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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія реагування на інциденти безпеки на основі інтеграції DLP та SIEM системи»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

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

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

_____ Данило ДІДЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
ДІДЕНКО Данило
(прізвище, ім'я)

Керівник БОРСУКОВСЬКИЙ Юрій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ДІДЕНКУ Данилу Юрійовичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія реагування на інциденти безпеки на основі інтеграції DLP та SIEM системи»

керівник кваліфікаційної роботи Борсуковський Юрій Володимирович
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення DLP Endpoint Protector та SIEM Wazuh;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми реагування на інциденти інформаційної безпеки в інформаційних системах організацій
2. Аналіз методів та засобів для моніторингу та реагування на інциденти безпеки на базі DLP Endpoint Protector та SIEM системи Wazuh
3. Технологія реагування на інциденти безпеки на основі інтеграції DLP та

SIEM систем

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми моніторингу та реагування на інциденти безпеки в інформаційній системі організації.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз проблеми ефективного реагування на інциденти кібербезпеки.	27.10.2024 р.	
4.	Технології використання DLP та SIEM систем для моніторингу та реагування на інциденти безпеки.	03.11.2024 р.	
5.	Створення архітектури для проведення моніторингу та реагування на інциденти безпеки з використанням інтегрованих систем DLP та SIEM.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Данило ДІДЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача ДІДЕНКА Данила

на тему: «Технологія реагування на інциденти безпеки на основі інтеграції DLP та SIEM системи»

Актуальність:

Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. В роботі чітко визначено зміст проблеми реагування на інциденти безпеки, мету дослідження та завдання, що відповідають сучасним викликам у сфері кібербезпеки.
2. Детально досліджено можливості DLP Endpoint Protector і SIEM системи Wazuh, розкрито їх функціональні можливості та обґрунтувано доцільність їх інтеграції.
3. Запропоновано технологію інтеграції DLP та SIEM для моніторингу та автоматичного реагування на інциденти безпеки, а також розроблено рекомендації для впровадження цієї технології в організаціях.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі було б корисно включити розрахунок витрат і очікуваної економії для організації від впровадження інтеграції.
2. Доцільно було б продемонструвати результати впровадження запропонованої технології на прикладі конкретної організації

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ДІДЕНКО Данило** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою Інформаційна та кібернетична безпека.

Рецензент: _____ _____ _____

(науковий ступінь, вчене звання) *(підпис)* *(ім’я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач ДІДЕНКО Данило до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія реагування на інциденти безпеки на основі інтеграції DLP та SIEM системи».
Кваліфікаційна робота і рецензія додаються.
Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач(ка) ***ДІДЕНКО Данило*** обрав тему роботи, метою якої було дослідити технології реагування на інциденти безпеки в інформаційних системах організації на основі інтеграції рішень кібербезпеки DLP та SIEM систем і розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ДІДЕНКО Данило*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача(ки) ***ДІДЕНКА Данила*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньо-професійної програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(ім'я, прізвище)*
"____" грудня 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ДІДЕНКО Данило** допускається до захисту даної кваліфікаційної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 76 сторінок, 41 рисунок, 6 таблиць, 12 джерел.

Об'єкт дослідження – автоматизація реагування на інцидент безпеки за рахунок інтеграції DLP та SIEM систем.

Предмет дослідження – технології моніторингу та реагування на інциденти безпеки на основі інтеграції DLP та SIEM систем.

Мета роботи – розробити порядок застосування технології інтеграції DLP та SIEM систем для ефективного моніторингу та реагування на інциденти безпеки в організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації систем DLP та SIEM, моделювання сценаріїв інцидентів та оцінка ефективності інтеграції.

Інтеграція систем Data Loss Prevention (DLP) і Security Information and Event Management (SIEM) забезпечує посилений захист даних та більш оперативне реагування на загрози кібербезпеки. DLP забезпечує моніторинг та контроль передачі конфіденційної інформації, тоді як SIEM об'єднує дані з різних джерел для виявлення аномалій і кореляції інцидентів. Інтегроване застосування обох технологій дозволяє підвищити точність і швидкість реагування на загрози витоку інформації.

У роботі проаналізовано проблему забезпечення кібербезпеки та витоку конфіденційної інформації на основі інтеграції DLP та SIEM систем, визначено її мету та завдання. Проведено аналіз існуючих технологій для моніторингу і реагування на інциденти безпеки в сучасних організаціях. Досліджено основні функції DLP та SIEM систем, їх переваги та обмеження, а також методи інтеграції. Визначено основні виклики та підходи до реалізації інтегрованої системи.

На основі проведених досліджень запропоновано порядок застосування технології інтеграції DLP та SIEM систем для моніторингу та реагування на інциденти безпеки. Розроблено рекомендації фахівцям з кібербезпеки щодо впровадження цієї інтеграції та методів оцінки її ефективності.

Галузь використання – кібербезпека, захист конфіденційної інформації та оперативне реагування на інциденти в організаціях.

ІНЦИДЕНТ БЕЗПЕКИ, DLP, SIEM, ІНТЕГРАЦІЯ СИСТЕМ, МОНІТОРИНГ БЕЗПЕКИ, ЗАХИСТ ДАНИХ, АВТОМАТИЗАЦІЯ РЕАГУВАННЯ, МОДУЛІ, ФУНКЦІЇ

ABSTRACT

Text part of the qualification work: 76 pages, 41 figures, 6 tables, 12 sources.

Object of research – automation of response to a security incident through the integration of DLP and SIEM systems.

Subject of research – technologies for monitoring and responding to security incidents based on the integration of DLP and SIEM systems.

The aim of research – to develop a procedure for applying the technology of integrating DLP and SIEM systems for effective monitoring and response to security incidents in the organization.

Research methods – studying the literature on this topic, analyzing the operational documentation of DLP and SIEM systems, modeling incident scenarios and evaluating the effectiveness of integration.

The integration of Data Loss Prevention (DLP) and Security Information and Event Management (SIEM) systems provides enhanced data protection and a more rapid response to information security threats. DLP monitors and controls the transmission of confidential information, while SIEM combines data from various sources to detect anomalies and correlate incidents. The integrated use of both technologies can increase the accuracy and speed of response to information leakage threats.

The paper analyzes the problem of information security and confidential information leakage based on the integration of DLP and SIEM systems, defines its purpose and objectives. An analysis of existing technologies for monitoring and responding to security incidents in modern organizations is carried out. The main functions of DLP and SIEM systems, their advantages and limitations, as well as integration methods are investigated. The main challenges and approaches to the implementation of an integrated system are identified.

Based on the research, the procedure for applying the technology of integrating DLP and SIEM systems for monitoring and responding to security incidents is proposed. Recommendations for information security professionals on the implementation of this integration and methods for evaluating its effectiveness are developed.

Field of application – cybersecurity, protection of confidential information and rapid response to incidents in organizations.

SECURITY INCIDENT, DLP, SIEM, SYSTEMS INTEGRATION, SECURITY MONITORING, DATA PROTECTION, RESPONSE AUTOMATION, MODULES, FUNCTIONS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

AWS – Amazon Web Services

CAP – Content Aware Protection

CVE – Common Vulnerabilities and Exposures

DLP – Data Loss Prevention

DDoS – Distributed Denial-of-Service

GCP – Google Cloud Platform.

GDPR – General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

ISO – International Organization for Standardization

NIST – National Institute of Standards and Technology

NTP – Network Time Protocol

NVD – National Vulnerability Database

PCI DSS – Payment Card Industry Data Security Standard.

SaaS – Software as a Service

SIEM – Security Information and Event Management

SOC – Security Operations Center

SSH – Secure Shell

SSL – Secure Sockets Layer

TLS – Transport Layer Security

WAF – Web Application Firewall

XDR – Extended Detection and Response

ОС – Операційна Система

ПК – Персональний комп'ютер

ВСТУП

Актуальність дослідження. Технології Data Loss Prevention (DLP) та Security Information and Event Management (SIEM) стали важливою складовою сучасних систем кібербезпеки в організаціях. Це зумовлено значним зростанням кількості інцидентів витоку даних і кібератак, які загрожують конфіденційності, цілісності та доступності інформації. Організації потребують ефективних рішень для моніторингу загроз і швидкого реагування на інциденти безпеки з метою мінімізації ризиків і забезпечення дотримання нормативних вимог.

Збільшення обсягів даних та ускладнення кіберзагроз створюють потребу в комплексних підходах до захисту інформаційних систем. Технології DLP дозволяють запобігати витоку конфіденційних даних, а SIEM-системи надають засоби для централізованого збору, аналізу та кореляції даних про події безпеки в реальному часі. Інтеграція цих технологій сприяє не лише виявленню загроз, але й автоматизації процесів реагування.

Завдяки використанню SIEM для обробки великих обсягів журналів і DLP для контролю витоку інформації організації можуть створити комплексні механізми безпеки, які дозволяють оперативно реагувати на потенційні інциденти та забезпечувати захист критичних даних. Окрім цього, інтеграція таких технологій відповідає потребам сучасних гібридних робочих середовищ, де значна частина співробітників працює віддалено, використовуючи різноманітні пристрої та платформи.

Таким чином, розробка інтегрованих рішень на основі DLP і SIEM є важливим завданням для сучасних організацій, які прагнуть мінімізувати ризики витоку даних та ефективно управляти інцидентами безпеки. Актуальність даної теми полягає у потребі впровадження ефективних методів моніторингу та реагування, що забезпечують надійний захист інформаційних активів.

Об'єкт дослідження – автоматизація реагування на інцидент безпеки за рахунок інтеграції DLP та SIEM систем.

Предмет дослідження – технології інтеграції DLP та SIEM для забезпечення комплексного моніторингу та реагування на інциденти безпеки.

Мета роботи – розробити підхід до інтеграції технологій DLP та SIEM з метою підвищення ефективності моніторингу та реагування на інциденти безпеки в інформаційних системах.

Наукові завдання:

- провести аналіз сучасних загроз та проблем моніторингу і реагування на інциденти безпеки;
- дослідити можливості технологій DLP та SIEM у контексті моніторингу загроз і запобігання витоку даних;
- проаналізувати сучасні методи інтеграції DLP та SIEM;
- запропонувати модель інтеграції DLP та SIEM для підвищення ефективності захисту інформаційних систем;
- розробити рекомендації щодо впровадження інтегрованої технології моніторингу та реагування.

Методи дослідження – аналіз літературних джерел і експлуатаційної документації, моделювання процесів моніторингу та реагування, порівняння міжнародних стандартів з кібербезпеки, обробка результатів експериментів з інтеграції систем.

Практичне значення одержаних результатів полягає у створенні рекомендацій для інтеграції технологій DLP та SIEM, що дозволить організаціям ефективно запобігати інцидентам безпеки, мінімізувати ризики витоку інформації та забезпечувати високий рівень захисту даних.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

1.1. Дослідження проблеми реагування на інциденти безпеки в інформаційних системах організацій

1.1.1. Актуальність проблеми інцидентів безпеки

Згідно з цьогорічним дослідженням від IBM Cost of a Data Breach Report 2024, середня світова вартість витоку даних зросла на 10% порівняно з попереднім роком, сягнувши відмітки у 4,88 млн доларів США, що є найбільшим стрибком з часів пандемії (рис. 1.1). Зростання витрат пов'язане з переривання роботи бізнесу, а також підтримкою та усуненням наслідків витоку даних вже після інциденту [1].

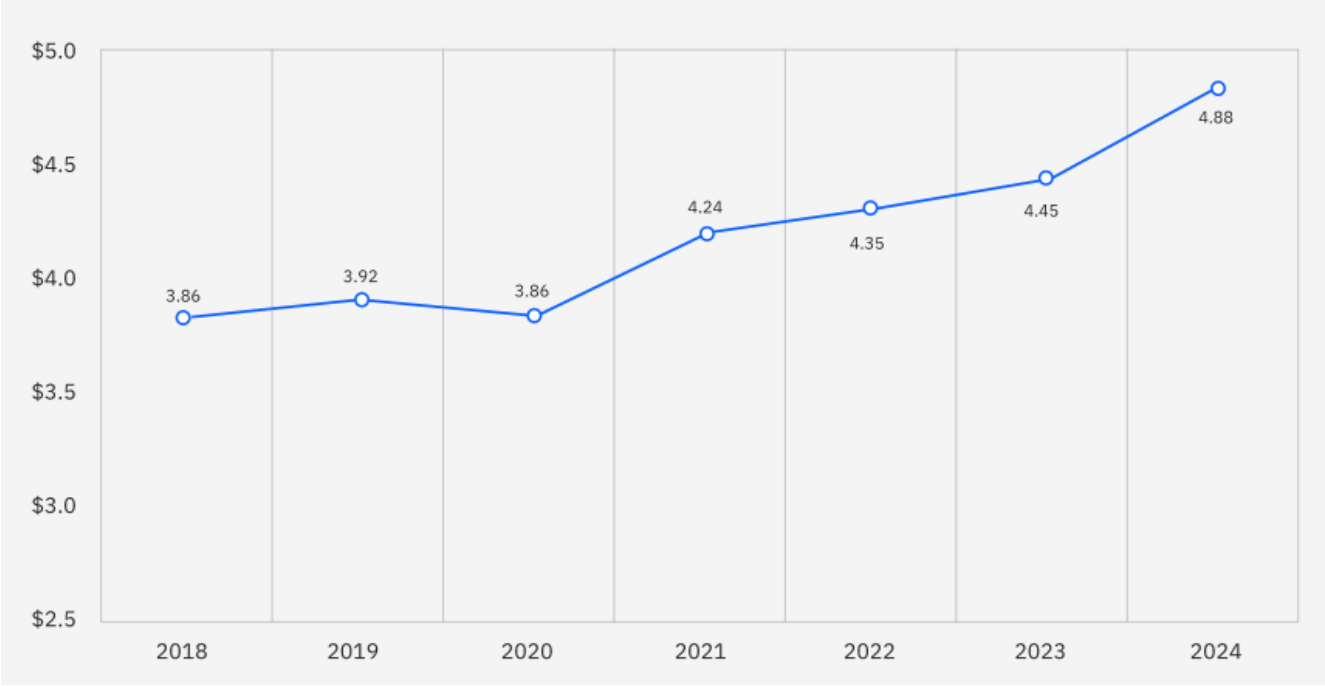


Рис. 1.1. Графік зростання вартості витоку даних

Команда дослідників також виявила, що застосування автоматизації безпеки та ШІ окупається, знижуючи витрати на порушення в деяких випадках в середньому на 2,2 мільйона доларів США. Рішення з використанням штучного інтелекту та автоматизації скорочують час, необхідний для виявлення та

локалізації порушень і пов'язаних з ними збитків. Інакше кажучи, команди з кібербезпеки без використання ШІ та автоматизації варто очікувати, що їм знадобиться більше часу на виявлення та локалізацію витоку, а це також означає, що відповідно зростуть збитки від кіберінциденту.

Цьогорічне дослідження показало, що більше половини організацій, які зазнали кібератак, зіткнулися з гострою нестачею кадрів у сфері кібербезпеки, причому розрив у навичках теж збільшився. Ця проблема зросла на 26,2% порівняно з попереднім роком, що призвело до збільшення збитків в середньому на 1,76 мільйона доларів США [1]. Незважаючи на те, що кожна п'ята організація стверджує, що використовує певні інструменти безпеки на основі штучного інтелекту, які, як очікується, допоможуть подолати цей розрив за рахунок підвищення продуктивності та ефективності, дефіцит навичок залишається серйозною проблемою. Нестача кваліфікованого персоналу зростає в міру того, як розширюється спектр загроз.

Порівняно з іншими векторами кібератак, зловмисні інсайдерські атаки призвели до найбільших витрат в цьому році, що в середньому становить 4,99 млн доларів США. Серед інших збиткових для організацій векторів атак: компрометація електронної пошти, фішинг, соціальна інженерія та викрадені або компрометація облікових даних. Засоби ШІ можуть відіграють вагому роль у створенні деяких з цих фішингових атак. Наприклад, завдяки штучному інтелекту навіть тим, хто не володіє мовою цілі, стає простіше, створювати граматично правильні та правдоподібні фішинг-повідомлення.

1.1.2. Поняття події та інциденту у контексті кібербезпеки

Передусім важливо зрозуміти, що таке подія та інцидент у контексті кібербезпеки.

Подія – це будь-яке явище, що спостерігається в системі або мережі. Події включають такі явища, як підключення користувача до загального файлового ресурсу, отримання сервером запиту, відправлення користувачем електронної пошти та блокування брандмауером спроби підключення [2].

Інцидент – це подія, яка фактично або потенційно загрожує конфіденційності, цілісності та доступності інформаційної системи або інформації, яку ця система обробляє, зберігає та передає, або подія яка є порушенням чи неминучою загрозою порушення політики безпеки, процедур безпеки або політики прийнятного використання [2].

Таким чином, інцидент у сфері кібербезпеки визначається як зловмисна подія. Це може статися внаслідок реальної атаки на систему, потенційної загрози, що виникла через нещодавню подію, або порушення політик безпеки. Коли такий інцидент виявляється, починається процес реагування на інцидент. Цей процес є необхідним, оскільки людський фактор часто призводить до надмірної реакції та недотримання необхідних дій під час обробки інциденту. Тому більшість організацій мають спеціалізовану команду, яка проходить навчання для роботи в таких ситуаціях і, маючи налагоджений процес реагування, здатна професійно локалізувати загрозу.

Процес реагування на інциденти складається з кількох етапів. Початковий етап включає в себе формування та навчання команди реагування на інциденти, а також набуття необхідних інструментів і ресурсів. Під час підготовки, організація також намагається обмежити кількість можливих інцидентів, обираючи та впроваджуючи набір заходів контролю на основі результатів оцінки ризиків. Однак залишковий ризик неминуче зберігатиметься. Тому виявлення порушень безпеки є необхідним для попередження організації про виникнення інцидентів. Залежно від серйозності інциденту, організація може пом'якшити його наслідки шляхом локалізації проблеми та в підсумку відновлення.

На цьому етапі діяльність часто повертається до виявлення та аналізу, наприклад, для визначення чи інфіковані додаткові кінцеві точки шкідливим ПЗ під час усунення інциденту з вірусом. Після належного оброблення інциденту організація складає звіт, у якому детально викладені причина та вартість інциденту, а також кроки, які слід вжити для запобігання подібним інцидентам у майбутньому.

У цій кваліфікаційній роботі детально описані основні етапи процесу реагування на інциденти: підготовка, виявлення та аналіз, локалізація, усунення та відновлення, а також заходи після інциденту (рис. 1.2).

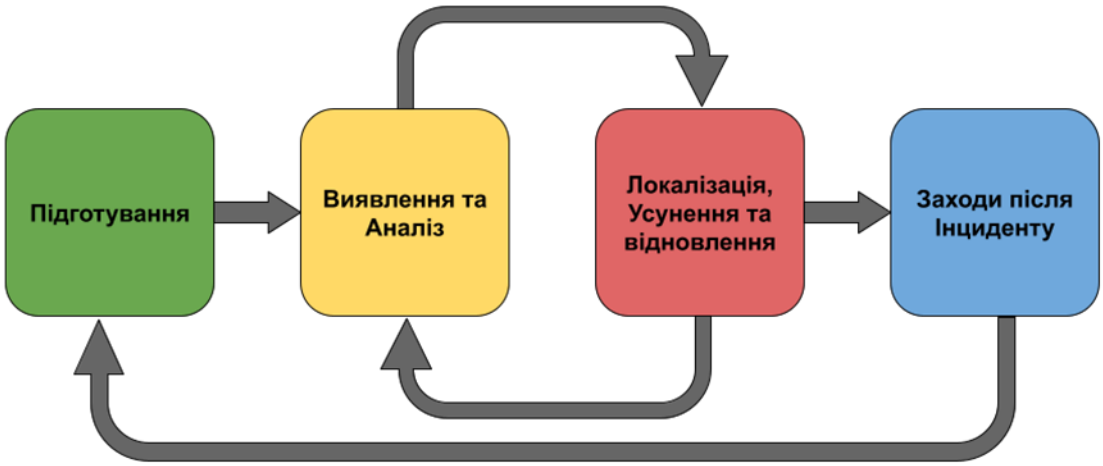


Рис. 1.2. Основні етапи процесу реагування на інциденти

1.2. Підготовка та необхідні ресурси для реагування на інциденти безпеки

1.2.1. Підготовка до управління інцидентами кібербезпеки

Етап перший – підготовка (рис. 1.3). Методології реагування на інциденти зазвичай підкреслюють важливість підготовки, не лише встановлення здатності реагувати на інциденти, щоб організація була готова до реагування на інциденти, а й запобігання інцидентам шляхом забезпечення постійного достатнього рівня безпеки систем, мереж і додатків. Правильне підготування є однією з основ успіху у питанні реагування на інциденти.

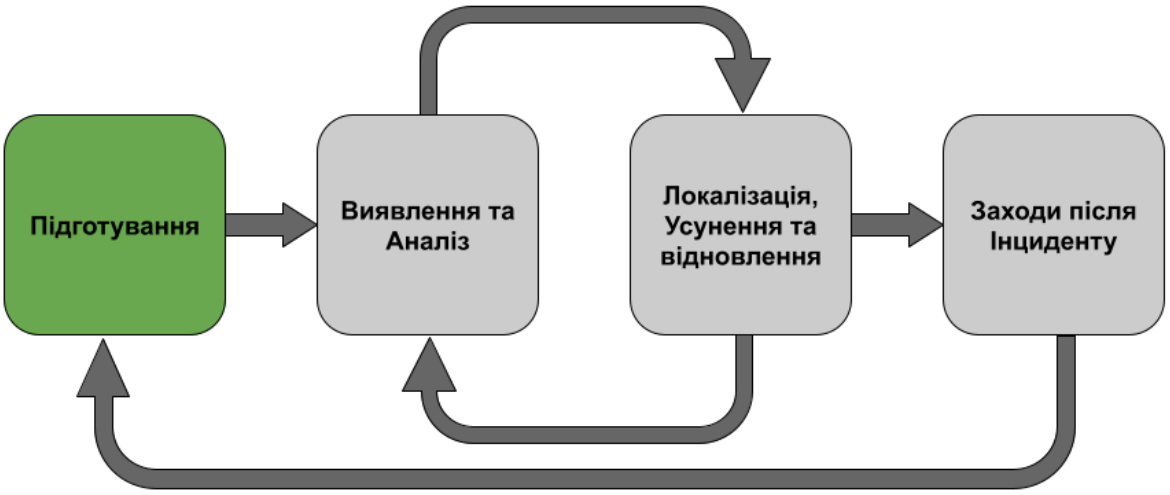


Рис. 1.3. Етап підготування

Нижчезазначений перелік надає приклади інструментів і ресурсів, які можуть бути корисними під час обробки інцидентів. Ці списки призначені для початкової дискусії про те, які інструменти та ресурси можуть бути потрібні фахівцям з управління інцидентами в організації. Наприклад, смартфони можуть слугувати надійним засобом для зв'язку та координації в надзвичайних ситуаціях. Організація повинна мати кілька (окремих і різних) механізмів зв'язку та координації на випадок відмови одного з механізмів, список яких вказано нижче [2]:

1) комунікації та засоби фахівців з управління інцидентами:

а - контактна інформація для членів команди та інших осіб в межах та за межами організації (основні та резервні контакти), такі як правоохоронні органи та інші команди реагування на інциденти; інформація може включати номери телефонів, адреси електронної пошти, публічні ключі шифрування (відповідно до нижчеописаного програмного забезпечення для шифрування) та інструкції для перевірки особи контакту;

б - інформація для інших команд в організації, включаючи дані про ескалацію та їх виклик за вимогою;

в - механізми звітування та повідомлення про інциденти, такі як номери телефонів, адреси електронної пошти, онлайн-форми та безпечні системи миттєвого обміну повідомленнями, які користувачі можуть використовувати для

повідомлення про підозрювані інциденти; щонайменше один механізм повинен дозволяти анонімне повідомлення про інциденти;

г - система для відстеження інформації про інциденти, їх статусу тощо;

ґ - смартфони для членів команди для підтримки поза робочими годинами та зв’язку на місці;

д - програмне забезпечення для шифрування, яке використовується для комунікацій між членами команди, в межах організації та зі сторонніми особами;

е - оперативний центр для централізованого зв'язку та координації SOC;

є - безпечне сховище для забезпечення збереження доказів та інших чутливих матеріалів;

2) апаратура та програмне забезпечення для аналізу інцидентів:

а - робочі станції для цифрової криміналістики та/або резервні пристрої для створення образів дисків, збереження лог-файлів та інших релевантних даних інциденту;

б - ноутбуки для аналізу даних, перехоплення пакетів та написання звітів;

в - запасні робочі станції, сервери та мережеве обладнання або віртуалізовані середовища, які можуть використовуватися для багатьох цілей, таких як відновлення резервних копій та тестування шкідливого ПЗ;

г - порожні знімні носії;

ґ - портативний принтер для друку копій лог-файлів та інших доказів;

д - пристрої для перехоплення пакетів і аналізу протоколів для захоплення та аналізу мережевого трафіку;

е - програмне забезпечення для цифрової криміналістики для аналізу образів дисків;

є - знімні носії з перевіреними версіями програм для збору доказів з систем;

3) ресурси для аналізу інцидентів:

а - списки портів, включаючи поширені порти та порти, що містять троянське ПЗ;

б - документація для операційних систем, додатків, протоколів, а також продуктів для виявлення вторгнень і антивірусного захисту;

в - схеми мережі та списки критичних активів, таких як сервери баз даних;

г - поточні базові графіки очікуваної активності мережі, системи та додатків;

ґ - криптографічні хеші критичних файлів для прискорення аналізу інцидентів, перевірки та усунення наслідків;

д - доступ до образів з «чистими» файлами для встановлення операційних систем і додатків для відновлення та оновлення.

Кожен фахівець з управління інцидентами повинен мати доступ принаймні до двох обчислювальних пристроїв (наприклад, персональний комп'ютер або ноутбук), щоб обробляти інформацію про інцидент та здійснювати свою роботу в зручному режимі. Один ноутбук, наприклад, слід використовувати для аналізу трафіку, аналізу зловмисного програмного забезпечення та всіх інших дій, які можуть зашкодити ноутбуку, який їх виконує. Перш ніж використовувати цей ноутбук для іншого інциденту, його слід очистити і перевстановити все програмне забезпечення.

1.2.2 Запобігання інцидентам кібербезпеки

Утримання кількості інцидентів на розумно низькому рівні є критично важливим для захисту бізнес-процесів організації. Якщо контроль безпеки є недостатнім, може виникнути більша кількість інцидентів, що перевантажить команду реагування на інциденти. Це може призвести до повільного та неповного реагування, що, в свою чергу призводить до більш негативного впливу на організацію (наприклад, до більш масштабних пошкоджень, довших періодів обслуговування та недоступності даних). Група реагування на інциденти може виявити проблеми, про які організація не знає; група може відігравати ключову роль в оцінці ризиків і навчанні, виявляючи слабкі місця.

Основні рекомендовані практики для захисту мереж, систем і додатків:

- Оцінювання ризиків. Періодичні оцінки ризиків систем і додатків повинні визначати, які ризики створюють комбінації загроз і вразливостей. Це повинно включати розуміння відповідних загроз, в тому числі загроз, характерних для організації. Кожному ризику слід визначити пріоритетність, відповідно ризики можна пом'якшити, передати або прийняти, поки не буде досягнутий

обґрунтований прийнятний загальний рівень ризику. Ще однією перевагою регулярного проведення оцінки ризиків є визначення критично важливих ресурсів, що дозволяє персоналу зосередити увагу на моніторингу та реагуванні на ці ресурси;

- Безпека кінцевих точок. Всі кінцеві точки повинні бути належним чином захищені за допомогою стандартних конфігурацій. На додаток до своєчасного оновлення кожної кінцевої точки, їх слід налаштувати за принципом найменших привілеїв, надаючи користувачам лише ті привілеї, які необхідні для виконання їхніх завдань. На кінцевих точках має проводитись неперервний аудит, і вони повинні реєструвати важливі події, пов'язані з безпекою. Безпека кінцевих точок та їхніх конфігурацій повинна постійно контролюватися. Багато організацій використовують протокол автоматизації безпеки контенту (SCAP), що містить контрольні списки конфігурації операційної системи та додатків, які допомагають послідовно та ефективно забезпечувати безпеку;

- Мережева безпека. Периметр мережі повинен бути налаштований таким чином, щоб заборонити будь-яку діяльність, яка не є прямо дозволеною. Це включає захист усіх точок підключення, таких як віртуальні приватні мережі (VPN) та виділені з'єднання з іншими організаціями;

- Запобігання шкідливому програмному забезпеченню. Програмне забезпечення для виявлення та блокування шкідливого ПЗ має бути розгорнуте в усій організації. Захист від шкідливого ПЗ має бути розгорнутий на рівні КТ (наприклад, операційні системи серверів та робочих станцій), на рівні сервера додатків (наприклад, сервер електронної пошти, веб-проксі сервери) та на рівні клієнта додатків (наприклад, клієнти електронної пошти, клієнти обміну миттєвими повідомленнями);

- Навчання користувачів. Користувачі повинні бути ознайомлені з політиками та процедурами щодо належного використання мереж, систем та додатків. Покращення обізнаності користувачів щодо інцидентів має зменшити частоту інцидентів. ІТ-персонал повинен бути навчений, щоб він мав можливість

підтримувати свої мережі, системи та додатки відповідно до стандартів безпеки організації.

1.3. Виявлення та аналіз інцидентів кібербезпеки

Етап другий – виявлення та аналіз (рис. 1.4). Виявлення інцидентів кібербезпеки є критичним етапом у забезпеченні захисту інформаційних систем, оскільки саме на цьому етапі закладається основа для подальшого ефективного реагування та мінімізації наслідків. Інциденти кібербезпеки можуть бути викликані як зовнішніми загрозами (атаки зловмисників, шкідливе ПЗ, фішинг), так і внутрішніми (зловмисна чи необережна поведінка співробітників). Тому важливим завданням є створення системи, яка дозволяє швидко ідентифікувати підозрілі дії та події, що порушують політики безпеки організації.

Процес виявлення базується на моніторингу подій із різних джерел, таких як журнали операційних систем, мережевий трафік, події доступу до файлів та дії користувачів.

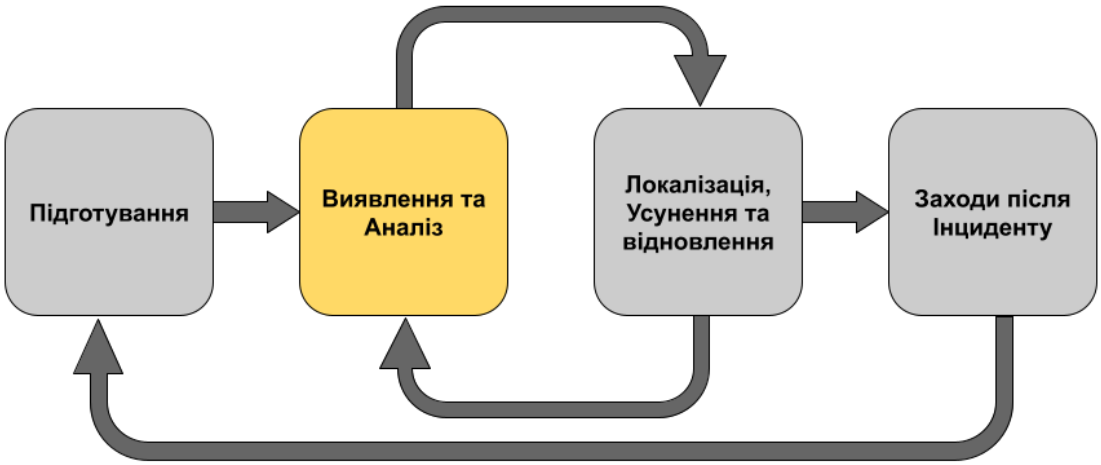


Рис. 1.4. Етап виявлення та аналізу

1.3.1. Вектори ймовірних атак

Існує незліченна кількість способів, як можуть відбуватися інциденти, тому розробка покрокових інструкцій для вирішення кожного окремого інциденту є недоцільною в цій ситуації. За ідеальних умов, організації повинні бути загалом

готові до будь-якого інциденту, але при цьому потрібно акцентувати увагу на готовності справлятися з інцидентами, що використовують поширені відомі вектори атак. Різні типи інцидентів потребують різних стратегій реагування.

Наведені нижче вектори атак не призначені для визначення остаточної класифікації інцидентів. Скоріше, вони перелічують загальні методи атак, які можуть слугувати основою для визначення більш специфічних процедур обробки:

- Зовнішні/знімні носії: атака, що виконується з використанням знімних носіїв або периферійних пристроїв, наприклад, розповсюдження шкідливого коду на систему з інфікованого USB накопичувача;

- Атака на виснаження: атака, що використовує методи брутфорсу для компрометації, деградації або знищення систем, мереж або відмовлення в обслуговуванні (наприклад, DDoS-атака, спрямована на ускладнення або блокування доступу до сервісу чи додатка; брутфорс-атака проти механізму автентифікації, такого як паролі, CAPTCHA, або цифрові підписи);

- Веб-атака: атака, що виконується з вебсайту або веб-додатку, наприклад,

атака «міжсайтового скриптингу» (XXS), використана для крадіжки облікових даних, або перенаправлення на сайт, що експлуатує вразливість браузера та встановлює шкідливе ПЗ;

- Електронна пошта: атака, що виконується через електронне повідомлення або вкладення, наприклад, експлойт-код, замаскований під вкладений документ, або посилання на шкідливий вебсайт в тілі електронного повідомлення;

- Атака підміни: атака, що полягає в заміні чогось безпечного на щось шкідливе. Сюди входять такі атаки як, наприклад: спуфінг, атаки "людина посередині" (MITM), злочинні бездротові точки доступу та SQL-ін’єкції;

- Неправильне використання: будь-який інцидент, що виникає внаслідок порушення користувачем затвердженої політики безпеки організації. Наприклад, користувач встановлює програмне забезпечення для обміну файлами, що призводить до втрати чутливих даних; або користувач виконує незаконні дії в системі;

- Втрати або крадіжка обладнання: втрата або крадіжка обчислювального пристрою або носія, що використовується організацією, наприклад, ноутбук, смартфон або токен автентифікації.

Однією з найскладніших частин реагування на інциденти є точне виявлення та оцінка можливих інцидентів, тобто визначення, чи дійсно відбувся інцидент, і, якщо це дійсно так, то якого типу, які масштаби та які наслідки він може спричинити.

Складність цього процесу обумовлюється наступними пунктами:

- Інциденти можуть бути виявлені багатьма різними способами, з різним рівнем деталізації та достовірності. Автоматизовані рішення виявлення включають мережеві та хостові системи виявлення вторгнень (Intrusion Detection and Prevention System IDPS), антивірусне програмне забезпечення та аналізатори журналів. Інциденти також можуть бути виявлені вручну, наприклад, через проблеми, про які повідомляють користувачі. Деякі інциденти мають явні ознаки, які можна легко виявити, проте інші виявити майже неможливо;

- Показник кількості потенційних ознак інцидентів зазвичай є високим. Наприклад, часто команда з реагування отримує тисячі або навіть мільйони сповіщень від сенсорів виявлення вторгнень на день, які насправді є хибнопозитивними;

- Для належного та ефективного аналізу даних, пов’язаних з інцидентами необхідні глибокі, спеціалізовані технічні знання та великий досвід.

Ознаки інциденту поділяються на дві категорії: прекурсор та індикатори [2].

Прекурсор – це ознака того, що інцидент може статися в майбутньому.

Індикатор – це ознака того, що інцидент, можливо, стався або може відбуватися зараз.

З погляду цілі, більшість атак не мають жодних прекурсорів, які можна ідентифікувати або виявити. Якщо ж прекурсори виявлено, в організації може з’явитися можливість запобігти інциденту шляхом зміни заходів убезпечення, для захисту цілі від атаки. Мінімально можливий варіант – коли організація уважніше стежить за всім, що пов’язане з ціллю.

Прикладами прекурсорів є:

- Записи журналу веб-сервера, які демонструють використання сканера вразливостей;

- Оголошення про новий експлойт, що націлюється на уразливість поштового сервера організації;

- Загроза від групи кіберзловмисників, яка заявляє, що буде атакувати організацію.

Індикатори, в свою чергу є дуже поширеними. Деякі їх приклади наведені нижче:

- Сенсор мережевого виявлення вторгнень сповіщає, коли відбувається спроба переповнення буфера на сервері бази даних;

- Антивірусне програмне забезпечення сповіщає, коли виявляє, що хост інфікований шкідливим ПЗ;

- Адміністратор системи бачить ім’я файлу з незвичайними символами;

- Програма реєструє кілька невдалих спроб входу з незнайомої віддаленої системи;

- Адміністратор електронної пошти бачить велику кількість відхилених електронних листів зі підозрілим вмістом;

- Адміністратор мережі помічає незвичайні відхилення від звичайних мережевих трафіків.

Попередники та індикатори виявляються за допомогою багатьох різних джерел, серед яких найпоширенішими є сповіщення програмного забезпечення з безпеки комп’ютерів, журнали, інформація, доступна публічно, та люди.

1.3.2. Рішення та засоби для сповіщення про інциденти, джерела прекурсорів та індикаторів

Для сповіщення про інциденти та визначення прекурсорів та індикаторів використовується багато різних джерел, серед яких найпоширенішими є сповіщення програмного забезпечення, що сприяє комп’ютерній безпеці, журнали, відкрита інформація та люди. У таблиці 1.1 представлено поширені джерела прекурсорів та індикаторів для кожної категорії.

Таблиця 1.1.

Загальні джерела попередників та індикаторів для кожної категорії

Джерело	Опис
Сповіщення від систем та рішень ІБ	
IDPS	Продукти категорії виявлення та запобігання атакам/вторгненням (IDPS) виявляють підозрілі події та записують відповідні дані про них, включаючи дату і час виявлення атаки, тип атаки, IP-адреси джерела та призначення, а також ім'я користувача (якщо це можливо і відомо). Більшість продуктів IDPS використовують сигнатури атак для виявлення зловмисної активності; сигнатури повинні постійно оновлюватися, щоб можна було виявити найновіші атаки. Програмне забезпечення IDPS часто видає помилкові спрацьовування - сповіщення, які вказують на наявність зловмисної активності, хоча насправді її не було.
Антивірусне та антиспамове програмне забезпечення	Антивірусне програмне забезпечення виявляє різні форми шкідливого програмного забезпечення, генерує попередження та запобігає зараженню комп'ютерів. Сучасні антивірусні продукти ефективно зупиняють багато видів шкідливого програмного забезпечення, якщо їхні сигнатури постійно оновлюються. Антиспам використовується для виявлення спаму та запобігання його потраплянню до поштових скриньок користувачів. Спам може містити шкідливе програмне забезпечення, фішингові атаки та інший шкідливий вміст, тому сповіщення від антиспаму можуть вказувати на спроби атаки.
DLP	Рішення для запобіганню витоку даних (DLP) виявляє та допомагає запобігти небезпечному або неналежному обміну, передачі чи використанню конфіденційної інформації, аналізуючи трафік передачі файлів та поведінку користувачів.

Продовження таблиці 1.1.

Програмне забезпечення для перевірки файлів на предмет порушень цілісності	Програмне забезпечення для перевірки цілісності файлів може виявити зміни, внесені до важливих файлів під час інцидентів. Воно використовує алгоритм хешування для отримання криптографічної контрольної суми для кожного визначеного файлу. Якщо файл змінено, а контрольну суму перераховано, існує надзвичайно висока ймовірність того, що нова контрольна сума не збігатиметься зі старою контрольною сумою. Регулярно перераховуючи контрольні суми і порівнюючи їх з попередніми значеннями, можна виявити зміни у файлах.
SIEM	Продукти для управління інформацією та подіями безпеки (SIEM) схожі на продукти IDPS, але вони генерують сповіщення на основі аналізу даних журналів.
Моніторингові сервіси від третіх сторін	Треті сторони пропонують різноманітні платні та безкоштовні послуги з моніторингу. Наприклад, служби виявлення шахрайства, які сповіщають організацію, якщо її IP-адреси, доменні імена тощо пов'язані з поточною активністю інцидентів за участю інших організацій. Існують також безкоштовні чорні списки в режимі реального часу з подібною інформацією. Іншим прикладом сторонньої служби моніторингу є список сповіщень CSIRC; ці списки часто доступні лише для інших команд реагування на інциденти.
Журнали та графіки	
Журнали операційної системи, служб і застосунків	Журнали операційних систем, служб та додатків (особливо дані, пов'язані з аудитом) часто мають велику цінність при виникненні інцидентів, наприклад, записи про те, до яких облікових записів було здійснено доступ та які дії були виконані. Організації повинні вимагати базовий рівень ведення журналів

Продовження таблиці 1.1.

Журнали операційної системи, служб і застосунків	Журнали операційних систем, служб та додатків (особливо дані, пов'язані з аудитом) часто мають велику цінність при виникненні інцидентів, наприклад, записи про те, до яких облікових записів було здійснено доступ та які дії були виконані. Організації повинні вимагати базовий рівень ведення журналів для всіх систем і більш високий базовий рівень для критично важливих систем. Журнали можна використовувати для аналізу шляхом зіставлення інформації про події. Залежно від інформації про подію може бути згенероване сповіщення, яке вказує на інцидент.
Журнали мережевих пристроїв	Журнали мережевих пристроїв, таких як брандмауери та маршрутизатори, зазвичай не є основним джерелом прекурсорів або індикаторів. Хоча ці пристрої зазвичай налаштовані на реєстрацію заблокованих спроб з'єднання, вони надають мало інформації про характер активності. Тим не менш, вони можуть бути цінними для виявлення мережевих тенденцій та кореляції подій, виявлених іншими пристроями.
Потік трафіку в мережі	Мережевий потік - це конкретний сеанс зв'язку, що відбувається між кінцевими точками. Маршрутизатори та інші мережеві пристрої можуть надавати інформацію про мережевий потік, яку можна використовувати для виявлення аномальної мережевої активності, спричиненої шкідливим програмним забезпеченням, витоком даних та іншими зловмисними діями. Існує багато стандартів для форматів даних про потік, зокрема NetFlow, sFlow та IPFIX.

Продовження таблиці 1.1.

Персонал	
Люди з організації	Користувачі, системні адміністратори, мережеві адміністратори, співробітники служби безпеки та інші працівники організації можуть повідомляти про ознаки інцидентів. Запис цієї оцінки разом з наданою інформацією може суттєво допомогти під час аналізу інциденту, особливо у випадку виявлення суперечливих даних.
Люди з інших організацій	До повідомлень про інциденти, які надходять ззовні, слід ставитися серйозно. Наприклад, до організації може звернутися особа, яка стверджує, що її системи атакують. Зовнішні користувачі можуть також повідомляти про інші ознаки, такі як пошкоджена веб-сторінка або недоступна послуга. Важливо мати механізми, за допомогою яких зовнішні користувачі можуть повідомляти про інциденти, а навчений персонал - ретельно відстежувати ці механізми.
Інформація з відкритих джерел	
Інформація про нові вразливості та експлойти	Відстеження нових вразливостей та експлойтів може запобігти деяким інцидентам, а також допомогти у виявленні та аналізі нових атак. Національна база даних вразливостей (NVD) містить інформацію про вразливості. Такі організації, як US-CERT та CERT періодично надають оновлену інформацію про загрози через брифінги, публікації в Інтернеті та списки розсилки.

1.3.3. Аналіз інцидентів кібербезпеки

Виявлення та аналіз інцидентів були б легшими, якби кожен прекурсор або індикатор був гарантовано точним, але це не так. Системи виявлення вторгнень можуть створювати помилки першого роду (хибнопозитивні спрацювання) – некоректні індикатори. В ідеальних умовах, спочатку потрібно перевірити кожен індикатор, щоб визначити, чи є він дійсним, це і робить виявлення та аналіз

реальних інцидентів кібербезпеки таким складним завданням, тому що загальна кількість індикаторів може становити тисячі або мільйони на день.

Навіть якщо індикатор точний, це не обов'язково означає, що інцидент стався. Деякі індикатори, такі як збій сервера або зміна критичних файлів, можуть статися з різних причин, окрім інциденту безпеки, включно з людськими помилками. У деяких випадках ситуацію слід обробляти однаково незалежно від того, пов'язана вона з безпекою чи ні. Наприклад, якщо організація втрачає підключення до Інтернету кожні 12 годин, і ніхто не знає причини, персонал захоче вирішити проблему якомога швидше і використає ті самі ресурси для діагностики проблеми незалежно від її причини.

Деякі інциденти легко виявити, наприклад очевидне пошкодження веб-сторінки. Проте багато інцидентів не мають таких чітких симптомів. Невеликі ознаки, такі як одна зміна в одному конфігураційному файлі системи, можуть бути єдиними індикаторами того, що інцидент дійсно стався. У роботі з інцидентами виявлення може бути найскладнішим завданням. Працівники, які займаються обробкою інцидентів, повинні аналізувати неоднозначні, суперечливі та неповні симптоми, щоб визначити, що сталося. Хоча існують технічні рішення, які можуть полегшити виявлення, найкращим засобом є створення команди висококваліфікованих і досвідчених співробітників, які можуть ефективно та швидко аналізувати прекурсори та індикатори й вживати відповідних заходів. Без добре навченого та компетентного персоналу виявлення та аналіз інцидентів будуть здійснюватися неефективно, що призведе до дорогих помилок.

Команда реагування на інциденти повинна швидко аналізувати та перевіряти кожен інцидент, дотримуючись заздалегідь визначеного процесу та документуючи кожен зроблений крок. Коли команда вважає, що інцидент стався, вона має швидко провести початковий аналіз, щоб визначити обсяг інциденту, наприклад, які мережі, системи або програми постраждали; хто або що спричинило інцидент; і як відбувається інцидент (наприклад, які інструменти або методи атаки використовуються, які вразливості експлуатуються). Початковий аналіз має надати

достатньо інформації, щоб команда могла пріоритизувати наступні дії, такі як стримування інциденту та глибший аналіз його наслідків.

Ось кілька рекомендацій для полегшення та підвищення ефективності аналізу інцидентів:

- Профілювання мережі та системи. Профілювання – це вимірювання характеристик очікуваної активності, щоб зміни можна було легше виявити. Прикладами профілювання є використання програмного забезпечення для перевірки цілісності файлів на кінцевих точках для отримання контрольних сум критичних файлів і моніторинг використання пропускної здатності мережі, щоб визначити середній і максимальний рівень використання в різні дні та години. На практиці виявляти інциденти точно за допомогою більшості технік профілювання важко, організації повинні використовувати профілювання як один із кількох методів виявлення та аналізу;

- Аналіз очікуваної поведінки. Члени команди реагування на інциденти повинні вивчати мережі, системи та програми, щоб зрозуміти, якою є їхня очікувана поведінка, щоб легше було розпізнавати аномалії. Часті перевірки журналів допоможуть зберегти знання актуальними, і аналітик зможе помічати тенденції та зміни з часом. Ці перевірки також дають аналітику уявлення про надійність кожного джерела;

- Створення політики збереження журналів. Інформація щодо інциденту може бути записана в кількох місцях, таких як журнали брандмауера, системи виявлення вторгнень і журнали додатків. Створення та реалізація політики збереження журналів, яка вказує, як довго слід зберігати дані журналів, може бути надзвичайно корисною для аналізу та дослідження, оскільки старі записи журналів можуть показати розвідувальну активність або попередні випадки подібних атак. Ще одна причина для збереження журналів – те, що інциденти можуть бути виявлені лише через дні, тижні або навіть місяці;

- Кореляція подій. Докази інциденту можуть бути зафіксовані в кількох журналах з різних джерел, кожен з яких містить різні типи даних, наприклад журнал брандмауера може мати IP-адресу джерела, тоді як журнал додатку може

містити ім’я користувача. Мережева система виявлення вторгнень може виявити атаку, запущену на певній кінцевій точці, але не може точно підтвердити, чи була атака успішною, аналітику може знадобитися перевірити різні журнали, щоб визначити це. Кореляція подій між кількома джерелами індикаторів може бути надзвичайно корисною для підтвердження того, що певний інцидент дійсно стався;

- Забезпечення синхронізації годинників усіх кінцевих точок**.** Протоколи, такі як протокол синхронізації часу (NTP), синхронізують годинники між кінцевими точками. Кореляція подій буде більш складною, якщо пристрої, що повідомляють про події, мають різні налаштування відображення часу. З точки зору доказової бази, бажано мати однакові часові мітки в журналах, наприклад, мати три журнали, які показують, що атака сталася о 18:12:24, замість журналів, які вказують, що атака сталася о 18:12:24, 15:12:24 і 13:40:06;

- Підтримка та використання бази знань в актуальному стані. База знань повинна містити інформацію, яку аналітики можуть швидко використовувати під час аналізу інцидентів. Текстові документи, електронні таблиці та відносно прості бази даних забезпечують ефективні та гнучкі пошукові механізми для обміну даними серед членів команди реагування. База знань також повинна містити різноманітну інформацію, включаючи пояснення значущості та дійсності прекурсорів та індикаторів, таких як сповіщення IDPS, записи журналів операційної системи та коди помилок додатків;

- Використання засобів перехоплення пакетів для збору додаткових даних. Іноді індикатори не реєструють достатньо деталей, щоб дозволити спеціалісту зрозуміти, що відбувається. Якщо інцидент відбувається в мережі, найшвидшим способом зібрати необхідні дані може бути запуск перехоплювача пакетів для захоплення мережевого трафіку, наприклад WireShark. Налаштування перехоплювача для запису трафіку, що відповідає певним критеріям, повинно зберегти обсяг даних керованим і зменшити випадкове захоплення іншої інформації. Через проблеми з конфіденційністю деякі організації можуть вимагати, щоб фахівці з управління інцидентами запитували та отримували дозвіл перед використанням перехоплювачів пакетів;

- Фільтрація даних. Зазвичай команді з реагування недостатньо часу, щоб переглядати та аналізувати всі індикатори, але принаймні найпідозріліша активність повинна бути розслідувана. Однією з ефективних стратегій є фільтрація категорій індикаторів, які зазвичай є незначними. Інша стратегія фільтрації полягає в показі лише категорій індикаторів, які визначені як пріоритетні. Однак цей підхід несе суттєвий недолік – нова шкідлива активність може не потрапити в одну з завчасно вибраних категорій індикаторів.

1.3.4. Пріоритизація інцидентів

Пріоритизація обробки інцидентів є одним з найкритичніших моментів у процесі обробки інцидентів. Інциденти не повинні оброблятися за принципом "черги" через обмеження ресурсів. Натомість обробка повинна бути пріоритизована на основі відповідних факторів, таких як:

- Функціональний вплив інциденту. Інциденти, які націлюються на IT-системи, зазвичай впливають на бізнес процеси. Фахівці з управління інцидентами повинні визначити поточний та потенційний вплив інциденту на організацію, якщо він не буде якнайшвидше локалізований;

- Вплив на інформацію. Інциденти можуть негативно вплинути на конфіденційність, цілісність та доступність інформації. Наприклад, витік чутливих даних може негативно вплинути не лише на організацію, але й на партнерів та акціонерів;

- Можливість відновлення. Масштаб інциденту та тип ресурсів на які він впливає, визначає скільки часу і ресурсів буде потрібно для відновлення. У деяких випадках відновитися після інциденту неможливо (наприклад, якщо була порушена конфіденційність таємної, службової чи конфіденційної інформації), і в такому випадку немає сенсу витрачати обмежені ресурси на подовжений цикл управління інцидентами, якщо ці зусилля не будуть спрямовані на забезпечення того, щоб подібного випадку не сталося в майбутньому. В інших випадках для управління інцидентом може знадобитися набагато більше ресурсів ніж ті, що є в організації. Фахівці з управління інцидентами мають враховувати зусилля, необхідні для фактичного відновлення після інциденту, і ретельно продумувати, наскільки ці

зусилля будуть варті мети, задля якої вони застосовуються, та як зусилля з відновлення співвідносяться з будь-якими вимогами з управління інцидентами [1].

Об'єднання оцінки функціонального та інформаційного впливу визначає вплив інциденту на бізнес процеси. Наприклад, атака DDoS на публічний веб-сервер може призвести до тимчасових труднощів у доступі користувачів, тоді як несанкціонований доступ може призвести до значної витоку даних, що може критично зашкодити репутації організації.

Можливість відновлення після інциденту визначає й можливе реагування, якого може вжити команда під час управління інцидентами. Інцидент із високими функціональними наслідками і низькими зусиллями для відновлення є ідеальним «кандидатом» для негайного вжиття дій від команди. Водночас для деяких інцидентів може не бути легких шляхів відновлення, і, можливо, реагування на них має бути на більш стратегічному рівні – наприклад для інциденту, який призводить до передачі зловмисником гігабайтів конфіденційних даних та їх оприлюднення, немає легкого шляху відновлення, оскільки витік даних вже стався. У цьому випадку команда може передати частину відповідальності за управління інцидентом з передачею даних команді більш стратегічного рівня, яка розробляє стратегію запобігання майбутнім порушенням і створює план роз’яснювальної роботи для оповіщення тих осіб або організацій, чиї дані було передано. Команда повинна пріоритезувати реагування на кожен інцидент на основі оцінювання наслідків для бізнесу, спричинених інцидентом, та попереднього оцінювання зусиль, необхідних для відновлення після інциденту [1].

1.4. Локалізація інциденту та подальше відновлення

Етап третій – локалізація, усунення та відновлення (рис. 1.5). Локалізація інциденту кібербезпеки є одним із найважливіших етапів реагування, оскільки саме на цьому етапі зусилля спрямовуються на обмеження впливу інциденту на інформаційну систему та мінімізацію шкоди. Основна мета локалізації полягає у відокремленні джерела загрози та запобіганні подальшому поширенню інциденту.

Ефективна локалізація базується на оперативному виявленні ключових компонентів, які залучені до інциденту, таких як скомпрометовані кінцеві точки, пошкоджені файли чи вектори атак.

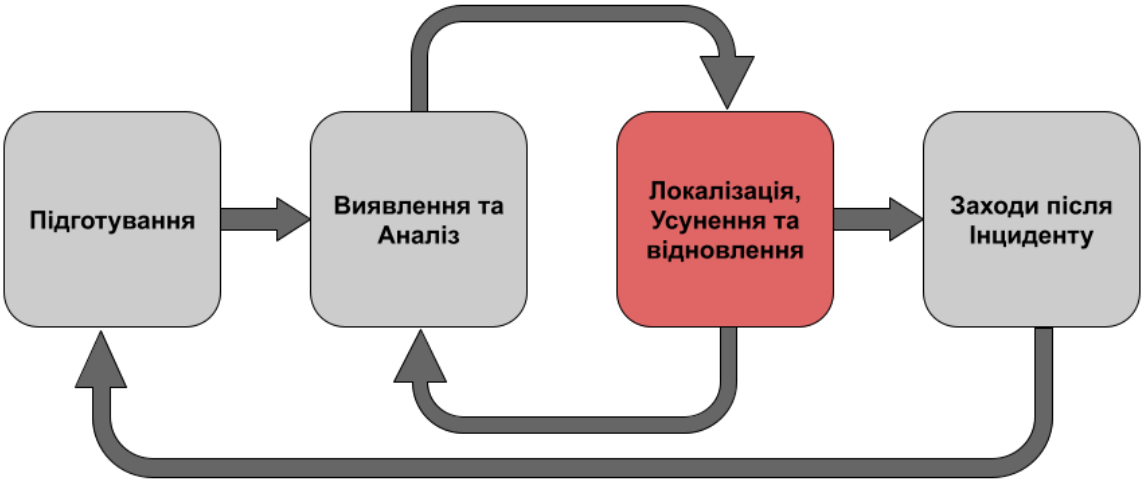


Рис. 1.5. Етап локалізації, усунення та відновлення

1.4.1. Стратегії локалізації інциденту

Своєчасна локалізація інциденту має вагомий вплив на подальші збитки для організації. Важливо локалізувати інцидент до того, як він перевантажить ресурси або збільшить збитки. Більшість інцидентів потребують локалізації, тому це важливо враховувати на ранній стадії роботи з кожним інцидентом. Локалізація дає час для розробки індивідуальної стратегії відновлення. Важливою частиною локалізації є прийняття певних рішень, наприклад: вимкнути систему, відключити її від мережі, вимкнути певні функції.

Стратегії локалізації інцидентів різняться залежно від типу інциденту. Наприклад, стратегія стримування зараження шкідливим програмним забезпеченням через електронну пошту суттєво відрізняється від стратегії стримування мережевої DDoS-атаки. Організації повинні розробити окремі стратегії стримування для кожного типу інциденту з чітко задокументованими критеріями, щоб полегшити процес прийняття рішень.

У певних випадках деякі організації перенаправляють зловмисника до так званої «пісочниці» (форма ізоляції), щоб можна було спостерігати за його діяльністю, як правило, для збору додаткових доказів та інформації про проведення

атаки, що являє собою стратегію відкладеної локалізації. Проте, не слід використовувати інші способи моніторингу діяльності зловмисника, окрім ізольованого середовища. Якщо організація знає, що система була скомпрометована, і дозволяє зловмиснику продовжувати виконувати атаку, вона може понести за це відповідальність, якщо зловмисник використає скомпрометовану систему для ланцюгової атаки на інші системи. Отже, стратегія відкладеного стримування небезпечна тим, що зловмисник може розширити несанкціонований доступ або скомпрометувати інші системи.

Ще однією потенційною проблемою локалізації є те, що деякі атаки можуть завдати додаткової шкоди, коли їх локалізують. Наприклад, скомпрометована кінцева точка може запустити зловмисну програму, яка періодично відправляє команду «ping» на іншу систему в мережі. Коли фахівець з реагування на інциденти намагається локалізувати інцидент, відключивши скомпрометовану систему від мережі, запити «ping» команди будуть невдалими, що в свою чергу може спровокувати шкідливе ПЗ запустити скрипт, який може перезаписати або зашифрувати дані на диску. Отже, фахівець з реагування не повинен робити завчасних висновків, що вимкненням кінцевої точки з мережі захистило її від подальшого пошкодження.

1.4.2. Ліквідація наслідків та відновлення.

Після локалізації інциденту може знадобитися ліквідація для усунення компонентів інциденту, таких як видалення шкідливого програмного забезпечення та відключення порушених облікових записів користувачів, а також виявлення та усунення всіх вразливостей, які були використані. Під час усунення інциденту важливо виявити всі уражені хости в організації, щоб їх можна було виправити. Для деяких інцидентів ліквідація або не потрібна, або виконується під час відновлення.

Під час відновлення адміністратори повертають системи до нормальної роботи, підтверджують, що системи функціонують нормально, і (якщо це можливо) усувають вразливості, щоб запобігти повторенню подібних інцидентів. Відновлення може включати такі дії, як відновлення систем з чистих резервних

копій, відновлення систем з нуля, заміна скомпрометованих файлів чистими версіями, встановлення патчів, зміна паролів і посилення безпеки мережевого периметра (наприклад, набори правил брандмауера, списки контролю доступу на граничних маршрутизаторах). Частиною процесу відновлення часто є вищий рівень системного логування або моніторингу мережі. Після успішної атаки на ресурс його часто атакують знову, або аналогічним чином атакують інші ресурси в організації.

Ліквідацію та відновлення слід здійснювати поетапно, щоб визначити пріоритетність заходів з відновлення. Для масштабних інцидентів відновлення може зайняти місяці; метою ранніх етапів має бути підвищення загальної безпеки за допомогою відносно швидких (від кількох днів до кількох тижнів) важливих змін для запобігання майбутнім інцидентам. На більш пізніх етапах слід зосередитися на довгострокових змінах (наприклад, змінах в інфраструктурі) і постійній роботі, спрямованій на забезпечення максимальної безпеки підприємства.

1.5. Організаційні заходи після інциденту

Етап четвертий – організаційні заходи після інциденту (рис. 1.6). Організаційні заходи після інциденту кібербезпеки є заключним етапом у забезпеченні довготривалої стійкості організації до загроз. Вони включають комплекс дій, спрямованих на аналіз причин інциденту, усунення системних недоліків, адаптацію процесів та покращення політик безпеки організації. Цей етап є критичним для підвищення кіберстійкості та мінімізації ризику повторення подібних інцидентів у майбутньому.

Першочерговим завданням після завершення технічного реагування є ретроспективний аналіз інциденту. Такий аналіз має включати визначення джерела загрози, оцінку вразливостей, які були використані, а також аналіз реакції команди на інцидент. Це дозволяє виявити не лише технічні слабкі місця, але й організаційні недоліки, такі як недостатня підготовка персоналу чи відсутність чітких інструкцій щодо дій у критичних ситуаціях.

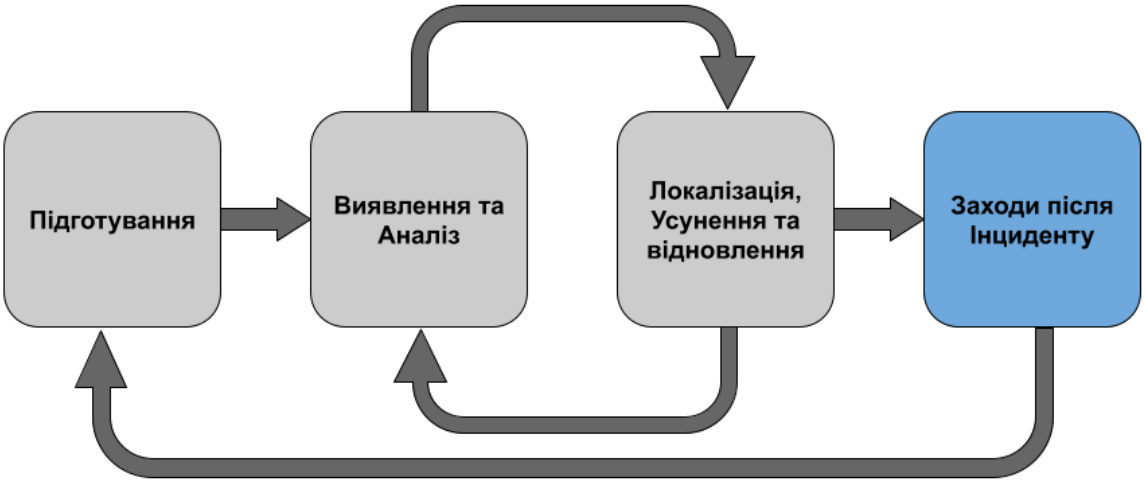


Рис. 1.6. Заходи після інциденту

Одна з найважливіших складових реагування на інциденти, про яку найчастіше забувають: навчання та вдосконалення. Кожна команда реагування на інциденти повинна розвиватися, щоб відображати нові загрози, вдосконалені технології та отримані уроки. Проведення зустрічі для обговорення отриманих уроків з усіма залученими сторонами після великого інциденту, а також, за бажанням, періодично після менших інцидентів, якщо дозволяють ресурси, може бути надзвичайно корисним для вдосконалення заходів безпеки та самого процесу реагування на інциденти. Кілька інцидентів можуть бути розглянуті на одній нараді з аналізу отриманих уроків. Ця зустріч дає можливість підбити підсумки щодо інциденту, проаналізувавши те, що сталося, що було зроблено для втручання та наскільки ефективним виявилося втручання. Зустріч має бути проведена протягом декількох днів після закінчення інциденту. Питання, на які слід відповісти на цій зустрічі, включають:

- Що саме сталося, в який день та о котрій годині?
- Наскільки добре впоралися працівники та керівництво під час боротьби з інцидентом? Чи всі дотримувалися задокументованого порядку? Він відповідав ситуації?
- Яку інформацію необхідно було отримати раніше?
- Чи було вжито якихось кроків або заходів, котрі, можливо, загальмували процес відновлення?

- Що персонал та керівництво робитимуть інакше, коли наступного разу станеться подібний інцидент?
- Як можна було покращити обмін інформацією з іншими організаціями?
- Які коригувальні заходи можуть запобігти подібним інцидентам у майбутньому?
- На які прекурсори чи індикатори слід звертати увагу в майбутньому, щоб виявити подібні випадки?
- Які додаткові інструменти чи ресурси необхідні для виявлення, аналізу та пом'якшення наслідків майбутніх інцидентів?

Завдяки опрацюванню засвоєного досвіду має виникнути набір об'єктивних та суб'єктивних даних щодо кожного інциденту. З часом зібрані дані про інциденти стануть корисними в кількох аспектах. Дані, зокрема загальна кількість годин роботи і витрати на ліквідацію наслідків, можуть бути використані для обґрунтування додаткового фінансування команди реагування на інцидент. Вивчення характеристик інцидентів може вказати на слабкості та загрози безпеки у системі, а також на зміни тенденцій у сфері інцидентів. Ці дані можна використати в процесі оцінювання ризику, що в кінцевому підсумку приведе до вибору та запровадження додаткових інструментів контролю. Ще один варіант використання даних із користю – це вимірювання успіху команди реагування на інциденти.

Дані про інциденти також можна збирати, щоб визначити, чи спричиняє зміна потенціалу реагування на інциденти відповідні зміни в роботі команди (наприклад, підвищення ефективності, зниження витрат). Більше того, організаціям, котрі зобов'язані повідомляти чи звітувати про інциденти, необхідно буде збирати необхідні дані, щоб відповідати поставленим вимогам.

Організації мають зосередитися на зборі даних, які можна корисно використати. Наприклад підрахунок кількості сканувань портів із прекурсорами, котрі відбуваються щотижня, і створення діаграми наприкінці року, яка показує збільшення кількості сканувань портів на вісім відсотків, не дуже корисно і може бути трудомістким процесом. Абсолютні цифри не інформативні – важливо

зрозуміти, яку вони становлять загрозу для бізнес-процесів організації. Організації мають вирішити, які дані про інциденти збирати на основі вимог до звітності та очікуваної ефективності інвестицій (наприклад, виявлення нової загрози та пом'якшення наслідків вразливостей, пов'язаних із нею, перш ніж ними скористаються). В таблиці 1.2 зібрані основні етапи реагування на інциденти, які варто додати в політику безпеки організації.

Таблиця 1.2.

Основні етапи реагування на інциденти

Етапи	
Виявлення та аналіз	
1	Визначення, чи інцидент насправді стався
1.1	Аналіз прекурсорів та індикаторів
1.2	Кореляція інформації
1.3	Проведення дослідження
1.4	Після підтвердження, що інцидент дійсно стався, почати документувати розслідування та збирати докази
2	Пріоритизація управління інцидентом на основі відповідних чинників (функціональні наслідки, інформаційні наслідки інциденту, зусилля, які необхідно докласти для відновлення після інциденту)
3	Відправка повідомлення та звіту про інцидент відповідному персоналу
Локалізація, ліквідація наслідків та відновлення	
4	Зберігання та документація доказів
5	Локалізація інциденту
6	Ліквідація інциденту
6.1	Виявлення і пом'якшення наслідків всіх вразливостей, котрими скористалися зловмисники
6.2	Видалення зловмисного ПЗ, скомпрометованих файлів та інших складових атаки
7	Відновлення після інциденту

Продовження таблиці 1.2.

7.1	Повернення систем, що постраждали, до стану готовності до роботи
7.2	Перевірка, що постраждалі системи, функціонують нормально
7.3	Впровадження додаткового моніторингу для пошуку майбутньої схожої активності
Заходи після інциденту	
8	Створення звіту та плану про подальші дії у разі виникнення схожого інциденту та проведення зустрічі для обговорення та засвоєння досвіду

2 АНАЛІЗ ВИКОРИСТАННЯ DLP ТА SIEM СИСТЕМ ДЛЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ НА БАЗІ ІНТЕГРАЦІЇ РІШЕНЬ ENDPOINT PROTECTOR ТА WAZUH

2.1. Призначення, можливості та функції DLP-систем

2.1.1. Визначення та основні завдання DLP-систем

DLP, або Data Leak Prevention, -- це рішення в сфері кібербезпеки, яке виявляє та запобігає витоку даних за межі організації. DLP дозволяє компаніям виявляти втрату даних, а також запобігати незаконній передачі даних за межі організації та небажаному знищенню конфіденційних або персональних даних (PII). DLP допомагає організаціям забезпечити безпеку даних і дотримуватися таких нормативних вимог, як: загальний регламент ЄС про захист даних (GDPR)Закон про переносимість і відповідальність у сфері медичного страхування (HIPAA) та Стандарт безпеки даних індустрії платіжних карток PCI DSS.

Отже, рішення DLP допомагає компаніям:

- Покращити та прискорити реагування на інциденти, дотримуватися політики безпеки компанії, швидко виявляючи мережеві аномалії та неналежну активність користувачів;

- Відповідати стандартам відповідності, таким як HIPAA, GDPR і PCI DSS, шляхом класифікації та зберігання конфіденційних, приватних, службових та інших важливих для бізнесу даних;

- Отримувати сповіщення про несанкціоновану передачу чутливих даних, та шифрування знімних носіїв;

- Покращити видимість конфіденційних даних на всіх кінцевих точках;

- Зменшити фінансові ризики, пов'язані з втратою або витоком даних, особливо в разі атак зловмисників з вимогою викупу;

- Зменшити ймовірність репутаційної шкоди шляхом запобігання витоку даних та швидкого виявлення інцидентів безпеки для мінімізації наслідків інцидентів.

Витік даних зазвичай відбувається одним із наведених нижче способів:

- Випадковий витік даних. Багато витоків даних є ненавмисними і непередбачуваними. Прикладом випадкового витоку може бути надсилання електронного листа з конфіденційною інформацією до неправильного списка розсилки.

- Загроза інсайдерів. Витік даних може статися через нинішніх або колишніх співробітників, підрядників або партнерів, які мають доступ до конфіденційних даних в організації. Цей тип зловмисників може здійснити витік інформації з різних причин: особиста вигода, помста або бажання забрати інформацію з собою, коли вони переходять на іншу роботу.

- Зловмисні атаки. Витік даних є кінцевою метою багатьох кібератак. Кіберзлочинці часто викрадають дані після отримання несанкціонованого доступу до IT-середовища за допомогою шкідливого програмного забезпечення, використаних вразливостей, фішингових атак, соціальної інженерії або атак з вимогою викупу.

- Незахищені або вкрадені пристрої. Пристрої, особливо портативні, можуть бути викрадені, що може призвести до втрати даних і витоку інформації. Вкрай важливо, щоб політики DLP впроваджували належні заходи використання цих пристроїв, щоб запобігти крадіжкам і компрометації даних.

2.1.2. Технології захисту від витоку даних

Рішення Data Leak Prevention аналізує вміст і контекст даних, що покидають периметр мережі організації, включно з даними, надісланими електронною поштою та миттєвими повідомленнями в чаті. Аналіз вмісту розглядає конкретний вміст повідомлень, а аналіз контексту – зовнішні фактори, такі як розмір і формат повідомлення.

Інструменти DLP використовують різні методи для аналізу вмісту файлу, щоб переконатися, що він відповідає політикам захисту від витоку даних. Якщо

дані, що передаються порушують політику DLP, система може заблокувати вихід інформації за межі організації, сповістивши про це службу безпеки.

2.2. Аналіз DLP рішення Endpoint Protector

Endpoint Protector (рис. 2.1) – це DLP рішення для запобігання витоку даних (Data Loss Prevention, DLP), яка забезпечує всебічний захист конфіденційної інформації в корпоративних середовищах. Рішення спрямоване на виявлення, моніторинг і блокування небажаних спроб передачі даних за межі організації через кінцеві пристрої.

Netwrix
Endpoint Protector

Рис 2.1. Логотип Endpoint Protector

Endpoint Protector підтримує всі популярні операційні системи, такі як macOS, Windows та більшість дистрибутивів Linux. Endpoint Protector посів перше місце в номінації «DLP» по версії G2 2022 році [3].

Рішення складається з модулів, які можна комбінувати та підбирати відповідно до потреб організації (див. рис. 2.2).

Рис 2.2. Зображення основних модулів в користувацькому інтерфейсі

1) Модуль Device Control. Зовнішні пристрої, такі як флеш-накопичувачі, Bluetooth та інші портативні USB-пристрої, є однією з головних причин інцидентів безпеки, які можуть завдати значної шкоди будь-якому бізнесу. Збитки варіюються від викрадення конфіденційних даних до величезних штрафів через порушення норм і правил стандартів відповідності. Кінцеві користувачі повинні усвідомлювати ризики, а компанії - вживати заходів для запобігання витоку даних із зовнішніх пристроїв.

Device Control – це перший рівень безпеки, який забезпечує Endpoint Protector. безпека кінцевих точок забезпечується завдяки визначенню детальних прав доступу до USB і периферійних портів, при збереженні продуктивності. Як крос-платформне рішення, воно захищає всю мережу, включно зі знімними пристроями, незалежно від того, чи працюють комп'ютери під управлінням Windows, macOS або Linux.

2) Модуль Content Aware Protection. Використовуючи перевірку вмісту та контекстне сканування даних, Content Aware Protection захищає конфіденційні дані від несанкціонованого доступу та проникнення зловмисників на кінцевих точках співробітників. Контекстне сканування запобігає неналежному обміну конфіденційними даними через електронну пошту, контролює корпоративні програми обміну повідомленнями такі як Slack, завантаження файлів в браузері, передачу файлів на USB-пристрої та по Bluetooth. При цьому політики блокування витоку продовжують працювати навіть коли кінцева точка знаходиться у режимі офлайн.

Знижуючи ризик внутрішніх загроз і втрати даних через зловмисних, недбалих і скомпрометованих користувачів, Content Aware Protection розширює можливості захисту, які вже пропонує модуль Device Control. Модуль неперервно захищає конфіденційні дані від випадкової або зловмисної передачі поза контролем.

3) Модуль Enforced Encryption. Enforced Encryption використовує 256-бітове шифрування AES для захисту даних, що передаються на портативні USB-накопичувачі, від втрати або крадіжки. Це рішення посилює політики контролю

пристроїв і замінює потребу в дорогих апаратних рішеннях, автоматично шифруючи конфіденційні дані, що передаються на дозволені та надійні USB-накопичувачі. Enforced Encryption дозволяє організації захистити конфіденційні дані та досягти відповідності нормативним вимогам NIST, HIPAA, PCI-DSS, GDPR, SOX та інших, уникаючи штрафів та інших збитків, накладених контролюючими органами.

Програма Enforced Encryption автоматично завантажується на USB-накопичувач під час першого використання. Після цього програма дозволяє переміщення файлів і автоматично розміщує їх у захищеному паролем зашифрованому контейнері на накопичувачі. Адміністратори безпеки можуть керувати зашифрованими пристроями за допомогою адміністративної консолі Endpoint Protector.

4) Модуль eDiscovery. eDiscovery застосовується для даних у стані спокою. Модуль сканує та ідентифікує конфіденційну інформацію на кінцевих точках організацій і дозволяє адміністраторам вжити заходів для виправлення ситуації, наприклад, зашифрувати або видалити дані у стані спокою. eDiscovery протидіє як внутрішнім, так і зовнішнім загрозам - неавторизованим співробітникам, які зберігають конфіденційні дані на своїх комп'ютерах, і зловмисникам, яким вдається обійти мережевий захист і спробувати заволодіти документацією компанії.

Endpoint Protector підтримує різноманітні варіанти розгортання, такі як:

- Віртуальна машина. Доступна у форматах VMX, PVA, OVF, OVA, XVA і VHD, сумісний з найпопулярнішими інструментами віртуалізації.

- Хмарний сервіс. Доступний для розгортання в наступних хмарних сервісах: Amazon Web Services, Microsoft Azure або Google Cloud Platform.

- Програмне забезпечення як послуга (SaaS). Зменшує складність та вартість розгортання, що дозволяє виділити більше ресурсів на виявленні та зменшенні ризиків для конфіденційних даних і менше на підтримці інфраструктури.

В таблиці 2.1 вказані мінімальні системні вимоги для локальної інсталяції системи.

Таблиця 2.1.

Системні вимоги при локальній інсталяції сервера EPP при масштабуванні до 100 агентів

CPU 2 Cores	4 GB RAM	320 GB HDD

В таблиці 2.2 вказані системні вимоги для використання агенту Endpoint Protector на кінцевій точці.

Таблиця 2.2.

Системні вимоги для функціонування агенту EPP на кінцевій точці для модулів EPP

Споживання ресурсів в умовах стрес-тесту			
Модуль	Device Control	Content Aware Protection	eDiscovery
CPU	1 GHz	1 GHz	1 GHz
RAM	30 MB	30 MB	30 MB
Пропускна здатність	Від 1 Kbs	Від 1 Kbs	Від 1 Kbs

2.3. Призначення, можливості та функції SIEM-систем

2.3.1. Поняття SIEM системи

Одним з найважливіших компонентів побудови ефективної кібербезпеки є рішення з інформаційної безпеки та управління подіями SIEM (Security Information and Event Management). SIEM системи збирають та аналізують великі обсяги даних з додатків, пристроїв, серверів та користувачів в режимі реального часу. Об'єднуючи цей величезний масив даних в єдину уніфіковану платформу, рішення SIEM надають комплексне уявлення про стан безпеки організації, дозволяючи центрам управління безпекою (SOC) швидко і ефективно виявляти, розслідувати і реагувати на інциденти безпеки.

Рішення SIEM можуть допомогти організаціям будь-якого розміру:

- Отримувати інформацію про стан безпеки завдяки централізації та аналізу даних з різних джерел;

- Виявляти та ідентифікувати потенційні порушення та загрози безпеки в режимі реального часу, мінімізуючи ризик компрометації;

- Розслідувати та фільтрувати інциденти безпеки, скорочуючи час та ресурси, необхідні для їх вирішення;

- Дотримуватися регуляторних та галузевих стандартів.

2.3.2. Основні компоненти SIEM системи

1) Управління журналами.

SIEM системи збирають і аналізують журнали з усієї організації, включаючи сервери, мережеві пристрої, брандмауери, інші рішення для забезпечення безпеки та хмарні додатки. Мета такого збору даних - виявити аномалії, які вказують на потенційну загрозу. Багато рішень SIEM також отримують канали розвідки загроз, які дозволяють командам безпеки виявляти і блокувати нові кіберзагрози.

2) Моніторинг та реагування на інциденти.

Щоб виявити загрози на ранніх стадіях і мінімізувати збитки, рішення SIEM здійснюють безперервний моніторинг систем організації. Результати аналізу відображаються в центральній інформаційній панелі (консолі), SIEM також надсилає сповіщення аналітикам з безпеки на основі заздалегідь визначених правил. Багато рішень SIEM також включають можливості автоматизованого реагування, тому в деяких випадках SIEM може діяти автоматично на основі правил, визначених SOC.

Наприклад, якщо рішення SIEM виявляє можливе шкідливе програмне забезпечення, воно може вжити заходів для ізоляції зараженої системи на основі попередньо визначених правил. Автоматизація допомагає прискорити реагування і звільняє аналітиків безпеки, щоб зосередитися на більш складних завданнях і проблемах.

3) Кореляція подій.

SIEM аналізують дані з різних систем організації шукаючи певні закономірності. Наприклад, якщо є дані про скомпрометований обліковий запис, а

також незвичайний мережевий трафік, SIEM може визначити, що ці дві події пов'язані між собою, і згенерувати сповіщення для команд безпеки для подальшого розслідування. Кореляція подій допомагає виявити активність, яка сама по собі здається нешкідливою, але в поєднанні з іншою активністю може бути індикатором компрометації.

2.4. Аналіз рішення SIEM системи Wazuh

2.4.1. Основний функціонал SIEM системи Wazuh

Wazuh - це безкоштовна платформа кібербезпеки з відкритим вихідним кодом, яка об'єднує можливості рішень розширеного виявлення та реагування XDR та SIEM систем. Вона забезпечує видимість подій безпеки в локальних, віртуалізованих, контейнерних і хмарних середовищах.

Як SIEM рішення, Wazuh допомагає організаціям захистити свої інформаційні активи від загроз безпеки пропонуючи наступні основні можливості:

- Аналіз журналів безпеки. Wazuh збирає, зберігає та аналізує дані про події безпеки, щоб виявити аномалії або ознаки компрометації. Платформа SIEM додає контекстну інформацію до сповіщень, щоб пришвидшити розслідування та скоротити середній час реагування;
- Виявлення вразливостей. Wazuh виявляє вразливості на відстежуваних кінцевих точках та визначає їх пріоритетність, щоб пришвидшити процес прийняття рішень;
- Оцінка конфігурації безпеки. Використовуйте можливості Wazuh SCA для виявлення неправильних конфігурацій і недоліків безпеки у вашій інфраструктурі. Wazuh сканує ваші системи на відповідність критеріям Центру інтернет-безпеки (CIS), щоб ви могли виявити та усунути вразливості, неправильні конфігурації або відхилення від найкращих практик і стандартів безпеки;
- Надсилання сповіщень. Wazuh відправляє сповіщення в режимі реального часу про інциденти, пов'язані з безпекою. Дане рішення співвідносить події з різних джерел, інтегрує канали розвідки загроз і надає інформаційні панелі та звіти. Це дає

змогу командам безпеки швидко реагувати на загрози та мінімізувати наслідки інцидентів безпеки.

Wazuh Extended Detection and Response (XDR) - це комплексне рішення для забезпечення безпеки, яке виявляє, аналізує та реагує на загрози на різних рівнях IT-інфраструктури. Wazuh збирає телеметричні дані з кінцевих точок, мережевих пристроїв, хмарних середовищ, сторонніх API та інших джерел для уніфікованого моніторингу та захисту безпеки.

З точки зору XDR системи, Wazuh містить такі основні вбудовані функції:

- Розширений аналіз поведінки. Можливості аналізу поведінки Wazuh передбачає використання розширеної аналітики для виявлення відхилень від нормальної поведінки, які можуть свідчити про потенційні загрози безпеці. Ця функція включає моніторинг цілісності файлів, мережевого трафіку, поведінки користувачів та аномалій у показниках продуктивності системи.

- Автоматизоване реагування. Wazuh автоматично реагує на загрози, щоб пом'якшити потенційний вплив на IT-інфраструктуру. Wazuh має вбудовані дії реагування на події, проте є можливість створювати власні дії відповідно до плану реагування на інциденти.

- Захист хмари. Wazuh забезпечує захист хмар і контейнерів. Wazuh має вбудовану інтеграцію з хмарними сервісами для збору та аналізу телеметрії. Рішення захищає хмарні середовища, включаючи інфраструктуру контейнеру, виявляючи та реагуючи на поточні та нові загрози.

- Розвідка загроз ІБ. Wazuh використовує канали розвідки загроз для виявлення відомих загроз і реагування на них. Він інтегрується з джерелами розвідки загроз, включаючи дані з відкритих джерел (OSINT), комерційні канали та дані, надані користувачами, щоб надавати актуальну інформацію про потенційні загрози.

2.4.2. Архітектура Wazuh

Рішення базується на агенті Wazuh, який розгортається на відстежуваних кінцевих точках, і на трьох центральних компонентах: сервері Wazuh, індексаторі Wazuh та інформаційній панелі Wazuh.

Призначення кожного компонента описано нижче:

- Сервер Wazuh аналізує дані, отримані від агентів. Він обробляє їх за допомогою декодерів і правил, використовуючи дані про загрози для пошуку відомих індикаторів компрометації (Indicators of compromise IOC). Один сервер може аналізувати дані від сотень і тисяч агентів. Цей центральний компонент також використовується для управління агентами, їх віддаленого налаштування та оновлення;

- Індексатор Wazuh - це високомасштабована повнотекстова пошуково-аналітична система. Цей центральний компонент індексує та зберігає сповіщення, згенеровані сервером Wazuh;

- Інформаційна панель Wazuh - це веб-інтерфейс користувача для візуалізації та аналізу даних. Вона включає в себе готові панелі для пошуку загроз, виявлених вразливих додатків, даних моніторингу цілісності файлів, результатів оцінки конфігурації, подій моніторингу хмарної інфраструктури та інших. Він також використовується для управління конфігурацією Wazuh та моніторингу її стану;

- Агенти Wazuh встановлюються на кінцевих точках, таких як ноутбуки, персональні комп'ютери, сервери, хмари або віртуальні машини. Вони надають можливості запобігання, виявлення та реагування на загрози. Вони працюють на таких операційних системах, як Linux, Windows, macOS, Solaris, AIX та HP-UX.

Архітектура Wazuh базується на агентах, які працюють на кінцевих точках, що контролюються, і пересилають дані про безпеку на центральний сервер. Підтримуються пристрої без агентів, такі як брандмауери, комутатори, маршрутизатори та точки доступу, які можуть активно надсилати дані журналів через Syslog, SSH або за допомогою свого API. Центральний сервер декодує та аналізує вхідну інформацію і передає результати індексатору Wazuh для індексації та зберігання.

Кластер індексаторів Wazuh - це сукупність одного або декількох вузлів, які взаємодіють між собою для виконання операцій читання та запису індексів. Кластери з декількома вузлами рекомендується використовувати, коли є багато

кінцевих точок, за якими ведеться спостереження, коли очікується великий обсяг даних або коли необхідна висока доступність.

Агент Wazuh постійно надсилає події на сервер Wazuh для аналізу та виявлення загроз. Щоб почати надсилати ці дані, агент встановлює з'єднання з серверною службою для підключення агентів, яка за замовчуванням працює через порт 1514. Потім сервер Wazuh декодує отримані події та перевіряє їх на відповідність правилам, використовуючи механізми аналізу. Події, які викликають спрацьовування правила, доповнюються такими даними, як ідентифікатор та назва правила.

Події можуть бути збережені в один або обидва з наступних файлів, залежно від того, чи спрацювало правило:

Файл /var/ossec/logs/archives/archives.json містить усі події, незалежно від того, чи спрацювало правило, чи ні.

Файл /var/ossec/logs/alerts/alerts.json містить лише події, які спрацювали правило з достатньо високим пріоритетом.

Протокол повідомлень Wazuh за замовчуванням використовує шифрування AES з 128 бітами на блок і 256-бітними ключами.

Вимоги до апаратного забезпечення значною мірою залежать від кількості кінцевих точок. Ця кількість може допомогти оцінити, скільки даних буде проаналізовано за певний проміжок часу і скільки оповіщень про загрози буде збережено та проіндексовано. У таблиці 2.3 показано рекомендоване обладнання для швидкого розгортання:

Таблиця 2.3.

Кількість агентів	CPU	RAM	Місце на диску
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

Центральні компоненти Wazuh можна встановити на 64-розрядну операційну систему Linux.

3 ТЕХНОЛОГІЯ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЇ НА БАЗІ ІНТЕГРАЦІЇ РІШЕНЬ DLP ENDPOINT PROTECTOR ТА SIEM WAZUH

3.1. Попередні налаштування DLP Endpoint Protector

Ефективне впровадження системи DLP Endpoint Protector (рис. 3.1) вимагає ретельного планування та налаштування її компонентів відповідно до потреб організації. Попередні налаштування включають конфігурацію основних політик захисту від витоку даних, визначення користувацьких груп та інтеграцію з іншими засобами безпеки.

Першочерговим кроком є ідентифікація конфіденційних даних, які підлягають захисту. Для цього необхідно провести аудит інформаційних активів організації, визначити категорії даних (наприклад, фінансова інформація, персональні дані, комерційна таємниця) та створити відповідні шаблони для їх виявлення. Endpoint Protector підтримує використання попередньо визначених шаблонів, а також створення власних із застосуванням ключових слів, регулярних виразів та інших критеріїв.

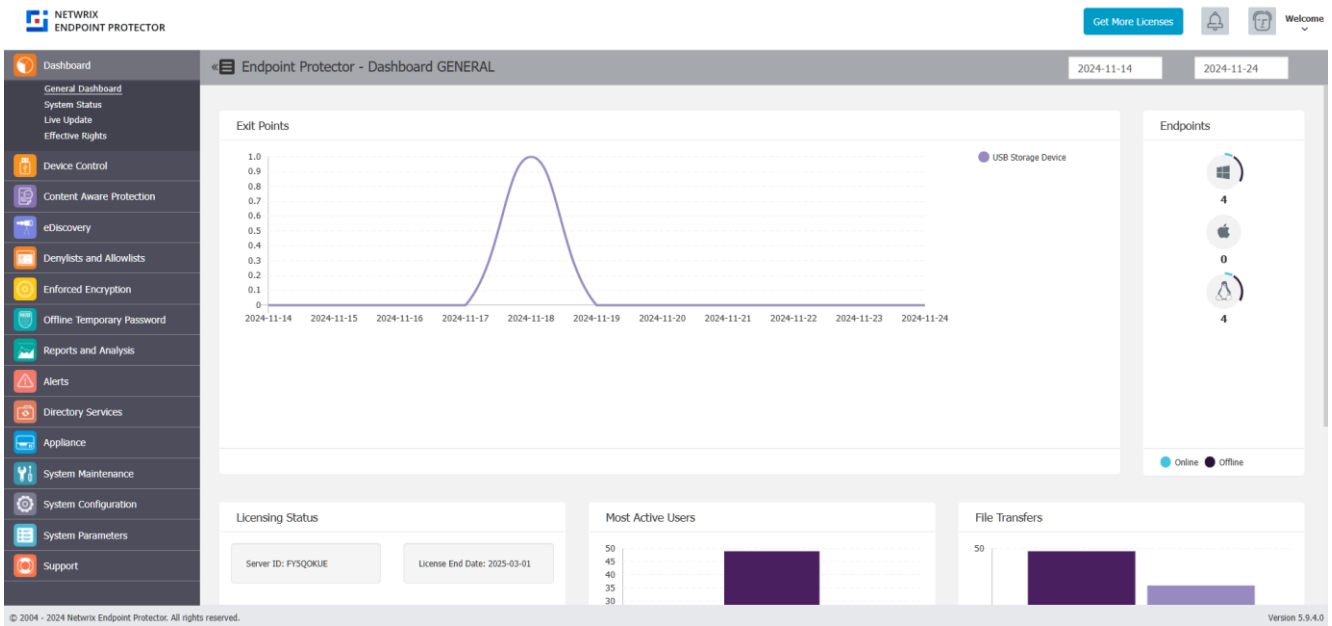


Рис 3.1. Інтерфейс консолі DLP Endpoint Protector

3.1.1. Налаштування політики безпеки Content Aware Protection

Для реалізації завдання моніторингу та реагування на інциденти безпеки можна використати модуль Content Aware Protection (CAP), що дозволяє створити і налаштувати політики моніторингу (див. рис. 3.2) та реагування на несанкціоновану передачу конфіденційної інформації.

Цей модуль підтримує детальні налаштування виявлення передачі файлів, що дозволяє зменшити кількість хибнопозитивних спрацювань та оптимізувати видимість руху файлів, що покидають периметр мережі організації.

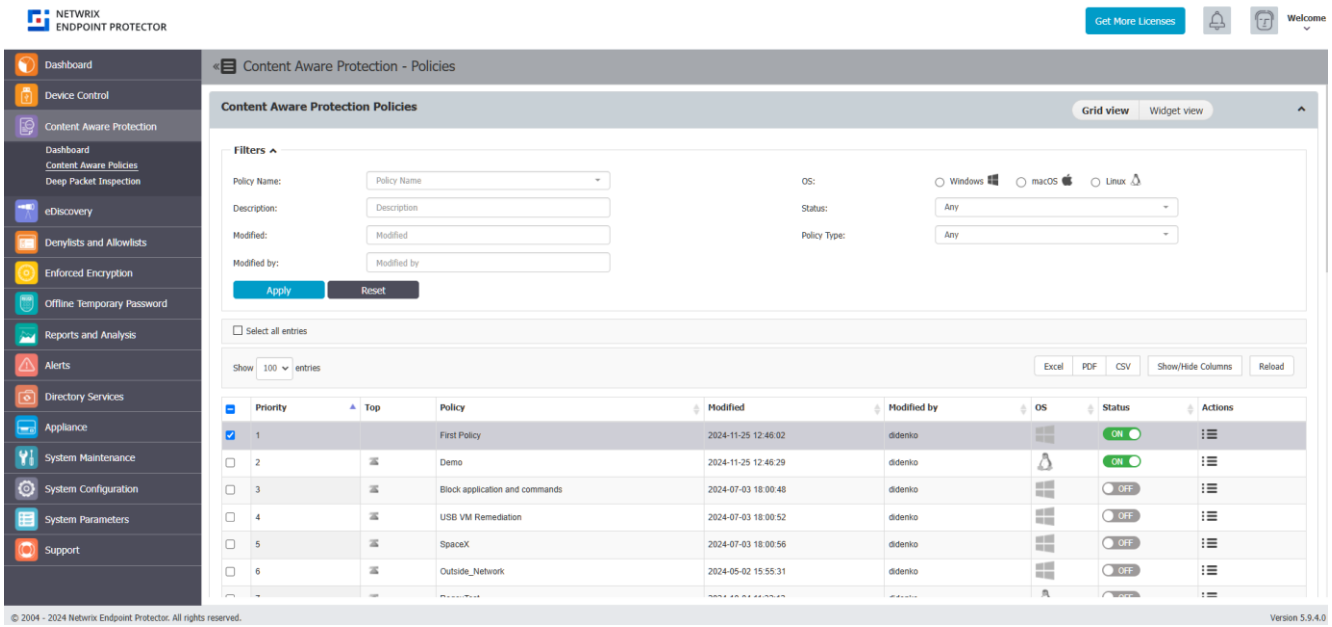


Рис 3.2. Список налаштованих політик CAP

Налаштування політики підтримує наступні дії реагування при виявлені спробі передачі конфіденційної інформації (див. рис. 3.3):

- Блокування та звіт – передача файлу буде повністю заблокована, у користувача з’явиться сповіщення, що він намагається передати конфіденційний файл та відповідний звіт про інцидент буде відправлено на сервер Endpoint Protector;

- Лише звіт – передача файлу не буде заблоковано, користувач також отримає сповіщення, що він намагається передати конфіденційний файл, звіт про подію буде відправлений на сервер;

- Лише блокування – передача файлу буде заблокована без відправлення звіту про подію на сервер;

- Блокування з можливістю виправдання – передача файлу буде заблокована, сповіщення про подію буде відправлено на сервер, проте у користувача буде можливість вказати причину в текстовому вигляді про причину відправлення конфіденційної інформації, після чого передача файлу може бути дозволена та файл буде передано.

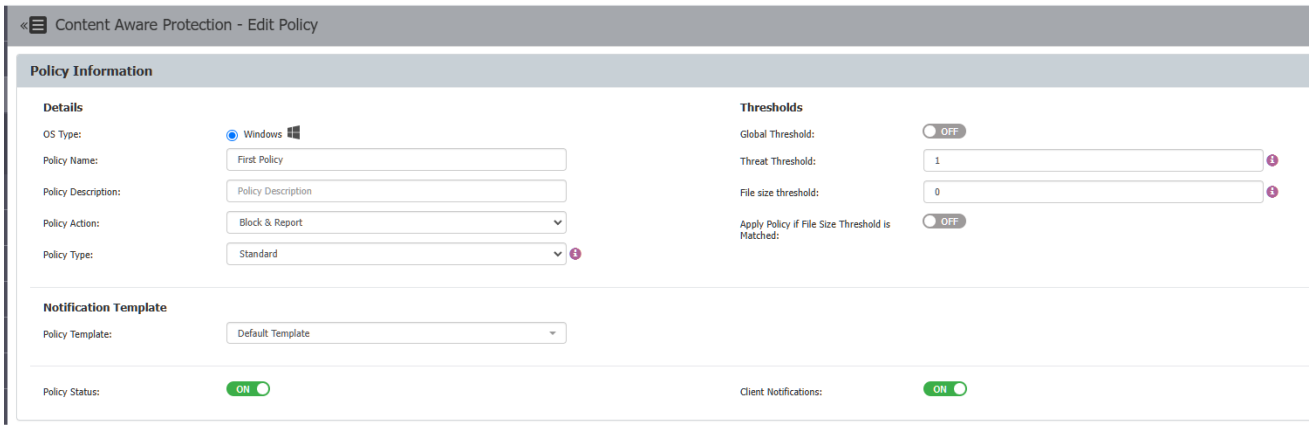


Рис 3.3. Налаштування дій при спрацюванні політики

Наступним кроком буде вибір точок виходу, які будуть моніторитись при передачі даних. Рішення підтримує багато вихідних точок, таких як: браузер, електронна пошта, обмін миттєвими повідомленнями, хмарні сервіси, ресурси обміну файлами та соціальні мережі. Додатково в цьому розділі налаштувань політики можна увімкнути моніторинг передачі файлів на портативні пристрої зберігання даних, контроль буферу обміну, передачу файлів на мережеві ресурси та відправлення файлів на друк до принтера (рисунок 3.4).

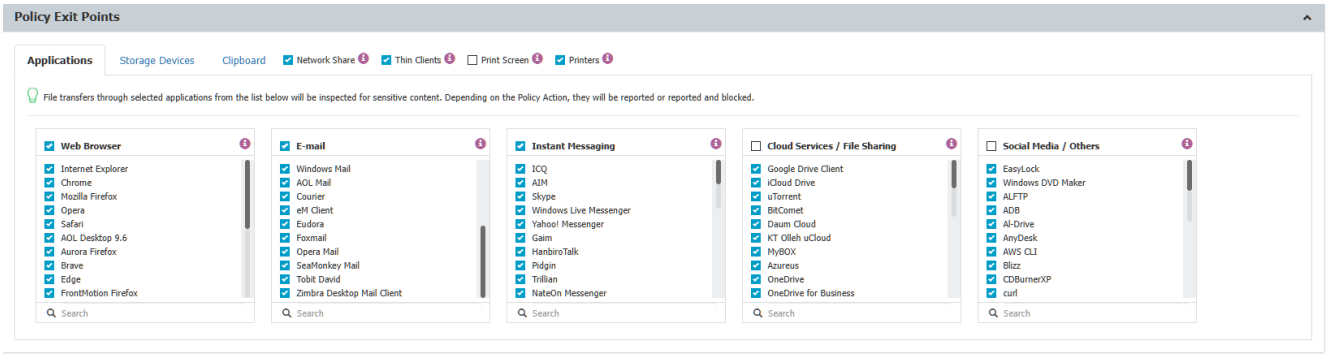


Рис 3.4. Налаштування контролю точок виходу

Далі необхідно вказати які саме файли потрібно відслідковувати. Це можна зробити різними способами (рисунок 3.5).

По типу файлів – в цьому розділі можна вибрати конкретні розширення файлів, які мають бути заблоковані. Це налаштування не переглядає вміст файлу та блокує лише по розширенню;

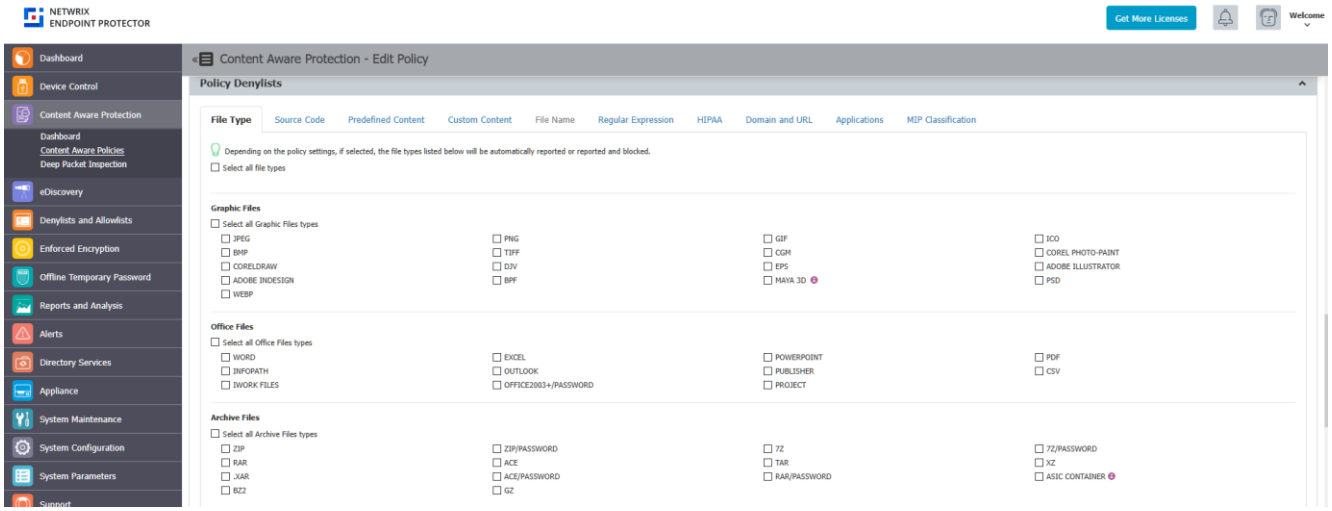


Рис 3.5. Налаштування блокування файлів за типом

Програмний код – Endpoint Protector завдяки алгоритмам автоматично визначить чи містить файл, що передається, заданий програмний код та заблокує передачу у разі виявлення (рис. 3.6).

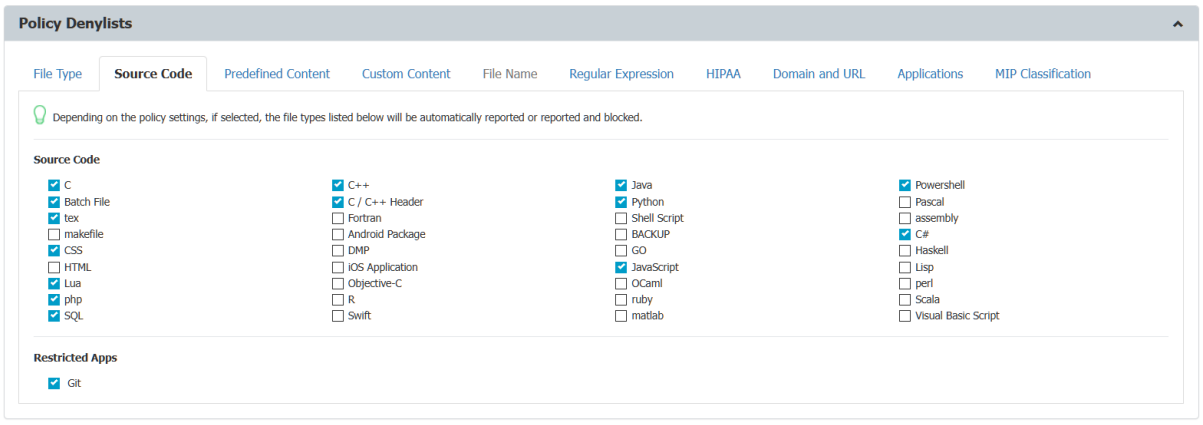


Рис 3.6. Налаштування блокування файлів за вмістом програмного коду

Попередньо визначений вміст – цей пункт налаштувань містить вбудовані алгоритми розпізнавання конфіденційної інформації у файлах. Сюди входить розпізнавання номерів кредитних карток, особиста інформація PII, номер IBAN, електронна пошта, адреси, номер телефону (рис. 3.7).

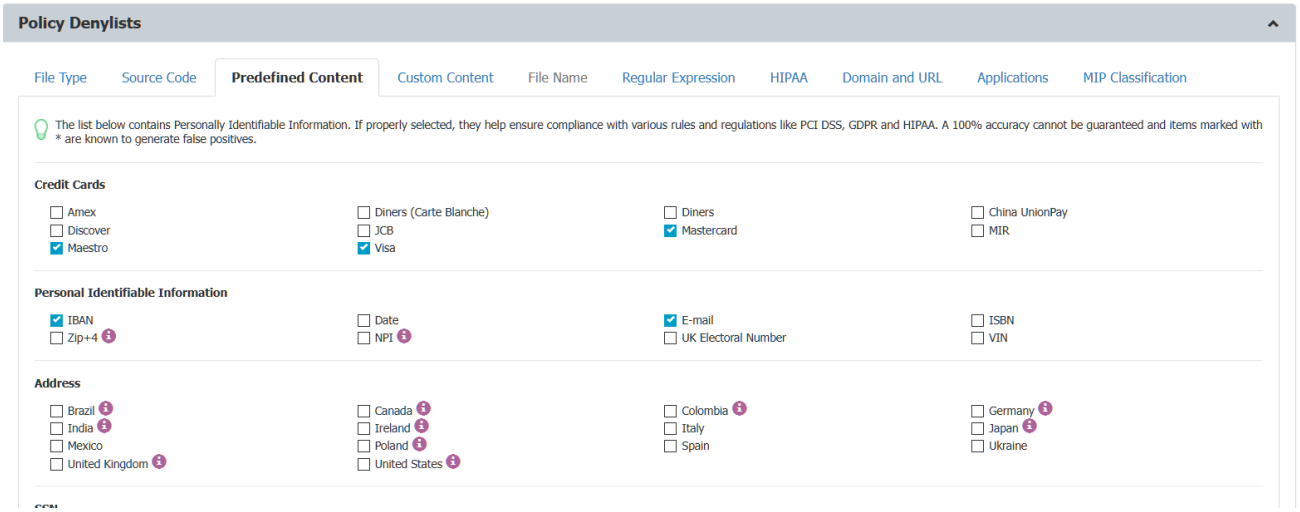


Рис 3.7. Налаштування блокування файлів за визначеним вмістом

Користувацький контент – в цьому пункті можна використати створені словники (рис. 3.8), вміст яких може вказувати на конфіденційний зміст файлів. Якщо в файлі буде знайдено хоча б одне слово із заданого словника – передача файлу буде заблокована.

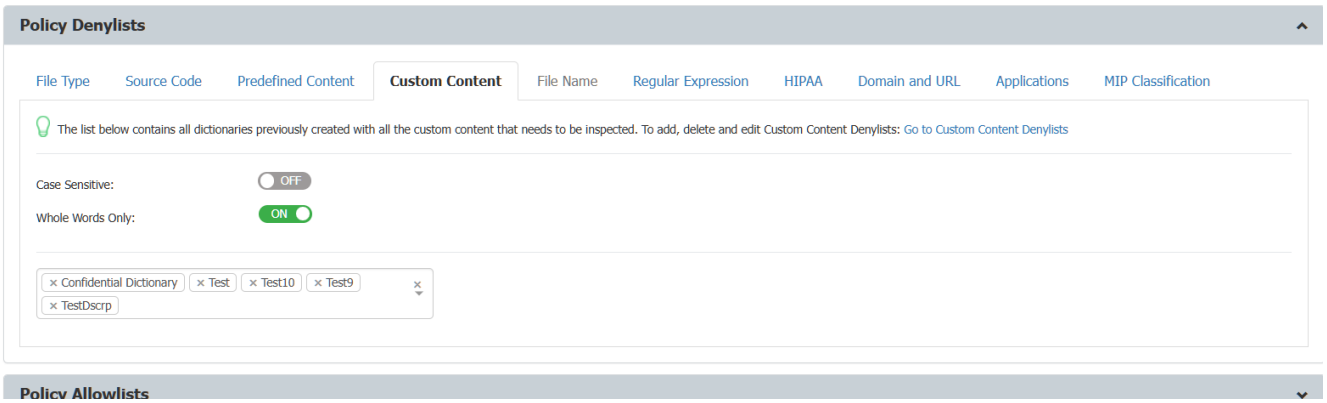


Рис 3.8. Налаштування блокування файлів за словниками

Розпізнавання за регулярними виразами Regex. В цьому пункті можна використати заздалегідь створений регулярний вираз Regex (рис. 3.9), що дозволяє більш гнучко налаштувати спрацювання політики безпеки.

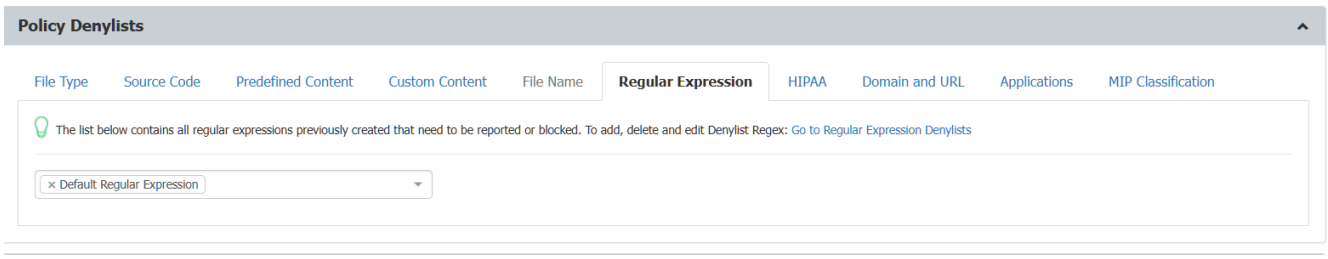


Рис 3.9. Налаштування блокування файлів за виразом Regex

Додатково рішення підтримує блокування заданих URL та контроль запуску додатків.

Після налаштування політики для розпізнавання конфіденційних файлів та точок виходу потрібно застосувати її на кінцеві точки (рис. 3.10).

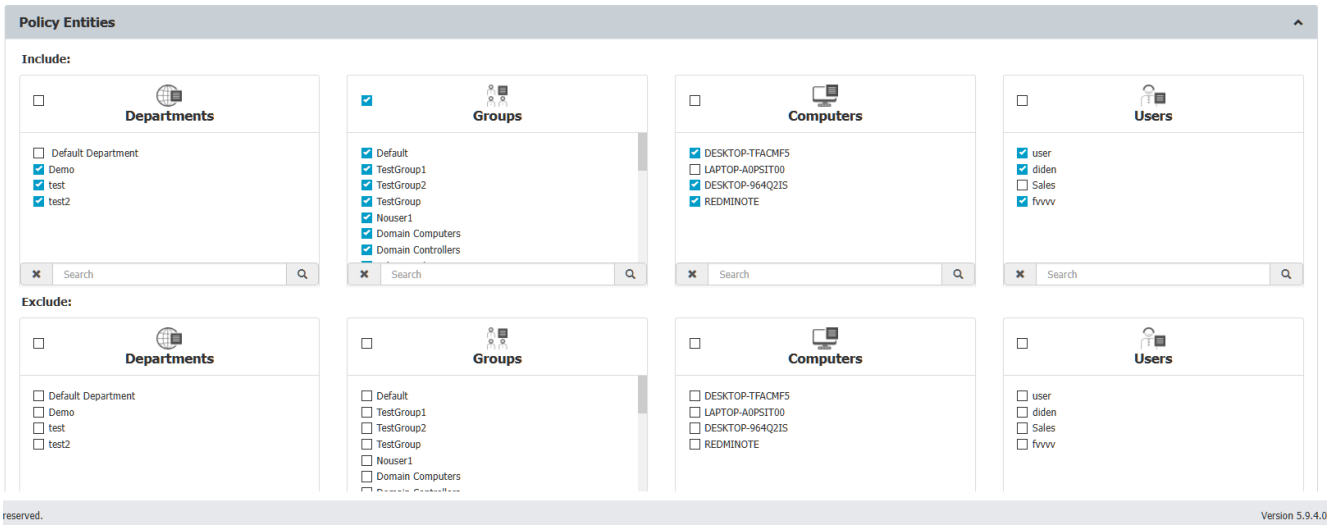


Рис 3.10. Застосування політики на вибраних кінцевих точках

Для того, щоб підключити кінцеву точку до сервера, на неї потрібно завантажити агент Endpoint Protector, вказавши IP та порт сервера при встановленні. Інтерфейс агенту має наступний вигляд (рисунок 3.11):

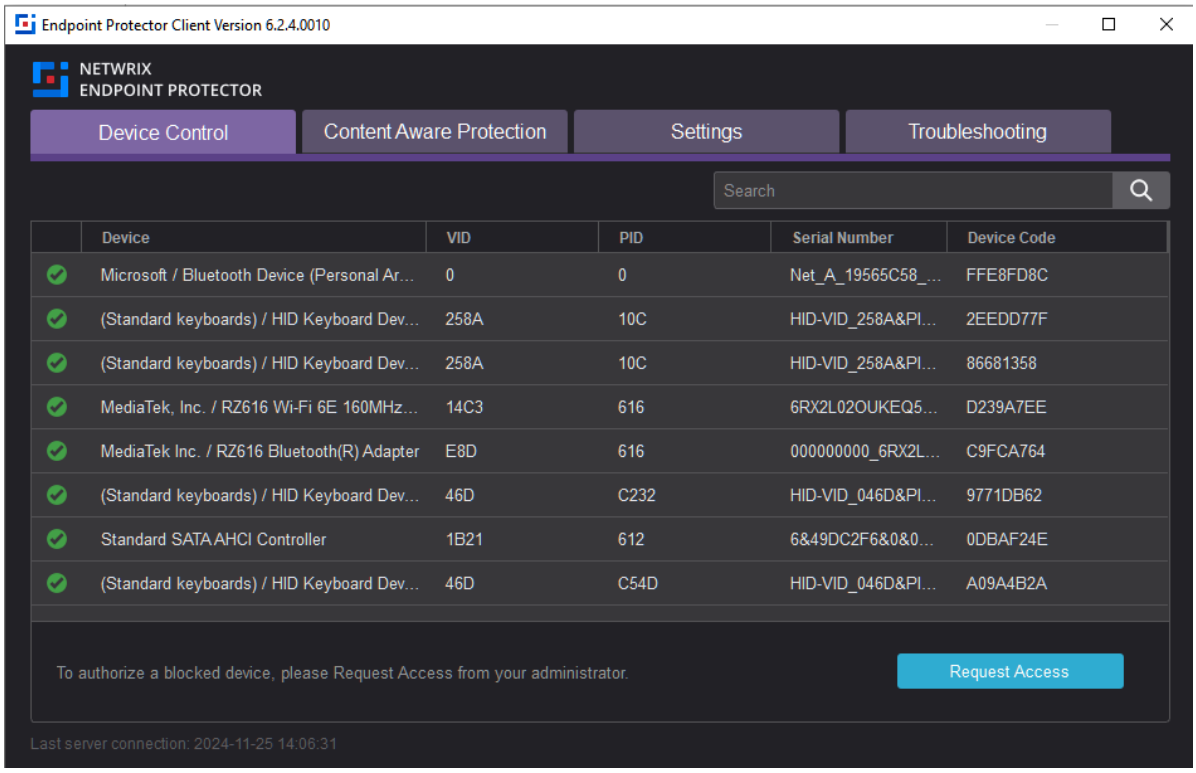


Рис 3.11. Інтерфейс агенту Endpoint Protector

Він перевіряє передачу файлів, слідкує за рухом файлів в системі та відправляє всі події та журнали на сервер для їх аналізу.

3.1.2. Перевірка працездатності налаштованої політики

Для того, щоб перевірити працездатність створеної політики буде використано зовнішній інтернет-ресурс для перевірки працездатності політик безпеки DLPTest.com (рис. 3.12).

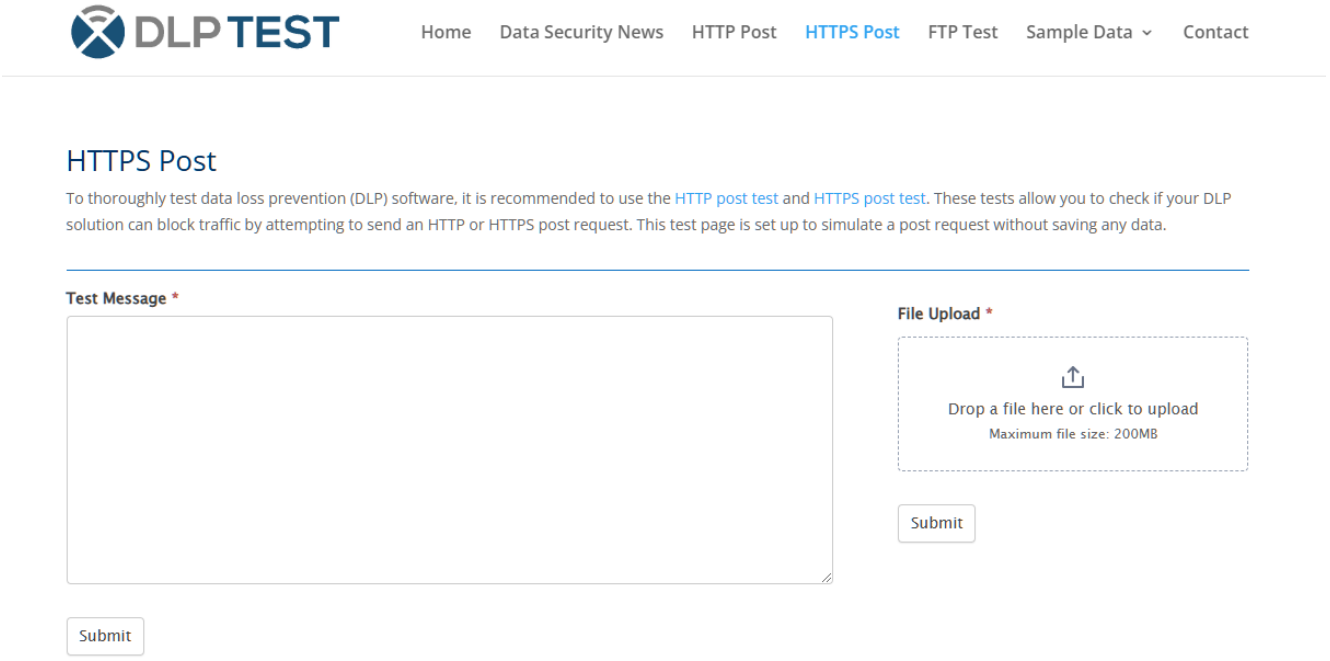


Рис 3.12. Зовнішній інтернет-ресурс DLPTest.com

Як приклад конфіденційного файлу буде використано тестовий Excel та Word файли, що містять номери карток користувачів (рис. 3.13).

A3 | Robert Aragon

	First and Last Name	SSN	Credit Card Number Visa MC AMEX
3	Robert Aragon	489-36-8350	4929-3813-3266-4295
4	Ashley Borden	514-14-8905	5370-4638-8881-3020
5	Thomas Conley	690-05-5315	4916-4811-5814-8111
6	Susan Davis	421-37-1396	4916-4034-9269-8783
7	Christopher Diaz	458-02-6124	5299-1561-5689-1938
8	Rick Edwards	612-20-6832	5293-8502-0071-3058
9	Victor Faulkner	300-62-3266	5548-0246-6336-5664
10	Lisa Garrison	660-03-8360	4539-5385-7425-5825
11	Marjorie Green	213-46-8915	4916-9766-5240-6147
12	Mark Hall	449-48-3135	4556-0072-1294-7415
13	James Heard	559-81-1301	4532-4220-6922-9909
14	Albert Iorio	322-84-2281	4916-6734-7572-5015
15	Charles Jackson	646-44-9061	5218-0144-2703-9266
16	Teresa Kaminski	465-73-5022	5399-0706-4128-0178
17	Tim Lowe	044-34-6954	5144-8691-2776-1108
18	Monte Mceachern	477-36-0282	5527-1247-5046-7780
19	Adriane Morrison	421-90-3440	4539-0031-3703-0728
20	Jerome Munsch	524-02-7657	5180-3807-3679-8221
21	Agnes Nelson	205-52-0027	5413-4428-0145-0036
22	Lynette Oyola	587-03-2682	4532-9929-3036-9308
23	Stacey Peacock	687-05-8365	5495-8602-4508-6804
24	Julie Renfro	751-01-2327	5325-3256-9519-6624
25	Danny Reyes	624-84-9181	4532-0065-1968-5602

Рис 3.13. Приклад тестового конфіденційного файлу

При спробі завантаження цього файлу на DLPTest, передачу буде заблоковано з відображенням повідомлення про блокування (рис. 3.14):

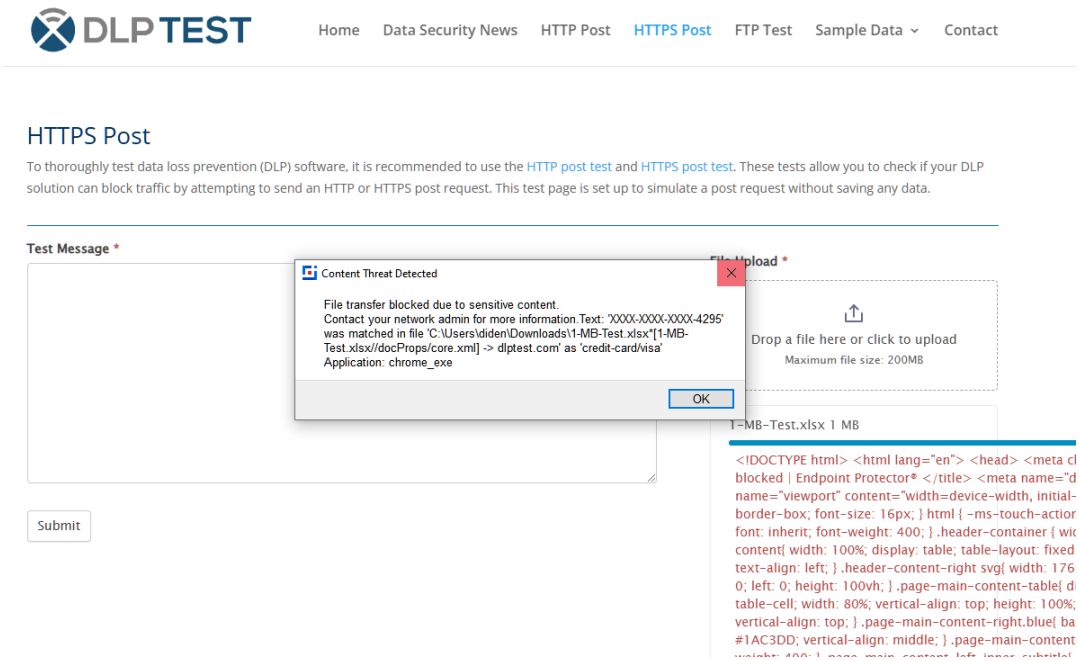


Рис 3.14. Приклад спрацювання політики на передачу файлу

З повідомлення можна зробити висновок, що номер кредитної картки було виявлено у файлі, який знаходиться за шляхом: C:\Users\diden\Download\1-MB-Test.xlsx, отже передачу файлу було заблоковано створеною політикою.

Також при спробі відправити конфіденційну інформацію у текстовому вигляді, а не файлом, відправку цього тексту також буде заблоковано:

1) Введення чутливої інформації для відправки текстом (рис. 3.15).

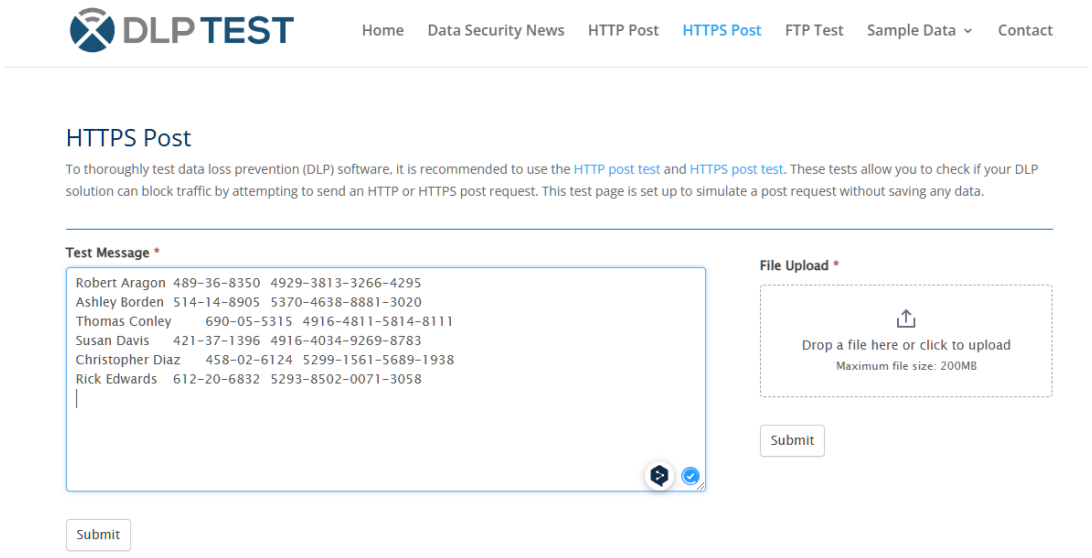


Рис 3.15. Перевірка блокування відправки конфіденційних даних текстом

2) Відповідна реакція Endpoint Protector після натискання кнопки «Відправити» (рис. 3.16):

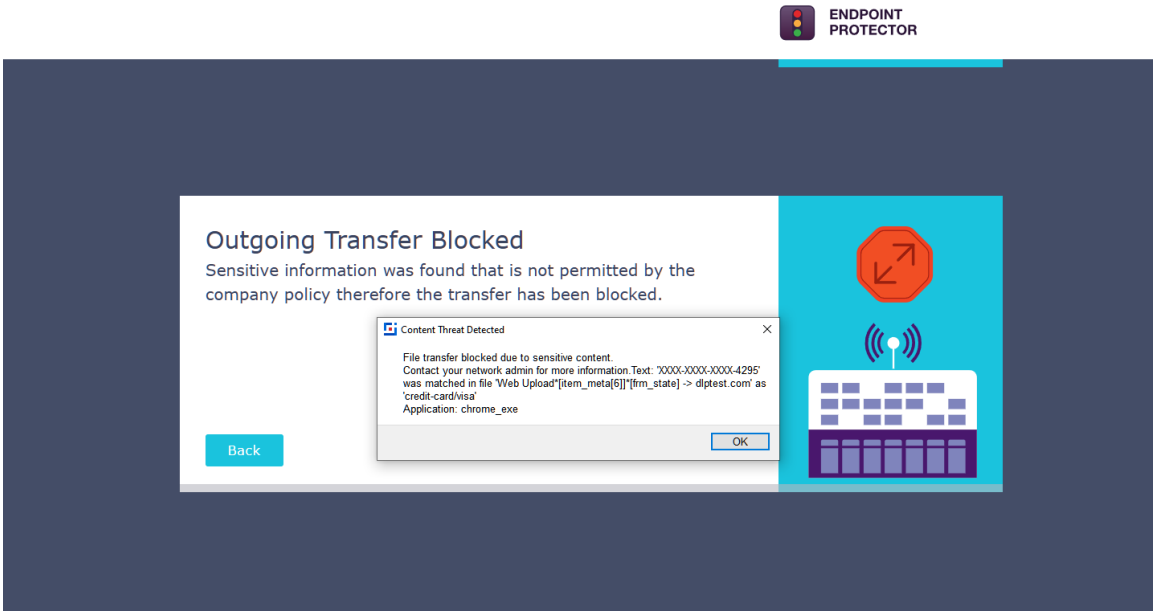


Рис 3.16. Блокування відправки конфіденційних даних текстом

Перейшовши до розділу Reports and Analysis, адміністратор консолі буде бачити звіт про всі події спрацювання політики Content Aware Protection. Тут вказано час інциденту, комп'ютер з якого передавались файли, ім'я користувача, що передавав файли, сам файл, його місце де він знаходиться та назва та пункт призначення передачі, в цьому випадку Chrome (рис. 3.17).

Також для проведення дослідження інциденту у адміністратора є можливість завантажити копію файлу, який намагались передати.

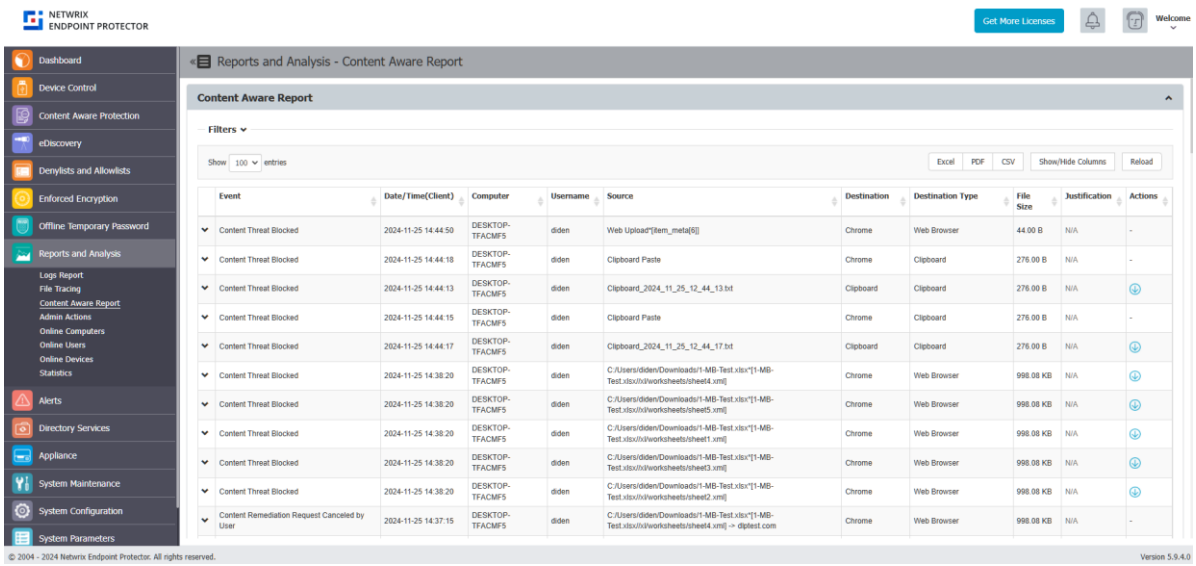


Рис 3.17. Інтерфейс звітування про інциденти витоку даних

3.1.3. Налаштування інтеграції з SIEM системою Wazuh

Для впровадження інтеграції на обох системах потрібно відкрити порт 515 по якому буде відправлятися системні журнали від Endpoint Protector до Wazuh (рисунок 3.18). Далі потрібно вказати адресу сервера Wazuh та вибрати які системні журнали передавати, наприклад підключення зовнішніх пристроїв та блокування передачі файлів.

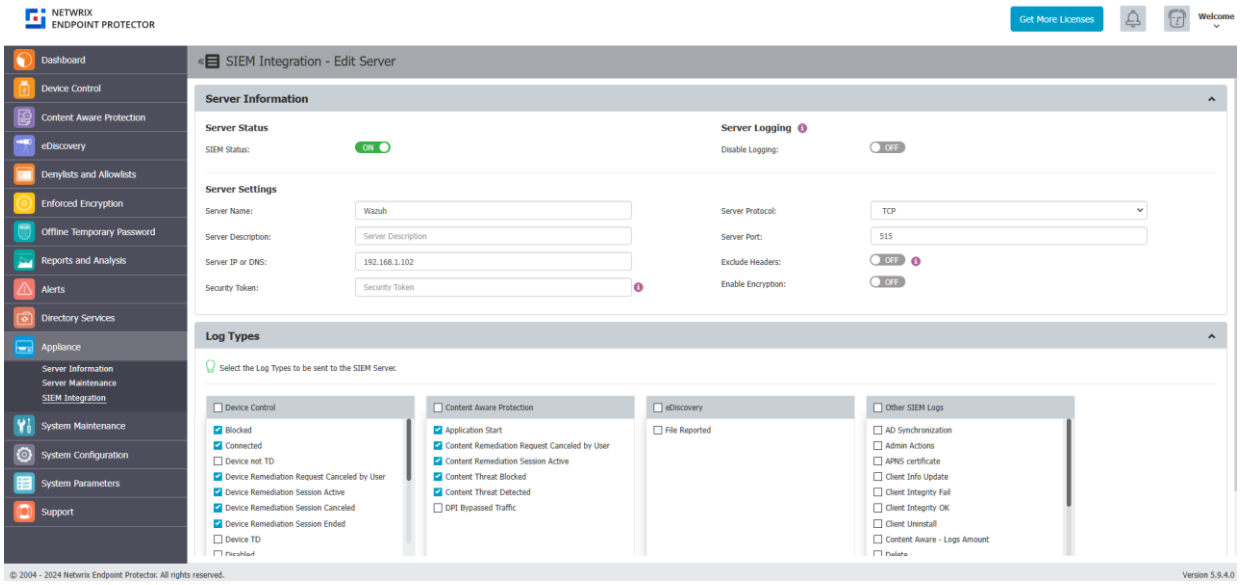


Рис 3.18 Налаштування інтеграції DLP з SIEM

Підключившись до сервера Wazuh по протоколу SSH та переглянувши файл в каталозі /var/ossec/logs/archives/archives.log, можна переконатись, що DLP відправляє системні журнали по порту 515 на сервер Wazuh, так як про це свідчать відповідні журнали на рисунку 3.19, отже інтеграція працює.

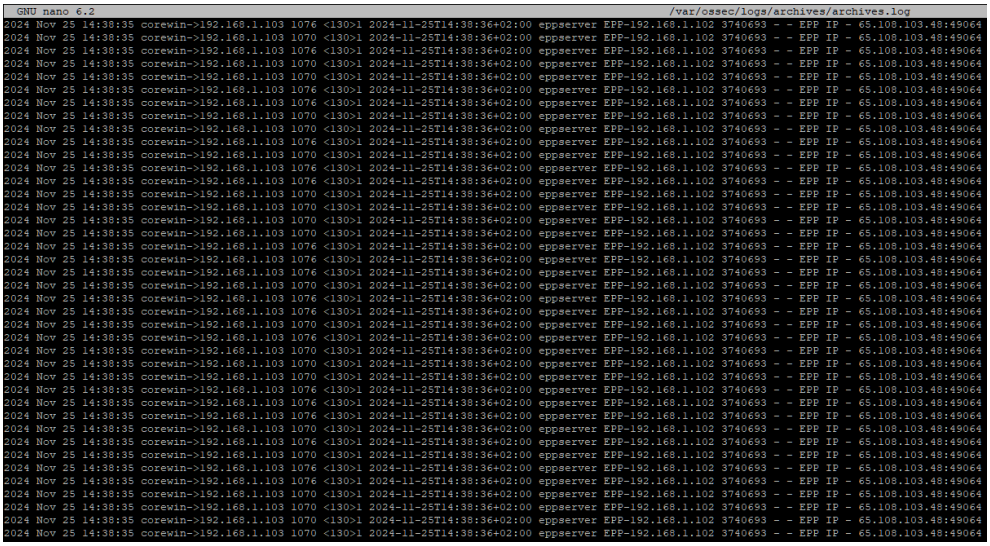


Рис 3.19. Перевірка отримання журналів від DLP по SSH

Якщо переглянути події з інтерфейсу сервера Wazuh події стосовно передачі конфіденційних файлів будуть виглядати наступним чином (рис. 3.20):

Рис 3.20. Приклад журналів DLP в інтерфейсі Wazuh

3.2 Налаштування SIEM системи Wazuh для обробки журналів DLP

Для того, щоб Wazuh зміг обробити журнали які надходять до сервера, потрібно розробити відповідний декодер та правила.

Один повний журнал події відправленої з DLP системи має такий вигляд: «2024-11-25T14:45:07+02:00 eppserver EPP-192.168.1.102 3743469 - - EPP IP - 65.108.103.48:49064 - Content Aware Protection - Content Threat Blocked: [Log ID] 4e0193d403d031c147f0c3c2a6d36a07 | [Client Computer] DESKTOP-TFACMF5 | [IP Address] 192.168.0.175 | [MAC Address] 04-7c-16-79-d1-ad | [Serial Number] To be filled by O.E.M. | [OS] Windows 10 Pro x64 22H2 (19045.5131) | [Client User] diden | [Content Policy] First Policy | [Content Policy Type] 1 | [Destination Type] Web Browser | [Destination] Chrome | [Destination Details] dlptest.com | [Email Sender] | [Email Subject] | [Device VID] 0 | [Device PID] 0 | [Device Serial] | [File Name] Web Upload*[item_meta[6]] | [File Hash] | [File Size] 44 | [Matched Item] XXXX-XXXX-XXXX-8783 | [Item Details] credit-card/visa | [Date/Time(Server)] 2024-11-25 14:45:07

| [Date/Time(Client)] 2024-11-25 14:44:50 | [Date/Time(Server UTC)] 2024-11-25T12:45:07Z | [Date/Time(Client UTC)] 2024-11-25T12:44:50»

Працювати з журналами такого вигляду дуже складно, тому потрібно розробити декодер, який буде структурувати корисну інформацію з журналів використовуючи мову XML та Regex (рисунок 3.21).

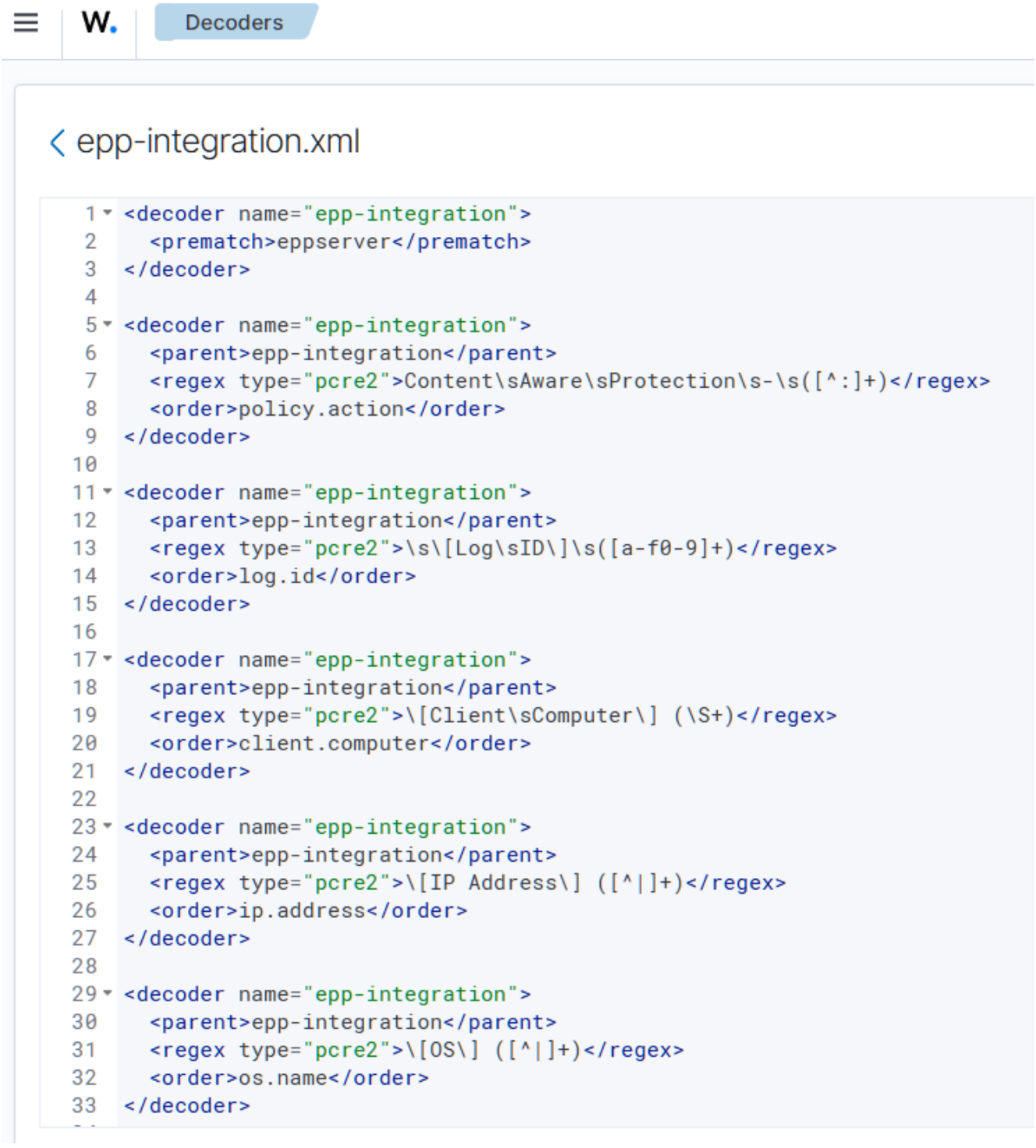


Рис 3.21. Розроблений декодер Wazuh

Перевірити роботу декодера можна в меню «Decoder test», результат перевірки зображено на рисунку 3.22:

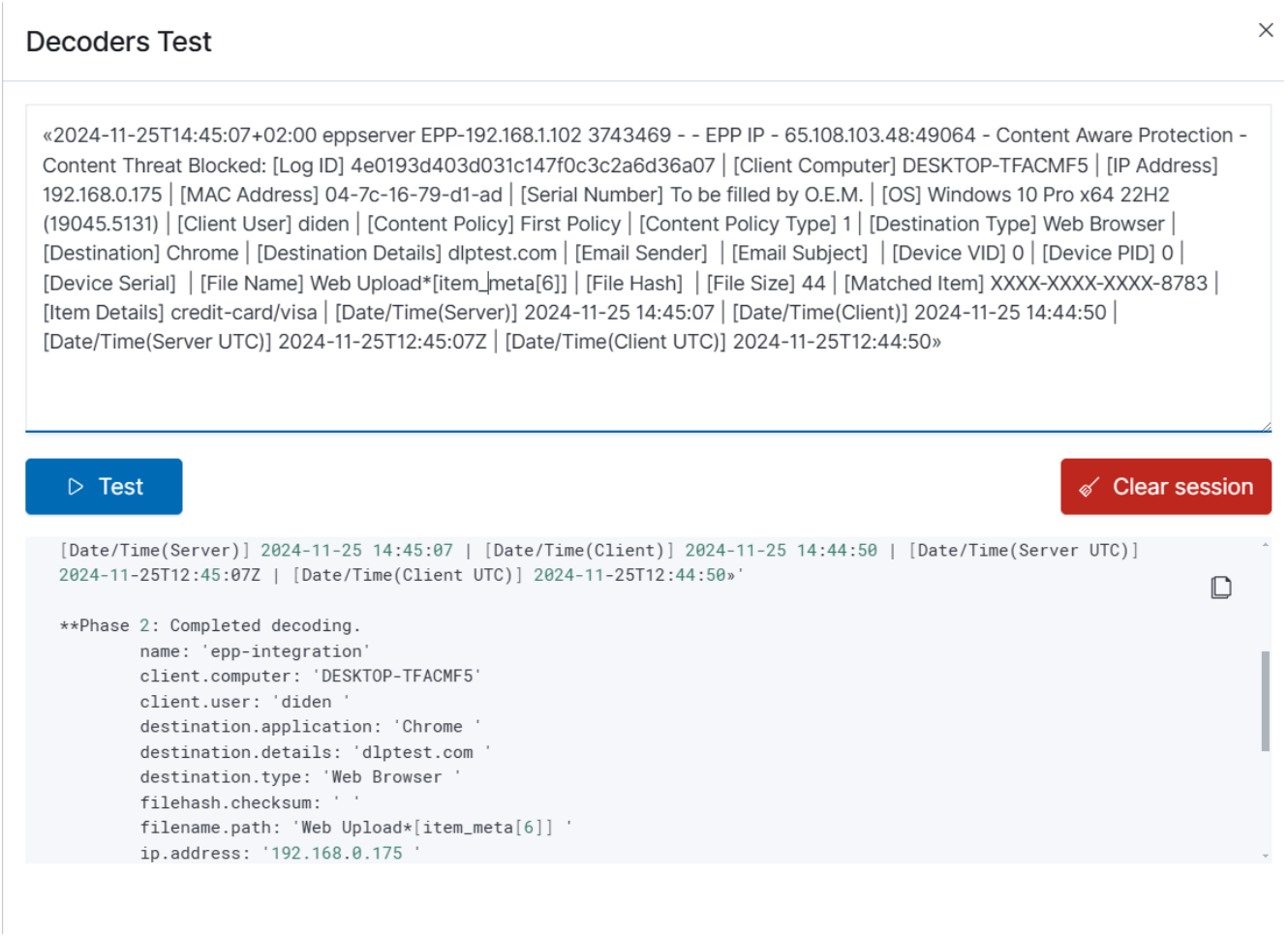


Рис 3.22. Перевірка створеного декодера

Отже, декодер успішно декодував журнал, виділивши з нього такі параметри як: назва ПК, ім'я користувача, призначення куди передавали файл (веб-ресурс dlptest.com), додаток куди передавали файл (Chrome), IP адреса кінцевої точки звідки була здійснена передача та операційна система, що на ній встановлена.

Після розробки та перевірки декодера потрібно розробити правила кореляції які будуть використовувати структуровану інформацію з журналу, яку надає декодер, щоб генерувати події кібербезпеки та присвоювати їм рівень серйозності відповідно до пріоритету. Створюємо правила кореляції використовуючи мову розмітки XML (рис. 3.23).

Rules

epp-rule.xml

```
<group name="syslog,">

<rule id="222000" level="1">
  <decoded_as>epp-integration</decoded_as>
  <description>File transfer was detected</description>
</rule>

<rule id="222001" level="7" frequency="20" timeframe="300">
  <if_matched_sid>222000</if_matched_sid>
  <field name="policy.action" type="pcre2">Content Threat Blocked</field>
  <description>File transfer was blocked due to confidential context</description>
</rule>

<rule id="222002" level="10" frequency="100" timeframe="300">
  <if_matched_sid>222001</if_matched_sid>
  <same_field>filehash.checksum</same_field>
  <field name="policy.action" type="pcre2">Content Threat Blocked</field>
  <description>File transfer was blocked due to confidential context</description>
</rule>

</group>
```

Рис 3.23. Розробка правила Wazuh

Дані правила спрацьовують коли декодер отримує з журналу інформацію про подію блокування файлу (Content Threat Blocked) та присвоює цій події 7-й рівень серйозності.

Приклад роботи інтеграції, декодера та правила можна побачити на рисунку 3.24:

22,334 hits

Nov 24, 2024 @ 17:24:52.789 - Nov 25, 2024 @ 17:24:52.789

Export Formated | 628 columns hidden | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Nov 25, 2024 @ 17:24:47.298	corewin	File transfer was blocked due to confidential context	7	222001
Nov 25, 2024 @ 17:24:47.292	corewin	File transfer was blocked due to confidential context	7	222001
Nov 25, 2024 @ 17:24:47.286	corewin	File transfer was blocked due to confidential context	7	222001
Nov 25, 2024 @ 17:24:47.281	corewin	File transfer was blocked due to confidential context	7	222001
Nov 25, 2024 @ 17:24:47.275	corewin	File transfer was blocked due to confidential context	7	222001
Nov 25, 2024 @ 17:24:47.269	corewin	File transfer was blocked due to confidential context	7	222001
Nov 25, 2024 @ 17:24:47.263	corewin	File transfer was blocked due to confidential context	7	222001

Рис 3.24. Перевірка працездатності правила

Створене правило має ідентифікатор 222001 та спрацьовує кожен раз, коли DLP система фіксує несанкціоновану передачу конфіденційної інформації за межі організації.

Додатково у фахівця з реагування на інциденти є можливість детально дослідити кожне спрацювання правила, відкривши меню з деталями інциденту (див. рис. 3.25):

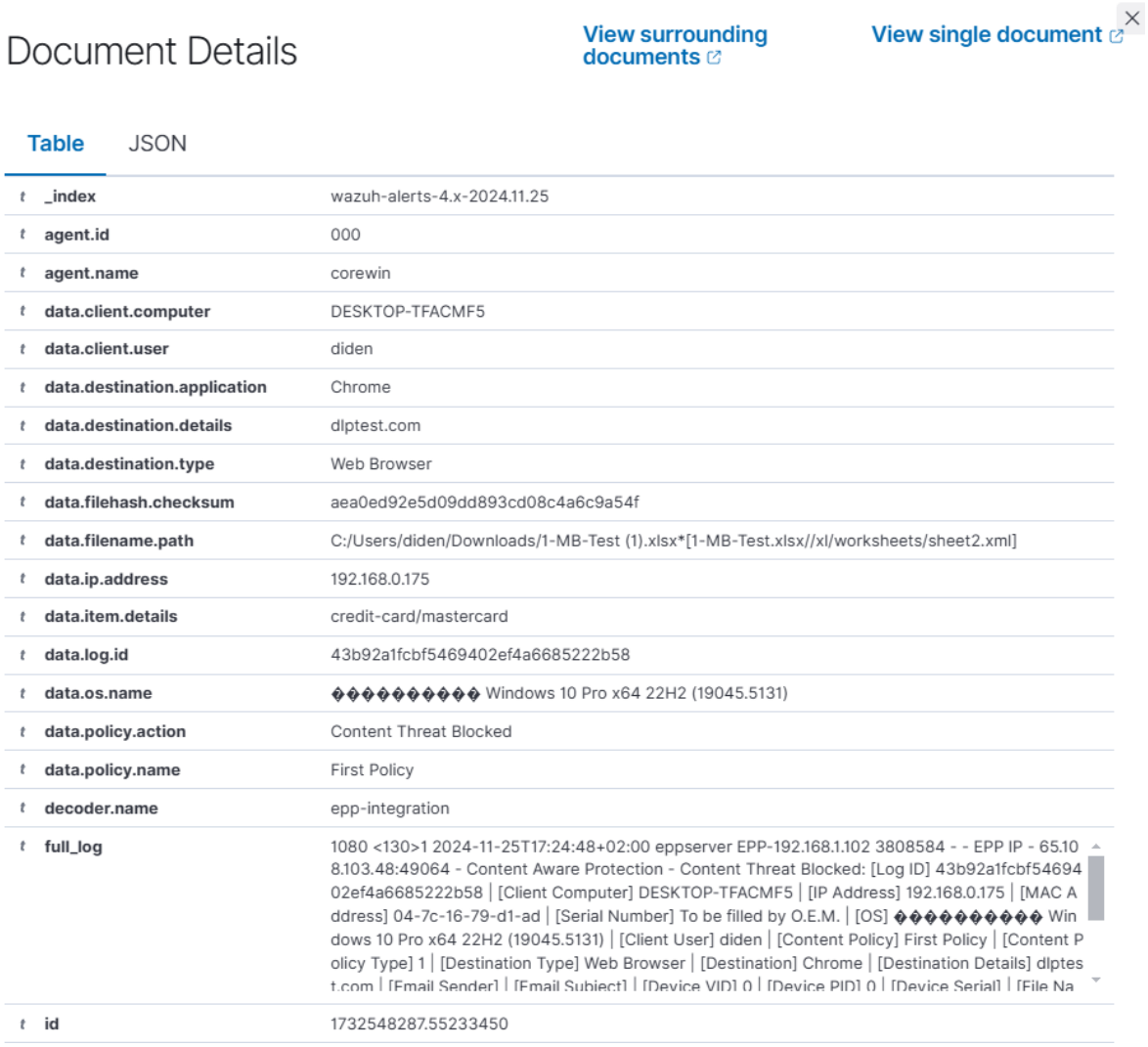


Рис 3.25. Деталі про подію передачі даних

3.3. Розробка методу автоматизованого реагування на інцидент безпеки використовуючи Wazuh XDR

3.3.1. Розробка скрипта та налаштування конфігурації модуля активного реагування

При реагуванні на інциденти команди безпеки часто можуть стикатися з такими проблемами як своєчасне реагування на події з високим ступенем критичності або забезпечувати якнайшвидше пом'якшення наслідків.

Рішення Wazuh має модуль активного реагування, який допомагає командам безпеки автоматизувати дії реагування на основі певних тригерів, що дозволяє їм більш ефективно керувати інцидентами безпеки. Автоматизація дій реагування гарантує, що високопріоритетні інциденти розглядаються та усуваються вчасно та якнайшвидше. Це особливо важливо в умовах, коли команди безпеки обмежені в ресурсах і повинні визначати пріоритети реагування.

Модуль активного реагування Wazuh виконує скрипти на контрольованих кінцевих точках, коли спрацьовує сповіщення за певним ідентифікатором правила.

Для виконання кваліфікаційної роботи був розроблений скрипт на мові програмування Python під назвою «localization», який використовує реєстр Windows для того, щоб вимкнути всі мережеві інтерфейси та підключені зовнішні носії USB на кінцевій точці для якнайшвидшої локалізації інциденту. Код написаного скрипта зображено на рисунку 3.26.

```python
#!/usr/bin/python3

import winreg
import os
import logging


logging.basicConfig(level=logging.INFO)
logger = logging.getLogger(__name__)


def disable_all_network_interfaces():
    interface_key = r"SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces"

    try:
        # Open the registry key for network interfaces
        with winreg.OpenKey(winreg.HKEY_LOCAL_MACHINE, interface_key, 0, winreg.KEY_READ) as key:
            # Enumerate all subkeys (network interfaces) under the Interfaces key
            subkey_index = 0
            while True:
                try:
                    subkey_name = winreg.EnumKey(key, subkey_index)
                    subkey_path = f"{interface_key}\\{subkey_name}"

                    # Open each interface key and set the "EnableDHCP" value to 0 to disable it
                    with winreg.OpenKey(winreg.HKEY_LOCAL_MACHINE, subkey_path, 0, winreg.KEY_SET_VALUE)
                        winreg.SetValueEx(subkey, "EnableDHCP", 0, winreg.REG_DWORD, 0)

                    print(f"Disabled network interface: {subkey_path}")
                    subkey_index += 1
                except OSError:
                    # No more subkeys to enumerate
                    break

        print("All network interfaces disabled successfully.")
    except Exception as e:
        print(f"Error disabling network interfaces: {str(e)}")


def disable_usbstor_driver():
    key_path = r"SYSTEM\CurrentControlSet\Services\USBSTOR"
    try:
        with winreg.OpenKey(winreg.HKEY_LOCAL_MACHINE, key_path, 0, winreg.KEY_SET_VALUE) as key:
            winreg.SetValueEx(key, "Start", 0, winreg.REG_DWORD, 4)
            logger.info("USB storage devices disabled.")
    except FileNotFoundError:
        logger.error("Registry key not found.")
    except PermissionError:
        logger.error("Permission error. Make sure you have the necessary permissions.")
    except Exception as e:
        logger.error(f"Error disabling USBSTOR driver: {e}")
```

Рис 3.26. Розробка скрипта автоматичного реагування

Щоб модуль активного реагування почав працювати необхідно створити певну конфігурацію на сервері Wazuh (рис. 3.27):

Рис 3.27. Створення конфігурації для запуску скрипта

Створена конфігурація буде запускати скрипт на кінцевій точці з ID 006, якщо спрацює правило з ID 222001, яке вказує, що відбувається витік конфіденційної інформації.

Після цього потрібно завантажити скрипт в папку C:\Program Files (x86)\ossec-agent\active-response\bin на кінцевій точці (рис. 3.28).

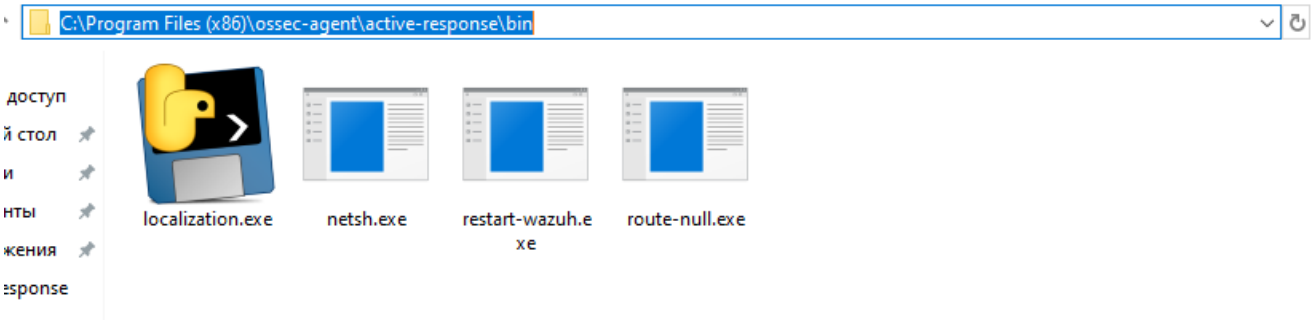


Рис 3.28. Завантаження скрипта на кінцеву точку

Тепер проведемо перевірку створеної конфігурації на працездатність. Для цього я спробую передати файл з конфіденційною інформацією, щоб створити події правила 222001.

Ось початковий стан кінцевої точки (рис. 3.29), з'єднання з інтернетом працює, команди ping проходять на DNS Google.com – 8.8.8.8 також до системи підключений зовнішній USB носій (рис. 3.29):

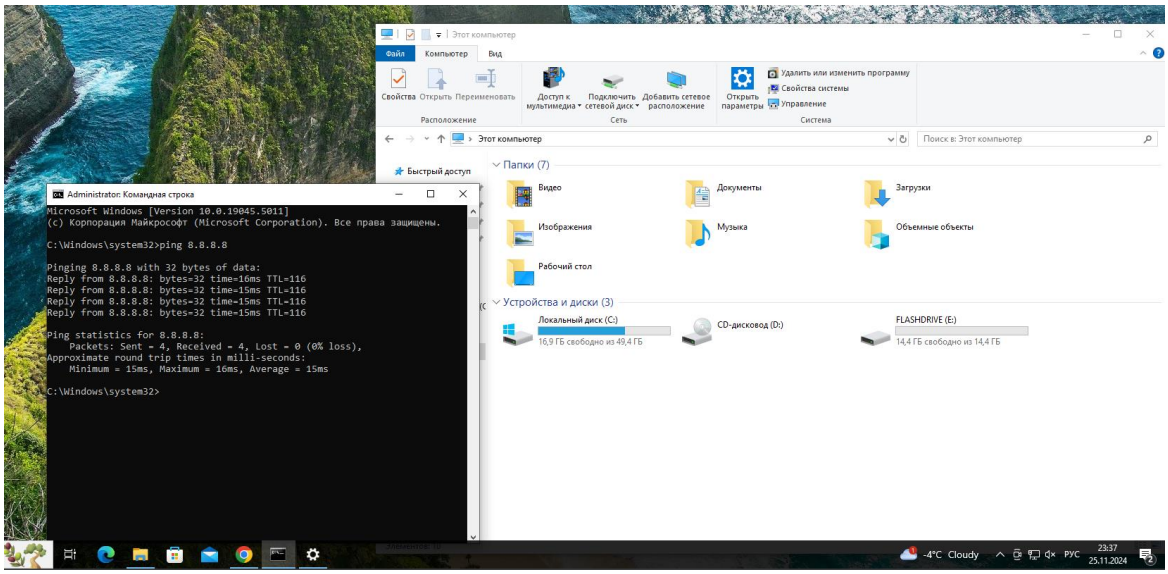


Рис 3.29. Працездатність тестової системи у звичайному стані

При спробі завантажити конфіденційний файл на зовнішній ресурс DLPTest.com – файл було заблоковано політикою DLP, після чого журнали цієї події відправляються до SIEM системи Wazuh де відбувається їх декодування, та генерується спрацювання створеного раніше правила під номером 222001, яке сповіщає про те, що відбувається несанкціонована передача чутливих даних (рис 3.30 та рис. 3.31).

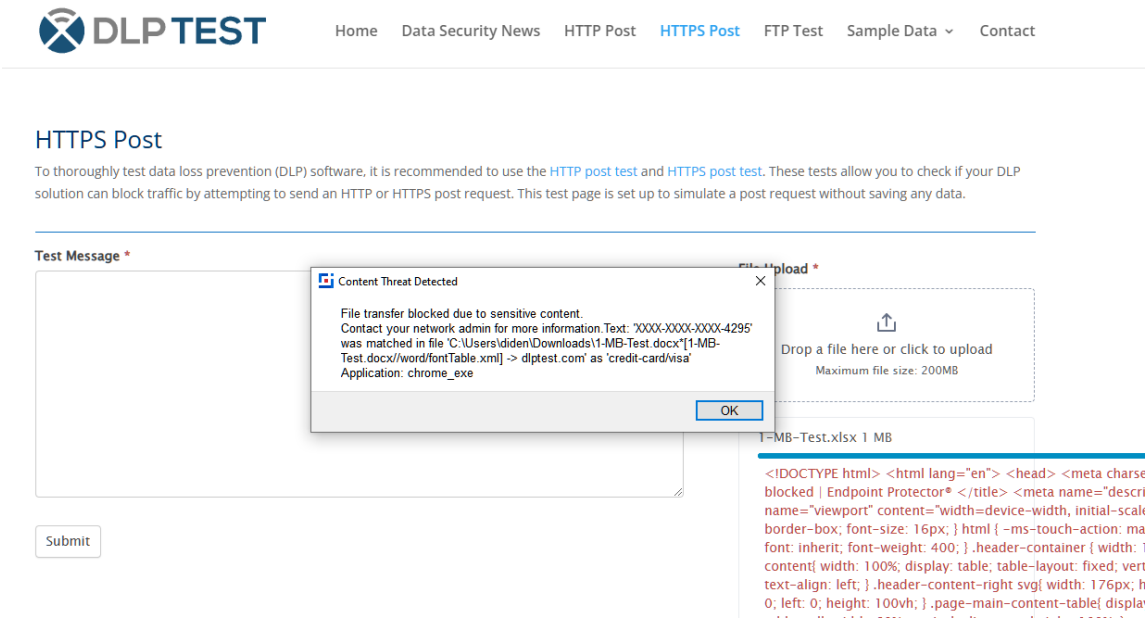
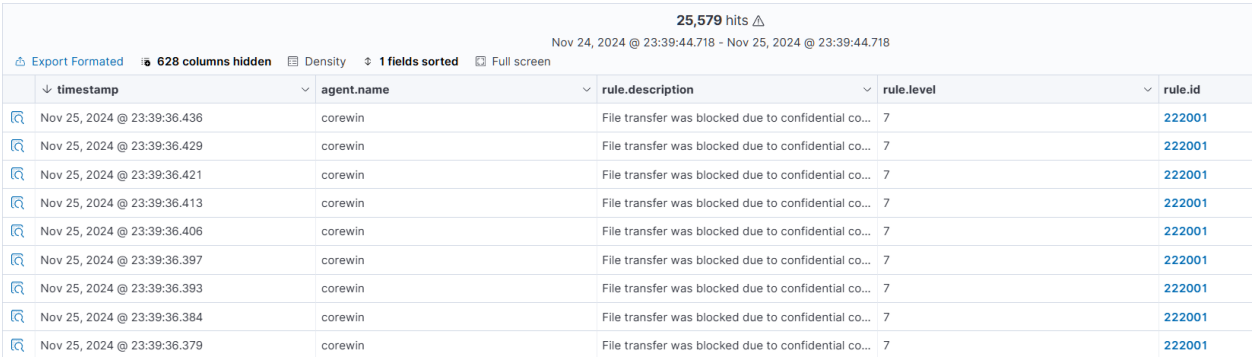


Рис 3.30. Генерація тестового інциденту витоку даних



25,579 hits

Nov 24, 2024 @ 23:39:44.718 - Nov 25, 2024 @ 23:39:44.718

Export Formated | 628 columns hidden | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Nov 25, 2024 @ 23:39:36.436	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.429	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.421	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.413	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.406	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.397	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.393	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.384	corewin	File transfer was blocked due to confidential co...	7	222001
Nov 25, 2024 @ 23:39:36.379	corewin	File transfer was blocked due to confidential co...	7	222001

Рис 3.31. Спрацювання правила SIEM на витік даних

Спрацювання правила 222001 запускає модуль активного реагування, який в свою чергу одразу запускає скрипт для негайної локалізації інциденту на кінцевій точці, відбувається відключення усіх зовнішніх накопичувачів USB та відключаються всі мережеві інтерфейси через реєстр Windows (див. рис. 3.32 та рис. 3.33).

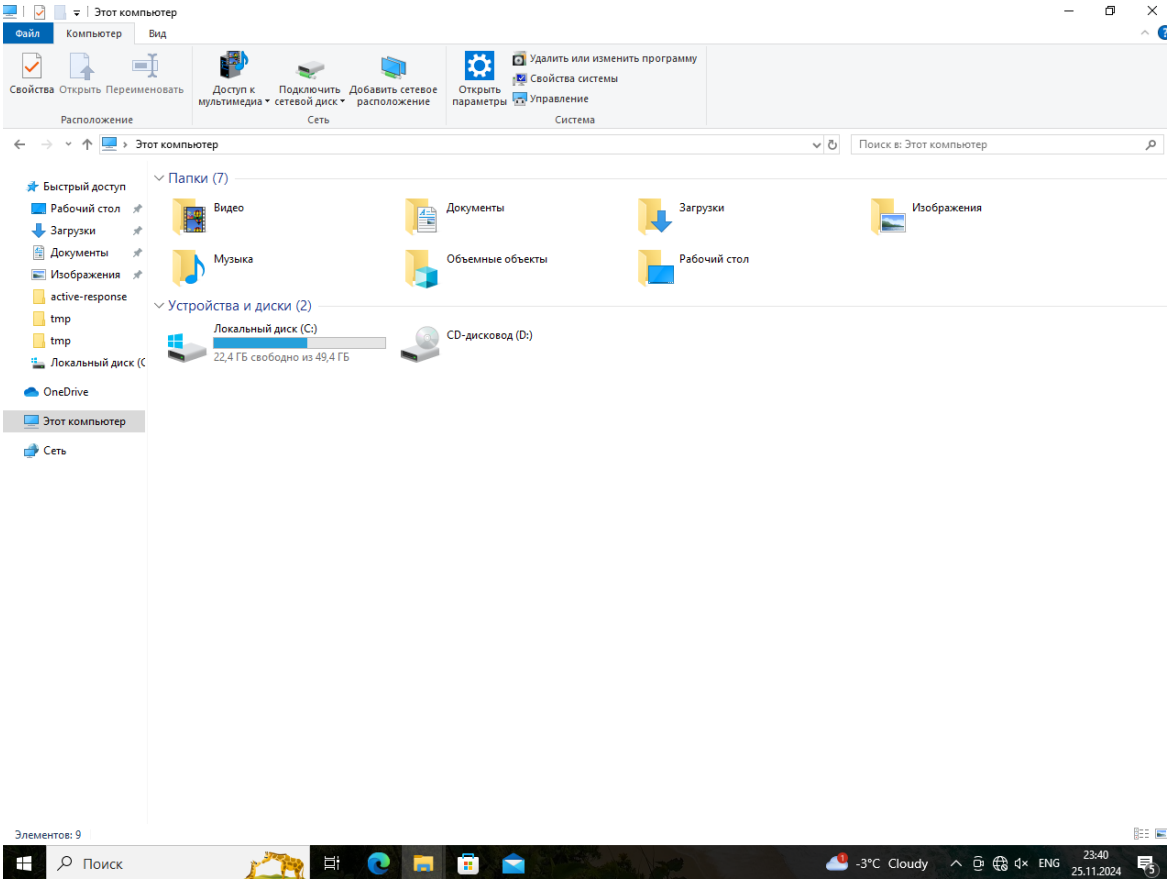


Рис 3.32. Приклад відключення зовнішнього USB носія

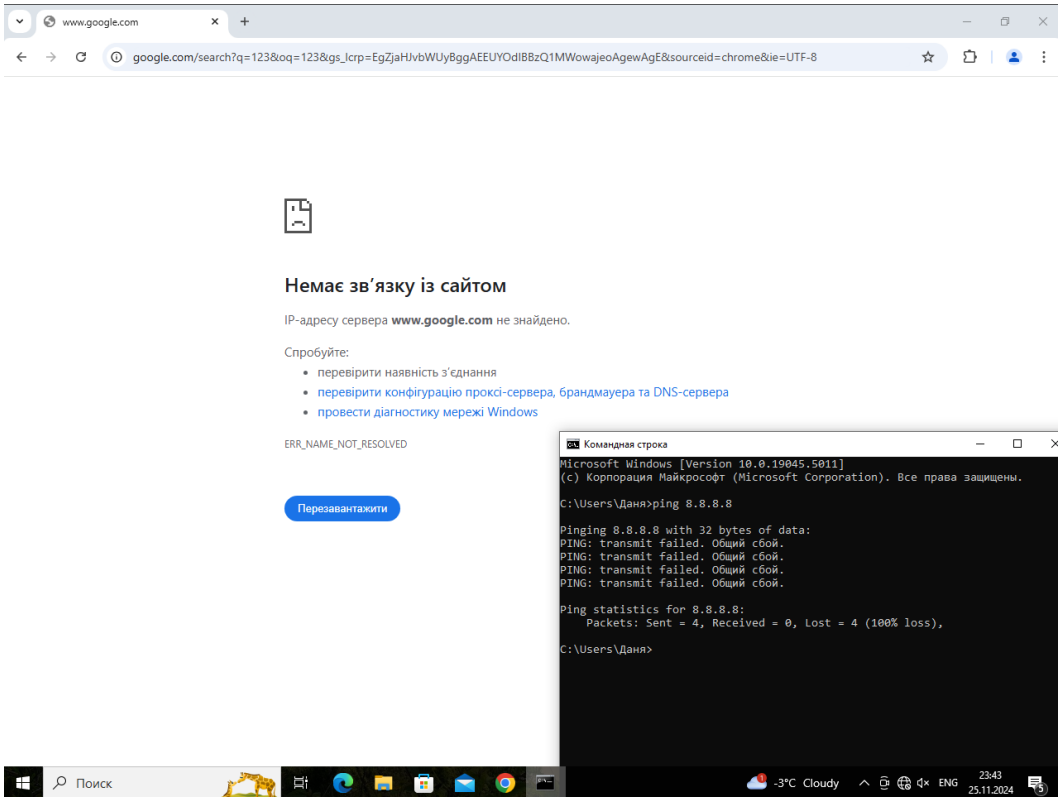


Рис 3.33. Розірвання інтернет з'єднання

Зі скріншотів нижче можна побачити, що підключений USB пристрій зник (був відключений), а інтернет з'єднання було розірвано, команда ping більше не проходить на адресу 8.8.8.8, отже інцидент було автоматично успішно локалізовано, відключивши скомпрометовану кінцеву точку від мережі. Даний метод реагування на інцидент спрацював менш ніж за хвилину від початку витоку даних, що значно перевищує швидкість ручного реагування.

3.3.2. Порівняння створеного методу реагування на основі Wazuh з іншими SIEM рішеннями

Створений метод реагування на інциденти кібербезпеки на основі Wazuh пропонує економічно ефективне та адаптивне рішення для організацій, що прагнуть автоматизувати процеси локалізації кіберінцидентів.

Цей підрозділ зосереджено на порівнянні розробленого підходу з іншими провідними SIEM-рішеннями. Оцінка базується на ключових параметрах, включаючи швидкість реагування, гнучкість налаштувань та вимоги до ресурсів (див. таб. 3.1).

Таблиця 3.1.

Порівняння розробленого методу автоматичного реагування з функціоналом рішень аналогів

	Оцінка				
Критерій	**Розроблений метод (Wazuh)**	**Splunk**	**QRadar**	**Arcsight**	**LogRhythm**
Швидкість реагування	Висока	Висока	Висока	Висока	Висока
Гнучкість налаштування	Висока	Середня	Висока	Середня	Висока
Підтримка кастомізації	Висока	Висока	Висока	Середня	Висока
Простота налаштування	Висока	Середня	Низька	Низька	Середня
Вимоги до ресурсів	Середня	Висока	Висока	Висока	Висока
Вартість	Низька (OpenSource)	Висока	Висока	Висока	Висока

Отже, розроблений метод автоматизованого реагування на інцидент витоку конфіденційної інформації має такі переваги серед інших схожих рішень:

1) Поєднує в собі використання двох інтегрованих рішень безпеки для зменшення вірогідності хибнопозитивних спрацювань, що збільшує точність. Використання DLP Endpoint Protector забезпечує гнучке налаштування політик безпеки, щодо витоку конфіденційної інформації, в той час як Wazuh забезпечує швидку обробку та реагування на відповідні події безпеки.

2) Легко кастомізується відповідно до потреб організації, що робить його використання зручним для впровадження в будь-яку політику безпеки;

3) Метод є економічним порівняно з іншими SIEM, так як Wazuh є OpenSource рішенням.

ВИСНОВОК

У ході виконання кваліфікаційної роботи було досягнуто основної мети дослідження – розроблено технологію реагування на інциденти кібербезпеки на основі інтеграції систем DLP Endpoint Protector і SIEM Wazuh. Дослідження продемонструвало актуальність даного підходу для вирішення завдань моніторингу, виявлення та автоматизації реагування на загрози в організаціях.

Робота підтвердила ефективність поєднання DLP і SIEM систем для забезпечення комплексного захисту інформаційних активів. Зокрема, інтеграція дозволила не лише підвищити точність виявлення інцидентів, але й скоротити час на їх локалізацію та мінімізувати потенційні ризики витоку даних. Впровадження розробленого скрипта, який автоматично відключає інтернет-з’єднання та блокує зовнішні USB носії, продемонструвало високу швидкість реагування та адаптивність до конкретних умов організації. Практична реалізація розробленого методу довела, що запропонований метод реагування є ефективним для організацій із обмеженими ресурсами, оскільки він базується на ПЗ з відкритим кодом. Успішне поєднання створених правил SIEM Wazuh із політиками блокування передачі даних DLP Endpoint Protector забезпечило виявлення та автоматичне блокування спроб передачі конфіденційних даних, що відповідає сучасним вимогам до забезпечення кібербезпеки. Запропонована технологія може бути впроваджена у середніх і малих організаціях, де важливі економічність та адаптивність рішень. Використання даного методу може бути розширене шляхом розробки додаткових скриптів під конкретні потреби.

Результати роботи мають практичну цінність і можуть бути використані для посилення безпеки в інформаційних системах, забезпечення відповідності нормативним вимогам.

ПЕРЕЛІК ПОСИЛАНЬ

1. IBM Cost of a Data Breach Report 2024. URL: https://www.ibm.com/reports/data-breach(дата звернення: 26.11.2024).

2. NIST. Computer Security Incident Handling Guide. Special Publication 800-61 Revision 2. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (дата звернення: 26.11.2024).

3. Endpoint Protector by CoSoSys Ranked #1 for DLP Configuration. URL: https://www.endpointprotector.com/blog/endpoint-protector-by-cososys-ranked-1-for-dlp-configuration/ (дата звернення: 26.11.2024).

4. Wazuh. SIEM Platform Overview. URL: https://wazuh.com/platform/siem/#:~:text=The%20Wazuh%20Security%20Information%20and,for%20threat%20detection%20and%20compliance (дата звернення: 26.11.2024).

5. Kent K., Chevalier S., Grance T., & Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. URL: https://csrc.nist.gov/publications/detail/sp/800-86/final (дата звернення: 26.11.2024).

6. Gartner. Market Guide for Data Loss Prevention. URL: https://www.gartner.com/en/documents/3997246 (дата звернення: 26.11.2024).

7. Bejtlich R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. Cambridge, 2013.

8. MITRE ATT&CK Framework. URL: https://attack.mitre.org/ (дата звернення: 26.11.2024).

9. Microsoft Security Documentation. Incident Response Playbook for Cloud and Hybrid Environments. URL: https://learn.microsoft.com/en-us/security/compass/incident-response-playbook (дата звернення: 26.11.2024).

10. Гнатюк С. М. Кібербезпека: Основи забезпечення інформаційної безпеки. Київ: Національний авіаційний університет, 2020.

11. Корченко О.Г., Дворжанський О.В. Системи інформаційної безпеки: концепції, технології, моделі. Харків: Видавництво ХНУРЕ, 2019.

12. Діденко Д.Ю. Актуальність використання DLP систем для запобігання та виявлення несанкціонованого витоку даних. *Актуальні проблеми кібербезпеки* : тези доп. всеукр. наук.-практ. конф. (м. Київ, 25 жовт. 2024 р.). Київ: ДУІКТ, 2024. – С. 55-57.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)