Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

Пояснювальна записка

до випускної кваліфікаційної роботи магістра

на тему: «Проєкт інформаційної системи управління інцидентами кібербезпеки на базі відкритого рішення Wazuh»

Виконала студентка 2-го курсу, групи КБм-21-1
спеціальності 125 «Кібербезпека»
Колощук М.С.

Керівник _____ Професор кафедри КІ та КБ, д.т.н., доцент Воротніков В.В.

Рецензент _____ Завідувач кафедри КІ та КБ, д.т.н., доцент Єфіменко А.А.

Житомир – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної
інженерії
та кібербезпеки
Єфіменко А. А.
«_25_» жовтня 2022 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу

Студентки _Колощук Марії Сергіївни_____

Тема роботи: _«Проєкт інформаційної системи управління інцидентами кібербезпеки на базі відкритого рішення Wazuh»_____

_____

Затверджена Наказом університету від «_25_» жовтня 2022 р. № _501С_
Термін здачі студентом закінченої роботи _19 грудня 2022 р._
Вихідні дані роботи (зазначається предмет і об'єкт дослідження) _____

_____

_____

_____

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	2.09.22	2.09.21
2	Покотило О.А.	6.10.22	6.10.22
3	Покотило О.А.	4.11.22	4.11.22

Керівник _____
(підпис)

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі. Пошук, огляд та аналіз аналогічних розробок. Формулювання технічного завдання. Опрацювання літературних джерел.	2 листопада 2022 – 5 листопада 2022	Виконано
2	Проєктування структури системи	6 листопада 2022 – 12 листопада 2022	Виконано
3	Налаштування мережі та системи захисту	13 листопада 2022 – 26 листопада 2022	Виконано
4	Тестування системи захисту	27 листопада 2022 – 4 грудня 2022	Виконано
5	Захист	29 грудня 2022	Виконано

Студент _____ **Колощук М.С.**

(підпис)

Керівник _____ **Воротніков В.В.**

(підпис)

РЕФЕРАТ

Випускна кваліфікаційна робота магістра складається з проекту захищеної мережі кол-центру та пояснювальної записки. Пояснювальна записка до випускної роботи містить 59 сторінок, 26 ілюстрацій та 8 таблиць.

Метою роботи є підвищення безпеки внутрішньої мережі безпеки шляхом створення інтерфейсу користувача за допомогою векторного механізму на основі додатку Wazuh.

В роботі визначено основні завдання на розробку мережі, проаналізовано інформацію яка буде використана для проектування мережі кол-центру. Представлено сценарії налаштування мереж, опис протоколів та топологій, які будуть використані протягом всієї роботи. Також наводяться результати тестування мережі.

КЛЮЧОВІ СЛОВА: РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ, SIEM, СИСТЕМИ ПОПЕРЕДЖЕННЯ ПРО КІБЕРБЕЗПЕКУ, СОЦІАЛЬНО-ТЕХНІЧНИЙ ПІДХІД, КУЛЬТУРА БЕЗПЕКИ ОРГАНІЗАЦІЇ.

ABSTRACT

The final qualification work of the master consists of a project of a secure call-centre network and an explanatory note. Explanatory note to the graduation work contains 59 pages, 26 illustrations and 8 tables.

The aim of the work is to improve the security of the internal security network by creating a user interface using a vector mechanism based on the Wazuh application.

The paper defines the main tasks for the development of the network, analyzes the information that will be used to design the call center network. The scenarios of network configuration, description of protocols and topologies that will be used throughout the work are presented. The results of network testing are also given.

KEYWORDS: CYBERSECURITY INCIDENT RESPONSE, SIEM, CYBERSECURITY ALERT SYSTEMS, SOCIO-TECHNICAL APPROACH, ORGANIZATION SECURITY CULTURE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AC	Автоматизована система
CSIRT	Computer Security Incident Response Team
CISO	Chief Information Security Officer
SOC	Security Operations Center
IRP	Incident Response Platform
CISA	Certified Information Systems Auditor
NIST	National Institute of Standards and Technology
SIEM	Security information and event management
EDR	Endpoint Detection and Response
SOAR	Security Orchestration, Automation and Response
XDR	External Data Representation
ASM	American Society of Microbiology
UEBA	User and Entity Behavior Analytics

ВСТУП

У сфері кібербезпеки управління інцидентами можна визначити, як процес ідентифікації, управління, реєстрації та аналізу загроз безпеці та інцидентів, пов’язаних з кібербезпекою. Належне управління інцидентами може зменшити несприятливі наслідки кіберруйнування та запобігти кібератаці. Організація без гарного плану реагування на інциденти може стати жертвою кібератаки, під час якої дані організації можуть бути скомпрометовані.

Навіть найкраща інфраструктура інформаційної безпеки не може гарантувати відсутність вторгнень чи інших зловмисних дій. Коли трапляються інциденти комп’ютерної безпеки, для організації вкрай важливо мати ефективні засоби керування ними та реагування на них. Швидкість з якою організація може розпізнати, проаналізувати, запобігти інциденту та реагувати на нього, обмежить завдані збитки.

Оскільки обсяг і складність загроз кібербезпеці продовжують зростати, організації впроваджують методи, які дозволяють їм швидко виявляти, реагувати та пом’якшувати ці типи інцидентів, одночасно стаючи більш стійкими та захищаючи від майбутніх інцидентів.

Наявність можливостей ефективного управління інцидентами є важливою частиною розгортання та впровадження будь-якого програмного забезпечення, апаратного забезпечення або бізнес-процесу. Організації починають усвідомлювати, що комунікація та взаємодія між розробниками системи програмного забезпечення та персоналом, який виконує дії з управління інцидентами, може надати інформацію для створення кращого захисту інфраструктури та процесів реагування, щоб подолати або запобігти зловмисній і несанкціонованій діяльності та загрозам.

Управління інцидентами безпеки, як один із найважливіших запобіжних засобів контролю в системі інформаційної безпеки, є інтегрованим процесом виявлення, звітування, ескалації та вирішення інцидентів безпеки. Цей процес також постійно вдосконалюється на основі результатів аналізів після інцидентів, щоб можна було своєчасно розглядати будь-які нові форми інцидентів безпеки.

Актуальність роботи полягає в тому, що сучасні системи поведінки користувачів не оперативні, в наслідок цього протягом тривалого часу нападники можуть перебувати у внутрішній мережі непоміченими.

Метою цього проєкту є підвищення безпеки внутрішньої мережі шляхом створення інтерфейсу користувача за допомогою механізму на основі додатку Wazuh.

Для досягнення поставлених цілей розроблено та виконано наступні завдання:

1) Визначити основні недоліки теперішніх методів виявлення інцидентів безпеки.

2) Переглянути параметри, доступні для створення профілів користувачів.

3) Порівняти відомі методи профілів і опорних машин.

4) Створити профіль користувача за допомогою системи підтримки Wazuh.

5) Використати більш структуровану модель.

Об’єктом дослідження є системи управління інцидентами інформаційної безпеки.

Предметом дослідження є захист інформації від витоку конфіденційних даних.

Наукова новизна отриманих результатів полягає в тому, що в результаті роботи створено персональну модель поведінки користувача та організовано групову роботу з вирішення завдань.

Практичне значення одержаного результату надзвичайно велика, адже це дозволяє краще знати поведінку користувача, що дозволяє заздалегідь ідентифікувати зловмисника в Інтернеті.

РОЗДІЛ 1. Аналіз проблем побудови систем управління інцидентами

1.1 Теоретичні аспекти управління інцидентами

Інцидент інформаційної безпеки можна визначити як спробу або успішний несанкціонований доступ, використання, розкриття, модифікацію або знищення інформації; втручання в роботу інформаційних технологій; або порушення явної або неявної політики прийнятного використання.

Це становить загрозу безпеці комп'ютера чи мережі на підприємстві щодо доступності, цілісності чи конфіденційності. Типовим прикладом є витік конфіденційної інформації, який негативно впливає на інтереси підприємства.

Як приклад інцидентів можна назвати такі події, як несанкціонована зміна даних на вебсайті організації, залишення комп'ютера розблокованим без нагляду, конфіденційна передача.

Немає єдиного найкращого способу зменшити ризики для інформаційної безпеки, незалежно від того, чи він добре розроблений. політика безпеки або сучасний брандмауер, не можуть захистити від виникнення в інформаційному середовищі подій, які можуть загрожувати діяльності організації. Статистика загроз інформаційній безпеці організації представлена на рис. 1.1.

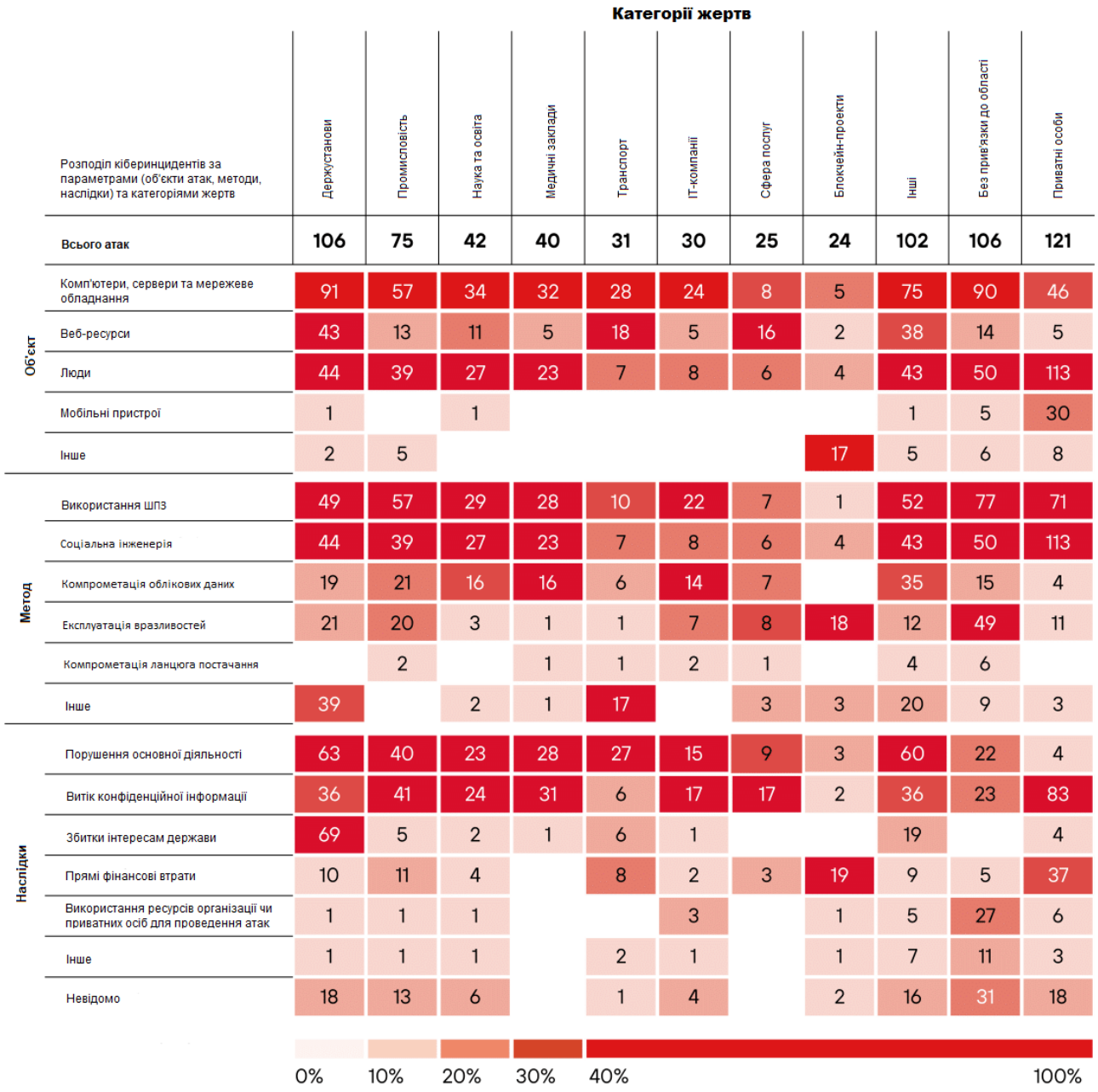

Рисунок 1.1 – Статистика загроз

Складність і різноманітність щоденного робочого середовища бізнесу визначає підвищений ризик незалежно від готовності, підготовки та оптимізації. Крім того, завжди існує ймовірність невідомих загроз інформаційній безпеці. Нехтування організацією вирішенням таких ситуацій може вплинути на відновлення бізнес-процесу та завдати ще більшої шкоди.

Процес управління інцидентами безпеки включає п’ять етапів, включаючи звітування про інциденти, оцінку впливу, посилення та вирішення інцидентів, моніторинг інцидентів і аналіз інцидентів.

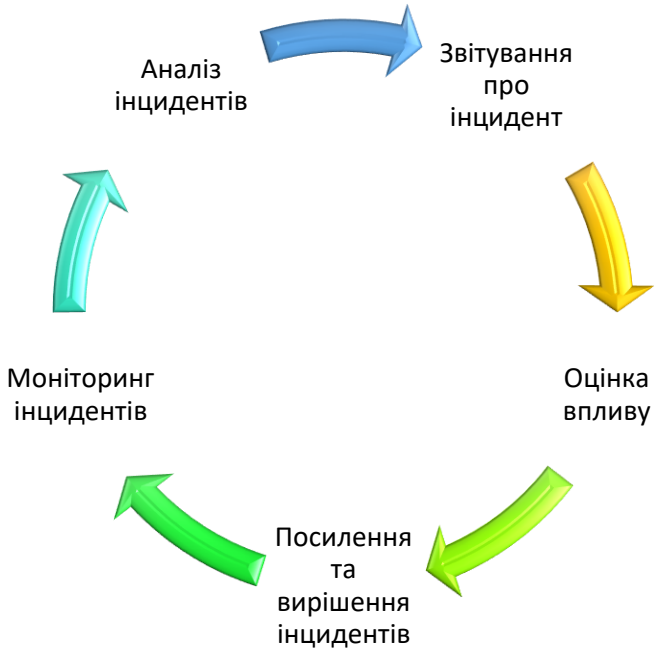

Рисунок 1.2 – Процес управління інцидентами

Кожен із зазначених вище етапів допомагає підприємству стримувати вплив інцидентів інформаційної безпеки та керувати процесом обробки якомога ефективніше.

Належним чином розроблене та реалізоване управління інцидентами безпеки також має допомогти підприємству запобігти майбутнім інцидентам безпеки.[4]

Таблиця 1

Загальні відомості про управління інцидентами безпеки

Звітування про інцидент	Етап звітування про інциденти має на меті створення дієвого механізму для виявлення інцидентів безпеки та звітування про них. Механізм передбачає використання людських ресурсів, таких як створення групи реагування на інциденти безпеки під керівництвом офіцера з інформаційної безпеки, а також отримання запитів і звітів від користувачів, які поінформовані про можливі інциденти безпеки в системах підприємства.

Продовження таблиці 1

Оцінка впливу	Для кожного повідомленого інциденту слід проводити оцінку, щоб визначити масштаб і вплив на підприємство. Наприклад, інцидент можна оцінити як такий, що має високий, середній або низький вплив на підприємство відповідно до суми грошових втрат, тривалості перерви в наданні послуг або масштабу шкоди репутації. Необхідно також провести коротке дослідження першопричини, щоб забезпечити ефективне планування вирішення інциденту. Метою виконання оцінки впливу є максимізація ефективності та результативності обробки, водночас мінімізація додаткових ресурсів, вкладених у вирішення інцидентів інформаційної безпеки.
Посилення та вирішення інцидентів	Значні інциденти безпеки, виявлені під час оцінки впливу, потребують передачі вищому керівництву для ознайомлення або участі у розв'язанні проблем безпеки, викликаних інцидентом. Розв’язання інцидентів передбачає розподіл роботи між членами групи реагування на інциденти безпеки та іншими відповідними користувачами чи відділами, керування зв’язком між різними сторонами та виконання плану вирішення.

Продовження таблиці 1

Моніторинг інцидентів	Інциденти безпеки різного характеру вказують на різні часові рамки, потреби в ресурсах і рішення. Таким чином, слід уважно стежити за станом процесу обробки кожного інциденту, щоб забезпечити надання індивідуального рішення в розумні терміни та обмеження ресурсів.
Аналіз інцидентів	У складному процесі управління інцидентами безпеки група реагування на інциденти безпеки повинна проявляти належну обачність, щоб досліджувати першопричину кожного інциденту безпеки та вчитися на цьому досвіді, щоб уникнути повторення інцидентів у майбутньому шляхом впровадження необхідних засобів контролю.

1.2 Основи управління інцидентами

Реагування на інциденти (іноді їх називають реагуванням на інциденти кібербезпеки) належать до процесів і технологій організації для виявлення та реагування на кіберзагрози, порушення безпеки або кібератаки. Мета реагування на інциденти полягає в тому, щоб запобігти кібератакам до того, як вони відбудуться, а також мінімізувати витрати та збої в роботі в результаті будь-яких кібератак.

Інцидент безпеки або подія безпеки — це будь-який цифровий або фізичний злом, який загрожує конфіденційності, цілісності чи доступності інформаційних систем або конфіденційних даних організації. Інциденти безпеки можуть варіюватися від навмисних кібератак хакерів або неавторизованих користувачів до ненавмисних порушень політики безпеки законними авторизованими користувачами.

Таблиця 2

Інструменти реагування на інциденти

Типи засобів реагування на інциденти	**Навіщо вони потрібні**	**Приклади інструментів**
SIEM	Збирає та об’єднує дані журналу, створені в технологічній інфраструктурі організації, включаючи програми, хост-системи, мережу та пристрої безпеки (наприклад, антивірусні фільтри та брандмауери). Надає звіти про інциденти, пов’язані з безпекою, включаючи активність зловмисного програмного забезпечення та входи. Він також надсилає сповіщення, якщо дія конфліктує з чинними наборами правил, що вказує на проблему безпеки.	Exabeam Security Operations Platform (включаючи Data Lake, Advanced Analytics, Incident Responder), QRadar, USM, ESM
Системи виявлення вторгнень (IDS) — на основі мережі та хосту	Використовує базові лінії або сигнатури атак, щоб видавати сповіщення про підозрілу поведінку або відомі атаки на сервері, системі виявлення вторгнень на основі хосту (HIDS) або системі виявлення вторгнень на основі мережі (NIDS).	Snort, Suricata, BroIDS, OSSEC, SolarWinds

Продовження таблиці 2

Аналізатори Netflow	Переглядає фактичний трафік через прикордонні шлюзи та всередині мережі. Netflow використовується для відстеження певного потоку активності, щоб побачити, які протоколи використовуються у вашій мережі, або щоб побачити, які активи спілкуються між собою.	ntop, NfSen, Nfdump
Сканери вразливостей	Виокремлює потенційні зони ризику, оцінює зону поверхні атаки вашої організації на наявність відомих слабких місць і надає інструкції щодо усунення. Уразливості можуть бути спричинені неправильною конфігурацією, помилками у ваших власних програмах або використанням сторонніх компонентів, якими можуть скористатися зловмисники.	OpenVAS
Моніторинг доступності	Метою реагування на інциденти є обмеження часу простою. Збій служби або програми може бути першою ознакою поточного інциденту. Моніторинг доступності запобігає несприятливим ситуаціям, вивчаючи час безвідмовної роботи компонентів інфраструктури, включаючи програми та сервери. Він повідомляє адміністратору про проблеми, перш ніж вони вплинуть на організацію.	Нагіос

Продовження таблиці 2

Вебпроксі	Контролює доступ до вебсайту і реєструє дані про підключення. Багато загроз працюють через HTTP, включаючи можливість входу на віддалену IP-адресу. З'єднання HTTP також може бути важливим для криміналістики та відстеження загроз.	Squid Proxy

Деякі з найпоширеніших інцидентів безпеки включають:

Програми-вимагачі. ПЗ-вимагач — це тип зловмисного програмного забезпечення або зловмисного програмного забезпечення, яке блокує дані або комп'ютерний пристрій жертви та загрожує залишити їх заблокованими — або ще гірше — якщо жертва не заплатить зловмисникові викуп.

Фішинг і соціальна інженерія. Фішингові атаки – це цифрові або голосові повідомлення, які намагаються маніпулювати одержувачами, щоб вони надали конфіденційну інформацію, завантажили шкідливе програмне забезпечення, переказали гроші чи активи не тим людям або вжили інших шкідливих дій. Шахраї створюють фішингові повідомлення так, щоб вони виглядали чи звучали так, ніби вони надходять від перевіреної чи надійної організації, чи особи — іноді навіть від особи, яку одержувач знає особисто.

Це також найпоширеніша форма соціальної інженерії — клас атак, які зламують людську природу, а не вразливі місця цифрової безпеки, щоб отримати несанкціонований доступ до конфіденційних особистих або корпоративних даних або активів.

DDoS атаки. У розподіленій атаці типу «відмова в обслуговуванні» (DDoS) хакери отримують дистанційний контроль над великою кількістю комп'ютерів і використовують їх, щоб переповнювати мережу або сервери цільової організації трафіком, роблячи ці ресурси недоступними для законних користувачів.

Атаки на ланцюги постачання. Атаки на ланцюг постачання— це кібератаки, які проникають у цільову організацію шляхом атаки на її постачальників, наприклад, шляхом викрадення конфіденційних даних із систем постачальника або використання послуг постачальника для розповсюдження шкідливого програмного забезпечення.

Інсайдерські загрози. Існує два типи внутрішніх загроз. Зловмисні інсайдери – це співробітники, партнери чи інші авторизовані користувачі, які навмисно порушують інформаційну безпеку організації. Недбалі інсайдери – це авторизовані користувачі, які ненавмисно порушують безпеку, не дотримуючись найкращих практик безпеки, наприклад, використовуючи слабкі паролі або зберігаючи конфіденційні дані в незахищених місцях.

1.2.1 Реагування на інциденти

Планування реагування на інциденти

Як зазначалося вище, зусилля організації з реагування на інциденти керуються планом реагування на інциденти. Зазвичай вони створюються та виконуються групою реагування на інциденти комп'ютерної безпеки (CSIRT), що складається з зацікавлених сторін з усієї організації — головного спеціаліста з інформаційної безпеки (CISO), операційного центру безпеки (SOC) та IT-персоналу, а також представників виконавчого керівництва. , право, кадри, дотримання нормативних вимог та управління ризиками.

План реагування на інцидент зазвичай включає:

- Ролі та обов'язки кожного члена CSIRT;
- Рішення безпеки — програмне забезпечення, апаратне забезпечення та інші технології — які будуть встановлені на підприємстві;
- План забезпечення безперервності бізнесу, в якому описано процедури якнайшвидшого відновлення критично уражених систем і даних у разі збою;
- Детальна методологія реагування на інциденти, яка визначає конкретні кроки, які необхідно виконати на кожному етапі процесу реагування на інциденти та ким;

- План комунікацій для інформування керівників компанії, співробітників, клієнтів і навіть правоохоронних органів про інциденти;
- Інструкції з документування для збору інформації та документування інцидентів для посмертного огляду та (за необхідності) судового розгляду.

Нерідко CSIRT складає різні плани реагування на інциденти різних типів, оскільки кожен тип може потребувати унікальної реакції. Більшість організацій мають конкретні плани реагування на інциденти, що стосуються DDoS-атак, зловмисного програмного забезпечення та програм-вимагачів, а також фішингу, і майже половина має плани щодо внутрішніх загроз.

Деякі організації доповнюють внутрішні CSIRT зовнішніми партнерами, які надають послуги з реагування на інциденти. Ці партнери часто працюють над утриманням, допомагають у різних аспектах процесу управління інцидентами, включаючи підготовку та виконання IRP.

Процес реагування на інцидент

Більшість IRP також дотримуються тієї самої загальної структури реагування на інциденти, заснованої на моделях реагування на інциденти, розроблених Інститутом SANS, Національним інститутом стандартів і технологій (NIST) і Агентством кібербезпеки та інфраструктури (CISA).

Підготовка

Ця перша фаза реагування на інцидент також є безперервною, щоб переконатися, що CSIRT завжди має найкращі можливі процедури та інструменти для реагування на ідентифікацію, локалізацію та відновлення після інциденту якнайшвидше та з мінімальними порушеннями роботи.

Завдяки регулярній оцінці ризиків CSIRT визначає вразливі місця в мережі, визначає різні типи інцидентів безпеки, які становлять загрозу для мережі, і визначає пріоритетність кожного типу відповідно до його потенційного впливу на організацію. На основі цієї оцінки ризику CSIRT може оновити заведені плани реагування на інциденти або розробити нові.

Виявлення та аналіз

Під час цього етапу члени команди безпеки відстежують мережу на наявність підозрілої активності та потенційних загроз. Вони аналізують дані, сповіщення та попередження, зібрані з журналів пристрою та з різних інструментів безпеки (антивірусне програмне забезпечення, брандмауери), встановлених у мережі, відфільтровуючи помилкові спрацьовування та сортуючи фактичні попередження в порядку серйозності.

Сьогодні більшість організацій використовують одне або кілька рішень безпеки, наприклад SIEM (інформація про безпеку та керування подіями) і EDR (виявлення кінцевих точок і реагування), щоб допомогти командам безпеки відстежувати й аналізувати події безпеки в режимі реального часу, а також автоматизувати процеси виявлення інцидентів і реагування на них. . (Детальніше дивіться «Технології реагування на інциденти» нижче.)

План спілкування також вступає в дію на цьому етапі. Після того, як CSIRT визначить, з якою загрозою чи порушенням вони мають справу, вони повідомлять відповідний персонал перед тим, як перейти до наступного етапу процесу реагування на інцидент.

Стримування

Команда реагування на інциденти вживає заходів, щоб запобігти подальшому збитку мережі. Діяльність стримування можна розділити на дві категорії:

Короткострокові заходи стримування зосереджені на запобіганні поширенню поточної загрози шляхом ізоляції уражених систем, наприклад шляхом виведення заражених пристроїв з мережі.

Довгострокові заходи стримування зосереджені на захисті незачеплених систем шляхом посилення контролю безпеки навколо них, наприклад, сегментування конфіденційних баз даних від решти мережі.

На цьому етапі CSIRT також може створити резервні копії уражених і неуражених систем, щоб запобігти додатковій втраті даних і отримати судово-медичні докази інциденту для подальшого вивчення.

Ерадикація

Після того як загрозу локалізовано, команда переходить до повного усунення та повного видалення загрози із системи. Це передбачає активне усунення самої загрози, наприклад, знищення зловмисного програмного забезпечення, завантаження неавторизованого або шахрайського користувача з мережі, а також перевірку як уражених, так і неуражених систем, щоб переконатися, що не залишилося слідів зламу.

Відновлення

Коли група реагування на інциденти впевнена, що загрозу повністю усунено, вони відновлюють уражені системи до нормального функціонування. Це може включати розгортання виправлень, відновлення систем із резервних копій і повернення виправлених систем і пристроїв у режим онлайн.

Огляд після інциденту. Протягом кожного етапу процесу реагування на інцидент CSIRT збирає докази порушення та документує кроки, які вона вживає для стримування та усунення загрози. На цьому етапі CSIRT перевіряє цю інформацію, щоб краще зрозуміти інцидент. CSIRT намагається визначити першопричину атаки, визначити, як вона успішно зламала мережу, і усунути вразливі місця, щоб у майбутньому не відбувалося подібних інцидентів.

CSIRT також перевіряє, що пройшло добре, і шукає можливості для вдосконалення систем, інструментів і процесів для посилення ініціатив реагування на інциденти проти майбутніх атак. Залежно від обставин порушення правоохоронні органи також можуть бути залучені до розслідування інциденту.

1.2.2 Технології реагування на інциденти

Як зазначалося вище, окрім опису кроків, які CSIRT повинні вжити у випадку інциденту безпеки, плани реагування на інцидент зазвичай окреслюють рішення безпеки, які повинні мати групи реагування на інциденти для виконання або автоматизації ключових робочих процесів реагування на інциденти, таких як збір кореляція даних безпеки, виявлення інцидентів у режимі реального часу та реагування на поточні атаки.

Рисунок 1.3 – Технології реагування на інциденти

Деякі з найбільш часто використовуваних технологій реагування на інциденти включають:

SIEM (інформація про безпеку та керування подіями) : SIEM агрегує та корелює дані про події безпеки з різних внутрішніх інструментів безпеки (наприклад, брандмауери, сканери вразливостей, канали розвідки про загрози) і з пристроїв у мережі. SIEM може допомогти командам реагування на інциденти боротися з «втомою сповіщень» за допомогою індикаторів реальних загроз від величезної кількості сповіщень, які створюють ці інструменти.

SOAR (оркестровка безпеки, автоматизація та реагування): SOAR дає змогу групам безпеки визначати — формалізовані робочі процеси, які координують різні операції та інструменти безпеки у відповідь на інциденти безпеки — і автоматизувати частини цих робочих процесів, де це можливо.

EDR (виявлення кінцевої точки та реагування на неї) : EDR — це програмне забезпечення, призначене для автоматичного захисту кінцевих користувачів організації, кінцевих пристроїв та IT-активів від кіберзагроз, які оминули антивірусне програмне забезпечення та інші традиційні інструменти безпеки кінцевих точок. EDR постійно збирає дані з усіх кінцевих точок мережі; він аналізує дані в режимі реального часу на наявність доказів відомих або

підозрюваних кіберзагроз і може автоматично реагувати, щоб запобігти або мінімізувати шкоду від виявлених загроз.

XDR (розширене виявлення та реагування): XDR — це технологія кібербезпеки, яка об'єднує засоби безпеки, контрольні точки, джерела даних і телеметрії, а також аналітику в гібридному IT-середовищі (кінцеві точки, мережі, приватні та публічні хмари) для створення єдиної центральної корпоративної системи. для запобігання загрозам, виявлення та реагування. Технологія XDR, яка все ще розвивається, має потенціал допомогти розширеним групам безпеки та центрам безпеки (SOC) робити більше з меншими витратами шляхом усунення силосів між інструментами безпеки та автоматизації реагування на всьому ланцюжку ліквідації кіберзагроз.

UEBA (аналітика поведінки користувачів і об'єктів) : (UEBA) використовує поведінкову аналітику, алгоритми машинного навчання та автоматизацію для визначення ненормальної та потенційно небезпечної поведінки користувачів і пристроїв. UEBA особливо ефективний у виявленні внутрішніх загроз — зловмисних інсайдерів або хакерів, які використовують скомпрометовані інсайдерські облікові дані — які можуть уникнути інших інструментів безпеки, оскільки імітують авторизований мережевий трафік. Функціональні можливості UEBA часто включають рішення SIEM, EDR і XDR.

ASM (керування приєднаною поверхнею) : рішення ASM автоматизують безперервне виявлення, аналіз, виправлення та моніторинг вразливостей і потенційних векторів атак на всіх активах на поверхні атаки організації. ASM може виявити мережеві активи, які раніше не контролювалися, відобразити зв'язки між активами.[10]

1.3 Аналіз сучасних підходів до створення груп реагування на інциденти інформаційної безпеки

Для підготовки до інцидентів та реагування на них слід сформувати централізовану групу реагування на інциденти, яка відповідає за виявлення порушень безпеки та вжиття заходів реагування. У великій організації це

спеціальна команда, відома як CSIRT. До складу CSIRT входять штатні співробітники служби безпеки. Ці особи аналізують інформацію про інцидент і реагують на нього.

У менших організаціях група реагування на інциденти може складатися з IT-персоналу, який має певну підготовку з питань безпеки, доповнену власними або залученими експертами з питань безпеки.

Група реагування на інциденти також взаємодіє із зацікавленими сторонами всередині організації та зовнішніми групами, такими як преса, юрисконсульти, постраждалі клієнти та правоохоронні органи.

До складу команди повинні входити

- **Менеджер з реагування на інцидент (керівник групи)** - координує всі дії команди та забезпечує зосередження команди на мінімізації збитків та швидкому відновленні. Визначає пріоритети дій під час ізоляції, аналізу та локалізації інциденту. Контролює всі дії та керує командою під час інцидентів високої складності.

- **Аналітики безпеки** - менеджеру допомагає команда аналітиків безпеки, які працюють у різних відділах для ізоляції та виправлення недоліків у системах безпеки організації, рішеннях та додатках. Вони рекомендують конкретні заходи для покращення загального стану безпеки.

- **Провідний дослідник** - визначає першопричину, аналізує всі докази, керує іншими аналітиками безпеки та проводить швидке відновлення систем та сервісів.

- **Дослідники загроз** - надають контекст інциденту та розвіддані про загрози. Вони використовують цю інформацію та записи про попередні інциденти для створення бази даних внутрішньої розвідки. У багатьох командах безпеки дослідники загроз поступово замінюються автоматизованими інструментами розвідки загроз.

- **Комунікації** - комунікації з усіма аудиторіями всередині та за межами компанії, включаючи керівництво, внутрішні зацікавлені сторони, юридичний відділ, пресу і клієнтів.

- **Документація та графік** - документує зусилля команди з розслідування, виявлення та відновлення. Створює графік для кожного етапу інциденту. Системи управління інформацією та подіями безпеки наступного покоління (SIEM) здатні автоматично генерувати документацію та хронологію інцидентів. Наприклад, див. модуль розширеної аналітики Exabeam Advanced Analytics, що пропонується платформою Exabeam Security Management Platform.

- **HR / юридичне представництво** - інцидент може перерости в кримінальне переслідування. Таким чином, ви повинні мати кадрове та юридичне керівництво.

Висновок до розділу 1

В першому розділі було розглянуто управління інцидентами безпеки, як один із найважливіших запобіжних засобів контролю в системі інформаційної безпеки, є інтегрованим процесом виявлення, звітування, ескалації та вирішення інцидентів безпеки, що сталися. Цей процес також постійно вдосконалюється на основі результатів аналізів після інцидентів, щоб можна було своєчасно розглядати будь-які нові форми інцидентів безпеки.

Керівництво, кваліфікована команда реагування на інциденти та хороша обізнаність користувачів є ключовими факторами побудови успішного процесу управління інцидентами безпеки. Залежить від природи різних інцидентів безпеки, додаткові ресурси для залучення третіх сторін (наприклад, постачальників, зовнішніх спеціалістів) також слід враховувати.

РОЗДІЛ 2. Проєктування інформаційних систем управління інцидентами

2.1 Аналіз інформаційних потоків для інформаційної системи підприємства

Поліпшення обміну інформацією безпосередньо впливає на вдосконалення загальної системи управління компанією, що може призвести до кращих результатів. З кожним роком зростає обсяг, складність та інтенсивність інформаційних обмінів, все більше уваги приділяється проблемі розробки методів опису, аналізу та аналізу інформаційних потоків.

Поняття «управління інформаційними потоками» нерозривно пов'язане з поняттям «управління інформаційною системою». Оскільки інформаційні потоки в бізнес-процесі діють як інтерфейс між усіма факторами та навколишнім середовищем, ці два поняття можна розглядати з тією лише різницею, що термін «управління інформаційною системою» зазвичай означає те саме апаратне та програмне забезпечення бази даних, технології обробки даних, управління людьми, термін «управління інформаційними потоками» охоплює процес розповсюдження інформації за допомогою різних каналів і людей.

Безперервна інформація — це добре структурований набір повідомлень в інформаційній системі в певному форматі, мові, тексті. Події мають такі характеристики: напрям потоку інформації, обсяг потоку інформації, час потоку інформації, вартість потоку інформації, інтенсивність потоку інформації, адекватність потоку інформації, інформативність потоку інформації, структура потоку інформації та інтеграція потоку інформації різних відділів.

Таким чином, галузеві інформаційні потоки мають як кількісні, так і якісні характеристики, які мотивують розподільні підходи до управління інформацією, що інформаційні потоки мають характеристики загальні для інших типів потоків (матеріальні, фінансові тощо), а також характеристики властиві тільки інформаційним потокам.

Аналіз українських компаній виявив різного роду недоліки в інформаційному потоці компанії: відсутність актуальної інформації, викривлення та дублювання

інформації, чіткий розподіл обов’язків по веденню документації, несвоєчасне або листове подання інформації, відсутність доходів.

Дані, зібрані в системі управління для аналізу та подальшої обробки, повинні відповідати наступним критеріям: своєчасність, точність, актуальність, корисність, повнота, значущість. Процес управління контентом вимагає постійного розвитку теоретичних основ управління контентом підприємства та практичних шляхів застосування сучасних інформаційних технологій для вдосконалення управління контентом в системі управління та зниження витрат на їх обслуговування.

2.2 Проєктування загальної структури підприємства

Кожна організаційна структура управління – це перш за все завжди формальне, для досягнення цілей, завдань господарської діяльності конкретного бізнесу, створеного за певними правилами та нормами. Організаційна структура, як правило, є одним із важливих елементів системи управління і показує зв'язок між виробництвом і економікою, що сприяє розвитку бізнесу.

Спеціалізація з питань управління, яка полягає в тому, що кожен структурний підрозділ виконує завдання на вищому рівні компетенції.

Інтеграція та децентралізація управління передбачає розподіл повноважень всередині організації. Іншими словами, центральне управління використовується лише на найвищому рівні, на відміну від державного управління, яке поширюється на нижчі рівні управління.

Ієрархічна структура системи управління виглядає наступним чином. Структурні підрозділи різних рівнів управління поділяються і створюються зверху вниз. Кожен елемент структури повинен виконувати обов'язки відповідно до своєї функції, сфери відповідальності та обов'язків.

Відокремлення завдань стратегічного управління від тактичних робіт підходить для створення організаційних структур.

Структури бізнес-організації, використовують принципи, дотримуючись відомих послідовних кроків:

1. Визначення бізнес-цілі.
2. Визначення та аналіз факторів впливу.
3. Побудова стилю управління бізнесом.
4. Створення цілей і функцій організаційної структури управління.
5. Вибір шляхів створення організаційної структури управління.

Отже, перший крок передбачає підсумовування головних цілей. Важливий аспект, який матиме важливі наслідки для подальшого розвитку бізнесу. Характер підприємницької діяльності впливає на формування цілей різних часових періодів, таких як короткострокові, середньострокові та довгострокові. Визначені цілі будуть конкретними, передбаченими, взаємоузгодженими та зрозумілими, щоб забезпечити оптимальний розвиток бізнесу. Цілі можуть бути спрямовані на виробничий процес, різні підрозділи або загальну продуктивність. Поліпшення фінансової ситуації, завоювання значної частки ринку, завоювання значної частки внутрішнього та міжнародного ринку, покращення бізнес-середовища та задоволеності споживачів. Не зважаючи на необхідність компанії насамперед орієнтовані на досягнення стратегічних цілей. Перспектива діяльності компанії визначається, перш за все, обраною стратегією. Між організаційною структурою управління та обраною стратегією завжди існує залежність.

На другому етапі – визначення та аналіз факторів впливу – враховуються прямі та опосередковані впливи зовнішнього середовища: економічні та політичні чинники, правові, соціальні та культурні фактори, технології, ринок праці, тощо.

При виконанні третього кроку - побудови моделі управління бізнес розробка найкращої моделі організаційної структури для конкретного бізнесу починається з розгляду різних показників, які впливають на продуктивність цієї організаційної структури.

Створює цільове дерево створеної організаційної структури, яке має бути реалізовано на основі аналізу заведений організаційної структури. Цей аналіз дозволяє змінити зміст деяких елементів структури управління, щоб деякі структурні елементи та активи були збережені та повністю доступні.

Результати кроку чотири визначатимуть, як буде створено корпоративне управління. Обґрунтована оцінка варіантів дозволяє вибрати найкращий спосіб створення корпоративного управління для бізнесу. Координація з керівниками всіх підрозділів забезпечує остаточний вибір організаційної структури.

Оскільки навколишнє середовище змінюється прискореними темпами, компаніям доводиться частіше, ніж будь-коли раніше, вдосконалювати стратегії, щоб відповідати вимогам ринку. Це означає, що зміни в стратегії передують і призводять до змін у структурі. Структура управління є найменш придатною зі стратегічної точки зору. Це пояснюється тим, що фактори, які безпосередньо впливають на вибір структури змінюються повільніше, ніж фактори, що впливають на вибір стратегії. Наприклад, якщо ви обираєте інноваційну стратегію, подумайте про створення організаційного менеджера з неофіційними повноваженнями.

2.3 Аналіз та вибір програмних рішень для побудови системи

Останнім часом сильно підвищилися складність та координованість атак на інформаційні системи. Разом з тим ускладнюється і комплекс засобів захисту інформації, що застосовується — мережеві та хостові системи виявлення вторгнень, DLP-системи, антивірусні системи та міжмережні екрани, сканери вразливостей та інше. Кожен засіб захисту генерує потік подій з різною деталізацією і найчастіше побачити атаку можна лише з накладення подій із різних систем.

Реагування на інцидент не повинно бути автоматизованим. Проте програмне забезпечення, яке самостійно запускає дії після виявлення вторгнення або дії зловмисного програмного забезпечення, стає все більш доступним. Цей тип системи реагування на інциденти називається SOAR.

Системи SOAR підключають ідентифікатори атак через утиліти аналізу до систем захисту, які припиняють атаку та усувають пошкодження, які сталися. SOAR є майже синонімом системи запобігання вторгненням (IPS). Однак SOAR інтегрує інший провідний стандарт виявлення атак: SIEM.

Оскільки SIEM є основною частиною SOAR, постачальники інструментів SIEM знаходяться на передньому краї SOAR, розширюючи свій досвід у сферах аналізу загроз і реагування на інциденти. Іншими великими гравцями у сфері реагування на інциденти є виробники антивірусних систем. Ці компанії вже давно займаються пошуком шкідливого програмного забезпечення та його видаленням. Щоб забезпечити повний інструмент реагування на інциденти, їм просто потрібно додати захист від хакерської діяльності та вторгнення до свого арсеналу.

1. AlienVault OSSIM

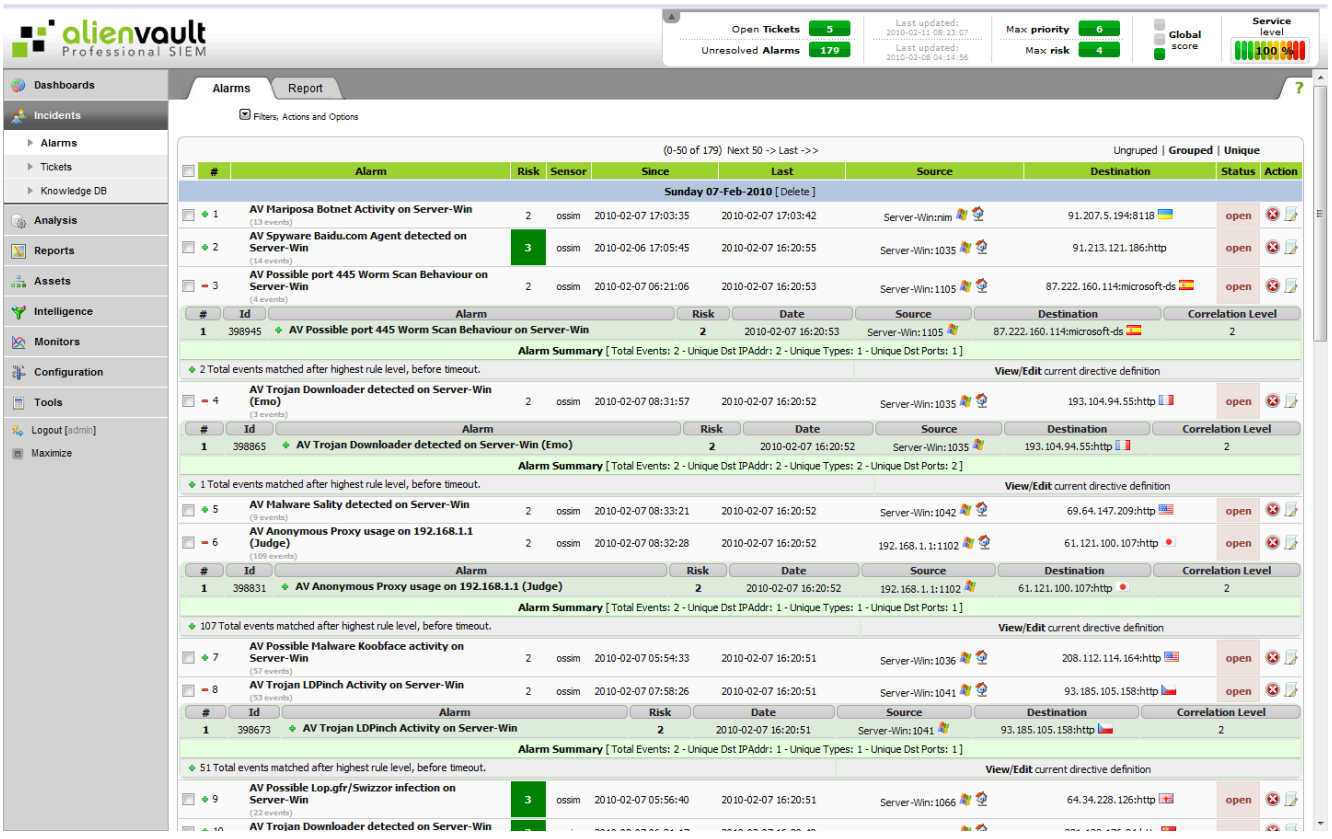

Рисунок 2.1 — Менеджер подій безпеки AlienVault OSSIM

AlienVault OSSIM – це open-source версія AlienVault USM, однієї з провідних комерційних SIEM-систем. OSSIM є фреймворком, що складається з декількох проєктів з відкритим вихідним кодом, включаючи мережну систему виявлення

вторгнень Snort, систему моніторингу мереж і вузлів Nagios, систему хоста виявлення вторгнень OSSEC і сканер вразливостей OpenVAS.

Для моніторингу за пристроями використовується AlienVault Agent, який відправляє журнали з хоста у форматі syslog в платформу GELF або може використовуватися плагін для інтеграції зі сторонніми сервісами, такими як сервіс реверсного проксіювання сайтів Cloudflare або багатофакторної аутентифікації Okta.

Версія USM відрізняється від OSSIM розширеною функціональністю управління журналами, моніторингу хмарної інфраструктури, автоматизації та оновлюваною інформацією про погрози та візуалізацією.

Переваги	**Недоліки**
Побудовано на перевірених open-source проєктах; Велика спільнота користувачів та розробників.	Не підтримує моніторинг хмарних платформ (наприклад, AWS чи Azure); Відсутнє керування логами, візуалізація, автоматизація та інтеграція зі сторонніми сервісами.

2. MozDef (Mozilla Defense Platform)

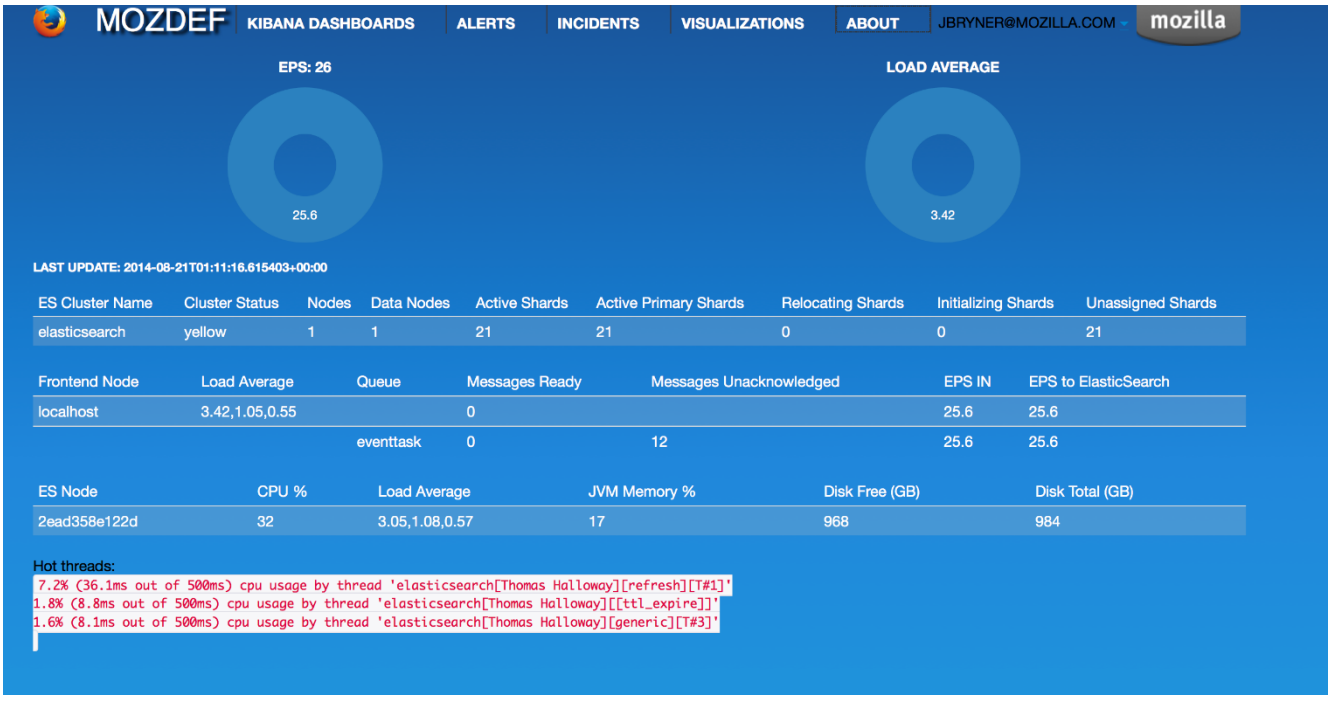

Рисунок 2.2 — Менеджер подій безпеки MozDef

Розроблена Mozilla SIEM-система MozDef використовується для автоматизації процесів обробки інцидентів безпеки. Система розроблена з нуля для отримання максимальної швидкодії, масштабованості та стійкості до відмов, з мікросервісною архітектурою – кожен сервіс працює в контейнері Docker.

Як і OSSIM, MozDef побудована на перевірених часом опенсорсних проєктах, що включають модуль індексування логів та пошуку Elasticsearch, платформу Meteor для побудови гнучкого web-інтерфейсу, та плагін Kibana для візуалізації та побудови графіків.

Кореляція подій та оповіщення виконується з використанням запиту Elasticsearch, що дозволяє написати власні правила обробки подій та оповіщення з використанням Python. За словами Mozilla, MozDef може обробляти понад 300 мільйонів подій на день. MozDef приймає події лише у форматі JSON, але є інтеграція зі сторонніми сервісами.

Переваги	**Недоліки**
Не використовує агентів – працює зі стандартними логами JSON; Легко масштабується завдяки мікросервісній архітектурі; Підтримує джерела даних хмарних сервісів, включаючи AWS CloudTrail та GuardDuty.	Нова і менш налагоджена система.

3. Wazuh

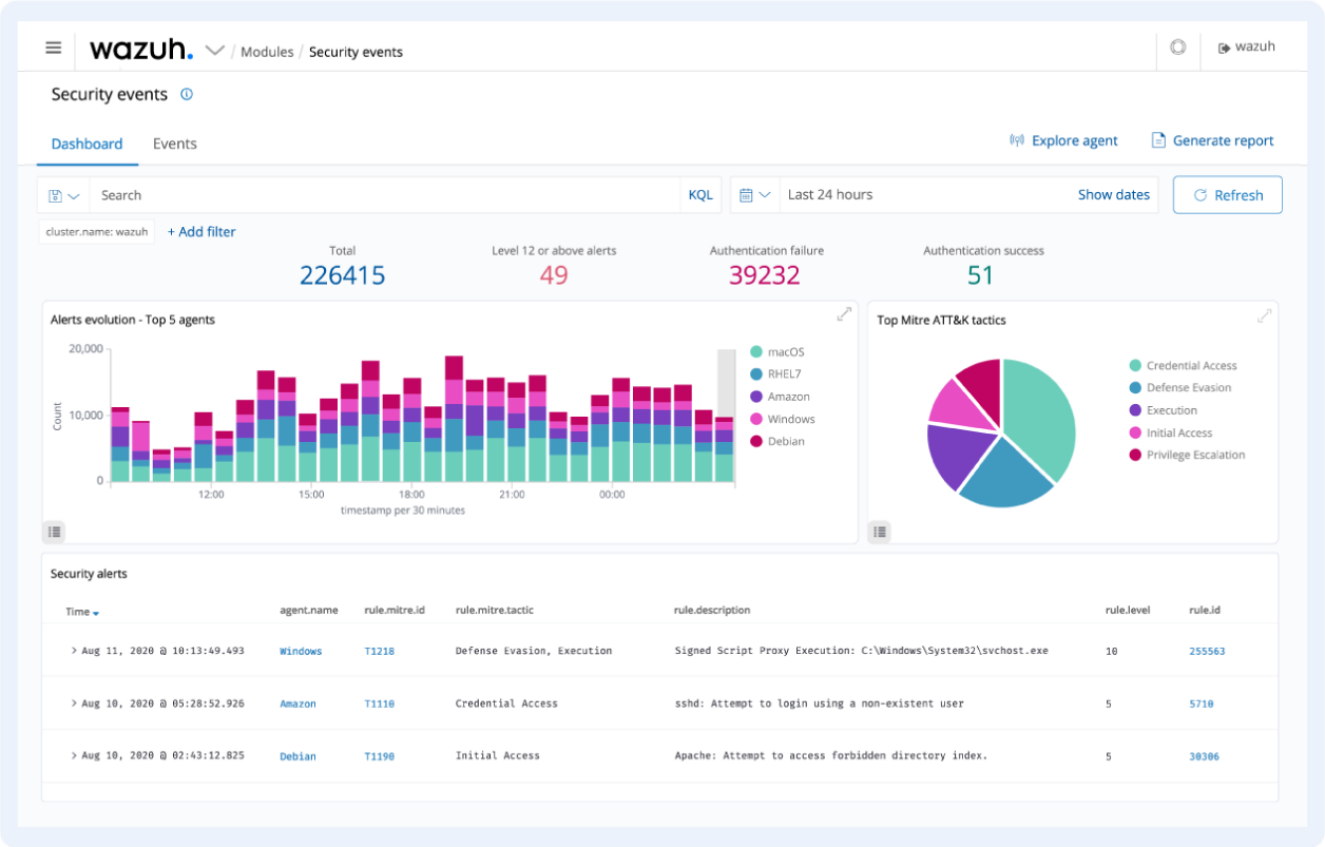

Рисунок 2.3 — Менеджер подій безпеки Wazuh

Wazuh почала розвивалася як форк OSSEC, однієї з найпопулярніших SIEM з відкритим кодом. І тепер це власне унікальне рішення з новою функціональністю, виправленими помилками та оптимізованою архітектурою.

Система побудована на стеку ElasticStack (Elasticsearch, Logstash, Kibana) і підтримує як збір даних на основі агентів, так і прийняття системних журналів. Це робить її ефективною для моніторингу пристроїв, які генерують журнали, але не підтримують встановлення агента - мережеві пристрої, принтери та периферія.

Wazuh підтримує наявні агенти OSSEC і навіть надає посібник із міграції з OSSEC на Wazuh. Хоча OSSEC все ще активно підтримують, Wazuh розглядають як продовження OSSEC через додавання нового вебінтерфейсу, REST API, повнішого набору правил і багатьох інших поліпшень.

Переваги	Недоліки
Заснована і сумісна з популярною SIEM OSSEC; Підтримує різні варіанти встановлення: Docker, Puppet, Chef, Ansible; Підтримує моніторинг хмарних сервісів, включно з AWS і Azure; Включає комплексний набір правил, для виявлення безлічі типів атак і дає змогу зіставляти їх відповідно до PCI DSS v3.1 і CIS. Інтегрується з системою зберігання та аналізу логів Splunk для візуалізації подій і підтримки API.	Складна архітектура - вимагає повного розгортання Elastic Stack на додаток до серверних компонентів Wazuh.

4. Prelude OSS

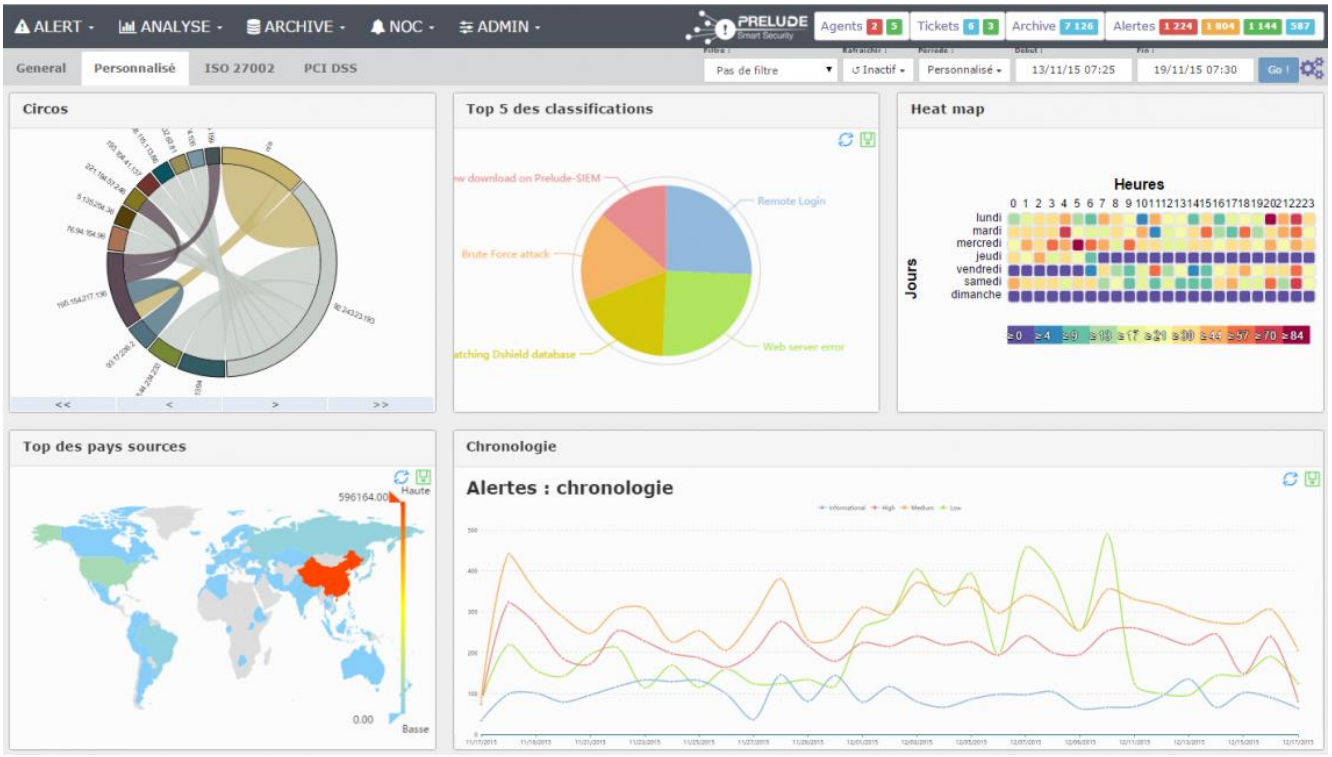

Рисунок 2.4 — Менеджер подій безпеки Prelude OSS

Prelude OSS - це open-source версія комерційної Prelude SIEM, розробленої французькою компанією CS. Рішення являє собою гнучку модульну SIEM-систему, що підтримує безліч форматів логів, інтеграцію зі сторонніми інструментами, такими як OSSEC, Snort і мережеву систему виявлення Suricata.

Кожна подія нормалізується в повідомлення за форматом IDMEF, що спрощує обмін даними з іншими системами. Але є і ложка дьогтю - Prelude OSS сильно обмежена за продуктивністю і функціональністю порівняно з комерційною версією Prelude SIEM, і призначена скоріше для невеликих проєктів або для вивчення рішень SIEM і оцінки Prelude SIEM.

Переваги	**Недоліки**
Випробувана часом система, що розробляється з 1998 р.; Підтримує безліч різних форматів логів; Нормалізує дані до формату IMDEF, що дає змогу легко передавати дані в інші системи безпеки.	Значно обмежена за функціональністю та продуктивністю порівняно з іншими open-source SIEM-системами.

5. Sagan

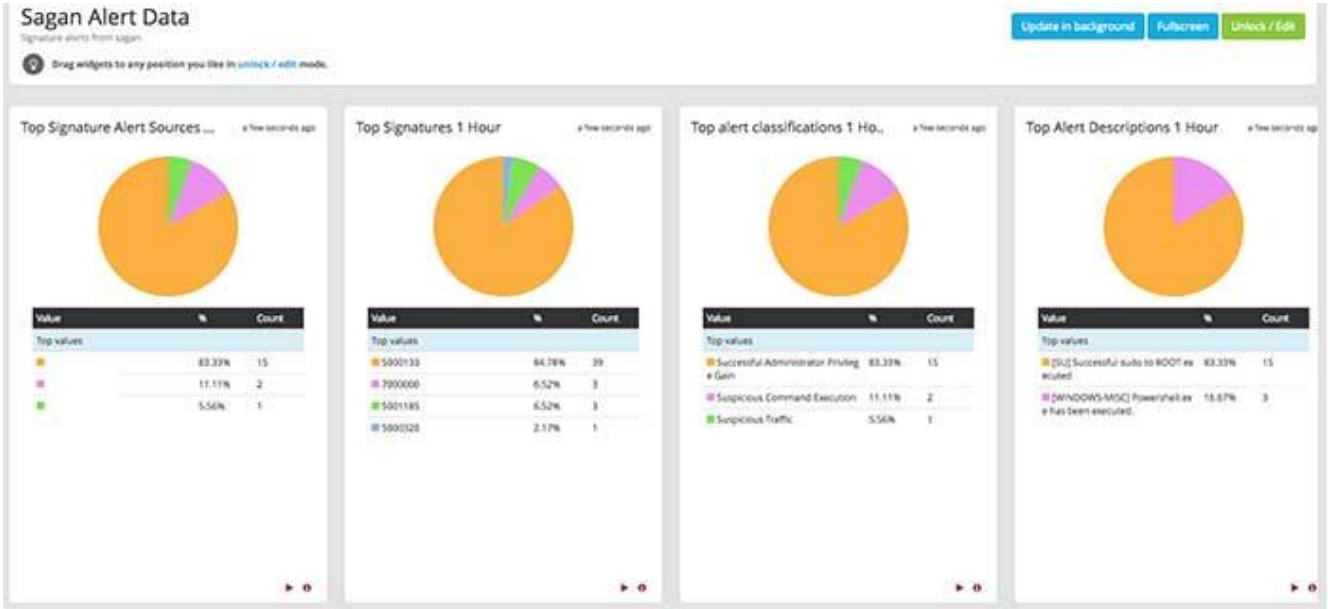

Рисунок 2.5 — Менеджер подій безпеки Sagan

Sagan - це високопродуктивна SIEM, яка підкреслює сумісність зі Snort. Крім підтримки правил, написаних для Snort, Sagan може виконувати запис у базу

даних Snort і навіть може використовуватися з інтерфейсом Shuil. По суті, це легке багатопотокове рішення, яке пропонує нові функції, залишаючись дружнім до користувачів Snort.

Переваги	**Недоліки**
Повністю сумісна з базою даних Snort, правилами, і призначеним для користувача інтерфейсом; Багатопотокова архітектура забезпечує високу продуктивність.	Порівняно новий проєкт із невеликою спільнотою; Складний процес інсталяції, що включає збірку всієї SIEM з вихідних кодів.

У кожної з описаних SIEM -систем є свої особливості та обмеження, тому їх не можна назвати універсальним рішенням для будь-якої організації. Однак у цих рішень відкритий код, що дає змогу розгортати, тестувати й оцінювати їх без надмірних витрат.

Висновок до розділу 2

В другому розділі було визначено, що кол-центр отримує, обробляє та зберігає велику кількість інформації, яку зловмисники можуть використати в подальшому, для вимагання грошей, зливу інформації в Інтернет та інші способи завдати шкоди людям.

Розібрали загальну структуру кол-центру, методи та способи проєктування підприємства.

Розглянули, проаналізували та вибрали програмне рішення для захисту, моніторингу та усуненню проблем в безпеці системи кол-центру. Проаналізувавши всі параиетри вибрали кращий варіант для застосування, було вибрано додаток Wazuh.

РОЗДІЛ 3. Практична реалізація та тестування спроєктованої системи

3.1 Аналіз обладнання та ПЗ мережі підприємства

Вибираючи мережеве обладнання чи пристрій готовий до живлення через Ethernet (PoE) чи підтримує він протокол передачі голосу через Інтернет (VoIP). Пристрої з повнодуплексними можливостями можуть передавати дані одночасно в обох напрямках і можуть бути стековими або монтованими в стійку. Такі функції продукту, як сигналізація та світлодіодні індикатори, надають звукові та візуальні сповіщення адміністраторам мережі.

Мережеве обладнання може бути розроблене або придатне для певних програм. Наприклад, загартовані продукти часто використовуються в телекомунікаційних додатках. Їхні корпуси забезпечують захист від погодних умов і можуть діяти як радіатор, відводячи високі температури від чутливих компонентів.

3.1.1 Комутатори

Комутатор зберігає обмежену інформацію про маршрутизацію вузлів у внутрішній мережі та дозволяє підключатись до таких систем, як концентратори або маршрутизатори. За допомогою комутаторів зазвичай з'єднуються гілки локальних мереж. Як правило, комутатори можуть зчитувати апаратні адреси вхідних пакетів для передачі їх за призначенням.

Використання комутаторів підвищує ефективність мережі в порівнянні з концентраторами або маршрутизаторами завдяки можливості створення віртуальних каналів. Комутатори також підвищують безпеку мережі, оскільки віртуальні ланцюги складніше досліджувати за допомогою мережевих моніторів. Ви можете думати про комутатор як про пристрій, який має деякі з кращих можливостей маршрутизаторів і концентраторів разом узятих. Комутатор може працювати як на канальному, так і на мережевому рівні моделі OSI. Багаторівневий комутатор - це комутатор, який може працювати на обох рівнях, тобто він може працювати і як комутатор, і як маршрутизатор. Багаторівневий

комутатор - це високопродуктивний пристрій, який підтримує ті ж протоколи маршрутизації, що і маршрутизатори.

Комутатори можуть піддаватися розподіленим атакам типу "відмова в обслуговуванні" (DDoS); для запобігання шкідливого трафіку, що призводить до зупинки роботи комутатора, використовуються засоби захисту від переповнення (flood guard). Безпека портів комутатора дуже важлива, тому обов'язково захищайте комутатори: Відключіть всі невикористовувані порти та використовуйте DHCP snooping, ARP інспекцію і фільтрацію MAC-адрес.

Під час побудови мережі кол-центру було використано комутатори моделі Cisco Catalyst Switch WS-C2960-48TC-L.

Рисунок 3.1 — Комутатор Cisco Catalyst Switch WS-C2960-48TC-L

3.1.2 Маршрутизатор

Маршрутизатори допомагають передавати пакети до місця призначення, прокладаючи шлях через море взаємопов'язаних мережевих пристроїв, що використовують різні мережеві топології. Маршрутизатори - це інтелектуальні пристрої, які зберігають інформацію про мережі, до яких вони підключені. Більшість маршрутизаторів можуть бути налаштовані на роботу в ролі брандмауерів з фільтрацією пакетів і використовувати списки контролю доступу (ACL). Маршрутизатори, в поєднанні з блоком обслуговування каналу/блоком обслуговування даних (CSU/DSU), також використовуються для переходу від кадрування локальної мережі до кадрування глобальної мережі. Це необхідно,

оскільки локальні та глобальні мережі використовують різні мережеві протоколи. Такі маршрутизатори відомі як прикордонні маршрутизатори. Вони служать зовнішнім з'єднанням локальної мережі з глобальною мережею і працюють на кордоні вашої мережі.

Маршрутизатори також використовуються для поділу внутрішніх мереж на дві або більше підмереж. Маршрутизатори також можуть бути підключені всередині до інших маршрутизаторів, створюючи зони, які працюють незалежно. Маршрутизатори встановлюють зв'язок, підтримуючи таблиці про пункти призначення та локальні з'єднання. Маршрутизатор містить інформацію про підключені до нього системи та про те, куди надсилати запити, якщо місце призначення невідоме. Маршрутизатори зазвичай передають інформацію про маршрутизацію та іншу інформацію, використовуючи один з трьох стандартних протоколів: Routing Information Protocol (RIP), Border Gateway Protocol (BGP) або Open Shortest Path First (OSPF).

Маршрутизатори є вашою першою лінією захисту, і вони повинні бути налаштовані на пропуск тільки того трафіку, який дозволений мережевими адміністраторами. Самі маршрути можуть бути налаштовані як статичні або динамічні. Якщо вони статичні, вони можуть бути налаштовані тільки вручну і залишаються такими до тих пір, поки не будуть змінені. Якщо вони динамічні, вони дізнаються про інші маршрутизатори навколо них і використовують інформацію про ці маршрутизатори для побудови своїх таблиць маршрутизації.

Під час побудови мережі кол-центру було використано маршрутизатори моделі Cisco 3700 Series Multiservice Access Router.

Рисунок 3.2 — Маршрутизатор Cisco 3700 Series Multiservice Access Router

3.1.3 Точка доступу

Хоча точка доступу (AP) технічно може містити в собі як дротове, так і бездротове з'єднання, вона зазвичай означає бездротовий пристрій. Точка доступу працює на другому рівні OSI, канальному рівні, і може працювати або як міст, що з'єднує стандартну дротову мережу з бездротовими пристроями, або як маршрутизатор, що передає дані від однієї точки доступу до іншої.

Для підключення до бездротової точки доступу потрібно ім'я ідентифікатора набору послуг (SSID). Бездротові мережі 802.11 використовують SSID для ідентифікації всіх систем, що належать до однієї мережі, і клієнтські станції повинні бути налаштовані з SSID, щоб пройти аутентифікацію в точці доступу. Точка доступу може транслювати SSID, дозволяючи всім бездротовим клієнтам в зоні бачити SSID точки доступу. Однак, з міркувань безпеки, точки доступу можуть бути налаштовані так, щоб не транслювати SSID, що означає, що адміністратор повинен надати клієнтським системам SSID замість того, щоб дозволити йому бути виявленим автоматично. Бездротові пристрої постачаються з SSID за замовчуванням, налаштуваннями безпеки, каналами, паролями та іменами користувачів. З міркувань безпеки настійно рекомендується змінити ці налаштування за замовчуванням якомога швидше, оскільки на багатьох інтернет-сайтах вказані налаштування за замовчуванням, що використовуються виробниками.

Точки доступу можуть бути товстими або тонкими. Товсті точки доступу, які іноді ще називають автономними точками доступу, потрібно вручну конфігурувати за допомогою мережевих налаштувань і налаштувань безпеки; потім вони, по суті, залишаються в спокої для обслуговування клієнтів до тих пір, поки вони не зможуть більше функціонувати. Тонкі точки доступу дозволяють віддалене налаштування за допомогою контролера. Оскільки тонкі клієнти не потрібно налаштовувати вручну, їх можна легко переналаштовувати та контролювати. Точки доступу також можуть бути на основі контролера або автономними.

Під час побудови мережі кол-центру було використано точку доступу, ноутбук Acer Extensa 15 EX215-22-R8RB.

Рисунок 3.3 — Ноутбук Acer Extensa 15 EX215-22-R8RB

3.1.4 Програмне забезпечення яке потрібно для функціонування кол-центру

Оскільки основною функцією кол-центру є здійснення та приймання дзвінків, правильна організація телефонії забезпечує якісний зв'язок та економію коштів. Sip-телефонія сьогодні вважається найкращим рішенням телефонії для контакт-центрів. Наразі вона є провідною, оскільки здатна забезпечити багатоканальний

зв'язок, високу якість та легке масштабування. Крім того, користуватися SIP-лініями можна в будь-якому місці, де є підключення до мережі Інтернет, тому географічних обмежень на використання номера практично немає. Слід відмовитися від аналогової телефонії, оскільки унікальне та складне масштабування значно знижує пропускну здатність та продуктивність вашого кол-центру. Цифрова телефонія (наприклад, E1) при власному впровадженні може задовольнити потреби сучасних кол-центрів, але є дорожчим варіантом. Для комунікації з колегами потрібна програма з максимальною захищеністю від зломів. Цю роль може виконувати Microsoft Teams. Програма з двофакторною автентифікацією в систему та захищеним кодом, який запобігає витоку інформації.

3.2 Налаштування системи захисту

Архітектура Wazuh базується на агентах, що працюють на контрольованих хостах, які пересилають дані журналу на центральний сервер. Крім того, підтримуються пристрої без агентів (такі як брандмауери, комутатори, маршрутизатори, точки доступу тощо), які можуть активно надсилати дані журналу через системний журнал або періодичне тестування змін їх конфігурації, щоб пізніше пересилати дані на центральний сервер. Центральний сервер декодує та аналізує вхідну інформацію та передає результати в кластер Elasticsearch для індексації та зберігання.

Багатовузлові кластери рекомендуються, коли існує велика кількість систем, що контролюються, коли очікується великий обсяг даних та/або коли потрібна висока доступність.

Коли сервер Wazuh і кластер Elasticsearch знаходяться на різних хостах, Filebeat використовується для безпечного пересилання сповіщень Wazuh та заархівованих подій на сервер Elasticsearch за допомогою шифрування TLS.

На наведеній нижче діаграмі показано, як розподіляються компоненти, коли сервер Wazuh і кластер Elasticsearch працюють на різних хостах.

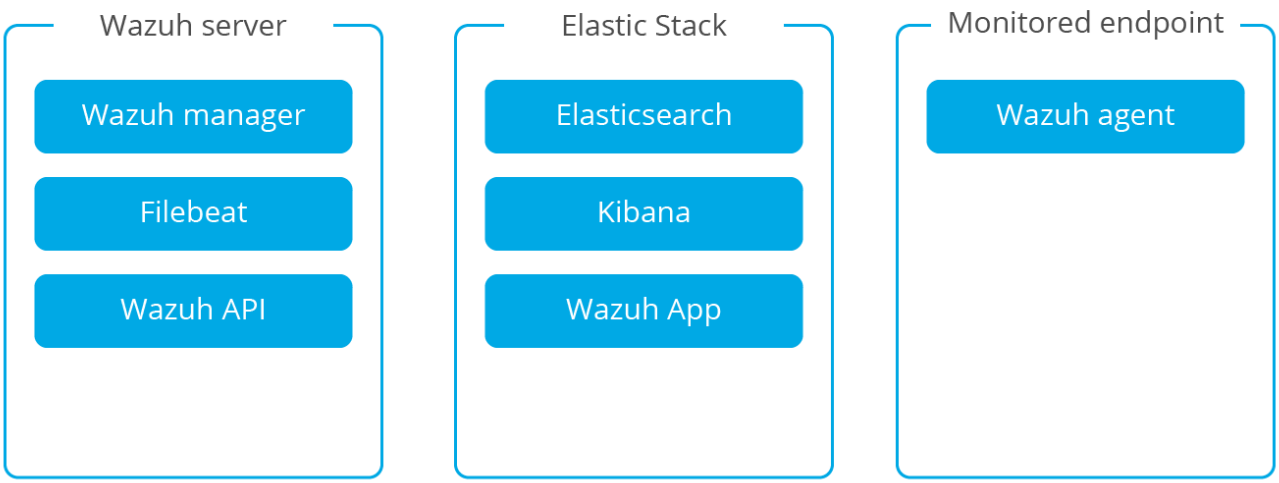

Рисунок 3.4 — Характеристика архітектури з кількома хостами

Для швидкого розгортання системи можна використати один з варіантів встановлення.

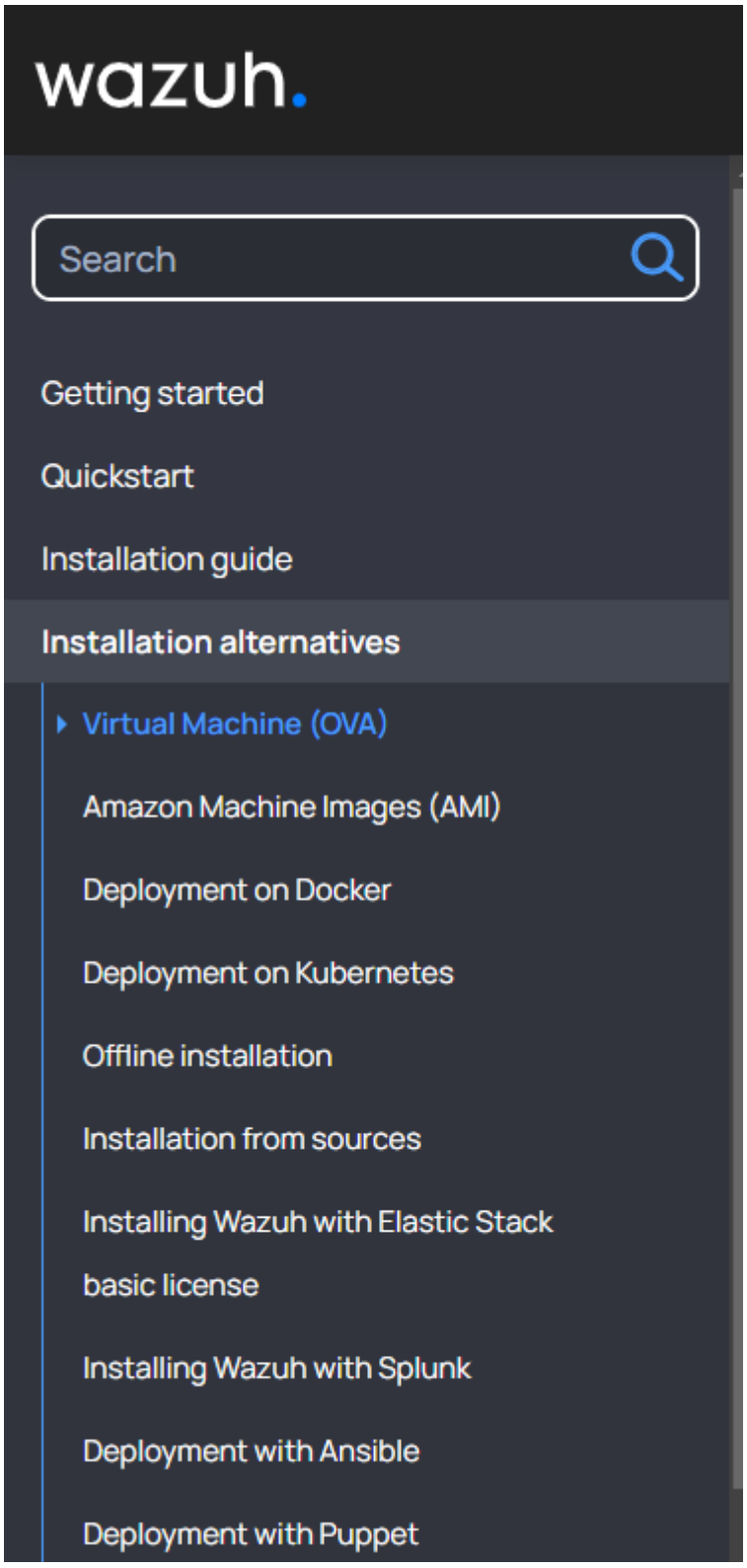

Рисунок 3.5 — Варіанти налаштування Wazuh server

В документації по розгортанню системи захисту Wazuh є багато варіантів по розгортанню системи захисту. Для розгортання мережі представленої в роботі підійде варіант з розгортанням образу віртуальної машини з всіма параметрами які вже налаштовані.

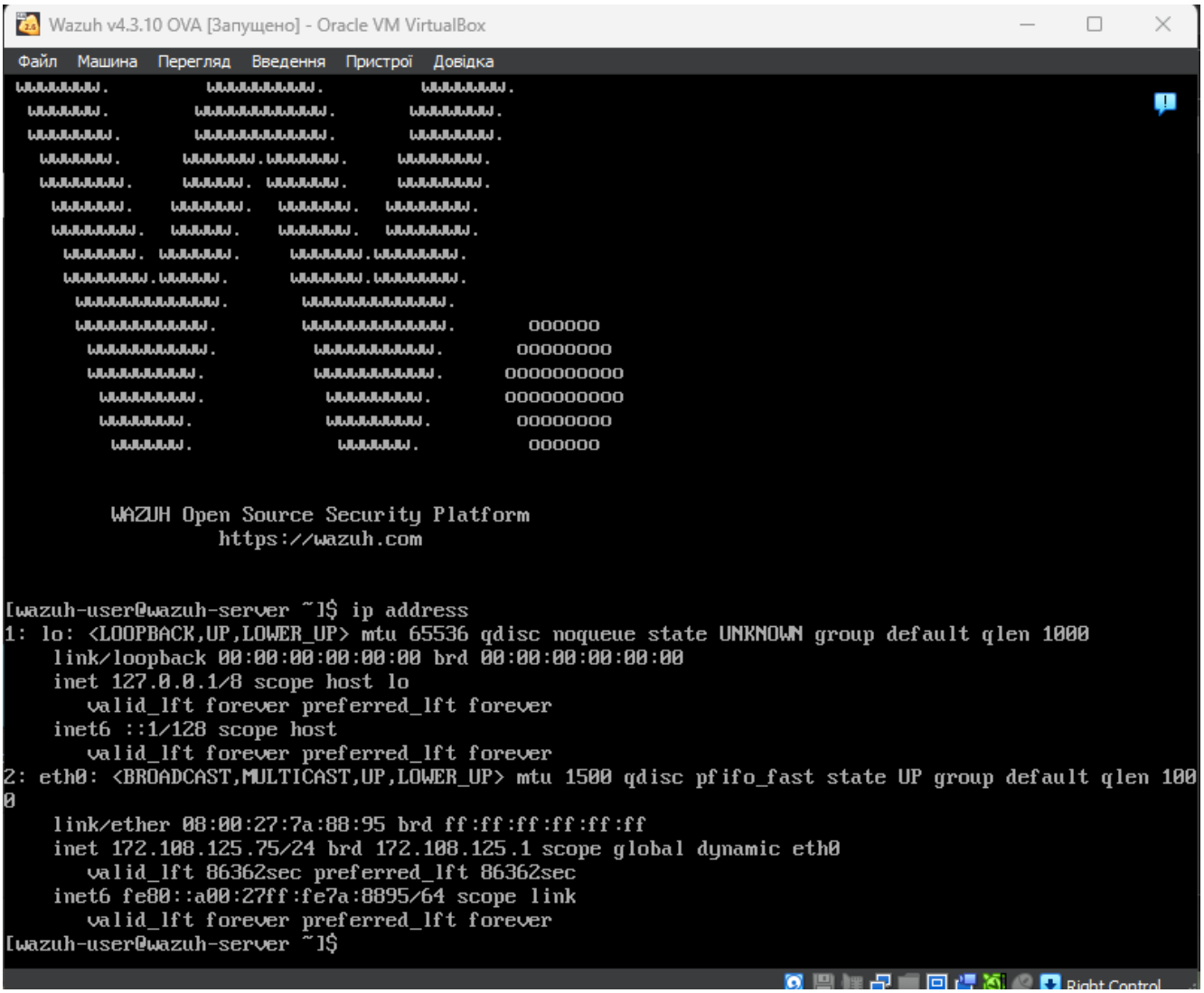

Рисунок 3.6 — Запуск Wazuh server

Для налаштування elastic stack можна використати ОС на базі Windows 11.

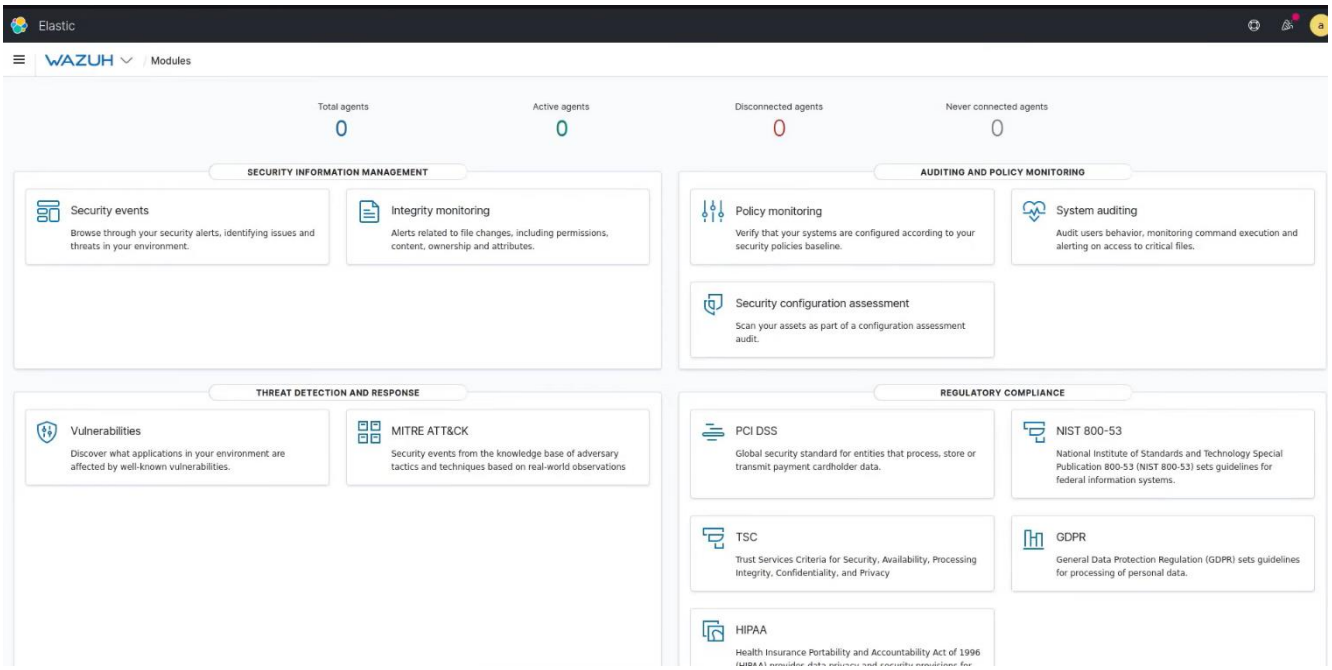

Рисунок 3.7 — Успішне підключення до сервера Wazuh

Після успішного підключення до сервера потрібно під'єднати Wazuh агент до кожної кінцевої точки мережі.

За допомогою Kibana додаємо інших користувачів.

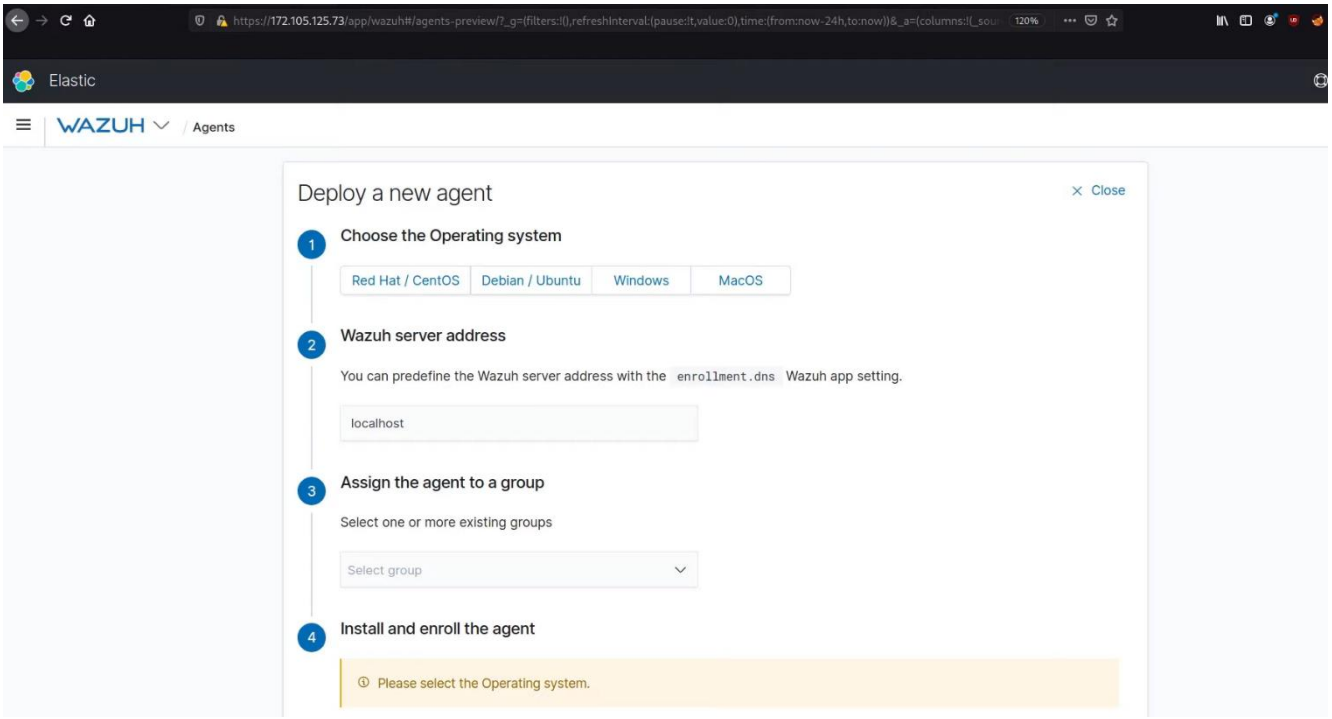

Рисунок 3.8 — Додавання нового користувача

На комп’ютері який буде підключений до системи Wazuh потрібно з офіційного сайту Wazuh звантажити «Агент Wazuh». За його допомогою комп’ютер з легкістю підключається до мережі захисту.

Рисунок 3.9 — Запущений Агент Wazuh

Як результат на комп'ютері адміністратора видно доданий комп'ютер.

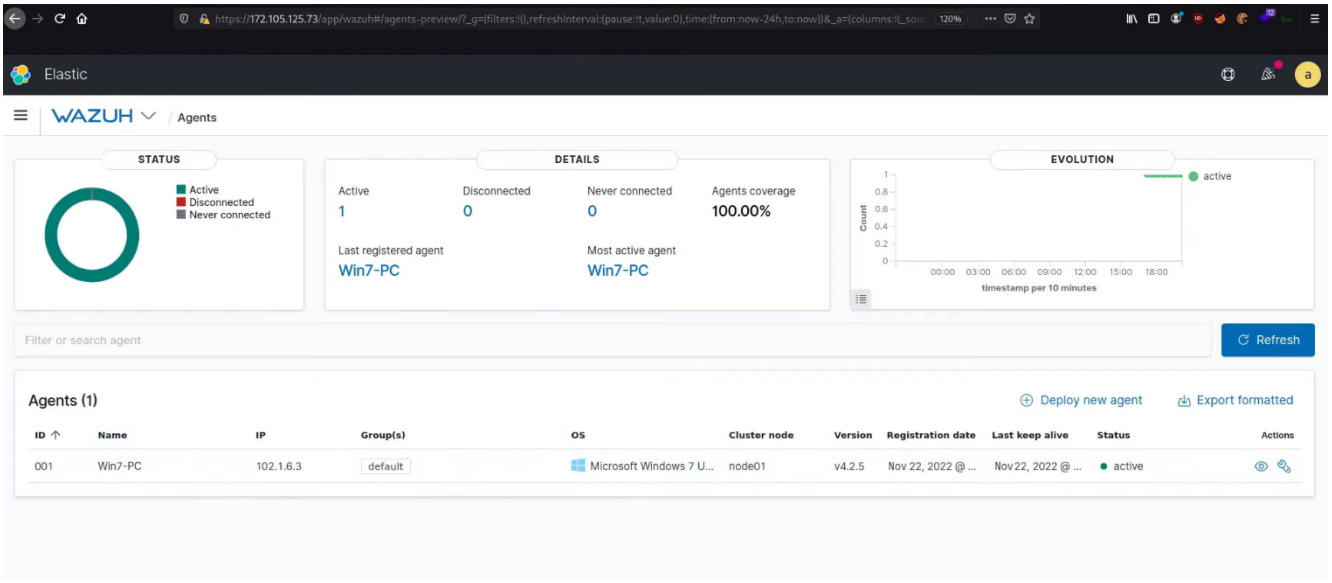

Рисунок 3.10 — Сторінка доданих агентів

3.3 Тестовий модельний приклад відпрацювання інциденту системою управління

Проводимо тестування на захищеність мережі.

Кіберзлочинець під'єднався до мережі кол-центру з намірами викрасти інформацію про клієнтів, співробітників та баз постачальників, які знаходяться на сервері. Доступ до сервера закритий, щоб до нього напряму під'єднатись.

Злочинець приєднався до офісу кол-центру.

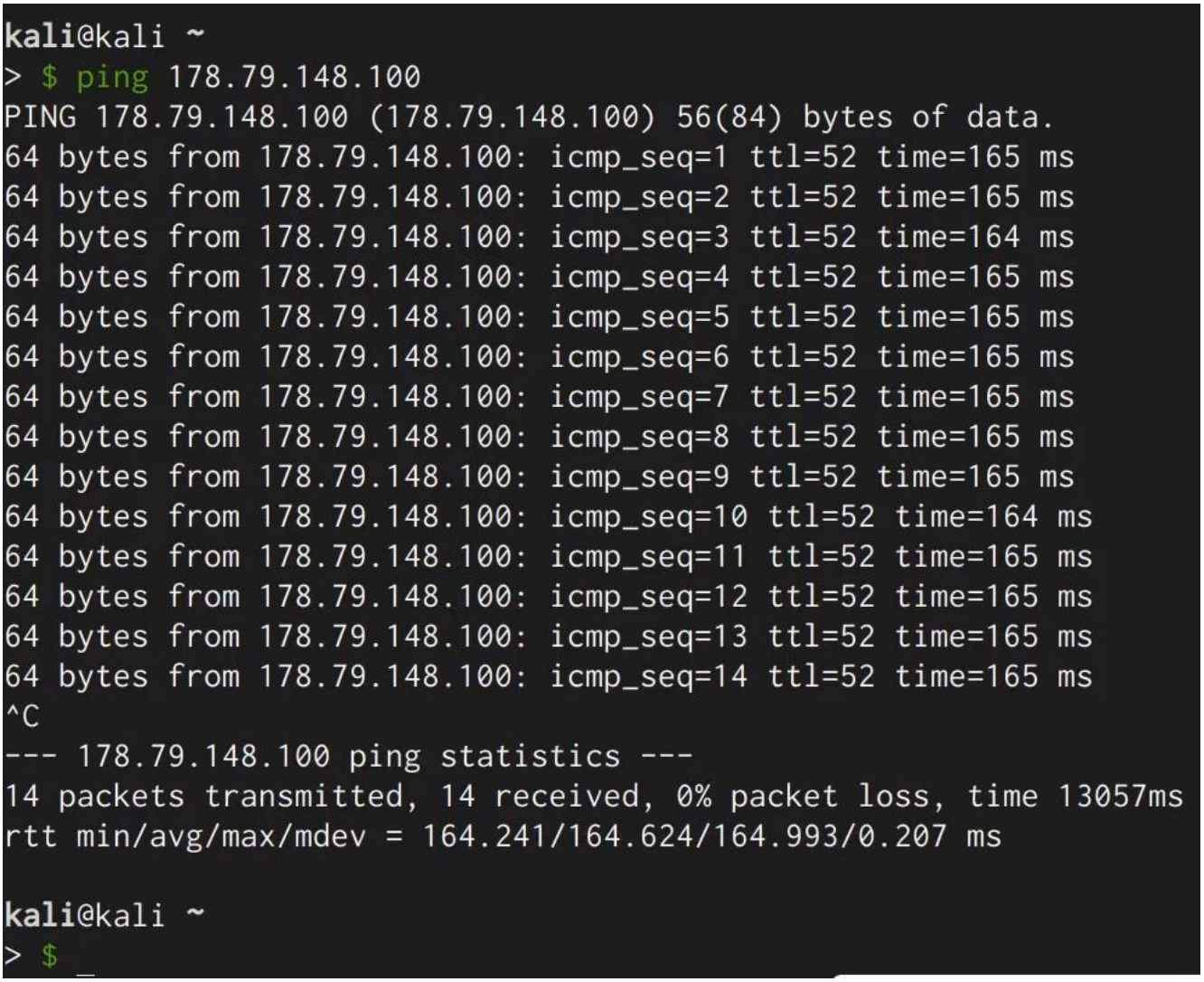

Рисунок 3.11 — Злочинець перевіряє з’єднання після підключення мережі кол-центру до сервера з даними

Після вдалої перевірки зв’язку між його комп’ютером та сервером, злочинець проводить спроби підключення до сервера. За допомогою утиліти ssh віддалено підключається до сервера, підбираючи паролі.

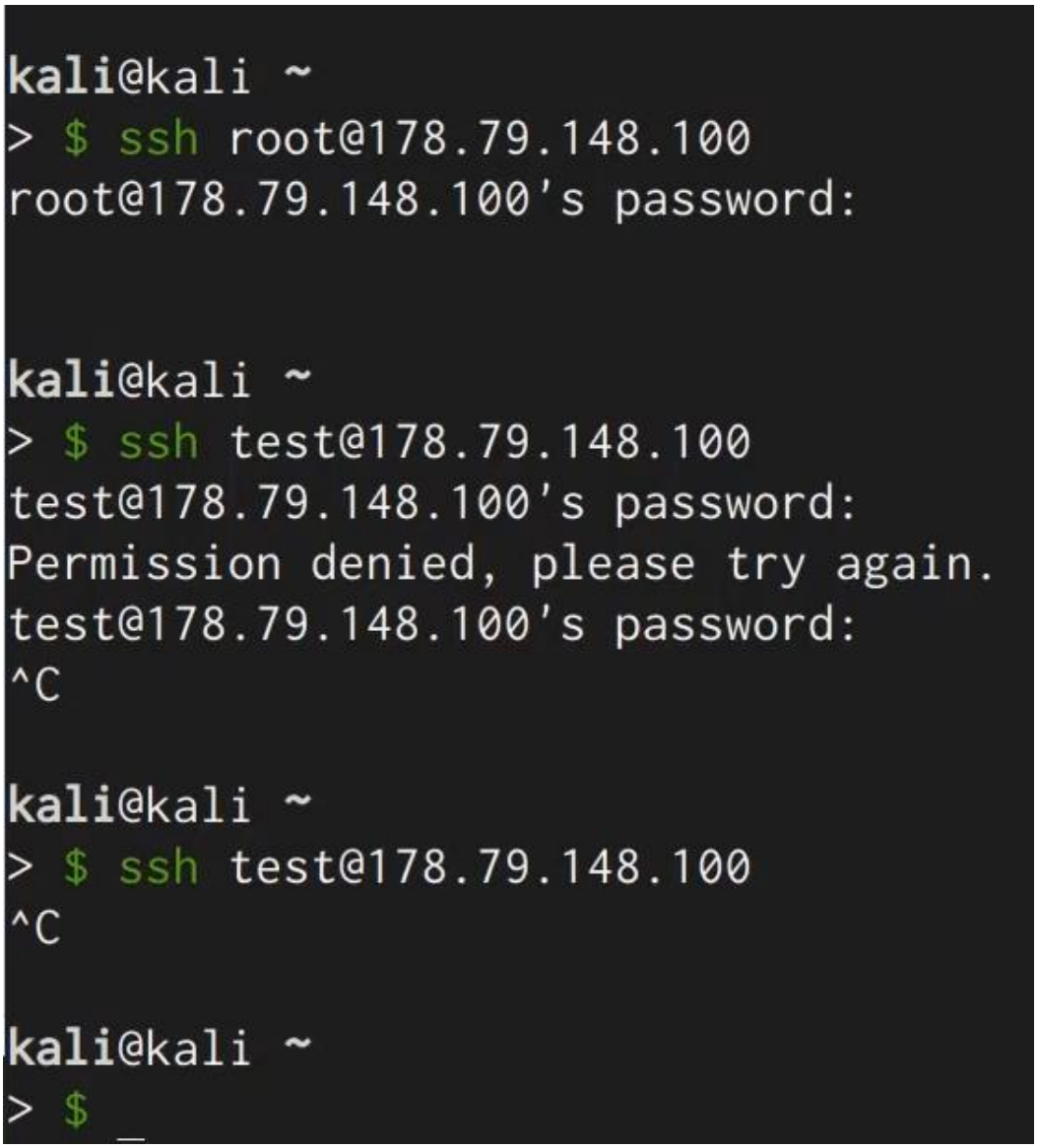

Рисунок 3.12 — Спроба приєднатись до сервера

Після невдалих спроб злочинця приєднатись до сервера в адміністратора системи видно повідомлення про те до сервера були спроби віддалено під'єднатися.

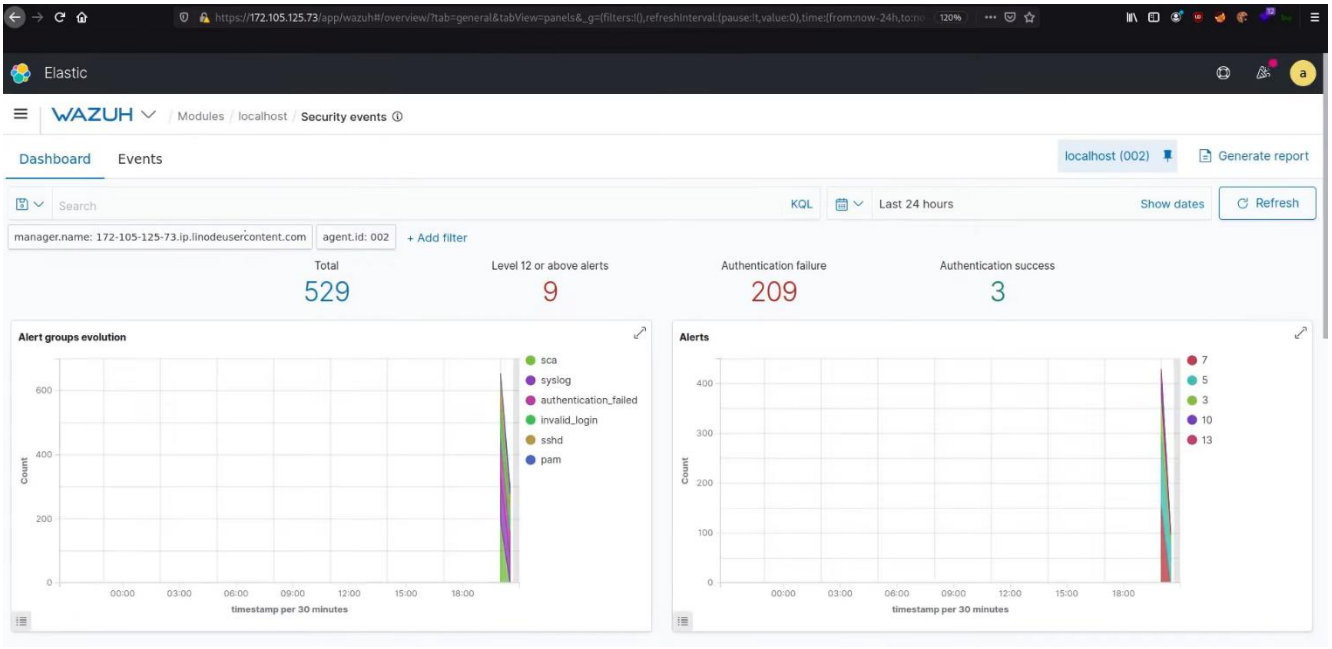

Рисунок 3.13 — Вікно менеджера подій Wazuh після спроби злому сервера

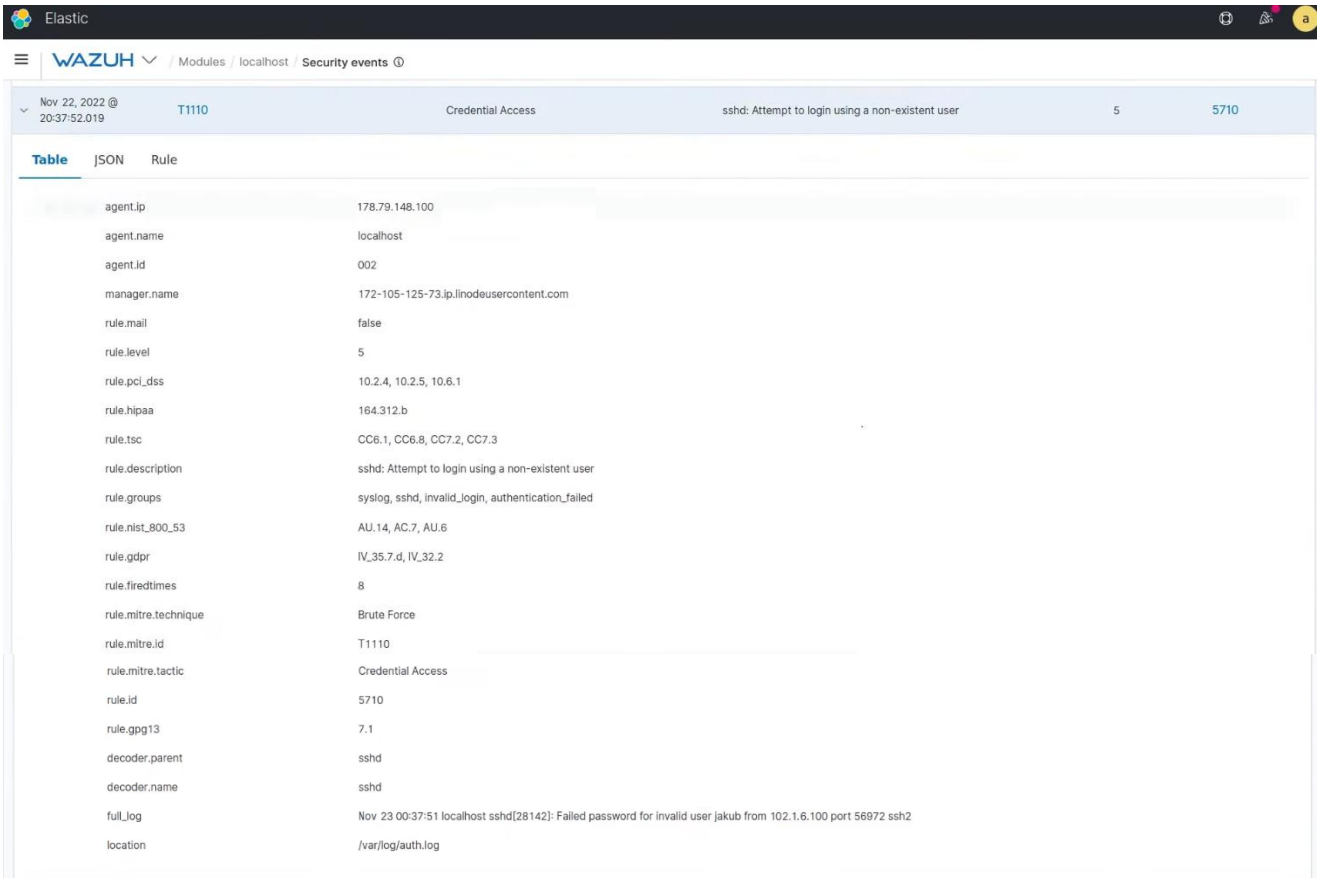

Рисунок 3.14 — Детальна інформація про подію

За допомогою додаткових параметрів можна додати параметр «Геолокація» і під час перегляду додаткової інформації про подію можна чітко побачити за координатами де знаходиться зловмисник.

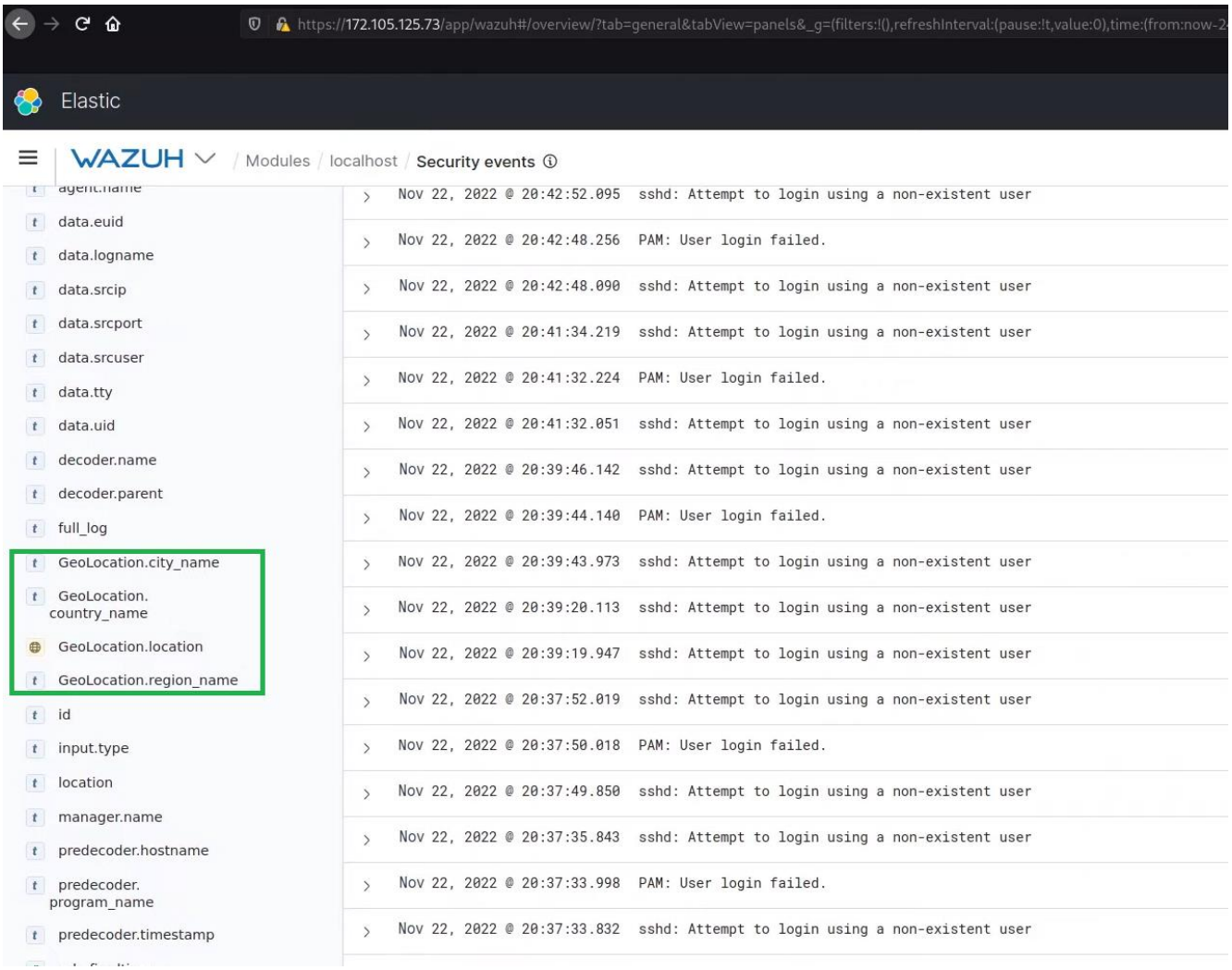

Рисунок 3.15 — Підключення додаткових параметрів «Геолокація»

Після підключення додаткових параметрів у звіті про подію можна побачити країну з якої відбулась кібератака та точні координати.

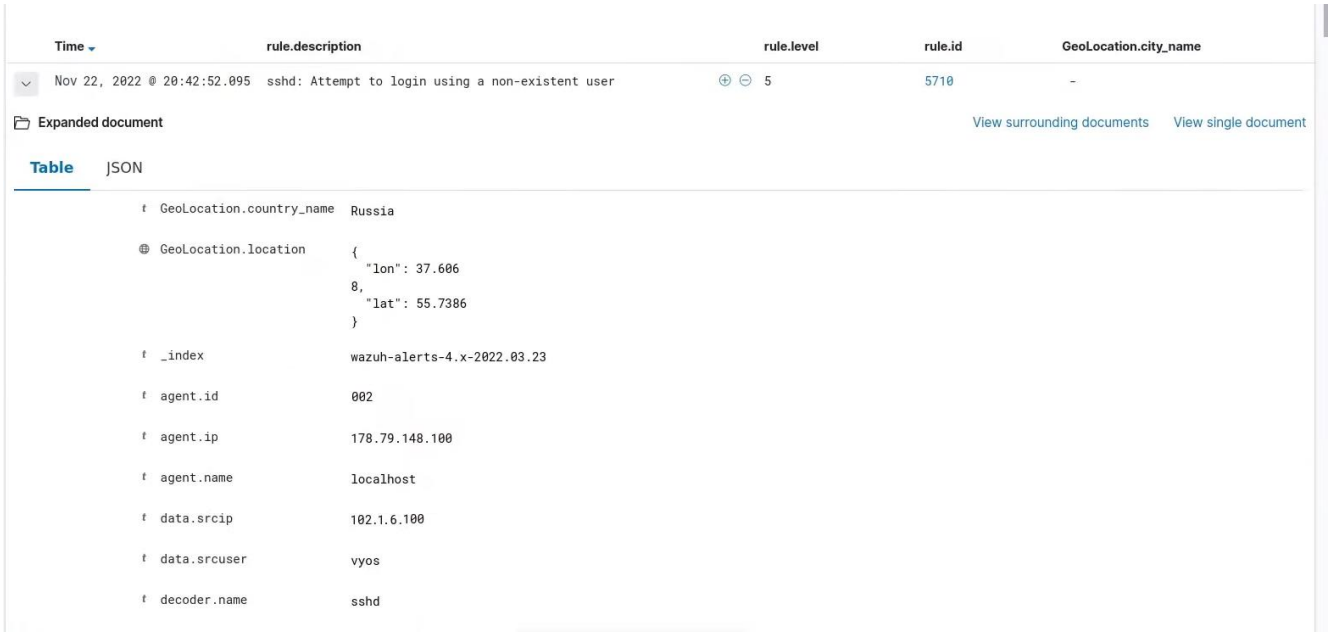

Рисунок 3.16 — Оновлена інформація про подію

Висновок до розділу 3

В розділі 3 проаналізували компоненти, які складають мережу кол-центру. Визначили яке програмне забезпечення потрібне для корректного функціонування кол-центру.

Підключення системи захисту за допомогою агента Wazuh до налаштованої мережі кол-центру. Перевірка функціонування системи захисту.

Провели тестування системи захист. Розглянули як вона діє в випадку атаки на сервер мережі. В результаті отримали позитивні результати на протидію атаки злочинця. За допомогою агента Wazuh можна отримати точне знаходження злочинця та всю інформацію про нього.

ВИСНОВКИ

Системи захисту постійно розвиваються й адаптуються до нових видів загроз. Кількість джерел інформації, з яких надходять дані щодо поточного стану захищеності, зростає з кожним днем.

ІТ-інфраструктура сучасного підприємства відрізняється високою складністю та різноманітністю. Системи захисту постійно розвиваються і адаптуються до нових видів загроз. При цьому кількість джерел, з яких надходять інформація щодо поточного стану захищеності, безперервно зростає. Адміністраторам інформаційної безпеки все складніше стежити за загальною картиною того, що відбувається. Адже, якщо своєчасно не аналізувати загрози, що виникають, і не намагатися запобігти їх, будь-яка система захисту виявиться марною. У умовах хорошу послугу нададуть системи класу Security Information and Event Management (SIEM) .

У переносному сенсі можна сказати, що продукти SIEM призначені для пошуку голки в стозі сіна. Тобто, серед багатьох записів у системних журналах SIEM-рішення виявляє сліди деяких підозрілих дій.

SIEM- система не лише автоматизує аналіз різних системних подій. Важливо, що з її допомогою можна виявити дії, які зовні виглядають цілком звичайними, але в сукупності є загрозою. Наприклад, якщо довірений користувач надсилає конфіденційні дані на email-адресу, яка лежить поза звичайним колом адресатів, то DLP-система не завжди відловлює такі дії, проте SIEM згенерує інцидент на базі накопиченої статистики.

Діапазон завдань, які здатна вирішити SIEM-система, справді дуже широкий. По-перше, про що вже згадувалося раніше, це автоматизація моніторингу та аналізу всіх подій, що відбуваються у численних системах захисту. Друге важливе завдання, мети, заради якої використовуються SIEM-технології: у разі інциденту SIEM здатна надати всю необхідну доказову базу, придатну як для внутрішніх розслідувань, так і для суду. Третє важливе призначення – SIEM допомагає проводити аудити на відповідність різним галузевим стандартам.

Варто зазначити, що SIEM можна назвати інструментом не тільки відділу ІБ, а й ІТ-департаменту загалом. Адже завдяки потужним кореляційним механізмам з'являється можливість забезпечувати безперервність роботи ІТ-сервісів, виявляти збої у роботі інформаційних та операційних систем та апаратного забезпечення. Тим самим можна забезпечити безперервність бізнесу в цілому. Простий приклад, актуальний більшості корпоративних мереж: конфлікт IP-адрес. За рахунок найпростішого правила можна дізнатися про інцидент задовго до дзвінка користувача. При цьому усунення причини потребує набагато менше часу, а отже, зменшуються можливі фінансові втрати бізнесу.

Для збирання даних SIEM-системи використовують кілька різних компонентів. Серед них: агенти, що встановлюються на інформаційну систему, що інспектується; колектори на агентах, призначених для «розуміння» конкретного журналу подій чи системи; сервери-колектори, що попередньо акумулюють події від безлічі джерел; сервер баз даних та сховища, що відповідає за зберігання журналів подій.

Крім того, дані про події збираються не тільки за допомогою встановлених на джерелах агентах, але й віддалено за допомогою з'єднання за протоколами NetBIOS, RPC, TFTP, FTP. Однак у цьому випадку виникає значне навантаження на мережу і саме джерело, оскільки деякі системи не можуть передати тільки ту частину журналу подій, який ще не був переданий, а відправляють у бік SIEM весь лог, що нерідко становить сотні мегабайт.

Необхідно відзначити, що довгий час SIEM-системи були доступні лише для великих підприємств із значним ІТ-бюджетом. Проте останніми роками з'явилися «коробкові» SIEM-системи класу all-in-one. У таких рішеннях механізми збирання, зберігання, пошуку, нормалізації та кореляції інформації реалізовані у межах одного цільного продукту. Такі продукти, як HP ArcSight express, Tibco Loglogic MX, McAfee Nitro ESM, QRadar 2100 All-In-One Appliance, надають функціональність SIEM, виходячи з потреб невеликих та середніх за величиною компаній.

За допомогою SIEM можна досягти майже абсолютної автоматизації процесу виявлення загроз. При коректному впровадженні такої системи підрозділ ІБ переходить абсолютно новий рівень надання сервісу. SIEM дозволяє акцентувати увагу лише на критичних і справді важливих загрозах, працювати не з подіями, а з інцидентами, своєчасно виявляти аномалії та ризики, запобігати фінансовим втратам.

Якщо аналізувати реальне використання SIEM на практиці, доводиться визнати, що у більшості випадків робота таких систем спрямована на консолідацію журналів подій від різних джерел. Фактично – використовується лише функціонал SIM. Якщо є задані правила кореляції, вони поповнюються.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber security incident management guide. – [S. l.] : The CCB and Cyber Security Coalition, 2021. – 38 p.
2. Computer security incident handling guide / Paul Cichonski [et al.]. – 2nd ed. – [S. l.] : National Institute of Standards and Technology, 2012. – 79 p.
3. Good practice guide for incident management. – 27th ed. – [S. l.] : ENISA, 2010. – 110 p.
4. Матендж Дж. Incident management: the complete guide / Джозеф Матендж. – [S. l.] : BMC, 2021.
5. Актуальные киберугрозы: II квартал 2022 года [Електронний ресурс] // https://www.ptsecurity.com/. – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/ (дата звернення: 04.12.2022). – Назва з екрана.
6. ENISA threat landscape 2022 / Claudio Ardagna [et al.]. – [S. l.] : ENISA, 2022. – 150 p.
7. Six steps for building a robust incident response strategy [Electronic resource] // https://www.ibm.com. – Mode of access: https://www.ibm.com/security/digital-assets/soar/six-steps-for-incident-response/ (date of access: 06.12.2022). – Title from screen.
8. Incident response [Electronic resource] // https://cyberlum.io/. – Mode of access: https://cyberlum.io/incident-response/ (date of access: 08.12.2022). – Title from screen.
9. Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. / Ю. Лісовська. – Київ : Кондор, 2019. – 272 с.
10. Колощук М. Види інструментів та програмного забезпечення для використання системи siem / Марія Колощук // Тези Всеукраїнської науково-практичної on-line конференції здобувачів вищої освіти і

молодих учених, присвяченої Дню науки : сеукр. науково-практ. on-line конф., Житомир, 16–26 трав. 2022 р. – Житомир, 2022. – С. 79.

11. Колощук М. Універсальний інструмент інформаційної безпеки – система siem / Марія Колощук // Комп'ютерні технології: інновації, проблеми, рішення : Всеукр. науково-техн. конф., Житомир, 1–2 груд. 2022 р. – Житомир, 2022.
12. Borkar P. Incident response: 6 steps, technologies, and tips [Electronic resource] / Pramod Borkar // https://www.exabeam.com/. – Mode of access: https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/ (date of access: 07.12.2022). – Title from screen.
13. Installation guide [Electronic resource] // Wazuh documentation. – Mode of access: https://documentation.wazuh.com/3.8/installation-guide/index.html (date of access: 17.12.2022). – Title from screen.
14. Wazuh · the open source security platform [Electronic resource] // Wazuh. – Mode of access: https://wazuh.com/ (date of access: 09.12.2022). – Title from screen.
15. Ноутбук acer extensa 15 EX215-22-R766 NX.EG9EU.00Z black [Електронний ресурс] // Інтернет-магазин КТС. – Режим доступу: https://ktc.ua/goods/noutbuk_acer_nx_eg9eu_00z.html (дата звернення: 15.12.2022). – Назва з екрана.
16. Network devices explained [Electronic resource] // Netwrix Blog | Insights for Cybersecurity and IT Pros. – Mode of access: https://blog.netwrix.com/2019/01/08/network-devices-explained/ (date of access: 01.12.2022). – Title from screen.
17. Яке обладнання необхідне для call центру? | Voiptime | VoIPTime [Електронний ресурс] // VoIPTime |. – Режим доступу: https://www.voiptime.net/uk/what-computer-to-choose-for-call-center-agent_uk.html#Telefonia_v_call-centri (дата звернення: 08.12.2022). – Назва з екрана.

18. Risk management [Electronic resource] // NCSC. – Mode of access: https://www.ncsc.gov.uk/collection/10-steps/risk-management (date of access: 02.12.2022). – Title from screen.
19. CISCO3745-2 cisco 3700 series multiservice access router [Electronic resource] // https://www.priceblaze.com/. – Mode of access: https://www.priceblaze.com/CISCO37452-Cisco-Network-Router?srsltid=AeTuncoHDKKQxeiPv1Q0b4FEexV40PvdBEOAgpi_H7hUPrdkccxhatHLYfE (date of access: 01.12.2022). – Title from screen.
20. What are the 7 phases of incident response? | RSI security [Electronic resource] // RSI Security. – Mode of access: https://blog.rsisecurity.com/what-are-the-7-phases-of-incident-response/ (date of access: 26.11.2022). – Title from screen.
21. OSSIM: The Open Source SIEM | AlienVault [Електронний ресурс] // AlienVault is now AT&T Cybersecurity. – Режим доступу: https://cybersecurity.att.com/products/ossim (дата звернення: 29.11.2022). – Назва з екрана.
22. Overview – mozilla enterprise defense platform documentation [Електронний ресурс] // Table of Contents – Mozilla Enterprise Defense Platform documentation. – Режим доступу: https://mozdef.readthedocs.io/en/latest/overview.html (дата звернення: 29.11.2022). – Назва з екрана.
23. Overview - PRELUDE SIEM - UNITY 360 [Електронний ресурс] // Overview - PRELUDE SIEM - UNITY 360. – Режим доступу: https://www.prelude-siem.org/ (дата звернення: 29.11.2022). – Назва з екрана.
24. Sagan User Guide – Sagan User Guide 1.2.2 documentation [Електронний ресурс] // Sagan User Guide – Sagan User Guide 1.2.2 documentation. – Режим доступу: https://sagan.readthedocs.io/en/latest/ (дата звернення: 29.11.2022). – Назва з екрана.

ДОДАТКИ

ДОДАТОК А

Розроблений мережевий проект

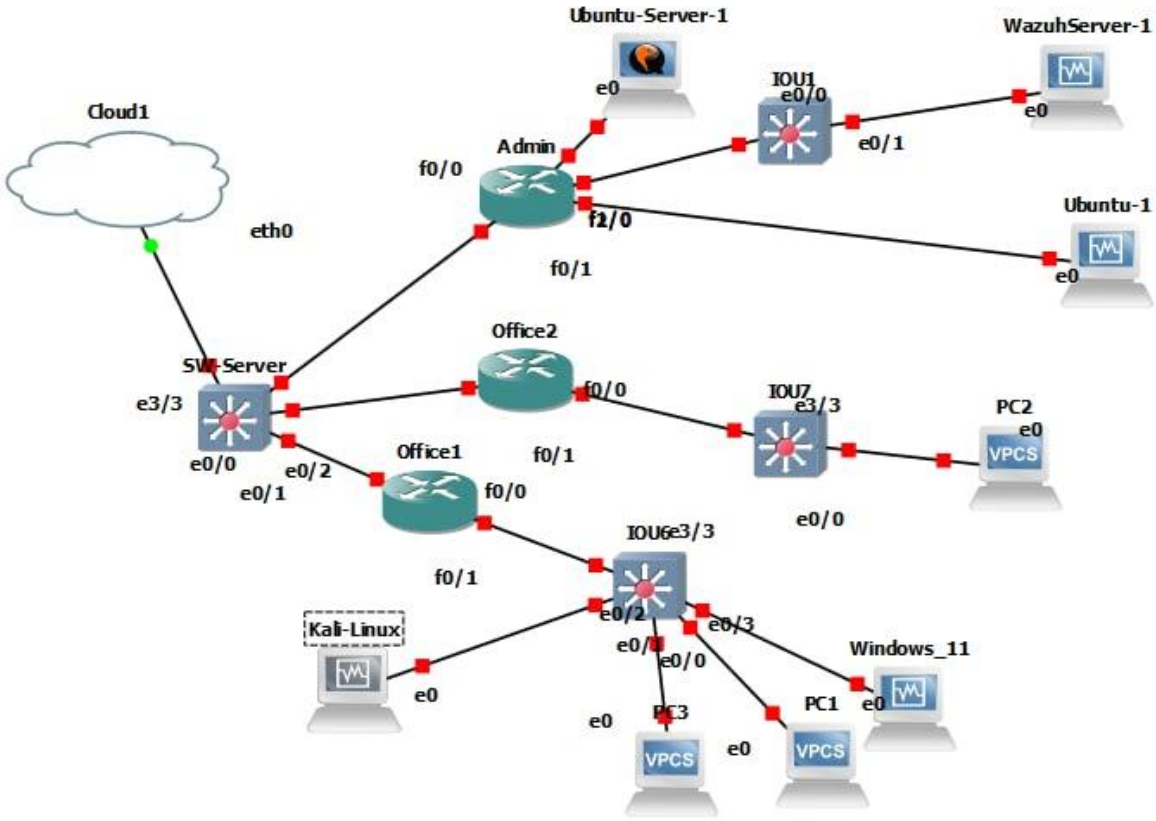

Рисунок 1 — Розроблена мережа кол-центру

ДОДАТОК Б

Адресація підмереж

Підмережа	IP-адреса	Маска мережі	Шлюз по замовчуванню
Підмережа A	101.1.8.0	255.255.255.224	101.1.8.1
Підмережа B	102.2.8.0	255.255.255.0	102.2.8.1
Підмережа C	103.3.8.0	255.255.255.0	103.3.8.1
Підмережа D	104.4.8.0	255.255.255.0	104.4.8.1
Підмережа E	172.105.105.0	255.255.255.0	172.105.105.1
Підмережа F	178.79.148.0	255.255.255.0	178.79.148.1

ДОДАТОК В

Конфігураційні файли пристроїв мережі

Конфігураційний файл маршрутизатора Office1

```
Office1(config)#do copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
OFFICE1(config)#do show run
Building configuration...

Current configuration : 2441 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Office1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$HXVE$SWTYY55sys36VaUBEQDzH1
!
aaa new-model
aaa local authentication attempts max-fail 6
!
!
aaa authentication login default local
!
aaa session-id common
memory-size iomem 5
clock timezone EET 2
clock summer-time zone recurring
no ip icmp rate-limit unreachable
ip cef
!
!
no ip dhcp use vrf connected
!
ip dhcp pool Office1
  network 102.1.6.0 255.255.255.0
  default-router 102.1.6.1
  domain-name office1.com
  dns-server 8.8.8.8 8.8.4.4
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin password 7 08316C5D1A0E5505164B1C16233D2D24363227535643
username nick password 7 08316C5D1A370C14194B1C16233D2D243632275356
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
 ip address 101.1.6.1 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 102.1.6.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
```

```
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
router rip
 version 2
 network 101.0.0.0
 network 102.0.0.0
 network 172.0.0.0
 network 178.0.0.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
no cdp run
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 140732181F137A3920
 logging synchronous
line aux 0
 exec-timeout 0 1
 privilege level 15
 logging synchronous
 no exec
 transport output none
line vty 0 4
 access-class 10 in
 access-class 11 out
 exec-timeout 2 0
 password 7 140732181F137A3920
 logout-warning 30
 absolute-timeout 10
 transport input telnet
 transport output telnet
line vty 5 15
 access-class 10 in
 access-class 11 out
 exec-timeout 2 0
 password 7 095C6E1A0A1247000F
 logout-warning 30
 absolute-timeout 10
 transport input telnet
 transport output telnet
!
!
End
```

Конфігураційний файл маршрутизатора Office2

```
Office2 (config)#do copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
Office2(config)#do show conf
Using 2441 out of 155640 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Office2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$DSR5$4eG0TkQxniVbm6BBrneyB/
!
aaa new-model
aaa local authentication attempts max-fail 6
!
!
aaa authentication login default local
!
aaa session-id common
memory-size iomem 5
clock timezone EET 2
clock summer-time zone recurring
no ip icmp rate-limit unreachable
ip cef
!
!
no ip dhcp use vrf connected
!
ip dhcp pool Office2
  network 103.1.6.0 255.255.255.0
  default-router 103.1.6.1
  domain-name office2.com
  dns-server 8.8.8.8 8.8.4.4
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin password 7 00143315174C5B140B615C5C000F0C1B170C09447B7E
username nick password 7 140732181F2A23282F6823272B050E1A0606531909
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
 ip address 101.1.6.2 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 103.1.6.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
router rip
 version 2
 network 101.0.0.0
 network 103.0.0.0
 network 172.0.0.0
 network 178.0.0.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
no cdp run
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 00143315174C5B140B
 logging synchronous
line aux 0
 exec-timeout 0 1
 privilege level 15
 logging synchronous
 no exec
 transport output none
line vty 0 4
 access-class 10 in
 access-class 11 out
 exec-timeout 2 0
 password 7 140732181F137A3920
 logout-warning 30
 absolute-timeout 10
 transport input telnet
 transport output telnet
line vty 5 15
 access-class 10 in
 access-class 11 out
 exec-timeout 2 0
 password 7 140732181F137A3920
 logout-warning 30
 absolute-timeout 10
 transport input telnet
 transport output telnet
!
!
End
```

Конфігураційний файл маршрутизатора Admin

```
Admin(config)#do show conf
Using 2441 out of 155640 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Admin
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$qv6/$iFb3u.WyJ0EazXEUIqJOB/
!
aaa new-model
aaa local authentication attempts max-fail 6
!
!
aaa authentication login default local
!
aaa session-id common
memory-size iomem 5
clock timezone EET 2
clock summer-time zone recurring
no ip icmp rate-limit unreachable
ip cef
!
!
no ip dhcp use vrf connected
!
ip dhcp pool Office3
  network 104.1.6.0 255.255.255.0
  default-router 104.1.6.1
  domain-name office3.com
  dns-server 8.8.8.8 8.8.4.4
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin password 7 095C6E1A0A1247000F4C14382232213F302516474756
username nick password 7 071F015F5D2710061C521B1E0D3C22282D34306242
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
 ip address 101.1.6.3 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.105.125.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 178.79.148.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
router rip
 version 2
 network 101.0.0.0
 network 104.0.0.0
 network 172.0.0.0
 network 178.0.0.0

 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
no cdp run
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 044B2B151C361C5C0D
 logging synchronous
line aux 0
 exec-timeout 0 1
 privilege level 15
 logging synchronous
 no exec
 transport output none
line vty 0 4
 access-class 10 in
 access-class 11 out
 exec-timeout 2 0
 password 7 071F015F5D1E491713
 logout-warning 30
 absolute-timeout 10
 transport input telnet
 transport output telnet
line vty 5 15
 access-class 10 in
 access-class 11 out
 exec-timeout 2 0
 password 7 071F015F5D1E491713
 logout-warning 30
 absolute-timeout 10
 transport input telnet
 transport output telnet
!
!
end
```

ДОДАТОК Г

Перевірка з’єднання між мережами

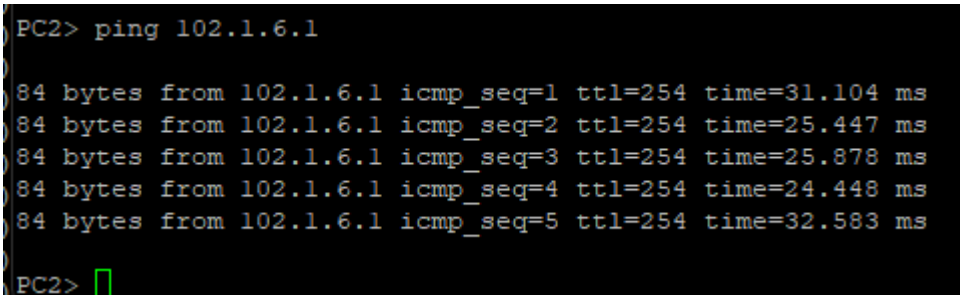

Рисунок 2 — Перевірка з’єднання між Office1 та Office2