

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

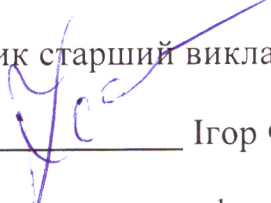
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра на
тему: «Проект SIEM-підсистеми для SOC на базі
рішення AlienVault OSSIM»

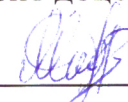
Виконав студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»

 Володимир ІОННІКОВ

Керівник старший викладач кафедри КІ та КБ

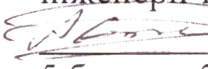
 Ігор ФАЛЬКОВСЬКИЙ

Рецензент доцент кафедри КІ та КБ, к.т.н.

 Олександр МАЄВСЬКИЙ

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Іонніков Володимир Миколайович

Тема роботи: «Проект SIEM-підсистеми для SOC на базі рішення AlienVault OSSIM»

затверджена Наказом університету від 5 березня 2024 р. № 98/с

Термін здачі студентом закінченої роботи 29 червня 2024 р.

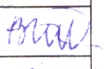
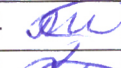
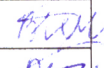
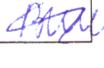
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

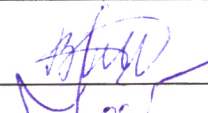
- Топологія мережі.
- Проект локальної мережі.
- Використання безкоштовного рішення AlienVault OSSIM.

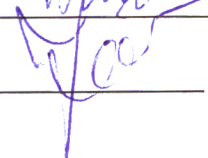
Обладнання та програмне забезпечення:

1. ОС Windows Server 2019 Standard (v.1809)
2. ОС Windows 10 (v.1909)
3. Мережевий емулятор GNS3 (v.2.2.46)
4. Гіпервізор Oracle VirtualBox (v.7.0.14)
5. SIEM – AlienVault OSSIM (v.5.8.11)

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

Розділ	Консультант	Дата	
		Завдання видав	Завдання прийняв
1	Головня О.С.	05.03.2024 	05.03.2024 
2	Головня О.С.	05.03.2024 	05.03.2024 
3	Головня О.С.	05.03.2024 	05.03.2024 

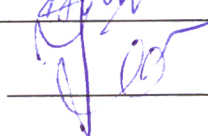
Студент  Володимир ІОННІКОВ

Керівник  Ігор ФАЛЬКОВСЬКИЙ

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітки
1	Постановка завдання	05.03.2024 – 05.03.2024	Виконано
2	Аналіз теоретичних аспектів SIEM	06.03.2024 – 15.03.2024	Виконано
3	Аналіз існуючих безкоштовних рішень SIEM	16.03.2024 – 22.03.2024	Виконано
4	Дослідження використання AlienVault OSSIM	23.03.2024 – 30.03.2024	Виконано
5	Проектування фізичної і логічної топології мережі проєкту	31.03.2024 – 04.04.2024	Виконано
6	Розробка схеми IP-адресації	05.04.2024 – 09.04.2024	Виконано
7	Проектування системи SIEM	10.04.2024 – 17.04.2024	Виконано
8	Вибір мережевого обладнання і визначення системних вимог	18.04.2024 – 22.04.2024	Виконано
9	Налагодження пристроїв мережі і OSSIM	23.04.2024 – 13.05.2024	Виконано
10	Тестування функціонування мережі та підсистеми SIEM	14.05.2024 – 20.05.2024	Виконано
11	Написання пояснювальної записки	20.05.2024 – 21.06.2024	Виконано
12	Захист	29.06.2024	Виконано

Студент  Володимир ІОННІКОВ

Керівник  Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки до курсового проєкту, яка складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 82 сторінках друкованого тексту. Пояснювальна записка має 6 додатків розміщених на 12 сторінках. Список використаних джерел містить 20 найменувань і займає 2 сторінки. В роботі наведено 70 рисунків та 3 таблиці. Загальний обсяг роботи – 94 сторінок.

Метою роботи є розробка проєкту SIEM-підсистеми для SOC на базі рішення AlienVault OSSIM

В роботі було розглянуто основні принципи роботи, призначення та ключові функціональні можливості SIEM. Визначено рекомендації та сучасні тенденції розвитку SIEM. Проведено огляд безкоштовних SIEM-рішень за підсумком якого визначено, що AlienVault OSSIM є збалансованим рішенням і буде в подальшому використаний для організації SIEM-підсистеми для SOC в проєкті мережі. Розроблено логічну і фізичну топології мережі, визначено кількість пристроїв, розроблено схему адресації, проведено проєктування роботи системи SIEM. Обґрунтовано вибір необхідних моделей пристроїв для мережі, зазначено їх мінімальні системні. Виконано проєктування проєкту мережі в мережевому емуляторі GNS3 з використанням гіпервізора VirtualBox. Описано процес налагодження пристроїв та AlienVault OSSIM в ролі SIEM-підсистеми. Результат роботи протестований та відповідає поставленим вимогам.

Ключові слова: МЕРЕЖА, ПРОЄКТ, БЕЗПЕКА, ЗАХИСТ, ПОДІЇ, SIEM, ALIENVAULT, OSSIM, GNS3, VIRTUALBOX, WINDOWS.

					КІК.КР.Б - 125 - 08 - 24 - ПЗ					
Змн.	Арк.	№ докум.	Підпис	Дата	Проект SIEM-підсистеми для SOC на базі рішення AlienVault OSSIM			Літ.	Арк.	Аркушів
Розроб.		Іонніков В.М.		16.06						
Керівник		Фальковський І.Г.		25.06					4	94
Реценз.		Масвський О.В.		25.06				ФІКТ, Гр. КБ-20-2		
Н. контр.		Фальковський І.Г.		25.06						
Затверд.		Єфіменко А.А.		25.06						

ANNOTATION

The final qualifying work of the bachelor consists of an explanatory note to the course project, which consists of an introduction, three sections, conclusions, a list of used literature and appendices. The text part is set out on 82 pages of printed text. The explanatory note has 6 appendices on 12 pages. The list of used sources contains 20 names and occupies 2 pages. The work contains 70 figures and 3 tables. The total volume of work is 94 pages.

The purpose of the work is to develop a SIEM subsystem project for SOC based on the AlienVault OSSIM solution

The paper considered the main principles of work, purpose and key functionalities of SIEM. Recommendations and current trends in SIEM development are defined. A review of free SIEM solutions was conducted, as a result of which it was determined that AlienVault OSSIM is a balanced solution and will be used in the future to organize the SIEM subsystem for SOC in the network project. The logical and physical topology of the network was developed, the number of devices was determined, the addressing scheme was developed, and the SIEM system was designed. The choice of necessary models of devices for the network is justified, their minimum system requirements are specified. The design of the network project was performed in the GNS3 network emulator using the VirtualBox hypervisor. The process of configuring devices and AlienVault OSSIM as a SIEM subsystem is described. The result of the work has been tested and meets the set requirements.

Keywords: NETWORK, PROJECT, SECURITY, SECURITY, EVENTS, SIEM, ALIENVAULT, OSSIM, GNS3, VIRTUALBOX, WINDOWS.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ	10
1.1 Теоретичні аспекти SIEM	10
1.1.1 Загальний опис роботи та призначення SIEM.....	10
1.1.2 Функціональні можливості SIEM.....	14
1.1.3 Рекомендації щодо використання SIEM	17
1.1.4 Сучасні тенденції розвитку SIEM.....	19
1.2 Огляд наявних безкоштовних рішень SIEM	24
1.3 AlienVault OSSIM	31
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	39
2.1. Розробка логічної топології мережної інфраструктури.....	39
2.2. Розробка фізичної топології мережні та адресація	42
2.3. Проєктування системи SIEM.....	44
2.4 Вибір обладнання для реалізації проєкту.....	46
РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ	50
3.1 Налагодження пристроїв мережі.....	50
3.2 Перевірка функціонування мережі.....	68
3.3 Перевірка функціонування SIEM.....	70
ВИСНОВКИ.....	80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	81
ДОДАТКИ.....	83

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SIEM – Security information and event management
 IDS/IPS – Intrusion Detection and Prevention System
 IP – Internet Protocol
 SOC – Security Operation Center
 SIM – Security Information Management
 SEM – Security Event Management
 SNMP – Simple Network Management Protocol
 GUI – Graphical User Interface
 HIDS – Host-based intrusion detection system
 UEBA – User and Entity Behavior Analytics
 RBR – Rule Based Reasoning
 APT – Advanced Persistent Threat
 SOAR – Security Orchestration Automation and Response
 NIDS – Network Intrusion Detection System
 WIDS – Wireless Intrusion Detection System
 ARP – Address Resolution Protocol
 XML – eXtensible Markup Language

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Жодна організація чи установа не застрахована від атак зловмисників. Незалежно від свого розміру, організації щодня стикаються зі різними спроби зловмисного втручання. Хоча пристрої безпеки, такі як брандмауери, антивіруси, системи виявлення і запобігання вторгнень (IDS/IPS, Intrusion Detection and Prevention System), здатні виявляти аномальні події та окремі атаки, втім вони погано оснащені для боротьби з комплексними атаками. Нині хакери все часто використовують розподілені, повільні та цілеспрямовані методи атаки, які важко виявити за допомогою вже згаданих вузькоспеціалізованих пристроїв безпеки.

Система SIEM (Security information and event management) збирає і об'єднує інформацію про журнали подій, щоб допомогти у виявленні та відстеженні порушень безпеки і стану IT-інфраструктури. Це надійний інструмент, який надає фахівцям із кібербезпеки розуміння в режимі реального часу того, що відбувається в їхньому IT-середовищі і аналізувати записи про події, що вже сталися раніше.

SIEM збирають та впорядковує дані журналів і подій в IT-інфраструктурі організації починаючи від кінцевих вузлів, програм і закінчуючи мережевими і захисними пристроями (брандмауери, антивіруси, IDS/IPS). Рішення SIEM спрямовані на кореляцію всіх цих даних, щоб надати фахівцям із безпеки необхідну інформацію для виявлення та відстеження інцидентів та інших важливих подій.

Тому нині є досить актуальним впровадження системи SIEM з безкоштовних рішень, яка б змогла забезпечити базовий функціонал безпеки для невеликої мережі організації.

Метою кваліфікаційної роботи є розробка та налаштування проєкту підсистеми SIEM для SOC (Security Operations Center) на базі рішення AlienVault OSSIM.

Визначена мета обумовлює наступні завдання:

— аналіз принципів роботи систем SIEM та її призначення;

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- функціональні можливості SIEM та сучасні тенденції розвитку;
- огляд наявних рішень SIEM та застосування безкоштовного рішення AlienVault OSSIM;
- розробка логічної, фізичної топології мережі та схеми адресації;
- проєктування системи SIEM;
- вибір обладнання, налаштування мережі та впровадження рішення AlienVault OSSIM в інфраструктурі мережі;
- тестування роботи мережі та системи SIEM.

Об’єктом дослідження є підсистема управління інформаційною безпекою (SIEM) на базі рішення AlienVault OSSIM для центру оперативного реагування на інциденти інформаційної безпеки (SOC), що включає дослідження теоретичних аспектів SIEM, проєктування мережної інфраструктури, налагодження та перевірка функціонування мережі та SIEM-системи.

Предметом дослідження є процес аналізу принципів роботи та функціоналу системи SIEM для центру оперативного реагування на інциденти інформаційної безпеки (SOC), проєктування логічної та фізичної топології мережі та налаштування системи SIEM з використанням безкоштовного рішення AlienVault OSSIM.

В результаті виконання кваліфікаційної роботи було розроблено та налаштовано проєкт підсистеми SIEM для SOC на базі рішення AlienVault OSSIM. Досліджено і перевірено працездатність мережі та налагодженої підсистеми SIEM.

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ

1.1 Теоретичні аспекти SIEM

1.1.1 Загальний опис роботи та призначення SIEM

Системи управління інформацією та подіями безпеки (англ. Security information and event management, SIEM) є відносно новим типом програмного забезпечення централізованого журналювання порівняно з Syslog [1].

SIEM є комбінацією двох технологій, рис.1.1:

- Управління подіями безпеки (англ. Security Information Management, SIM), яка збирає дані з журналів мережевих пристроїв, робочих станцій, серверів та додатків для аналізу, моніторингу активності та виявлення загроз безпеки.
- Керування подіями безпеки (анг. Security Event Management, SEM), яка займається виявленням та відстеженням подій в режимі реального часу та сповіщає мережевих адміністраторів про критичні проблеми та встановлює кореляції між подіями безпеки.



Рисунок 1.1 – Складові SIEM

Переваги і обмеження SIEM

SIEM збирає журнали та дані про події з додатків, пристроїв безпеки та хостів систем і об'єднує це все в єдиній централізованій платформі[2]. SIEM визначає ризики, генерує сповіщення системи безпеки та класифікує їх, як прийнятні або небезпечні. Наприклад, якщо хтось невдало виконує вхід в

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

обліковий запис декілька разів підряд, то це може бути типовою помилкою користувача (не та розкладка клавіатури, мова, регістру). Проте спроба понад 10 разів поспіль може розцінюватись, як намір взлому (атака типу брутфорс).

Використанням SIEM може дати для організації ряд наступних переваг:

- Підвищення ефективності роботи спеціалістів з кібербезпеки та заощадливе використання часових ресурсів;
- Запобігання перетворенню потенційних загроз безпеки у масштабний інцидент безпеки;
- Зниження загальних витрат організації на безпеку;
- Забезпечення кращої системи звітності, аналізу журналів і збереження даних;
- Зведення до мінімуму впливу порушень безпеки;
- Можливість миттєво в режимі реального часу реагувати на інциденти та швидко впроваджувати заходи щодо їх ліквідації;
- Більш високий рівень прозорості при моніторингу дій користувачів, програм та пристроїв, з попередженнями та звітами про порушення політик та підозрілу поведінку, які надають докладні відомості для встановлення контексту;
- Виявлення внутрішніх та зовнішніх загроз з моніторингом практично в реальному часі в кількох додатках та системах;
- Бібліотеки перевірених правил та сценаріїв, а також готові інформаційні панелі та звіти;
- Розслідування подій, що забезпечує кореляцію та аналітику подій, таких як аномальна поведінка;
- Більш просте дотримання нормативних вимог конфіденційності та безпеки даних.

Однак, перш ніж приступити до впровадження SIEM, слід врахувати наступне: комерційні рішення SIEM дорогі і можуть бути складні у розгортанні та налаштуванні[3]. Їх необхідно точно налаштувати для вашого ІТ-середовища та підтримувати у міру зміни ваших систем та вектору загроз. Більш того, SIEM часто генерують численні сповіщення не надаючи значимих даних для аналізу та

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

реагування. В результаті ІТ-команда може витратити надмірну кількість часу на пошук хибних спрацьовувань, водночас дозволяючи реальним загрозам безпеці залишатися непоміченими. Перш ніж розпочати свою роботу із SIEM, необхідно виконати деяку підготовчу роботу. Наприклад, слід оцінити, які типи даних наявні в мережі, загрози, з якими найчастіше стикаються і слабкі місця, а також визначити, які дані наражаються на найбільший ризик. Необхідно спланувати, як можна інтегрувати SIEM програмне забезпечення з іншими рішеннями, щоб максимізувати його цінність.

Способи збору журналів

Системи SIEM, як правило, мають один або декілька серверів журналювання, які виконують аналіз подій, і один або більше серверів баз даних, які забезпечують функцію зберігання логів. Більшість продуктів SIEM підтримують два способи збору журналів:

- **Безагентний (Agentless).** Сервер SIEM отримує дані з окремих хостів, що генерують журнали без необхідності встановлення будь-якого спеціального програмного забезпечення на кінцевих пристроях. Деякі сервери витягують журнали з хостів шляхом аутентифікації сервера на кожному хості, а в інших випадках хости самі надсилають свої журнали на сервер, що зазвичай передбачає реєстрацію кожного хоста на сервері. Незалежно від налаштованого способу отримання журналів, сервер виконує фільтрацію, агрегацію, нормалізацію та аналіз отриманих файлів подій.

- **Агентний (Agent-Based).** Спеціальна програма (агент) встановлюється на хості, що генерує журнали, щоб виконувати фільтрацію, агрегацію та нормалізацію журналів перед відправкою даних вже на сервер SIEM. Якщо хост має кілька типів журналів, то тоді може знадобитися інсталиувати кілька агентів. Деякі продукти SIEM також пропонують агентів для загальних форматів, як Syslog і SNMP або навіть дозволяють адміністраторам створювати спеціальних агентів для обробки непідтримуваних джерел журналів.

Кожен з обраних способів має переваги та недоліки. Основна перевага безагентного підходу полягає в тому, що не потрібно встановлювати,

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

налаштовувати та підтримувати спеціальні програми на кожному хості журналювання. Основним недоліком ж є відсутність фільтрації та агрегації на рівні окремого комп'ютера, що може призвести до передачі значно більших обсягів даних через мережі та збільшення часу необхідного для фільтрації та аналізу журналів. Іншим потенційним недоліком безагентного методу є те, що серверу SIEM можуть знадобитися облікові дані для аутентифікації на кожному хості журналювання. Також в деяких випадках безагентний підхід неможливо використати, через певні технічні складнощі або налаштовані політики безпеки і тоді вже доведеться прибїгати до другого методу – встановлення та налаштування спеціального агента на кожному хості.

Дані для SIEM надсилають з різноманітних джерел, зокрема:

1. Журнали подій. Операційна система та сторонні програми можуть реєструвати події та записувати їх у журнали, які потім передаються до системи SIEM.
2. Мережеве обладнання. Маршрутизатори, проксі-сервери, шлюзи та інше мережеве обладнання можуть генерувати логи про мережну активність, які можуть бути використані для виявлення та аналізу потенційних загроз.
3. Робочі станції користувачів. Логи подій з робочих станцій користувачів можуть містити інформацію про дії користувачів, включаючи аномальну активність або спроби несанкціонованого доступу.
4. Міжмережеві екрани (firewall). Логи роботи міжмережевих екранів містять інформацію про вхідний та вихідний мережевий трафік, дозволяючи виявляти підозрілу активність або несанкціонований доступ.
5. Сканери вразливостей. Спеціальне програмне забезпечення для сканування вразливостей може виявляти потенційні вразливості в інфраструктурі та реєструвати відповідні події.
6. CRM-системи. CRM-системи зберігають інформацію про клієнтів та можуть реєструвати події, пов'язані з обслуговуванням клієнтів, такі як запити на підтримку або проблеми з обслуговуванням.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

7. Антивірусне програмне забезпечення. Антивірусні програми можуть реєструвати події, пов'язані з виявленням та блокуванням шкідливого програмного забезпечення.

8. Інші ресурси. Існують інші ресурси, здатні реєструвати події і передавати їх у SIEM через агентів або вбудовані засоби. Це може включати системи моніторингу доступу, системи реєстрації часу, системи керування конфігурацією та інші.

Інтеграція даних з різних джерел дозволяє системі SIEM отримувати всебічну інформацію про безпеку та проводити аналіз та виявлення потенційних загроз та порушень безпеки. Також для кожного підтримуваного типу джерела журналу системи SIEM зазвичай знають, як класифікувати найважливіші поля журналу (наприклад, значення в полі 5 в журналі від певної програми означає IP-адресу джерела). Це значно покращує нормалізацію, аналіз і кореляцію даних журналу порівняно з програмним забезпеченням із менш детальним розумінням конкретних джерел і форматів журналів. Крім того, програмне забезпечення SIEM може ігнорувати ті поля даних, які не мають значення для безпеки комп'ютера, тим самим потенційно зменшуючи навантаження на мережу і використання сховища даних.

1.1.2 Функціональні можливості SIEM

Продукти SIEM зазвичай ряд наступних функцій, але в залежності від виробника і особливості кожної системи вони можуть відрізнятися:

1. Збір інформації. SIEM здійснює збір даних з різних джерел, як фаєрволи, системи реєстрації подій, антивіруси, системи виявлення вторгнень (IDS/IPS), програми та інші.

2. Агрегація даних. Отримані дані агрегуються та обробляються для подальшого аналізу та використання.

3. Аналіз подій. SIEM забезпечує збереження журналів подій для подальшого аналізу, а також для проведення розслідувань після виникнення інцидентів.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Кореляція подій. Система аналізує дані та встановлює взаємозв'язки між різними подіями, що можуть вказувати на потенційні загрози або аномальну активність.

5. Виявлення загроз. На основі кореляції та аналізу даних SIEM виявляє потенційні загрози безпеки, що може містити вторгнення, витоки даних, зловживання привілеями тощо.

6. Моніторинг в реальному часі. SIEM надає можливість моніторити події безпеки в реальному часі, дозволяючи спеціалістам з безпеки вчасно реагувати на потенційні загрози.

7. Попередження про інциденти. Система може автоматично генерувати попередження та сповіщення про інциденти, що дозволяє швидко реагувати на них і вживати необхідні дії.

8. Автоматичні відповіді на інциденти. SIEM може бути налаштована на автоматичну відповідь на загрози, наприклад, блокування IP чи MAC-адрес, програм чи комп'ютера або виконання інших заздалегідь налаштованих заходів безпеки.

Продукти SIEM можуть включати кілька додаткові функцій, які допомагають персоналу краще здійснювати свою роботу:

- Графічний інтерфейс користувача (Graphical User Interface, GUI) спеціально розроблений для допомоги аналітикам у виявленні потенційних проблем і перегляді всіх доступних даних, пов'язаних з кожною проблемою;

- База знань з інформацією про відомі вразливості та інші технічні дані. Подібний функціонал пришвидшує час правильної ідентифікації загрози;

- Можливість відстеження інцидентів і автоматичного генерування звітів;

- Збереження інформації про активи та їх кореляцію (наприклад, надання вищого пріоритету для атаки націленої на вразливу ОС або більш важливий хост).

Не існує спеціальних стандартів для SIEM, тому кожен продукт здійснює зберігання та передачу даних в будь-якому обраному форматі. Однак зазвичай пропонують можливості для захисту конфіденційності, цілісності та доступності

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

даних журналу. Наприклад, мережевий зв'язок між агентами та серверами SIEM зазвичай зашифрований і відбувається через протокол TCP. Крім того, агентам на хостах і серверах SIEM може знадобитися надати один одному облікові дані та пройти успішну аутентифікацію перш ніж вони зможуть передавати журнали подій.

Інші типи програмного забезпечення також можуть бути корисними для керування журналами і використовуватись разом з продуктами SIEM (або навіть бути вже інтегрованими), зокрема такі як :

- Системи виявлення вторгнень на основі хоста (англ. Host-based intrusion detection system, HIDS). HIDS відстежує характеристики окремого хоста та події, що відбуваються на наявність підозрілої активності. Багато продуктів HIDS здатні відстежувати системні події, антивіруси, брандмауери та журнали програм. Деякі HIDS використовують журнали, як одне з кількох джерел даних для виявлення підозрілої активності, тоді як інші відстежують лише журнали. Як правило, HIDS, який використовує дані журналу, має базу даних сигнатур відомих зловмисних активностей, які він зіставляє із записами журналу для ідентифікації подій. Однак такі продукти часто зосереджені на журналах операційної системи та найпоширенішому програмному забезпеченні безпеки та програмах, а менш поширені програмні забезпечення не підтримується або майже не підтримується.

- Інструменти візуалізації. Інструмент візуалізації представляє дані подій в графічному форматі. Наприклад, інструмент може відображати дані, згруповані або відсортовані за значеннями різних характеристик події, як-от адреса джерела, дата, тип використаної програми. Потім аналітик може обирати необхідні шаблони відображення даних, щоб відображалися лише необхідний тип подій. Інструменти візуалізації можуть бути дуже ефективними для аналізу певних типів даних журналу, наприклад для демонстрації послідовності подій, що відбулися під час атаки за участю кількох хостів. Багато продуктів SIEM мають вбудовані засоби візуалізації, але інструменти сторонніх розробників також можуть бути додатково встановлені, якщо вбудовані інструменти не

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

задовольняють потреби. Імпортувати дані в сторонній інструмент і відображати їх зазвичай відносно просто, але навчитися ефективно використовувати цей інструмент, щоб скоротити великі набори даних до кількох цікавих подій, може потребувати значних зусиль і багато практики.

- Утиліти ротації журналів[4]. Ротація журналу — це практика стиснення, архівування та видалення старих файлів журналу на комп'ютері для економії місця на диску. Системні адміністратори використовують утиліти ротації журналів, щоб керувати розмірами файлів, встановлюючи правила, коли файли журналів слід переносити, стискати чи видаляти.

- Утиліти перетворення журналів. Багато постачальників програмного забезпечення пропонують утиліти перетворення журналів, які можна використовувати для перетворення власних форматів журналів у стандартні. Ці утиліти допомагають включати дані з менш поширених джерел журналу в інфраструктуру керування журналами, коли продукт SIEM не підтримує певний формат журналу.

1.1.3 Рекомендації щодо використання SIEM

Ряд опитувань доводить, що SIEM-системи для багатьох організацій працюють за принципом: "Використовуємо для відповідності нормативним вимогам".

Однією з найбільших помилок сьогодення під час використання SIEM є хибне уявлення, що просто наявність цього інструменту забезпечує відповідність стандартам чи вимогам. Насправді, ті установи, які мали на меті лише відповідати нормативним вимогам, зрозуміли, що вони не тільки не досягають цих вимог, але й не забезпечують достатній рівень захисту. Підприємства, які зосередилися на покращенні захисту через використання SIEM-систем, виявили, що вони як підвищили рівень безпеки, так і досягли відповідності належним нормативам безпеки.

Великою помилкою при задіяні SIEM-систем в інфраструктурі мережі є те, що достатньо лише формувати журнали подій. При цьому нехтується

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

нормалізація журналів подій, захистом цих журналів, ранжуванням даних за важливістю, ступенем деталізації подій, опрацюванням несподіваних ситуацій тощо.

Окремо слід зазначити необхідність зважливого налаштування SIEM-систем, оскільки без точних налаштувань гарантовані часті «хибнопозитивні» спрацювання і ефективність такої системи буде під питанням.

Саме тому дотримуючись ряду наступних рекомендацій, організації зможуть підвищити здатність SIEM виявляти загрози безпеки та реагувати на них, зменшити кількість хибних спрацювань та покращити загальний стан безпеки мережі[5]:

1. Визначте чіткі цілі. Визначте чіткі цілі для впровадження SIEM у тому числі те, що хочете відстежувати, як ви хочете відслідковувати це і які оповіщення хочете отримувати. Це допоможе переконатися, що реалізація SIEM відповідає вашим потребам.

2. Централізуйте свої дані. Збирайте усі дані, пов'язані з безпекою, в одному місці. Це допоможе вам більш ефективно виявляти закономірності та аномалії у ваших даних. Дуже важливо забезпечити інтеграцію всіх відповідних джерел даних у вашу платформу SIEM.

3. Оптимізація прийому даних. Оптимізуйте процес прийому даних, відфільтровуючи непотрібні дані та збираючи лише важливі дані для аналізу безпеки. Це допоможе зменшити обсяг даних, що обробляються платформою SIEM, підвищити продуктивність та зменшити кількість хибних спрацювань.

4. Регулярно налаштовуйте систему. Регулярно налаштовуйте систему SIEM, щоб вона збирала правильні дані та генерувала точні оповіщення. Сюди входить регулярна перевірка та оновлення правил кореляції, порогових значень та інших конфігурацій.

5. Автоматизуйте робочі процеси. Автоматизуйте робочі процеси скрізь, де можна скоротити обсяг ручних операцій і скоротити час відгуку. Наприклад, можна налаштувати SIEM для автоматичної ескалації попереджень

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

відповідним членам команди або ініціювання відповіді на основі попередньо визначених критеріїв.

6. Забезпечте належне зберігання даних. Переконайтеся, що система SIEM налаштована на збереження даних протягом відповідного періоду часу. Зазвичай це диктують нормативні вимоги чи потреби бізнесу.

7. Навчіть свій персонал. Навчіть персонал тому, як ефективно використовувати систему SIEM. Сюди входить розуміння того, як інтерпретувати оповіщення, розслідувати інциденти та реагувати на загрози.

8. Проводьте регулярні перевірки. Проводьте періодичні перевірки вашої системи SIEM, щоб переконатися, що вона відповідає потребам вашого бізнесу та цілям безпеки.

9. Інтеграція з іншими інструментами безпеки. Інтегруйте SIEM з іншими інструментами безпеки, такими як сканери вразливостей, системи виявлення вторгнень та платформи захисту кінцевих точок. Це забезпечить більш повне уявлення про стан безпеки та дозволить швидше реагувати на інциденти безпеки.

1.1.4 Сучасні тенденції розвитку SIEM

Аналітики виділяють три покоління можливостей і технологій безпеки SIEM[6]:

1) Перше покоління SIEM, представлене у 2005 році, поєднує системи керування журналами та керування подіями, які раніше були окремими. Вони обмежені в обсязі даних, які можуть обробити, та в складності сповіщень і візуалізацій, які вони генерують.

2) Друге покоління SIEM, яке було представлено починаючи з 2010 року, було краще обладнане для обробки великих даних — великих обсягів журналів з історичними даними (Big Data SIEM). Такі SIEM можуть співвідносити історичні дані журналів з подіями в реальному часі та даними з каналів аналізу загроз.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

3) Третє покоління SIEM, запропоноване Gartner у 2017 році, поєднує традиційні можливості SIEM із двома новими технологіями. Це аналітика поведінки користувачів і об'єктів (User and Entity Behavior Analytics, UEBA), яка використовує машинне навчання для встановлення базових показників поведінки користувачів або IT-систем і виявлення аномалій. Це також включає автоматизацію безпеки, оркестрування та реагування (Security Orchestration Automation and Response, SOAR), як може допомогти аналітикам швидко розслідувати інциденти.

Протягом останніх двох десятиліть SIEM-системи зарекомендували себе, як потужні та ефективні інфраструктури для команд інформаційної безпеки. Водночас корпоративні SIEM-системи відомі високою вартістю, складністю впровадження та використанням, а також труднощами зі масштабуванням.

Ці виклики були подолані новішими поколіннями технологій, які легше впроваджувати та використовувати, вони вимагають менше обчислювальних ресурсів. SIEM-рішення з безпеки також пропонуються в хмарі та через керованих постачальників послуг безпеки (MSSP), що забезпечує кілька варіантів розгортання, які балансують витрати та простоту впровадження.

Функціональність класичних SIEM

SIEM-системи першого покоління, які прийнято називати класичними, не призначені і в принципі не здатні запобігати інцидентам порушення інформаційної безпеки. Їх функціональність закладена в їх назві: аналіз інформації, що надходить з різних джерел (DLP, IDS, антивірусні засоби захисту, міжмережеві екрани і т. д.), та подальше виявлення відхилень від норм за заданими критеріями. До фундаментальних функцій класичних SIEM-систем належать такі:

- консолідація та зберігання журналів подій від різних джерел;
- надання інструментів для аналізу подій та розбору інцидентів;
- кореляція та обробка подій за правилами кореляції;
- автоматичне оповіщення та керування інцидентами.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Збір даних SIEM-системою, як правило, здійснюється за допомогою спеціальних програмних агентів, які локально збирають журнали подій на кінцевих точках (endpoints) і по можливості передають їх на сервер. Для обробки джерела даних, агенти використовують колектори – бібліотеки для аналізу конкретного журналу подій або системи. Колектори допомагають привести всі ці події до загального вигляду – нормалізувати події. Також інформацію можна збирати віддалено за допомогою протоколів NetBIOS, RPC, TFTP, FTP. Однак у цьому випадку може виникнути проблема з навантаженням на мережу, так як частина систем дозволяє передавати лог-журнали лише однією частиною. У найпростішому випадку у SIEM-системах правила кореляції представлені у форматі RBR (Rule Based Reasoning) та містять набір умов, тригери, лічильники, сценарій дій.

SIEM-системи здатні виявляти:

- мережеві атаки у внутрішньому та зовнішньому периметрах;
- вірусні епідемії або окремі вірусні зараження;
- спроби несанкціонованого доступу до конфіденційної інформації;
- помилки та збої у роботі інформаційних систем;
- вразливості;
- помилки змін у засобах захисту та інформаційних системах;
- цільові атаки (APT - Advanced Persistent Threat).

Функціональні особливості SIEM-рішень третього покоління

В даний час класичне SIEM рішення, що поєднує в собі тільки інструменти по роботі з журналами подій, що надходять від компонентів ІТ-інфраструктури (збір, зберігання, кореляція, перевірка на відповідність вимогам, повідомлення), є застарілим і не може задовольнити всіх потреб будь-якої великої компанії. Сьогодні саме поняття SIEM стало набагато ширшим. Зокрема, від SIEM-рішень потрібні нові функції та механізми, які здатні швидше і точно не тільки виявляти, а й запобігати інцидентам ІБ, при цьому, не обмежуючись аналізом даних тільки з журналів подій. SIEM-рішення. Рішення, що відносяться до передових, прагнуть поєднувати в собі «традиційний» функціонал SIEM, а також функції

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

аналізу мережевого трафіку та управління ризиками. За даними на 2020 рік, на ринку SIEM-систем лідируючі позиції займають:

- Dell Technologies (RSA), США – RSA NetWitness (RSA NWP);
- Exabeam, США - Security Management Platform (SMP);
- IBM, США - QRadar Security Intelligence;
- LogRhythm, США - XDR;
- Rapid7, США - Insigh;
- Securonix, США – Securonix SIEM
- Splunk, США – Splunk Enterprise Security (ES).

Близькі до лідерів світового ринку з реалізованої функціональності такі SIEM рішення:

– AT&T Cybersecurity, США – Unified Security Management (USM) Anywhere;

- AT&T Cybersecurity, США – AlienVault OSSIM;
- FireEye, США - Helix;
- Fortinet, США – FortiSIEM;
- LogPoint, Данія – LogPoint SIEM;
- ManageEngine, Індія – ManageEngine Log360
- McAfee, США – Enterprise Security Manager (ESM);
- AlienVault, США, AlienVault OSSIM
- SolarWinds, США SolarWind Security Event Manager (SEM).

Зазначимо, що SIEM-платформи лідерів ринку на даний момент позиціонуються як рішення третього покоління. Вони надають такі розширені в порівнянні з класичними можливості:

1) Ідентифікація складних загроз (Threat Intelligence) - правила кореляції не можуть охопити багато складних атак, оскільки їм не вистачає контексту або вони не можуть реагувати на нові типи інцидентів. За допомогою автоматичного профілювання SIEM може виявити поведінку, що передбачає загрозу;

2) «Боковий рух» (Lateral movement) – зловмисники «переміщаються» по мережі, використовуючи IP-адреси, облікові дані та комп'ютери, у пошуках

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

ключових активів. Аналізуючи дані по всій мережі та безлічі системних ресурсів, SIEM може виявити цей рух;

3) Аналіз поведінки об'єкта (User and Entity behavior analysis) – критичні елементи та активи в мережі, такі як сервери, медичне обладнання або обладнання, мають унікальні моделі поведінки. SIEM можуть вивчати ці моделі та автоматично виявляти аномалії, які припускають загрозу;

4) Виявлення без правил або сигнатур (Detection without rules or signatures) – багато загроз, не можуть бути зафіксовані за допомогою певних вручну налаштованих правил або відомих сигнатур атак. SIEM можуть використовувати машинне навчання для виявлення інцидентів без існуючих раніше визначень;

5) Автоматичне реагування на інцидент (Automated incident response) – як тільки SIEM виявляє певний тип події безпеки, вона може виконати заздалегідь заплановану послідовність дій для стримування та «пом'якшення» інциденту. SIEM стають повноцінними інструментами забезпечення безпеки та оркестрування (SOAR).

SIEM третього покоління надають технологію аналізу поведінки користувачів і сутностей (UEBA), яка використовує машинне навчання та поведінкове профілювання для інтелектуальної ідентифікації аномалій або тенденцій, навіть якщо вони не були відображені у правилах або статистичних кореляціях традиційних. Розвитком UEBA-інструментарію, є поява нового шару у вигляді штучної імунної системи SIEM-платформи з глибокою її інтеграцією («зрощуванням») з корпоративною IT-інфраструктурою. При цьому SIEM наступного покоління, використовуючи недороге розподілене сховище із застосуванням технік блокчейн, дозволять організаціям зберігати повні вихідні дані та контролювати їх цілісність. Це дозволяє проводити глибокий поведінковий аналіз історичних даних, щоб виявити ширший спектр аномалій та проблем безпеки.

Платформи SIEM третього покоління вже зараз інтегруються з великою різноманітністю джерел безпеки та організаційних джерел даних і можуть аналізувати, агрегувати та аналізувати дані для забезпечення безпеки. Вони

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

поставляються з готовими інтеграційними роз'ємами для тимчасових хмарних сервісів. SIEM надають API-інтерфейси, які дозволяють додавати інтеграції користувачів у власні системи безпеки або IT-системи або постачальників, які ще не підтримуються інструментом SIEM.

Починаючи з третього покоління SIEM включають технологію автоматичного реагування на інциденти. Це вимагає нових видів інтеграцій, які замість вилучення даних з корпоративних систем (вхідних) можуть виконувати автоматичні зміни в корпоративних системах (вихідних). Тенденції розвитку інтеграції в SIEM-рішеннях наступного покоління полягають у початковій інкапсуляції механізмів моніторингу та реагування на події безпеки безпосередньо в складі IT-засобів на всіх рівнях - від кінцевих точок до систем бізнес-аналізу.

1.2 Огляд наявних безкоштовних рішень SIEM

Безкоштовні SIEM-рішення є важливим інструментом для багатьох організацій, особливо тих, хто шукає способи підвищити свою кібербезпеку без значних фінансових вкладень. Вони надають необхідний функціонал для моніторингу та аналізу подій безпеки та пропонують високу гнучкість та можливість налаштування під конкретні потреби організації.

Сучасний ринок пропонує безліч безкоштовних SIEM рішень, але розглянемо найбільш популярні та актуальні:

1) Wazuh – це масштабована система виявлення вторгнень на основі хоста з відкритим вихідним кодом[7], рис.1.2. Дана платформа була створена як відгалуження OSSEC, потужного та надійного механізму кореляції та аналізу. Це рішення стало більш комплексним завдяки інтеграції з OpenScap та Elastic Stack. Wazuh працює на багатьох популярних операційних системах, таких як Linux, OpenBSD, FreeBSD, Solaris, MacOS та Windows, а також забезпечує моніторинг реєстру Windows, аналіз журналів, перевірку цілісності файлів, виявлення загроз, оповіщення у реальному часі та багато іншого.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

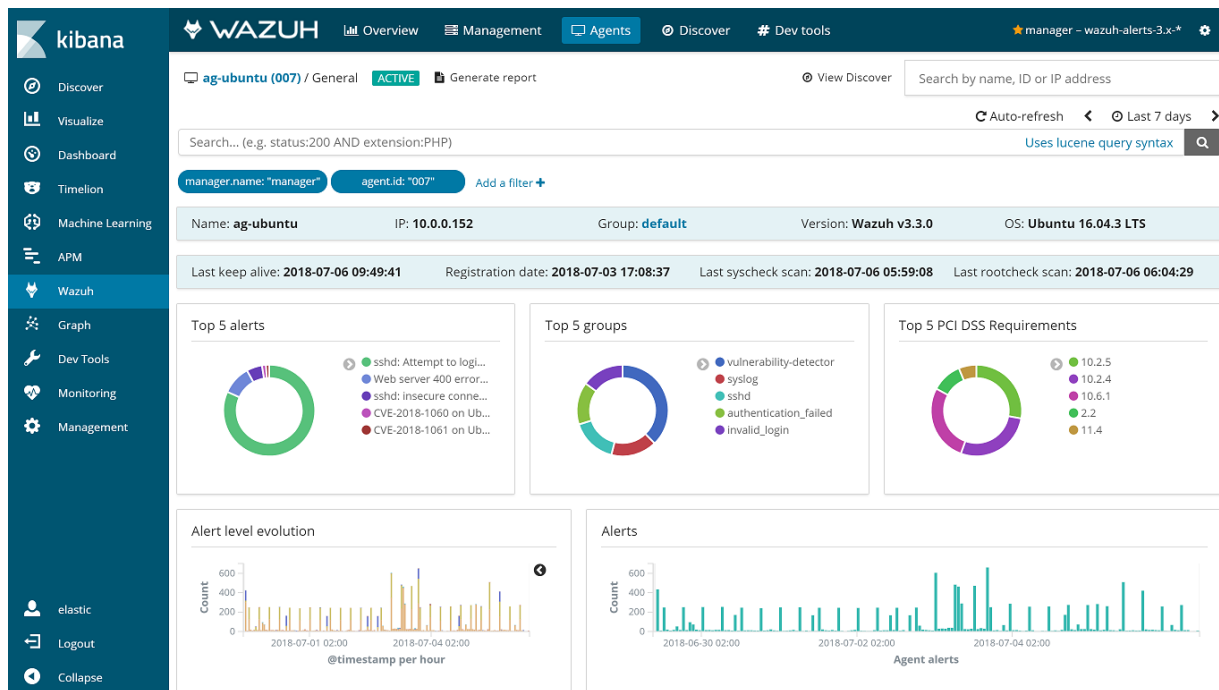


Рисунок 1.2 – Головне вікно Wazuh

Wazuh може використовуватися для моніторингу кінцевих точок, хмарних сервісів, контейнерів, а також для агрегування та аналізу даних зі сторонніх джерел. Агенти Wazuh проводять сканування контрольованої інформаційної системи з метою пошуку шкідливих програм, руткітів, підозрілих аномалій і т.д. В результаті сканування можуть бути виявлені приховані файли, приховані процеси або незареєстровані мережні прослуховувачі, а також невідповідності в кодах у відповідь на системні виклики.

Можливості Wazuh SEIM включають:

- Аналіз журналів безпеки
- Виявлення вразливостей
- Оцінка конфігурації системи безпеки
- Відповідність нормативним вимогам
- Оповіщення та повідомлення
- Складання звітів

Агенти Wazuh працюють на різних платформах, включаючи Windows, Linux, Mac OS X, AIX, Solaris та HP-UX. Вони можуть бути налаштовані та

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

керуватися з сервера Wazuh, тобто сервер здатний відправляти команди агентам, наприклад, щоб ініціювати відповідь при виявленні загрози. Основні можливості агентів:

- Збір даних журналу та подій
- Моніторинг цілісності файлів та ключів реєстру
- Інвентаризація запущених процесів та встановлених програм
- Моніторинг відкритих портів та конфігурації мережі
- Виявлення руткітів та артефактів
- Оцінка конфігурації та моніторинг політики
- Активна реакція на виявлені загрози

Області застосування Wazuh включають аналітику безпеки, виявлення вторгнень, аналіз журнальних даних, моніторинг цілісності файлів, виявлення вразливостей, оцінку конфігурації, реагування на інциденти, хмарну безпеку і т.д.

2) Sagan спеціалізується на аналізі мережових входів у режимі реального часу та оцінці їх кореляції[8], рис.1.3. Сумісний із програмним забезпеченням для керування правилами типу Snort або Suricata. Має відкритий вихідний код, написаний мовою C та розповсюджується безкоштовно.

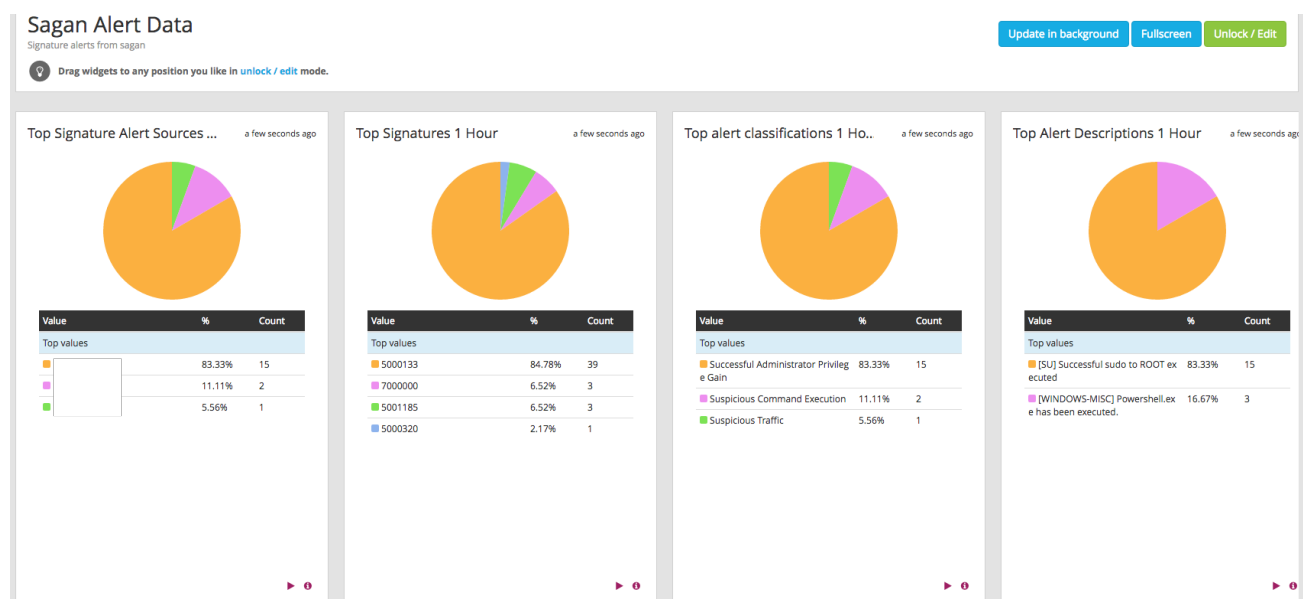


Рисунок 1.3 – Головне вікно Sagan

Sagan здатен в реальному часі аналізувати входи та корелювати їх. Веде журнали, підтримує їх багаторядкові типи, при виявленні загроз запускає заздалегідь налаштовані скрипти, автоматично моніторить міжмережевий екран. Багатопотокова структура даного інструменту дозволяє обробляти журнали в реальному часі, використовуючи повний потенціал всіх процесорних ядер. Серед інших переваг — сумісність із графічними консолями Snorby, BASE, EveBox.

Можливості Sagan включають:

- Аналіз пакетів
- Власна аналітика погроз «блакитна точка»
- Визначення місця призначення зловмисного програмного забезпечення та вилучення файлів
- Відстеження доменів
- Користувальницькі правила та звітність
- Хмарна безпека
- Дотримання нормативних вимог

3) AlienVault OSSIM[9], рис.1.4 – одна зі старіших та популярних SIEM з відкритим вихідним кодом, яку розробила компанія AlienVault, також відомою як AT&T Cybersecurity з 2019 по 2024 рік, а нині LevelBlue.

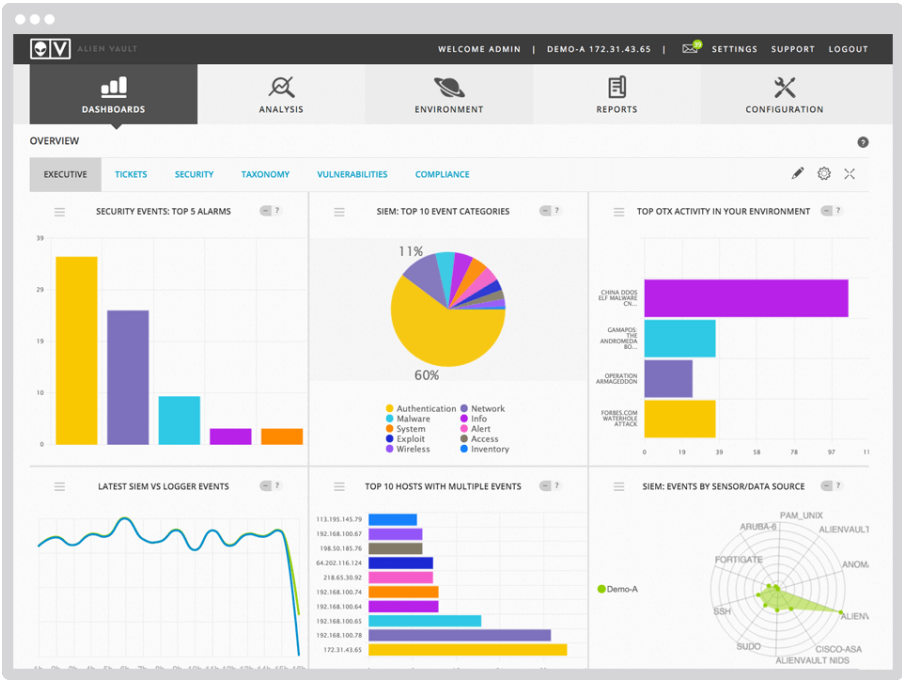


Рисунок 1.4 – Головне вікно AlienVault OSSIM

Головна перевага даного рішення — ефективний моніторинг поведінки та виявлення підозрілої активності. OSSIM є досить багатофункціональною системою із можливістю запису подій, нормалізацією даних та іншими додатковими кореляційними утилітами.

Дана SIEM здатна оцінювати загрози в довгостроковій перспективі, аналізувати та архівувати дані, має вбудований алгоритм автовідповідей на загрози та безперервне сповіщення користувача, який може дізнаватися про загрози або їх відсутність у реальному часі. Також існує комерційний варіант даної системи під назвою AlienVault Unified Security Management з платни але більше розширеним функціоналом.

OSSIM може бути задіяний, як для захисту корпоративних мереж, так і в невеликих домашніх. Але найбільш ефективно він себе проявляє у великих організаціях, де є кілька захисних пристроїв, таких як брандмауер, IDS/IPS, антивірус і відповідно є змога збирати та аналізувати події з декількох пристроїв водночас.

Можливості AlienVault OSSIM включають:

- Розширене виявлення погроз на основі аналізу поведінки;
- Управління журналами;
- Централізоване виявлення загроз та реагування на інциденти у хмарній та локальній інфраструктурі;
- Може бути розгорнуте як на фізичному пристрої, так і у віртуальних середовищах.

4) Prelude OSS — це безкоштовна SIEM з відкритим вихідним кодом [10], рис.1.5. Підтримує кілька форматів журналів і може легко інтегруватися зі сторонніми інструментами, такими як Suricata, OSSEC і Snort. Prelude OSS використовується для збору, нормалізації, сортування, агрегування, кореляції та створення звітів про всі події, пов'язані з безпекою. Prelude допомагає здійснювати постійний моніторинг безпеки та спроби вторгнення, ефективно аналізувати сигнали для швидкого реагування та виявляти тонкі загрози.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Глибоке виявлення загроз у Prelude SIEM проходить різні етапи з використанням найновіших методів поведінкового аналізу чи машинного навчання.

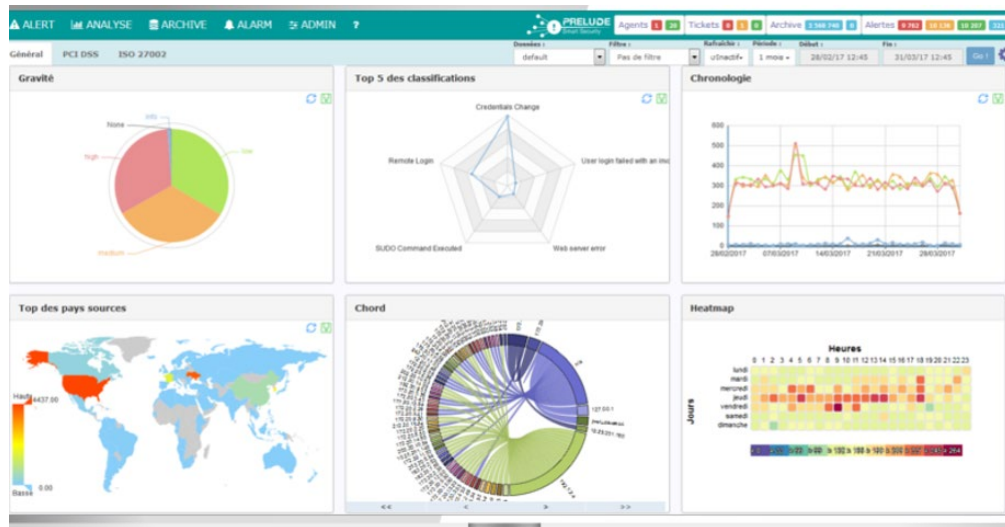


Рисунок 1.5 – Головне вікно Prelude OSS

Prelude ідеально підходить для середніх і великих корпорацій, державних установ і організацій зі складною мережевою інфраструктурою, які потребують розширеного виявлення загроз, аналізу та управління відповідністю. Потужна платформа для аналізу в реальному часі мережевого обладнання та попереджень про безпеку програм робить Prelude SIEM зручною для аналітиків безпеки, мережевих адміністраторів і команд з кібербезпеки.

Його широкі можливості реєстрації, моніторингу та звітності роблять його чудовим для підприємств, які дотримуються різноманітних нормативних зобов'язань.

Можливості Prelude OSS включають:

- Легко інтегрується з рішеннями Suricata, OSSEC і Snort;
- Підтримує різні варіанти встановлення: Docker, Puppet, Chef, Ansible;
- Підтримує моніторинг хмарних сервісів, включаючи AWS та Azure;
- Включає комплексний набір правил для виявлення безлічі типів атак і дозволяє зіставляти їх у відповідність до PCI DSS v3.1 і CIS;

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

- Інтегрується з системою зберігання та аналізу логів Splunk візуалізації подій та підтримки API.

Для зручності наведемо порівняльну таблицю з основними характеристиками згаданих SIEM, табл.1.1.

Таблиця 1.1

Порівняльна характеристика SIEM

SIEM	Wazuh	Sagan	AlienVault OSSIM	Prelude OSS
Ліцензія	Open Source (GPLv2)	Open Source	Open Source (GPLv3)	Open Source
Підтримка ОС	Linux, Windows, macOS	Linux	Linux, Windows	Linux, Windows
Інтеграції	Elastic Stack, Ansible, Docker, Kubernetes	Snort, Suricata	OpenVAS, Suricata, Nmap	Snort, Suricata, Bro
Масштабованість	Висока, зручна для великих інфраструктур	Висока, залежить від інфраструктури	Висока, підходить для малих та середніх бізнесів	Висока, залежить від конфігурації
Інтерфейс	Веб-інтерфейс (Kibana)	Немає власного GUI	Веб-інтерфейс	Веб- інтерфейс (Prelude- Manager)
Підтримка спільноти	Сильна, активна спільнота	Обмежена	Сильна, активна спільнота	Відносно обмежена
Аналіз в режимі реального часу	Так	Так	Так	Так
Документація	Добре документована	Відносно обмежена	Добре документована	Відносно обмежена

Виходячи з таблиці та вищеперерахованих характеристик обраних SIEM можна сказати, що Sagan і Prelude OSS погано підходять для проєкту підсистеми SIEM, оскільки дані продукти мають обмежену підтримку з боку спільноти та недостатню кількість документації, що в подальшому значно ускладнить процес налаштування та підтримку роботи систем.

Wazuh та OSSIM – обидва достойні кандидати на роль майбутньої системи SIEM в даному проєкті. Вони обидва мають вбудований графічний інтерфейс, можуть бути встановлені на ОС Windows та Linux, активно підтримуються спільнотою, гарно задокументовані і в цілому є досить популярними безкоштовними рішеннями на сьогоднішній день. Втім OSSIM є дещо простішим в налаштуванні і має інтуїтивно зрозумілий графічний інтерфейс. До того ж, за потреби, можна буде придбати комерційну версію AlienVault Unified Security Management, яка має досить подібний інтерфейс до OSSIM і додасть ряд цікавих та корисних нововведень.

Тому AlienVault OSSIM є збалансованим рішенням, яке поєднує в собі функціональність, зручність використання та активну підтримку спільноти. Це робить його привабливим варіантом для організацій, які шукають комплексний та надійний інструмент для управління інформацією та подіями безпеки без необхідності значних фінансових та технічних ресурсів.

1.3 AlienVault OSSIM

AlienVault OSSIM (Open Source Security Information Management) - це багатофункціональна система управління інформацією та подіями безпеки (SIEM) з відкритим вихідним кодом, яка забезпечує збір, нормалізацію та кореляцію подій. [11]. AlienVault OSSIM була розроблена інженерами через брак доступних рішень з відкритим вихідним кодом, щоб вирішити поширену проблему, з якою стикаються багато спеціалістів з безпеки: SIEM-системи, незалежно від того, чи є вони з відкритим кодом чи комерційні, не приносять користі, якщо не забезпечують візуалізацію безпеки.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Система OSSIM є комплексним рішенням щодо управління безпекою, яка дозволяє виявляти та класифікувати кібератаки на основі аналізу, оцінки ризиків та кореляції подій у реальному часі [12]. Базою даних системи є SQL-орієнтованою, у ній зберігається вся інформація, необхідна функціонування OSSIM. Сервер управління включає консоль, яка використовується для контролю над іншими компонентами, та сервер OSSIM, який обробляє дані, що надходять від сенсорів.

Як система SIEM, OSSIM призначена для того, щоб дати аналітикам безпеки та адміністраторам більш повне уявлення про всі пов'язані з безпекою аспекти їх системи за рахунок об'єднання управління журналами, яке може бути розширено за допомогою плагінів, що підключаються додатково[13]. Потім ця інформація зіставляється, щоб створити повний контекст для інформації. Передбачене надсилання сигналів тривоги та доступності, а також можливості створення звітів для спеціалістів з безпеки та системних інженерів.

Компоненти OSSIM

Структурно OSSIM може бути розділений на 4 компоненти[14]:

- Сенсори (Sensos) – дані компоненти збирають і нормалізують події створені різними програмними засобами (фаєрвол, IDS, антивірус, тощо). Можна розгорнути скільки завгодно датчиків на одному пристрої. Сенсори використовують плагіни для аналізу даних та пересилання їх до серверу.

- Сервер (Server) – отримує події від сенсорів і виконує завдання нормалізації даних, оцінки ризиків і пріоритетів подій, кореляції даних.

- База даних (Database) – служить для зберігання конфігурацій та подій. Використовується база даних MySQL.

- Фреймворк або фронтенд (Framework) – надає графічний інтерфейс для керування OSSIM у формі зручного та простого веб-інтерфейсу керування або через консоль.

Значна частина роботи з розгортання відбувається під час підключення бажаних джерел даних до сервера OSSIM. Як вже зазначалось OSSIM потребує спеціальні плагіни для кожного джерела для аналізу даних та пересилання їх до

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

серверу. Плагін — це файл конфігурації на основі XML. Нижче наведено список найбільше популярних безпекових рішень для яких OSSIM має плагіни:

- Suricata: потужна мережева система виявлення вторгнень/система запобігання вторгненням (IDS/IPS) використовує перевірку на основі сигнатур, протоколів і аномалій.

- OSSEC: хостова система виявлення вторгнень мережева система виявлення вторгнень (Network Intrusion Detection System, NIDS);

- Kismet: бездротова система виявлення вторгнень (Wireless Intrusion Detection System, WIDS);

- Arpwatch: реєструючи дії та виявляє аномалії пов'язані з ARP наприклад, спроба підробки ARP. Він реєструє комбінації IP/MAC-адрес і повідомляє про зловмисні зміни на рівні каналу передачі даних.

- P0f – ефективний пасивний інструмент розвідки для ідентифікації типу ОС і програмного забезпечення на кінцевих пристроях. Це все робиться без генерування мережевого трафіку, як це можуть роблять інструменти активної розвідки.

- PADS – The Passive Asset Detection System використовується для виявлення аномалій обслуговування. Наприклад, PADS і Nmap разом використовуються для виявлення нових мережевих служб або змін у існуючих.

- Tcptrack: простий сніфер для отримання інформації про мережеві з'єднання.

- Munin: потужний інструмент моніторингу мережі та інфраструктури. Він не тільки відстежує та сповіщає, але й надає корисні графіки через веб-інтерфейс, щоб допомогти зрозуміти, що відбувається у мережі;

- OpenVas: потужний сканер для сканування вразливостей та керування ними;

- Nfdump – інструмент збору та обробки даних NetFlow. NfSen використовуються для візуалізації та дослідження NetFlow для nfdump;

- Fprobe – інструмент на основі libpcap, який збирає дані про мережевий трафік і збирає їх як потоки NetFlow;

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

•Nagios: багатофункціональна програма моніторингу мережі хостів та зазначених портів щодо доступності. За необхідності сповіщає про виявлені проблеми;

•OSVDB – Open Source Vulnerability Database – це відкрита база даних про вразливості. OSVDB безпосередньо інтегровано в OSSIM;

•Open Threat Exchange або (OTX) – відкрита платформа для обміну інформацією про проблеми та загрози безпеці. OTX забезпечує доступ до інформації у режимі реального часу. Це дає можливість користувачеві вчитися на помилках інших людей, які вже зазнали зловмисного впливу.

•Та багато інших плагінів для збору інформації або ж парсингу та кореляції логів з різних зовнішніх пристроїв та служб.

Функціональні можливості

Нижче наведено ряд суттєвих можливостей, які може надати використання OSSIM [15]:

•Виявлення нових пристроїв: OSSIM може активно сканувати мережу та додавати нові виявлені активи до своєї бази даних. Ця функція є важливою, особливо коли невідомий пристрій намагається отримати підключитися до інфраструктури мережі. OSSIM зберігає інформацію про кожен пристрій мережі, наприклад MAC-адресу, внутрішню IP-адресу, модель та операційну систему.

•Оцінка вразливості: можна налаштувати розклад сканування мережі, щоб відшукати найбільш вразливі місця в мережі.

•Виявлення вторгнень: активний моніторинг дозволяє OSSIM повідомляти про спроби та успішні вторгнення із зовнішніх і внутрішніх джерел. Попередньо налаштована база даних під час інсталяції вже попередньо містить з низку інформації та шаблони атак.

•Кореляція: є однією з основних функцій, яка визначає OSSIM як платформу інтелектуального керування подіями безпеки та відрізняє її від IDS/IPS. Це допомагає зменшити кількість помилкових спрацьовувань шляхом перетворення кількох вхідних подій і тривог на більш надійний вихід, щоб мати меншу кількість подій на які слід звернути увагу. Функція кореляції складається

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

з перехресної кореляції та логічної кореляції (кореляційні директиви). Перехресна кореляція працює лише з подіями, які мають визначені IP-адреси призначення, оскільки OSSIM має перевірити хост призначення, щоб визначити, чи є вразливі місця, які не містяться в базі даних, і відповідно змінює значення надійності події. Значення надійності події є одним із показників, який використовується для розрахунку ризику в OSSIM.

•Кореляційна директива: є ще однією основною функцією OSSIM. OSSIM постачається з 200 кореляційними директивами, які написані на синтаксисі, базованому на XML. Кореляційна директива містить одне або кілька правил кореляції, визначають, чи потрібно з'єднувати певні події. Основна мета директиви — аналізувати кілька подій і вирішувати, чи генерувати тривогу на основі правил директиви. Вона використовує логічні та часові залежності між подіями, щоб ідентифікувати шаблони, які можуть вказувати на інцидент, рис.1.6.

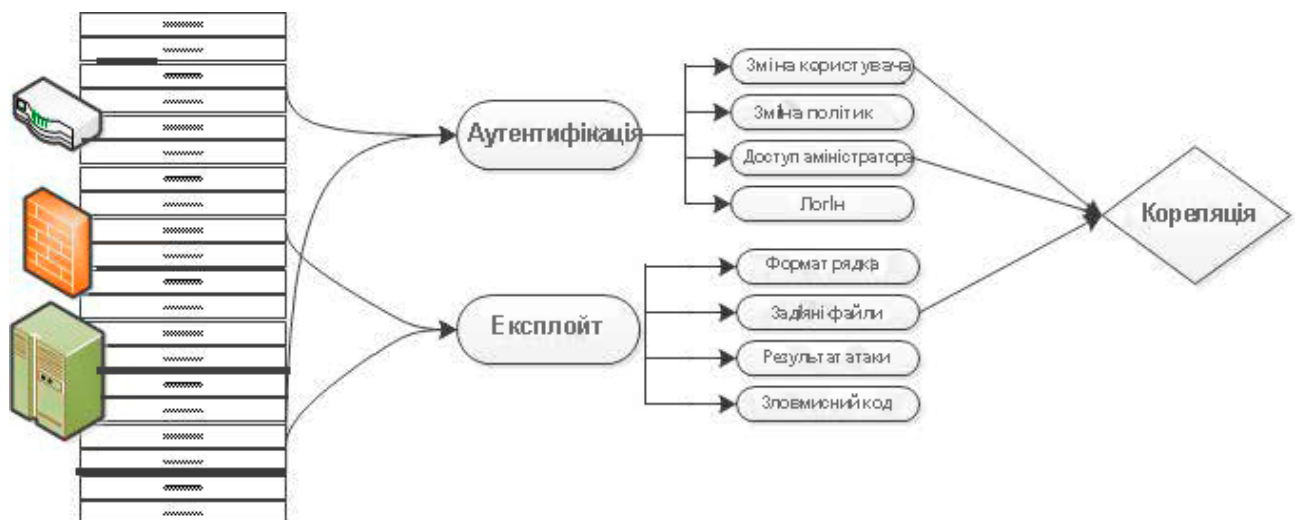


Рисунок 1.6 – Приклад аналізу та кореляції подій

•Кореляційні директиви дозволяють системі зменшувати кількість хибнопозитивних спрацьовувань та виявляти складні атаки, які можуть залишитися непоміченими при аналізі окремих подій. Ця функція може запобігати атакам нульового дня або невідомим вразливостям, оскільки вона генерує тривогу, дотримуючись правил, а не перевіряючи подію в списку

відомих вразливостей. Простий приклад використання директиви може полягати в тому, щоб згенерувати тривогу, коли хтось намагається підключитися до веб-сервера через SSH використовуючи більше 3 спроб.

•Розрахунок ризику: керування даними в OSSIM складається з необроблених журналів, подій, тривог і квитків. Необроблені журнали отримуються з різних джерел даних на сервер OSSIM і нормалізуються. Нормалізовані журнали відображаються у веб-інтерфейсі управління під SIEM як події. Квитки можуть бути відкриті вручну або автоматично генеруватися в OSSIM. Типове використання для обробки інцидентів в OSSIM полягає у перегляді тривог, створенні квитка для відповідних інцидентів та призначенні його відповідному персоналу. Тривоги генеруються, коли значення ризику події дорівнює або перевищує одиницю. Ризик розраховується за такою формулою: **ВАРТІСТЬ АКТИВУ[0-5] * (ПРІОРИТЕТ[0-5] * НАДІЙНІСТЬ[0-10] / 25) = РИЗИК ПОДІЇ[0-10]**, рис.1.7.



Рисунок 1.7 – Приклад розрахунку значення ризику

Кожен актив в OSSIM має значення активу між 0 і 5. Чим вище число, тим цінніший актив. Актив може бути хостом, групою хостів, мережею або групою мереж. Пріоритет вимірює важливість події. Показник надійності - це ймовірність атаки; наприклад, високе значення (9 або 10) означає, що атака є реальною.

•Інтеграція API до найбільшої у світі бази даних безпеки: OSSIM може бути інтегрована з Open Threat Exchange. Це найбільша в світі база даних поточних атак, шкідливих програм, програм-вимагачів і журналів підозрілих IP-адрес. Це допомагає платформі завжди бути в курсі про більшість зловмисних активностей.

•Моніторинг цілісності файлів: OSSIM можна налаштувати для сканування та моніторингу всіх конфіденційних файлів і документів у мережі, щоб попередити про спробу або поточну атаку програм-вимагачів. Чим швидше ці атаки будуть припинені, тим менше буде простою мережі під час відновлення.

•Використання мережі: OSSIM відстежує мережу, яка складається з кінцевих пристроїв користувачі, мережевого обладнання та серверів, щоб допомогти виявити аномальну активність. Це робиться за допомогою моніторингу поведінки. Наприклад, якщо користувач використовував лише 2 ГБ даних у вівторок, а до п'ятниці цей обсяг збільшився до 30 ГБ, OSSIM може згенерувати відповідне сповіщення, щоб адміністратори мережі могли провести розслідування та внести необхідні корективи.

Розгортання та підтримка системи

Системні вимоги включають мінімум 4 ГБ оперативної пам'яті, 64-бітний процесор і мережеву карту з пропускною здатністю 1000Mbit. Також слід зазначити, що документація з встановлення AlienVault вказує, що вимоги до апаратного забезпечення в основному залежать від кількості подій за секунду та пропускної здатності мережі, яку ви хочете захистити.

Встановлення OSSIM досить просте, особливо якщо виконувати автоматичне встановлення за замовчуванням, яке називається профілем "все-в-одному" (all-in-one). Профіль "все-в-одному" включає відразу всі 4 компоненти OSSIM: сенсор, сервер, базу даних і фронтенд.

Висновки до 1 розділу

В ході розробки даного розділу було розглянуто основні принципи роботи та призначення систем управління інформацією та подіями безпеки (SIEM). Визначено, що SIEM-системи є критично важливими для сучасних організацій,

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

оскільки вони забезпечують збір, аналіз та кореляцію даних з різних джерел для виявлення та реагування на загрози безпеці.

Розглянуто ключові функціональні можливості SIEM-систем. Наведено повний перелік функцій, які використовуються в SIEM у контексті забезпечення комплексного захисту інформації.

Наведено перелік рекомендації щодо ефективного та використання SIEM-систем. Підкреслено важливість належного налаштування та інтеграції SIEM з іншими системами безпеки для досягнення максимальної ефективності, проведення регулярного навчання персоналу, постійного моніторингу та важливості зберігання даних про події в IT-інфраструктурі.

Було досліджено сучасні тенденції розвитку SIEM-технологій. Визначено основні функції та можливості першого, другого та третього поколінь можливостей і технологій безпеки SIEM. Визначено сучасні системи SIEM, які максимально відповідають третьому поколінню. Визначено загальні тенденції розвитку SIEM, що включає розвиток UEBA-інструментарію за рахунок появи нового шару у вигляді штучної імунної системи SIEM-платформи з глибокою її інтеграцією з корпоративною IT-інфраструктурою, покращенням технології автоматичного реагування за рахунок глибокої інтеграції в інфраструктурі мережі, застосуванням технік блокчейн.

Було проведено огляд безкоштовних SIEM-рішень, таких як Wazuh, Sagan, AlienVault OSSIM та Prelude OSS. Визначено їх функціональні можливості та переваги. Наведено порівняльну таблицю характеристик зазначених SIEM та проведено її аналіз в ході якого було визначено, що AlienVault OSSIM є збалансованим рішенням, яке поєднує в собі функціональність та зручність використання і є гарним варіантом для її використання в проєкті. Також було детально розглянуто систему AlienVault OSSIM з повним визначенням функціональних можливостей, компонентів, архітектури та способів розгортання.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1. Розробка логічної топології мережної інфраструктури

При проектуванні мережі буде використано трирівневу ієрархічну модель мережі, яка включає в собі [16]:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

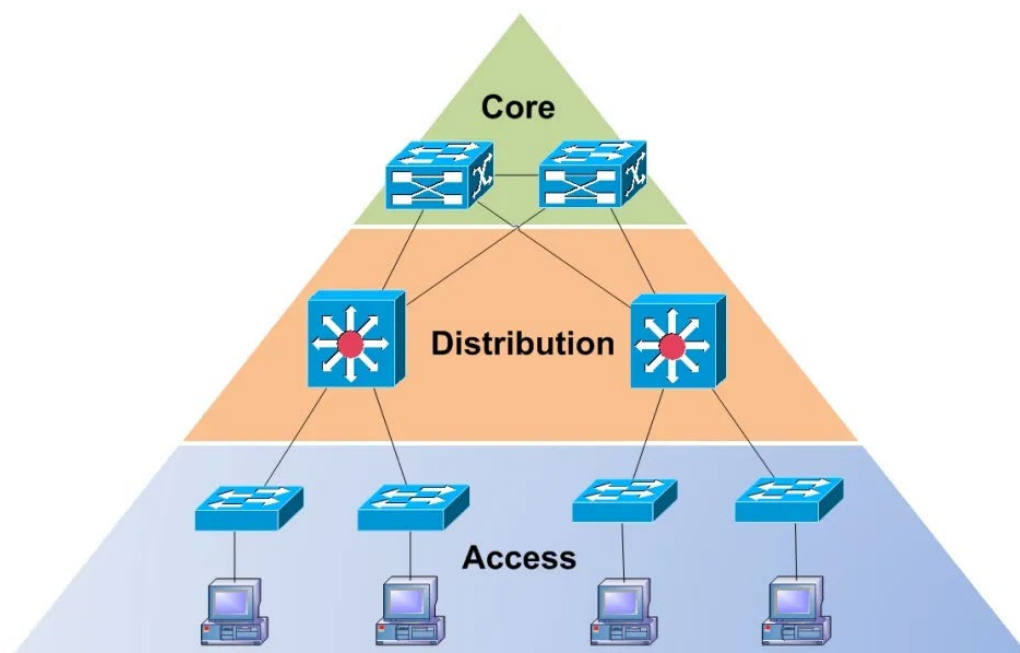


Рисунок 2.1 – Трирівнева модель мережі

Трирівнева модель мережі використовується для кращої організації та управління комп'ютерною мережею. Ця модель забезпечує структуру, яка дозволяє забезпечити ряд важливих функцій: масштабованість, надійність, легке управління, безпека, легке обслуговування.

Рівень ядра – формує ядро мережі. Це найвищий рівень ієрархії, яка відповідає за швидке пересилання великих обсягів трафіку по мережі, тому тут часто використовується маршрутизатори та комутатори з високими пропускними здатностями. Це рівень є серцем мережі, тому є вкрай важливим забезпечити його відмовостійкість та надійність.

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Рівень розподілу розташований посередині. Основні функції рівня розподілу полягають у маршрутизації, фільтрації, керування трафіку між рівнями ядра та доступу. Рівень розподілу повинен забезпечувати найшвидший спосіб обробки запитів до служб і також тут часто налаштовуються політики безпеки. В залежності від розміру мережі тут можуть використовуватися маршрутизатори, багаторівневі комутатори або ж звичайні керовані комутатори.

Рівень доступу забезпечує пряму взаємодію з кінцевими користувачами та їх пристроями (комп'ютери, сервери, принтери, смартфони та інше). На цьому рівні здійснюється доступ до мережі и застосовуються певні методи контролю трафіку. Основна задача рівня доступу – це забезпечити ефективний та безперервний доступ до мережі для кінцевих пристроїв. Як правило тут задіяні комутатори та точки доступу.

Наступним питанням є розміщенням OSSIM в топології мережі. Подібні системи рекомендовано встановити ближче до центру мережі аби SIEM могла збирати та аналізувати дані з усіх вузлів і пристроїв мережі. На рис.2.2 та рис.2.3 наведено приклади можливих розміщень OSSIM в інфраструктурі мережі [17].

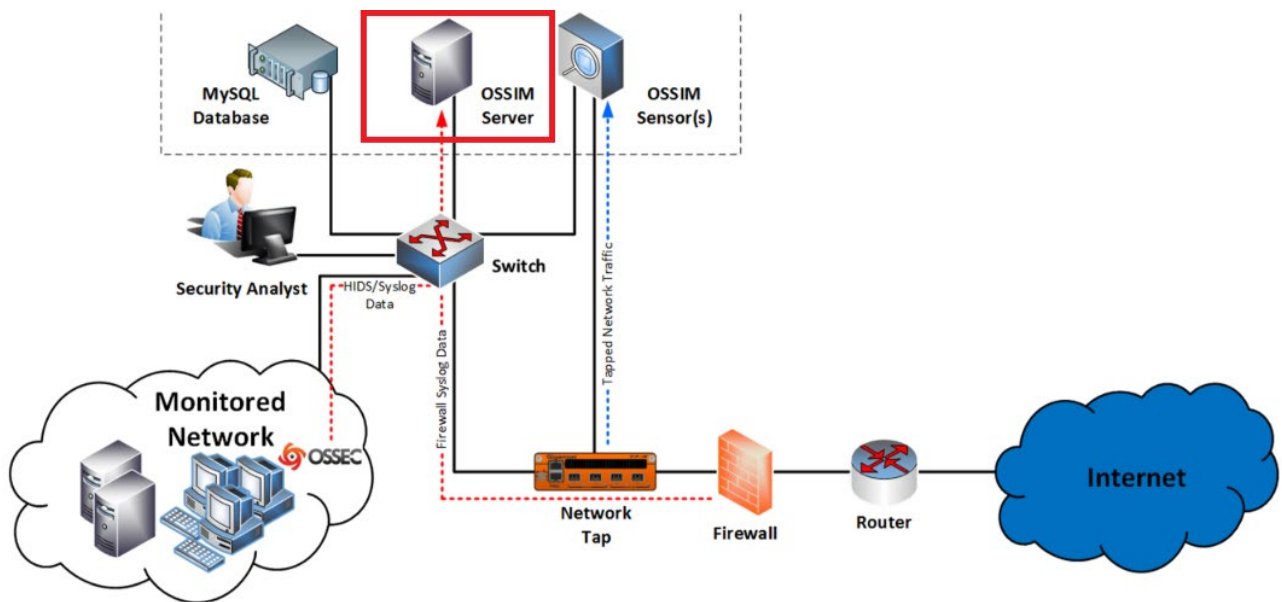


Рисунок 2.2 – Перший приклад розміщення OSSIM

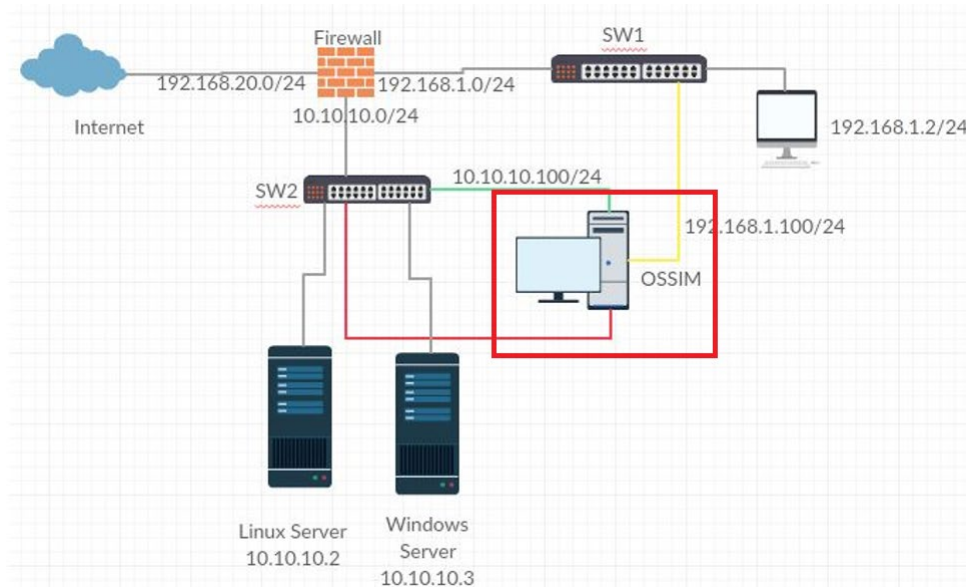


Рисунок 2.3 – Другий приклад розміщення OSSIM

Зважаючи на трирівневу модель мережі та викладені приклади розміщення OSSIM було складено логічну топологію невеликої мережі організації, рис.2.4.

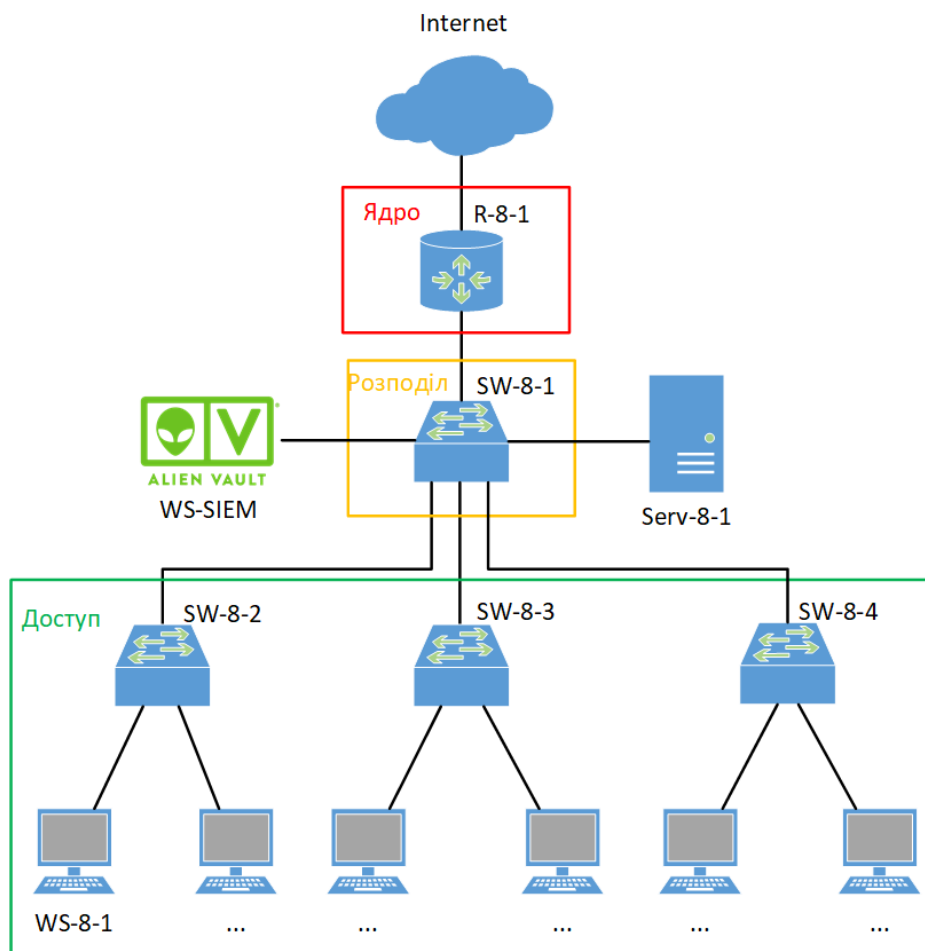


Рисунок 2.4 – Логічна топологія мережі

На рівні ядра розміщено маршрутизатор R-8-1, який забезпечуватиме доступ локальної мережі до Інтернету.

На рівні розподілу розташовано комутатор SW-8-1, який займає центральне положення в мережі та забезпечуватиме всім іншим пристроями зв'язок між собою та з маршрутизатором R-8-1. До цього ж комутатора підключений комп'ютер зі встановленою системою OSSIM (WS-SIEM) і Windows Server 2019 (Serv-8-1).

На рівні доступу розміщено комутатори SW-8-2, SW-8-3 та SW-8-4 до яких підключаються кінцеві робочі станції. Ці ж комутатори в свою чергу підключені до центрального комутатора SW-8-1 рівня розподілу.

2.2. Розробка фізичної топології мережі та адресація

Загалом в розробленій мережі задіяно 1 маршрутизатор, 4 комутатори, 1 робоча станція зі встановленою OSSIM та 30 робочих станцій. Для забезпечення зв'язку між пристроями необхідно використати дві мережі. Для каналу між маршрутизатором задіяно мережу 214.10.8.0/30, а для всіх інших пристроїв локальної мережі – 192.168.8.0/24.

Маршрутизатор, комутатори та станція з OSSIM матимуть статичні параметри адресації, а кінцеві робочі станції – динамічні. Параметри розподілу адресації між пристроями наведено на табл.2.1.

Таблиця 2.1

Параметри адресації пристроїв мережі

Мережа/Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Internet – R-8-1	–	214.8.8.0	255.255.255.252	/30
LAN	–	192.168.8.0	255.255.255.0	/24
Internet	Fa0/0	214.8.8.1	255.255.255.252	/30
Маршрутизатор R-8-1	Fa0/0	214.8.8.2	255.255.255.252	/30
	Fa0/1	192.168.8.254	255.255.255.0	/24
Комутатор SW-8-1	Інтерфейс Vlan 1	192.168.8.253	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.8.254	255.255.255.0	/24

Параметри адресації пристроїв мережі

Комутатор SW-8-2	Інтерфейс Vlan 1	192.168.8.252	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.8.254	255.255.255.0	/24
Комутатор SW-8-3	Інтерфейс Vlan 1	192.168.8.250	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.8.254	255.255.255.0	/24
Станція WS-SIEM	Eth0	192.168.8.240	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.8.254	255.255.255.0	/24
Сервер Serv-8-1	Eth0	192.168.8.240	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.8.254	255.255.255.0	/24
Робочі станції WS-8-1 – WS-8-30	Eth0	DHCP		
	Шлюз за замовчуванням			

На рис.2.5 наведена фізична топологія мережі з розташування мережевих пристроїв, розподілом робочих станцій та схемої адресації. Всі пристрої мережі належать домену ionnikov.net.

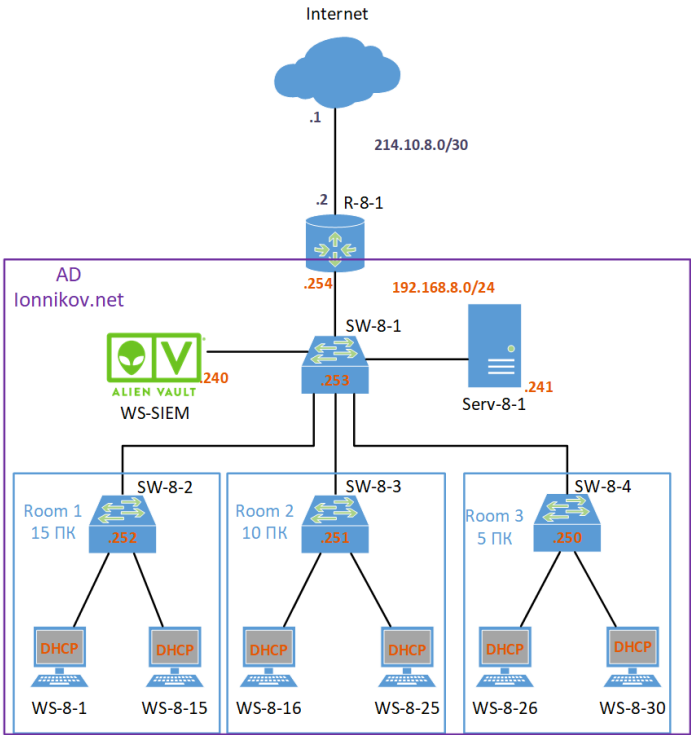


Рисунок 2.5 – Фізична топологія мережі з адресацією пристроїв та їх способом підключенням між собою

2.3. Проектування системи SIEM

AlienVault OSSIM складається з 4 основних компонентів:

- Сенсори - відповідають за збір даних з різних джерел, включаючи мережеві пристрої, сервери та інші кінцеві точки з подальшим пересиланням нормалізованих даних подій на сервер.
- Сервер – отримує дані від сенсорів, нормалізує, корелює їх та зберігає для подальшого аналізу.
- База даних – використовується MySQL для зберігання зібраних та даних, а також для зберігання конфігурацій та інших важливих налаштувань.
- Фронтенд або фреймворк – забезпечує користувачів зручним веб-інтерфейсом та консоллю для доступу до системи, конфігурації налаштувань, перегляду звітів та моніторингу стану безпеки.

Дані перераховані компоненти можна розмістити на одній фізичній машині (за замовчуванням), на одній віртуальній машині, на різних віртуальних або фізичних машинах. Все залежно від розміру та потреб мережі. Для відносно невеликої мережі, як в даному випадку, доцільним рішенням буде встановити всі компоненти на одній фізичній чи віртуальній машині, що є найпростішою конфігурацією. Сенсори ж розміщуються на кінцевих пристроях. Однак для великих мереж бажано розміщувати сервер, базу даних, фронтенд окремо.

Для сенсорів використовується два методи пересилання повідомлень на сервер:

- 1) Служба rsyslog, яка на сервері прослуховує порт TCP/UDP 514 і отримує журнали від пристроїв через цей порт.
- 2) OSSIM-агент, який встановлюється на кінцевих пристроях і здатен виконувати базовий аналіз і нормалізація журналів та подальше їх надсилання до сервера.

Найзручнішим способом передачі подій для Windows та Linux систем є використання OSSIM-агентів, оскільки вони дозволяють нормалізувати дані журналів перед їх відправкою і одним з найпоширеніших таких агентів є OSSEC

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

– хостова система виявлення вторгнень (Host-Based Intrusion Detection System , HIDS), яка відразу виконує декілька функцій:

- аналіз системних логів;
- перевірку цілісності файлів;
- перевірку цілісності реєстру (для ОС Windows);
- виявлення руткітів у системі;
- надсилання сповіщень на сервер за розкладом та за подією..

На рис.2.6. показана структура збору подій з кінцевих пристроїв в даній топології. На WS-SIEM будуть розміщувати сервер, база даних та фронтенд, а логи подій з кінцевих пристроїв та сервера в нормалізованому вигляді будуть передаватись на обробку до сервера через використання OSSEC-агентів.

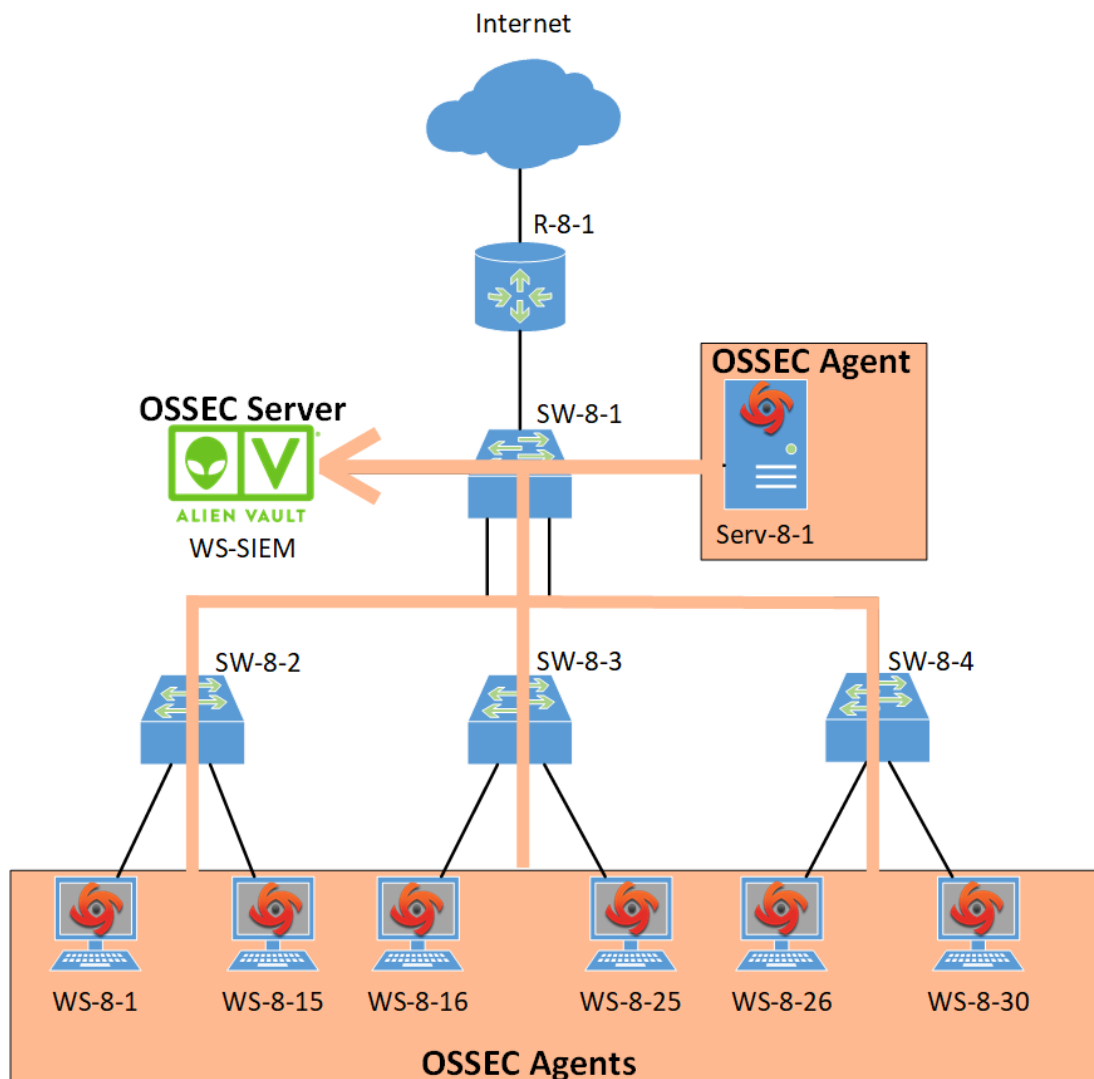


Рисунок 2.6 – Структура збору подій з кінцевих пристроїв в проєкті мережі

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4 Вибір обладнання для реалізації проєкту

Важливим моментом під час проєктування мереж, є вибір мережевого обладнання.

При виборі маршрутизатора (R-8-1) для офісу підприємства слід увагу звернути на достатню кількість інтерфейсів та високу продуктивність. Ці перераховані вимоги може задовільнити маршрутизатор від компанії Cisco, а саме ISR4221/K9, рис.2.7 [18]. Дана модель призначена для обслуговування невеликих та середніх організацій. Даний пристрій має високу продуктивність передачі даних від 50 Мбіт/с до 2 Гбіт/с, вбудовані WAN порти Gigabit Ethernet і SFP порти. Об'єм оперативної пам'яті складає 4 ГБ (доступне розширення до 8 ГБ), а обсяг флеш-пам'яті за замовчуванням 8 ГБ. Пристрій підтримує підключення уніфікованими портами USB 2.0. Також перевагами моделі є низька температура експлуатації – від 0 до 40 градусів за Цельсієм та низьке енергоспоживання – від 100 до 240 Вт. Дана модель підтримує функцію резервного живлення.



Рисунок 2.7 – Маршрутизатор Cisco ISR4221/K9

При виборі комутаторів слід звернути увагу, щоб вони забезпечувала гарну продуктивність та підтримували стандарт FastEthernet. Ці вимоги може задовольнити комутатор моделі Cisco WS-C2960-24PC-S, рис.2.8 [19]. Пристрої Cisco Catalyst 2960 серії є лінійкою комутаторів з фіксованою конфігурацією та портами Fast Ethernet та Gigabit Ethernet, що мають розширені LAN сервіси для

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

підприємств початкового та середнього рівня. Комутатори Cisco Catalyst 2960 підтримують передачу голосу, даних та відео, а також безпечний доступ. Крім того, вони мають комбіновані гігабітні аплінки, підтримують QoS, покроковий Rate Limiting, ACL, multicast services, можливість регулювати швидкість передачі на кожному порту з кроком 64 кбіт, Link Aggregation, 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID.



Рисунок 2.8 – Комутатор Cisco WS-C2960-24PC-S

Для кінцевих користувачів обрано робочі станції з операційною системою Windows 10. Це забезпечить сумісність з більшістю актуальних корпоративних програм, інтеграцію з Active Directory та забезпечить належний рівень безпеки та продуктивності.

Рекомендовані системні вимоги для комп'ютерів з Windows 10:

- Процесор: Intel Core i5 або еквівалентний;
- Оперативна пам'ять: 8 ГБ RAM (рекомендовано 16 ГБ для більшої продуктивності);
- Жорсткий диск: 256 ГБ SSD (рекомендовано 512 ГБ SSD для швидшого доступу до даних);
- Графіка: Інтегрована або дискретна графічна карта;
- Операційна система: Windows 10 Pro або Enterprise.

На роль сервера (Serv-8-1) буде використовуватись Windows Server 2019. Дана операційна система дозволить реалізувати широкі можливості для управління мережею, розгортанню Active Directory і забезпечення високого рівня безпеки.

Рекомендовані системні вимоги для сервера:

- Процесор: 2.0 ГГц або швидший, 64-розрядний процесор (двоядерний або багатоядерний)

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

- Оперативна пам'ять: 16 ГБ RAM (рекомендовано 32 ГБ для кращої продуктивності)

- Жорсткий диск: 1 ТБ HDD (рекомендовано 1 ТБ SSD для швидшого доступу до даних)

- Мережева карта: Gigabit Ethernet адаптер

- Операційна система: Windows Server 2019 Standard або Datacenter.

AlienVault OSSIM постачається як готовий образ (ISO-файл) з попередньо налаштованою операційною системою на базі Debian, тому для нього не потрібно попередньо встановлювати спеціальні додаткові пакети чи проводити будь-які інші налаштування системи. AlienVault OSSIM також можна розгорнути у віртуальному середовищі, якщо це відповідає вимогам інфраструктури. В будь-якому випадку для розгортання OSSIM рекомендовано використовувати комп'ютер з наступними мінімальними системними вимогами:

- Процесор: 4-ядерний процесор (Intel Xeon або еквівалент)

- Оперативна пам'ять: 8 ГБ RAM

- Жорсткий диск: 250 ГБ HDD або SSD

- Мережева карта: 1 Gigabit Ethernet адаптер

Висновки до 2 розділу

В ході виконання даного розділу було проведено розробку логічної топології мережі проєкту з дотриманням трирівневої ієрархічної моделі мережі, що включає рівень ядра, розподілу, доступу. Даний підхід спрощує управління, покращує безпеку та легко масштабувати. Систему SIEM (AlienVault OSSIM) буде розміщено в центрі мережі, щоб забезпечити максимальний охоплення та доступ до інформації про події з усіх частин мережі.

Було визначено необхідну кількість мережевого обладнання для організації проєкту та розроблено схему адресації зважаючи на необхідну кількість пристроїв. Визначено пристрої, які матимуть статичні параметри адресації та наведено фізичну топологію мережі.

Виконано проєктування системи SIEM, що включало аналіз компонентів AlienVault OSSIM, способи розміщення компонентів системи в мережі, методи

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

збору та передачі даних до серверу для подальшого опрацювання та основні функції OSSEC в ролі агента.

Обґрунтовано вибір необхідних моделей для маршрутизатора та комутаторів з урахування потреби проєкту мережі, а саме Cisco ISR4221/K9 та Cisco WS-C2960-24PC-S. Для кінцевих користувачів обрано робочі станції з ОС Windows 10, для сервера комп'ютер з ОС Windows Server 2019, а для AlienVault OSSIM підійде, як фізичний так і віртуальний комп'ютер без прив'язки до ОС, оскільки AlienVault постачається як готовий образ (ISO-файл) з попередньо налаштованою операційною системою на базі Debian.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1 Налагодження пристроїв мережі

Безпосереднє налаштування проєкту і демонстрацію роботи мережі буде виконано з використанням емулятора мережі GNS3 в поєднанні з гіпервізором VirtualBox. При цьому кількість кінцевих пристроїв, в порівнянні зі схемою з другого розділу, буде дещо зменшена у зв'язку з технічними можливостями комп'ютера на якому виконуватиметься емуляція проєкту. Параметри адресації лишаються такими ж, як і в розділі 2.1. На табл.3.1 наведено параметри з'єднання пристроїв в спроектованій мережі.

Таблиця 3.1

1 Параметри підключення пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Internet	Fa0/0	R-8-1	Fa0/0
Маршрутизатор R-8-1	Fa0/0	Internet	Fa0/0
	Fa0/1	SW-8-1	Eth3/3
Комутатор SW-8-1	Eth0/0	WS-SIEM	Eth0
	Eth0/1	Serv-8-1	Eth0
	Eth3/0	SW-8-4	Eth3/3
	Eth3/1	SW-8-3	Eth3/3
	Eth3/2	SW-8-2	Eth3/3
	Eth3/3	R-8-1	Fa0/1
Комутатор SW-8-2	Eth0/0	WS-8-1	Eth0
	Eth0/1	WS-8-2	Eth0
	Eth3/3	SW-8-1	Eth3/2
Комутатор SW-8-3	Eth0/0	WS-8-3	Eth0
	Eth0/1	WS-8-4	Eth0
	Eth3/3	SW-8-1	Eth3/1
Комутатор SW-8-4	Eth0/0	WS-8-5	Eth0
	Eth0/1	WS-8-6	Eth0
	Eth3/3	SW-8-1	Eth3/0

На рис.3.1 продемонстрована топологія мережі в GNS3.

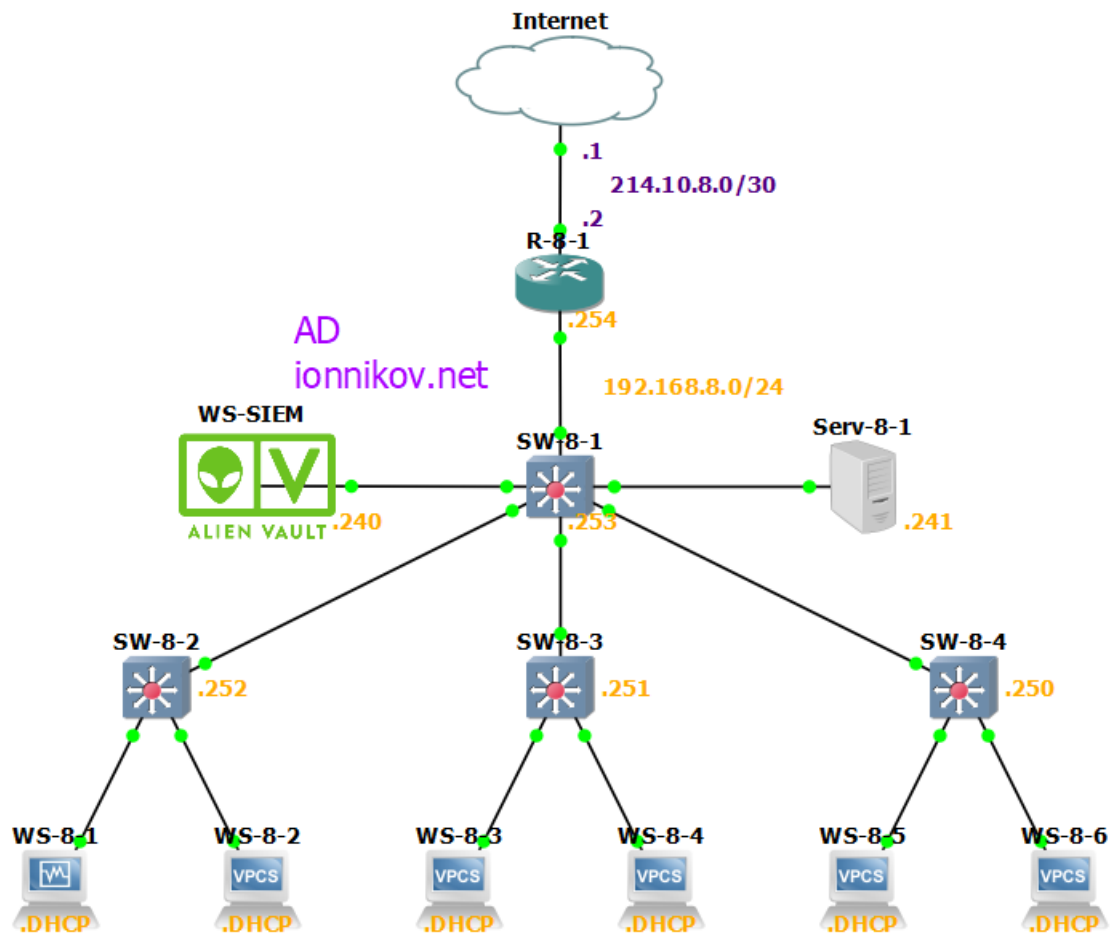


Рисунок 3.1 – Топологія проєкту в мережевому емуляторі GNS3

Налагодження розпочато з налаштування маршрутизатора R-8-1. На R-8-1 налаштовуються адресація, маршрутизація, адреса DNS-серверу та належність до домену, рис.3.2.

```
R-8-1(config)#ip route 0.0.0.0 0.0.0.0 214.10.8.1
R-8-1(config)#ip name-server 192.168.8.241
R-8-1(config)#ip domain-name ionnikov.net
R-8-1(config)#int fa0/0
R-8-1(config-if)#description link-to-internet
R-8-1(config-if)#ip address 214.10.8.2 255.255.255.252
R-8-1(config-if)#no shutdown
R-8-1(config-if)#exit
R-8-1(config)#int fa0/1
R-8-1(config-if)#description link-to-sw-8-1
R-8-1(config-if)#ip address 192.168.8.254 255.255.255.0
R-8-1(config-if)#no shutdown
```

Рисунок 3.2 – Налагодження маршрутизатора R-8-1

Далі переходимо на налаштувань комутаторів. На них слід призначити адресу Vlan 1, задати шлюз за замовчуванням, адрес DNS-серверу і належність до домену. На рис.3.3 наведено налаштування для SW-8-1, але інші комутатори налаштовуються тим же чином.

```
SW-8-1(config)#int vlan 1
SW-8-1(config-if)#ip address 192.168.8.253 255.255.255.0
SW-8-1(config-if)#no shutdown
SW-8-1(config-if)#exit
SW-8-1(config)#ip default-gateway 192.168.8.254
SW-8-1(config)#ip name-server 192.168.8.241
SW-8-1(config)#ip domain-lookup
SW-8-1(config)#ip domain-name ionnikov.net
```

Рисунок 3.3 – Налагодження комутатора SW-8-1

І налаштовуємо базові засоби захисту мережевих пристроїв, що включає створення користувача, встановлення паролю на вхід в привілейований режим та налаштування роботи SSH, рис.3.4.

```
R-8-1(config)#username admin privilege 15 secret admin4ik-pass
R-8-1(config)#enable secret enable-pass
R-8-1(config)#line cons 0
R-8-1(config-line)#login local
R-8-1(config-line)#exit
R-8-1(config)#access-list 1 permit 192.168.8.241 0.0.0.255
R-8-1(config)#line vty 0 15
R-8-1(config-line)#transport input ssh
R-8-1(config-line)#login local
R-8-1(config-line)#access-class 1 in
R-8-1(config-line)#exit
R-8-1(config)#crypto key generate rsa modulus 1024
% You already have RSA keys defined named R-8-1.ionnikov.net.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R-8-1(config)#ip ssh version 2
R-8-1(config)#ip ssh time-out 30
```

Рисунок 3.4 – Налагодження користувача, паролю, входу, SSH

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Тепер переходимо до налаштувань Windows Server 2019, тобто до сервера Serv-8-1. Перш за все налаштовується адресація, рис.3.5.

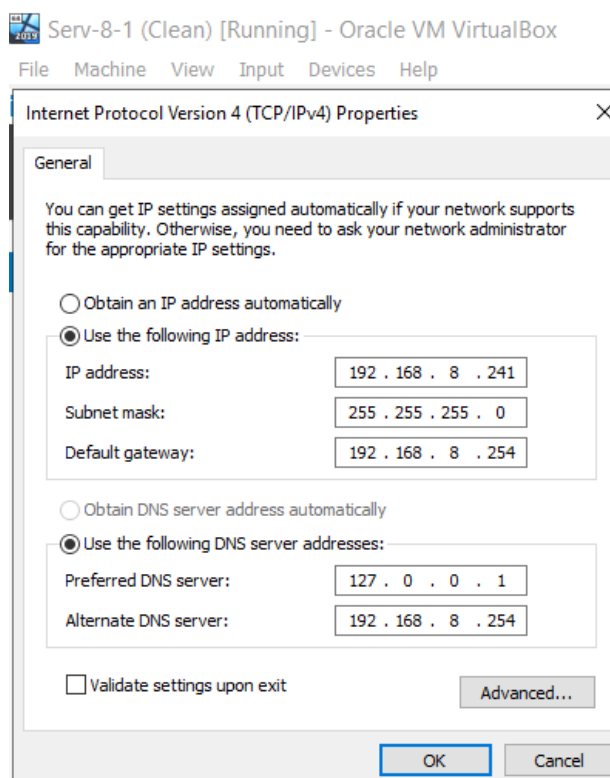


Рисунок 3.5 – Налаштування адресації на Serv-8-1

Тепер можна перейти до ініціалізації роботи Active Directory, додання необхідних ролей та створення домену ionnikov.net, рис.3.6 і рис.3.7.

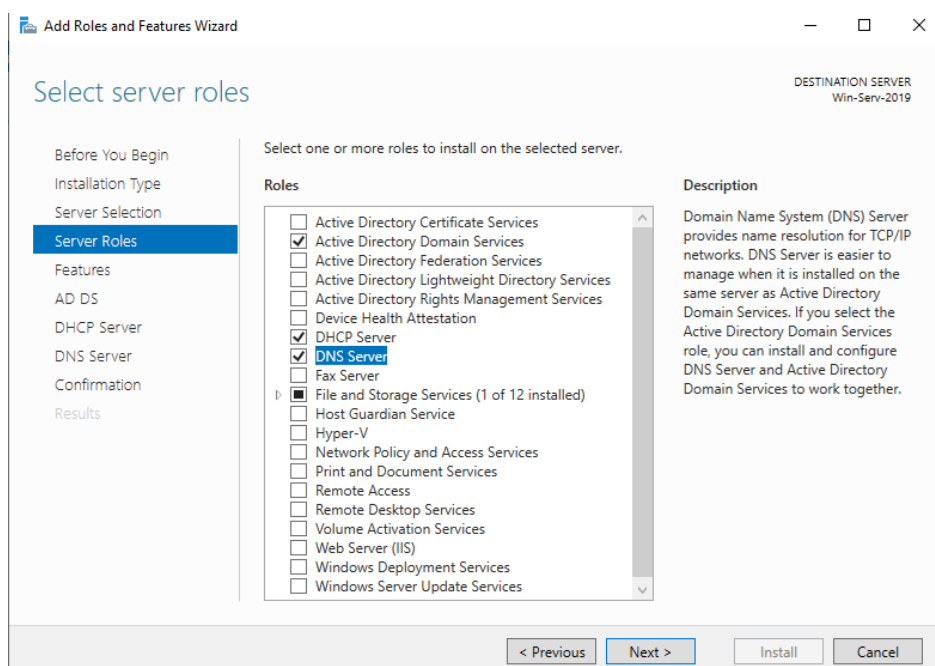


Рисунок 3.6 – Додання необхідних ролей

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

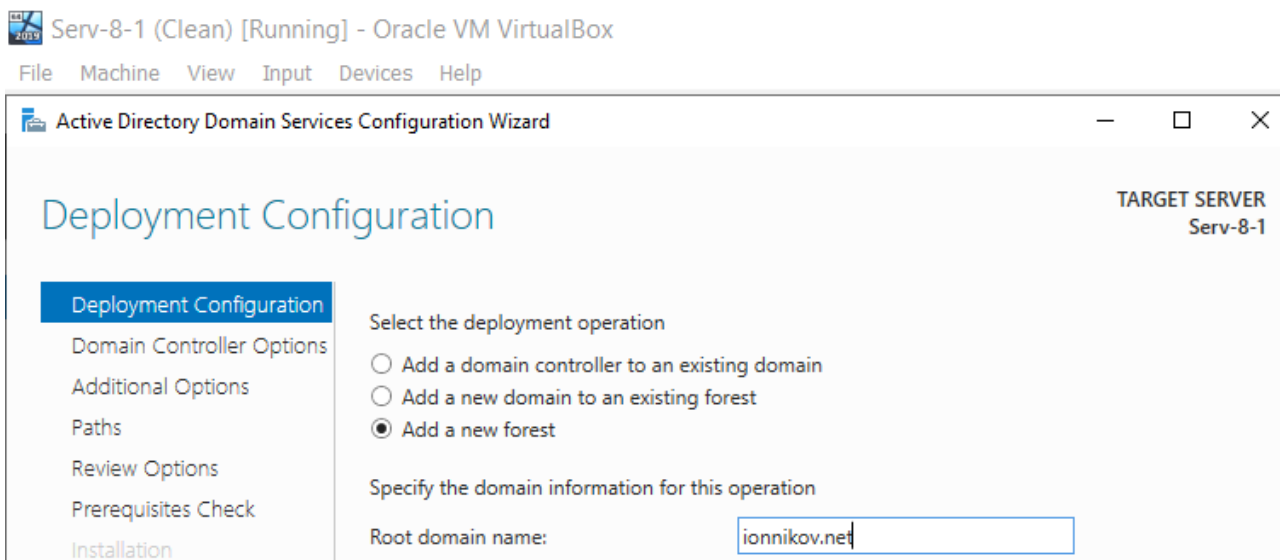


Рисунок 3.7 – Створення домену ionnikov.net на Serv-8-1

Тепер необхідно створити та налаштувати DHCP-сервер для того, щоб робочі станції могли автоматично отримувати IP-адреси. Для цього я створюється область під назвою "lan-scope", рис. 3.8.

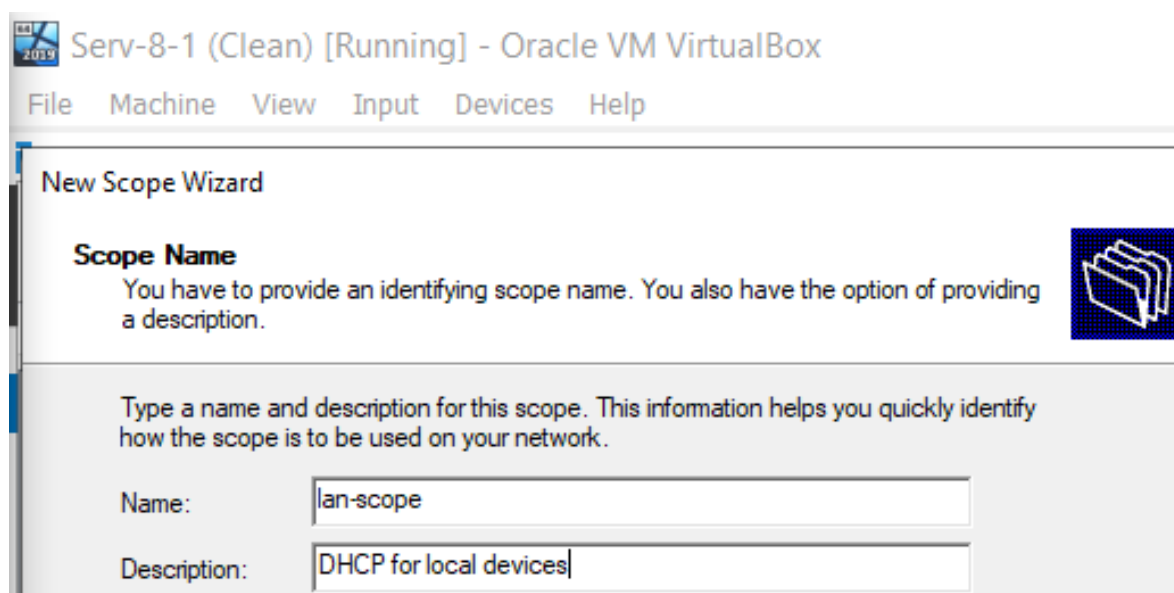


Рисунок 3.8 – Створення області lan-scope

І тепер налаштовується діапазон роздачі адрес, шлюз за замовчуванням та адреси DNS-серверів, рис.3.9 – 3.12.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Serv-8-1 (Clean) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 8 . 1

End IP address: 192 . 168 . 8 . 254

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Рисунок 3.9 – Задання діапазону роздачі адрес

Serv-8-1 (Clean) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

New Scope Wizard

Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address:

Add

Excluded address range:

192.168.8.240 to 192.168.8.254

Remove

Subnet delay in milli second:

0

< Back Next > Cancel

Рисунок 3.10 – Виключення статичних адрес з пулу

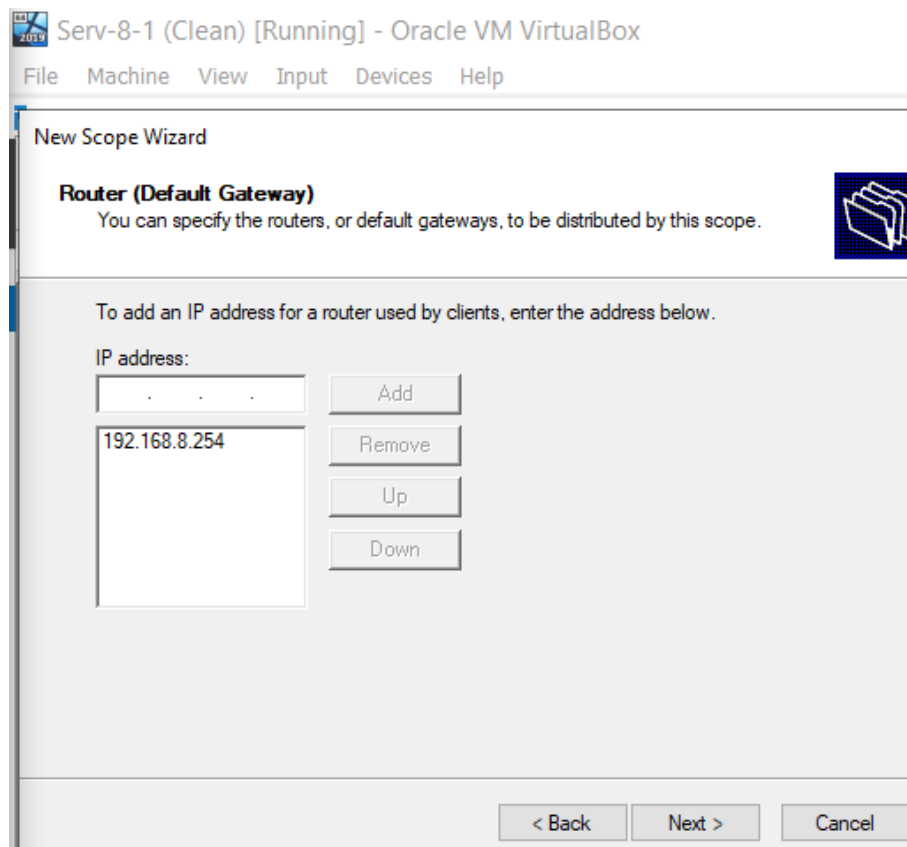


Рисунок 3.11 – Додання шлюзу за замовчуванням

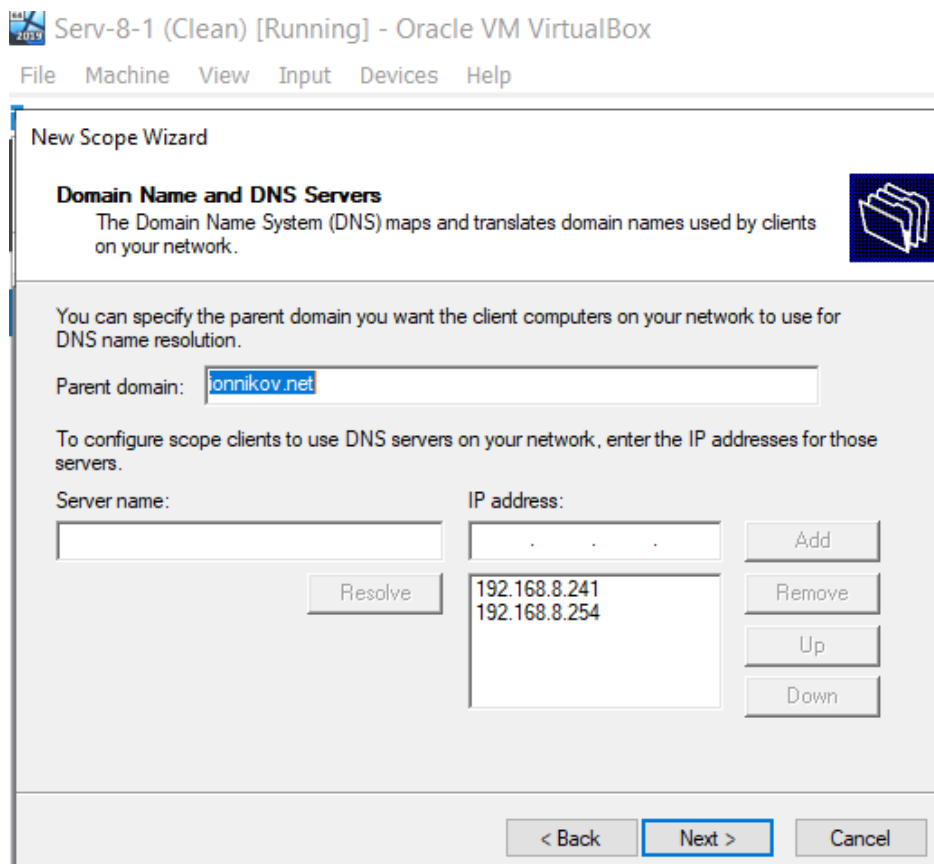


Рисунок 3.12 – Додання DNS серверів

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Тепер слід створити облікові записи користувачів, які будуть використовуватися на кінцевих пристроях. На рис.3.13 наведено приклад створення одного з таких записів.

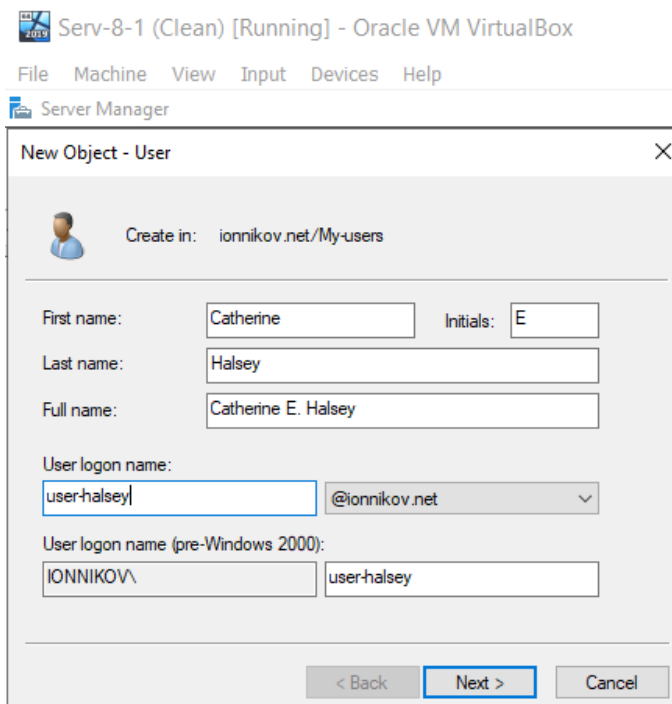


Рисунок 3.13 – Створення облікового запису користувача

Тепер можна виконати приєднання робочих станцій до домену ionnikov.net. На рис.3.14 показано приклад такого налагодження для WS-8-1.

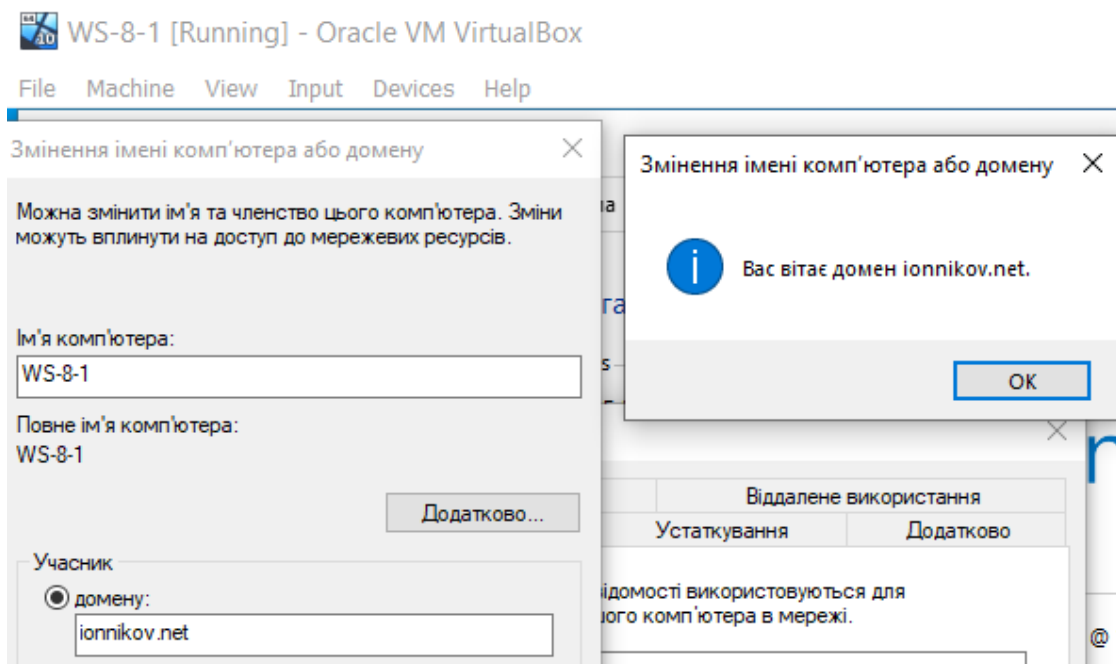


Рисунок 3.13 – Приєднання комп'ютера WS-8-1 до домену ionnikov.net

Тепер переходимо до WS-SIEM [20]. Заздалегідь на даному комп'ютері було виконано встановлення Alien Vault OSSIM використовуючи завантажений .iso файл. Процес інсталяції є досить інтуїтивним і не потребує окремих пояснень. Якщо встановлення пройшло успішно, то побачимо подібне вікно, де необхідно ввести облікові дані для входу, рис.3.15. За замовчуванням логін root, а пароль був налаштований під час встановлення OSSIM.

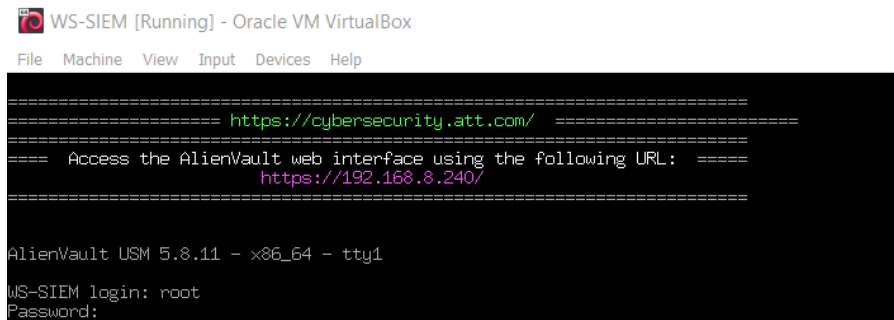


Рисунок 3.15 – Аутентифікація на WS-SIEM

Якщо дані було введено правильно, то потрапляємо в головне вікно OSSIM. В самому низу вікна наведено веб-адресу за якою можна потрапити у веб-інтерфейс OSSIM, рис.3.16. Крім цього, тут можна виконати деякі базові налаштування, але основні налаштування вже виконуватимуться з використанням веб-інтерфейсу.

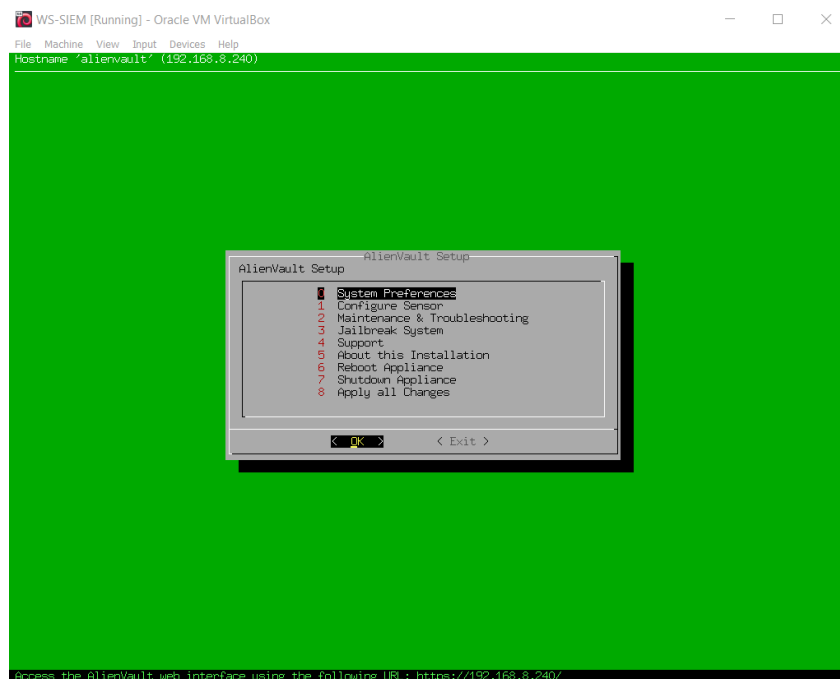


Рисунок 3.16 – Головне вікно консолі OSSIM

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Налаштування роботи SIEM

Для подальшої роботи з налаштування SIEM необхідно скористатися будь-якою наявний комп’ютером в мережі, в даному випадку це буде Serv-8-1. Використовуючи будь-який доступний браузер (для прикладу Microsoft Edge) необхідно перейти за адресою веб-інтерфейсу OSSIM, тобто `https://192.168.8.240`. Якщо з’явиться повідомлення про незахищене підключення, то ігноруємо, оскільки зараз використовується самопідписаний сертифікат. В отриманому вікні необхідно заповнити власні персональні дані адміністратора, що включає ім’я, логін, пароль, назву компанія, рис.3.17.

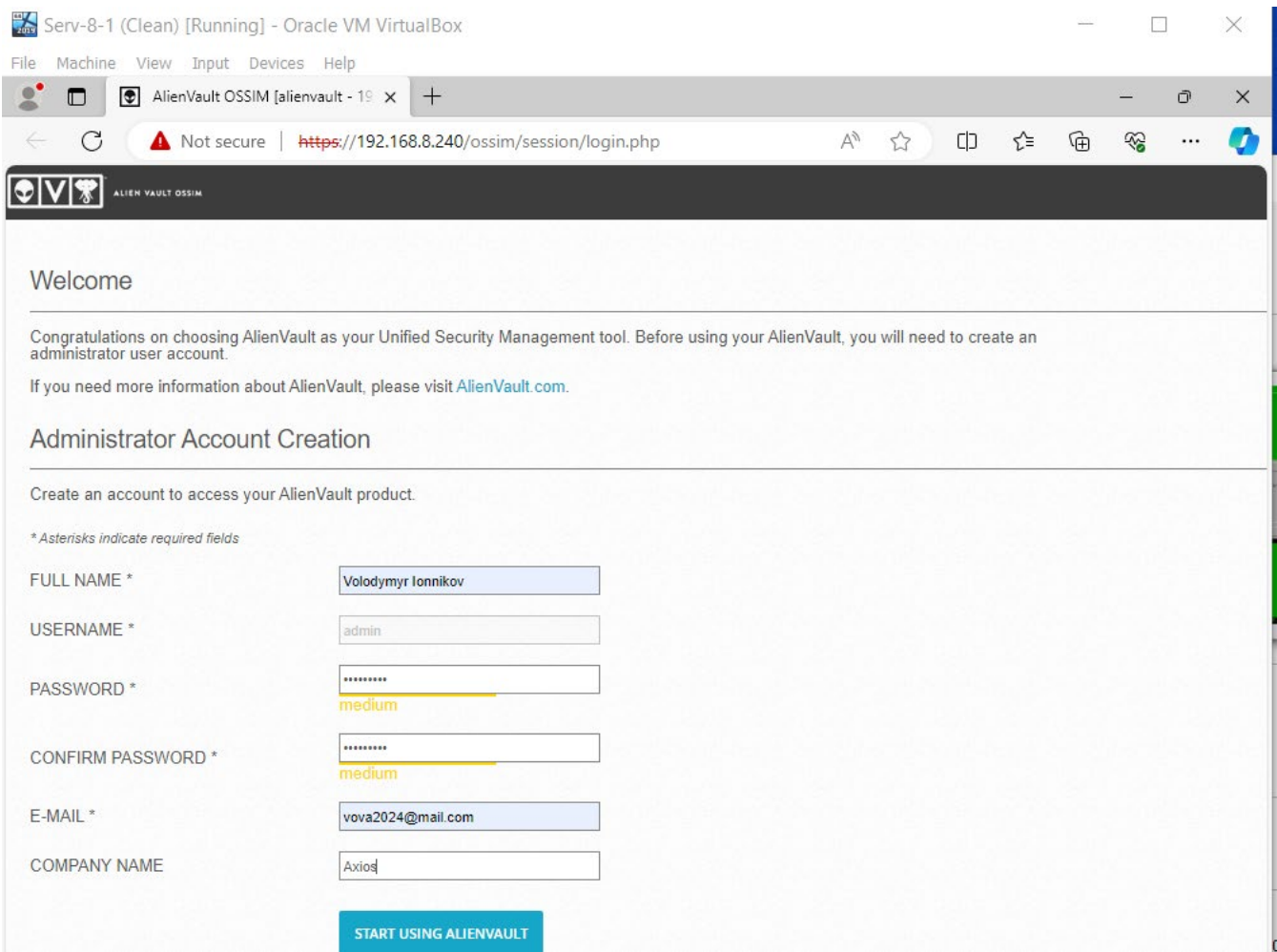


Рисунок 3.17 – Заповнення облікових даних адміністратора

І тепер слід використати створені облікові дані для входу в систему, рис.3.18.

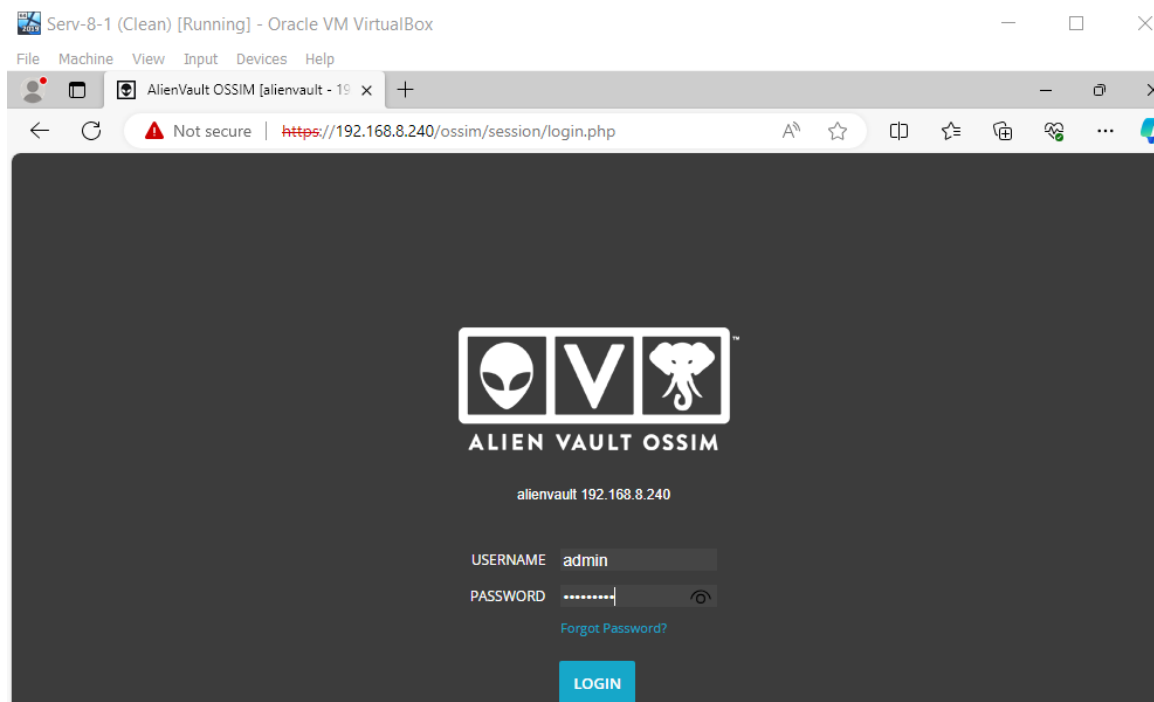


Рисунок 3.18 – Аутентифікація в веб-інтерфейсі

При вході в систему нас зустрічає майстер-налаштувань (Started Wizard).
Погоджуємось натискаючи кнопку «Start», рис.3.19.

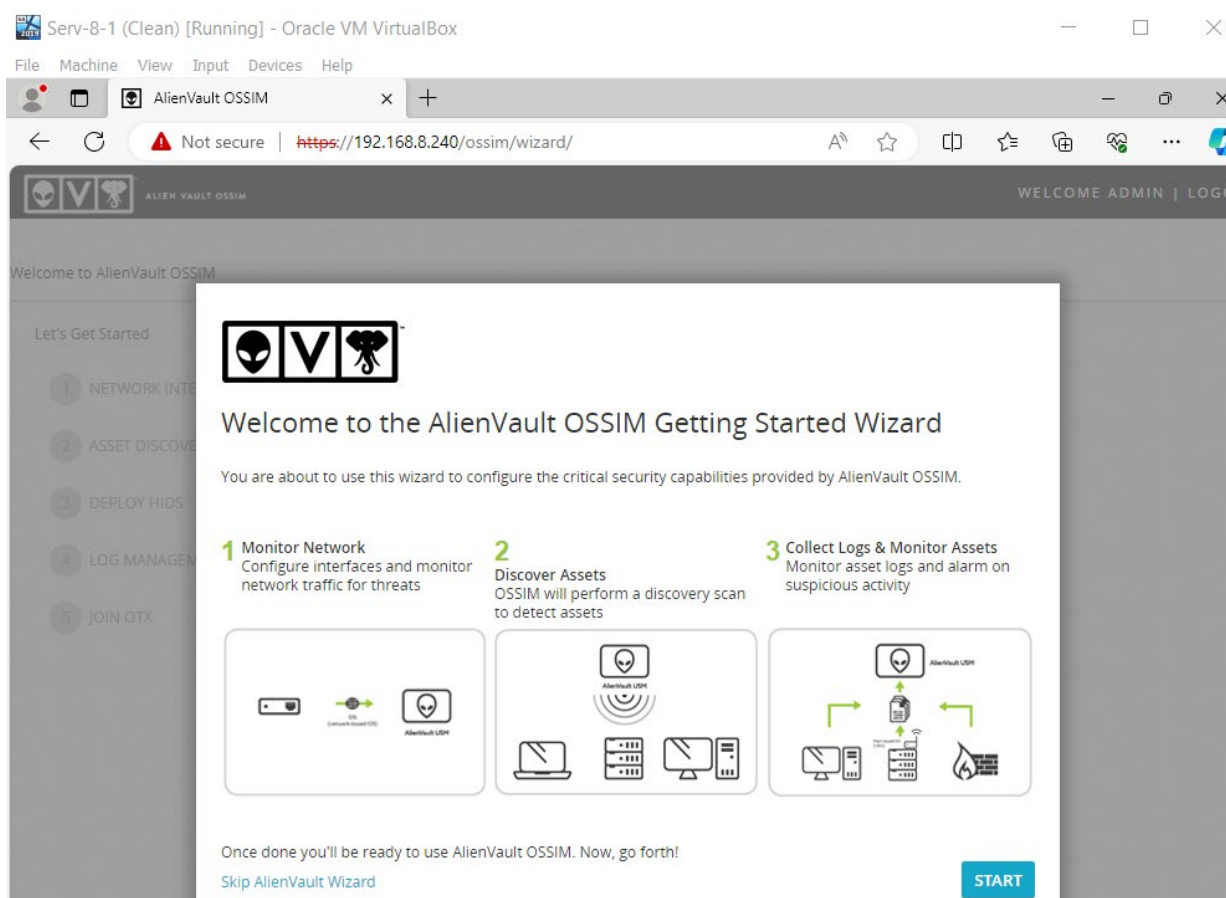


Рисунок 3.19 – Майстер налаштувань

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

На першому кроці можна переглянути встановлені інтерфейси на WS-SIEM, рис.3.20. За замовчуванням нічого змінювати не треба і переходимо далі.

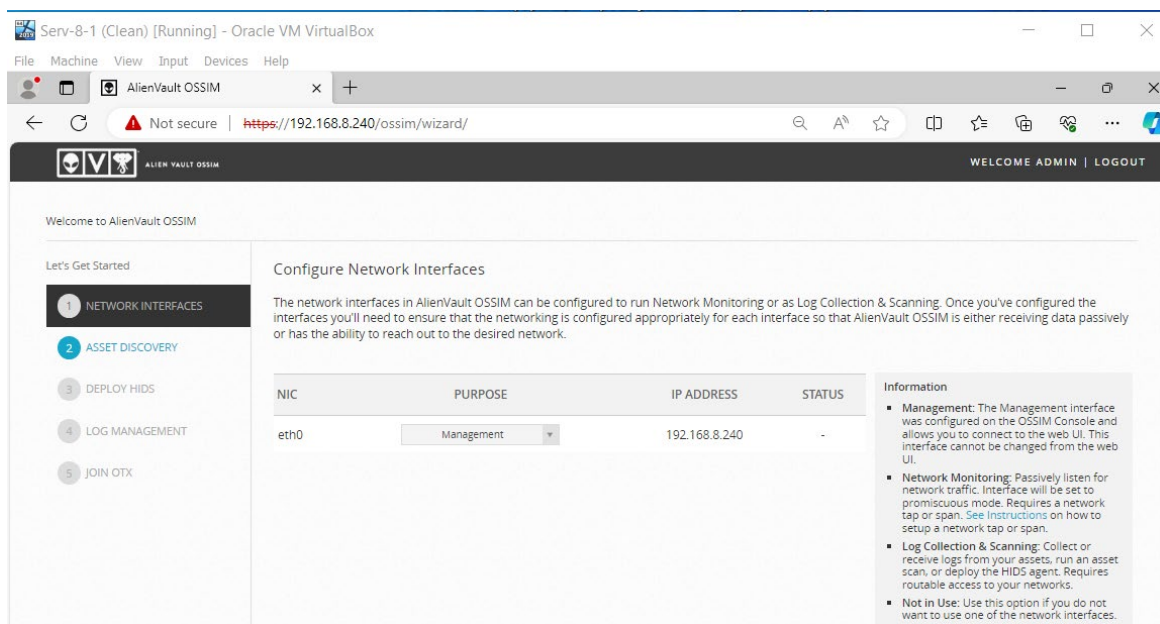


Рисунок 3.20 – Параметри мережевих інтерфейсів WS-SIEM

Наступним етапом нам пропонується додати наявне обладнання в мережі до відстеження. Перш за все слід виконати сканування мережі на виявлення всіх об'єктів, рис.3.21. Але також можна вручну додати всі необхідні пристрої, якщо відомі їх IP-адреси.

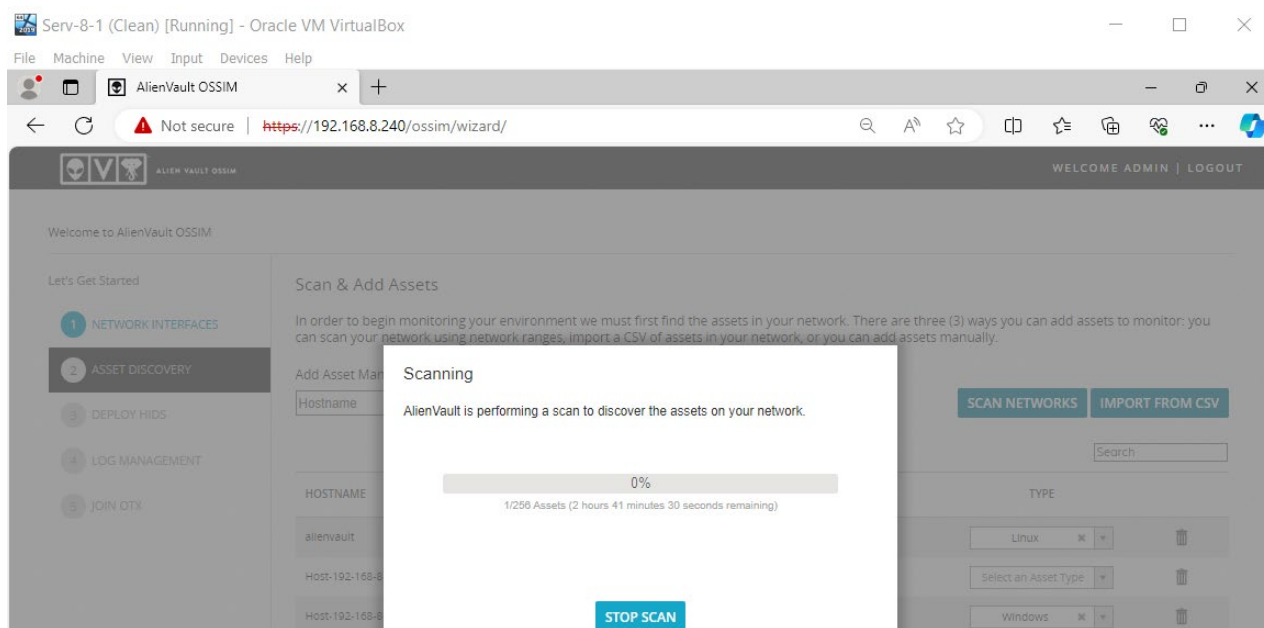


Рисунок 3.21 – Виявлення активів (пристроїв) в мережі

Після ідентифікації всіх пристроїв необхідно кожному з них задати його тип (Windows, Linux або мережевий пристрій) рис.3.22. Наступні етапи майстра-налаштувань можна пропустити.

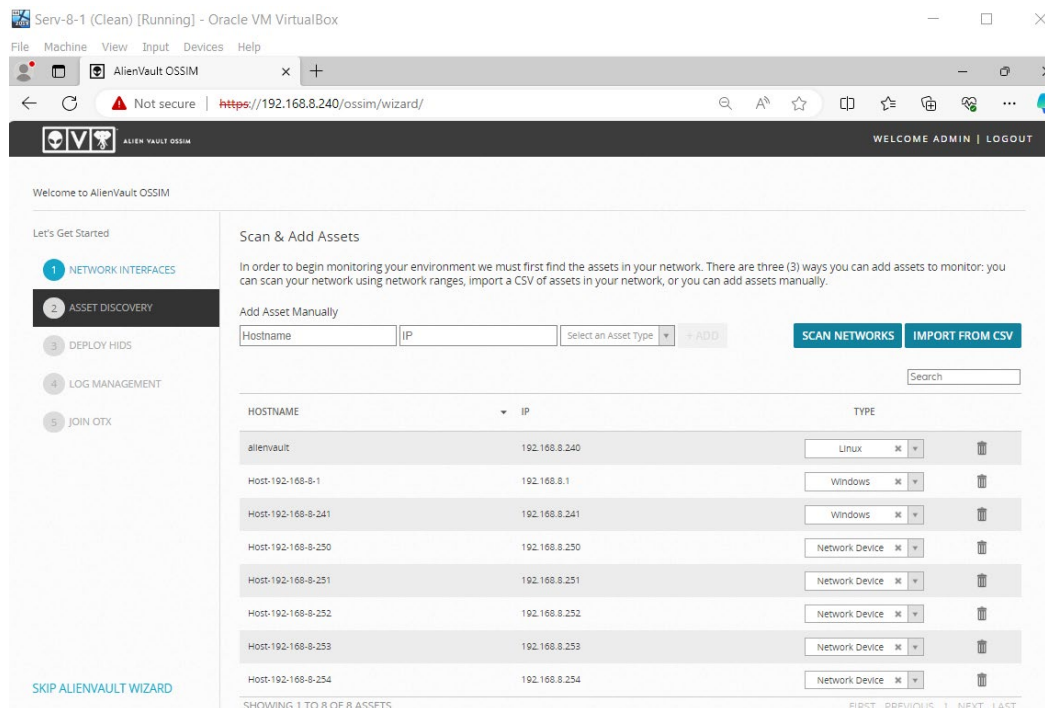


Рисунок 3.22 – Виявлені пристрої мережі

Після цього вже безпосередньо потрапляємо в головне меню OSSIM, рис.3.23.

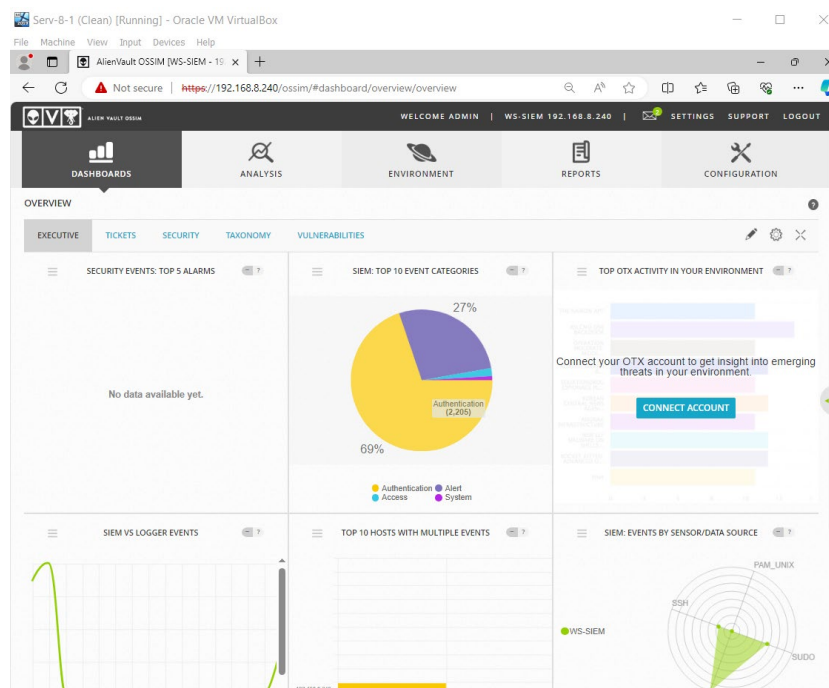


Рисунок 3.23 – Головне меню OSSIM

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Перейдемо в пункт «Environment» - «Asset & Groups». Тут відображені раніше додані пристрої мережі. Для полегшення адміністрування доцільно для кожного з об'єктів вказати детальну інформацію: тип пристрою, його ім'я та операційну систему, рис.3.24.

☐	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS	
☐	WS-SIEM	192.168.8.240		AllenVault OS	2	No	Connected	
☐	WS-8-1	192.168.8.1	Endpoint:Workstation	Microsoft Windows 10 64-bit	2	No	Not Deployed	
☐	SW-8-4	192.168.8.250	Network Device:Switch	Cisco IOS	2	No	Not Deployed	
☐	SW-8-3	192.168.8.251	Network Device:Switch	Cisco IOS	2	No	Not Deployed	
☐	SW-8-2	192.168.8.252	Network Device:Switch	Cisco IOS	2	No	Not Deployed	
☐	SW-8-1	192.168.8.253	Network Device:Switch	Cisco IOS	2	No	Not Deployed	
☐	Serv-8-1	192.168.8.241	Server	Microsoft Windows Server 2019 Standard Edition on x64	2	No	Not Deployed	
☐	R-8-1	192.168.8.254	Network Device:Router	Cisco IOS	2	No	Not Deployed	

SHOWING 1 TO 8 OF 8 ASSETS

Рисунок 3.24 – Перелік всіх доданих пристрої мережі

Можна виконати розподіл пристроїв по групах в розділі «Asset Groups» для зручного використання та їх пошуку, рис.3.25.

☐	NAME	OWNER(S)	ASSETS	ALARMS	VULNERABILITIES	EVENTS	
☐	Servers		1	-	-	-	
☐	Network devices		5	-	-	-	
☐	Endpoints		1	-	-	-	

SHOWING 1 TO 3 OF 3 GROUPS

Рисунок 3.25 – Розподіл пристроїв по групах Servers, Network devices, Endpoints

Переходимо в пункт «Environment» - «Agents» – «Agent Control». За замовчуванням тут вже встановлений агент для WS-SIEM, однак слід його додати і для Windows систем. Для цього необхідно натиснути кнопку «Add Agent» і обрати необхідні пристрої, в даному випадку це WS-8-1 та Serv-8-1, рис.3.26.

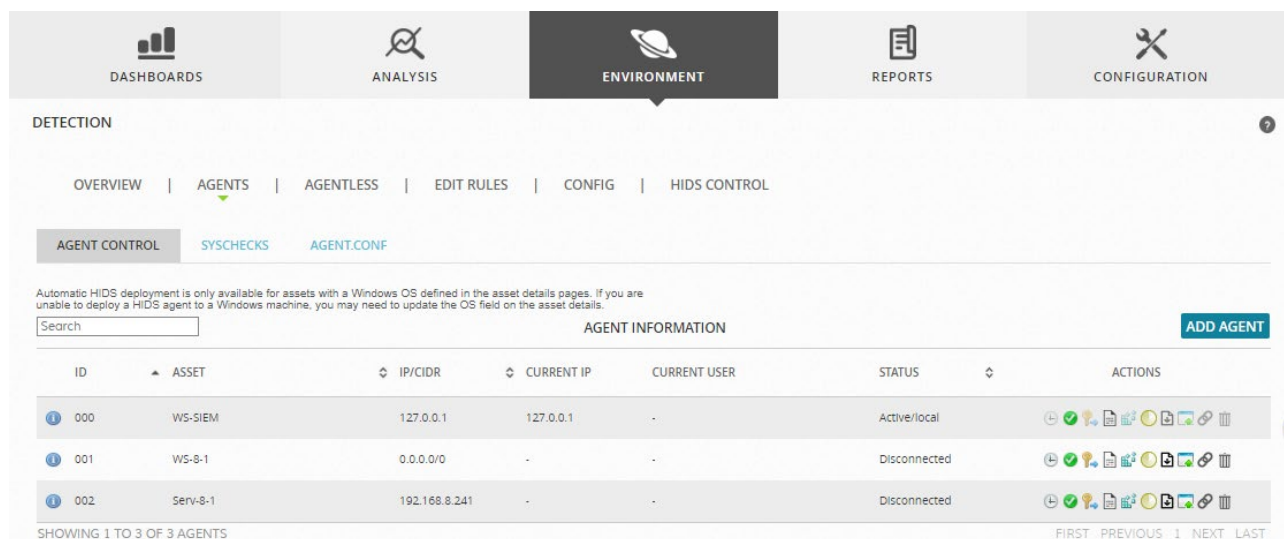


Рисунок 3.26 – Створення агентів для Windows пристроїв

В меню «Actions» для об'єкту Serv-8-1 (з якого зараз відбувається підключення до веб-інтерфейсу OSSIM) натискаємо на відповідну кнопку в колонці «Actions», яка завантажить вже налаштований агент для цього девайсу, рис.3.27.

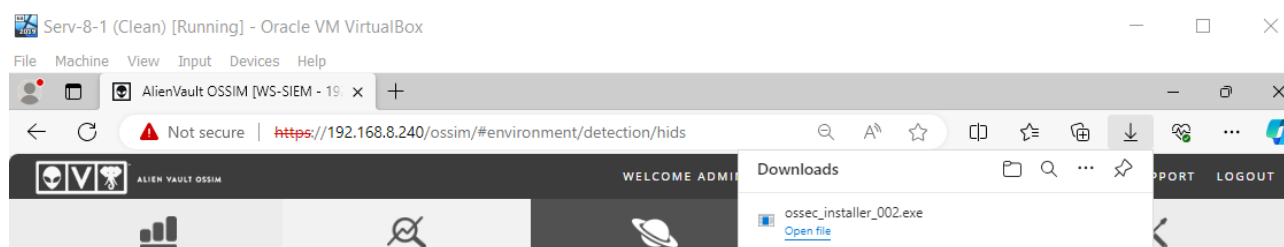


Рисунок 3.27 – Завантаження агента для Serv-8-1

Після запуску файлу виконуємо встановлення і запускаємо агент, рис.3.28 і рис.3.29.

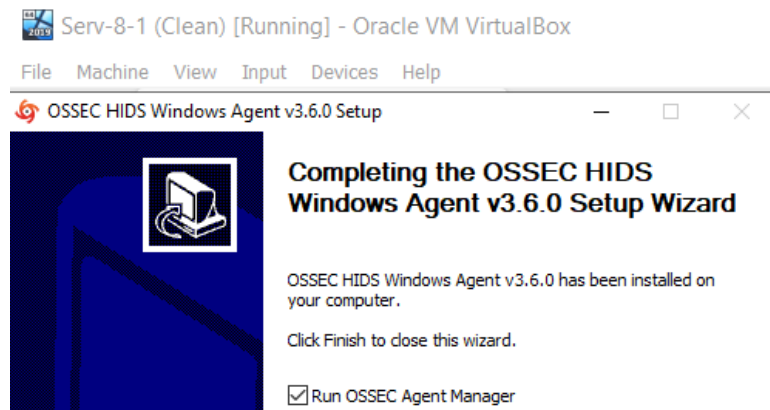


Рисунок 3.28 – Успішне встановлення агента на Serv-8-1

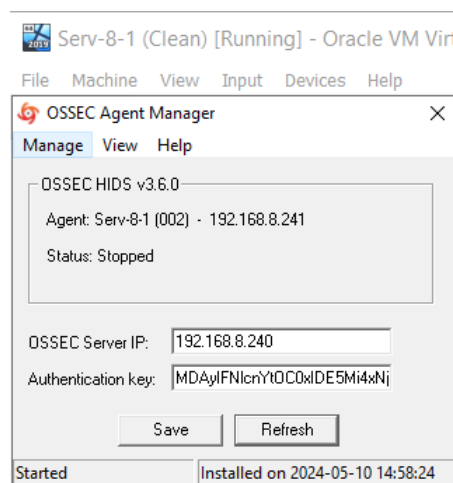


Рисунок 3.29 – Запущений агент на Serv-8-1

Якщо все було виконано правильно, то навпроти відповідних пристроїв з'явиться статус «Active», рис.3.30. Аналогічно встановлення відбувається і для всіх інших пристроїв з ОС Windows. Також є можливість скачувати налаштований агент на один пристрій і вручну виконувати його перенесення на інший, все залежить від вподобань адміністратора.

Automatic HIDS deployment is only available for assets with a Windows OS defined in the asset details pages. If you are unable to deploy a HIDS agent to a Windows machine, you may need to update the OS field on the asset details.

Search

AGENT INFORMATION

ADD AGENT

ID	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	WS-SIEM	127.0.0.1	127.0.0.1	-	Active/local	      
001	WS-8-1	0.0.0.0/0	-	-	Active	      
002	Serv-8-1	192.168.8.241	192.168.8.241	-	Active	      

Рисунок 3.30 – Агенти на Serv-8-1 та WS-8-1 успішно працюють і передають дані

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Повернувшись в пункт «Environment» - «Assets» помітимо, що інформація про події зі Serv-8-1 та WS-8-1 починають надходити до нашої системи, рис.3.31. Значить додання агентів було виконано правильно.

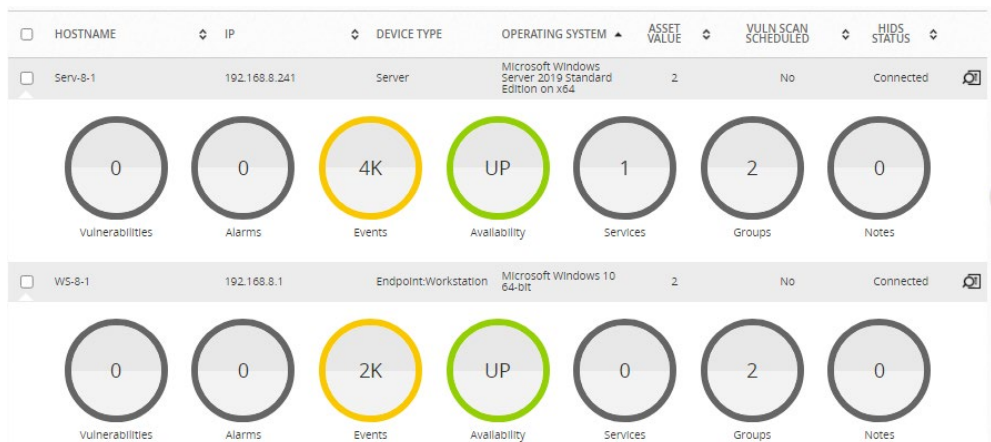


Рисунок 3.31 – Події зі Serv-8-1 та WS-8-1 успішно передаються до систем

Функція сканування вразливостей в AlienVault OSSIM дозволяє сканувати та оцінювати системи, програми та пристрої на відомі вразливості. При цьому використовується велика база даних сигнатур вразливостей, яка постійно оновлюється. AlienVault OSSIM надає докладні звіти та сповіщення, що дозволяє фахівцям із безпеки визначати пріоритети та ефективно усувати вразливості. Тому з цією метою на OSSIM буде налаштований графік щоденного сканування для робочої станції та сервера, рис.3.32.

Рисунок 3.32 – Налаштування графіку щоденного сканування пристроїв

Лишається налаштувати параметри виконання бекапів, рис.3.33 та створити сам бекап системи OSSIM, рис.3.34.

WELCOME ADMIN | WS-SIEM 192.168.8.240 | SETTINGS SUPPORT LOGOUT

DASHBOARDS ANALYSIS ENVIRONMENT REPORTS CONFIGURATION

ADMINISTRATION

USERS MAIN BACKUPS

BACKUP

Find Word SEARCH

ENABLE DESKTOP NOTIFICATIONS

UPDATE CONFIGURATION

Backup configuration: backup database, directory, interval

Enable SIEM database backup Yes

Allowed free disk space for the SIEM backups 10%

Number of Backup files to keep in the filesystem 5

Events to keep in the Database (Number of days) 5

Events to keep in the Database (Number of events) 4000000

Backup start time 01:00

Active Netflow Window 45

Alarms Expire Yes

Alarms Lifetime 90

Logger Expiration No

Active Logger Window 0

Password to encrypt backup files

Рисунок 3.33 – Налаштування параметрів бекапів

WELCOME ADMIN | WS-SIEM 192.168.8.240 | SETTINGS SUPPORT LOGOUT

DASHBOARDS ANALYSIS ENVIRONMENT REPORTS CONFIGURATION

ADMINISTRATION

USERS MAIN BACKUPS

EVENTS | CONFIGURATION

VIEW BACKUP LOGS

Search

AlienVault Configuration Backups

Show Backups for: WS-SIEM [192.168.8.240]

Backup History

	SYSTEM	DATE	BACKUP	TYPE	VERSION	SIZE	DOWNLOAD
☐	WS-SIEM (192.168.8.240)	2024-06-17 16:50:23	Configuration	Manual	OSSIM 5.8.11	22.61 MB	

SHOWING 1 TO 1 OF 1 BACKUP FILES

Backup Actions

RUN BACKUP NOW

Рисунок 3.34 – Створений бекап OSSIM

3.2 Перевірка функціонування мережі

Спершу на Windows Server 2019 виконаємо перевірку налаштованих параметрів адресації і чи домен був справді створений, рис.3.35.

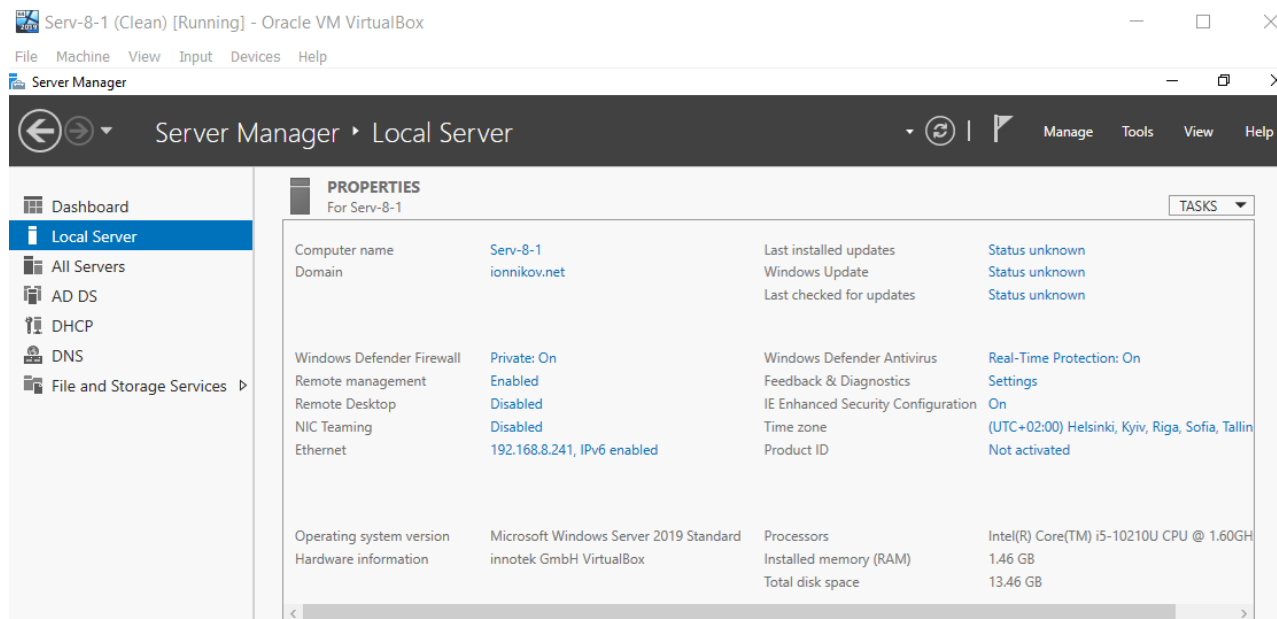


Рисунок 3.35 – Інформація щодо контролеру домену Serv-8-1

Далі поглянемо на роздані адреси на DHCP-сервері контролера домену, рис.3.36.

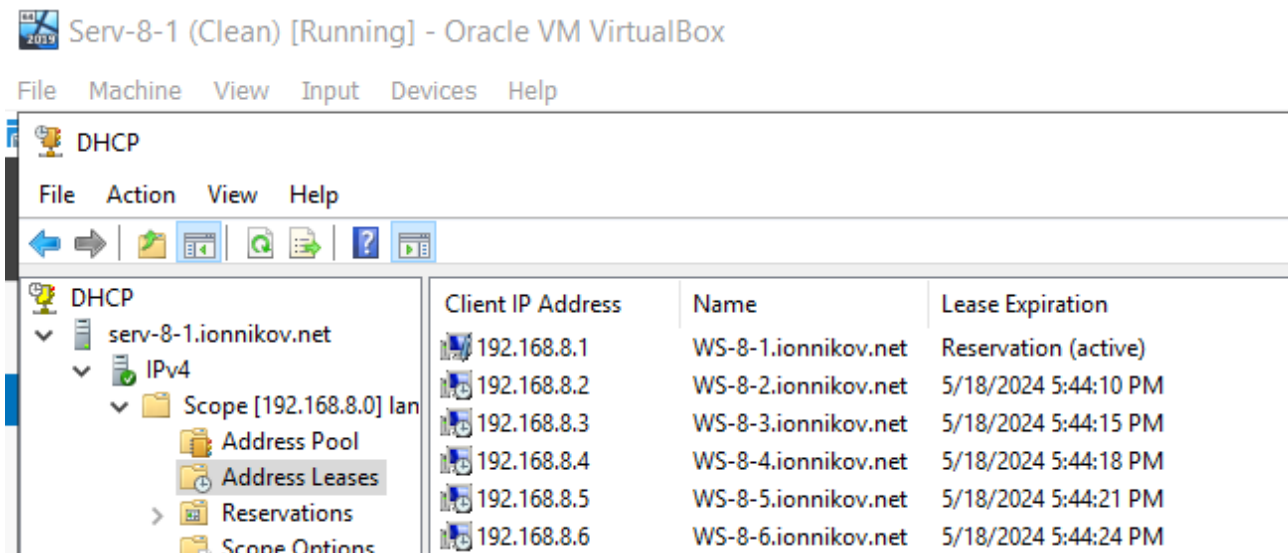


Рисунок 3.36 – Список динамічно розданих адрес для робочих станцій

Виконаємо перевірку наявності створених користувачів, рис.3.37.

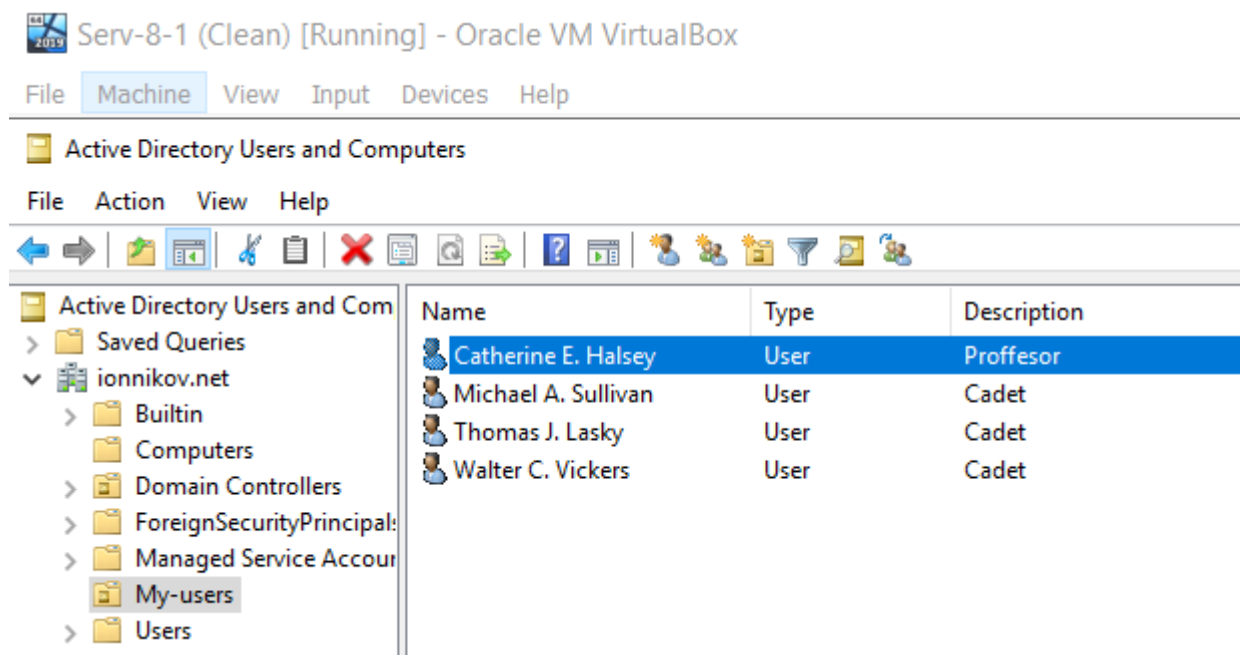


Рисунок 3.37 – Список створених користувачів

Виконаємо Echo запити (ping) зі сервера до інших пристроїв мережі за їхніми доменними іменами, рис.3.38. Тим самим перевіряємо і наявність зв'язку, і роботу DNS-серверу.

```
C:\Users\Administrator>ping WS-SIEM

Pinging WS-SIEM.ionnikov.net [192.168.8.240] with 32 bytes of data:
Reply from 192.168.8.240: bytes=32 time=1ms TTL=64
Reply from 192.168.8.240: bytes=32 time=1ms TTL=64
Reply from 192.168.8.240: bytes=32 time=1ms TTL=64
Reply from 192.168.8.240: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.8.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>ping WS-8-1

Pinging WS-8-1.ionnikov.net [192.168.8.1] with 32 bytes of data:
Reply from 192.168.8.1: bytes=32 time=1ms TTL=128
Reply from 192.168.8.1: bytes=32 time=1ms TTL=128
Reply from 192.168.8.1: bytes=32 time=1ms TTL=128
Reply from 192.168.8.1: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Рисунок 3.38 – Echo запит до пристроїв мережі за їх доменними іменами

Виконуємо перевірку можливості віддаленого підключення до мережесих пристроїв зі сервера, рис.3.39.

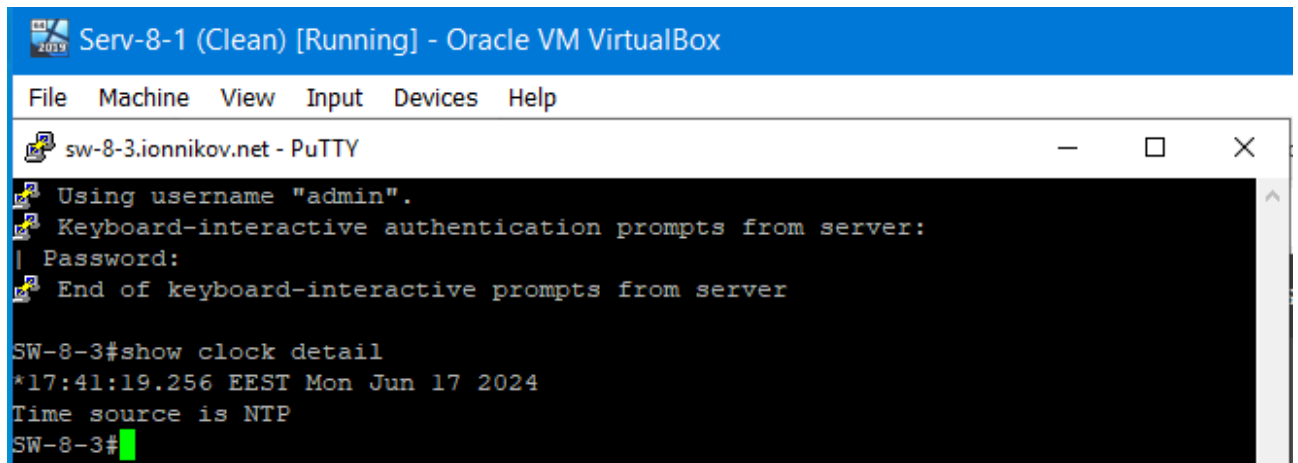


Рисунок 3.39 – Підключення через SSH до SW-8-3

Переходимо до кінцевих пристроїв. На WS-8-1 виконуємо вхід в систему з використанням одного зі створених облікових записів користувачів, рис.3.40.

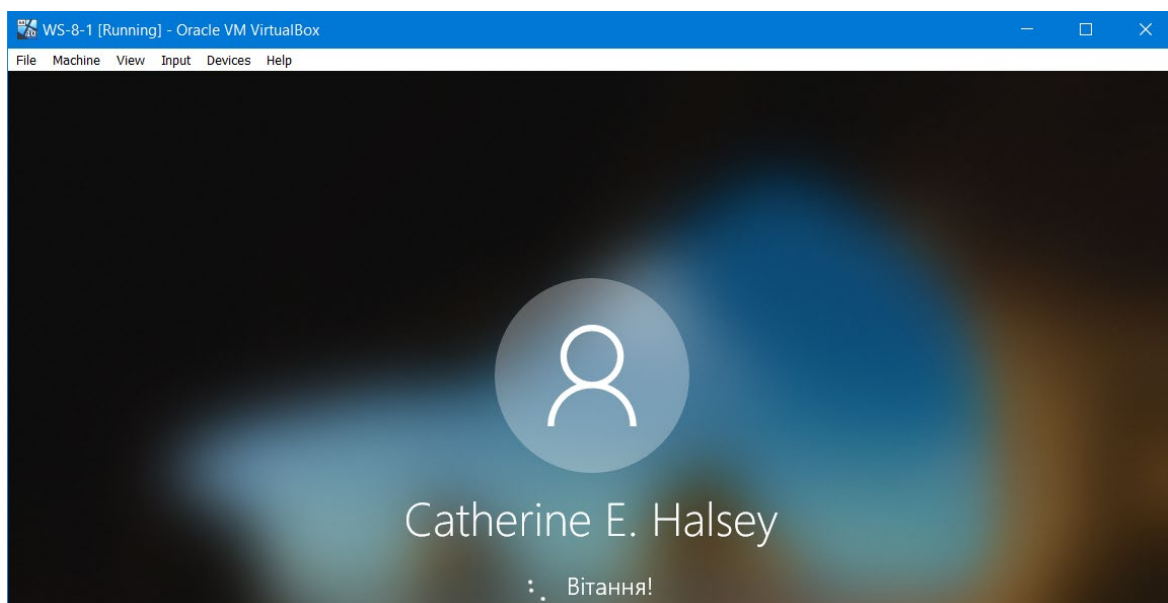


Рисунок 3.40 – Вхід в систему

3.3 Перевірка функціонування SIEM

Переходимо до OSSIM, тобто до WS-SIEM. Спершу переглянемо отримані події від WS-8-1 в OSSIM, рис.3.41. В таблиці переважно наведені події пов'язані з щойно виконаним входом в систему на WS-8-1. Більший приклад отриманих подій наведено в додатку Г.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

DASHBOARDS

ANALYSIS

ENVIRONMENT

REPORTS

CONFIGURATION

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.

7,399 TOTAL EVENTS IN DATABASE.

☐	EVENT NAME	▼ DATE GMT+3:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK	
	AlienVault HIDS: Windows Successful Logon: Unlo ck	2024-06-18 12:10:06	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: Windows Logon Success.	2024-06-18 12:10:06	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:10:06	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: A Kerberos User authentication ti cket was requested: Success.	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49984	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: A Kerberos service ticket was req uested: Success.	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49988	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: A Kerberos service ticket was req uested: Success.	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49985	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: Windows Network Logon	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49991	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: Windows Network Logon	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49990	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: Windows Network Logon	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49987	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: A Kerberos service ticket was req uested: Success.	2024-06-18 12:09:56	WS-SIEM	N/A	WS-8-1:49980	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: A Kerberos service ticket was req uested: Success.	2024-06-18 12:09:56	WS-SIEM	N/A	WS-8-1:49979	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: Windows Network Logon	2024-06-18 12:09:56	WS-SIEM	N/A	WS-8-1:49978	Serv-8-1	2 → 2	LOW (0)	
	AlienVault HIDS: Special privileges assigned to ne w logon	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	

Рисунок 3.41 – Отримані події з пристроїв

Виконаємо фільтрацію подій, де джерелом виступає WS-8-1, рис.3.42.

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.							7,463 TOTAL EVENTS IN DATABASE.		
☐	EVENT NAME	▼ DATE GMT+3:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK	
🔍	AlienVault HIDS: Special privileges assigned to ne	2024-06-18 12:12:14	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Windows machine logon.	2024-06-18 12:12:14	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Windows error event.	2024-06-18 12:11:17	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Windows Network Logon	2024-06-18 12:11:08	WS-SIEM	N/A	WS-8-1:50010	Serv-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Windows Network Logon	2024-06-18 12:11:08	WS-SIEM	N/A	WS-8-1:50009	Serv-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Windows Network Logon	2024-06-18 12:11:08	WS-SIEM	N/A	WS-8-1:50008	Serv-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Special privileges assigned to ne	2024-06-18 12:10:15	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Windows machine logon.	2024-06-18 12:10:15	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	🔍
🔍	AlienVault HIDS: Windows Successful Logon: Unlo	2024-06-18 12:10:06	WS-SIEM	N/A	WS-8-1	WS-8-1	2 → 2	LOW (0)	🔍

Рисунок 3.42 – Фільтрація подій де джерелом виступає WS-8-1

По кожній події можна отримати детальну інформацію. Для прикладу переглянемо одну з подій, що стосується входу в систему на WS-8-1, рис.3.43. Тут зазначено час (2024-06-18 12:10:06), категорію події (Authentication), підкатегорію (Login), ім'я пристрою (WS-8-1), його IP (192.168.8.1) та MAC-адресу (08:00:27:24:91:5C), домен (IONNIKOV), логін користувача (user-halsey) який був використаний для входу та іншу інформація.

Event details

AlienVault HIDS: Windows Successful Logon: Unlock

DATE	2024-06-18 12:10:06 GMT+3:00	CATEGORY	Authentication
ALIENVault SENSOR	WS-SIEM [192.168.8.240]	SUB-CATEGORY	Login
DEVICE IP	192.168.8.1 [eth0]	DATA SOURCE NAME	AlienVault HIDS- authentication_success
EVENT TYPE ID	700004	DATA SOURCE ID	7009
UNIQUE EVENT ID#	2d5211ef-aa61-0800-27f5-83218e3faee6	PRODUCT TYPE	Authentication and DHCP
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
1	5	LOW (0)	0

SOURCE	WS-8-1 [192.168.8.1]	DESTINATION	WS-8-1 [192.168.8.1]
Hostname: WS-8-1	Location: N/A	Hostname: WS-8-1	Location: N/A
MAC Address: 08:00:27:24:91:5C	Context: N/A	MAC Address: 08:00:27:24:91:5C	Context: N/A
Port: 0	Asset Groups: Endpoints	Port: 0	Asset Groups: Endpoints
Latest update: N/A	Networks: Local_192_168_8_0_24	Latest update: N/A	Networks: Local_192_168_8_0_24
Username & Domain: N/A	Logged Users: N/A	Username & Domain: N/A	Logged Users: N/A
Asset Value: 2	OTX IP Reputation: No	Asset Value: 2	OTX IP Reputation: No
SERVICE ▲ PORT ▼ PROTOCOL ▼		SERVICE ▲ PORT ▼ PROTOCOL ▼	
No services available		No services available	
SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST		SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST	

USERNAME	USERDATA1	USERDATA2	USERDATA3	USERDATA4	USERDATA5
user-halsey	5	windows,	WS-8-1\$	4624	7
USERDATA6	USERDATA7	USERDATA8	USERDATA9		
IONNIKOV	0x1c210c	C:\Windows\System32\lsass.exe	WS-8-1		

RAW LOG
AV - Alert - "1718701806" --> RID: "700004"; RL: "5"; RG: "windows,"; RC: "Windows Successful Logon: Unloc k"; USER: "WS-8-1\$ Account Domain: IONNIKOV Logon ID: 0x3e7 Logon Type: 7 New Logon: Security ID: S-1-5-21-3230124944-4147248380-420184 9514-1111 Account Name: user-halsey "; SRCIP: "-"; HOSTNAME: "(WS-8-1) 192.168.8.1->WinEvtLog"; LOCATION: "(WS-8-1) 192.168.8.1->Win EvtLog"; EVENT: "[INIT]2024 Jun 18 12:10:04 WinEvtLog: Security: AUDIT_SUCCESS(4624): Microsoft-Windows-Security-Auditing: user-halsey: IONNIKO V: WS-8-1.ionnikov.net: An account - was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WS-8-1\$ Account Domain: IONNI KOV Logon ID: 0x3e7 Logon Type: 7 New Logon: Security ID: S-1-5-21-3230124944-4147248380-4201849514-1111 Account Name: user-halsey Acc ount Domain: IONNIKOV Logon ID: 0x1c210c Logon GUID: {7157fa06-b73d-c7c9-c614-3d7a39f22ac2} Process Information: Process ID: 0x214 Pro cess Name: C:\Windows\System32\lsass.exe Network Information: Workstation Name: WS-8-1 Source Network Address: - So urce Port: - Detailed Authentication Information: Logon Process: Negotiat Authentication Package: Negotiate Transited Service s: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer tha t was accessed.[END]";

Рисунок 3.43 – Перегляд детальної інформації про подію входу в систему

Також агенти OSSEC здатні відслідковувати навіть встановлення нових програм та зміни в реєстрі Windows. На WS-8-1 було виконано встановлення програми «PuTTY» і на панелі SIEM відразу відобразилась дана подія, рис.3.44

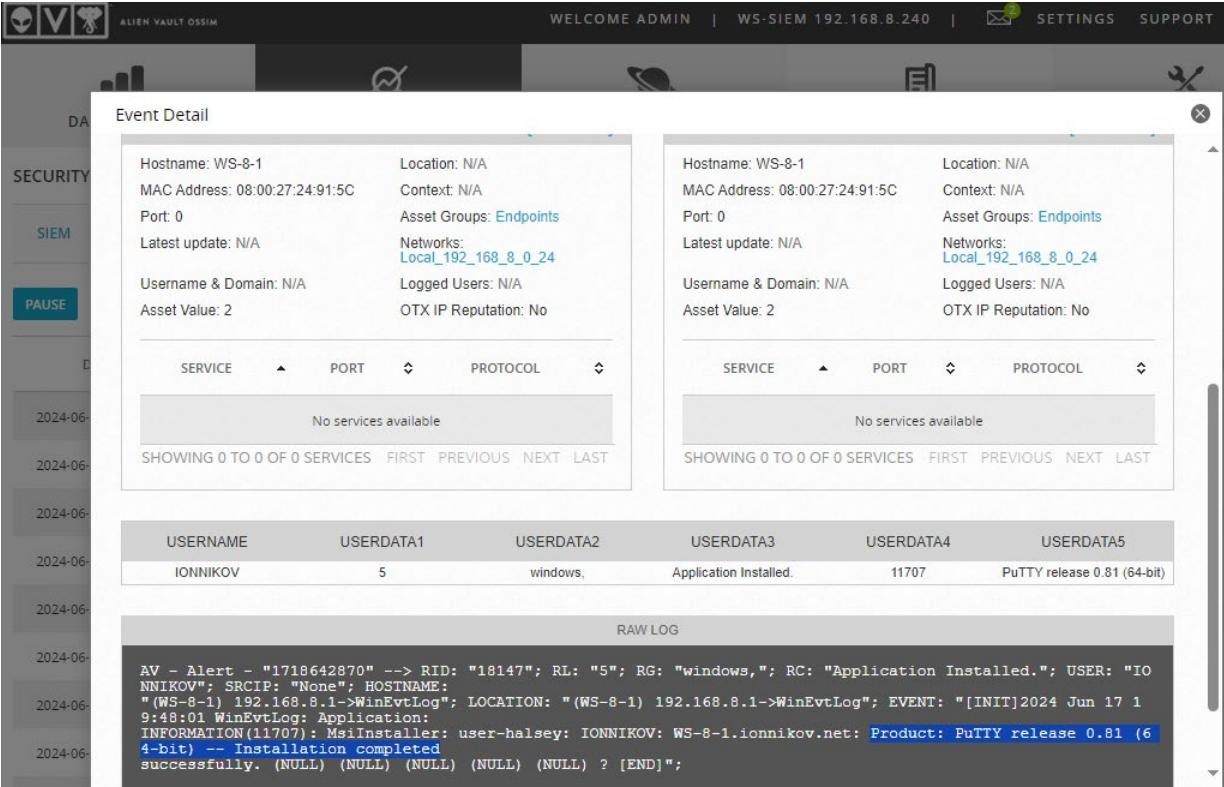


Рисунок 3.44 – Перегляд інформації про подію встановлення програми

Тепер проведемо базове сканування серверу (Serv-8-1) на наявні вразливості та переглянемо результат, рис.3.45 – 3.46. Повний звіт наведено в додатку Д.

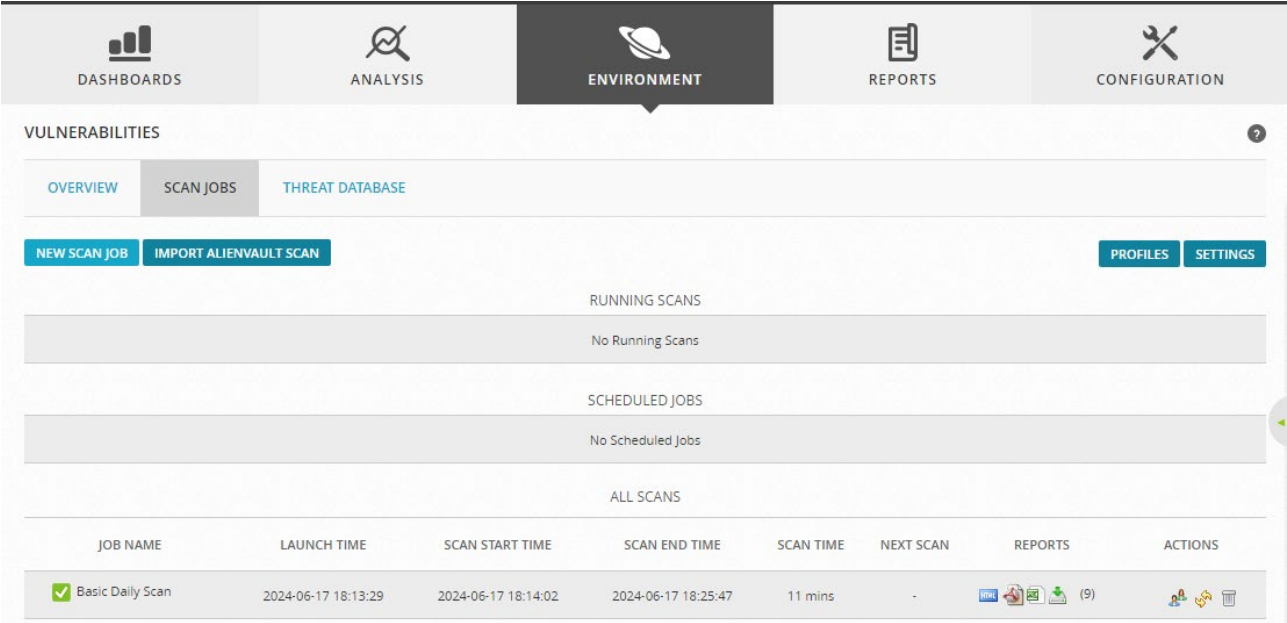


Рисунок 3.45 – Успішне виконання сканування вразливостей для Serv-8-1

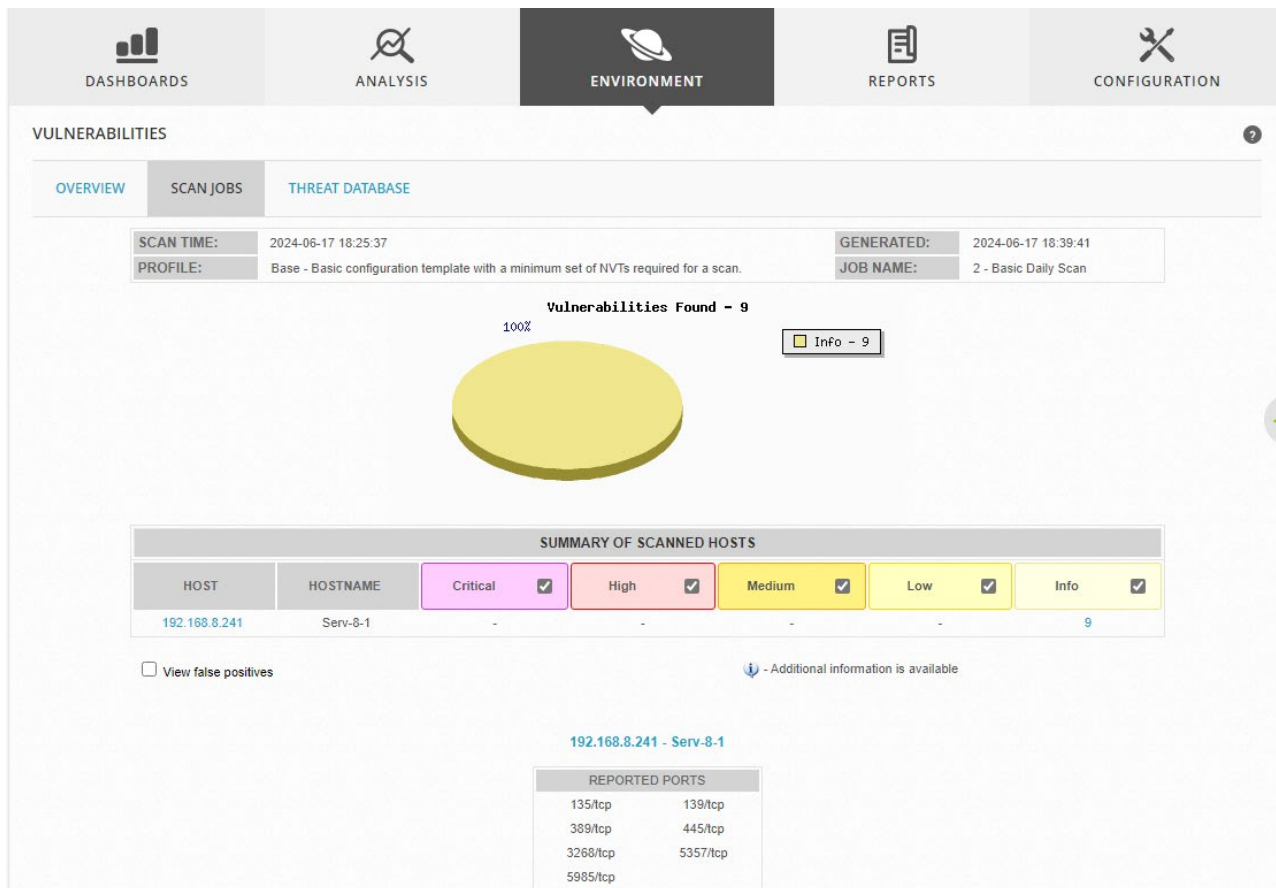


Рисунок 3.46 – Успішне виконання сканування вразливостей для Serv-8-1

Отож, при скануванні Serv-8-1 було виявлено 9 вразливостей найнижчого рівня (info). При цьому залучені наступні TCP порти: 135, 139, 389, 445, 3268, 5357, 5985.

Прогорнувши нижче отримаємо інформацію по кожній вразливості. Для прикладу переглянемо одну з виявлених, рис.3.47. Тут дано назву вразливості (SMB log in), id (10394), сервіс (445/tcp), сімейство (Windows), категорію (infos), час створення та модифікації (2008-09-10 та 2021-08-11), опис (It was possible to log into the remote host using the SMB protocol.), CVSS вектор (AV:N/AC:L/Au:N/C:N/I:N/A:N), загальний висновок (This script attempts to logon into the remote host using login/password credentials.) і оцінку CSVV (0.0)

SMB log in	10394	microsoft-ds (445/tcp)	Info
References: Vulnerability Detection Result: It was possible to log into the remote host using the SMB protocol. CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: This script attempts to logon into the remote host using login/password credentials. CVSS Base Score: 0.0	Family name: Windows Category: infos Created: 2008-09-10T08:22:48Z Modified: 2021-08-11T09:39:10Z		

Рисунок 3.47 –Інформація стосовно однієї вразливості

Також є можливість конвертувати звіт по даному скануванню в формат PDF або Excel, рис.3.48 і 3.49, що може бути зручним для пересилання та аналізу.

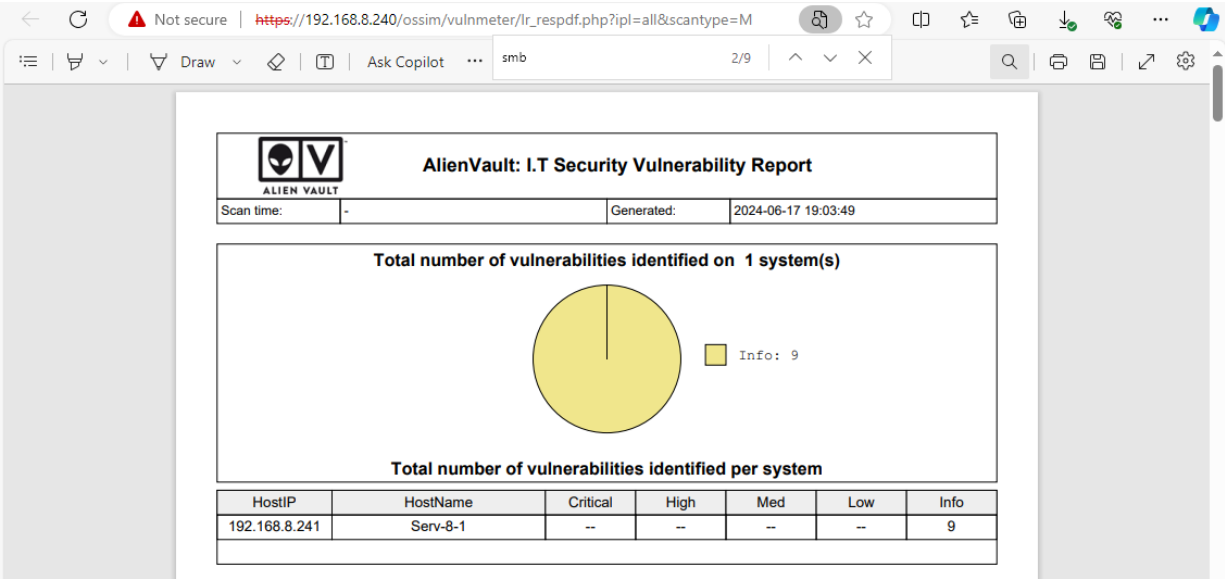


Рисунок 3.48 –Звіт по скануванню вразливостей в PDF форматі

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	AlienVault: I.T Security Vulnerability Report												
2	Scan time	2024-06-17 19:05:38											
3	Generated	2024-06-17 16:05:38											
4	Profile	-											
5	Hostname	Host IP	Service	Vuln ID	CVSS	CVEs	Risk Level	Vulnerability	Observation	Remediation	Consequences	Test Output	Operating System/Software
6	Serv-8-1	192.168.8.241	msrpc (135/tcp)	108044	0 -	-	Info	DCE/RPC and MSRPC Services Enumeration Family name: Service detection Category: info Created: 2005-11-03T13:08:04Z Modified: 2021-04-15T13:23:31Z	Distribute Filter incoming traffic to this port. Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and		Impact: An attacker may use this fact to gain more knowledge about the remote host.	A DCE endpoint resolution in service seems to be running on this port.	n/a
7	Serv-8-1	192.168.8.241	general (tcp)	108449	0 -	-	Info	Hostname Determination Reporting Family name: Service detection Category: end Created: 2018-07-05T06:03:26Z Modified: 2018-11-19T11:11:31Z	The script n/a reports information on how the hostname of the target was determined.	n/a	n/a	Hostname determination for IP: 192.168.8.241 [Source: 192.168.8.241] IP: The LDAP Server supports	n/a
8	Serv-8-1	192.168.8.241	globalcatLDAP (3268/tcp)	100082	0 -	-	Info	LDAP Detection Family name: Service detection Category: info	A LDAP Server is running	n/a	n/a		n/a

Рисунок 3.49 –Звіт по скануванню вразливостей в Excel форматі

В цілому виявлені вразливості для Serv-8-1 мають інформаційний характер і не є вкрай суттєвими проблемами на які слід звертати увагу, однак можливо буде доцільним закрити ряд портів для Serv-8-1, якщо вони активно не використовуються.

На головному вікні можна переглянути загальну статистику, рис.3.50.

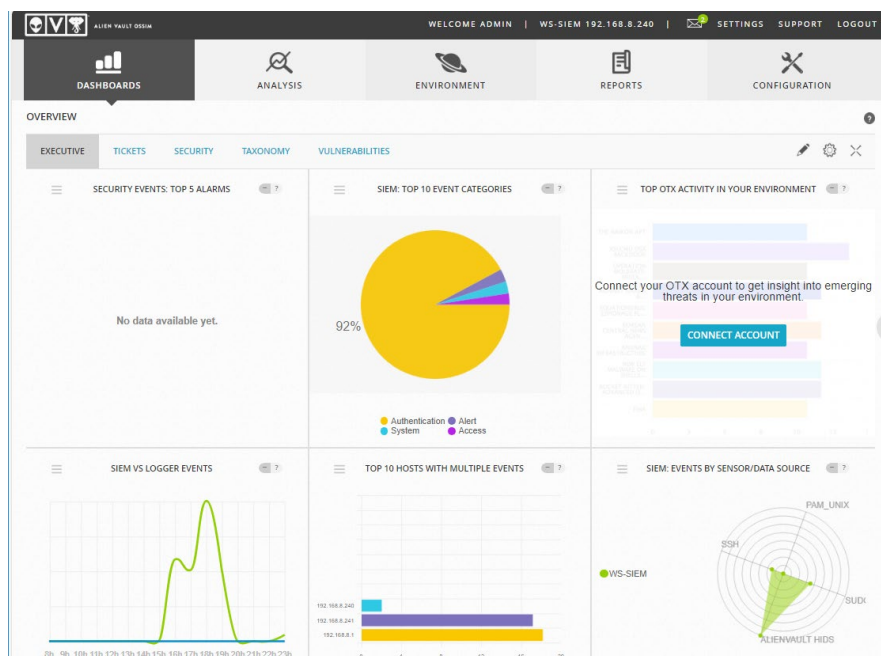


Рисунок 3.50 – Загальна статистика

Переглянути загальну інформацію щодо типів сповіщень та пристроїв з яких вони надійшли, рис.3.51.

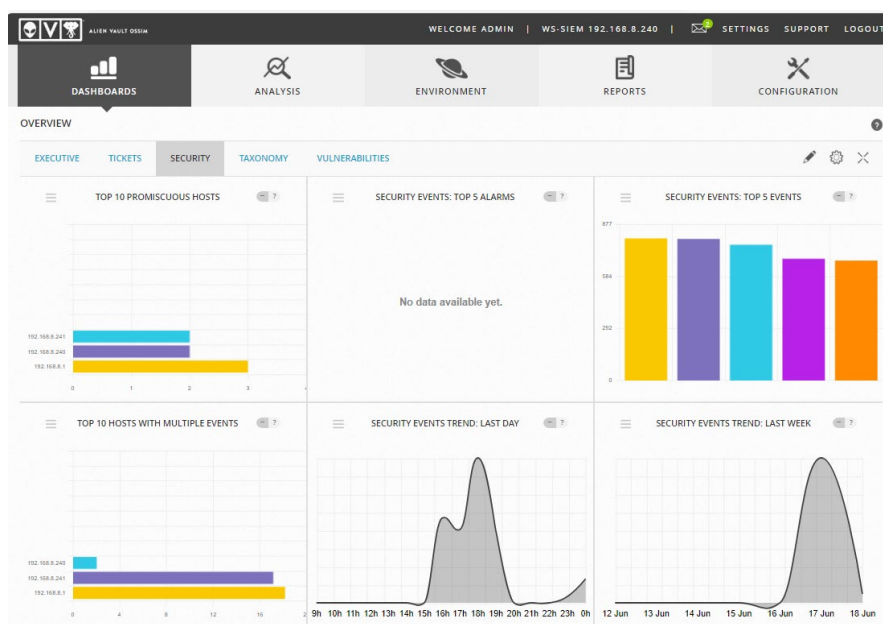


Рисунок 3.51 – Загальна статистика по типам подій

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

Переглянути статистику зважаючи на джерело подій та пристрої з яких вони надійшли, рис.3.52.

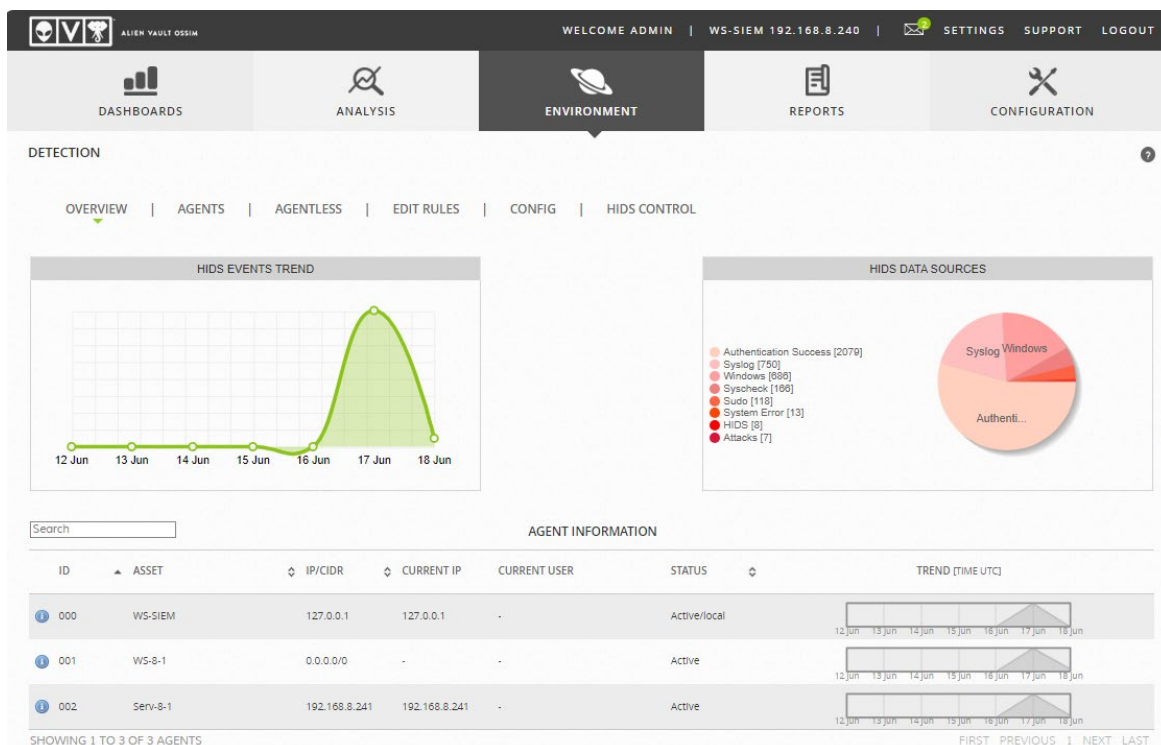


Рисунок 3.52 – Інформація щодо джерел подій з пристроїв

Переглянути згенеровану мапу підключень, рис.3.53.



Рисунок 3.53 – Мапа підключень

Перевірити інформація про стан WS-SIEM та статистику використання системних ресурсів, рис.3.54.

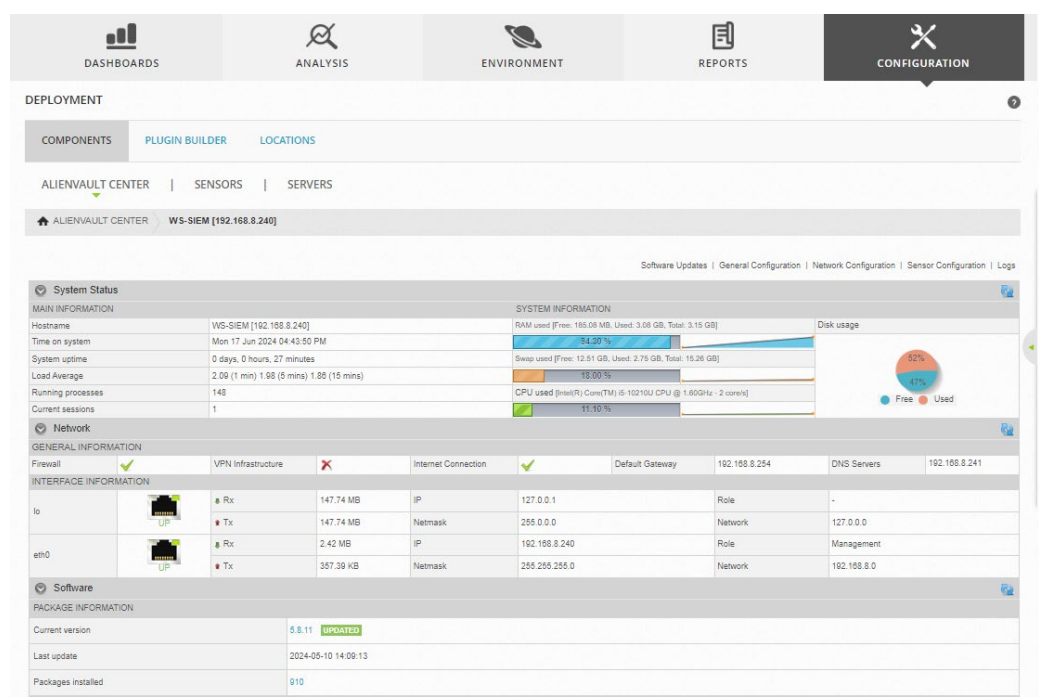


Рисунок 3.54 – Інформація про роботу WS-SIEM

І є можливість згенерувати звіти по будь-якій інформації щодо роботи OSSIM, рис.3.55.

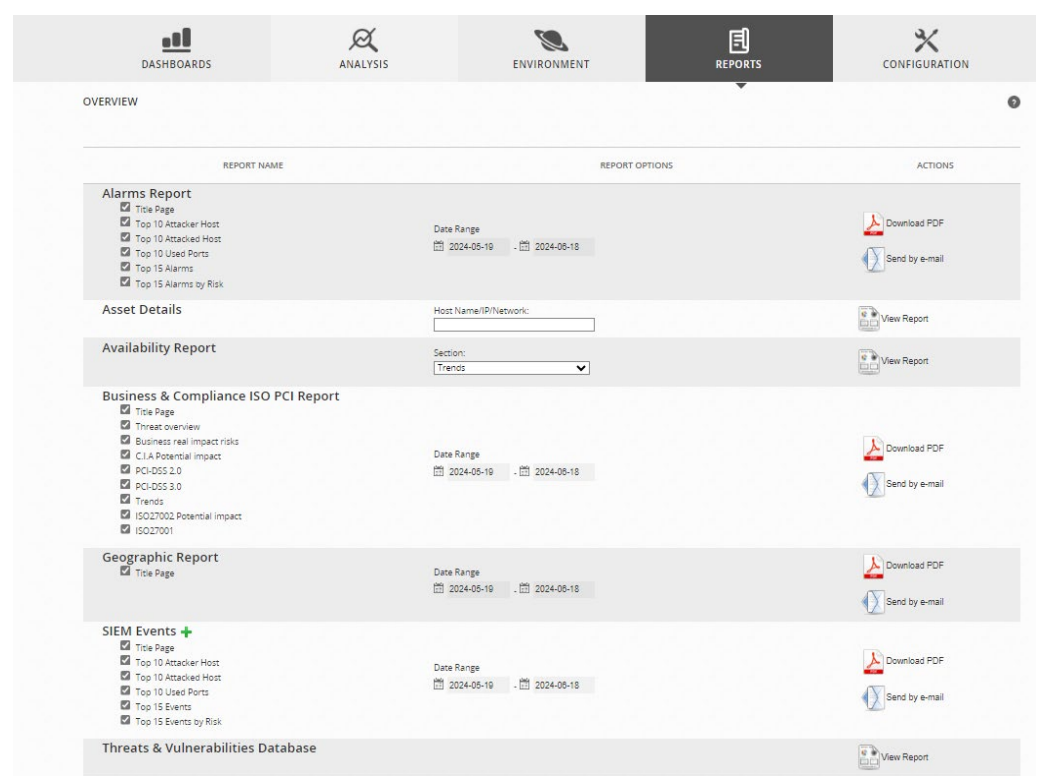


Рисунок 3.55 – Можливість створення звітів по роботу OSSIM

Висновки до 3 розділу

В результаті виконання 3 розділу було виконано проєктування топології мережі проєкту з використання мережевого емулятора GNS3 та гіпервізора VirtualBox. Наведено таблицю параметрів підключень пристроїв між собою.

Було розглянуто процес налагодження пристроїв проєкту, що включало проведення налаштувань маршрутизатора, комутатора, сервера з ОС Windows Server 2019, станції з OSSIM та кінцевої робочої станцію з ОС Windows 10. Налагодження передбачало призначення адрес, налаштування домену ionnikov.net і Active Directory, приєднання пристроїв до домену, налагодження параметрів OSSIM, встановлення відповідних агентів на сервері та робочій станції з метою збору та передачі даних до SIEM системи.

Після виконаних налаштувань було проведено перевірку функціонування мережі, що включало проведення інформаційних обмінів між різними вузлами, перевірку роботи DHCP та DNS серверу та можливість виконувати вхід в систему з використання облікових записів. Також було проведено перевірку роботи OSSIM шляхом перегляду детальної інформації щодо отриманих подій з кінцевих пристроїв та переглядом загальної інформації стосовно роботи системи SIEM.

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи бакалавра було розроблено проєкт SIEM-підсистеми для SOC на базі рішення Alien Vault OSSIM.

В ході розробки першого розділу було розглянуто основні принципи роботи, призначення та ключові функціональні можливості SIEM. Наведено перелік рекомендацій щодо ефективного використання SIEM-систем. Досліджено сучасні тенденції розвитку SIEM-технологій. Проведено огляд безкоштовних SIEM-рішень за підсумком якого визначено, що AlienVault OSSIM є збалансованим рішенням і буде в подальшому використаний для організації SIEM системи в проєкті мережі. Також було детально розглянуто особливості AlienVault OSSIM з повним визначенням її функціональних можливостей, компонентів, архітектури та способів розгортання.

В ході виконання даного розділу було проведено розробку логічної та фізичної топологій мережі проєкту з дотриманням трирівневої ієрархічної моделі мережі. Було визначено необхідну кількість мережевого обладнання для організації проєкту мережі та розроблено схему адресації зважаючи на необхідну кількість пристроїв. Проведено проєктування роботи системи SIEM з використання OSSEC-агентів задля збору подій з кінцевих вузлів. Обґрунтовано вибір необхідних моделей для маршрутизатора та комутаторів з урахування потреби проєкту мережі, зазначено мінімальні системні параметри для серверу, робочих станцій та станції з SIEM.

В результаті виконання третього розділу було виконано проєктування топології мережі проєкту з використання емулятора GNS3 та гіпервізора VirtualBox. Розглянуто процес налагодження пристроїв проєкту, що включало проведення налаштувань маршрутизатора, комутатора, сервера з ОС Windows Server 2019, станції з OSSIM та кінцевої робочої станцію з ОС Windows 10. Проведено перевірку функціонування мережі та побудованої системи SIEM. В підсумку було отримано повноцінний функціональний проєкт мережі відповідно до всіх поставлених цілей та задач даної роботи.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST Special Publication 800-92, "Guide to Computer Security Log Management"
2. Sanders C., Smith J. Applied Network Security Monitoring. USA: Elsevier, 2014. 672 с.
3. The essential guide to Security Information and Event Management (SIEM) [Електронний ресурс]. – Режим доступу: <https://www.defense.com/white-papers/defense.com-siem-whitepaper.pdf>
4. What Is Log Rotation? [Електронний ресурс]. – Режим доступу: <https://www.xcitium.com/log-rotation/>
5. Recommendation for Best SIEM for Managed SOC. [Електронний ресурс]. – Режим доступу: <https://cybriant.com/recommendation-for-best-siem-for-managed-soc/>
6. A SIEM Security Primer: Evolution and Next-Gen Capabilities. [Електронний ресурс]. – Режим доступу: <https://www.exabeam.com/explainers/siem-security/a-siem-security-primer/>
7. Wazuh. [Електронний ресурс]. – Режим доступу: <https://wazuh.com>
8. 7 Best Open Source SIEM Systems to Improve Your Cyber Security. [Електронний ресурс]. – Режим доступу: <https://geekflare.com/best-open-source-siem-systems/>
9. What is OSSIM? [Електронний ресурс]. – Режим доступу: <https://espprojects.co.uk/news/news-general/what-is-ossim/>
10. Prelude OSS. [Електронний ресурс]. – Режим доступу: <https://prelude-ids.org/8-2/>
11. AlienVault OSSIM. [Електронний ресурс]. – Режим доступу: <https://cybersecurity.att.com/products/ossim>
12. Open Source Security Information and Event Management system. [Електронний ресурс]. – Режим доступу: <https://www.admin-magazine.com/Archive/2014/20/Open-Source-Security-Information-and-Event-Management-system>

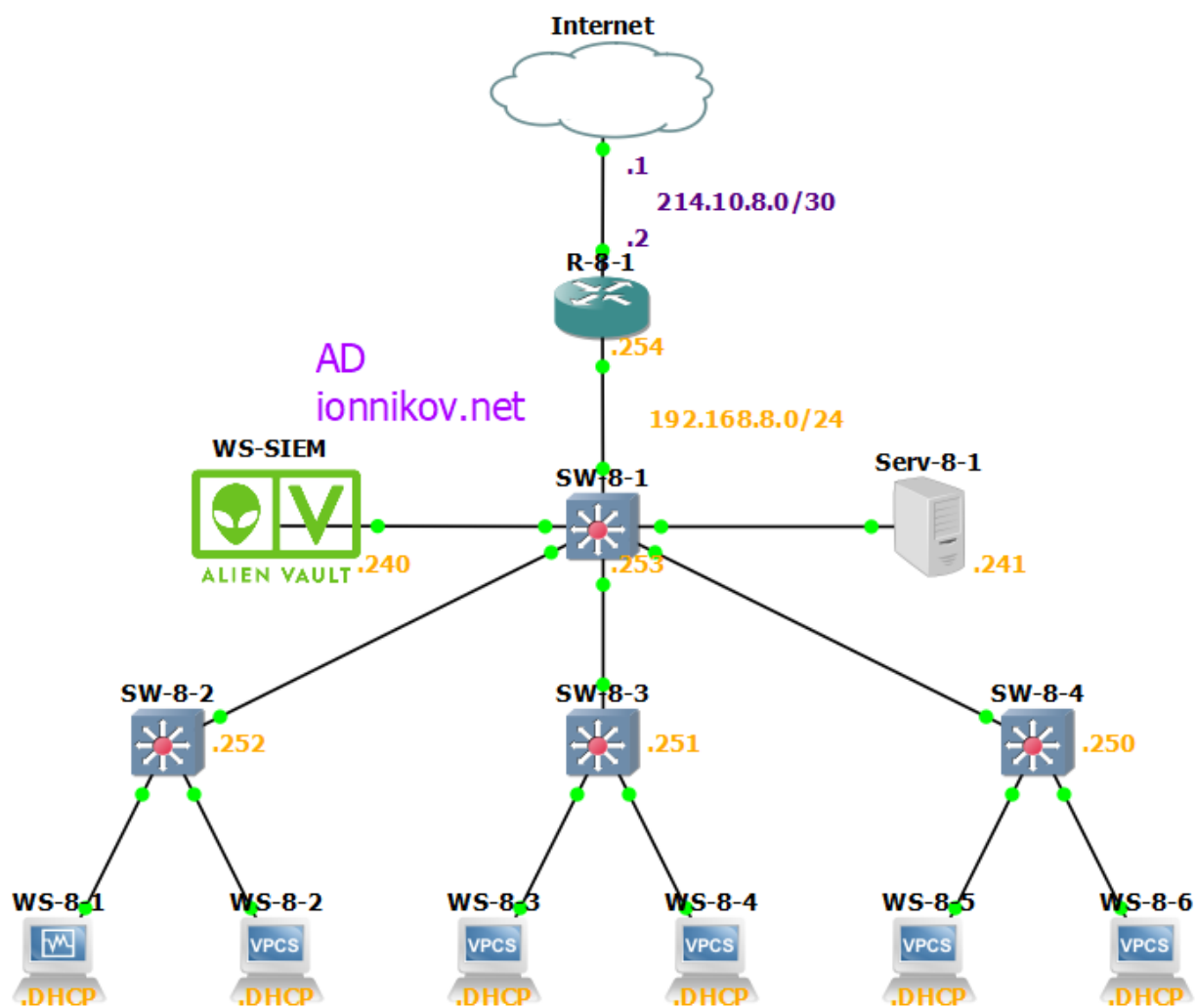
		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

13. Monitoring and Security Information and Event Management. [Електронний ресурс]. – Режим доступу: https://www.wisto.at/wp-content/uploads/2022/02/3_DIHW_Monitor_SIEM_v1.pdf
14. OSSIM architecture. [Електронний ресурс]. – Режим доступу: <https://dl.acm.org/doi/fullHtml/10.5555/2642922.2642924>
15. AlienVault OSSIM Review - Open Source SIEM. [Електронний ресурс]. – Режим доступу: <https://www.infosecinstitute.com/resources/network-security-101/alienvault-ossim-review-open-source-siem/>
16. What is Hierarchical Network Design? [Електронний ресурс]. – Режим доступу: <https://www.auvik.com/franklyit/blog/hierarchical-network-design/>
17. Monitoring and Security Information and Event Management. [Електронний ресурс]. – Режим доступу: https://www.wisto.at/wp-content/uploads/2022/02/3_DIHW_Monitor_SIEM_v1.pdf
18. Маршрутизатор Cisco ISR4221/K9. [Електронний ресурс]. – Режим доступу: <https://stack-systems.com.ua/marshrutizator-cisco-isr4221-k9>
19. Комутатор Cisco WS-C2960+24PC-S. [Електронний ресурс]. – Режим доступу: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24pc-s>
20. AlienVault Installation. [Електронний ресурс]. – Режим доступу: https://scadahacker.com/library/Documents/Manuals/AlienVault_Installation_Guide.pdf

ДОДАТКИ

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема побудованої мережі



		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

Порівняльна характеристика баз даних вразливостей

Характеристика	NVD	CVE	OSVD	OTX
Ліцензування	Безкоштовна	Безкоштовна	Безкоштовна	Безкоштовна
Дата виявлення вразливості	Ні	Так	Так	Так
Дата розголошення вразливості	Так	Так	Так	Так
Дата виправлення вразливості	Ні	Так	Так	Так
Дата виявлення експлойту	Ні	Так	Так	Так
Опис уразливості	Так	Так	Так	Так
Оцінка ризику	Так	Так	Ні	Так
Додаткові ресурси	Так	Так	Ні	Так
Частота оновлень	Висока	Висока	Низька	Висока
Можливість пошуку	Так	Так	Так	Так
Підтримка формату CVE	Так	Так	Так	Так

Поетапна інструкція встановлення AlienVault OSSIM

Крок 1: Встановіть AlienVault OSSIM

- 1.Завантажте останню версію AlienVault OSSIM з офіційного сайту.
- 2.Запишіть завантажений образ на DVD або завантажувальний USB-диск.
- 3.Вставте DVD або USB-диск у систему та перезавантажте, щоб запустити програму встановлення.
- 4.Дотримуйтеся вказівок на екрані, щоб завершити встановлення.

Крок 2: Налаштування AlienVault OSSIM

- 1.Облікові дані для входу за замовчуванням — «admin» як для імені користувача, так і для пароля.
- 2.Увійдіть у консоль AlienVault і змініть пароль на надійний та унікальний.
- 3.Налаштуйте параметри мережі вашої системи, включаючи IP-адресу, маску мережі, шлюз, DNS та ім'я хоста.

Крок 3: Налаштуйте сенсори

- 1.Сенсори є ключовими для функціональності AlienVault OSSIM. Вони збирають дані про мережеву діяльність, які OSSIM використовує для моніторингу вашої мережі.
- 2.Перейдіть до Configuration > Deployment > Sensors на консолі AlienVault.
- 3.Натисніть «Додати сенсор» і заповніть необхідні дані, включаючи назву датчика, IP-адресу.
- 4.Дотримуйтеся вказівок на екрані, щоб завершити налаштування сенсора.

Крок 4: Налаштуйте моніторинг мережі

- 1.Щоб налаштувати моніторинг мережі, вам потрібно буде визначити, які дії OSSIM має контролювати.
- 2.Перейдіть до Environment > Detection > Directives на консолі AlienVault.

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

3. Тут ви можете вибрати з попередньо налаштованих правил або створити власні відповідно до ваших конкретних потреб.

Крок 5: Налаштуйте реагування на інциденти

1. У разі виявлення потенційного інциденту безпеки OSSIM може реагувати різними способами залежно від ваших налаштувань.

2. Перейдіть до Configuration > Threat Intelligence > Responses у консолі AlienVault.

3. Налаштуйте дії, які слід виконувати у відповідь на різні типи інцидентів. Ви можете вибрати попередньо налаштовані відповіді або налаштувати власні.

Крок 6: Налаштуйте сенсори

1. Захист вашої мережі не закінчується після початкового налаштування. Регулярні перевірки та оновлення мають вирішальне значення.

2. Часто перевіряйте консоль AlienVault на наявність попереджень або сповіщень.

3. Регулярно переглядайте журнали та звіти, створені OSSIM, щоб виявити можливі проблеми.

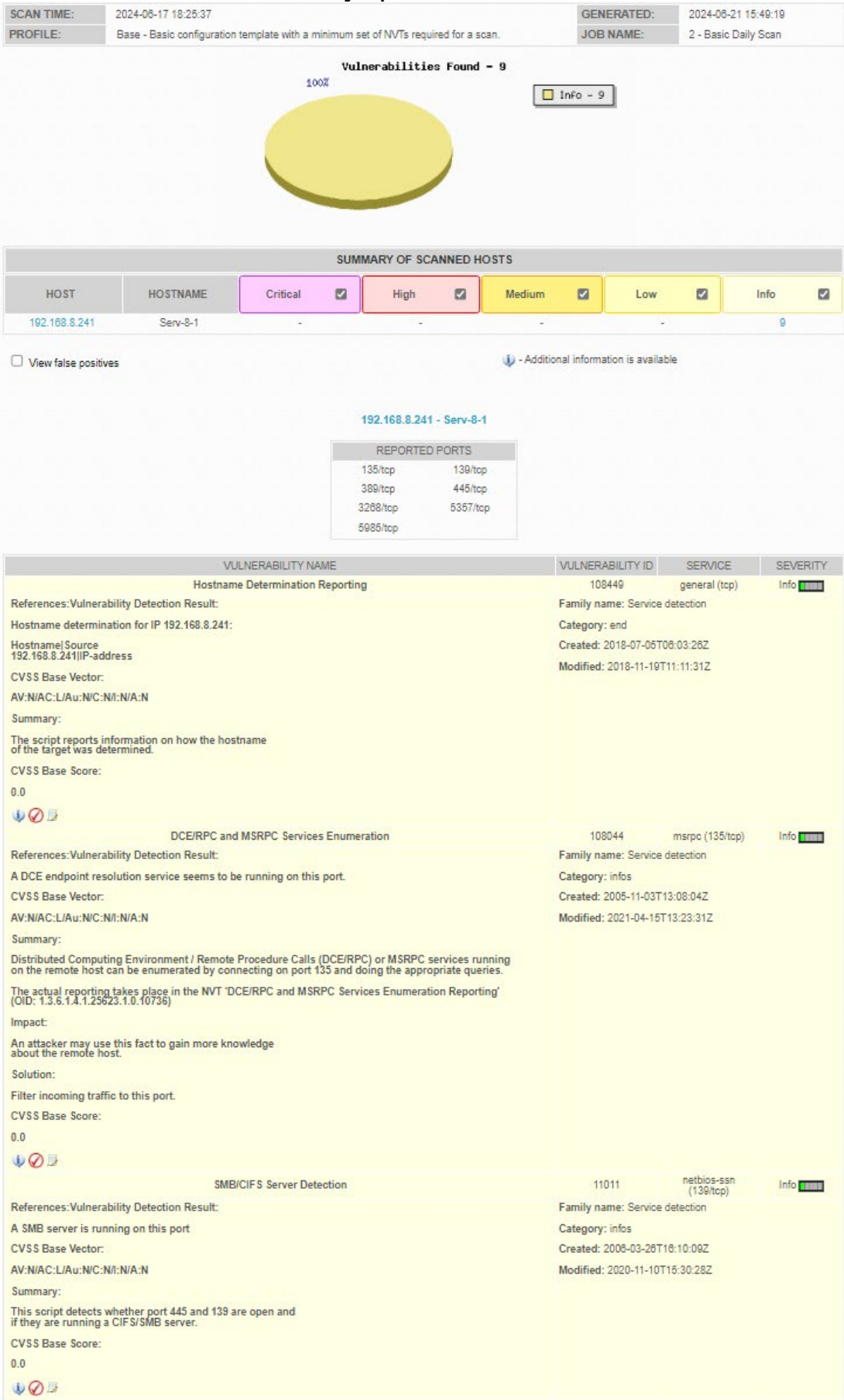
4. Оновлюйте свої правила, датчики та відповіді на основі ваших висновків, щоб підтримувати надійний захист.

		Іонніков В.М.			КІК.КР.Б – 125 – 08 – 25 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

DISPLAYING 1 TO 100 OF THOUSANDS OF EVENTS. 11,015 TOTAL EVENTS IN DATABASE.

☐	EVENT NAME	▼ DATE GMT+3:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK	
◆ ☐	SSHd: Connection closed	2024-06-18 12:10:50	WS-SIEM	N/A	0.0.0.0:54424	0.0.0.0:22	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:10:36	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Special privileges assigned to new logon	2024-06-18 12:10:28	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Network Logon	2024-06-18 12:10:28	WS-SIEM	N/A	Serv-8-1:51548	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:10:28	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Special privileges assigned to new logon	2024-06-18 12:10:15	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows machine logon.	2024-06-18 12:10:15	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:10:08	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:10:08	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Successful Logon: Unlock	2024-06-18 12:10:06	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Logon Success.	2024-06-18 12:10:06	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:10:06	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: A Kerberos User authentication ticket was requested: Success.	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49984	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: A Kerberos service ticket was requested: Success.	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49988	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: A Kerberos service ticket was requested: Success.	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49985	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Network Logon	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49991	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Network Logon	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49990	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Network Logon	2024-06-18 12:10:04	WS-SIEM	N/A	WS-8-1:49987	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:10:04	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: A Kerberos service ticket was requested: Success.	2024-06-18 12:09:56	WS-SIEM	N/A	WS-8-1:49980	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: A Kerberos service ticket was requested: Success.	2024-06-18 12:09:56	WS-SIEM	N/A	WS-8-1:49979	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Network Logon	2024-06-18 12:09:56	WS-SIEM	N/A	WS-8-1:49978	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Special privileges assigned to new logon	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Special privileges assigned to new logon	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Console Logon	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Console Logon	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Console Logon	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows console logoff.	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows console logoff.	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows console logoff.	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:09:53	WS-SIEM	N/A	WS-8-1	WS-8-1	2→2	LOW (10)	🔊
◆ ☐	SSHd: Connection closed	2024-06-18 12:09:46	WS-SIEM	N/A	0.0.0.0:47578	0.0.0.0:22	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Special privileges assigned to new logon	2024-06-18 12:09:38	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows machine logon.	2024-06-18 12:09:38	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Special privileges assigned to new logon	2024-06-18 12:09:27	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows Network Logon	2024-06-18 12:09:27	WS-SIEM	N/A	Serv-8-1:51519	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Windows User Logoff.	2024-06-18 12:09:27	WS-SIEM	N/A	Serv-8-1	Serv-8-1	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Login session closed.	2024-06-18 12:09:24	WS-SIEM	N/A	0.0.0.0	0.0.0.0	2→2	LOW (10)	🔊
◆ ☐	sudo: Session closed	2024-06-18 12:09:22	WS-SIEM	N/A	0.0.0.0	0.0.0.0	2→2	LOW (10)	🔊
◆ ☐	SSHd: Session disconnected	2024-06-18 12:09:22	WS-SIEM	N/A	WS-SIEM:55522	WS-SIEM:22	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Login session opened.	2024-06-18 12:09:20	WS-SIEM	N/A	0.0.0.0	0.0.0.0	2→2	LOW (10)	🔊
◆ ☐	AlienVault HIDS: Login session closed.	2024-06-18 12:09:20	WS-SIEM	N/A	0.0.0.0	0.0.0.0	2→2	LOW (10)	🔊

Звіт аналізу вразливостей Serv-8-1



LDAP Detection		10082	ldap (389/tcp)	Info
References: Vulnerability Detection Result: The LDAP Server supports LDAPv3. CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: A LDAP Server is running at this host. The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP. CVSS Base Score: 0.0 		Family name: Service detection Category: infos Created: 2009-03-27T11:39:47Z Modified: 2020-11-10T15:30:28Z		
SMB log in		10394	microsoft-ds (445/tcp)	Info
References: Vulnerability Detection Result: It was possible to log into the remote host using the SMB protocol. CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: This script attempts to logon into the remote host using login/password credentials. CVSS Base Score: 0.0 		Family name: Windows Category: infos Created: 2008-09-10T08:22:48Z Modified: 2021-08-11T09:39:10Z		
SMB/CIFS Server Detection		11011	microsoft-ds (445/tcp)	Info
References: Vulnerability Detection Result: A CIFS server is running on this port CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server. CVSS Base Score: 0.0 		Family name: Service detection Category: infos Created: 2008-03-26T16:10:09Z Modified: 2020-11-10T15:30:28Z		
LDAP Detection		10082	globalcatLDAP (3268/tcp)	Info
References: Vulnerability Detection Result: The LDAP Server supports LDAPv3. CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: A LDAP Server is running at this host. The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP. CVSS Base Score: 0.0 		Family name: Service detection Category: infos Created: 2009-03-27T11:39:47Z Modified: 2020-11-10T15:30:28Z		
Services		10330	unknown (5357/tcp)	Info
References: Vulnerability Detection Result: A web server is running on this port CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines. CVSS Base Score: 0.0 		Family name: Service detection Category: infos Created: 2011-01-14T09:12:23Z Modified: 2021-03-15T10:42:03Z		
Services		10330	unknown (5985/tcp)	Info
References: Vulnerability Detection Result: A web server is running on this port CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.		Family name: Service detection Category: infos Created: 2011-01-14T09:12:23Z Modified: 2021-03-15T10:42:03Z		

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арх.
		Фальковський І.Г.				90
Змн.	Арх.	№ докум.	Підпис	Дата		

Конфігураційні файли окремих пристроїв

R-8-1:

```
!
!  
!  
!  
!  
  
!  
upgrade fpd auto  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R-8-1  
!  
boot-start-marker  
boot-end-marker  
!  
logging message-counter syslog  
enable secret 5 $1$XP71$u/nNcp4b78LjiFo6r40H.1  
!  
no aaa new-model  
ip source-route  
no ip icmp rate-limit unreachable  
ip cef  
!  
!  
!  
!  
ip domain name ionnikov.net  
ip name-server 8.8.8.8  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
username admin privilege 15 secret 5  
$1$tZyt$LBxno6XKV36c7ADE7Yn/L0  
archive  
    log config  
        hidekeys  
!  
!  
!  
!  
!  
ip tcp synwait-time 5  
ip ssh time-out 30  
ip ssh version 2
```

SW-8-1:

```

!
! Last configuration change at 14:39:21 UTC
Mon Jun 17 2024
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-8-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
zK0wlfTtCkX2vCykKR1a66B9cuSBm.LdMfoyqxEsZZ6
!
username admin privilege 15 secret 4
Zhg.JW5gobPrWhU/V/eMA.F.Io4YqafsA30/Dekdw3.
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip routing
no ip icmp rate-limit unreachable
!
ip domain-name ionnikov.net
ip name-server 192.168.8.241
no ip cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
!
interface Ethernet0/0
 duplex auto
!
interface Ethernet0/1
 duplex auto
!
interface Ethernet0/2
 duplex auto
!
interface Ethernet0/3

```

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
interface FastEthernet0/0
description link-to-internet
ip address 214.10.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
description link-to-sw-8-1
ip address 192.168.8.254 255.255.255.0
duplex auto
speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 214.10.8.1
no ip http server
no ip http secure-server
!
!
!
access-list 1 permit 192.168.8.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
access-class 1 in
login local
transport input ssh
line vty 5 15
access-class 1 in
login local
transport input ssh
!
End

duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.8.253 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.8.254
!
no ip http server
!
!
access-list 1 permit 192.168.8.0 0.0.0.255
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
access-class 1 in
login local
transport input ssh
!
ntp server serv-8-1
end

```

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-8-2:

```
!  
! Last configuration change at 17:40:25 EEST  
Mon Jun 17 2024  
!  
version 15.1  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname SW-8-2  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops 6  
msg-body drops EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
enable secret 4  
zK0wlfTcKX2vCykKR1a66B9cuSBm.LdMfoyqxEsZZ6  
!  
username admin privilege 15 secret 4  
Zhg.JW5gobPrWhU/V/eMA.F.Io4YqafsA30/DekdW3.  
no aaa new-model  
clock timezone EEST 3 0  
no ipv6 cef  
ipv6 multicast rpf use-bgp  
no ip icmp rate-limit unreachable  
!  
ip domain-name ionnikov.net  
ip name-server 192.168.8.241  
ip cef  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
vlan internal allocation policy ascending  
!  
ip tcp synwait-time 5  
ip ssh time-out 30  
ip ssh version 2  
!  
!  
!  
!  
!  
interface Ethernet0/0  
duplex auto  
!  
interface Ethernet0/1  
duplex auto  
!  
interface Ethernet0/2  
duplex auto  
!  
interface Ethernet0/3  
duplex auto
```

SW-8-3:

```
!  
! Last configuration change at 17:38:56 EEST  
Mon Jun 17 2024  
!  
version 15.1  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname SW-8-3  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops 6  
msg-body drops EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
enable secret 4  
zK0wlfTcKX2vCykKR1a66B9cuSBm.LdMfoyqxEsZZ6  
!  
username admin privilege 15 secret 4  
Zhg.JW5gobPrWhU/V/eMA.F.Io4YqafsA30/DekdW3.  
no aaa new-model  
clock timezone EEST 3 0  
no ipv6 cef  
ipv6 multicast rpf use-bgp  
no ip icmp rate-limit unreachable  
!  
ip domain-name ionnikov.net  
ip name-server 192.168.8.241  
ip cef  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
vlan internal allocation policy ascending  
!  
ip tcp synwait-time 5  
ip ssh time-out 30  
ip ssh version 2  
!  
!  
!  
!  
!  
interface Ethernet0/0  
duplex auto  
!  
interface Ethernet0/1  
duplex auto  
!  
interface Ethernet0/2  
duplex auto  
!  
interface Ethernet0/3  
duplex auto
```

```

!
interface Ethernet1/0
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Vlan1
 ip address 192.168.8.252 255.255.255.0
!
ip default-gateway 192.168.8.254
!
no ip http server
!
!
access-list 1 permit 192.168.8.0 0.0.0.255
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 access-class 1 in
 login local
 transport input ssh
!
ntp server serv-8-1
end

```

```

!
interface Ethernet1/0
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Vlan1
 ip address 192.168.8.251 255.255.255.0
!
ip default-gateway 192.168.8.254
!
no ip http server
!
!
access-list 1 permit 192.168.8.0 0.0.0.255
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 access-class 1 in
 login local
 transport input ssh
!
ntp server Serv-8-1
end

```

		Іонніков В.М.			КІК.КР.Б - 125 - 08 - 25 - ПЗ	Арк.
		Фальковський І.Г.				94
Змн.	Арк.	№ докум.	Підпис	Дата		