевих пристроях та вимагають викуп за їх розблокування. Згідно з дослідженнями, атаки програм-вимагачів зросли на 150% за останні роки, причому організації фінансового сектора, охорони здоров'я та державних установ є першочерговими цілями таких атак [20].

Суттєвим викликом для організацій залишається недостатня видимість активності на кінцевих точках, що перешкоджає своєчасному виявленню підозрілої поведінки та потенційних загроз. Багато організацій не мають централізованої системи збору та аналізу логів з кінцевих пристроїв, що обмежує можливості для проактивного виявлення та розслідування інцидентів безпеки.

Шкідливе програмне забезпечення часто використовує механізми персистентності для забезпечення свого функціонування після перезавантаження системи, модифікуючи реєстр Windows, планувальник завдань або інші компоненти операційної системи. Виявлення таких механізмів вимагає глибокого аналізу системи та розуміння нормальної поведінки, що значно ускладнює процес ідентифікації загроз.

Актуальною проблемою залишається несвоєчасне оновлення програмного забезпечення та операційних систем на кінцевих точках, що створює вікна вразливості, які можуть бути використані зловмисниками [29]. Згідно з даними дослідження, близько 60% успішних кібератак використовують вразливості, для яких існують патчі, але вони не були встановлені на цільових системах.

Існує також проблема високої кількості помилкових спрацьовувань (false positives) під час виявлення шкідливого програмного забезпечення, що призводить до зниження ефективності роботи команд безпеки через необхідність обробки значної кількості потенційно помилкових тривог. Це створює ризик пропуску реальних інцидентів безпеки через "втому від тривог" (alert fatigue) у аналітиків безпеки.

Стало очевидно, що для ефективної протидії сучасним загрозам необхідне впровадження комплексних рішень, здатних забезпечити багаторівневий захист, проактивне виявлення та швидке реагування на інциденти безпеки на кінцевих точках. Одним з перспективних напрямків є використання платформ Endpoint Detection and Response (EDR), які поєднують функціональність моніторингу, аналізу та реагування на загрози.

1.2. Аналіз підходів до виявлення шкідливого програмного забезпечення на кінцевих точках організації

Сигнатурний аналіз залишається одним із основних підходів до виявлення шкідливого програмного забезпечення на кінцевих точках організації. Цей метод ґрунтується на порівнянні двійкових сигнатур файлів з базою даних відомих зразків шкідливого програмного забезпечення. Незважаючи на простоту реалізації та низьку кількість помилкових спрацьовувань, сигнатурний аналіз демонструє обмежену ефективність проти нових та модифікованих загроз, які не мають відповідних сигнатур у базі даних.

Евристичний аналіз розширює можливості виявлення шкідливого програмного забезпечення шляхом ідентифікації підозрілих характеристик та поведінки, навіть якщо точна сигнатура загрози відсутня в базі даних. Для реалізації цього підходу використовуються набори правил та алгоритми, що дозволяють виявляти аномальну поведінку, характерну для різних типів шкідливого програмного забезпечення [13]. Однак евристичний аналіз може призводити до збільшення кількості помилкових спрацьовувань та потребує постійного оновлення правил для відповідності сучасним загрозам.

Поведінковий аналіз фокусується на моніторингу та аналізі активності програм та процесів у системі для виявлення підозрілих дій, характерних для шкідливого програмного забезпечення. Цей підхід передбачає відстеження системних викликів, мережевих з'єднань, доступу до файлів та реєстру, а також інших аспектів поведінки програм. Поведінковий аналіз демонструє вищу ефективність проти невідомих та модифікованих загроз порівняно з сигнатурним

аналізом, однак вимагає більш складних алгоритмів та інфраструктури для реалізації.

Методи машинного навчання та штучного інтелекту все частіше застосовуються для вдосконалення процесів виявлення шкідливого програмного забезпечення. Алгоритми класифікації, такі як метод опорних векторів (SVM), дерева рішень та нейронні мережі, використовуються для автоматичного виявлення шкідливого коду на основі його статичних та динамічних характеристик [23]. Перевагою цього підходу є здатність адаптуватися до нових типів загроз шляхом навчання на нових зразках шкідливого програмного забезпечення, проте ефективність значною мірою залежить від якості та репрезентативності навчальних даних.

Аналіз аномалій базується на створенні моделей нормальної поведінки системи та виявленні відхилень від цих моделей, які можуть вказувати на наявність шкідливого програмного забезпечення. Для реалізації цього підходу застосовуються статистичні методи, алгоритми кластеризації та інші техніки аналізу даних. Аналіз аномалій потенційно здатен виявляти раніше невідомі загрози, однак точність виявлення залежить від якості моделей нормальної поведінки та здатності розрізняти легітимні зміни в активності системи від зловмисних дій.

Пісочниці (sandboxing) представляють підхід, що передбачає виконання підозрілих файлів або програм у ізольованому середовищі для спостереження за їх поведінкою без ризику для реальної системи. Цей метод дозволяє детально аналізувати дії програм, включаючи спроби модифікації системних файлів, встановлення механізмів персистентності або комунікацію з командно-контрольними серверами [7]. Пісочниці ефективні для виявлення складних загроз, проте мають обмеження, пов'язані з можливістю шкідливого програмного забезпечення виявляти середовище пісочниці та змінювати свою поведінку для уникнення детектування.

Контроль цілісності файлів (File Integrity Monitoring, FIM) передбачає регулярну перевірку цілісності системних та прикладних файлів шляхом

обчислення та порівняння контрольних сум. Зміни в файлах, які не відповідають легітимним оновленням або модифікаціям, можуть вказувати на наявність шкідливого програмного забезпечення [5]. Цей підхід особливо ефективний для виявлення модифікацій системних файлів та бібліотек, які часто використовуються для встановлення персистентності в системі.

Репутаційний аналіз базується на оцінці репутації файлів, програм та мережевих ресурсів на основі даних, зібраних з численних джерел. Файли з низькою репутацією або невідомого походження розглядаються як потенційно небезпечні та піддаються додатковому аналізу. Цей підхід дозволяє швидко ідентифікувати відомі загрози та зменшити кількість файлів, що потребують детального аналізу, однак ефективність залежить від розміру та актуальності бази даних репутацій.

Моніторинг активності в пам'яті системи є необхідним для виявлення безфайлових атак, які не залишають слідів на жорсткому диску. Цей підхід передбачає аналіз процесів, потоків, регіонів пам'яті та інших компонентів, що функціонують в оперативній пам'яті, для виявлення ознак шкідливої активності. Моніторинг пам'яті дозволяє виявляти просунуті методи атак, включаючи впровадження коду, перехоплення API та інші техніки, що використовуються сучасним шкідливим програмним забезпеченням.

Аналіз мережевого трафіку кінцевих точок є невід'ємною частиною комплексного підходу до виявлення шкідливого програмного забезпечення. Цей метод фокусується на моніторингу мережевих комунікацій пристроїв для виявлення підозрілих з'єднань, взаємодії з відомими зловмисними доменами або IP-адресами, а також аномальних патернів передачі даних. Аналіз мережевого трафіку особливо ефективний для виявлення активності командно-контрольних каналів та спроб ексфільтрації даних.

Динамічний аналіз коду передбачає виконання та моніторинг підозрілого програмного забезпечення в контрольованому середовищі для спостереження за його реальною поведінкою. На відміну від статичного аналізу, який досліджує код без його виконання, динамічний аналіз дозволяє виявляти складні техніки

обфускації та шифрування, які можуть приховувати зловмисну функціональність від статичного аналізу. Однак цей підхід вимагає значних обчислювальних ресурсів та спеціалізованих середовищ для безпечного виконання потенційно шкідливого коду.

Розширений моніторинг індикаторів компрометації (IOC) включає систематичне відстеження та аналіз артефактів, які можуть вказувати на присутність шкідливого програмного забезпечення в системі. До таких індикаторів належать хеш-суми файлів, назви процесів, ключі реєстру, мережеві індикатори та інші характеристики, асоційовані з відомими загрозами [10]. Ефективність цього підходу залежить від актуальності та повноти бази даних індикаторів компрометації, а також від можливості швидкого оновлення цієї бази у відповідь на нові загрози.

Threat hunting представляє проактивний підхід до виявлення шкідливого програмного забезпечення, що передбачає цілеспрямований пошук ознак компрометації в системі на основі гіпотез та відомих тактик, технік і процедур (TTP) зловмисників [9]. Цей метод виходить за рамки автоматизованих систем виявлення та вимагає участі кваліфікованих аналітиків безпеки, які застосовують свої знання та досвід для ідентифікації прихованих загроз. Незважаючи на ресурсомісткість, threat hunting дозволяє виявляти просунуті персистентні загрози (APT), які можуть залишатися непоміченими для автоматизованих систем.

Комплексні підходи до виявлення шкідливого програмного забезпечення, які поєднують різні методи та техніки, демонструють найвищу ефективність у протидії сучасним загрозам. Платформи Endpoint Detection and Response (EDR) та розширені платформи захисту кінцевих точок (Extended Detection and Response, XDR) інтегрують численні підходи до виявлення, аналізу та реагування на загрози в єдину систему, що забезпечує всебічний захист кінцевих точок. Особливими компонентами таких платформ є безперервний моніторинг, збір та аналіз телеметрії, автоматизоване реагування на загрози та інтеграція з іншими компонентами інфраструктури безпеки.

Інтеграція рішень для виявлення шкідливого програмного забезпечення з системами управління інформаційною безпекою та подіями (SIEM) дозволяє забезпечити централізований збір, кореляцію та аналіз даних з різних джерел, що підвищує ефективність виявлення складних загроз. Платформи SIEM, такі як Splunk, використовують алгоритми кореляції та аналітичні інструменти для ідентифікації патернів атак та аномалій у великих об'ємах даних, що надходять від кінцевих точок та інших компонентів інфраструктури. Така інтеграція забезпечує повну видимість подій безпеки та дозволяє реалізувати ефективний процес виявлення, розслідування та реагування на інциденти.

1.3. Аналіз існуючих рішень щодо виявлення шкідливого програмного забезпечення на кінцевих точках організації

Сучасний ринок рішень для виявлення шкідливого програмного забезпечення на кінцевих точках представлений широким спектром продуктів та сервісів, що відрізняються функціональністю, архітектурою та підходами до забезпечення безпеки. Згідно з даними Gartner, сегмент рішень для захисту кінцевих точок демонструє стабільне зростання, що відображає зростаючу потребу організацій у надійних засобах захисту від сучасних кіберзагроз [38]. Аналіз ринку дозволяє виділити кілька категорій рішень: традиційні антивірусні продукти, платформи Endpoint Protection Platform (EPP), системи Endpoint Detection and Response (EDR) та Extended Detection and Response (XDR).

Microsoft Defender for Endpoint представляє собою комплексну платформу для захисту кінцевих точок, що поєднує функціональність запобігання загрозам, виявлення, розслідування та реагування на інциденти. Архітектура рішення включає агенти для кінцевих точок, хмарну аналітичну платформу, що використовує механізми машинного навчання, та інтеграцію з іншими продуктами Microsoft Security Stack. Перевагами Microsoft Defender for Endpoint є глибока інтеграція з операційною системою Windows, що забезпечує розширені можливості моніторингу та захисту, а також використання глобальної розвідувальної мережі Microsoft для виявлення нових загроз.

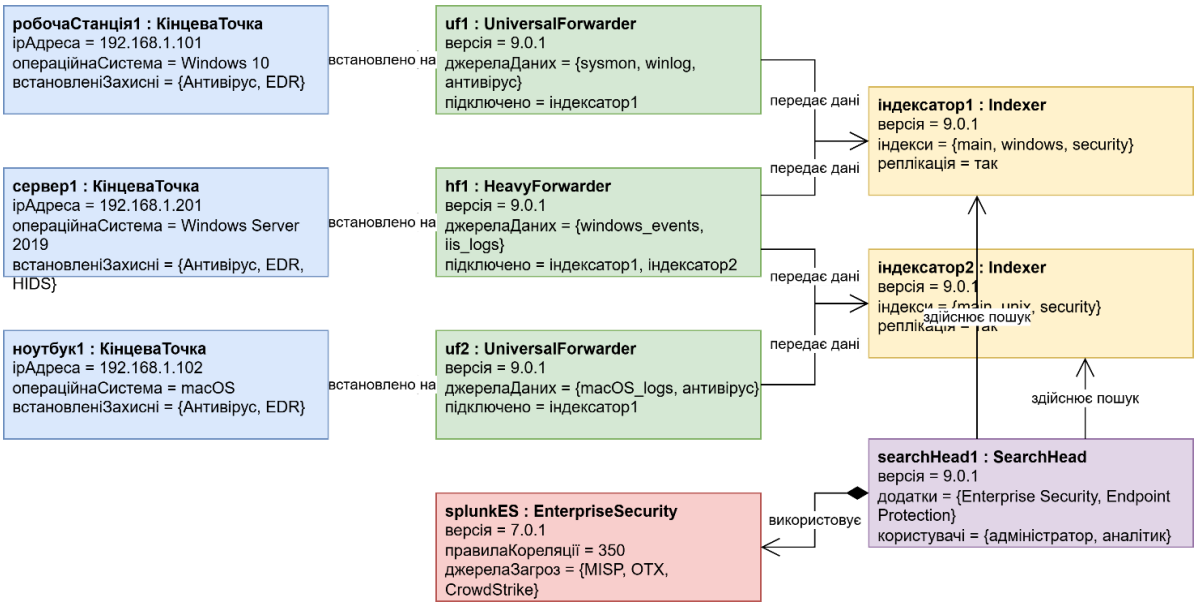

Рис. 1.3. Діаграма об'єктів взаємодії компонентів рішення Splunk з кінцевими точками

VMware Carbon Black представляє собою платформу для захисту кінцевих точок, що фокусується на поведінковому аналізі та застосуванні технологій машинного навчання для виявлення шкідливого програмного забезпечення. Рішення використовує запатентовану технологію "streaming prevention", яка забезпечує моніторинг та аналіз поведінки всіх процесів на кінцевих точках у режимі реального часу [41]. Особливістю Carbon Black є здатність виявляти та блокувати безфайлові атаки та інші просунуті техніки, що використовуються сучасним шкідливим програмним забезпеченням.

BlackBerry Cylance представляє інноваційний підхід до захисту кінцевих точок, який радикально відрізняється від традиційних антивірусних рішень. Замість реактивного виявлення вже відомих зразків шкідливого програмного забезпечення, Cylance застосовує проактивну стратегію, засновану на використанні алгоритмів штучного інтелекту та машинного навчання. Ці алгоритми аналізують мільйони бінарних файлів для виявлення патернів та характеристик, які можуть вказувати на їх потенційну шкідливість. Унікальність цього підходу полягає в можливості виявлення та блокування загроз ще до їх виконання, що суттєво знижує ризик успішної атаки на кінцеві точки організації.

Математичні моделі, що використовуються в Cylance, дозволяють проводити глибокий аналіз характеристик файлів без необхідності їх виконання

в реальному середовищі або в пісочниці. Система аналізує статичні властивості файлів, такі як структура заголовків, використані функції API, ентропія даних, розміри секцій та інші атрибути, які формують унікальний "відбиток" файлу. На основі цього аналізу алгоритми машинного навчання обчислюють ймовірність шкідливості файлу та приймають рішення про його блокування або дозвіл на виконання. Такий підхід дозволяє ефективно виявляти не лише відомі загрози, але й нові, раніше невідомі зразки шкідливого програмного забезпечення, включаючи модифіковані версії та нульові дні.

Рішення захисту кінцевих точок, подібні до BlackBerry Cylance, демонструють високу ефективність проти сучасних загроз, таких як програми-вимагачі, безфайлові атаки та складні цільові атаки на організації. Однак для забезпечення комплексного захисту інформаційної інфраструктури необхідна інтеграція таких спеціалізованих рішень з централізованими системами управління інформаційною безпекою та подіями (SIEM). Саме такі системи забезпечують збір, зберігання та аналіз даних про події безпеки з усіх компонентів інфраструктури, включаючи кінцеві точки, мережеве обладнання, сервери та хмарні сервіси.

Платформа Splunk Enterprise Security є одним з провідних SIEM-рішень на ринку, яке надає потужні інструменти для виявлення, аналізу та реагування на загрози. Основною перевагою Splunk є здатність обробляти великі обсяги даних з різних джерел та виявляти корельовані події, які можуть вказувати на складні багатоетапні атаки. Платформа використовує розширену аналітику, включаючи машинне навчання та статистичні моделі, для виявлення аномалій та підозрілої активності, яка може вказувати на наявність загрози [10]. Інтерактивні панелі моніторингу та інструменти візуалізації дозволяють аналітикам безпеки ефективно досліджувати виявлені інциденти та приймати обґрунтовані рішення щодо реагування.

Інтеграція Splunk з рішеннями для захисту кінцевих точок, такими як BlackBerry Cylance, створює потужну екосистему безпеки, яка поєднує переваги обох підходів. Splunk може збирати та аналізувати дані про події безпеки від

Cylance, включаючи інформацію про заблоковані загрози, підозрілу активність та спроби обходу захисних механізмів. Така інтеграція дозволяє створити єдиний центр управління безпекою, що забезпечує повну видимість загроз та можливість оперативного реагування на інциденти. Це особливо цінно для великих організацій з розподіленою інфраструктурою, де необхідно забезпечити централізоване управління безпекою багатьох кінцевих точок.

Особливо суттєву еволюцію у сфері захисту кінцевих точок представляють системи Endpoint Detection and Response (EDR), які виходять за рамки традиційних антивірусних рішень. За визначенням аналітичної компанії Gartner, EDR-системи фокусуються на розширених можливостях моніторингу активності на кінцевих точках, детальному аналізі зібраних даних для виявлення загроз, проведенні розслідувань та автоматизованому реагуванні на інциденти. Такі системи забезпечують неперервний моніторинг процесів, мережевих з'єднань, доступу до файлів та інших аспектів роботи кінцевих точок, що дозволяє виявляти складні атаки, які можуть залишатися непоміченими для традиційних засобів захисту.

Сучасний ринок EDR-рішень представлений такими продуктами, як CrowdStrike Falcon, SentinelOne та Cisco Secure Endpoint, кожен з яких пропонує унікальні підходи до виявлення та реагування на загрози. Ці рішення забезпечують глибоку видимість активності на кінцевих точках, можливості для проведення детальних розслідувань інцидентів та автоматизованого реагування на виявлені загрози. Інтеграція цих рішень з Splunk дозволяє розширити можливості аналізу та кореляції подій безпеки, забезпечуючи більш ефективне виявлення складних багатоетапних атак.

Для організацій, які шукають рішення з відкритим кодом для захисту кінцевих точок, Wazuh пропонує цікаву альтернативу комерційним продуктам. Ця платформа поєднує функціональність системи виявлення вторгнень на хості (HIDS), моніторингу цілісності файлів та аналізу журналів. Wazuh забезпечує збір та аналіз даних з кінцевих точок, що дозволяє виявляти ознаки шкідливого програмного забезпечення, аномальну поведінку та інші індикатори

компрометації [10]. Модульна архітектура Wazuh дозволяє організаціям налаштовувати систему відповідно до своїх специфічних потреб та інтегрувати її з існуючими компонентами інфраструктури безпеки.

Особливою перевагою Wazuh є можливість інтеграції з Splunk, що дозволяє розширити можливості для аналізу та візуалізації даних безпеки. Завдяки такій інтеграції, організації можуть використовувати потужні інструменти Splunk для створення панелей моніторингу, пошуку та аналізу даних, зібраних агентами Wazuh на кінцевих точках. Це забезпечує ефективне виявлення загроз та реагування на інциденти без необхідності великих фінансових інвестицій у комерційні рішення.

Комплексний підхід до захисту кінцевих точок організації передбачає поєднання різних технологій та рішень, включаючи системи на базі штучного інтелекту, такі як BlackBerry Cylance, EDR-рішення, такі як CrowdStrike Falcon, SentinelOne та Cisco Secure Endpoint, SIEM-системи, такі як Splunk Enterprise Security, та рішення з відкритим кодом, такі як Wazuh. Інтеграція цих рішень створює багаторівневу систему захисту, здатну ефективно протидіяти сучасним кіберзагрозам, включаючи складні цільові атаки, програми-вимагачі та безфайлові атаки. Такий підхід забезпечує не лише превентивний захист від відомих загроз, але й можливості для виявлення та реагування на нові, раніше невідомі типи атак, що є необхідною умовою для забезпечення надійного захисту інформаційних ресурсів організації в умовах динамічного ландшафту кіберзагроз.

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) та системи запобігання вторгненням (Intrusion Prevention Systems, IPS) залишаються компонентами для захисту кінцевих точок від шкідливого програмного забезпечення [16]. Ці системи здійснюють моніторинг мережевого трафіку та активності на хості для виявлення ознак зловмисних дій, використовуючи сигнатурний аналіз, поведінкові методи та інші техніки. Сучасні IDS/IPS-рішення для кінцевих точок інтегруються з іншими компонентами

інфраструктури безпеки, забезпечуючи комплексний захист від мережевих та хостових загроз.

Data Loss Prevention (DLP) системи, хоча першочергово призначені для запобігання витоку даних, також відіграють роль у виявленні шкідливого програмного забезпечення, особливо того, що спрямоване на крадіжку конфіденційної інформації. Ці системи здійснюють моніторинг та контроль даних, що передаються через мережу, зберігаються на кінцевих точках або обробляються додатками. Виявлення аномальних патернів доступу до даних або спроб несанкціонованої передачі інформації може вказувати на наявність шкідливого програмного забезпечення, такого як трояни або шпигунське ПЗ.

Сучасні рішення для виявлення шкідливого програмного забезпечення на кінцевих точках організації продовжують еволюціонувати у відповідь на зростаючу складність кіберзагроз. Аналіз існуючих технологій демонструє тенденцію до конвергенції різних підходів у єдині інтегровані платформи, що поєднують функціональність запобігання, виявлення, розслідування та реагування на інциденти безпеки. Дослідження ринку показує зростання популярності рішень XDR (Extended Detection and Response), які розширюють можливості традиційних EDR-систем шляхом інтеграції даних з різних джерел, включаючи мережеві пристрої, хмарні сервіси та контейнери, що забезпечує комплексний підхід до виявлення загроз на всіх рівнях інфраструктури.

Впровадження розширеної аналітики даних, машинного навчання та автоматизації в сучасні рішення для захисту кінцевих точок дозволяє значно підвищити ефективність виявлення шкідливого програмного забезпечення та скоротити час реагування на інциденти безпеки. Інтеграція різних технологій захисту, таких як EDR, SIEM, антивірусне програмне забезпечення та засоби моніторингу мережевого трафіку в рамках комплексного підходу до забезпечення безпеки кінцевих точок, дозволяє організаціям ефективно протидіяти сучасним кіберзагрозам, знижуючи ризик успішних атак та мінімізуючи потенційні збитки від інцидентів безпеки.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ НА БАЗІ SPLUNK

2.1. Архітектура та компоненти рішення SPLUNK

Universal Forwarder (UF) є спеціалізованим компонентом Splunk, розробленим для ефективного збору та передачі даних з мінімальним впливом на продуктивність систем, де він встановлений. Цей компонент здатен збирати різноманітні типи даних, включаючи файли журналів, вихідні дані команд операційної системи, дані журналу подій Windows, метрики продуктивності та інші джерела машинних даних. Universal Forwarder встановлюється на кінцевих точках мережі та забезпечує надійну передачу даних до індексаторів Splunk з функціями буферизації та відновлення після збоїв.

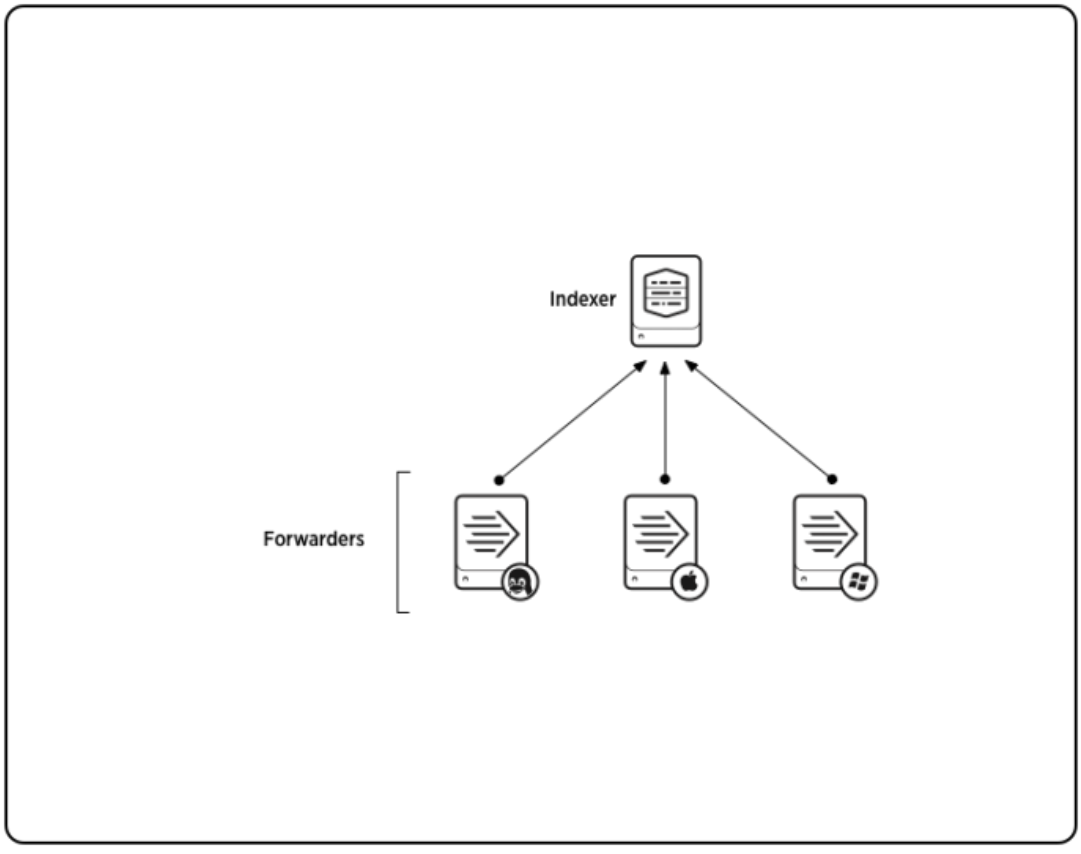

Рис. 2.1. Компонент Universal Forwarder [24]

Heavy Forwarder (HF) розширює функціональність Universal Forwarder, додаючи можливості локальної обробки даних перед їх передачею до індексаторів [14]. Цей компонент може виконувати парсинг, фільтрацію, маскування конфіденційних даних та маршрутизацію даних на основі їх змісту. Heavy Forwarder особливо корисний у сценаріях, де необхідно зменшити обсяг даних, що передаються через мережу, або забезпечити попередню обробку даних перед їх індексацією.

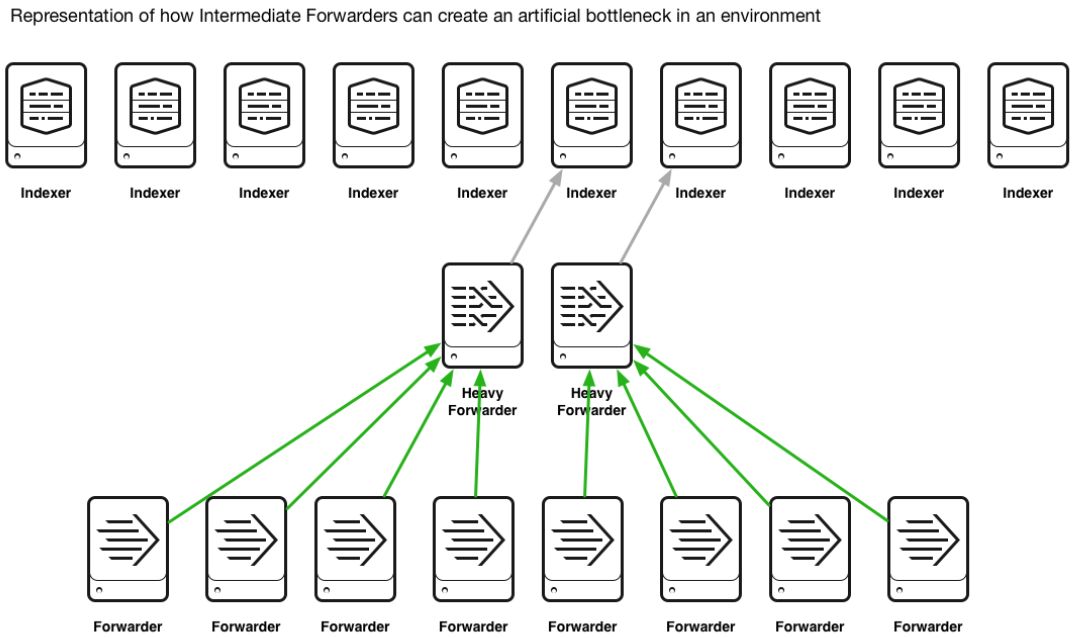

Рис. 2.2. Компонент Heavy Forwarder [24]

Indexer (індексатор) є фундаментальним компонентом архітектури Splunk, який виконує кілька функцій: прийом даних від пересилачів, парсинг даних у події, індексацію подій для забезпечення швидкого пошуку та відповідь на пошукові запити від пошукових вузлів. Індексатор перетворює отримані необроблені дані в події шляхом ідентифікації часових міток, виділення полів та застосування конфігурацій парсингу відповідно до типу даних. Після обробки події зберігаються в індексах – логічних сховищах даних на диску, організованих за часовими проміжками для оптимізації пошуку.

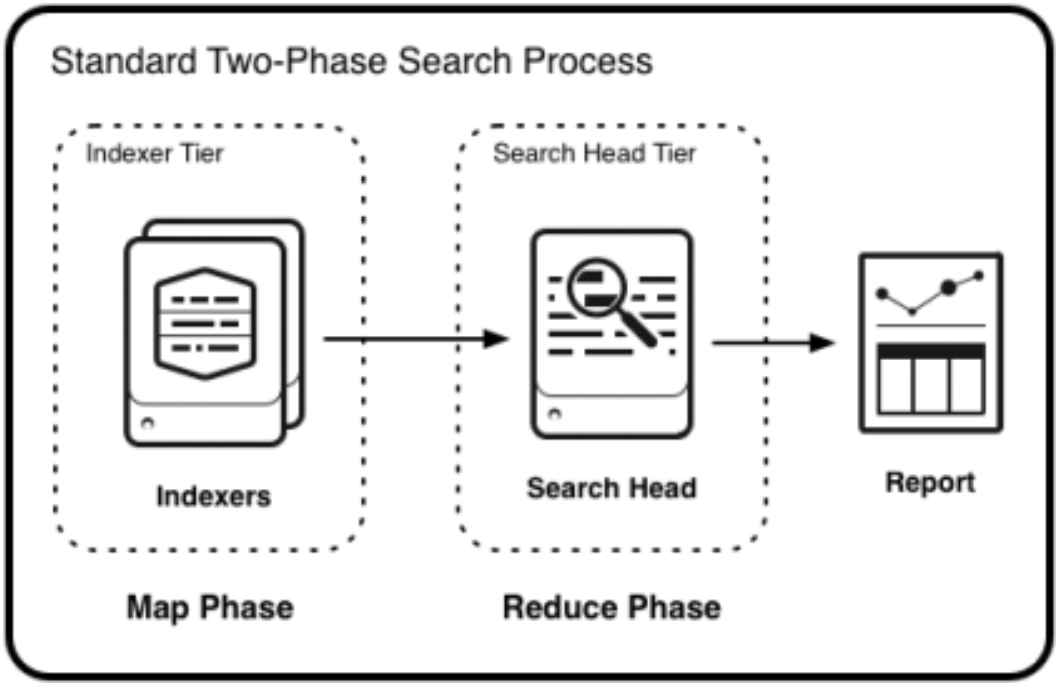

Рис. 2.3 Компонент Indexer [26]

Search Head (пошуковий вузол) забезпечує інтерфейс для користувачів Splunk, дозволяючи формулювати пошукові запити, створювати панелі моніторингу, звіти та попередження. Цей компонент розподіляє пошукові запити між індексаторами, консолідує результати та представляє їх користувачам в зручній формі [10]. Пошуковий вузол також відповідає за виконання запланованих пошуків, створення та розсилку звітів, а також генерацію сповіщень на основі визначених умов.

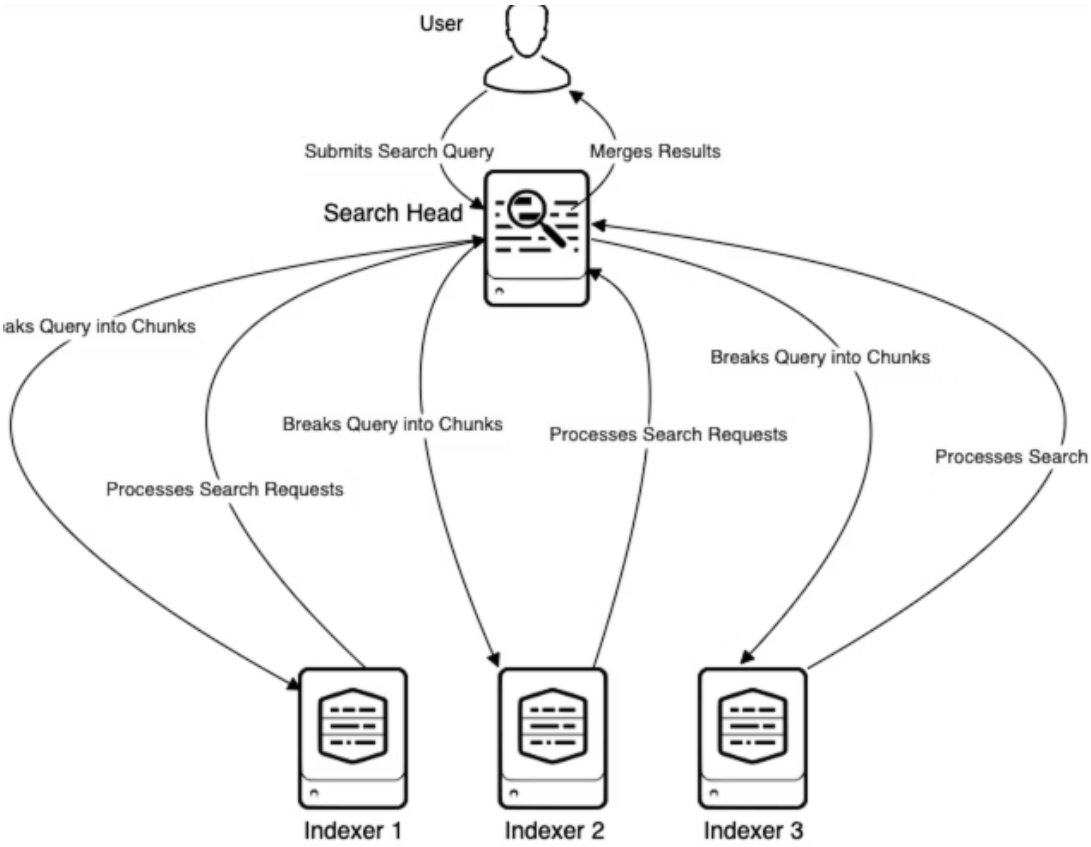

Рис. 2.4. Компонент Search Head [30]

Deployment Server (сервер розгортання) спрощує управління розподіленою інфраструктурою Splunk, надаючи централізовані засоби для розгортання конфігурацій, додатків та оновлень на множині компонентів Splunk. Цей компонент дозволяє групувати клієнти (пересилачі, індексатори тощо) та застосовувати специфічні набори конфігурацій для кожної групи, забезпечуючи узгоджене функціонування всіх компонентів системи [14]. Використання Deployment Server значно знижує адміністративне навантаження в масштабних розгортаннях Splunk та мінімізує ризик помилок конфігурації.

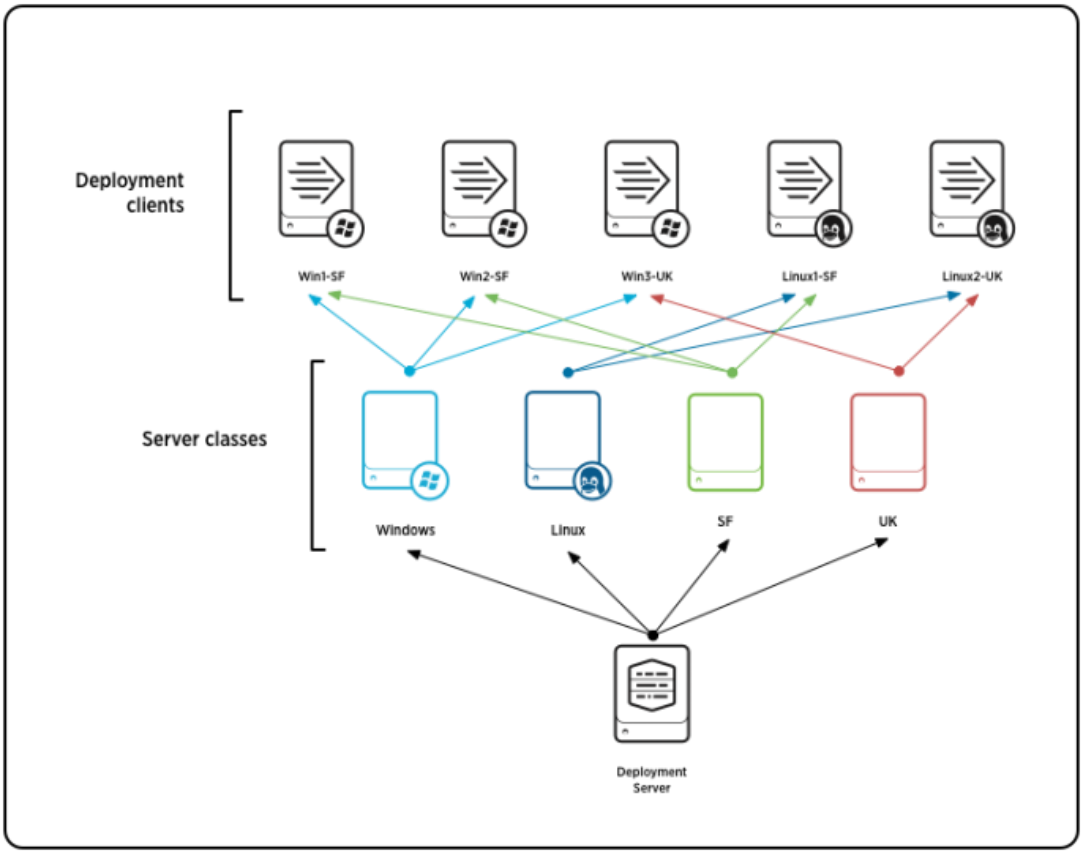

Рис. 2.5. Компонент Deployment Server [25]

Cluster Master (майстер кластера) управляє кластером індексаторів, забезпечуючи координацію реплікації даних між вузлами кластера, моніторинг стану вузлів та перепризначення первинних копій даних у випадку відмови індексаторів. Цей компонент реалізує політики реплікації, що визначають кількість копій даних, які повинні зберігатися в кластері, та забезпечує відмовостійкість системи. Cluster Master також координує пошукові запити, направляючи їх до найбільш підходящих індексаторів для оптимального виконання.

Таблиця 2.1

Функціональні можливості основних компонентів Splunk

Компонент	Основні функції	Додаткові можливості
Universal Forwarder	Збір даних, буферизація, передача на індексатори	Моніторинг файлів, фільтрація на основі вихідних даних
Heavy Forwarder	Парсинг даних, маскування, маршрутизація	Локальна індексація, трансформація даних

Продовження таблиці 2.1

Компонент	Основні функції	Додаткові можливості
Indexer	Обробка подій, індексація, зберігання даних	Реплікація, пошук, архівування даних
Search Head	Обробка запитів, візуалізація, створення звітів	Планування завдань, генерація сповіщень, API доступ
Deployment Server	Управління конфігурацією, розгортання оновлень	Моніторинг компонентів, групування клієнтів
Cluster Master	Координація реплікації, моніторинг вузлів	Балансування навантаження, відновлення після збоїв

License Master (майстер ліцензій) відповідає за управління ліцензіями Splunk та забезпечення дотримання ліцензійних обмежень на обсяг даних, що індексуються. Цей компонент відстежує використання ліцензій усіма індексаторами в розгортанні та забезпечує централізований контроль над ліцензуванням. License Master також надає інформацію про поточне використання ліцензій та генерує попередження при наближенні до ліцензійних обмежень [10].

Monitoring Console (консоль моніторингу) надає централізований інтерфейс для моніторингу продуктивності та стану всіх компонентів Splunk у розгортанні. Цей компонент збирає метрики з різних вузлів Splunk, включаючи використання CPU, пам'яті, диску, статистику індексації та пошуку, та представляє їх у зручних для аналізу панелях моніторингу. Monitoring Console допомагає адміністраторам виявляти потенційні проблеми, оптимізувати продуктивність системи та планувати масштабування.

Search Head Cluster (кластер пошукових вузлів) забезпечує високу доступність та масштабованість функцій пошуку та аналізу даних в архітектурі Splunk. Цей компонент розподіляє навантаження пошукових запитів між декількома пошуковими вузлами та забезпечує безперебійну роботу системи навіть при відмові окремих вузлів. Search Head Cluster також забезпечує реплікацію конфігурацій, знань (збережених пошуків, панелей моніторингу,

звітів) між усіма членами кластера, гарантуючи узгодженість досвіду користувачів.

Knowledge Objects (об'єкти знань) у Splunk – це конфігурації та налаштування, які допомагають інтерпретувати, аналізувати та візуалізувати дані. До них відносяться поля, витяги полів, трансформації пошуку, збережені пошуки, панелі моніторингу, звіти та сповіщення. Ці об'єкти можуть створюватися, змінюватися та поширюватися між користувачами та компонентами Splunk, формуючи базу знань організації для ефективного аналізу даних.

Data Models (моделі даних) представляють собою ієрархічні структури, що описують взаємозв'язки між даними та спрощують доступ до них для користувачів без глибоких знань мови пошуку Splunk (SPL). Моделі даних використовуються як основа для прискореного пошуку та створення звітів, а також служать фундаментом для функціональності Pivot у Splunk, що дозволяє користувачам створювати звіти та візуалізації без написання пошукових запитів.

Common Information Model (CIM) у Splunk – це стандартизована система полів та тегів, що забезпечує узгоджене представлення даних з різних джерел. CIM визначає схеми даних для різних типів подій, таких як мережевий трафік, системні події, події безпеки, що спрощує створення запитів та візуалізацій, які працюють з даними з різнорідних джерел. Використання CIM значно підвищує ефективність аналізу даних та сприяє впровадженню готових рішень та додатків Splunk.

Apps and Add-ons (додатки та розширення) розширюють функціональність Splunk, надаючи попередньо налаштовані панелі моніторингу, пошуки, звіти та інші компоненти для конкретних випадків використання або джерел даних. Додатки можуть надавати комплексні рішення для специфічних задач, таких як моніторинг безпеки, аналіз продуктивності додатків або дотримання нормативних вимог, тоді як розширення зазвичай забезпечують інтеграцію з конкретними джерелами даних. Splunk підтримує екосистему додатків,

доступних через Splunkbase – онлайн-репозиторій, що містить сотні додатків від Splunk та сторонніх розробників.

Splunk Enterprise Security (ES) – це спеціалізоване рішення на базі Splunk для моніторингу, виявлення та реагування на загрози безпеки [10]. Цей додаток надає функціональність SIEM (Security Information and Event Management), включаючи кореляцію подій безпеки, виявлення аномалій, моніторинг відповідності нормативним вимогам та управління інцидентами. Splunk ES забезпечує централізоване відображення стану безпеки організації та автоматизує процеси виявлення та реагування на загрози.

Інтеграційні можливості Splunk забезпечуються через розширені API, які дозволяють взаємодіяти з іншими системами та компонентами IT-інфраструктури. REST API надає можливість програмного управління всіма аспектами платформи Splunk, включаючи інтеграцію пошуку, індексації та маніпуляції даними. SDK для різних мов програмування (Python, Java, JavaScript, C#) спрощують розробку інтеграційних рішень. Використання цих API та SDK дозволяє створювати складні автоматизовані робочі процеси, інтегрувати Splunk з іншими IT-системами та розширювати функціональність платформи відповідно до специфічних потреб організації.

Мобільний доступ до платформи Splunk забезпечується через спеціалізовані мобільні додатки, які надають можливість перегляду панелей моніторингу, пошуку та аналізу даних з мобільних пристроїв. Це дозволяє адміністраторам та аналітикам залишатися в курсі актуального стану систем та отримувати сповіщення про інциденти навіть поза офісом. Мобільні додатки підтримують функції аутентифікації та авторизації, забезпечуючи безпечний доступ до даних відповідно до визначених ролей та прав доступу користувачів.

Розширення функціональності Splunk здійснюється через механізми модульних додатків (Apps) та доповнень (Add-ons). Модульна архітектура Splunk дозволяє розробникам створювати спеціалізовані рішення для конкретних сценаріїв використання та інтеграції з різними джерелами даних. Додатки та доповнення можуть бути розроблені власними силами, отримані з

публічного репозиторію Splunkbase або придбані у партнерів Splunk. Цей екосистемний підхід забезпечує гнучкість та розширюваність платформи, дозволяючи організаціям адаптувати Splunk до своїх унікальних потреб та інтегрувати його з існуючими системами та процесами.

2.2. Призначення та основні функції компонентів SPLUNK

Splunk представляє собою потужну платформу для збору, індексації, аналізу та візуалізації машинних даних з різноманітних джерел, що робить її незамінним інструментом для моніторингу IT-інфраструктури та забезпечення кібербезпеки організацій. За визначенням, Splunk – це програмна платформа, призначена для пошуку, аналізу та візуалізації машинних даних, зібраних з веб-сайтів, додатків, датчиків, пристроїв та IT-інфраструктури, що дозволяє організаціям отримувати оперативні аналітичні дані для покращення сервісу, зниження експлуатаційних витрат та мінімізації ризиків безпеки [10].

Архітектура Splunk побудована на основі модульного підходу, що забезпечує гнучкість та масштабованість рішення відповідно до потреб організації. У своїй базовій конфігурації Splunk складається з трьох основних компонентів: Forwarder (пересилач), Indexer (індексатор) та Search Head (пошуковий вузол), кожен з яких виконує специфічні функції в рамках загальної архітектури. Ця трирівнева архітектура забезпечує ефективний збір, обробку та аналіз даних, а також розподіл навантаження між компонентами системи.

Forwarder (пересилач) представляє собою компонент, який встановлюється на джерелах даних і відповідає за збір та передачу логів та інших машинних даних до індексаторів. В архітектурі Splunk виділяють три типи пересилачів: Universal Forwarder (UF), Heavy Forwarder (HF) та Light Forwarder (LF), що відрізняються функціональністю та вимогами до ресурсів. Universal Forwarder є найбільш розповсюдженим типом пересилача і потребує мінімум ресурсів для роботи, оскільки виконує тільки функції збору та передачі даних без їх обробки.

Indexer (індексатор) є центральним компонентом архітектури Splunk, який відповідає за прийом даних від Forwarder, їх обробку, індексацію та зберігання [10]. Індексатор перетворює вхідні дані у події, додає часові мітки, виділяє поля та зберігає їх у індексах для подальшого пошуку. У масштабних розгортаннях Splunk може використовуватися кластер індексаторів для забезпечення відмовостійкості та розподілу навантаження, що підвищує надійність та продуктивність системи.

Search Head (пошуковий вузол) надає користувацький інтерфейс для пошуку, аналізу та візуалізації даних, збережених в індексаторах. Цей компонент відповідає за обробку пошукових запитів, їх оптимізацію та маршрутизацію до відповідних індексаторів, а також за консолідацію та представлення результатів пошуку користувачам. У великих розгортаннях Splunk може використовуватися Search Head Cluster для забезпечення високої доступності та розподілу навантаження при виконанні пошукових запитів.

Deployment Server (сервер розгортання) в архітектурі Splunk відповідає за централізоване управління конфігурацією та оновлення компонентів Splunk, розгорнутих в інфраструктурі. Цей компонент спрощує процеси адміністрування та підтримки системи, дозволяючи централізовано розгортати конфігурації, додатки та оновлення на множину пересилачів та інших компонентів Splunk.

Cluster Master (майстер кластера) є компонентом, який забезпечує управління кластером індексаторів, відповідаючи за моніторинг стану вузлів, координацію реплікації даних та перенаправлення запитів у випадку відмови окремих індексаторів. Цей компонент забезпечує високу доступність та надійність зберігання даних у розподілених розгортаннях Splunk.

License Master (мастер ліцензій) відповідає за управління ліцензіями Splunk та контроль обсягу даних, що індексуються, відповідно до придбаних ліцензій. Цей компонент здійснює моніторинг використання ліцензій та забезпечує дотримання ліцензійних обмежень у масштабі всієї інфраструктури Splunk.

Архітектура Splunk також включає компонент Monitoring Console (консоль моніторингу), який забезпечує централізований моніторинг стану та продуктивності всіх компонентів Splunk у розгортанні. Ця консоль надає адміністраторам інструменти для відстеження метрик продуктивності, виявлення потенційних проблем та оптимізації роботи системи.

Для забезпечення високої доступності та відмовостійкості в архітектурі Splunk використовуються механізми реплікації та кластеризації. Індексатори можуть бути організовані в кластери з визначеним фактором реплікації, що забезпечує збереження копій даних на декількох вузлах і запобігає втраті інформації у випадку відмови окремих компонентів [14].

Архітектура Splunk передбачає можливість горизонтального масштабування для обробки зростаючих обсягів даних через додавання нових індексаторів та пошукових вузлів без необхідності заміни існуючого обладнання. Ця здатність до масштабування дозволяє організаціям поступово розширювати свої розгортання Splunk відповідно до зростаючих потреб в обробці та аналізі даних.

Компонент Smart Store у сучасній архітектурі Splunk забезпечує розділення обчислювальних ресурсів та ресурсів зберігання, дозволяючи використовувати об'єктні сховища (наприклад, Amazon S3, Google Cloud Storage) для довготривалого зберігання даних. Цей підхід оптимізує використання локальних дискових ресурсів індексаторів та знижує витрати на зберігання великих обсягів історичних даних.

Центральним елементом взаємодії користувачів з платформою Splunk є Splunk Web – веб-інтерфейс, що забезпечує доступ до функцій пошуку, аналізу та візуалізації даних. Цей компонент надає інтуїтивно зрозумілий інтерфейс для створення пошукових запитів, панелей моніторингу, звітів та попереджень на основі зібраних та проіндексованих даних.

З точки зору масштабування та управління продуктивністю, архітектура Splunk підтримує як вертикальне, так і горизонтальне масштабування. При вертикальному масштабуванні збільшуються ресурси (CPU, RAM, сховище)

окремих компонентів, тоді як горизонтальне масштабування передбачає додавання нових екземплярів компонентів (індексатори, пошукові вузли) для розподілу навантаження. Такий підхід забезпечує гнучкість при зростанні обсягів даних та кількості користувачів, дозволяючи організаціям поступово розширювати інфраструктуру Splunk відповідно до своїх потреб.

Захист даних в архітектурі Splunk реалізується через механізми шифрування, управління доступом та аудиту. Дані можуть шифруватися під час передачі між компонентами, під час зберігання в індексах, а також при створенні резервних копій. Рольова модель доступу забезпечує гранулярний контроль над доступом до даних та функціональності, дозволяючи реалізувати принцип найменших привілеїв. Аудит дій користувачів та системних подій забезпечує відстежуваність та допомагає у виявленні потенційних порушень безпеки.

Архітектура Splunk постійно еволюціонує, інтегруючи нові технології та підходи для підвищення ефективності обробки та аналізу даних. Сучасні тенденції включають розширення можливостей використання штучного інтелекту та машинного навчання для автоматизованого виявлення аномалій та прогнозної аналітики, поглиблення інтеграції з хмарними платформами та сервісами, а також розширення можливостей для аналізу даних Інтернету речей (IoT) та операційних технологій (OT). Ці еволюційні зміни забезпечують актуальність та конкурентоспроможність платформи Splunk у динамічному ландшафті технологій обробки даних.

2.3. Процеси функціонування рішення SPLUNK

Процес збору даних у Splunk починається з Universal Forwarder або Heavy Forwarder, які моніторять визначені джерела даних, такі як файли журналів, мережеві потоки або виводи команд. За своїм визначенням, процес збору даних у Splunk – це послідовність дій, спрямованих на виявлення, читання, буферизацію та передачу машинних даних з джерел до компонентів, відповідальних за їх обробку та зберігання. Пересилачі відстежують зміни в

джерелах даних та збирають нові записи, застосовуючи налаштовані фільтри та трансформації.

Процес індексації даних у Splunk включає кілька етапів: парсинг вхідних даних, виділення часових міток та полів, категоризацію подій та їх зберігання в індексах. Індексатор розбиває потік даних на окремі події, визначаючи межі подій відповідно до налаштованих правил, та присвоює кожній події часову мітку. Далі виконується категоризація подій за допомогою джерел (source), типів джерел (sourcetype) та хостів (host), що спрощує подальший пошук та аналіз. Після обробки події зберігаються на диску у вигляді індексів, організованих за часовими проміжками (бакетами) для оптимізації пошуку.

Таблиця 2.2

Етапи процесу індексації даних у Splunk

Етап індексації	Опис процесу	Результат етапу
Парсинг даних	Розбиття потоку даних на окремі події	Виділені окремі події з необроблених даних
Часові мітки	Визначення часу події з даних або присвоєння поточного	Події з часовими мітками
Виділення полів	Автоматична або настроювана екстракція полів	Події з структурованими полями
Категоризація	Призначення джерела, типу джерела, хоста	Категоризовані події для ефективного пошуку
Індексація	Створення інвертованих індексів для швидкого пошуку	Індексовані події, готові для пошуку
Зберігання	Запис подій у файлову систему з організацією за часом	Події, збережені в індексах на диску

Процес пошуку в Splunk базується на мові пошуку Splunk (SPL), яка дозволяє користувачам формулювати запити для знаходження, фільтрації, аналізу та візуалізації даних. Процес пошуку починається з введення користувачем пошукового запиту в інтерфейсі Search Head, який аналізує запит, оптимізує його та розподіляє по відповідних індексаторах. Індексатори

виконують пошук у своїх локальних даних та повертають результати до Search Head, який агрегує їх та представляє користувачу [14]. Складні пошукові запити можуть включати операції фільтрації, трансформації, статистичного аналізу, кореляції та візуалізації даних.

Реплікація даних у Splunk забезпечує надійність та відмовостійкість системи шляхом створення копій даних на різних індексаторах у кластері. Процес реплікації координується Cluster Master, який визначає розміщення первинних та реплікованих копій даних відповідно до налаштованого фактора реплікації. При отриманні нових даних індексатор, який виступає в ролі первинного для цих даних, індексує їх та реплікує на інші вузли кластера згідно з політикою реплікації. Цей процес гарантує збереження даних навіть у разі відмови окремих індексаторів.

Процес виявлення та розслідування інцидентів безпеки у Splunk Enterprise Security (ES) включає збір та аналіз даних безпеки з різних джерел, кореляцію подій, виявлення аномалій та підозрілої активності, а також автоматизоване чи ручне реагування на виявлені загрози. Splunk ES використовує механізми кореляції в реальному часі для виявлення складних патернів атак, що можуть залишатися непоміченими при аналізі окремих подій. При виявленні потенційного інциденту безпеки генерується сповіщення, яке містить детальну інформацію про подію, задіяні системи та потенційний вплив.

Моніторинг продуктивності інфраструктури Splunk є безперервним процесом відстеження метрик та показників, що забезпечує оптимальну роботу всіх компонентів системи. Цей процес включає збір та аналіз даних про використання ресурсів CPU, пам'яті, диску, пропускної здатності мережі, а також специфічних метрик Splunk, таких як швидкість індексації, затримки пошуку, кількість пошукових запитів тощо [14]. Monitoring Console забезпечує централізований інтерфейс для візуалізації цих метрик та налаштування порогових значень для автоматичного сповіщення про потенційні проблеми.

Архівування та відновлення даних у Splunk дозволяє організаціям ефективно управляти життєвим циклом даних, зберігаючи їх доступність

відповідно до вимог бізнесу та нормативних актів. Процес архівування передбачає переміщення старих даних з активних індексів до архівних сховищ з можливістю їх відновлення при необхідності. Splunk підтримує різні стратегії архівування, включаючи холодне зберігання, заморожене зберігання та архівування у зовнішні системи, таких як Amazon S3, з можливістю відновлення даних для пошуку та аналізу.

Управління знаннями у Splunk є процесом створення, організації та поширення об'єктів знань, таких як поля, витяги полів, збережені пошуки, макроси, панелі моніторингу та звіти, для ефективного використання даних. Цей процес включає створення та налаштування об'єктів знань користувачами, їх валідацію та тестування, а також поширення через додатки або безпосередньо між користувачами [14]. Ефективне управління знаннями забезпечує стандартизацію аналізу даних в організації та сприяє повторному використанню кращих практик.

Автоматизація та оркестрація процесів у Splunk досягається за допомогою функціоналу Event Management та Adaptive Response, що дозволяє створювати автоматизовані робочі процеси для реагування на визначені події та умови. Ці механізми забезпечують автоматичне виконання послідовності дій у відповідь на виявлені інциденти безпеки, аномалії продуктивності чи інші події, що вимагають оперативного реагування. Автоматизовані робочі процеси можуть включати внутрішні дії в Splunk, такі як запуск додаткових пошуків або створення нових подій, а також інтеграцію з зовнішніми системами для виконання коригувальних дій, таких як блокування IP-адрес, карантин пристроїв або оновлення конфігурацій системи безпеки.

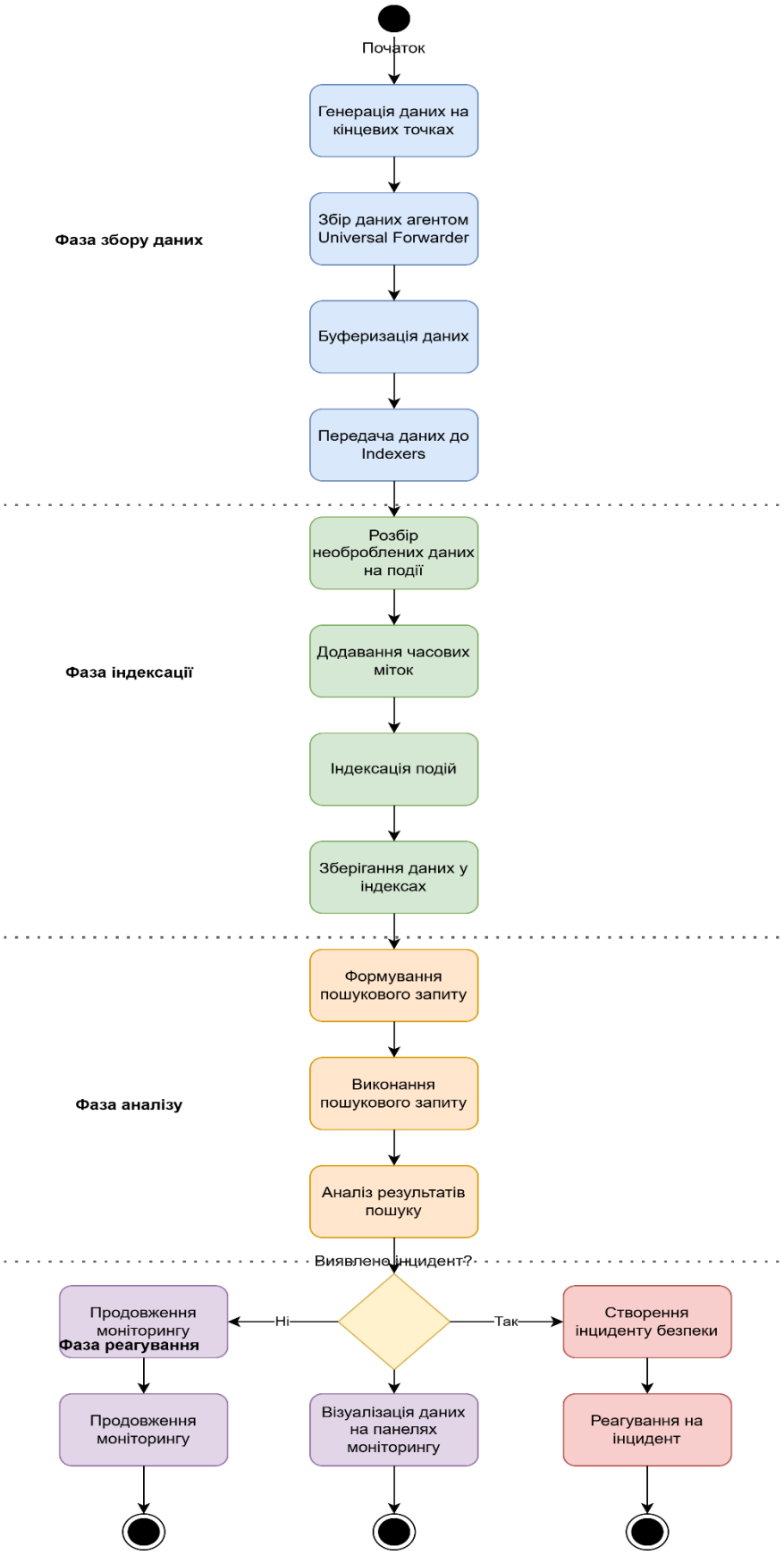

Рис. 2.6. Діаграма активностей процесу збору та аналізу даних в Splunk

Інтеграція Splunk з екосистемою безпеки та IT-інфраструктурою організації забезпечує створення комплексного середовища для моніторингу,

аналізу та реагування на події у режимі реального часу. За допомогою технологій API, Webhook, модулів розширення та спеціалізованих додатків, Splunk може обмінюватися даними з системами управління інцидентами, мережевими екранами, системами управління вразливостями, хмарними платформами та іншими компонентами інформаційної інфраструктури. Така інтеграція створює єдиний центр управління безпекою та операційною діяльністю, дозволяючи організаціям своєчасно виявляти та ефективно реагувати на загрози, забезпечувати відповідність нормативним вимогам та підтримувати стабільну роботу IT-середовища в умовах постійно еволюціонуючого ландшафту кіберзагроз.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ НА БАЗІ SPLUNK

3.1. Порядок виявлення шкідливого програмного забезпечення на кінцевих точках організації на базі SPLUNK

Виявлення шкідливого програмного забезпечення може відбуватися різними шляхами. Автоматичні сповіщення, згенеровані на основі заздалегідь налаштованих правил кореляції в Splunk Enterprise Security, є одним з основних механізмів виявлення інцидентів.

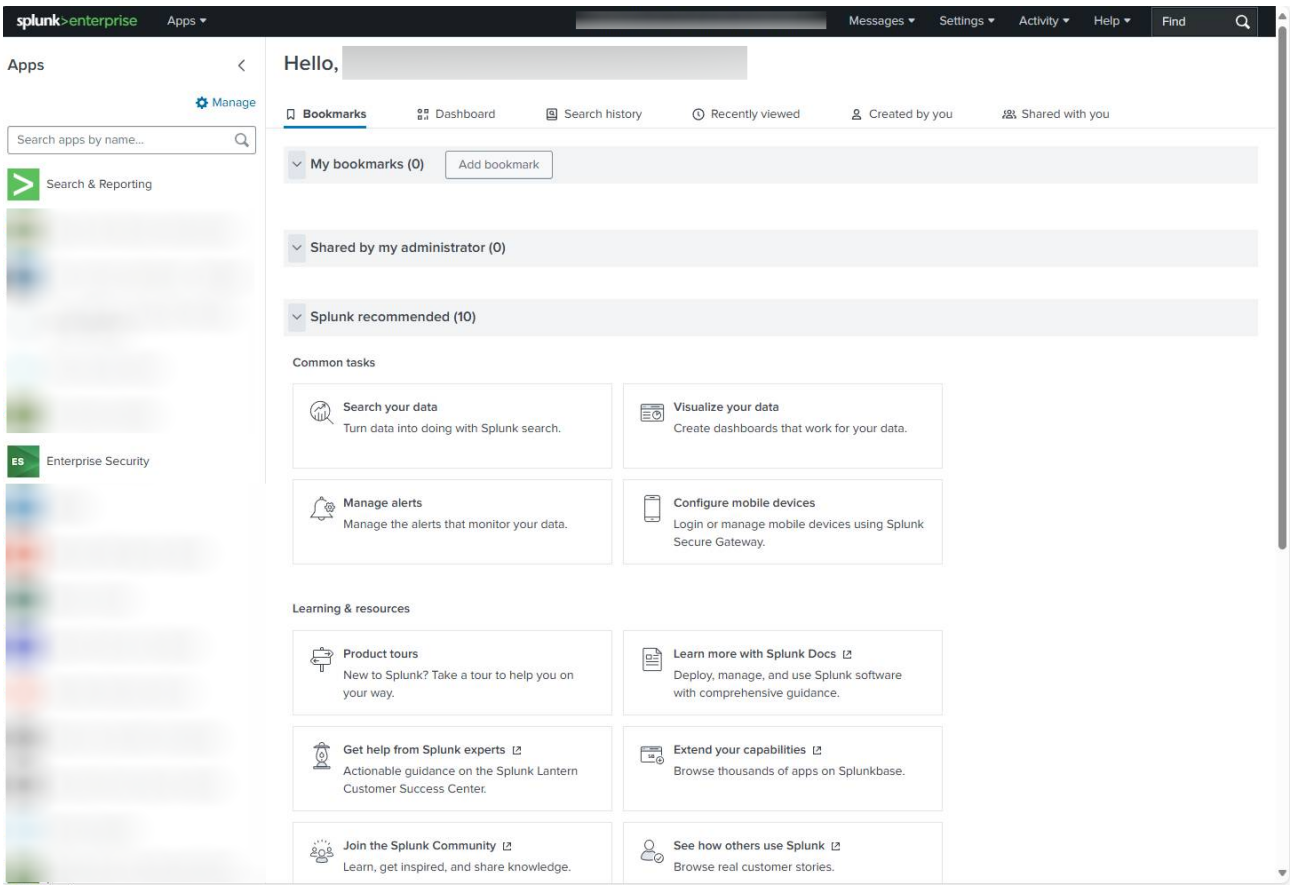

Рис. 3.1. Головна сторінка Splunk

Маємо SHA256 хеш файлу RDPWRAPPER 798af20db39280f90a1d35f2ac2c1d62124d1f5218a2a0fa29d87a13340bd3e4, який, згідно з інформацією з CERT-UA, реалізує функціонал паралельних RDP-сесій

[37]. Також, згідно з інформації з VirusTotal, 41 вендор безпеки детектує його як шкідливий [31].

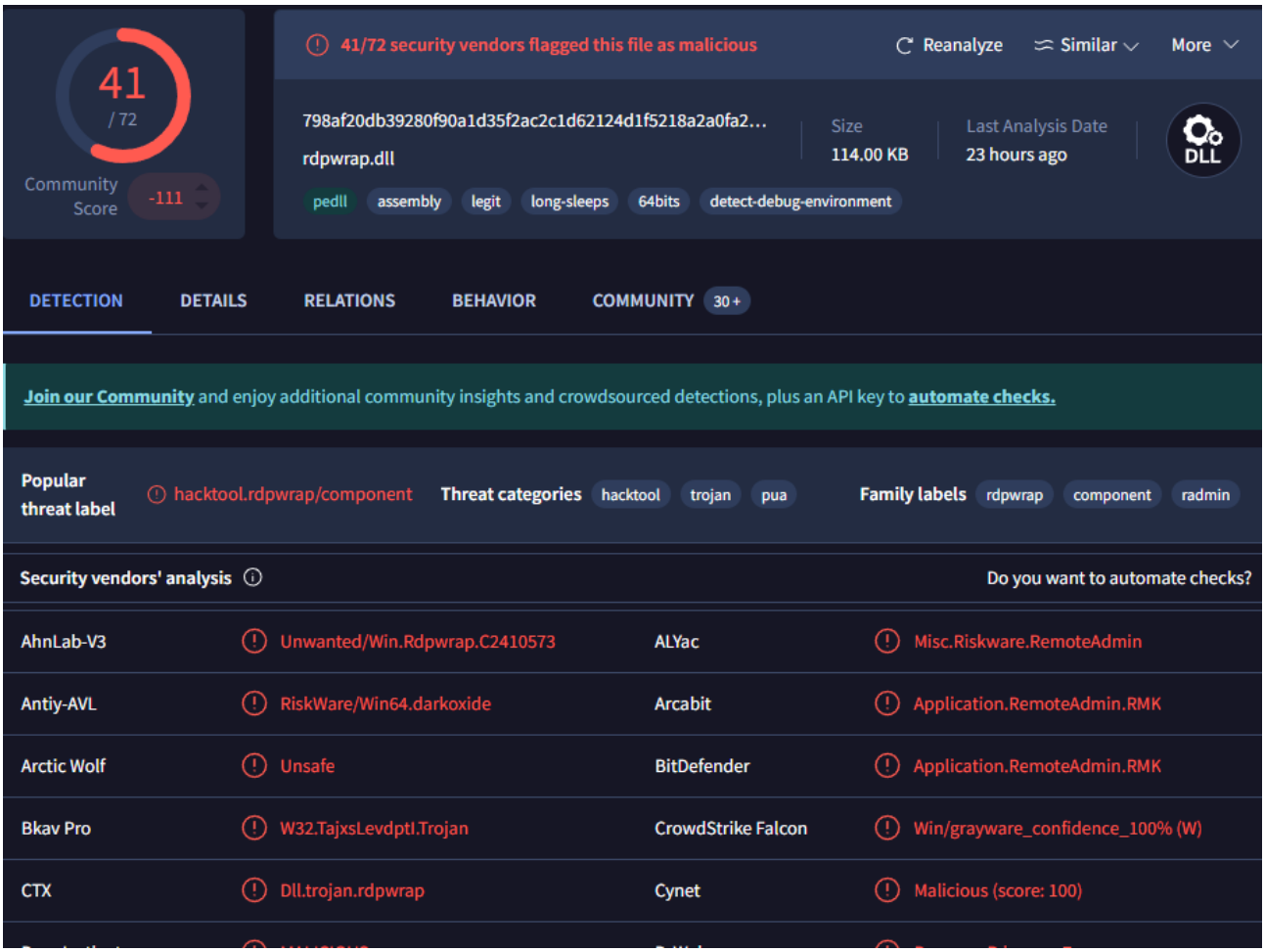

Рис. 3.2. Результат перевірки файлу на VirusTotal [31]

Першим етапом в створенні кореляційного правила є додавання назви правила в полі Detection description та вибір Manual методу вводу, після чого за допомогою SPL задаємо параметри пошуку. В розділі Analyst queue вказуємо назву кореляційного правила, опис та додаткові параметри Investigation type (тип розслідування), Security domain (тип домену безпеки) та Severity (ступінь тяжкості). Для успішного створення кореляційного правила необхідно також заповнити розділи Analyst queue, що відповідає за створення результатів пошуку, Assign risk, за допомогою якої визначається оцінка ризику, що в подальшому накопичується в залежності від кількості подій, Annotations, які використовується як коментарі щодо спрацювань на часових діаграмах. Time range встановлює графік відпрацювання правила і налаштовується за допомогою планувальника завдань Cron schedule. Поля Conditions та Throttling

використовуються для управління генеруванням результатів. За допомогою Adaptive response створюються додаткові завдання при відпрацюванні правила, наприклад, сповіщення на електронну пошту.

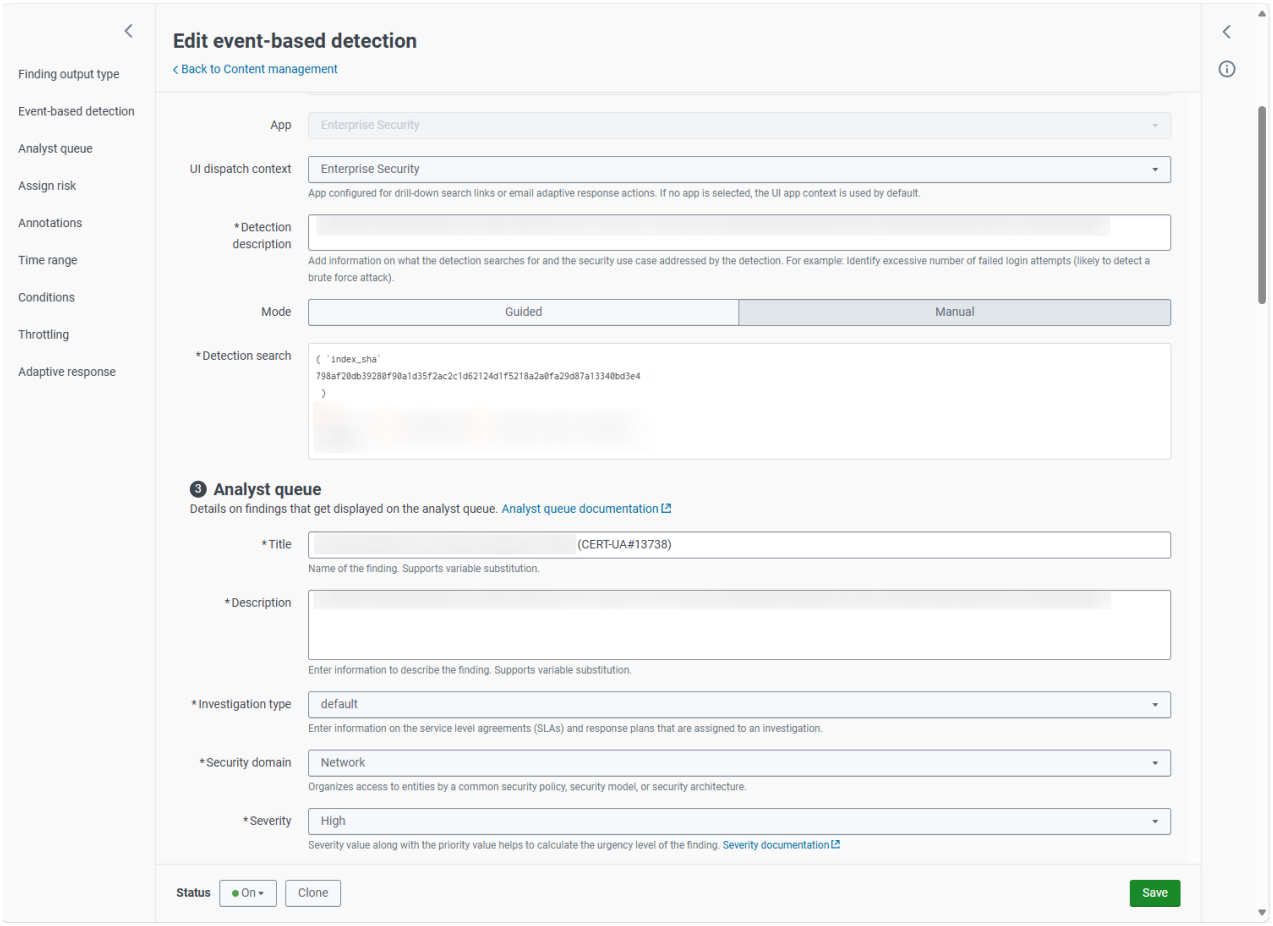

Рис. 3.3. Вікно створення кореляційного правила

Хоча заповнення усіх розділів і не є обов'язковою умовою при створенні кореляційного правила, але є важливою складовою для його ефективності та якості.

Після збереження усіх параметрів правило необхідно зберегти, після чого воно автоматично вмикається.

3.2. Порядок реагування на шкідливе програмне забезпечення в рішенні SPLUNK

Перший етап реагування починається з виявлення потенційного інциденту безпеки за допомогою автоматичного сповіщення, згенерованого на основі

налаштованого правила кореляції в Splunk Enterprise Security. В розгорнутій інформації є поля Owner, Status та Urgency, за якими відзначають відповідального за його розгляд, статус розгляду та пріорітету. В полі Detection знаходиться активне посилання на правило. Також наявні додаткові поля з інформацією про сам потенційний інцидент, що дає змогу моментально зібрати первинну інформацію.

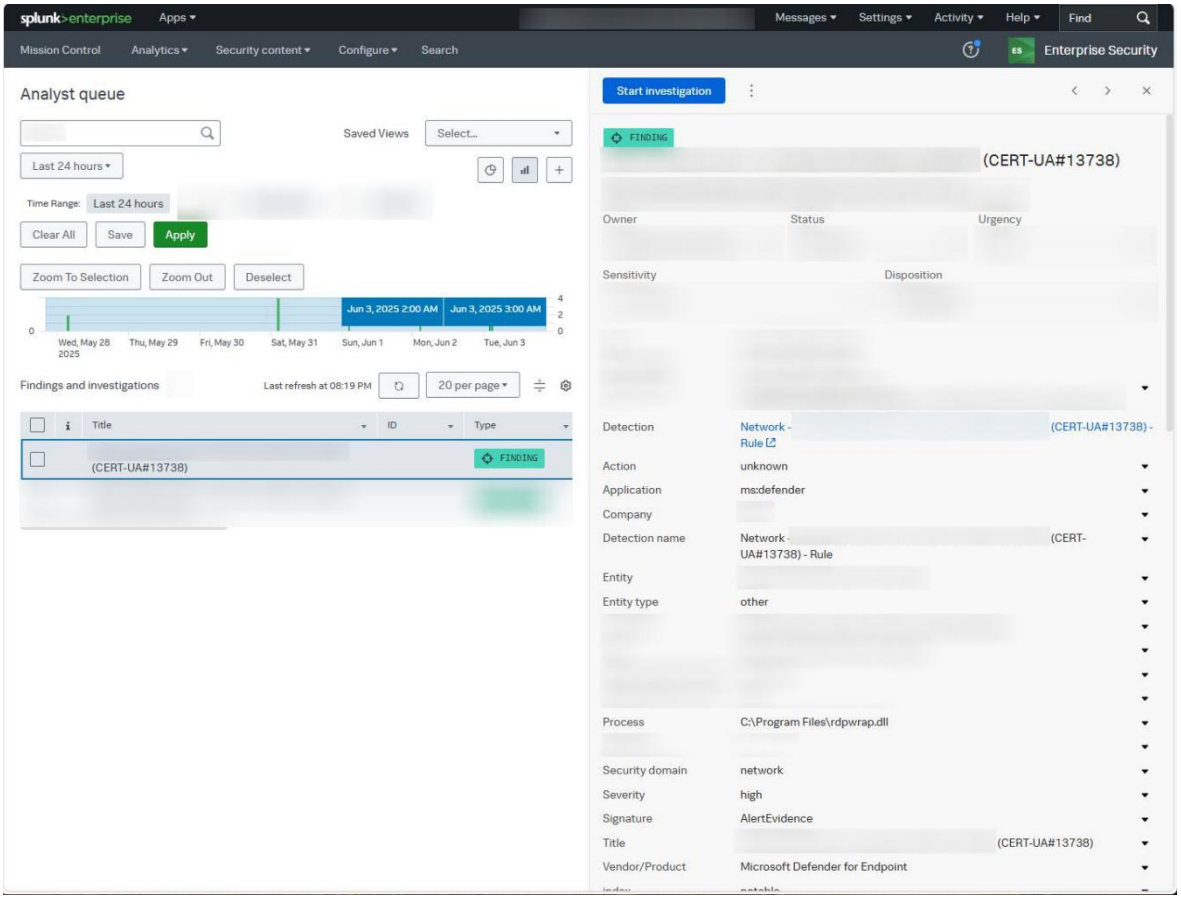

Рис. 3.4. Згенероване сповіщення

Наступним етапом є перегляд логу з кінцевої точки, на якій був виявлений хеш шкідливого файлу. Характерно, що їх було згенеровано 2, так як шкідливе програмне забезпечення було виявлене за допомогою Microsoft Defender. Завдяки налаштованій CIM вигляд логу має зрозумілу структуру. Це дає змогу швидко його проаналізувати.

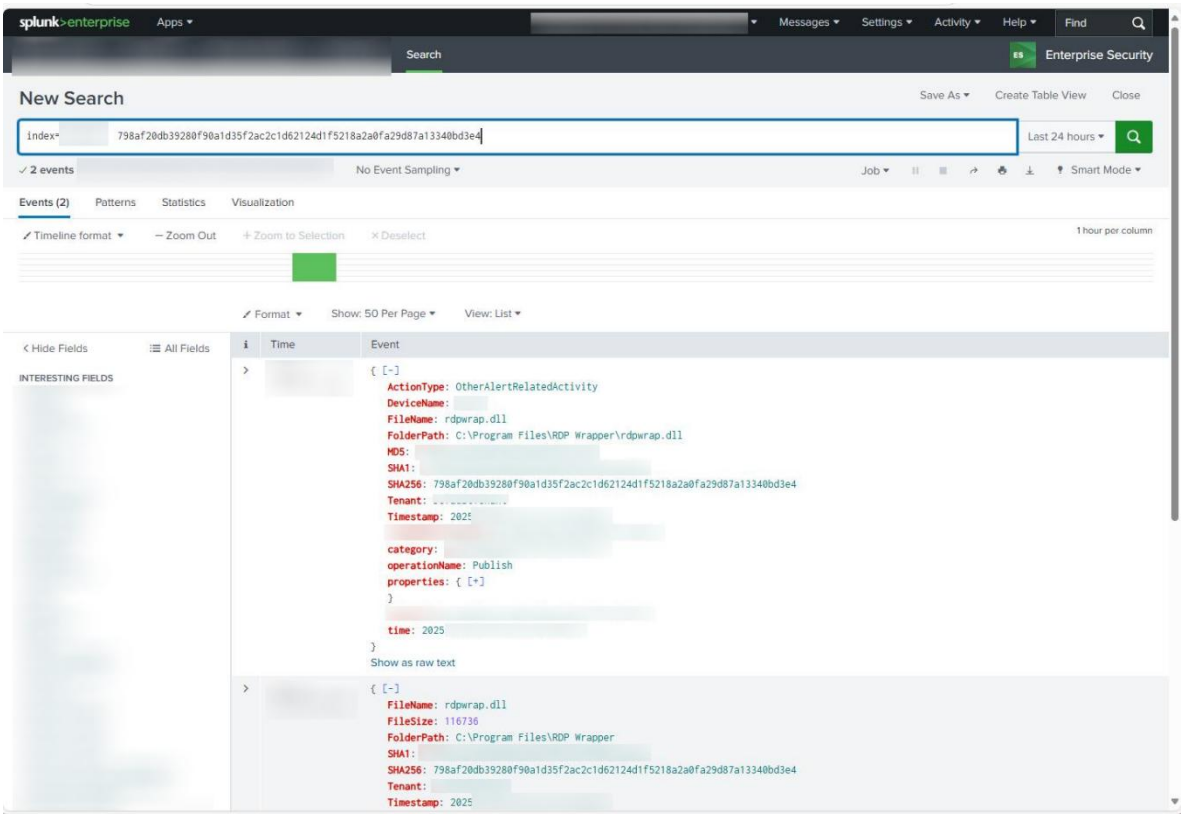

Рис. 3.5. Отримані логи

При детальному перегляді видно інформацію про назву файлу (FileName), назву кінцевої точки (DeviceName), хеш файлу (SHA256), результат виконання (action), застосунок (app), який процес було запущено (process_name), тека в якій знаходиться шкідливе програмне забезпечення (process_path_no_filename).

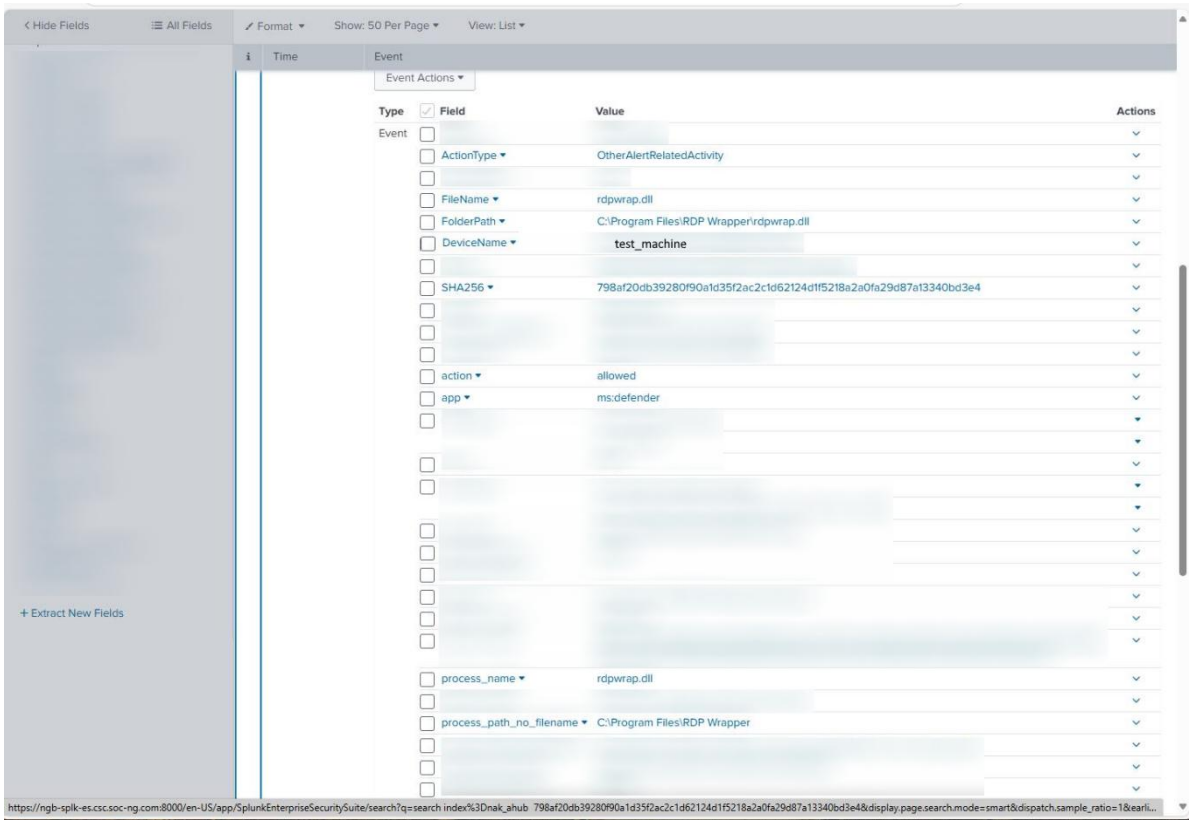

Рис. 3.6 Детальна інформація в отриманому логу

Після перегляду логу можна зробити висновок, що у вказаний час на кінцевій точці test_machine був виконаний успішний запуск файлу «rdpwrap.dll», який вважається частиною шкідливого програмного забезпечення. Наступним кроком є ізоляція кінцевої точки та блокування усіх загроз.

Після завершення розслідування інциденту та реалізації заходів з пом'якшення наслідків, проводиться аналіз уроків, отриманих під час інциденту. Це включає ідентифікацію вразливостей та недоліків у системах безпеки, які дозволили інциденту статися, а також розробку рекомендацій для покращення захисту в майбутньому. Уроки, отримані під час розслідування, використовуються для оновлення правил виявлення загроз, політик безпеки та процедур реагування на інциденти.

3.3. Рекомендації щодо застосування методів та засобів виявлення шкідливого програмного забезпечення на кінцевих точках організації

Ефективний захист кінцевих точок організації вимагає комплексного підходу, що поєднує технічні засоби, організаційні процедури та навчання персоналу. За визначенням, захист кінцевих точок організації – це сукупність методів, технологій та процесів, спрямованих на запобігання, виявлення та реагування на загрози безпеці робочих станцій, серверів, мобільних пристроїв та інших кінцевих систем, які використовуються для доступу до корпоративних ресурсів та даних. Розвиток технологій та еволюція кіберзагроз вимагають постійного вдосконалення підходів до захисту кінцевих точок.

Впровадження багаторівневої стратегії захисту кінцевих точок організації представляє собою фундаментальний підхід до забезпечення інформаційної безпеки в сучасних умовах. Така стратегія базується на принципі глибинного захисту, який передбачає створення декількох рівнів безпеки, що взаємно доповнюють один одного. При формуванні превентивного рівня захисту доцільно зосередитись на впровадженні механізмів контролю доступу з використанням багатофакторної аутентифікації, регулярному оновленні програмного забезпечення для усунення відомих вразливостей, а також застосуванні технологій шифрування даних для мінімізації наслідків потенційної компрометації пристроїв. Додатково варто впровадити механізми контролю додатків через білі та чорні списки, що суттєво обмежить можливості зловмисників з виконання шкідливого коду.

Детективний рівень захисту має ґрунтуватися на постійному моніторингу та аналізі поведінки систем для виявлення ознак компрометації. Для цього доцільно застосовувати технології EDR (Endpoint Detection and Response), які забезпечують безперервний збір та аналіз телеметрії з кінцевих точок, включаючи інформацію про процеси, мережеві з'єднання, модифікації файлів та реєстру. Платформа Splunk у поєднанні з EDR-агентами створює потужну систему виявлення загроз, здатну ідентифікувати як відомі, так і нові, раніше

невідомі загрози через аналіз аномальної поведінки та застосування моделей машинного навчання [21]. Моніторинг має охоплювати не лише технічні аспекти, але й дії користувачів, оскільки значна кількість інцидентів безпеки пов'язана з людським фактором.

Реактивні механізми захисту забезпечують швидке та ефективне реагування на виявлені загрози. Вони мають включати автоматизовані сценарії реагування, які активуються при виявленні підозрілої активності та виконують попередньо визначені дії, такі як блокування IP-адрес, ізоляція скомпрометованих систем від мережі, завершення підозрілих процесів чи відкат системи до попереднього стану. Інтеграція Splunk з платформами оркестрації та автоматизації безпеки (SOAR) дозволяє значно скоротити час реагування на інциденти та мінімізувати можливий збиток від атаки. Додатково варто розробити та регулярно тестувати плани реагування на інциденти, щоб забезпечити готовність команди безпеки до ефективних дій у разі виявлення загрози.

Впровадження технологій EDR має супроводжуватися розробкою детальних процедур розслідування інцидентів, які визначатимуть послідовність дій аналітиків при виявленні підозрілої активності. Ці процедури мають охоплювати збір доказів, аналіз індикаторів компрометації, відтворення хронології атаки та визначення шляхів проникнення зловмисників. Аналітичні можливості платформи Splunk дозволяють проводити глибоке розслідування інцидентів через пошук корельованих подій, аналіз поведінки користувачів та систем, а також застосування технік розслідування на основі MITRE ATT&CK та інших фреймворків безпеки.

Таблиця 3.1

Порівняння методів захисту кінцевих точок Splunk

Метод захисту	Основні функції	Ефективність проти загроз	Обмеження
Традиційний антивірус	Сигнатурний аналіз, евристика	Середня для відомих загроз	Низька ефективність проти новітніх загроз

Продовження таблиці 3.1

Метод захисту	Основні функції	Ефективність проти загроз	Обмеження
Система EDR	Моніторинг процесів, виявлення аномалій, реагування	Висока для більшості типів загроз	Вимагає спеціалізованих знань для управління
Система XDR	Інтегрований захист, аналіз даних з різних джерел	Висока для комплексних, складних атак	Висока вартість, складність впровадження
Контроль додатків	Білі та чорні списки, управління дозволами	Висока для запобігання виконанню шкідливих програм	Зниження гнучкості, адміністративне навантаження
Шифрування даних	Захист конфіденційності даних на пристроях	Висока для захисту від витоку даних	Не захищає від активних загроз

Система управління вразливостями є основоположним елементом у комплексному захисті кінцевих точок організації, оскільки дозволяє систематично виявляти, оцінювати та усувати вразливості програмного забезпечення до того, як вони будуть використані зловмисниками. Сучасний підхід до управління вразливостями включає розгортання спеціалізованих рішень, які здійснюють автоматизоване сканування кінцевих точок з метою виявлення відомих вразливостей у операційних системах, прикладному програмному забезпеченні та драйверах пристроїв [33]. Результатом сканування є детальний звіт про виявлені вразливості з інформацією про їх характер, ступінь ризику та потенційний вплив на безпеку системи. На основі цієї інформації проводиться пріоритизація вразливостей для усунення, враховуючи такі фактори, як оцінка CVSS (Common Vulnerability Scoring System), наявність експлойтів у публічному доступі, цінність активів та потенційний вплив на бізнес-процеси організації.

Процес управління вразливостями має бути безперервним циклом з чіткими часовими рамками для усунення вразливостей різного рівня ризику. Для

вразливостей з високим ризиком, таких як можливість віддаленого виконання коду або підвищення привілеїв, рекомендується встановлення патчів протягом 24-72 годин після їх виявлення. Для вразливостей середнього рівня ризику цей термін може бути збільшений до 7-14 днів, а для низькоризикових – до 30 днів. Аспектом є автоматизація процесу встановлення оновлень та патчів, що дозволяє значно знизити так зване "вікно вразливості" – період часу, протягом якого система залишається вразливою після публікації відповідного патча. Для цього можуть використовуватися спеціалізовані системи управління патчами, які забезпечують централізоване розгортання оновлень на всіх кінцевих точках організації з мінімальним впливом на бізнес-процеси.

Контроль додатків є ефективним превентивним механізмом захисту, який суттєво обмежує можливості зловмисників з виконання шкідливого програмного забезпечення на кінцевих точках. Технології контролю додатків можуть бути реалізовані в різних формах, включаючи білі списки (дозволено тільки затверджене програмне забезпечення), чорні списки (блокується відоме шкідливе програмне забезпечення) або гібридний підхід. Найбільш надійним вважається підхід, заснований на білих списках, оскільки він дозволяє запускати лише перевірені та схвалені програми, блокуючи будь-яке неавторизоване програмне забезпечення незалежно від того, чи було воно раніше ідентифіковане як шкідливе. Цей підхід особливо ефективний у середовищах з високими вимогами до безпеки, таких як фінансові установи, державні організації та критична інфраструктура.

Додатковим рівнем захисту є використання технологій "пісочниці" (sandbox), які забезпечують виконання підозрілих файлів та програм в ізольованому середовищі, де вони не можуть нашкодити основній системі. Підхід "пісочниці" дозволяє безпечно аналізувати поведінку потенційно шкідливого програмного забезпечення, спостерігаючи за його діями, доступом до системних ресурсів та комунікацією з зовнішніми серверами. Результати такого аналізу можуть бути використані для визначення характеру програми та прийняття обґрунтованого рішення щодо дозволу або блокування її виконання в

робочому середовищі. Сучасні рішення "пісочниці" інтегруються з іншими компонентами захисту кінцевих точок, такими як антивірусне програмне забезпечення, системи виявлення та запобігання вторгненням, забезпечуючи комплексний захист від складних загроз.

Безфайлові атаки, які виконуються виключно в пам'яті системи та не залишають слідів на жорсткому диску, становлять серйозну проблему для традиційних механізмів захисту, орієнтованих на сканування файлів. Для ефективного виявлення таких атак необхідне впровадження поведінкового аналізу та моніторингу процесів на кінцевих точках. Поведінковий аналіз базується на відстеженні діяльності системи та виявленні аномальної поведінки, яка може вказувати на компрометацію. Це включає моніторинг запусків процесів, звернень до реєстру, мережевих з'єднань, доступу до файлів та інших системних дій. Послідовність дій, які самі по собі можуть виглядати безпечними, але в певній комбінації вказують на наявність зловмисної активності, може бути ідентифікована за допомогою спеціалізованих алгоритмів виявлення аномалій та моделей машинного навчання.

Поведінковий аналіз є особливо ефективним проти невідомих та "нульового дня" загроз, оскільки він зосереджується на виявленні аномальної поведінки замість пошуку відомих сигнатур шкідливого програмного забезпечення. Це дозволяє виявляти нові та модифіковані загрози, які ще не були включені до баз даних сигнатур антивірусних продуктів. Для реалізації поведінкового аналізу можуть використовуватися спеціалізовані агенти, встановлені на кінцевих точках, які збирають телеметрію про активність системи та передають її до центральної платформи аналізу, такої як Splunk. У Splunk ця інформація може бути проаналізована з використанням пошукових запитів, правил кореляції та моделей машинного навчання для виявлення підозрілих патернів поведінки та генерації сповіщень про потенційні інциденти безпеки [7].

Особливою рекомендацією є впровадження принципів найменших привілеїв (Principle of Least Privilege) та контролю доступу на кінцевих точках [8].

Це передбачає надання користувачам та процесам лише тих прав та дозволів, які необхідні для виконання їх функцій, обмежуючи можливість поширення шкідливого програмного забезпечення у разі компрометації. Додатково рекомендується використання технологій ізоляції додатків (Application Isolation) для запобігання впливу скомпрометованих програм на інші компоненти системи.

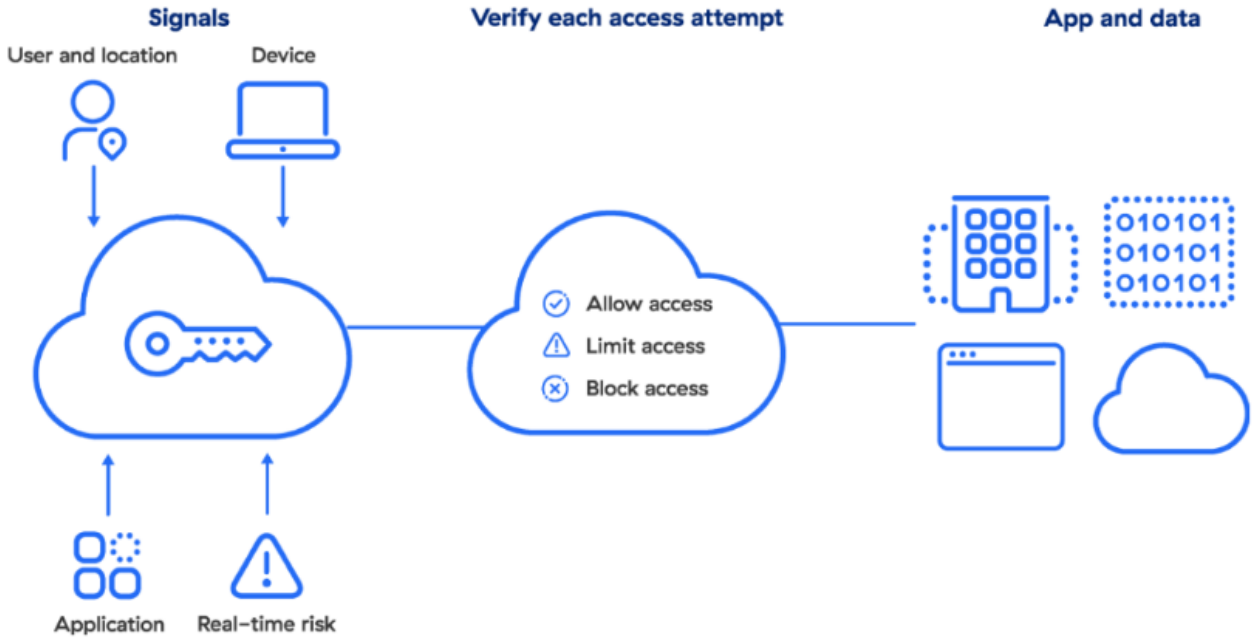

Рис. 3.7 – Принцип роботи Principle of Least Privilege [8]

Для ефективного захисту від просунутих персистентних загроз (APT) рекомендується впровадження методів проактивного пошуку загроз (Threat Hunting) на кінцевих точках. Це включає систематичний пошук ознак компрометації та підозрілої активності в системах організації, використовуючи тактики, техніки та процедури, характерні для відомих груп загроз. Проактивний пошук загроз дозволяє виявляти скриті загрози, які можуть залишатися непоміченими для автоматизованих систем виявлення.

Таблиця 3.2

Рекомендовані технології для комплексного захисту кінцевих точок

Технологія	Рівень захисту	Призначення	Приклади рішень
Endpoint Protection Platform (EPP)	Превентивний	Запобігання виконанню шкідливого коду	Symantec, McAfee, Microsoft Defender

Продовження таблиці 3.2

Технологія	Рівень захисту	Призначення	Приклади рішень
Endpoint Detection and Response (EDR)	Детективний	Виявлення та реагування на підозрілу активність	CrowdStrike, Carbon Black, SentinelOne
Extended Detection and Response (XDR)	Інтегрований	Виявлення складних загроз через інтеграцію даних	Palo Alto Cortex, Trend Micro XDR
Управління мобільними пристроями (MDM)	Контроль	Управління та захист мобільних пристроїв	MobileIron, AirWatch, Intune
Моніторинг цілісності файлів (FIM)	Детективний	Виявлення несанкціонованих змін у файловій системі	Tripwire, Wazuh, Splunk UF з osquery

Для захисту конфіденційних даних на кінцевих точках рекомендується впровадження рішень для запобігання витоку даних (Data Loss Prevention, DLP). Ці рішення забезпечують моніторинг та контроль руху конфіденційних даних на кінцевих точках, включаючи виявлення та блокування спроб несанкціонованої передачі даних через електронну пошту, месенджери, знімні носії та інші канали. Додатково рекомендується використання технологій шифрування для захисту конфіденційних даних, які зберігаються на кінцевих пристроях [24].

У контексті захисту мобільних пристроїв та віддалених робочих станцій рекомендується впровадження рішень для управління мобільними пристроями (Mobile Device Management, MDM) та управління мобільними додатками (Mobile Application Management, MAM). Ці рішення забезпечують централізоване управління налаштуваннями безпеки, розгортання додатків та контроль за дотриманням політик безпеки на мобільних пристроях, які використовуються для доступу до корпоративних ресурсів. Особливу увагу слід приділяти стратегіям для безпечної підтримки концепцій BYOD (Bring Your Own Device) та COPE (Corporate Owned, Personally Enabled).

Для захисту від загроз, пов'язаних з фішингом та соціальною інженерією, рекомендується комбінація технічних засобів та навчання користувачів. Технічні засоби включають фільтрацію електронної пошти, блокування підозрілих веб-сайтів та використання рішень для безпечної роботи в інтернеті. Навчання користувачів має фокусуватися на розпізнаванні фішингових атак, безпечних практиках роботи в інтернеті та процедурах повідомлення про підозрілі повідомлення та інциденти [20]. Регулярні тренінги та симуляції фішингових атак сприяють підвищенню обізнаності та пильності користувачів.

Також рекомендацією є впровадження регулярного резервного копіювання та розробка плану відновлення даних для мінімізації наслідків успішних атак на кінцеві точки. Це включає автоматизоване створення резервних копій даних, їх безпечне зберігання (бажано в offline-режимі або з обмеженим доступом) та регулярне тестування процедур відновлення. Особливу увагу слід приділяти захисту від програм-вимагачів, які шифрують дані на кінцевих точках та вимагають викуп за їх розблокування.

Для забезпечення централізованого моніторингу та управління безпекою кінцевих точок рекомендується інтеграція рішень захисту кінцевих точок з системами управління інформаційною безпекою та подіями (SIEM) та платформами оркестрації безпеки, реагування та автоматизації (SOAR). Така інтеграція забезпечує єдиний центр управління безпекою, автоматизацію рутинних завдань та підвищення ефективності реагування на інциденти. Платформа Splunk може слугувати основою для такої інтеграції, забезпечуючи збір, аналіз та візуалізацію даних з різних джерел безпеки.

Рекомендацією ще є впровадження практик безпечної розробки та управління конфігураціями для зниження ризиків, пов'язаних з вразливостями програмного забезпечення. Це включає використання шаблонів та базових конфігурацій для розгортання нових кінцевих точок, регулярний аудит налаштувань безпеки та автоматизоване виявлення відхилень від затверджених конфігурацій. Додатково рекомендується впровадження процесів управління

змінами для контролю за модифікаціями конфігурацій та програмного забезпечення на кінцевих точках.

Для забезпечення безпеки кінцевих точок в умовах гібридної інфраструктури, яка включає як локальні, так і хмарні компоненти, рекомендується впровадження хмарних рішень для захисту кінцевих точок [6]. Ці рішення забезпечують централізоване управління безпекою незалежно від місцезнаходження пристроїв, спрощують розгортання та оновлення агентів безпеки, а також надають можливість масштабування відповідно до потреб організації. Хмарні рішення також забезпечують доступ до актуальної інформації про загрози та автоматичне оновлення механізмів захисту.

Заключною рекомендацією є впровадження регулярної оцінки та вдосконалення програми захисту кінцевих точок на основі аналізу ефективності існуючих заходів, вивчення нових загроз та технологій, а також уроків, отриманих під час інцидентів безпеки. Рекомендується проводити регулярні перевірки безпеки кінцевих точок, включаючи пентестинг та оцінку вразливостей, для виявлення потенційних слабких місць та їх усунення. Безперервне вдосконалення є необхідною умовою для забезпечення ефективного захисту кінцевих точок в умовах динамічного ландшафту кіберзагроз.

Застосування концепції Zero Trust (нульової довіри) представляє сучасний підхід до захисту кінцевих точок, відмовляючись від традиційної парадигми периметрального захисту на користь принципу "ніколи не довіряй, завжди перевіряй". В рамках цієї концепції кожен запит доступу до ресурсів організації перевіряється незалежно від джерела, а доступ надається на основі оцінки стану безпеки пристрою, контексту запиту та профілю ризику користувача. Впровадження Zero Trust для захисту кінцевих точок вимагає комбінації технологій багатофакторної аутентифікації, мікросегментації мережі, контролю доступу на основі ролей та постійного моніторингу та оцінки стану безпеки пристроїв.

Інтеграція штучного інтелекту та машинного навчання у системи захисту кінцевих точок дозволяє суттєво підвищити їх ефективність у виявленні нових

та складних загроз. Алгоритми машинного навчання здатні аналізувати великі обсяги даних для виявлення аномалій та підозрілої поведінки, які можуть вказувати на наявність раніше невідомих загроз. Предиктивна аналітика допомагає прогнозувати потенційні вектори атак та вразливості, дозволяючи організаціям проактивно зміцнювати свої системи захисту. При впровадженні таких технологій необхідно забезпечити баланс між автоматизацією та людським контролем, щоб запобігти надмірній кількості хибних спрацьовувань та забезпечити контекстне розуміння виявлених аномалій.

Розвиток культури кібербезпеки в організації є не менш особливим аспектом, ніж впровадження технічних засобів захисту кінцевих точок. Це включає розробку чітких політик безпеки, проведення регулярних тренінгів та підвищення обізнаності користувачів, створення процедур для безпечного використання пристроїв та даних, а також формування середовища, де безпека розглядається як відповідальність кожного. Лідерство та підтримка з боку керівництва організації, визнання та заохочення безпечної поведінки, а також інтеграція питань безпеки у повсякденні робочі процеси – все це сприяє формуванню стійкої культури кібербезпеки, яка доповнює та підсилює технічні заходи захисту кінцевих точок.

ВИСНОВКИ

У ході виконання роботи було проведено комплексне дослідження проблеми виявлення шкідливого програмного забезпечення на кінцевих точках організації та розроблено рекомендації щодо застосування платформи Splunk для вирішення цієї проблеми. Аналіз сучасного стану галузі показав, що традиційні методи захисту, засновані на сигнатурному аналізі, демонструють недостатню ефективність проти сучасних загроз, що постійно еволюціонують та використовують різноманітні техніки обходу стандартних механізмів захисту. Це обумовлює необхідність впровадження комплексних рішень, здатних забезпечити багаторівневий захист, проактивне виявлення та швидке реагування на інциденти безпеки на кінцевих точках.

Дослідження підходів до виявлення шкідливого програмного забезпечення показало, що найбільш ефективним є комбінований підхід, який поєднує сигнатурний аналіз, евристичні методи, поведінковий аналіз та технології машинного навчання. Такий підхід забезпечує високу ефективність виявлення як відомих, так і нових, раніше невідомих загроз, мінімізуючи при цьому кількість хибних спрацьовувань. Платформа Splunk надає потужні можливості для реалізації цього підходу через збір, індексацію та аналіз різноманітних даних безпеки з кінцевих точок.

Аналіз архітектури та компонентів рішення Splunk дозволив визначити оптимальний варіант розгортання системи захисту кінцевих точок. Запропонована архітектура включає компоненти для збору даних (Universal Forwarder), індексації та зберігання (Indexer), пошуку та аналізу (Search Head), а також спеціалізовані додатки, такі як Splunk Enterprise Security для виявлення загроз та управління інцидентами. Така архітектура забезпечує масштабованість, відмовостійкість та високу продуктивність системи, що є необхідними умовами для ефективного захисту кінцевих точок у великих організаціях.

Розроблено порядок проведення розслідування інцидентів у рішенні Splunk, який включає етапи виявлення інциденту, первинної оцінки та сортування, детального аналізу, встановлення хронології подій, збору

індикаторів компрометації, визначення масштабу компрометації та реагування на інцидент. Особлива увага приділена використанню автоматизації та оркестрації процесів реагування через інтеграцію з інструментами SOAR, що дозволяє значно скоротити час від виявлення загрози до її нейтралізації та мінімізувати негативний вплив на бізнес-процеси організації.

Сформульовано рекомендації щодо застосування методів та засобів виявлення та реагування на шкідливе програмне забезпечення на кінцевих точках організації, які базуються на впровадженні багаторівневої стратегії захисту, що включає превентивні, детективні та реактивні механізми. Рекомендовано використання сучасних технологій Endpoint Detection and Response (EDR) у поєднанні з платформою Splunk для забезпечення повної видимості активності на кінцевих точках та швидкого реагування на виявлені загрози. Додатково рекомендовано впровадження принципів найменших привілеїв, контролю додатків, шифрування даних та регулярного резервного копіювання для мінімізації ризиків, пов'язаних з компрометацією кінцевих точок.

Практична цінність роботи полягає у розробці конкретних рекомендацій та підходів до впровадження системи виявлення шкідливого програмного забезпечення на базі Splunk, які можуть бути застосовані в організаціях різного масштабу та сфер діяльності. Запропоновані рішення дозволяють забезпечити ефективний захист кінцевих точок від сучасних кіберзагроз, включаючи складні цільові атаки, програми-вимагачі та безфайлові атаки, які становлять значний ризик для інформаційних ресурсів організацій.

Результати даної роботи демонструють, що впровадження платформи Splunk в якості основи для системи виявлення шкідливого програмного забезпечення на кінцевих точках організації є ефективним підходом до вирішення проблеми захисту від сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2022 Endpoint Security Report. Cybersecurity Insiders. URL: https://20645266.fs1.hubspotusercontent-na1.net/hubfs/20645266/CSI-2022-Endpoint-Security-Report-Adaptiva-Final-03282022%20(1).pdf (Дата звернення: 15.05.2025).

2. 2024 Attack Surface Threat Intelligence Report. Cybersecurity Insiders. URL: https://www.cybersecurity-insiders.com/wp-content/uploads/2024-Attack-Surface-Threat-Intelligence-Report-Cogility.pdf (Дата звернення: 28.04.2025).

3. Automate incident response with playbooks. Splunk Inc. 2023. URL: https://docs.splunk.com/Documentation/MC/Current/Detect/AutomationRun (Дата звернення: 30.04.2025).

4. Azugo P., Venter H., Wa Nkongolo M. Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset. arXiv:2404.12855v1 [cs.CR]. Ithaca, NY: Cornell University, 2024. URL: https://arxiv.org/abs/2404.12855. (Дата звернення: 28.04.2025).

5. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide: NIST Special Publication 800-61 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Дата звернення: 03.05.2025).

6. Create response templates. Splunk Inc. 2023. URL: https://docs.splunk.com/Documentation/MC/Current/Detect/CreateResponse (Дата звернення: 30.04.2025).

7. Endpoint Detection and Response (EDR). BlackBerry. URL: https://www.blackberry.com/us/en/solutions/endpoint-security/endpoint-detection-and-response#how-it-works (Дата звернення: 13.05.2025).

8. Endpoint Detection and Response (EDR). Solutions Reviews and Ratings. GARTNER. URL: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions (Дата звернення: 13.05.2025).

9. Example incident response workflow. Splunk Inc. 2023. URL: https://docs.splunk.com/Documentation/MC/Current/Detect/ExampleWorkflow (Дата звернення: 30.04.2025).

10. Fileless Malware: A Growing Threat. Symantec. 2023. URL: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/fileless-malware (Дата звернення: 02.05.2025).

11. Incident Management Guide. Splunk Inc. 2023. URL: https://www.splunk.com/en_us/blog/learn/incident-management.html (Дата звернення: 02.05.2025).

12. Incident Response Plans Guide. Splunk Inc. 2023. URL: https://www.splunk.com/en_us/blog/learn/incident-response-plans.html (Дата звернення: 30.04.2025).

13. Joe Security LLC. (2019). Dive deeper with the Joe Sandbox Splunk Add-On. Joe Security. URL: https://www.joesecurity.org/blog/7329507958131886524 (дата звернення: 29.04.2025).

14. Joint Task Force. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach: NIST Special Publication 800-37 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (Дата звернення: 13.05.2025).

15. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (Дата звернення: 28.04.2025).

16. Microsoft Defender for Endpoint series – What is Defender for Endpoint? – Part1. URL: https://www.microsoft.com/en-us/security/blog/2023/03/02/microsoft-is-named-a-leader-in-the-2022-gartner-magic-quadrant-for-endpoint-protection-platforms/ (Дата звернення: 13.05.2025).

17. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: NIST, 2023. URL: https://www.nist.gov/cyberframework (Дата звернення: 02.05.2025).

18. Nkongolo M., Tokmak M. Ransomware detection using stacked autoencoder for feature selection. arXiv preprint arXiv:2402.11342. URL: https://arxiv.org/abs/2402.11342 (Дата звернення: 28.04.2025).

19. Respond to incidents. Splunk Inc. 2023. URL: https://docs.splunk.com/observability/splunkplatform/practice-reliability/incident-response.html (Дата звернення: 30.04.2025).

20. Azugo P., Venter H., Wa Nkongolo M. Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset. arXiv:2404.12855v1 [cs.CR]. Ithaca, NY: Cornell University, 2024. URL: https://arxiv.org/abs/2404.12855 (Дата звернення: 15.05.2025).

21. Ross R., McEvilley M., Barrett R. Guide for Cybersecurity Event Recovery: NIST Special Publication 800-184. Gaithersburg, MD: National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf (Дата звернення: 03.05.2025).

22. Souppaya M., Barrett M., Scarfone K. Guide to Enterprise Patch Management: NIST Special Publication 800-40 Revision 3. Gaithersburg, MD: National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf (Дата звернення: 04.05.2025).

23. Souppaya M., Scarfone K. Malware Incident Handling Guide: NIST Special Publication 800-83 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf (Дата звернення: 03.05.2025).

24. Splunk Blog. Universal or Heavy: That is the Question. URL: https://www.splunk.com/en_us/blog/tips-and-tricks/universal-or-heavy-that-is-the-question.html (Дата звернення: 08.05.2025).

25. Splunk Documentation. Deployment server: architecture and components. URL: https://docs.splunk.com/Documentation/Splunk/9.4.2/Updating/Deploymentserverarchitecture (Дата звернення: 08.05.2025).

26. Splunk Documentation. Parallel reduce search processing overview. URL: https://docs.splunk.com/Documentation/Splunk/9.4.2/DistSearch/Parallelreduceoverview (Дата звернення: 05.06.2025).

27. Splunk Inc. How to Set Up Monitoring for Your Hybrid Environment. 2023. URL: https://www.splunk.com/en_us/blog/devops/how-to-set-up-monitoring-for-your-hybrid-environment.html (Дата звернення: 30.04.2025).

28. Splunk Inc. Як налаштувати моніторинг для вашого гібридного середовища. URL: https://www.splunk.com/en_us/blog/devops/how-to-set-up-monitoring-for-your-hybrid-environment.html (Дата звернення: 29.04.2025).

29. Start investigations. Splunk Inc. 2023. URL: https://docs.splunk.com/Documentation/ES/8.0.3/User/StartInvestigation (Дата звернення: 02.05.2025).

30. The Sec Master. How to Deploy Splunk Search Head (SH). URL: https://medium.com/thesecmaster/how-to-deploy-splunk-search-head-sh-8f0b85ff2cba (Дата звернення: 09.05.2025).

31. VirusTotal. Аналіз файлу SHA256: 798af20db39280f90a1d35f2ac2c1d62124d1f5218a2a0fa29d87a13340bd3e4. URL: https://www.virustotal.com/gui/file/798af20db39280f90a1d35f2ac2c1d62124d1f5218a2a0fa29d87a13340bd3e4 (Дата звернення: 05.05.2025).

32. VMware Carbon Black. Endpoint Detection and Response (EDR). Datasheet. URL: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-datasheet-edr.pdf (Дата звернення: 15.05.2025).

33. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: National Institute of Standards and Technology, 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (Дата звернення: 02.05.2025).

34. What Is Incident Response? Splunk Inc. 2023. URL: https://www.splunk.com/en_us/blog/learn/incident-response.html (Дата звернення: 30.04.2025).

35. Zscaler. What Is Least-Privileged Access? URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-least-privilege-access (Дата звернення: 29.04.2025).

36. Zuhair H., Selamat A. An Empirical Analysis of Machine Learning Efficacy in Anti-Ransomware Tools. ICT for Engineering & Critical Infrastructures. 2024. С. 65–78. DOI: https://doi.org/10.1007/978-3-031-49309-6_6 (Дата звернення: 28.04.2025).

37. Державна служба спеціального зв’язку та захисту інформації України. Держспецзв’язку: зловмисники експлуатують вразливості у популярних програмних продуктах. URL: https://cert.gov.ua/article/6282536 (Дата звернення: 05.05.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)