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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЇ ЗАХИСТУ ХМАРНОГО СХОВИЩА ОРГАНІЗАЦІЇ НА БАЗІ SIEM СИСТЕМИ ALIENVAULT USM»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач(ка) вищої освіти групи БСДМ-61
ВРАДІН Клим
(ПРІЗВИЩЕ, Ім'я)

Керівник: КУЗНЕЦОВ Олександр
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
д.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Київ 2024

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

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____Галина ГАЙДУР
"___"_____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Врадіну Климу Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
«Технології захисту хмарного сховища організації на базі SIEM системи AlienVault USM»
керівник кваліфікаційної роботи: КУЗНЕЦОВ Олександр, д.т.н., професор,
(ПРІЗВИЩЕ, Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз необхідності захисту хмарного сховища організації від загроз.
2. Методики протидії загрозам хмарного сховища організації за допомогою SIEM-системи AlienVault USM.
3. Розроблення рекомендації щодо налаштування SIEM-системи AlienVault USM.

5. Перелік ілюстративного матеріалу:
Презентація:PowerPoint

6. Дата видачі завдання 19.10.2023р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності захисту хмарного сховища організації	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз необхідності захисту хмарного сховища організації на базі SIEM системи AlienVault USM	27.10. 2023р.	
4.	Вивчення рішення AlienVault USM Anywhere для захисту хмарного сховища організації	03.11.2023 р.	
5.	Розроблення рекомендацій щодо налаштування SIEM-системи AlienVault USM для захисту хмарного сховища організації	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	12.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач вищої освіти _____ Клим ВРАДІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Олександр КУЗНЕЦОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Врадін К.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: « Технології захисту хмарного сховища організації на базі SIEM системи AlienVault USM ».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***ВРАДІН Клим*** обрав тему роботи, метою якої було дослідити технології захисту хмарного сховища організації на базі SIEM системи AlienVault USM. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ВРАДІН Клим*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ВРАДІН Клим*** на оцінку «добре» та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Олександр КУЗНЕЦОВ
(підпис) *(Ім'я,ПРІЗВИЩЕ)*
"____" _____2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач ВРАДІН Клим допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 73 сторінок, 14 малюнків, 0 таблиць, 15 джерел та додатків.

Об'єкт дослідження – процес захисту хмарного сховища організації.

Предмет дослідження – технологія захисту хмарного сховища організації на прикладі рішення AlienVault USM.

Мета роботи – розробити технологію та рекомендації щодо захисту хмарного сховища на базі рішення AlienVault USM.

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

В роботі проведено аналіз поняття хмарне сховище організації. Розкрито необхідність захисту хмарного сховища організації за допомогою рішення AlienVault USM.

Досліджено загрози та проблеми хмарного сховища на схильність до несанкціонованого доступу до хмарного сховища організації. Проаналізовано методики протидії несанкціонованого доступу.

На основі досліджень проведених в роботі розроблено рекомендація щодо застосування технології виявлення та реагування на загрози у хмарному середовищі організації.

Галузь використання – захист хмарного сховища організації від несанкціонованого доступу на базі SIEM системи AlienVault USM.

ТЕХНОЛОГІЯ ЗАХИСТУ ХМАРНОГО СХОВИЩА ОРГАНІЗАЦІЇ, SIEM СИСТЕМА, ALIENVAULT USM ANYWHERE, АТАКИ, ПРАЦІВНИКИ ОРГАНІЗАЦІЇ, ТЕХНІЧНІ ЗАСОБИ

ABSTRACT

The text part of the qualification work: 73 pages, 14 figures, 0 tables, 15 sources and appendices.

The object of research is technologies aimed at protecting an organization's cloud storage.

The subject of research is the AlienVault USM technology designed to protect an organization's cloud storage.

The purpose of the work is to develop recommendations for configuring the use of AlienVault USM cloud storage protection.

Research methods - study of the literature on this topic, analysis of operating documentation, international standards and their comparison.

The article analyses the concept of cloud storage of an organization. The necessity of protecting the organization's cloud storage with the help of the AlienVault USM solution is revealed.

The threats and problems of cloud storage for the susceptibility to unauthorized access to the organization's cloud storage are investigated. The methods of counteracting unauthorized access are analyzed.

Based on the research conducted in the paper, a recommendation for the use of technology for detecting and responding to threats in the cloud environment of an organization has been developed.

Field of use – protection of an organization's cloud storage from unauthorized access based on the SIEM system AlienVault USM.

TECHNOLOGY FOR PROTECTING AN ORGANIZATION'S CLOUD STORAGE, SIEM SYSTEM, ALIENVAULT USM ANYWHERE, ATTACKS, EMPLOYEES OF THE ORGANIZATION, TECHNICAL MEANS

ЗМІСТ

ВСТУП

Актуальність дослідження.

У сучасному світі організації дедалі більше вдаються до хмарних технологій для зберігання й обробки даних через їхню масштабованість і зручність. Через такі особливості відбувається швидкісне зростання обсягу даних у хмарних сховищах. А чим більше зростає кількість даних – тим більше зростають ризики атак та спроб отримання несанкціонованого доступу до інформації, що підкреслює критичну необхідність забезпечення їх надійного захисту.

У зв'язку з активним використанням та розвитком хмарних сховищ це привертає увагу зловмисників, і з кожним роком загрози кібербезпеки стають складнішими та витонченішими. Дослідження в галузі захисту хмарних сховищ актуальне для боротьби з новими і різноманітними видами кіберзагроз.

Також необхідно дотримуватися вимог до нормативів, оскільки багато галузей підпорядковані суворим нормативам і стандартам безпеки даних. Дослідження в галузі захисту хмарних сховищ допомагають компаніям дотримуватися вимог регуляторів і уникнути можливих штрафів і шкоди репутації.

Через сучасну діджиталізацію та цифрова трансформацію бізнесу - організації все активніше переходять до хмарних сервісів. Також не слід забувати і загрози безпеки здоров'ю працівників через COVID 19, що лише збільшує бажання організацій працювати віддалено. З'являється все більше розподілених команд, і, врешті-решт, Сучасне робоче середовище все частіше використовує хмарні сховища. Тож забезпечення безпеки хмарних сховищ стає ключовим фактором для успішної цифрової стратегії та сталого розвитку.

Також, не слід забувати, що у цифровому світі стрімко розвиваються Інтернет речі (IoT) та штучний інтелект (ШІ). Із розвитком цих технологій – хмарні сховища стають ключовим елементом їхньої інфраструктури, що робить дослідження в галузі забезпечення захисту хмарних сховищ в контексті нових технологій актуальним, як ніколи.

Об'єкт дослідження – процес захисту хмарного сховища організації.

Предмет дослідження – технологія захисту хмарного сховища організації на прикладі рішення AlienVault USM.

Мета роботи – розробити технологію та рекомендації щодо захисту хмарного сховища на базі рішення AlienVault USM.

Наукові завдання:

- Провести аналіз застосування хмарного середовища;
- Дослідити загрози хмарного середовища;
- Проаналізувати технології захисту хмарного середовища;
- Розробити рекомендації з використання засобу захисту хмарного середовища AlienVault USM.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів

Практичне значення одержаних результатів. Шляхом аналізу функцій AlienVault USM і розгляду методів застосування цієї SIEM-системи для забезпечення безпеки в хмарному середовищі, дослідження прагне надати рекомендації щодо ефективного використання цього інструменту в контексті сучасної безпеки хмарних сховищ.

1 ОГЛЯД ПЛАТФОРМИ ALIENVAULT USM ТА SIEM-СИСТЕМ

1.1. Аналіз застосування хмарного сховища організаціями

Хмара (хмарна інфраструктура) - сукупність динамічно розподілюваних та налаштовуваних хмарних ресурсів, що можуть бути оперативно надані користувачу хмарних послуг і вивільнені через глобальну та локальні мережі передачі даних.

Центр обробки даних - спеціалізований технічний комплекс, що складається з інженерної (системи безперебійного електроживлення, вентиляції, охолодження та регулювання вологості, пожежної безпеки, фізичної охорони), інформаційної, електронної комунікаційної та програмно-апаратної інфраструктури, засоби якого забезпечують або реалізують надання послуг із зберігання та обробки даних, у тому числі, але не обмежуючи: надання хмарних послуг, резервного копіювання даних, передачі даних, оренди комунікаційних стійок, послуг хостингу.

Історія хмарних обчислень сягає корінням у 1960-ті роки, коли вперше було запропоновано "міжгалактичну комп'ютерну мережу".

У 1963 році DARPA (the Defense Advanced Research Projects Agency) виділило Массачусетському технологічному інституту 2 мільйони доларів на проект MAC. Субсидування включало умову, що інститут повинен був створювати нові технології з урахуванням того, що "комп'ютер буде використовуватися щонайменше двома особами"

У 1969 році Джозеф Карл Роббнет Ліклайдер (далі - Лік) створив ARPANET (Advanced Research Projects Agency Network), надзвичайно простий варіант Інтернету. Лік був одночасно і терапевтом, і дослідником комп'ютерів, і втілював мрію під назвою "Міжгалактична комп'ютерна мережа", в якій всі люди на планеті

були б пов'язані між собою за допомогою комп'ютерів і могли б отримати доступ до даних з будь-якого місця.

Рух віртуалізації розпочався в 1970-х роках, і зараз включає в себе створення віртуальної машини, яка працює так само, як справжній ПК, з цілком практичним і робочим середовищем. Ідея віртуалізації також розвинулася з появою Інтернету, коли організації почали пропонувати "віртуальні" приватні системи в оренду. Використання віртуальних ПК почало набирати обертів у 1990-х роках, що призвело до розвитку передових хмарних обчислень.

Між 1970-ми та 90-ми роками було досягнуто значного прогресу у розвитку хмарних обчислень. Наприклад, монстр комп'ютерної індустрії IBM у 1972 році створив робочу платформу під назвою VM (Virtual Machine - віртуальна машина). У 1990-х роках кілька медіа-організацій запропонували власні варіанти віртуалізованих приватних систем (VPN).

Коли хмарні обчислення почали поширюватися, вони швидко пішли вперед і продовжували розвиватися. Хоча існують певні розбіжності щодо походження цього терміну, до 1996 року хмарні обчислення енергійно розвивалися, для організацій, освітніх установ та численних підприємств.

Хмарні сховища надають організаціям гнучке та ефективне середовище для зберігання, управління та обробки даних. Я опишу декілька способів, якими організації використовують хмарні сховища:

1. Зберігання та обмін файлами:

Використання хмарних сховищ для зберігання та обміну файлами надає організаціям зручний і безпечний спосіб спільної роботи. Ось більш детальне пояснення:

- *Централізоване зберігання даних.* Хмарні сховища надають централізоване і надійне місце для зберігання даних. Співробітники можуть завантажувати файли в хмару, що дає їм змогу легко отримувати доступ до цих файлів з будь-якого пристрою з підключенням до інтернету.

- *Спільна робота над файлами.* Організації можуть створювати спільні папки і проекти в хмарних сховищах, де співробітники можуть спільно працювати над документами, таблицями, презентаціями та іншими файлами. Співробітники можуть одночасно редагувати файли, стежити за змінами та коментувати вміст, що полегшує спільну розробку, редагування та обмін ідеями в реальному часі.
- *Управління правами доступу.* Хмарні сховища надають гнучкі налаштування прав доступу. Адміністратори можуть керувати, хто має доступ до яких файлів, і визначати рівні дозволів, що забезпечує безпеку та конфіденційність даних.
- *Синхронізація між пристроями.* Файли, завантажені в хмарне сховище, автоматично синхронізуються між пристроями. Це дає змогу співробітникам отримувати доступ до своїх файлів з комп'ютера, планшета або смартфона, що особливо корисно в умовах віддаленої роботи.
- *Історія версій файлів.* Хмарні сховища зберігають історію версій файлів, що дає змогу відновлювати попередні версії та відстежувати зміни. Це корисно для запобігання втрати даних і відновлення попередніх станів документів.
- *Інтеграція з додатками.* Багато хмарних сховищ інтегруються з різними додатками, як-от офісні пакети (Microsoft Office 365, Google Workspace), що полегшує редагування та обмін документами прямо в хмарному середовищі.
- *Зручність використання.* Простота використання хмарних сховищ робить процес обміну файлами інтуїтивно зрозумілим для співробітників. Вони можуть просто перетягувати і завантажувати файли, не вимагаючи спеціальних технічних навичок.

2. Резервне копіювання та відновлення:

Є декілька факторів, які роблять хмарні сховища привабливим варіантом для резервного копіювання даних, забезпечуючи ефективність, безпеку та доступність:

- *Гнучкість*. Хмарні сховища надають гнучку інфраструктуру для резервного копіювання даних. Організації можуть легко збільшувати або зменшувати обсяг збережених даних залежно від своїх потреб.

- *Автоматизація процесів резервного копіювання*. Багато хмарних платформ надають інструменти для автоматизації процесів резервного копіювання. Це включає в себе створення регулярних розкладів копіювання, автоматичне виявлення змін у даних і автоматичне виконання копіювання.
- *Висока доступність і відмовостійкість*. Хмарні сховища забезпечують високу доступність і відмовостійкість. Дані резервних копій можуть бути розміщені в розподілених центрах обробки даних, що забезпечує збереження даних навіть у разі збоїв обладнання або мережі.
- *Шифрування та безпека даних*. Хмарні платформи забезпечують механізми шифрування даних у спокої та в процесі їх передачі. Це важливо для захисту конфіденційної інформації, коли співробітники отримують доступ до даних з мобільних пристроїв у громадських місцях або через відкриті мережі, а також забезпечує додатковий рівень безпеки для збережених резервних копій.

3. Обробка великих обсягів даних:

Хмарні сховища надають низку можливостей для ефективного зберігання та обробки великих обсягів даних:

- *Масштабованість*. Однією з основних переваг хмарних сховищ є те, що вони забезпечують масштабовану інфраструктуру, що дає змогу збільшувати обсяг даних, що зберігаються, у міру необхідності, яка може легко справлятися навіть з величезними обсягами даних, що генеруються пристроями IoT. Це особливо важливо з огляду на величезну кількість пристроїв, що відправляють дані в режимі реального часу. Це дозволяє організаціям адаптуватися до зростаючих потреб і уникати неефективного використання ресурсів.
- *Платформи обробки даних*. Багато хмарних провайдерів надають платформи для обробки даних у хмарі, як-от Amazon Web Services (AWS) з його сервісами Amazon S3 і Amazon EC2, Microsoft Azure з Azure Blob Storage і Azure HDInsight, а також Google Cloud Storage і BigQuery. Ці сервіси дають змогу проводити різні операції обробки та аналізу даних просто в хмарі.

- *Прискорений доступ до даних*. Хмарні сховища забезпечують швидкий і зручний доступ до даних з будь-якої точки світу. Це досягається за рахунок використання географічно розподілених серверних центрів і технологій кешування, що особливо важливо для ефективного обміну та обробки даних.
- *Хмарні бази даних*. Багато хмарних провайдерів надають послуги хмарних баз даних, такі як Amazon Aurora, Microsoft Azure SQL Database, Google Cloud Firestore та інші. Ці сервіси забезпечують масштабовані та високопродуктивні рішення для зберігання й обробки структурованих даних.
- *Інструменти для аналізу даних*. Хмарні сховища надають доступ до різних інструментів і сервісів для аналізу даних, таких як Apache Spark, Hadoop та інші. Ці інструменти дають змогу проводити складні операції аналізу та обробки даних у хмарі.
- *Інтеграція з Big Data та аналітикою*. Хмарні сховища добре інтегруються з платформами для Big Data та аналітики даних, що дає змогу ефективно проводити аналіз великих обсягів структурованих і неструктурованих даних.

4. Робота з мобільними пристроями:

Є декілька механізмів, що забезпечують високий рівень мобільності та доступності, дозволяючи співробітникам ефективно працювати з даними у хмарних сховищах у будь-якій точці світу та з будь-якого пристрою:

- *Мобільні додатки*. Хмарні сховища надають мобільні додатки, які можна встановити на смартфони та планшети. Ці додатки забезпечують зручний інтерфейс для доступу до файлів, синхронізації даних і виконання інших завдань.
- *Синхронізація даних*. Багато хмарних сховищ пропонують функцію автоматичної синхронізації даних між пристроями. Це означає, що якщо співробітник завантажує файл у хмарне сховище з комп'ютера, цей файл автоматично стає доступним на його мобільному пристрої.
- *Хмарний доступ через веб-інтерфейс*. Крім мобільних додатків, співробітники можуть отримувати доступ до своїх даних через веб-інтерфейс

хмарного сховища. Це означає, що вони можуть використовувати веб-браузер на своєму мобільному пристрої для входу в систему і роботи з файлами.

- *Управління правами доступу*. Хмарні сховища надають гнучку систему управління правами доступу. Співробітники можуть налаштовувати, кому і які права надаються на їхні файли. Це дає їм змогу безпечно спільно використовувати інформацію, обмежуючи доступ тільки тим, кому це необхідно.
- *Мультиплатформність*. Хмарні сховища розробляються з урахуванням Мультиплатформності, що забезпечує роботу на різних операційних системах, включно з iOS, Android і Windows. Це дає змогу співробітникам обирати пристрої на свій смак.
- *Повідомлення та моніторинг*. Багато хмарних сховищ надають функції сповіщень, тож співробітники можуть бути проінформовані про важливі зміни в даних або про активність у їхніх акаунтах. Моніторинг забезпечує контроль за безпекою та активністю облікових записів.

5. Зберігання та аналіз даних IoT:

Для організацій, що працюють з даними Інтернет речей (IoT), хмарні сховища надають кілька значних переваг:

- *Гнучкість зберігання даних*. Для IoT-додатків важлива гнучкість у зберіганні різноманітних даних, таких як часові ряди, логи, зображення, відео та інші формати. Хмарні сховища забезпечують можливість зберігання та обробки різних типів даних.
- *Обробка даних у реальному часі*. Хмарні сховища дають змогу організаціям обробляти дані IoT в режимі реального часу. Це важливо для оперативного реагування на події, що генеруються пристроями, і ухвалення рішень у реальному часі.
- *Аналітика даних*. За допомогою хмарних сховищ організації можуть виконувати аналітику даних IoT, виявляти тренди, проводити прогнозування і виявляти аномалії. Це може бути корисно для оптимізації виробничих процесів, передбачення відмов обладнання та інших додатків.

- *Інтеграція з іншими хмарними сервісами*. Хмарні сховища легко інтегруються з іншими хмарними сервісами, такими як аналітика даних, машинне навчання і штучний інтелект. Це дає змогу створювати комплексні рішення для оброблення та аналізу даних IoT.
- *Безпечне зберігання та обмін даних*. Хмарні сховища надають засоби для безпечного зберігання та обміну даними IoT. Це включає в себе механізми шифрування, контроль доступу та інші заходи безпеки, які захищають дані від несанкціонованого доступу.
- *Глобальний доступ*. Організації можуть отримувати доступ до даних IoT з будь-якої точки світу, що особливо важливо в контексті глобальних мереж IoT. Це підтримує гнучкість і мобільність в управлінні та моніторингу пристроїв.

6. Хостинг веб-сайтів і додатків:

Загальна перевага використання хмарних сховищ для хостингу веб-сайтів та додатків досягається завдяки:

- *Веб-сайти*. Багато хмарних провайдерів надають послуги хостингу веб-сайтів. Організації можуть завантажувати свої веб-сайти на хмарні сервери, що забезпечує високу доступність і швидкодію. Хмарні сховища дають змогу масштабувати ресурси залежно від навантаження, забезпечуючи стабільну роботу навіть за різкого збільшення відвідуваності.
- *Додатки*. Розробники додатків використовують хмарні сховища для хостингу своїх додатків. Хмарні платформи надають інфраструктуру, необхідну для виконання і масштабування додатків. Це особливо актуально для мікросервісної архітектури, де різні компоненти програми можуть бути розміщені на різних хмарних серверах.
- *Сервіси*. Багато хмарних сховищ надають також сервіси для виконання різних функцій, як-от бази даних, кешування, обробка зображень та інші. Компанії можуть використовувати ці хмарні сервіси у своїх додатках, уникаючи необхідності самостійного управління складною інфраструктурою.

- *Глобальне розгортання*. Хмарні сховища забезпечують можливість глобального розгортання. Веб-сайти та додатки можуть бути розміщені на серверах у різних частинах світу, що покращує продуктивність і скорочує затримки для користувачів у різних регіонах.
- *Управління навантаженням*. Хмарні платформи надають засоби для балансування навантаження, що дає змогу рівномірно розподіляти трафік між різними серверами. Це допомагає забезпечити стабільну роботу веб-сайтів і додатків навіть за високих навантажень.
- *Висока доступність*. Хмарні сховища забезпечують високу доступність за рахунок розподілу даних і застосунків на кількох серверах. У разі збою в одному з центрів обробки даних, інші можуть продовжувати забезпечувати працездатність.

7. Спільна робота та віддалена робота:

Хмарні сховища відіграють ключову роль у забезпеченні спільної роботи та ефективної віддаленої роботи команд:

- *Інтеграція з комунікаційними засобами*. Багато хмарних сховищ інтегруються з комунікаційними інструментами, як-от чати, відеоконференції та електронна пошта, полегшуючи комунікацію та обговорення проектів.
- *Можливості коментування та зворотного зв'язку*. Користувачі можуть залишати коментарі та зворотний зв'язок безпосередньо у файлі, що скорочує необхідність обміну електронними листами і прискорює процес прийняття рішень.

Відповідно закону України «Про хмарні послуги» хмарні послуги надаються в один із таких способів:

- *Приватна хмара* - хмарна інфраструктура, що підготовлена для використання єдиним користувачем хмарних послуг та контролюється ним;
- *Колективна хмара* - хмарна інфраструктура, що поділена між визначеною групою взаємопов’язаних користувачів хмарних послуг, які мають

спільні потреби, та контролюється користувачами хмарних послуг самостійно або їх представниками;

- *Публічна хмара* - хмарна інфраструктура, що потенційно доступна для невизначеного кола користувачів хмарних послуг та контролюється надавачем хмарних послуг;
- *Гібридна хмара* - хмарна інфраструктура, що є композицією з двох або більше різних хмарних інфраструктур (приватні, колективні або публічні), що є самостійними об'єктами, пов'язаними між собою технологіями, що дозволяють переносити дані або комп'ютерні програми між цими об'єктами.

У сфері хмарних розгортань ми виявляємо розмаїття моделей хмарних сервісів, що охоплюють інфраструктуру, платформи та програмне забезпечення. Ці моделі хмарних сервісів не є ізольованими варіантами, навпаки, вони надають гнучку основу для створення комбінованих рішень, які цілком можуть бути використані в симбіозі або навіть паралельно.

Давайте розглянемо три основні моделі хмарних сервісів:

1. *IaaS (Infrastructure-as-a-Service)* – надає віртуальні обчислювальні ресурси через інтернет. Це включає в себе віртуальні машини, сховище даних і мережеві ресурси. Користувачі IaaS можуть орендувати інфраструктурні компоненти в міру необхідності, замість того щоб інвестувати у власні фізичні сервери та інфраструктуру.

Основні характеристики IaaS:

- Віртуалізація ресурсів: IaaS надає віртуальні ресурси, такі як віртуальні машини (VMs), сховище та мережеві елементи. Це дає змогу користувачам гнучко масштабувати свою інфраструктуру залежно від потреб.
- Самообслуговування та миттєвий доступ: Користувачі IaaS можуть самостійно керувати та налаштовувати віртуальні машини та інші ресурси через інтерфейс управління. Доступ до ресурсів відбувається миттєво за запитом.

- Еластичність і масштабованість: Користувачі мають можливість масштабувати ресурси вгору або вниз відповідно до вимог додатків або бізнесу. Це дає змогу оптимізувати використання ресурсів і знижувати витрати.
- Оплата за використанням (Pay-as-You-Go): Користувачі платять за використання застосунку залежно від своїх потреб. Це забезпечує гнучкість та оптимізацію витрат.

Приклад постачальника послуг IaaS: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Softlayer, Amazon EC2, GigaCloud.

2. PaaS (Platform-as-a-Service) – надає платформу розробки та розгортання застосунків через інтернет, прибираючи необхідність управління нижчою інфраструктурою. Це охоплює інструменти та сервіси, необхідні для розробки, тестування та розгортання застосунків.

Основні характеристики PaaS:

- Розробка додатків без турбот про інфраструктуру: PaaS дає змогу розробникам фокусуватися на створенні додатків, не витрачаючи час на управління інфраструктурою, такою як сервери та мережі.
- Інструменти для розробки: PaaS надає інтегровані інструменти розробки, як-от мови програмування, середовища виконання, бази даних і засоби тестування.
- Автоматичне масштабування: Системи PaaS забезпечують автоматичне масштабування ресурсів залежно від вимог додатків, що полегшує управління навантаженням і забезпечує стабільну продуктивність.
- Високий рівень абстракції: PaaS абстрагує деталі інфраструктури, надаючи простий і єдиний інтерфейс для розробників.

Приклад постачальника послуг PaaS: Google App Engine, IBM Bluemix, Microsoft Azure, VMWare Cloud Foundry, Heroku.

3. SaaS (Software-as-a-Service) – це модель хмарних обчислень, що надає доступ до програмного забезпечення через інтернет. Користувачі отримують

доступ до додатків через веб-браузер, без необхідності встановлення, налаштування та обслуговування програмного забезпечення на своїх пристроях.

Основні характеристики SaaS:

- Доступ через інтернет: Додатки SaaS забезпечуються і доступні через інтернет. Користувачі можуть отримати до них доступ з будь-якого місця і з будь-якого пристрою.
- Багатокористувацький режим: Додатки SaaS підтримують багатокористувацький режим, що дає змогу кільком користувачам одночасно працювати з одним і тим самим додатком.
- Автоматичне оновлення: Уся робота з обслуговування, включно з оновленнями та поліпшеннями, здійснюється провайдером SaaS автоматично. Користувачам не потрібно піклуватися про підтримку та оновлення.
- Оплата за використанням (Pay-as-You-Go): Користувачі платять за використання застосунку залежно від своїх потреб. Це забезпечує гнучкість та оптимізацію витрат.

Приклад постачальника послуг SaaS: Dropbox, Google Doc, Microsoft Office 365, Facebook, Salesforce.

4. Безсерверні обчислення – це модель хмарних обчислень, у якій розробники можуть створювати та виконувати функції (невеликі фрагменти коду) без необхідності управління інфраструктурою. У цій моделі забезпечується автоматичне масштабування та виділення ресурсів під час виконання функцій.

Основні характеристики безсерверних обчислень:

- Відсутність управління інфраструктурою: Розробники концентруються на написанні коду функцій, не турбуючись про сервери, операційні системи або віртуальні машини.
- Автоматичне масштабування: Ресурси автоматично масштабуються залежно від навантаження. Система надає ресурси для виконання функцій і автоматично масштабується вгору або вниз.

- Оплата за фактичне використання: Плата стягується тільки за фактично використані ресурси під час виконання функцій, що робить цю модель економічно ефективною.
- Подієво-орієнтована архітектура: безсерверні обчислення часто використовуються в архітектурі, що базується на подіях, де функції виконуються у відповідь на події, як-от зміни в сховищі даних або запити від користувачів.

Приклад постачальника послуг безсерверних обчислень: AWS Lambda, Azure Functions, Google Cloud Functions.

1.2. Аналіз загроз хмарних сховищ організацій

Хмарні системи надають доступне і зручне рішення для зберігання та управління даними з мінімальними витратами для IT-відділу. Крім того, вони забезпечують вбудовані засоби аварійного відновлення і доступні в будь-який час і в будь-якому місці. Однак, якщо конфіденційні дані, що зберігаються в цих системах, потраплять до рук шахраїв або зловмисників, це може призвести до серйозних наслідків для організації. Зокрема, це може призвести до штрафів від регулюючих установ, збільшення витрат на IT-інфраструктуру, зниження продуктивності та обсягів продажів, а також до втрати клієнтів і підриву репутації.

Тож зараз розглянемо деякі загрози для хмарних сховищ:

1. Міжмережеві атаки (Intercloud Attacks): Міжмережеві атаки являють собою загрози безпеці, які спрямовані на хмарні сервіси через їхню внутрішню інфраструктуру або пов'язані мережі. Ці атаки можуть мати різні форми та цілі, і вони підкреслюють необхідність посилення безпеки хмарних середовищ.

Види міжмережевих атак:

- *Сніффер-атаки* - це крадіжки даних, спричинені перехопленням мережевого трафіку за допомогою сніфферів пакетів, які можуть незаконно отримати доступ до незашифрованих даних і прочитати їх. Пакети даних

перехоплюються, коли вони проходять через комп'ютерну мережу. Сніффери пакетів - це пристрої або носії інформації, які використовуються для здійснення сніффер-атаки та перехоплення мережевих пакетів даних. Їх називають аналізаторами мережевих протоколів. Якщо пакети не зашифровані за допомогою надійного мережевого захисту, хакери зможуть викрасти дані і отримати до них доступ. Існують різні аналізатори пакетів, такі як Wireshark, Dsniff, Etherpeek тощо.

- *Спуфінг* – це акт маскування комунікації або ідентичності таким чином, щоб створити враження, що вона пов'язана з довіреним, авторизованим джерелом. Спуфінг-атаки можуть набувати різних форм, від звичайних підробок електронної пошти, які використовуються у фішингових кампаніях, до підробок ідентифікаторів абонентів, які часто використовуються для шахрайства. Зловмисники також можуть націлюватися на більш технічні елементи мережі організації, такі як IP-адреса, сервер системи доменних імен (DNS) або служба протоколу дозволу адрес (ARP), в рамках підміни.

- Атаки за допомогою *SQL-ін'єкцій* полягають у вставці або "впровадженні" SQL-запиту через вхідні дані від клієнта до програми. Успішний експлойт SQL-ін'єкції може зчитувати конфіденційні дані з бази даних, модифікувати дані бази даних (вставляти/оновлювати/видаляти), виконувати операції адміністрування бази даних (наприклад, вимикати СУБД), відновлювати вміст певного файлу, присутнього у файловій системі СУБД, а в деяких випадках - віддавати команди операційній системі. Атаки типу SQL-ін'єкція - це різновид ін'єкційних атак, в яких команди SQL вводяться у вхідні дані для того, щоб вплинути на виконання попередньо визначених команд SQL.

2. DDoS-атаки (Distributed Denial of Service): DDoS-атаки являють собою форму кібератак, під час якої безліч комп'ютерів або пристроїв використовують для одночасного нападу на цільовий ресурс, перевантажуючи його і роблячи недоступним для легітимних користувачів. Ось кілька ключових аспектів DDoS-атак:

1) Мета атак:

- Сайти і веб-додатки: Основні цілі DDoS-атак включають в себе сайти, онлайн-магазини, банківські системи і веб-додатки.
- Інфраструктура мережі: Атаки можуть бути спрямовані на мережеву інфраструктуру, включаючи DNS-сервери, маршрутизатори та інші ключові компоненти.

2) Види DDoS-атак:

- Напад на пропускну здатність (Bandwidth-Based Attacks): Нападники намагаються перевантажити канал зв'язку цілі, засмічуючи його трафіком.
- Атаки на рівні додатків (Application Layer Attacks): Зловмисники прагнуть створити високе навантаження на служби, такі як HTTP або DNS, щоб спотворити доступність для легітимних запитів.
- Напад на рівень протоколу (Protocol-Based Attacks): Атаки, спрямовані на слабкості в мережевих протоколах, наприклад, атаки SYN/ACK, ICMP-атаки.

3) Навіщо проводять DDoS-атаки:

- Відмова в обслуговуванні: Метою атак є надання недоступності цільового ресурсу для легітимних користувачів.
- Політичні або ідеологічні мотиви: Деякі DDoS-атаки проводять для вираження протесту, утвердження ідеології або вираження політичної позиції.

4) Distributed Nature (Розподілена природа):

- Ботнети: Нападники використовують ботнети, мережі скомпрометованих комп'ютерів і пристроїв, щоб посилити масштаб атаки.
- Ампліфікація: Атаки можуть використовувати вразливості в протоколах, щоб створити ампліфіковану відповідь, що збільшує обсяг трафіку.

5) Заходи щодо запобігання та захисту:

- Використання CDN (Content Delivery Network): CDN може допомогти розподіляти трафік і забезпечувати доступність навіть в умовах DDoS-атаки.
- Фільтрація трафіку: Використання технологій фільтрації для розпізнавання і блокування шкідливого трафіку.

- Використання WAF (Web Application Firewall): WAF може допомогти захистити веб-додатки від атак на рівні додатків.
- Моніторинг і виявлення: Системи моніторингу та виявлення аномалій можуть допомогти виявити DDoS-атаку на ранніх стадіях.

3. Дослідження слабких місць (Cloud Service Exploitation): Хмарні сховища надають безліч переваг, але вони також схильні до різних загроз безпеці. Дослідження слабких місць у безпеці хмарних сховищ може виявити вразливості, які можуть бути використані зловмисниками. Ось кілька типових загроз із дослідженням слабких місць:

1) Незадовільне управління доступом:

- Слабкі облікові записи: Використання слабких паролів або недостатнє управління обліковими записами може призвести до несанкціонованого доступу до хмарних даних.
- Відсутність багатофакторної автентифікації: Якщо ввімкнено тільки однофакторну автентифікацію, це може зробити облікові записи більш уразливими.

2) Необґрунтований розподіл прав доступу:

- Привілеї за замовчуванням: Деякі хмарні сховища можуть надавати зайві привілеї за замовчуванням, що збільшує ризик компрометації даних.

3) Недостатній захист даних:

- Відсутність шифрування: Якщо дані не шифруються в спокої або в процесі передачі, це може створити можливості для несанкціонованого доступу.
- Відсутність оновлень і патчів: Неоновлене програмне забезпечення може мати відомі вразливості, які зловмисники можуть використовувати.

4) Недостатній захист від загроз на рівні додатків:

- Дослідження слабких місць у коді: Зловмисники можуть шукати вразливості в коді застосунків, що працюють із хмарними даними.
- Несанкціоновані API-запити: Зловмисники можуть використовувати несанкціоновані API-запити для отримання доступу до даних.

5) Відсутність моніторингу та виявлення:

- Неактивні системи моніторингу: Якщо системи моніторингу неактивні або неправильно налаштовані, атаки можуть залишатися непоміченими.
- Недостатні журнали аудиту: Відсутність докладних журналів аудиту ускладнює виявлення аномальної активності.

6) Загрози, пов'язані з делегованим управлінням і передбачуваними довіреними відносинами:

- Компрометація довірених акаунтів: Якщо акаунти з довіреними правами доступу компрометовані, це може створити серйозні загрози безпеці.
- Недостатні контрольні заходи в делегованих відносинах: Відсутність суворих контрольних заходів у відносинах між хмарними постачальниками і клієнтами може стати джерелом загроз.

7) Недостатні засоби реагування та відновлення:

- Відсутність плану реагування на інциденти: Якщо організація не має чіткого плану з реагування на інциденти, це може ускладнити ефективне управління загрозами.

1.3. Технологія SIEM-систем та їх роль у забезпеченні безпеки

Компанія Gartner запровадила термін "SIEM" у звіті 2005 року під назвою "Покращення IT-безпеки за допомогою управління вразливостями". Цей термін об'єднує концепції управління подіями безпеки (SEM) та управління інформацією безпеки (SIM), щоб досягти найкращого з обох світів.

SEM охоплює моніторинг і кореляцію подій в режимі реального часу, а також оповіщення конфігурації і консолі, пов'язаних з цими діями. SIM переносить ці дані на наступний етап, який включає зберігання, аналіз та звітування про результати.

Система управління інформацією та подіями безпеки (SIEM) - це рішення для забезпечення безпеки, яке допомагає організаціям розпізнавати та усувати

потенційні загрози та вразливості безпеки до того, як вони встигнуть порушити бізнес-операції. SIEM-системи допомагають командам корпоративної безпеки виявляти аномалії в поведінці користувачів і використовувати штучний інтелект (ШІ) для автоматизації багатьох ручних процесів, пов'язаних з виявленням загроз і реагуванням на інциденти. Ось декілька ключових аспектів SIEM-систем:

1. Збір даних:
   - Логи та події: SIEM-системи збирають дані з різних джерел, таких як журнали подій, системи безпеки, мережеві пристрої та застосунки.
2. Нормалізація та агрегація:
   - Перетворення даних: Отримані дані нормалізуються і агрегуються для забезпечення стандартизації формату і спрощення аналізу.
3. Зберігання даних і аудит:
   - База даних: SIEM зберігає дані для подальшого аналізу та аудиту, забезпечуючи можливість ретроспективного розслідування подій.
   - Аудит безпеки: Ведення докладних журналів аудиту для відповідності нормативним вимогам і забезпечення відстежуваності подій.
4. Відповідь на інциденти:
   - Автоматизована відповідь: SIEM може надавати можливості для автоматизованого реагування на певні типи подій або інцидентів.
   - Повідомлення та попередження: Система генерує повідомлення та попередження для оперативного реагування на потенційні загрози.
5. Інтеграція з іншими системами:
   - Спільна робота з іншими інструментами: SIEM інтегрується з іншими системами безпеки та моніторингу, такими як фаєрволи, антивіруси та системи виявлення вторгнень.
6. Управління відповідністю:
   - Відповідність стандартам: SIEM-системи надають засоби для управління відповідністю організації стандартам безпеки та регуляторним вимогам.
7. Масштабованість:

- Масштабована архітектура: SIEM розробляється з урахуванням можливості масштабування, що дає змогу їй обробляти великі обсяги даних.

Одна із основних задач SIEM-систем – це Аналіз та виявлення інцидентів. Аналіз і виявлення інцидентів у SIEM-системах відіграють важливу роль у забезпеченні безпеки, даючи змогу виявляти й реагувати на загрози на ранніх стадіях, мінімізуючи потенційні наслідки для організації. Основні задачі, які виконує SIEM-система:

1. Кореляція подій:

- Визначення зв'язків: SIEM-системи здійснюють аналіз даних, щоб виявляти зв'язки між різними подіями, що відбуваються в мережі. Наприклад, вони можуть визначати, що певні події відбуваються одночасно або в певній послідовності.
- Створення шаблонів: Алгоритми кореляції дають змогу створювати шаблони, які визначають типові сценарії атак або незвичайну поведінку.

2. Виявлення аномалій:

- Порівняння з нормальною поведінкою: SIEM-системи вивчають звичайну поведінку мережі та пристроїв, визначаючи типові зразки активності. Коли з'являються аномалії, система їх виявляє.
- Математичні моделі: Деякі SIEM-системи використовують математичні моделі для передбачення очікуваної поведінки мережі та виявлення відхилень.

3. Контекстуальний аналіз:

- Збір контексту: SIEM враховує контекст подій, аналізуючи дані, зібрані з різних джерел. Це дає змогу системі краще розуміти значення подій.
- Аналіз у межах ширшого контексту: Система оцінює не тільки окремі події, а й їхній взаємозв'язок з іншими, що сприяє глибшому аналізу та розумінню потенційних загроз.

4. Виявлення подій безпеки:

- Використання сигнатур: SIEM використовує бібліотеки сигнатур, які включають відомі зразки шкідливої поведінки або атак. Коли виявляються події, що відповідають цим сигнатурам, система генерує попередження.
- Розширене виявлення: Деякі системи використовують складніші методи, як-от машинне навчання, для розпізнавання нестандартних загроз.

5. Генерація алертів і повідомлень:

- Автоматичне сповіщення: У разі виявлення потенційних інцидентів SIEM-системи можуть автоматично генерувати алерти та сповіщення.
- Класифікація рівня загрози: Системи можуть присвоювати рівень серйозності виявленим інцидентам відповідно до їхнього потенційного впливу.

Ось декілька найпопулярніших SIEM-систем, що використовуються організаціями у всьому світі:

1. Splunk Enterprise Security:

Особливості: Splunk надає потужні інструменти для збору, аналізу та візуалізації даних безпеки. Splunk Enterprise Security призначений спеціально для вирішення завдань інформаційної безпеки.

2. IBM QRadar:

Особливості: QRadar від IBM пропонує функції збору та аналізу даних, а також інструменти для виявлення загроз і реагування на інциденти.

3. ArcSight (Micro Focus):

Особливості: ArcSight, тепер у складі Micro Focus, надає широкий спектр функцій для збору, аналізу та реагування на події безпеки.

4. LogRhythm:

Особливості: LogRhythm надає рішення з моніторингу та аналізу подій безпеки, включно з інтеграцією з іншими системами безпеки.

5. SolarWinds Security Event Manager (SEM):

Особливості: SEM від SolarWinds пропонує інструменти для збору та аналізу даних безпеки, а також для управління інцидентами.

6. AlienVault USM (тепер AT&T Cybersecurity):

Особливості: AlienVault USM надає функції SIEM, а також інтегровані інструменти виявлення загроз, управління активами та власну базу даних загроз.

7. RSA NetWitness:

Особливості: RSA NetWitness забезпечує моніторинг подій, виявлення загроз і реагування на інциденти, включно з аналізом трафіку і пакетів даних.

8. Symantec Security Information Manager (SSIM):

Особливості: SSIM від Symantec надає засоби збору та аналізу даних безпеки, а також інструменти для роботи із загрозами.

9. Fortinet FortiSIEM:

Особливості: FortiSIEM від Fortinet надає SIEM-функції, включно з виявленням загроз та інструментами для управління безпекою.

10. Cisco SecureX Threat Response:

Особливості: Це рішення Cisco надає інтегровану платформу для збору та аналізу даних безпеки з метою забезпечення виявлення та реагування на загрози.

2 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ХМАРНОГО СХОВИЩА ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ ПЛАТФОРМИ ALIENVAULT USM

2.1. Архітектура SIEM-систем AlienVault USM у забезпеченні безпеки хмарних сховищ

AlienVault USM була розроблена компанією AlienVault. Наразі, після придбання, вона стала частиною корпорації AT&T Cybersecurity.

Компанія AlienVault була заснована в 2007 році з метою надання рішень у сфері інформаційної безпеки, доступних для невеликих і середніх підприємств. У компанії було стратегічне бачення у створенні всеосяжного рішення, що об'єднує кілька аспектів безпеки в єдину платформу.

З моменту свого створення AlienVault стала однією з провідних компаній у сфері управління подіями інформаційної безпеки (SIEM) і виявлення загроз. Вони також відомі своїм підходом до створення інтегрованих рішень, які об'єднують функціонал SIEM з іншими аспектами безпеки.

У 2018 році AT&T придбала AlienVault, інтегрувавши її у свій підрозділ Cybersecurity. Це придбання дало початок новому етапу в розвитку AlienVault, а тепер вона функціонує як частина більшої структури AT&T Cybersecurity.

Після інтеграції в AT&T Cybersecurity, AlienVault USM стала відомою як AT&T Cybersecurity USM (Unified Security Management). Це рішення поєднує в собі безліч інструментів безпеки, як-от SIEM, виявлення загроз, управління вразливостями та інші, для забезпечення комплексного підходу до інформаційної безпеки.

AlienVault USM (AT&T Cybersecurity) продовжує надавати організаціям ефективні інструменти для моніторингу та забезпечення безпеки своїх інформаційних систем.

AlienVault USM – це єдина уніфікована платформа для виявлення загроз, реагування на інциденти та забезпечення відповідності вимогам.

AlienVault Unified Security Management (USM) пропонує виявлення загроз, реагування на інциденти та дотримання нормативних вимог на єдиній платформі. USM централізує моніторинг безпеки мереж і пристроїв у хмарі, в приміщеннях і на віддалених об'єктах, допомагаючи вам виявляти загрози практично будь-де.

Станом на зараз компанія AT&T Cybersecurity надає доступ до свого продукту за 4 способами (Рис.2.1.):

- Безкоштовна, пробна версія на 14 діб;
- Базова версія за 1075$ на рік;
- Стандартна версія за 1695$ на рік;
- Преміум версія за 2595$ на рік.

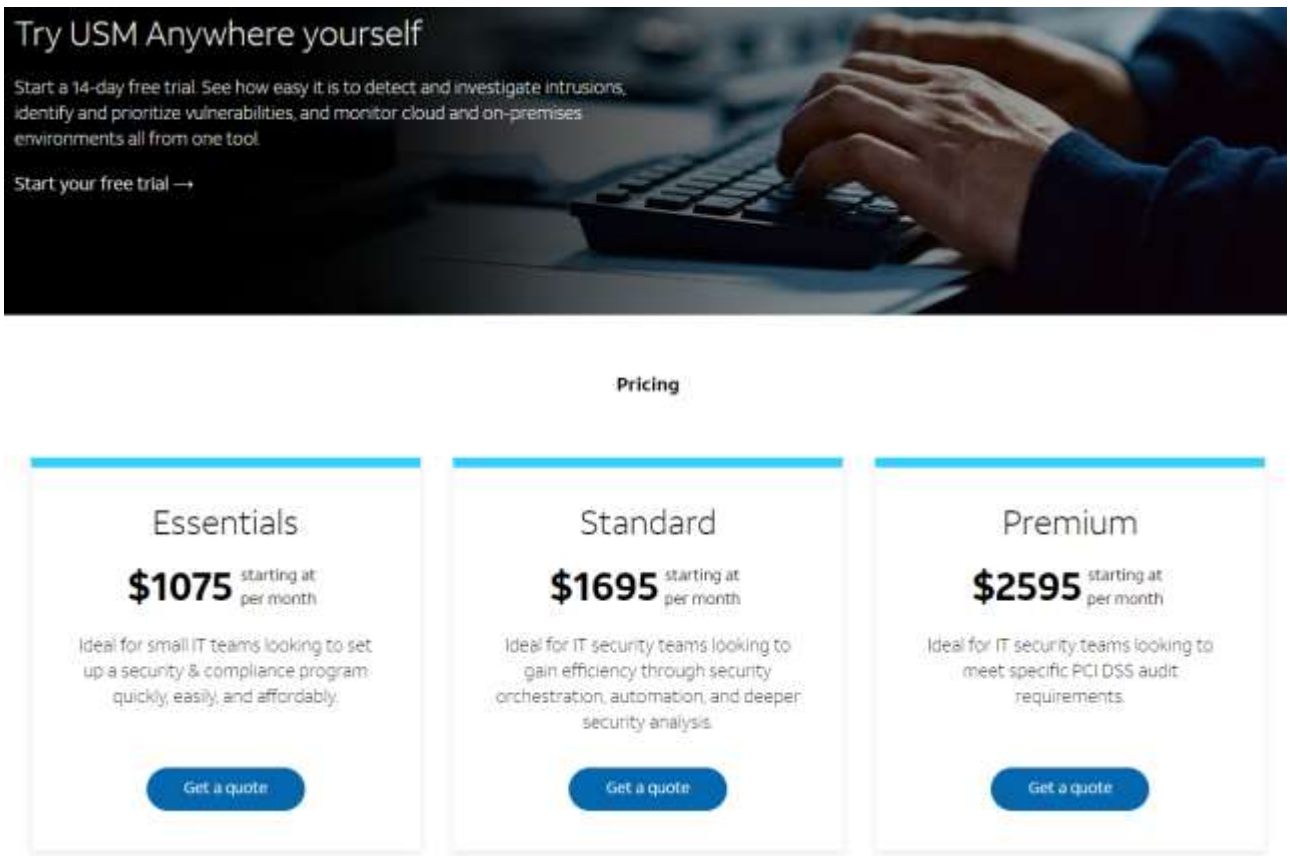

Рис.2.1. Цінова політика компанії

AT&T Cybersecurity робить дотримання нормативних вимог головним пріоритетом як для організації з якою вона співпрацює, так і для самої себе. AT&T

Cybersecurity впровадили Систему кібербезпеки NIST (NIST Cybersecurity Framework, CSF), узгодивши свої засоби контролю та процеси безпеки з перевіреними галузевими передовими практиками. Ця компанія використовує власну платформу USM для демонстрації та підтримки відповідності, співпрацюючи зі сторонніми аудиторами для регулярного тестування своїх систем, засобів контролю та процесів.

AlienVault USM має багато особливостей:

- Розумний, автоматизований збір та аналіз даних

AlienVault USM автоматично збирає та аналізує дані по всій поверхні атаки, допомагаючи організаціям швидко отримати централізовану видимість безпеки без складнощів, пов'язаних з використанням декількох розрізнених технологій безпеки.

- Автоматизоване виявлення загроз від AT&T Alien Labs

Завдяки аналітиці загроз, що надається AT&T Alien Labs, AlienVault USM автоматично оновлюється, щоб залишатися в курсі нових загроз, а організація могла зосередитися на реагуванні на сповіщення.

- Координація реагування на інциденти за допомогою AlienApps

AlienVault USM підтримує зростаючу екосистему AlienApps, дозволяючи компаніям організовувати та автоматизувати дії з іншими технологіями безпеки, щоб компанії могли швидко та легко реагувати на інциденти.

AlienVault USM надає підтримку багатьох послуг своїм клієнтам:

- Виявлення мережевих ресурсів
- Виявлення програмного забезпечення та послуг
- Виявлення ресурсів AWS
- Виявлення ресурсів Azure
- Виявлення ресурсів Google Cloud Platform

Також дозволяє аналізувати інформацію та виявляти загрози:

- Кореляція подій SIEM, автопріоритезація тривог
- Моніторинг активності користувачів

- До 90 днів подій в режимі онлайн з можливістю пошуку
- Виявлення вторгнень у хмару (AWS, Azure, GCP)
- Виявлення мережевих вторгнень (NIDS)
- Виявлення вторгнень на хост (HIDS)
- Виявлення та реагування на кінцевих точках (EDR)

Користувачі AlienVault USM мають широкий функціонал:

1. Відповідь на запити

- Формування запитів на експертизу
- Автоматизація та організація реагування
- Сповіщення та тикетування

2. Оцінка

- Сканування вразливостей
- Оцінка хмарної інфраструктури
- Конфігурація користувачів та активів
- Моніторинг темного інтернету

3. Звітність

- Готові шаблони звітів про комплаєнс
- Готові шаблони звітів про події
- Налаштовувані подання та дашборди
- Зберігання логів

USM Anywhere - це високорозширювана платформа, яка використовує AlienApps - модульні програмні компоненти, тісно інтегровані в платформу USM Anywhere, які розширюють, організовують і автоматизують функціональність між вбудованими засобами контролю безпеки в USM Anywhere та іншими інструментами безпеки. З AlienApps організації можуть:

- збирати критичні дані з локальної та хмарної інфраструктури, а також хмарних сервісів

- Збагачувати свої дані та аналізувати їх за допомогою новітньої системи AlienVault Threat Intelligence
- Організовувати та автоматизувати розслідування інцидентів та реагування на них
- Отримуйте нові можливості захисту, оскільки нові AlienApps впроваджуються в USM Anywhere в міру того, як розвивається ландшафт загроз

Тож AlienVault USM – це одне з найбільш конкурентоспроможних SIEM-рішень - є дуже привабливою пропозицією. По суті, це традиційний SIEM-продукт із вбудованими функціями виявлення вторгнень, моніторингу поведінки та оцінки вразливостей. AlienVault має вбудовану аналітику, яку можна очікувати від масштабованої платформи.

Компанія AT&T Cybersecurity також надає рішення AlienVault OSSIM, що часто порівнюють з AlienVault USM за їх функції та можливості (Рис.2.2., Рис.2.3, Рис.2.4)

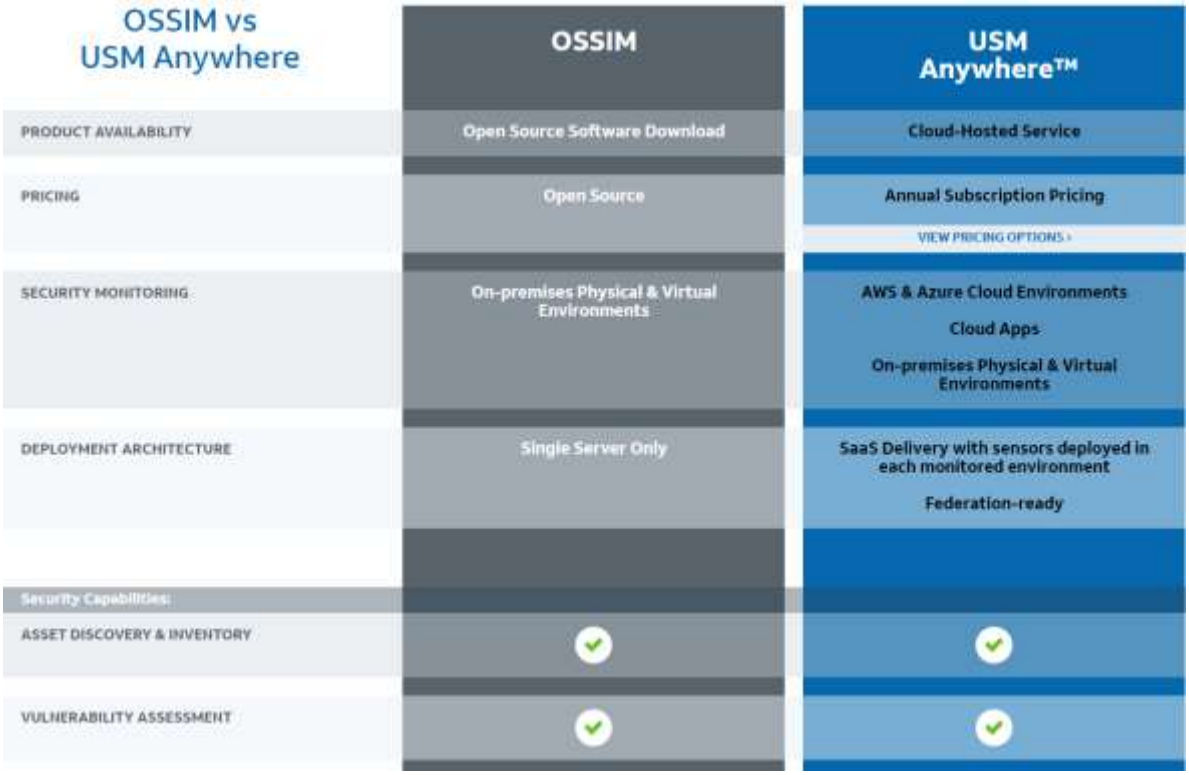

Рис.2.2. Порівняння AlienVault OSSIM з AlienVault USM (Частина 1)

Рис.2.3. Порівняння AlienVault OSSIM з AlienVault USM (частина 2)

Рис.2.4. Порівняння AlienVault OSSIM з AlienVault USM (частина 3)

Також USM Anywhere використовує інтеграцію AlienApps зі сторонніми рішеннями безпеки, моніторингу та спільної роботи, щоб розширити можливості виявлення загроз і реагування на інциденти. Наприклад, рішення інтегрується з MS Azure, Office 365, G Suite, Jira, Cisco Umbrella та іншими.

Нижче наведені деякі аспекти у результаті інтеграції AlienVault USM з Microsoft Azure:

1. Збір журналів подій:

- AlienVault USM може інтегруватися з Azure для збору журналів подій з різних служб, як-от Azure Active Directory, Azure Security Center, Azure Monitor, та інших. Це включає в себе моніторинг активності в хмарі, а також забезпечення видимості в події безпеки.

2. Виявлення загроз:

- Інтеграція дає змогу AlienVault USM аналізувати дані з Azure для виявлення потенційних загроз і аномалій у хмарному середовищі. Це включає в себе використання сигнатур, алгоритмів кореляції подій та інших методів виявлення загроз.

3. Управління вразливостями:

- AlienVault USM може інтегруватися з Azure для моніторингу та управління вразливостями в хмарній інфраструктурі. Це дає змогу організаціям оперативно реагувати на виявлені вразливості та вживати заходів щодо їх усунення.

4. Контекстуальний аналіз:

- Інтеграція з Microsoft Azure дає змогу AlienVault USM аналізувати дані в контексті хмарного середовища. Це важливо для правильного розуміння подій і загроз, враховуючи специфіку роботи в хмарі.

5. Інтеграція з Azure Sentinel:

- AlienVault USM може інтегруватися з Azure Sentinel, платформою для моніторингу безпеки та реагування на інциденти в хмарному середовищі Microsoft Azure. Це дає змогу створювати єдиний центр управління безпекою для аналізу даних із різних джерел.

6. Автоматизована відповідь на інциденти:

- Інтеграція дає змогу налаштовувати автоматизовані дії та відповіді на виявлені загрози в хмарному середовищі Azure.

Інтеграція AlienVault USM із сервісами, Office 365, G Suite, AWS (amazon web services):

1. Office 365:

- AlienVault USM може інтегруватися з Office 365 для збору журналів подій та моніторингу безпеки в хмарному середовищі. Це включає в себе відслідковування активності користувачів, подій у системі та реагування на потенційні загрози безпеки.

2. G Suite:

- Для G Suite (Google Workspace) AlienVault USM може здійснювати збір журналів подій для моніторингу безпеки в Google Cloud. Це дозволяє вам аналізувати активність користувачів, події та зміни в конфігураціях.

3. Amazon Web Services (AWS):

- AlienVault USM інтегрується з AWS для отримання журналів подій та метрик з сервісів AWS. Це включає в себе моніторинг конфігурацій, виявлення аномалій та реагування на події, які можуть вказувати на потенційні проблеми безпеки.

4. Автоматизовані відповіді на загрози:

- Після інтеграції AlienVault USM з цими сервісами, ви можете налаштовувати автоматичні відповіді на виявлені загрози, що дозволяє швидше реагувати та вирішувати потенційні проблеми безпеки.

5. Користувацький інтерфейс:

- Інформація з інтегрованих сервісів доступна у зручному для аналізу інтерфейсі AlienVault USM, де можна відслідковувати та вивчати події безпеки, виявляти аномалії та проводити аналіз загроз.

AlienVault USM (AT&T Cybersecurity) відповідає кільком стандартам безпеки та забезпечення якості інформаційних технологій:

1. Common Criteria (ISO/IEC 15408):

- Common Criteria - міжнародний стандарт, який визначає вимоги до безпеки і захисту інформації в інформаційних технологіях. За певних умов, Common Criteria може бути застосований до безпекових продуктів, таких як AlienVault USM, для підтвердження їх відповідності вимогам безпеки.

2. ISO/IEC 27001:

- ISO/IEC 27001 є міжнародним стандартом для систем управління інформаційною безпекою. Відповідно до цього стандарту, організації встановлюють, впроваджують, підтримують та постійно вдосконалюють систему управління інформаційною безпекою.

3. PCI DSS (Payment Card Industry Data Security Standard):

- PCI DSS є стандартом безпеки, призначеним для захисту платіжних карткових даних. Якщо AlienVault USM використовується в середовищі обробки платіжної інформації, він повинен відповідати вимогам PCI DSS.

4. GDPR (General Data Protection Regulation):

- Якщо AlienVault USM обробляє особисті дані громадян Європейського Союзу, він повинен відповідати стандартам GDPR, що регулює захист особистих даних.

5. FISMA (Federal Information Security Management Act):

- У випадку використання AlienVault USM в агентствах федерального уряду США, він повинен відповідати вимогам FISMA, який визначає стандарти безпеки для інформаційних систем у федеральних установах.

6. NIST (National Institute of Standards and Technology) Standards:

- AlienVault USM може відповідати стандартам NIST, таким як NIST SP 800-53, які надають рекомендації з безпеки інформаційних систем у федеральних установах США.

Також AlienVault USM використовує кілька стратегій для усунення "сліпих зон" та забезпечення повного покриття системи моніторингу безпеки:

- Комбінована архітектура збору даних:
- Система виявлення загроз (IDS/IPS):
- Кореляція подій:
- Машинне навчання:
- Інтеграція з Threat Intelligence:
- Відстеження конфігурацій:

Нижче наведена більш докладна інформація про стратегії відповідно:

- AlienVault USM використовує комбіновану архітектуру для збору даних з різних джерел. Це включає сбір логів, метрик, дані з сенсорів та інші дані про безпеку. Комбінація різних джерел дозволяє отримувати повний обсяг інформації про події в середовищі.
- Вбудована система IDS/IPS AlienVault USM виявляє та аналізує потенційно небезпечні події в мережі. Це дозволяє виявляти вразливості та аномальну активність, яку може пропустити інші методи моніторингу.
- AlienVault USM використовує технологію кореляції подій, що дозволяє пов'язувати різні події та сповіщення для визначення складніших атак або аномалій, які можуть бути пропущені при поверхневому аналізі.
- Система використовує методи машинного навчання для аналізу стандартного поведінки системи та виявлення аномалій. Це дозволяє виявляти нові атаки або непередбачувані зміни в середовищі.
- AlienVault USM використовує інформацію про загрози з різних джерел Threat Intelligence. Це допомагає виявляти та відповідати на відомі методи атак та загрози, що дозволяє більш ефективно визначати аномалії.
- AlienVault USM виявляє зміни в конфігураціях систем та активах, що може вказувати на невизначені загрози або вразливості.

2.2. Компоненти SIEM-систем AlienVault USM для захисту хмарного сховища організації

SIEM (Security Information and Event Management) - це інтегрована система, яка об'єднує в собі інструменти збору, аналізу та реагування на інформацію про безпеку. SIEM включає різні компоненти, які працюють разом для забезпечення безпеки інформаційної системи. Компоненти SIEM-системи працюють разом для забезпечення повного циклу моніторингу та реагування на події в інформаційній системі. Спершу розглянемо основні компоненти SIEM систем загалом:

1. *Збір подій* (Event Collection):

Цей компонент відповідає за збір інформації про події з різних джерел, таких як системні журнали, файли логів, мережеві пристрої та безліч інших джерел. Збір подій забезпечує повний огляд подій в інформаційній системі.

2. *Нормалізація* (Event Normalization):

Цей компонент відповідає за стандартизацію та нормалізацію зібраної інформації, щоб уніфікувати формат подій. Це полегшує подальший аналіз і спрощує порівняння подій з різних джерел.

3. *Кореляція* (Event Correlation):

Компонент кореляції виявляє зв'язки між різними подіями та сповіщеннями. Він дозволяє розпізнавати складні атаки та аномалії, які можуть бути непомітні при окремому аналізі.

4. *Система виявлення вторгнень* (Intrusion Detection System, IDS):

IDS-компонент виявляє потенційно шкідливі дії та атаки, базуючись на аналізі подій та паттернів, які можуть вказувати на загрози безпеці.

5. *Аналіз та візуалізація* (Analysis and Visualization):

Цей компонент відповідає за обробку та аналіз великої кількості інформації, а також відображення цієї інформації в зручному для сприйняття вигляді. Візуалізація допомагає аналітикам та адміністраторам швидше розпізнавати загрози та приймати рішення.

6. *Машинне навчання* (Machine Learning):

Машинне навчання використовується для навчання системи розпізнавати нові, раніше невідомі загрози та аномалії, що дозволяє покращити ефективність виявлення.

7. *Правила та політики безпеки* (Security Rules and Policies):

Цей компонент визначає набір правил та політик безпеки, які використовуються для аналізу подій і генерації сповіщень. Він допомагає визначати нормальну та аномальну активність в системі.

8. *Система реагування* (Incident Response):

Компонент реагування відповідає за автоматизовані або напівавтоматизовані дії у відповідь на виявлені загрози. Це може включати блокування атак, генерацію звітів або автоматичне відновлення систем.

Система AlienVault USM (Unified Security Management) використовує різні методи для збору подій з різних джерел в інформаційній системі. Ось основні аспекти *збору подій* у SIEM-системі AlienVault USM:

- Збір журналів (Log Collection):

AlienVault USM може збирати системні журнали (логи) з різних компонентів і систем, таких як операційні системи (Windows, Linux), бази даних, веб-сервери та інші сервіси. Цей збір дозволяє системі отримати детальну інформацію про активність в різних частинах інфраструктури.

- Збір мережевої активності (Network Activity):

AlienVault USM може аналізувати дані про мережеву активність, зокрема журнали мережевих пристроїв, таких як мережеві маршрутизатори та комутатори. Це допомагає виявляти аномалії та паттерни, пов'язані з мережевою безпекою.

- Дані з сенсорів (Sensor Data):

AlienVault USM використовує сенсори для отримання інформації про безпекові події та загрози в реальному часі. Сенсори можуть бути розгорнуті на різних точках мережі та систем для виявлення атак.

- Логи безпекового обладнання (Security Appliance Logs):

Інформація від різних безпекових пристроїв, таких як фаерволи, системи виявлення вторгнень (IDS/IPS), антивіруси та інші, також включається в збір подій. Це надає додатковий шар безпеки та виявлення загроз.

- Threat Intelligence Feeds:

AlienVault USM інтегрує дані з Threat Intelligence Feeds, що дозволяє системі оновлювати свої бази даних з відомими підозрілими IP-адресами, доменами та іншими параметрами. Це допомагає ідентифікувати та відсіювати потенційно небезпечний трафік.

Нормалізація в SIEM-системі, зокрема в AlienVault USM, є процесом перетворення різноманітної та розподіленої інформації про події в стандартизований формат для однакового оброблення та аналізу. У контексті AlienVault USM, нормалізація має кілька ключових аспектів:

- Стандартизація формату:

AlienVault USM нормалізує дані про події до стандартного формату. Це включає визначення уніфікованих полів та структур для різних типів подій. Наприклад, для подій із файлових логів різних систем.

- Розпізнавання подій:

Нормалізація дозволяє AlienVault USM розпізнавати різні типи подій і відокремлювати їх за їхнім значенням та призначенням. Це важливо для коректного інтерпретування та аналізу даних.

- Об'єднання подій:

Нормалізація також може включати об'єднання пов'язаних подій для визначення комплексних атак або аномалій. Це полегшує кореляцію подій та виявлення складних сценаріїв атак.

- Підтримка різних джерел:

AlienVault USM може нормалізувати дані з різних джерел, таких як файли логів операційних систем, мережеві пристрої, системи виявлення вторгнень тощо. Це дозволяє системі працювати з різноманітною інформацією безпеки.

Кореляція в SIEM-системі AlienVault USM - це процес аналізу та співставлення різних подій для виявлення складніших атак або аномалій, які можуть бути пропущені при окремому аналізі. Основні аспекти кореляції в AlienVault USM включають:

- Кореляція подій:

AlienVault USM взаємодіє з різними джерелами подій, такими як файли логів, системні журнали, мережеві пристрої тощо. Події з цих джерел обробляються та аналізуються для визначення специфічних паттернів, які можуть вказувати на потенційні загрози.

- Кореляція сповіщень:

AlienVault USM також корелює сповіщення, які генеруються внаслідок виявлення певних подій або аномалій. Кореляція сповіщень дозволяє системі розпізнавати взаємодії між різними сповіщеннями, що може вказувати на більш складні загрози.

- Кореляція Threat Intelligence:

Система використовує дані Threat Intelligence для кореляції подій з відомими шаблонами атак та загрозами. Це допомагає визначати, чи виявлені події співпадають з відомими сценаріями атак.

- Кореляція часу та контексту:

AlienVault USM враховує часові параметри та контекст подій для визначення логічних зв'язків між ними. Наприклад, кореляція може виявити несподіваний обсяг активності або послідовність подій, які можуть вказувати на атаку.

- Кореляція мережевих подій:

У випадку мережево-орієнтованих загроз, система корелює події з різних мережевих джерел для виявлення аномалій або незвичайних з'єднань.

- Кореляція конфігурацій та вразливостей:

USM корелює дані про конфігурації та відомості про вразливості для виявлення можливих точок атаки або проблем безпеки.

Система виявлення вторгнень (Intrusion Detection System, IDS) у SIEM-системі AlienVault USM грає ключову роль у виявленні потенційно шкідливих дій та атак в інформаційній системі. Основні риси системи виявлення вторгнень у AlienVault USM включають:

- Сигнатурний аналіз:

AlienVault USM використовує сигнатурний аналіз для виявлення вже відомих загроз. Це включає в себе порівняння активності з великою базою сигнатур, які представляють відомі атаки та вразливості.

- Поведінковий аналіз:

Система виявлення вторгнень AlienVault USM використовує поведінковий аналіз для розпізнавання аномальних паттернів поведінки, які можуть вказувати на

нові атаки або загрози. Вона базується на аналізі стандартного поведінки системи та вчиться визначати невизначені ризики.

- Системи розпізнавання зловживань (Misuse Detection):

IDS AlienVault USM визначає зловживання та атаки на основі відомих атак, що використовується для незаконного використання ресурсів чи отримання несанкціонованого доступу.

- Збагачення Threat Intelligence:

Система виявлення вторгнень у AlienVault USM інтегрується з Threat Intelligence, щоб виявляти відомі методи атак та нові загрози, які можуть виникнути.

- Виявлення аномалій мережі:

IDS в AlienVault USM може виявляти аномалії у мережевому трафіку, такі як надмірні з'єднання, незвичайні порти чи інші аномалії, що можуть свідчити про атаки чи компрометацію.

Аналіз та візуалізація в SIEM-системі AlienVault USM грають важливу роль у розпізнаванні та реагуванні на загрози безпеки. Основні аспекти цих компонентів включають:

- Аналіз Даних:

AlienVault USM використовує аналізатори для обробки та аналізу різноманітної інформації, що включає лог-файли, дані мережі, метрики та інші джерела. Аналізатори автоматично визначають аномалії, небезпечні події та потенційні загрози.

- Візуалізація Даних:

AlienVault USM надає графічні інтерфейси для візуалізації даних. Графіки, діаграми та інші візуальні елементи допомагають аналітикам швидше розпізнавати та аналізувати великий обсяг інформації.

- Дашборди та Звіти:

AlienVault USM має функціональність створення різноманітних дашбордів та звітів. Дашборди надають зведену інформацію про стан безпеки, а звіти дозволяють детальніше дослідження конкретних аспектів.

- Відслідковування Змін:

Система відслідковує зміни в конфігураціях систем та мережевих активах. Це допомагає виявляти потенційні загрози та невизначені зміни, які можуть бути викликані атаками.

- Реагування на Інциденти:

AlienVault USM дозволяє аналітикам та адміністраторам взаємодіяти з інцидентами через інтерфейс, що спрощує прийняття рішень та реалізацію заходів безпеки.

Машинне навчання у SIEM-системі AlienVault USM грає ключову роль у виявленні нових, раніше невідомих загроз та аномалій у безпеці інформаційної системи. Основні аспекти використання машинного навчання в AlienVault USM включають:

- Автоматичне навчання:

AlienVault USM використовує алгоритми машинного навчання для автоматичного навчання моделей на основі накопичених даних безпеки. Це дозволяє системі адаптуватися до змін в середовищі та розпізнавати нові атаки або аномальні зміни.

- Аналіз поведінки:

Машинне навчання використовується для аналізу стандартного поведінки системи та користувачів. Система вивчає типові моделі активності і сприймає аномалії як потенційні загрози.

- Виявлення нульових днів:

Моделі машинного навчання в AlienVault USM можуть виявляти атаки "нульового дня", які раніше не були відомі. Вони аналізують аномальність дій чи паттерни, що можуть свідчити про нові загрози.

- Кластеризація:

Машинне навчання допомагає групувати події в кластери на основі їх схожості. Це дозволяє виявляти зв'язки між різними атаками та інцидентами, а також розпізнавати загрози з подібними характеристиками.

- Оцінка ризику:

Система використовує машинне навчання для оцінки ризику подій та сповіщень, що дозволяє приділяти увагу найбільш критичним або небезпечним інцидентам.

- Автоматизоване вивчення:

Моделі машинного навчання неперервно оновлюються та вдосконалюються, вивчаючи нові тренди та зміни в атаках. Це допомагає забезпечити стабільну ефективність системи в умовах постійно мінливого кіберпростору.

У SIEM-системі AlienVault USM, правила та політики безпеки грають ключову роль у визначенні та аналізі подій, а також в генерації сповіщень та реагуванні на безпекові події. Нижче розглянемо основні аспекти правил та політик безпеки в AlienVault USM:

- Створення Правил:

Користувачі можуть створювати правила для визначення конкретних умов або подій, які є важливими для безпеки системи. Це може бути базове порівняння значень, аналіз текстових логів або виявлення паттернів, характерних для атак.

- Застосування Політик Безпеки:

Політики безпеки дозволяють групувати правила і визначати, як AlienVault USM має реагувати на різні види подій. Наприклад, політика може включати правила для виявлення атак, а також визначати, які заходи повинні бути вжиті у випадку виявлення аномалій.

- Призначення Пріоритетів:

Кожному правилу або політиці може бути призначений пріоритет в залежності від його важливості. Це допомагає фокусуватися на найбільш критичних або термінових аспектах безпеки.

- Автоматизоване Реагування:

Система може мати вбудовані автоматизовані дії, які виконуються при виявленні конкретних подій. Це може включати блокування IP-адрес, відсилання сповіщень адміністраторам або виконання інших заходів для обмеження загроз.

- Адаптація до Змін:

Правила та політики можуть бути легко адаптовані до змін в середовищі або нових загроз. Це дозволяє системі підтримувати високий рівень ефективності в змінних умовах.

Система реагування (Incident Response) в SIEM-системі AlienVault USM відіграє важливу роль у виявленні та обробці загроз безпеки. Основні аспекти системи реагування AlienVault USM включають:

- Автоматизовані відповіді:

AlienVault USM дозволяє налаштовувати автоматичні відповіді на конкретні типи подій чи загроз. Це може включати блокування підозрілого трафіку, відключення акаунтів або автоматичне відновлення конфігурацій.

- Повідомлення та сповіщення:

Система генерує сповіщення та повідомлення для операторів та адміністраторів при виявленні потенційних загроз. Це дозволяє швидко реагувати на події та приймати вчасні заходи безпеки.

- Інтеграція з іншими інструментами:

AlienVault USM інтегрується з іншими інструментами безпеки, щоб забезпечити швидше та ефективне реагування на загрози. Це може включати інтеграцію з фаерволами, системами блокування загроз, антивірусами тощо.

- Підтримка правил та сценаріїв:

Система реагування дозволяє визначати правила та сценарії, за якими вона буде діяти. Це дозволяє персоналу безпеки налаштовувати реакцію на різні загрози відповідно до конкретних вимог організації.

- Ведення журналів та аналіз інцидентів:

AlienVault USM забезпечує можливість ведення детальних журналів та аналізу інцидентів. Це включає в себе запис подій, відповідей та вирішень, що допомагає у вивченні та покращенні стратегій реагування.

- Підтримка командної роботи:

Система реагування AlienVault USM підтримує командну роботу, дозволяючи різним членам безпекової команди взаємодіяти та обговорювати заходи щодо реагування на конкретний інцидент.

- Реалізація планів інцидентів:

Організації можуть створювати та використовувати плани інцидентів, які включають в себе структуровані процедури та заходи для реагування на різні типи загроз.

2.3. Функції панелі керування та звітності у SIEM-системі AlienVault USM

Рішення AlienVault USM має зручний для користувача інтерфейс у якому легко орієнтуватися (Рис.2.5.)

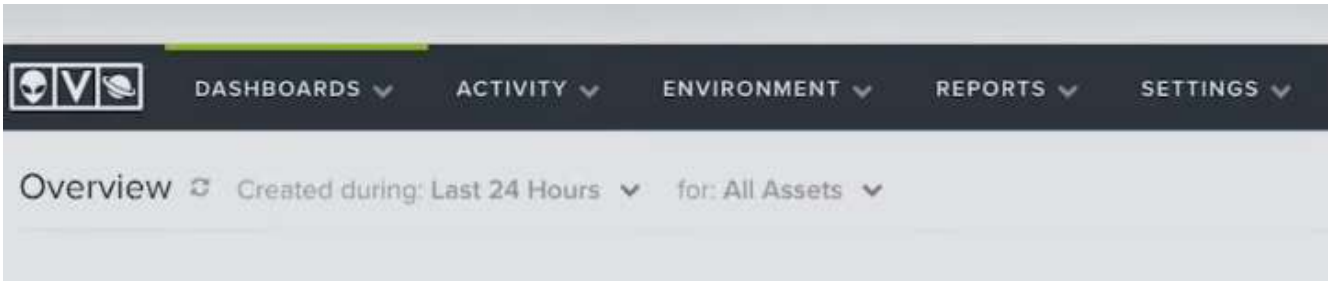

Рис.2.5. Інтерфейс рішення AlienVault USM

AlienVault USM забезпечує необхідний контроль безпеки. Звіти та подання даних, необхідні для забезпечення відповідності, в одному повністю інтегрованому рішенні (Рис.2.6.) з вбудованими функціями виявлення вразливостей активів, оцінки вразливостей, виявлення вторгнень (Рис.2.7) і моніторингу поведінки (Рис.2.8.), а також управління журналами імітаційного моделювання та кореляції подій (Рис.2.9.). AlienVault USM надає вам інструменти, необхідні для досягнення відповідності нормативним вимогам (Рис.2.10.).

Рис.2.6. Одне повністю інтегрованому рішення AlienVault USM

Рис.2.7. Виявлення вторгнень

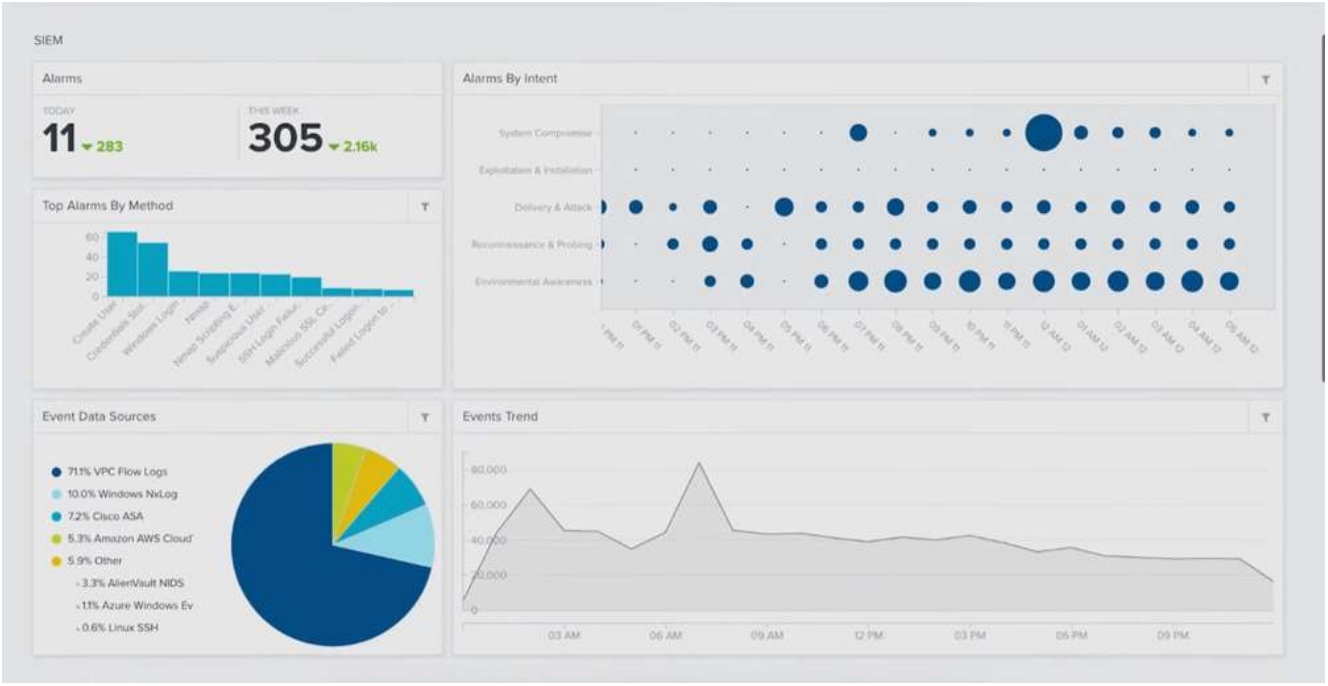

Рис.2.8. Моніторингу поведінки

Рис.2.9. Управління журналами імітаційного моделювання та кореляції подій

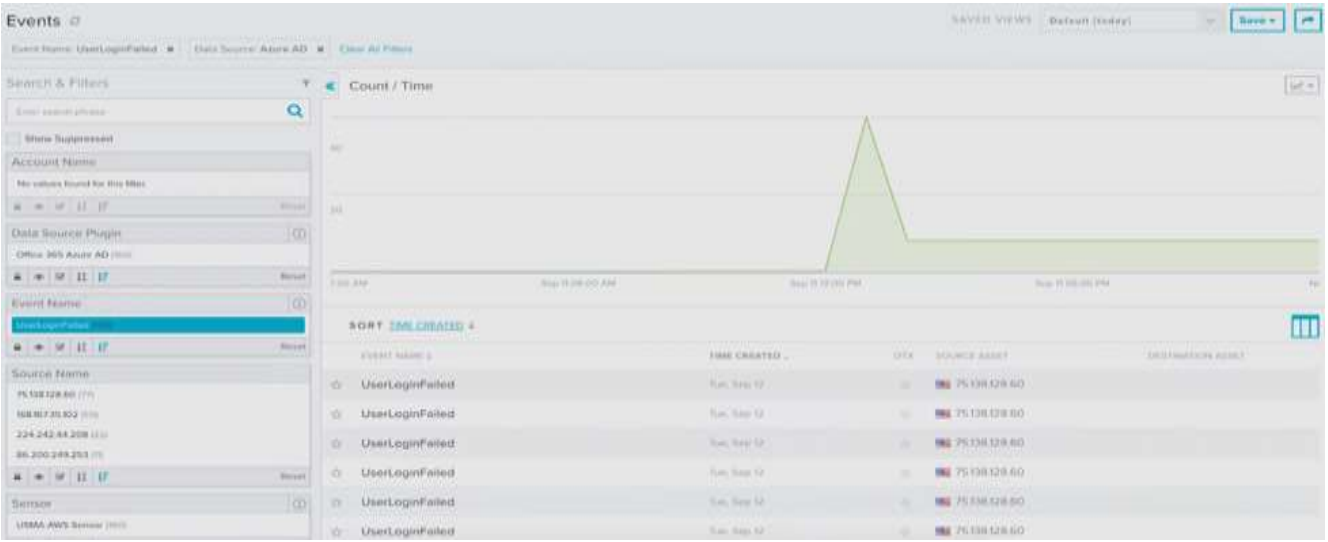

Рис.2.10 інструменти, необхідні для досягнення відповідності нормативним вимогам

Можливості виявлення вторгнень включають в себе виявлення вторгнень на основі хоста, мережі і хмари (Рис.2.11.), а також моніторинг цілісності файлів для відстеження дій користувачів і системи, що допоможе вам відповідати вимогам більшості нормативних стандартів.

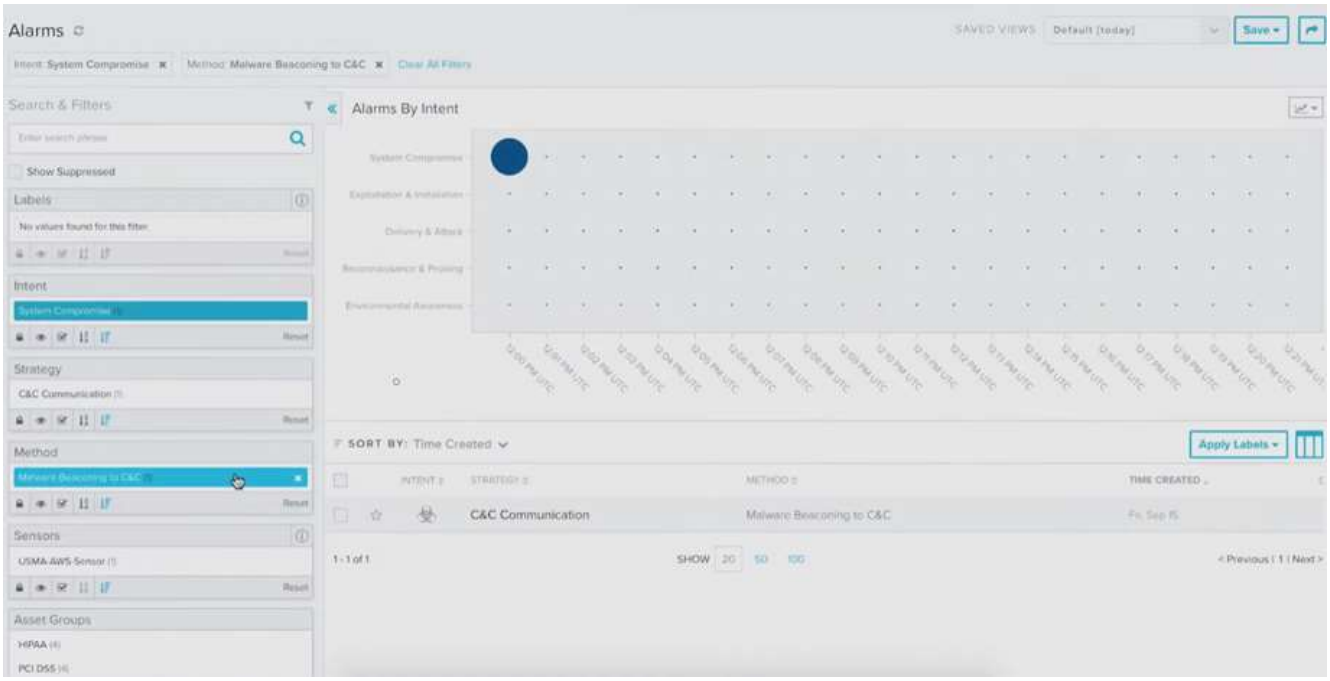

Рис.2.11. Панель виявлення вторгнень

Alienvault USM поєднує і зберігає журнали та події з локальних і хмарних середовищ протягом 12 місяців, спрощуючи управління журналами та їх перегляд, а також допомагаючи організаціям відповідати нормативним вимогам щодо зберігання журналів.

Вбудовані звіти для таких нормативних документів, як PCI DSS і HIPAA, дозволяють швидко і легко проводити щоденні перевірки безпеки, задовольняти запити керівництва і аудиторів і захищати організацію від дорогих штрафів, оскільки Alienvault USM Anywhere сертифікований на відповідність стандартам PCI DSS HIPAA та іншим (Рис.2.12., Рис.2.13., Рис.2.14.)

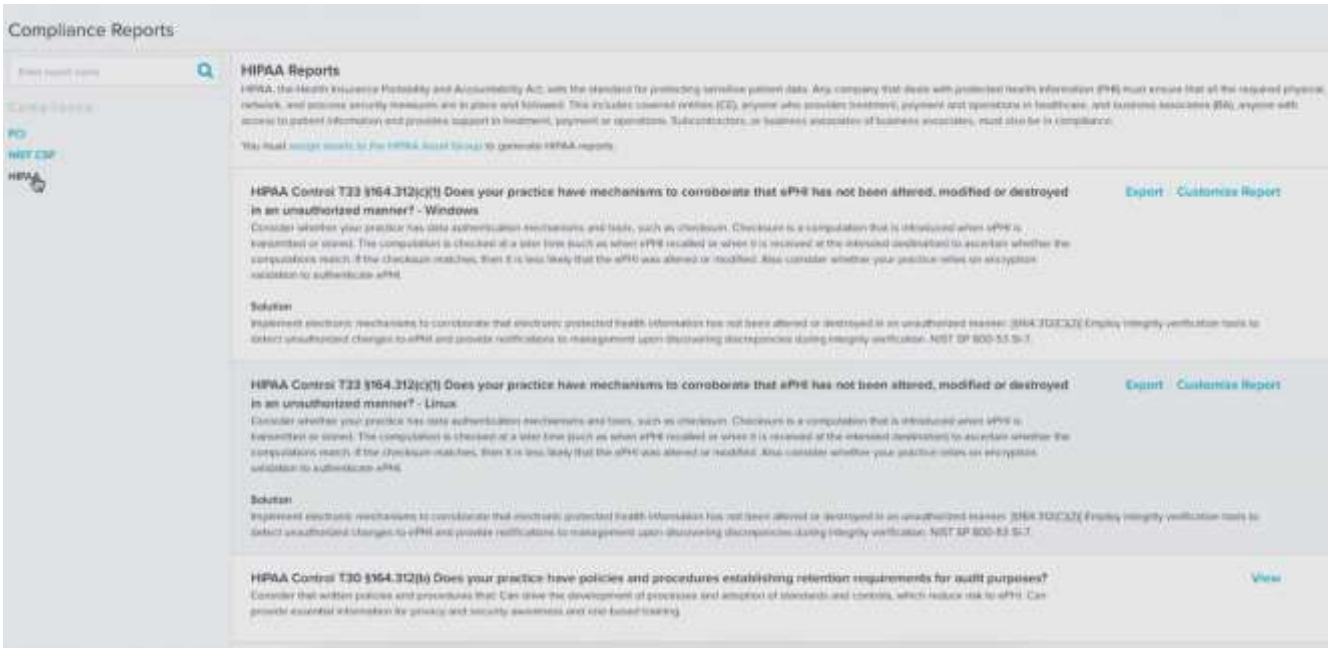

Рис.2.12 Вбудовані звіти що відповідають стандартам HIPPA

Рис.2.13 Вбудовані звіти що відповідають стандартам PCI

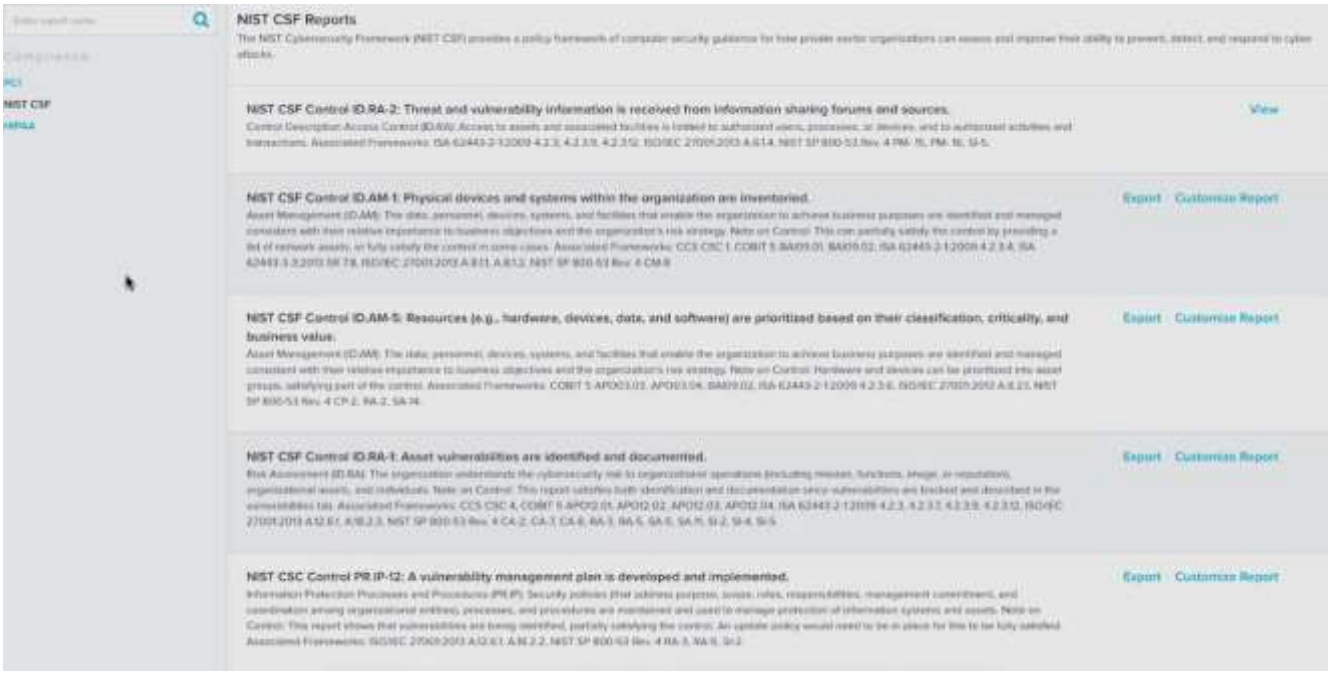

Рис.2.14 Вбудовані звіти що відповідають стандартам NIST CSF

3 ТЕХНОЛОГІЯ ВИКОРИСТАННЯ ПЛАТФОРМИ ALIENVAULT USM ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОГО СХОВИЩА ОРГАНІЗАЦІЇ

3.1. Рекомендації по налаштуванню платформи AlienVault USM у хмарній мережі організації

Першочергово організації необхідно проаналізувати та визначити власні потреби безпеки:

1. Ідентифікація важливих даних:

Розуміння того, які саме типи даних (особисті, фінансові, конфіденційна інформація) обробляються в хмарному середовищі. Визначення, які з цих даних вважаються найбільш критичними та вимагають особливого захисту.

2. Оцінка потенційних загроз:

Аналіз можливих загроз для безпеки даних в хмарному середовищі. Це можуть бути зовнішні атаки, внутрішні загрози, програмні уразливості або неправильна конфігурація систем.

3. Визначення вимог до відповідності:

Якщо організація працює в галузі, що регулюється (наприклад, з вимогами GDPR, HIPAA), необхідно врахувати відповідність цим стандартам при виборі і налаштуванні системи моніторингу безпеки.

4. Оцінка потреб у відслідковуванні подій:

Розглянути, які саме типи подій організація хоче відслідковувати та аналізувати в реальному часі. Це може бути доступ до файлів, зміни конфігурацій, спроби неуспішного входу в систему та інші.

5. Оцінка масштабу системи:

Переконатися, що AlienVault USM може масштабуватися відповідно до потреб організації. Це включає кількість хмарних середовищ, які потрібно моніторити, кількість пристроїв, обсяги даних тощо.

6. Виявлення слабких місць:

Визначити можливі слабкі місця в поточних системах моніторингу безпеки або існуючих пропусках у захисті даних в хмарному середовищі.

7. План дій:

На основі отриманих даних розробити план дій для інтеграції AlienVault USM, відповідно до конкретних потреб організації.

Цей аналіз допоможе організації розуміти власні потреби щодо безпеки даних в хмарному середовищі та створити базу для подальших кроків з налаштування платформи AlienVault USM.

Ідентифікація та інтеграція хмарних ресурсів:

1. Аналіз хмарної інфраструктури:

Ретельно вивчити, які саме хмарні платформи використовуються в організації (наприклад, AWS, Azure, Google Cloud тощо) та які сервіси вони надають.

2. Інвентаризація ресурсів:

Зробити повний перелік хмарних ресурсів, що використовуються організацією: віртуальні машини, контейнери, сховища даних, мережеві компоненти тощо.

3. Оцінка можливостей інтеграції:

Необхідно провести дослідження, як AlienVault USM може інтегруватися з цими хмарними платформами. Перевірити, чи є наявні засоби або агенти для збору даних та моніторингу подій у хмарному середовищі.

4. Створення точок збору даних:

Налаштувати точки збору даних у хмарному середовищі для передачі інформації до системи AlienVault USM. Це може включати налаштування логів, встановлення агентів або інших засобів збору даних.

5. Конфігурація API та підключення:

Якщо доступні API хмарних платформ, треба налаштувати їх для взаємодії з AlienVault USM. Це може допомогти отримувати дані про події та стан системи безпосередньо з хмарної інфраструктури.

6. Тестування інтеграції:

Перед завершенням інтеграції здійснити тестування, щоб переконатися, що AlienVault USM правильно отримує та обробляє дані з хмарних ресурсів.

7. Документація та план моніторингу:

Створити документацію процесу інтеграції, включаючи інструкції щодо моніторингу та підтримки інтегрованих хмарних ресурсів у майбутньому.

Ці пункти дозволять організації ефективно і безпечно інтегрувати хмарні ресурси з платформою AlienVault USM, забезпечуючи моніторинг та захист у хмарному середовищі.

Наступний крок – конфігурація правил моніторингу та ресурсів:

1. Визначення типів правил:

Спочатку необхідно визначити, які саме типи правил необхідно створити для моніторингу хмарної інфраструктури. Це можуть бути правила для виявлення незвичайних подій, доступу до критичних ресурсів, змін конфігурацій тощо.

2. Створення правил моніторингу:

Використовуючи інтерфейс AlienVault USM, створити правила моніторингу, які відповідають виявленим потребам організації. Налаштувати їх для виявлення аномалій або потенційно шкідливих дій.

3. Конфігурація сповіщень:

Налаштувати сповіщення для активації при спрацюванні певних правил. Це може бути електронна пошта, SMS або інші засоби комунікації для оперативного реагування на події.

4. Встановлення порогів і винятків:

Встановити пороги для правил, щоб вони активувалися лише при досягненні певних умов, і виключення, які можуть призвести до спрацьовування правила без реальної загрози.

5. Адаптація правил до конкретних потреб:

Підлаштувати правила до конкретних особливостей хмарної інфраструктури організації, враховуючи типи даних, ресурси та загрози, які є найбільш критичними.

6. Тестування та перевірка працездатності правил:

Перед впровадженням здійснити тестування правил на ізольованих сценаріях для переконливості у їх ефективності та точності виявлення загроз.

7. Документація та моніторинг правил:

Після створення правил, документувати їх, зазначаючи призначення, умови спрацювання та дії для відповіді на події, а також налаштувати моніторинг їх роботи для виявлення можливих проблем або покращень.

Цей процес дозволить оптимізувати моніторинг безпеки в хмарному середовищі за допомогою AlienVault USM шляхом належного налаштування правил та ресурсів для ефективного виявлення та реагування на потенційні загрози.

Далі необхідне навчання персоналу з користування AlienVault USM:

1. Ознайомлення з інтерфейсом:

Почати з ознайомлення співробітників з інтерфейсом AlienVault USM. Пояснити основні розділи, панелі і функції, щоб користувачі могли легко орієнтуватися.

2. Теоретична частина:

Надати персоналу загальне розуміння процесів моніторингу безпеки, виявлення загроз та реагування на них за допомогою AlienVault USM. Це включає концепції аналізу журналів, виявлення аномалій, важливість реагування на попередження та події.

3. Практичні навички:

Надати практичні заняття, де персонал матиме можливість працювати з реальними або симульованими сценаріями. Демонструвати, як виявляти та реагувати на загрози через інтерфейс AlienVault USM.

4. Сценарії та кейси використання:

Провести тренінг, показуючи реальні кейси використання для конкретних ситуацій, що можуть виникнути в хмарній мережі. Це допоможе персоналу розуміти, як застосовувати знання у реальних умовах роботи.

5. Налагодження процедур безпеки:

Навчити персонал не лише використовувати платформу, але й слідкувати за процедурами безпеки. Це включає правильне реагування на попередження, звітність про події та процедури реагування на інциденти.

6. Постійна підтримка та оновлення:

Забезпечити постійну підтримку для персоналу через навчальні матеріали, вебінари, а також оновлення з врахуванням нових функцій чи змін у платформі AlienVault USM.

7. Тестування знань та оцінка:

Завершення навчання включає проведення тестів або оцінювання для перевірки зрозуміння персоналом матеріалу та його готовності до використання AlienVault USM у реальних умовах.

Цей підхід допоможе персоналу організації освоїти і ефективно використовувати AlienVault USM для моніторингу безпеки в хмарному середовищі.

Тестування системи AlienVault USM для хмарної мережі:

1. Створення тестового середовища:

Розгорнути тестове середовище, яке відтворює хмарну інфраструктуру організації. Встановіть AlienVault USM і підключіть його до цього середовища.

2. Симуляція загроз:

Створити сценарії та симулювати можливі загрози в цьому тестовому середовищі. Використовувати інструменти для створення загроз та намагатися виявити їх через систему моніторингу.

3. Відстеження та аналіз реакції системи:

Спостерігати, як AlienVault USM реагує на симульовані загрози. Визначити, як швидко та ефективно система виявляє, реєструє та реагує на ці загрози.

4. Перевірка логів та звітності:

Перевірити, як система реєструє події, логи та створює звіти. Впевнітися, що вся необхідна інформація фіксується і може бути легко доступна для подальшого аналізу.

5. Тестування реагування на попередження:

Симулювати різні рівні попереджень та перевірити, як система опрацьовує ці попередження. Переконайтися, що вони правильно спрямовані та інтерпретовані.

6. Аналіз продуктивності та використання ресурсів:

Перевірити продуктивність системи AlienVault USM під час тестування та переконайтися, що вона відповідає очікуванням та вимогам організації.

7. Документування результатів тестування:

Записати всі виявлені проблеми, успіхи, рекомендації та висновки з тестування. Це допоможе в подальшому виправити проблеми та підготувати звіт для внутрішнього використання.

Цей процес дозволить організації переконатися у працездатності та ефективності системи AlienVault USM в хмарному середовищі перед її остаточним впровадженням.

Оновлення та моніторінг системи AlienVault USM:

1. Система оновлень:

Після впровадження переконайтися, що система AlienVault USM має налаштовану автоматичну систему оновлень. Постійно відслідковувати нові версії програмного забезпечення та вчасно оновлювати систему.

2. Перевірка оновлень:

Ретельно перевіряти оновлення перед їх встановленням, враховуючи можливі впливи на існуючу систему, щоб уникнути можливих помилок або проблем після оновлення.

3. Стабільність та продуктивність:

Слідкувати за стабільністю та продуктивністю системи після кожного оновлення. Якщо виникають проблеми, вирішувати їх швидко та ефективно.

4. Моніторінг захисту:

Після впровадження системи AlienVault USM, постійно моніторити захист хмарної мережі організації. Виявляти, аналізувати та реагувати на будь-які потенційні загрози або події.

5. Оновлення процедур:

Якщо виникають нові загрози або проблеми, оновлювати процедури безпеки, включаючи правила моніторингу та реагування, щоб врахувати нові сценарії загроз.

6. Аудит та аналіз даних:

Проводити регулярний аудит та аналіз даних, збираючи відомості про події та виявлені загрози. Це допоможе вдосконалити систему та покращити реагування на події.

7. Постійне навчання персоналу:

Забезпечте постійне навчання персоналу організації з використання системи AlienVault USM, оновлюючи їх знання з урахуванням нових функцій та можливостей.

Цей процес дозволить забезпечити стабільну та захищену роботу системи AlienVault USM у хмарному середовищі, вдосконалюючи її ефективність та відповідність мінливим умовам та загрозам.

Після розгляду ключових аспектів впровадження та налаштування платформи AlienVault USM у хмарній мережі організації, можна зробити наступний висновок:

Впровадження системи моніторингу безпеки, такої як AlienVault USM, у хмарній мережі є ключовим кроком у забезпеченні захищеності, виявленні та реагуванні на потенційні загрози для організації. Процес налаштування системи AlienVault USM вимагає комплексного підходу та уваги до деталей.

Аналіз потреб безпеки організації перед впровадженням допомагає зрозуміти, які саме аспекти потрібно врахувати, визначаючи критичні дані, потенційні загрози та вимоги до відповідності. Цей аналіз становить основу для подальших кроків у налаштуванні системи.

Ідентифікація та інтеграція хмарних ресурсів в AlienVault USM дозволяє забезпечити повноту моніторингу захищеності у хмарному середовищі, створюючи точки збору даних та налагоджуючи взаємодію системи з цими ресурсами.

Конфігурація правил моніторингу та ресурсів у системі AlienVault USM грає важливу роль у виявленні та реагуванні на загрози. Ретельне налаштування правил та стеження за їх ефективністю дозволяє підвищити рівень безпеки.

Навчання персоналу щодо користування AlienVault USM є важливою складовою успішного впровадження. Це допомагає організації бути впевненою, що персонал володіє необхідними знаннями та навичками для ефективного використання системи.

Тестування системи AlienVault USM у хмарному середовищі перед впровадженням є критичним етапом для впевненості в її працездатності та ефективності. Це дозволяє виявити можливі проблеми та виправити їх до практичного застосування.

Після впровадження системи важливо забезпечити постійне оновлення та моніторинг AlienVault USM. Це дозволить підтримувати систему в актуальному стані, реагувати на нові загрози та постійно підвищувати рівень безпеки організації.

Загальною метою цього процесу є створення динамічної та ефективної системи моніторингу безпеки, яка відповідає конкретним потребам та вимогам організації, забезпечуючи високий рівень захисту в хмарному середовищі.

3.2. Рекомендація щодо застосування технології виявлення та реагування на загрози у хмарному середовищі організації

Використання технологій виявлення та реагування на загрози (Threat Detection and Response, TDR) у хмарних середовищах є критичним для забезпечення безпеки та захисту цифрових активів організації. Обираючи інструменти Threat Detection and Response (TDR) для застосування в хмарному середовищі, важливо врахувати кілька ключових аспектів:

1. Сумісність з хмарним середовищем:

Обирати рішення TDR, які мають інтеграцію та сумісність з провідними хмарними платформами, такими як AWS, Azure, Google Cloud тощо. Це важливо для того, щоб інструмент міг ефективно працювати у хмарному середовищі, збирати дані та аналізувати їх без проблем у великих масштабах.

2. Масштабованість та ефективність:

Обирати TDR-інструменти, які можуть легко масштабуватися відповідно до потреб організації. Здатність обробки великої кількості даних та ефективне виявлення загроз у реальному часі є критичними для успішного застосування в хмарних обчисленнях.

3. Аналіз та візуалізація даних:

Вибрати інструменти, які пропонують продуктивний аналіз та візуалізацію даних. Інтуїтивний та зрозумілий інтерфейс допомагає швидко виявляти аномалії та потенційні загрози.

4. Автоматизація та інтелектуальний аналіз:

Важливо, щоб інструмент TDR мав можливість автоматизації процесів виявлення та реагування на загрози. Це включає в себе застосування штучного інтелекту та машинного навчання для автоматичного виявлення аномалій та аналізу паттернів поведінки.

5. Реакція на загрози та інциденти:

Обирати інструмент, який надає можливість швидкої реакції на виявлені загрози. Це може бути автоматичне блокування певних дій або систем або швидке сповіщення адміністраторів для подальшого аналізу та реагування.

6. Відповідність та стандарти безпеки:

Переконатися, що обраний інструмент відповідає всім необхідним стандартам та вимогам безпеки, які встановлені для організації або відповідає вимогам регуляторних органів, якщо це необхідно.

Обираючи правильний інструмент TDR для хмарного середовища, важливо враховувати конкретні потреби та специфіку організації, а також здатність інструменту адаптуватися до змін у загрозах та технологічних вимогах.

Централізований моніторинг та аналіз даних - це ключовий аспект у виявленні та реагуванні на загрози в хмарному середовищі. Цей підхід передбачає збір, обробку, аналіз та візуалізацію даних з різних джерел для виявлення аномалій, загроз та вразливостей. Ось кілька ключових аспектів централізованого моніторингу та аналізу даних:

1. Збір та агрегація даних:

Централізований моніторинг передбачає збір даних з різних джерел у хмарному середовищі. Це можуть бути дані з журналів подій, інформація про мережевий трафік, дані з безпеки додатків та систем, метрики про продуктивність та багато іншого. Ці дані агрегуються та направляються до централізованого центру обробки для подальшого аналізу.

2. Централізований аналіз та виявлення загроз:

Після збору даних вони проходять через аналізатори та системи виявлення аномалій. Це дозволяє виявляти незвичайні паттерни, непередбачувану активність чи потенційні загрози для безпеки системи. Аналітичні інструменти, операційні центри безпеки та машинне навчання можуть використовуватися для виявлення цих аномалій.

3. Візуалізація та сповіщення:

Централізована платформа надає можливість візуалізації результатів аналізу даних у зручному та зрозумілому форматі. Графіки, діаграми, звіти та панелі керування дозволяють швидко відслідковувати стан безпеки, виявлені загрози та їхній вплив.

4. Реагування та відповідь на інциденти:

Після виявлення загроз чи аномалій, централізована система може автоматично реагувати на інциденти, застосовуючи правила безпеки або інші заходи безпеки для мінімізації шкоди. Крім того, автоматичні сповіщення можуть надсилатися адміністраторам для подальшої ручної реакції та виправлення проблем.

5. Аналіз і вдосконалення:

Централізований моніторинг також дозволяє аналізувати ефективність застосованих заходів безпеки та вдосконалювати їх. Регулярний аналіз результатів аналітики допомагає виявляти слабкі місця, вдосконалювати стратегії та підвищувати рівень захисту.

Використання штучного інтелекту (AI) та машинного навчання (ML) в сфері безпеки хмарних середовищ дозволяє ефективно виявляти, аналізувати та реагувати на загрози у режимі реального часу, а також підвищує рівень захисту організацій. Ось деякі ключові аспекти:

1. Аналіз великих обсягів даних:

AI та ML дозволяють обробляти великі обсяги даних, зокрема дані з різних джерел у хмарному середовищі, такі як журнали подій, дані мережі, системні дані тощо. Алгоритми виявлення паттернів та аномалій виявляють незвичайну або підозрілу активність.

2. Виявлення аномалій та підозрілих паттернів:

AI використовується для аналізу ідентифікованих паттернів поведінки користувачів та систем, визначаючи нормальну поведінку та виявляючи відхилення, які можуть вказувати на потенційні загрози або порушення безпеки.

3. Автоматизація процесів безпеки:

Машинне навчання використовується для розробки моделей, які можуть автоматично виявляти, аналізувати та класифікувати загрози. Це допомагає вирішувати проблеми безпеки в режимі реального часу, зменшуючи необхідність мануального втручання.

4. Покращення систем:

Алгоритми ML постійно вдосконалюються через навчання на нових даних та зміну у шаблонах загроз. Це дозволяє адаптуватися до нових видів загроз та уникати їх.

5. Застосування у прогностичному аналізі:

AI допомагає не лише в реагуванні на загрози, а й у прогнозуванні майбутніх загроз. Він використовує накопичені дані для передбачення можливих атак або проблем з безпекою, що дозволяє приймати проактивні заходи.

6. Оптимізація безпеки:

Використання AI та ML дозволяє автоматизувати процеси виявлення, аналізу та реагування на загрози, що приводить до підвищення ефективності та точності систем безпеки.

Загальною метою використання AI та ML в безпеці хмарних середовищ є створення інтелектуальних систем, які можуть працювати автономно або разом з людськими експертами для забезпечення безпеки систем в реальному часі.

Четвертий пункт, який стосується реактивного та превентивного реагування на загрози в хмарному середовищі, зосереджується на двох ключових аспектах заходів безпеки:

Реактивне реагування:

Реактивне реагування означає вжиття заходів у відповідь на виявлену загрозу або інцидент. Це може бути автоматичне або ручне втручання для припинення загрози та мінімізації її наслідків. Ось кілька підходів:

1. Автоматичні реакції:

Система може мати набір правил або скриптів, які автоматично виконують певні дії при виявленні певних загроз. Наприклад, блокування IP-адреси або програмного забезпечення, що порушує безпеку, змінює права доступу тощо.

2. Сповіщення та реагування операторів:

   Команда безпеки отримує сповіщення про загрози, відкриває інцидент та вживає відповідних заходів для усунення загрози.

Превентивне реагування:

Превентивне реагування полягає у запобіганні або зменшенні впливу можливих загроз шляхом прийняття заходів безпеки заздалегідь. Ось деякі методи:

1. Політики та процедури безпеки:

   Розроблення та виконання політик безпеки, які включають правила доступу, шифрування, процедури аутентифікації, регулярні оновлення тощо.

2. Моніторинг та аналіз:

   Постійний моніторинг систем та мережі для виявлення аномальних дій або незвичайної активності, що може свідчити про потенційні загрози. Забезпечення швидкого реагування до того, як справжня загроза буде реалізована.

3. Навчання та постійне вдосконалення:

   Навчання персоналу, використання найновіших технологій та оновлення систем безпеки для запобігання новим формам загроз.

Реактивне та превентивне реагування об'єднуються для забезпечення повного кругу захисту від загроз у хмарному середовищі: реагування на виявлені загрози негайно та ефективно, а також запобігання можливим загрозам до їх реалізації.

Постійне навчання та адаптація в контексті безпеки хмарних середовищ є важливою складовою для ефективного протистояння постійно мінливим загрозам та технологічним викликам. Ось докладніші вказівки:

1. Оновлення знань про загрози та технології:

Стрімкий розвиток кіберзлочинності вимагає постійного оновлення знань у сфері безпеки. Це означає слідкування за останніми трендами у кібербезпеці, аналіз нових видів атак, вивчення нових методів оборони та оновлення кваліфікації персоналу.

2. Проведення тренувань та симуляцій:

Організація тренувань на випадок кібератак дозволяє персоналу набути практичних навичок у реальному часі, без ризику для реальних даних або систем. Це допомагає перевірити та вдосконалити реакцію на інциденти.

3. Внутрішні та зовнішні навчальні програми:

Залучення до внутрішніх або зовнішніх навчальних програм, семінарів, вебінарів та конференцій є корисним методом постійного підвищення кваліфікації. Вони дозволяють отримувати інсайди від експертів з безпеки, обмінюватися досвідом та найкращими практиками.

4. Адаптація до нових технологій та інструментів:

Сфера кібербезпеки постійно еволюціонує, тому важливо бути готовим до використання новітніх інструментів, технологій та методів аналізу та захисту. Розробка гнучких стратегій для адаптації до нових технологічних відкриттів є ключовою.

5. Оцінка та вдосконалення процесів:

Постійна оцінка ефективності застосованих стратегій та процесів безпеки дозволяє виявляти слабкі місця та вносити відповідні зміни для поліпшення. Регулярні огляди та аналіз інцидентів допомагають у покращенні стратегій захисту.

6. Створення культури кібербезпеки:

Посилення усвідомлення персоналу про важливість кібербезпеки та відповідальності кожного працівника у захисті даних є важливою складовою постійного навчання. Регулярні навчальні програми та інформаційні кампанії сприяють у формуванні цієї культури.

Постійне навчання та адаптація є ключовими для ефективного управління безпекою в хмарних середовищах. Це дозволяє бути готовим до нових викликів,

уникати застарілих підходів та ефективно реагувати на постійно змінюючийся ландшафт кібербезпеки.

Шостий пункт, який стосується політики безпеки та перевірки відповідності, є важливим елементом забезпечення безпеки в хмарних середовищах. Це охоплює розробку та виконання набору правил, процедур та стандартів безпеки, а також перевірку, що ці правила дотримуються. Ось кілька ключових аспектів:

1. Розробка політики безпеки:

Це перший крок у створенні безпечного хмарного середовища. Політика безпеки має визначати правила та стандарти для захисту даних, мережі та інфраструктури. Вона повинна охоплювати аспекти, такі як доступ, шифрування, резервне копіювання, рівень доступу до даних, аутентифікація тощо.

2. Виконання стандартів та регулятивних вимог:

Політика безпеки повинна відповідати стандартам безпеки (наприклад, ISO/IEC 27001) та вимогам регуляторів, які стосуються конкретної галузі вашої організації (наприклад, GDPR, HIPAA тощо). Виконання цих стандартів і вимог дозволяє забезпечити високий рівень захисту даних.

3. Перевірка відповідності:

Це процес періодичної перевірки того, чи відповідають дії та практики організації встановленим політикам безпеки та регулятивним вимогам. Це може включати в себе аудити, сканування, тестування на проникнення та оцінку ризиків для переконання в тому, що системи та процедури відповідають встановленим стандартам.

4. Постійне оновлення та удосконалення:

Політика безпеки має бути живою та постійно оновлюваною, оскільки загрози безпеки постійно еволюціонують. Організація повинна реагувати на нові загрози та вразливості, оновлюючи політику та процедури безпеки для відповідності новим стандартам та технологічним вимогам.

Всі ці кроки сприяють створенню ефективної політики безпеки та перевірки її відповідності, що є ключовими для забезпечення безпеки та відповідності стандартам у хмарних середовищах.

ВИСНОВКИ

Хмарні сховища стають невід'ємною частиною сучасної інфраструктури, надаючи організаціям можливість скорочення витрат, підвищення продуктивності та забезпечення безпеки даних.

Хмарні сховища мають як свої переваги, так і свої недоліки. У той самий час як хмарні сховища дуже гнучкі, легко масштабуються та підлаштовуються під потреби організації, так вони і залежні від Інтернету, що їм потрібне постійне стабільне Інтернет-з'єднання. Так само як хмарні сховища мають зручний доступ та дозволяються працівникам організацій працювати та розвивати організацію з будь-якої точки світу, так і хмарні сховища постійно стають об'єктами кібератак.

Дійсно, ефективність у зберіганні великих обсягів даних, особливо для бізнесів, що розвиваються та великих корпорацій – беззаперечна. Але й не менш важливим стає захист даних хмарних сховищ.

SIEM-система AlienVault USM, котру вважають однією великою інтегрованою системою, прекрасно підходить для захисту хмарних сховищ, так як і доступ до цього рішення – хмарний.

Як і самі хмарні сховища AlienVault USM – це не ідеальне рішення, яке також має свої переваги та недоліки. Поєднання збору подій, детекторів загроз, аналізу та системи реагування робить AlienVault USM комплексним інструментом для моніторингу безпеки. AlienVault USM використовує Threat Intelligence, що дозволяє системі завжди ефективно виявляти відомі методи атак та загрози. Але є і недоліки, наприклад, складність конфігурації. Для повноцінного використання системи може знадобитися час та навички в налаштуванні.

Тож застосування хмарних сховищ та SIEM-системи AlienVault USM в сучасних умовах є важливим етапом для забезпечення безпеки та ефективного управління інформаційними ресурсами. Комбінування гнучкості хмарних технологій з потужністю інтегрованої SIEM-системи дозволяє організаціям досягати високого рівня захисту та оперативності в управлінні безпекою.

ПЕРЕЛІК ПОСИЛАНЬ

1. Capacity : History of Cloud Storage. URL: https://capacity.com/cloud-storage/history-of-cloud-storage/ (дата звернення: 04.12.2023).
2. ЗУ : Про хмарні послуги 2022. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 19.10.2023).
3. Google Cloud : What are the different types of cloud computing? URL: https://cloud.google.com/discover/types-of-cloud-computing (дата звернення: 18.10.2023).
4. GIGACLOUD : ХМАРНА ПІРАМІДА: IAAS, PAAS І SAAS. URL: https://gigacloud.ua/blog/navchannja/hmarna-piramida-iaas-paas-i-saas (дата звернення: 20.11.2023).
5. >the_kernel : ХМАРНА БЕЗПЕКА ДЛЯ УКРАЇНСЬКОГО БІЗНЕСУ — МІФ ЧИ РЕАЛЬНІСТЬ? URL: https://thekernel.ua/khmarna-bezpeka-dlia-ukrainskoho-biznesu-mif-chy-realnist/#:~:text=Але%20загрозу%20для%20хмарних%20сховищ,правильно%20організувати%20розгортання%20хмарної%20структури. (дата звернення: 17.11.2023).
6. ESET : Зберігання даних компаній у хмарному сховищі – наскільки це наразі безпечно. URL: https://www.eset.com/ua/about/newsroom/blog/business-security/khraneniye-dannykh-kompaniy-v-oblachnom-khranilishche-naskolko-eto-seychas-bezopasno/ (дата звернення: 15.10.2023).
7. Intellipaat : Sniffing Attacks. URL: https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/sniffing-attacks/#:~:text=What%20is%20Sniffing%20Attacks%3F,flow%20through%20a%20computer%20network. (дата звернення: 26.09.2023).
8. FORTINET: DoS Attack vs. DDoS Attack. URL: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=A%20denial-of-

service%20(,to%20flood%20a%20targeted%20resource. (дата звернення: 03.11.2023).

9. Owasp: SQL Injection. URL: https://owasp.org/www-community/attacks/SQL_Injection (дата звернення: 10.10.2023).
10. IBM : What is SIEM? URL: https://www.ibm.com/topics/siem (дата звернення: 07.10.2023).
11. CSO: 12 top SIEM tools rated and compared. URL: https://www.csoonline.com/article/566677/12-top-siem-tools-rated-and-compared.html (дата звернення: 02.12.2023).
12. FORTRA: What is SIEM? URL: https://www.coresecurity.com/siem (дата звернення: 04.11.2023).
13. infosec-jobs.com: AlienVault explained. URL: https://infosec-jobs.com/insights/alienvault-explained/#:~:text=and%20industry%20relevance.-,Origins%20and%20History,to%20organizations%20of%20all%20sizes. (дата звернення: 26.11.2023).
14. AT&T Cybersecurity: USM Anywhere. URL: https://cybersecurity.att.com/products/usm-anywhere (дата звернення: 30.09.2023).
15. AT&T: Cybersecurity. AlienApps. URL: https://cybersecurity.att.com/products/alienapps (дата звернення: 02.10.2023).