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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розроблення рекомендацій щодо моніторингу безпеки віртуального середовища на базі VMWare App Defence»

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

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

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

_____ Ярослав ВАСИЛЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ВАСИЛЕНКО Ярослав
(прізвище, ім'я)

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

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

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

HIDS – Host-Based Intrusion Detection System

IDS – Intrusion Detection System

NIDS – Network Based Intrusion Detection System

SIEM – Security Information and Event Monitoring

TVD – Trusted Virtual Domains

VIB – vSphere Installable Bundle

ВСТУП

Актуальність дослідження. У сучасному цифровому світі віртуалізація та хмарні обчислення є основними компонентами інформаційної інфраструктури багатьох організацій. Використання віртуальних середовищ дозволяє ефективніше використовувати ресурси та знижувати витрати, але одночасно підвищує ризик кіберзагроз. Забезпечення безпеки віртуальних машин є критично важливим для запобігання несанкціонованому доступу, витоку даних та інших кібератак, що можуть призвести до значних фінансових та репутаційних втрат.

Моніторинг безпеки віртуальних середовищ є ключовим аспектом захисту інформаційних систем організації. Кібератаки на віртуальні машини можуть порушити роботу всієї корпоративної мережі, спричинити простої та негативно вплинути на продуктивність і безперервність бізнесу. В умовах зростання обсягу віддаленої роботи, коли співробітники використовують віртуальні машини для доступу до корпоративних ресурсів, питання безпеки стають ще більш актуальними.

VMWare App Defence є рішенням для моніторингу безпеки віртуальних середовищ. Цей інструмент автоматично виявляє та реагує на підозрілі дії у віртуальних середовищах, що дозволяє забезпечити високий рівень захисту. Проте для ефективного використання VMWare App Defence необхідно глибше дослідити методи його інтеграції та застосування в реальних умовах.

Актуальність дослідження зумовлена потребою організацій у надійних засобах моніторингу та захисту віртуальних середовищ від постійно еволюціонуючих загроз. Впровадження VMWare App Defence може значно підвищити рівень безпеки, забезпечуючи видимість у реальному часі та можливість швидкого реагування на інциденти.

Об’єкт дослідження – моніторинг безпеки віртуального середовища організації.

Предмет дослідження – методи та засоби моніторингу безпеки віртуальних

середовищ на базі VMWare App Defence.

Мета роботи розробити рекомендації щодо застосування методів та засобів моніторингу безпеки віртуальних середовищ за допомогою VMWare App Defence.

Наукові завдання:

дослідити сутність проблеми моніторингу безпеки віртуальних середовищ;

проаналізувати основні підходи до моніторингу безпеки віртуальних середовищ;

вивчити існуючі рішення для моніторингу безпеки віртуальних середовищ;

проаналізувати методи та засоби моніторингу безпеки на базі VMware App Defence;

запропонувати варіант системи моніторингу безпеки віртуальних середовищ на базі VMware App Defence;

розробити рекомендації щодо застосування методів та засобів моніторингу безпеки віртуальних середовищ.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів моніторингу безпеки віртуальних середовищ, а також рекомендації фахівцям з кібербезпеки щодо їх реалізації. Це дозволить організаціям забезпечити надійний захист від широкого спектру кіберзагроз та підвищити загальну безпеку своїх інформаційних систем.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ МОНІТОРИНГУ БЕЗПЕКИ ВІРТУАЛЬНОГО СЕРЕДОВИЩА

1.1. Аналіз проблеми моніторингу безпеки віртуального середовища

У сучасному світі віртуалізація стала невід'ємною частиною IT-інфраструктури багатьох організацій. За даними дослідження Spiceworks, серверна віртуалізація використовується у 92% бізнесів, що свідчить про її надзвичайну поширеність. Вона дозволяє підвищити ефективність використання ресурсів, гнучкість і швидкість розгортання нових сервісів. Проте, разом із зростанням популярності віртуалізації, зростає і кількість загроз, пов'язаних з безпекою віртуальних середовищ [1].

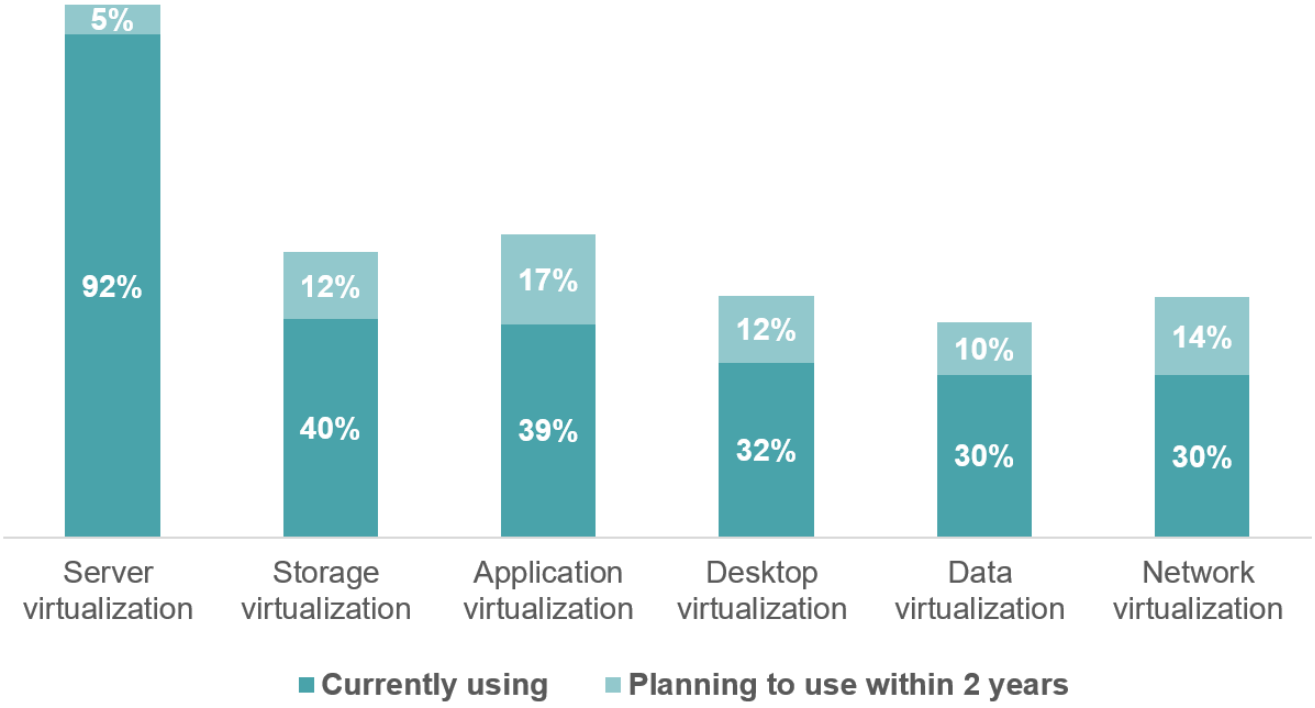

Рис. 1.1. Впровадження технологій віртуалізації в бізнесі [1]

Основними загрозами для віртуальних середовищ є шкідливе програмне забезпечення, атаки на гіпервізор та уразливості в конфігураціях віртуальних

машин. Це підтверджують і дані досліджень, згідно з якими значна частина інцидентів безпеки у віртуальних середовищах пов'язана з людськими помилками та неправильними налаштуваннями. Крім серверної віртуалізації, значного поширення набувають і інші технології віртуалізації. Згідно з дослідженням Spiceworks, віртуалізація сховищ (40%), додатків (39%) та інфраструктури віртуальних робочих столів (32%) також активно впроваджуються у багатьох організаціях [1].

За даними різних досліджень, організації відзначають значне зростання ризиків у віртуальних середовищах, відчуваючи недостатню готовність до протидії новим загрозам. Безпека віртуального середовища ускладнюється через відсутність єдиного підходу до моніторингу та захисту всіх компонентів інфраструктури, включаючи фізичні сервери, гіпервізори та віртуальні машини. За прогнозами, більше половини бізнесів планують впровадити віртуалізацію сховищ та додатків до 2021 року. Очікується, що віртуалізація додатків зросте з 39% до 56%, що вказує на необхідність підвищеної уваги до безпеки цих нових технологій [1].

Віртуалізація стала невід'ємною частиною сучасної IT-інфраструктури, забезпечуючи гнучкість та ефективність управління ресурсами. Проте, разом із перевагами віртуалізації виникають і значні проблеми та ризики безпеки, які потребують особливої уваги. Для забезпечення всебічного захисту віртуальних середовищ необхідно не лише проводити загальний моніторинг, але й розуміти конкретні типи загроз, з якими можуть зіткнутися організації. Кожен з цих типів загроз потребує окремого підходу та детального аналізу, щоб мінімізувати ризики та підвищити рівень безпеки.

Розглянемо ключові загрози, що можуть впливати на безпеку віртуальних середовищ.

Розростання віртуальних машин. Однією з основних проблем є неконтрольоване розростання віртуальних машин. Це трапляється, коли віртуальні машини створюються для конкретних завдань і після виконання своїх функцій залишаються без нагляду. Такий стан речей може призвести до серйозних проблем, зокрема до компрометації віртуальних машин з чутливою інформацією. Коли

віртуальні машини не отримують активного управління та оновлень, вони стають вразливими до різноманітних загроз. Наприклад, без належного моніторингу, старі віртуальні машини можуть залишатися без оновлень безпеки, що робить їх легкою мішенню для зловмисників. Крім того, надмірна кількість віртуальних машин створює додаткове навантаження на адміністраторів, ускладнюючи процес управління і підвищуючи ризики недогляду за важливими аспектами безпеки [2, 3].

Атаки шкідливих програм та програм-вимагачів. Віртуальні машини також вразливі до атак шкідливих програм та програм-вимагачів. Шкідливі програми можуть потрапити у віртуальну інфраструктуру через різні канали, зокрема через заражені образи віртуальних машин або недостатньо підготовлених користувачів. Інфікована віртуальна машина здатна поширювати шкідливе програмне забезпечення по всій віртуальній інфраструктурі, особливо якщо не забезпечено належну ізоляцію та контроль безпеки. Віруси, трояни та програми-вимагачі можуть завдати серйозної шкоди, шифруючи дані або викрадаючи конфіденційну інформацію. Відсутність регулярних оновлень та патчів для віртуальних машин збільшує ризик успішних атак, адже відомі вразливості залишаються незахищеними [2, 3].

Контроль доступу. Крім основних загроз, існує ще низка проблем, пов'язаних із забезпеченням безпеки у віртуальних середовищах. Наприклад, складнощі з управлінням правами доступу. У великих віртуальних інфраструктурах часто важко відстежувати та контролювати, хто має доступ до певних ресурсів. Невірні налаштування прав доступу можуть призвести до несанкціонованого доступу до критично важливих систем і даних. Крім того, конфігураційні помилки в налаштуваннях віртуальних машин і гіпервізорів можуть створювати додаткові вразливості, які зловмисники можуть використовувати для своїх цілей. Сюди також можна віднести проблеми з централізованим управлінням обліковими записами та відсутність належної сегментації мережі, що може полегшити зловмисникам доступ до важливих компонентів інфраструктури. Відсутність регулярного аудиту та моніторингу також сприяє виникненню і накопиченню вразливостей, які можуть бути використані для компрометації

системи. [2, 3].

Конфігурація мережі. Наступним критерієм є управління конфігурацією мережі в контексті віртуалізації це являється собою складним завданням, що вимагає значних зусиль навіть при використанні передових рішень типу VMware vSphere. Основна проблема полягає в тому, що неправильні конфігурації можуть створити серйозні вразливості, якими можуть скористатися зловмисники. Наприклад, дозвіл на спільне використання файлів між віртуальними машинами або відкриття незахищених портів брандмауера може дати змогу зловмисникам отримати несанкціонований доступ до вашої віртуальної інфраструктури. Такі конфігураційні помилки можуть дозволити шкідливому програмному забезпеченню або хакерам проникнути в систему, що може призвести до серйозних наслідків. Питання конфігурації мережі стосується не лише віртуальних машин, але й фізичних серверів. Якщо фізичні сервери не оновлюються регулярно і не отримують останніх патчів безпеки, вони можуть стати серйозним ризиком для всієї інфраструктури. Застаріле програмне забезпечення та прошивки можуть містити відомі вразливості, які зловмисники можуть легко експлуатувати. Таким чином, для забезпечення безпеки необхідно постійно відстежувати та оновлювати всі компоненти мережі, включаючи як віртуальні, так і фізичні елементи [2, 3].

Безпека офлайн-віртуальних машин. Наступним критерієм загрози являється безпека офлайн-віртуальних машин. Цей критерій є важливим аспектом, що потребує особливої уваги при плануванні та управлінні віртуальною інфраструктурою. Офлайн або віддалені резервні копії відіграють критичну роль у плані відновлення після аварій. Вони забезпечують можливість відновлення роботи систем після непередбачених подій, таких як збої обладнання, програмні помилки або кібератаки. Проте, важливо розуміти, що будь-які віртуальні машини, які зберігаються офлайн, залишаються з тими ж оновленнями безпеки та конфігураціями, які були на момент їх резервування. Це означає, що віртуальні машини, які довгий час перебували в офлайн-режимі, можуть містити застарілі конфігурації та відсутні критичні оновлення безпеки. Коли такі машини повертаються в онлайн-режим, вони стають потенційним ризиком для безпеки

всього віртуального середовища. Застарілі офлайн-віртуальні машини можуть бути вразливими до вже відомих експлойтів та атак, які були усунуті в останніх оновленнях. Таким чином, перш ніж повернути такі машини в онлайн, необхідно провести ретельний аналіз їх конфігурацій та застосувати всі необхідні оновлення безпеки. Це допоможе уникнути можливих вразливостей, які можуть бути використані зловмисниками для проникнення у віртуальну інфраструктуру. Крім того, важливо регулярно перевіряти та оновлювати резервні копії, щоб вони залишалися актуальними та відповідали сучасним вимогам безпеки [2, 3].

Контроль безпеки гіпервізора. Гіпервізор є платформою, яка до зволяє запускати віртуальні машини, і його безпека має вирішальне значення для захисту всієї віртуальної інфраструктури. Гіпервізор виступає як посередник між апаратним забезпеченням та віртуальними машинами, і тому він може стати єдиною точкою відмови для всієї віртуальної інфраструктури. Якщо зловмисник отримає доступ до гіпервізора або зможе його скомпрометувати, це може призвести до серйозних наслідків, включаючи повний контроль над усіма віртуальними машинами, що працюють на цій платформі

Однією з найбільших загроз для гіпервізора є атаки типу "розрив гіпервізора" (hypervisor breakout). У випадку такої атаки зловмисник може отримати доступ до гіпервізора з однієї з віртуальних машин, що дозволяє йому контролювати інші віртуальні машини на тому ж хості. Ще однією значною загрозою є атаки типу "відмова в обслуговуванні" (Denial of Service, DoS), які можуть привести до зупинки роботи гіпервізора, а отже, й усіх залежних від нього віртуальних машин. Для захисту від таких атак необхідно впроваджувати багаторівневі заходи безпеки, які включають як технічні, так і організаційні аспекти [2, 3].

Технічні заходи безпеки включають регулярне оновлення гіпервізора та всіх компонентів віртуальної інфраструктури для виправлення вразливостей, застосування сучасних методів аутентифікації та шифрування для захисту від несанкціонованого доступу, а також налаштування мережевих фільтрів і брандмауерів для обмеження доступу до гіпервізора лише з довірених джерел. Важливим елементом є також моніторинг та аналіз активності на гіпервізорі з

метою виявлення підозрілих дій та швидкого реагування на інциденти безпеки[2, 3].

API провайдерів хмарних сервісів. API провайдерів хмарних сервісів відіграють важливу роль у сучасних IT-інфраструктурах, особливо для організацій, що використовують гібридні рішення з публічною та приватною хмарною інфраструктурою. Ці API (інтерфейси прикладного програмування) призначені для забезпечення ефективної комунікації між віртуальними та хмарними середовищами, дозволяючи інтегрувати різні сервіси та додатки. Однак разом із зручністю та гнучкістю, які надають API, виникають і значні ризики безпеки, що потребують особливої уваги та ретельного управління. Одним із основних ризиків, пов’язаних із використанням API провайдерів хмарних сервісів, є потенційні спроби вторгнення. Зловмисники можуть спробувати використовувати вразливості в API для отримання несанкціонованого доступу до системи. Якщо API недостатньо захищені, це може призвести до серйозних наслідків, таких як витік конфіденційної інформації, компрометація даних або навіть повний контроль над віртуальною інфраструктурою. Наприклад, за допомогою атак типу "людина посередині" (MITM), зловмисники можуть перехоплювати дані, що передаються через API, змінювати їх або використовувати для подальших атак [2, 3].

У цьому підрозділі було проаналізовано проблеми моніторингу безпеки віртуального середовища, що є критичним аспектом сучасної IT-інфраструктури. На основі наданої інформації можна зробити кілька важливих висновків.

Серверна віртуалізація є широко використовуваною технологією, яка присутня у 92% бізнесів, що підкреслює її важливість для сучасних організацій. Вона забезпечує підвищення ефективності використання ресурсів, гнучкість і швидкість розгортання нових сервісів. Однак разом із перевагами віртуалізації виникають численні загрози, такі як шкідливе програмне забезпечення, атаки на гіпервізор, уразливості в конфігураціях віртуальних машин, людські помилки та неправильні налаштування.

Однією з основних проблем є неконтрольоване розростання віртуальних машин, що створює додаткове навантаження на адміністраторів і підвищує ризики

безпеки. Без належного моніторингу старі віртуальні машини можуть залишатися без оновлень безпеки, що робить їх вразливими до атак. Віртуальні машини також можуть бути інфіковані шкідливими програмами, які здатні поширюватися по всій віртуальній інфраструктурі. Відсутність регулярних оновлень та патчів збільшує ризик успішних атак.

Управління правами доступу у великих віртуальних інфраструктурах є складним завданням. Невірні налаштування можуть призвести до несанкціонованого доступу до критично важливих систем і даних. Крім того, неправильні конфігурації мережі можуть створити серйозні вразливості, які можуть бути використані зловмисниками для проникнення у систему. Регулярне оновлення програмного забезпечення та прошивок фізичних серверів є необхідним для забезпечення безпеки всієї інфраструктури.

Офлайн або резервні копії віртуальних машин можуть містити застарілі конфігурації та відсутні оновлення безпеки. Перед поверненням таких машин в онлайн-режим необхідно провести ретельний аналіз і оновлення. Гіпервізор є ключовим елементом віртуальної інфраструктури, і його компрометація може призвести до серйозних наслідків, включаючи повний контроль над усіма віртуальними машинами.

Використання API провайдерів хмарних сервісів створює додаткові ризики безпеки. Недостатньо захищені API можуть стати об'єктом атак, таких як атаки типу "людина посередині" (MITM), що призводить до витоку конфіденційної інформації та інших серйозних наслідків.

Таким чином, для забезпечення безпеки віртуального середовища необхідний комплексний підхід, що включає регулярний моніторинг, своєчасне оновлення всіх компонентів інфраструктури, правильне налаштування прав доступу, безпеку гіпервізора та належне управління офлайн-віртуальними машинами. Всі ці заходи спрямовані на мінімізацію ризиків та підвищення рівня захисту віртуальних середовищ від сучасних загроз.

1.2. Аналіз підходів до моніторингу безпеки віртуального середовища

Віртуалізація стала невід'ємною частиною IT-інфраструктури, що дозволяє підвищити ефективність використання ресурсів, гнучкість та швидкість розгортання нових сервісів. Проте, разом із зростанням популярності віртуалізації, збільшується кількість загроз, пов'язаних з безпекою віртуальних середовищ. Основними загрозами для них є шкідливе програмне забезпечення, атаки на гіпервізор та уразливості в конфігураціях віртуальних машин.

Цей аналіз підходів до моніторингу безпеки віртуального середовища включає в себе низку інструментів та технік, які допомагають виявляти та запобігати можливим загрозам, а саме:

Інструменти та техніки моніторингу безпеки віртуального середовища являють собою важливий інструмент для забезпечення безперервної роботи IT-інфраструктури. У сучасних умовах, коли кількість та складність кіберзагроз постійно зростає, застосування ефективних методів моніторингу стає критично важливим. Ці інструменти та техніки дозволяють не лише виявляти потенційні загрози, але й своєчасно реагувати на них, мінімізуючи можливі збитки та порушення в роботі системи.

Одним із основних інструментів моніторингу безпеки є збір та аналіз логів. Логи є важливим джерелом інформації про всі дії та події, що відбуваються у віртуальному середовищі. Інструменти для збору та аналізу логів дозволяють автоматизувати процес збирання даних з різних джерел, включаючи сервери, мережеві пристрої, додатки та бази даних. Аналіз цих логів допомагає виявляти аномалії та потенційні загрози. Наприклад, якщо в логах спостерігається значна кількість спроб входу з неправильними паролями, це може свідчити про можливу атаку методом перебору паролів. Вчасно виявивши таку активність, адміністратори можуть вжити необхідних заходів для захисту системи[4].

Інший важливий аспект моніторингу безпеки – це техніки виявлення аномалій. Аномалії у віртуальному середовищі можуть бути ознакою підозрілої або шкідливої активності. Техніки виявлення аномалій базуються на аналізі звичайної

поведінки системи та виявленні відхилень від цієї поведінки. Наприклад, якщо певний сервер зазвичай не генерує багато мережевого трафіку, а раптом починає активно обмінюватися даними, це може бути ознакою компрометації або витоку даних. Виявлення таких аномалій дозволяє швидко реагувати на потенційні загрози, знижуючи ризики для безпеки[5].

Крім збору та аналізу логів, важливо впроваджувати системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). IDS працюють шляхом моніторингу трафіку та системних подій для виявлення підозрілої активності, яка може свідчити про спроби вторгнення. Якщо така активність виявлена, система IDS може сповістити адміністраторів, щоб вони могли вжити відповідних заходів. IPS, у свою чергу, не тільки виявляють, але й автоматично блокують підозрілу активність, запобігаючи можливим атакам[5].

Ще одним корисним інструментом є системи управління подіями та інформацією безпеки. SIEM об'єднують функції збору логів, виявлення аномалій, моніторингу та аналізу, надаючи єдину платформу для управління безпекою. Вони дозволяють автоматизувати процеси, зменшуючи навантаження на IT-персонал і підвищуючи ефективність реагування на інциденти. SIEM також можуть інтегруватися з іншими системами безпеки, забезпечуючи комплексний підхід до захисту віртуального середовища.

Не менш важливим є регулярне проведення тестування та аудитів безпеки. Тестування, такі як пентести, допомагають виявити вразливості, що можуть бути використані зловмисниками. Аудити безпеки дозволяють оцінити стан захисту системи, виявити слабкі місця та розробити рекомендації для їх усунення. Регулярне проведення таких заходів допомагає підтримувати високий рівень безпеки та своєчасно реагувати на нові загрози.

Навчання персоналу також є ключовим елементом забезпечення безпеки віртуального середовища. Користувачі повинні бути обізнані про основні принципи інформаційної безпеки, сучасні загрози та методи їх запобігання. Регулярне проведення тренінгів та підвищення обізнаності сприяє зменшенню ризиків, пов'язаних з людським фактором.

Автоматичне реагування є важливою складовою сучасних систем забезпечення інформаційної безпеки, оскільки надає можливість автоматизувати процес виявлення та реагування на інциденти безпеки. Ці механізми дозволяють значно скоротити час реагування на загрози, забезпечуючи швидке та ефективне вирішення проблем. У світі, де кіберзагрози стають дедалі складнішими та численнішими, автоматичне реагування стає ключовим фактором успішного управління безпекою інформаційних систем.

Система автоматичного реагування працює за принципом виявлення аномальної або підозрілої активності у віртуальному середовищі та автоматичного виконання дій для її нейтралізації. Наприклад, якщо система виявляє підозрілий вхід до мережі з невідомої IP-адреси або аномальну активність користувача, вона може автоматично заблокувати доступ, сповістити адміністратора та розпочати розслідування. Це дозволяє мінімізувати шкоду від потенційних атак і швидко реагувати на інциденти, не чекаючи на втручання людини.

Крім того, автоматичне реагування допомагає знизити навантаження на IT-персонал, що особливо важливо у великих організаціях з розгалуженою інфраструктурою. Використання автоматичних систем дозволяє персоналу зосередитися на більш стратегічних завданнях, залишаючи рутинні операції та первинну обробку інцидентів автоматизованим системам. Це підвищує загальну ефективність управління безпекою та сприяє більш раціональному використанню ресурсів організації.

Шифрування та управління ключами є ще одним важливим елементом забезпечення безпеки у віртуальних середовищах. Шифрування використовується для забезпечення конфіденційності та цілісності даних, зменшуючи ризик несанкціонованого доступу та розголошення інформації. У віртуальних середовищах дані можуть передаватися між різними віртуальними машинами, серверами та сховищами, і без належного шифрування вони можуть стати легкою здобиччю для зловмисників.

Процес шифрування передбачає перетворення даних у формат, що не може бути прочитаним без спеціального ключа розшифрування. Це означає, що навіть

якщо зловмисники отримають доступ до зашифрованих даних, вони не зможуть їх прочитати без відповідного ключа. Шифрування забезпечує захист як даних у стані спокою, так і даних під час передачі. Це особливо важливо у віртуальних середовищах, де дані можуть переміщуватися між різними фізичними та віртуальними пристроями.

Управління ключами є невід'ємною частиною процесу шифрування. Це включає створення, зберігання, розповсюдження та оновлення ключів шифрування. Ефективне управління ключами є критично важливим для забезпечення надійності шифрування. Ключі повинні бути надійно захищені від несанкціонованого доступу, а їх використання та зберігання повинні відповідати встановленим політикам безпеки.

Сучасні системи управління ключами можуть автоматизувати багато процесів, пов'язаних з обробкою ключів, що підвищує їх безпеку та зручність використання. Наприклад, ключі можуть автоматично оновлюватися через певні проміжки часу або за певними подіями, що знижує ризик їх компрометації. Крім того, такі системи можуть надавати можливості для централізованого управління ключами, дозволяючи адміністраторам легко контролювати доступ до них та забезпечувати їхню безпеку.

Застосування шифрування та управління ключами у віртуальних середовищах має також відповідати певним стандартам та нормативним вимогам. Багато галузей, таких як фінанси, охорона здоров'я та державний сектор, мають суворі вимоги до безпеки даних, і шифрування є одним з основних методів їх дотримання. Використання сучасних алгоритмів шифрування та надійних методів управління ключами допомагає забезпечити відповідність цим вимогам та захистити конфіденційну інформацію від несанкціонованого доступу.

Механізми контролю доступу є ключовими елементами захисту віртуальних середовищ, які дозволяють обмежити доступ до різних компонентів цих середовищ. Основна мета цих механізмів полягає в запобіганні несанкціонованій активності та забезпеченні безпеки системи. Контроль доступу забезпечує, що тільки авторизовані користувачі можуть отримати доступ до певних ресурсів або

виконувати визначені дії. Це досягається за допомогою різних методів і технологій, таких як аутентифікація, авторизація та аудит.

Аутентифікація полягає в перевірці особи користувача перед наданням доступу. Це може включати використання паролів, біометричних даних або токенів. Авторизація, у свою чергу, визначає права доступу користувача до ресурсів після успішної аутентифікації. Наприклад, користувач може мати права лише на читання файлу, але не на його зміну або видалення. Аудит же передбачає моніторинг і запис дій користувачів для виявлення можливих порушень безпеки та проведення розслідувань у разі необхідності.

Віртуальні довірчі платформи є ще одним важливим аспектом забезпечення безпеки у віртуальних середовищах. Вони забезпечують перевірку та підтвердження безпеки та достовірності віртуальних об'єктів. Це допомагає уникнути атак і забезпечити надійність ідентифікації. Віртуальні довірчі платформи використовують різні методи для перевірки цілісності та автентичності даних, такі як цифрові підписи та сертифікати безпеки.

Ці платформи грають важливу роль у захисті від атак, що спрямовані на віртуальні об'єкти. Наприклад, вони можуть запобігати атакам типу "людина посередині", де зловмисник намагається перехопити і змінити інформацію між двома сторонами. Завдяки віртуальним довірчим платформам можна забезпечити захищений канал зв'язку, що гарантує цілісність переданих даних і неможливість їх підробки.

Додатково, віртуальні довірчі платформи допомагають забезпечити відповідність стандартам безпеки та регуляторним вимогам. Вони можуть використовуватися для створення та управління ключами шифрування, які забезпечують конфіденційність даних. Важливим аспектом є також можливість регулярного оновлення та перевірки систем безпеки, що дозволяє швидко реагувати на нові загрози і вразливості.

Забезпечення безпеки віртуальних середовищ є складним завданням, яке вимагає інтегрованого підходу. Використання механізмів контролю доступу та віртуальних довірчих платформ є ефективним способом забезпечення захисту від

широкого спектра загроз. Ці механізми дозволяють створити багаторівневу систему захисту, яка включає не тільки технічні заходи, але й організаційні процедури та політики.

Наприклад, одна з ключових політик безпеки – це принцип мінімальних привілеїв, який передбачає надання користувачам лише тих прав доступу, які необхідні для виконання їхніх завдань. Це допомагає зменшити ризик зловживань та несанкціонованого доступу до критично важливих ресурсів. Крім того, важливо забезпечити регулярне навчання та підвищення кваліфікації співробітників щодо питань безпеки, щоб вони могли своєчасно виявляти і реагувати на потенційні загрози.

Також важливим аспектом є створення резервних копій даних і планів відновлення після аварій. Це дозволяє мінімізувати втрати у випадку інцидентів і забезпечити швидке відновлення роботи систем. Важливо, щоб резервні копії зберігалися у захищених місцях і регулярно перевірялися на цілісність та актуальність.

Віртуальні міжмережеві екрани відіграють важливу роль у захисті віртуальних середовищ, створюючи ефективні бар'єри між різними мережами. Їхня основна мета полягає у запобіганні несанкціонованого доступу та захисті систем від зовнішніх загроз і атак. Ці екрани працюють на рівні мережевого роутингу, контролюючи трафік між різними мережами та фільтруючи його згідно з визначеними правилами безпеки.

Їхня робота полягає у перехопленні та аналізі всього мережевого трафіку, який перетинає їхню межу. Під час цього процесу вони виявляють та блокують спроби несанкціонованого доступу до мережевих ресурсів, а також атаки зовнішніх загроз, такі як віруси, хакерські атаки тощо.

Важливою функцією віртуальних міжмережевих екранів є їхня здатність встановлювати та контролювати правила доступу для різних типів трафіку. Це дозволяє адміністраторам налаштовувати параметри безпеки відповідно до потреб та вимог конкретної мережевої інфраструктури. Наприклад, можна встановити

правила, що дозволяють тільки певним користувачам або пристроям здійснювати підключення до певних мереж або ресурсів.

Іншою важливою функцією є здатність віртуальних міжмережевих екранів до виявлення та блокування потенційно небезпечного трафіку. Вони можуть аналізувати пакети даних на предмет відомих сигнатур загроз, а також використовувати різноманітні техніки інтелектуального аналізу, щоб виявляти нові атаки та загрози, які ще не були ідентифіковані.

Загалом, віртуальні міжмережеві екрани є невід'ємною частиною стратегії безпеки мережі в будь-якому віртуальному середовищі. Вони забезпечують ефективний захист від зовнішніх загроз та несанкціонованого доступу, допомагаючи зберегти цілісність та безпеку мережевої інфраструктури.

У цьому підрозділі було проаналізовано ключові аспекти забезпечення безпеки в віртуальних середовищах. Основними елементами безпеки є шифрування та управління ключами, механізми контролю доступу, віртуальні довірчі платформи та віртуальні міжмережеві екрани.

Шифрування відіграє ключову роль у забезпеченні конфіденційності та цілісності даних у віртуальних середовищах. Управління ключами є невід'ємною частиною цього процесу, забезпечуючи ефективну роботу шифрування та захист ключів від несанкціонованого доступу.

Механізми контролю доступу, такі як аутентифікація, авторизація та аудит, дозволяють обмежувати доступ до ресурсів віртуальних середовищ тільки авторизованим користувачам та моніторити їхню діяльність для виявлення можливих загроз.

Віртуальні довірчі платформи та віртуальні міжмережеві екрани є важливими засобами захисту від зовнішніх загроз і атак. Вони дозволяють виявляти та блокувати несанкціонований трафік та забезпечують контроль прав доступу до мережевих ресурсів.

У цілому, інтегрований підхід до забезпечення безпеки включає в себе застосування різних технологій та стратегій, таких як шифрування, контроль доступу та віртуальні захисні механізми, для забезпечення безпеки та захисту

віртуальних середовищ.

1.3. Аналіз існуючих рішень із моніторингу безпеки віртуального середовища

Моніторинг безпеки віртуального середовища є ключовим аспектом захисту сучасних IT-інфраструктур. Різноманіття рішень, представлених на ринку, дозволяє організаціям обирати найбільш підходящі варіанти, виходячи з конкретних потреб і можливостей. У цьому підрозділі розглянемо найпопулярніші рішення для моніторингу безпеки віртуальних середовищ, їх функціонал, переваги та недоліки.

Розглянемо рішення VMware AppDefense.

Огляд та функціонал: VMware AppDefense є спеціалізованим рішенням для моніторингу безпеки віртуальних машин, яке інтегрується безпосередньо з гіпервізором VMware. Це рішення дозволяє визначати нормальну поведінку додатків і виявляти аномалії, які можуть свідчити про загрози. Основні функції включають:

автоматичний захист на основі поведінкових моделей;

ізоляція загроз;

інтеграція з іншими інструментами безпеки;

контроль цілісності системи.

Переваги:

глибока інтеграція з VMware vSphere: Забезпечує тісний зв'язок між віртуальними машинами та платформою управління, що дозволяє більш ефективно виявляти і реагувати на загрози.

Автоматичне виявлення аномалій:

використання поведінкових моделей для виявлення відхилень від нормальної роботи додатків.

зручний інтерфейс управління з інтуїтивно зрозумілим інтерфейсом, що полегшує налаштування і управління безпекою;

можливість ізоляції загроз у режимі реального часу: Швидка реакція на загрози з мінімальним впливом на роботу системи.

Недоліки:

висока вартість - це рішення може бути занадто дорогим для малих і середніх підприємств;

обмежені можливості для не-VMware середовищ: VMware AppDefense оптимізовано для роботи з продуктами VMware, що може обмежити його ефективність у змішаних середовищах[6].

Розглянемо рішення Cisco Tetration.

Огляд та функціонал: Cisco Tetration - це комплексне рішення для моніторингу безпеки, яке охоплює центри обробки даних та хмарні середовища. Воно забезпечує детальний аналіз трафіку, виявлення аномалій, управління політиками безпеки і забезпечення відповідності нормативним вимогам. Основні функції включають:

глибокий аналіз мережевого трафіку;

виявлення аномалій і загроз;

управління політиками безпеки;

забезпечення відповідності стандартам безпеки.

Переваги:

підтримка фізичних і віртуальних середовищ: Cisco Tetration може моніторити як фізичні сервери, так і віртуальні машини, що забезпечує комплексний підхід до безпеки;

інтеграція з мережевими пристроями Cisco: глибока інтеграція з існуючою мережевою інфраструктурою, що полегшує впровадження і управління;

потужний аналітичний двигун: використання передових алгоритмів для аналізу трафіку і виявлення загроз;

автоматизація управління політиками безпеки: зменшення кількості ручних операцій і помилок, пов'язаних з управлінням безпекою.

Недоліки:

складність налаштування та впровадження: потребує значних зусиль для

налаштування та інтеграції у існуючу інфраструктуру;

висока вартість: рішення може бути дорогим для малих і середніх підприємств[7].

Розглянемо рішення Splunk

Огляд та функціонал: Splunk - це потужна платформа для збору, індексації та аналізу машинних даних у реальному часі. Вона надає інструменти для моніторингу та забезпечення безпеки віртуальних середовищ, включаючи:

збір та аналіз логів;

виявлення аномалій;

автоматизація реагування на інциденти;

інтеграція з різноманітними джерелами даних.

Переваги:

потужний аналітичний функціонал: можливість обробки великих обсягів даних у реальному часі з використанням передових алгоритмів;

гнучкість налаштувань: можливість кастомізації під конкретні потреби організації;

інтеграція з різноманітними джерелами даних: підтримка широкого спектру форматів даних і джерел;

широкі можливості автоматизації: зменшення ручних операцій і покращення ефективності управління безпекою.

Недоліки:

висока вартість ліцензування: вартість може бути значною для малих і середніх підприємств;

складність у навчанні персоналу: потребує значного часу та ресурсів для навчання користувачів і адміністраторів[8].

Розглянемо рішення Elastic Security

Огляд та функціонал: Elastic Security - це комплексне рішення для моніторингу та забезпечення безпеки на базі Elastic Stack. Воно включає засоби для збору, аналізу та візуалізації даних, а також для виявлення загроз та автоматизації реагування. Основні функції включають:

збір даних з різноманітних джерел;

аналіз та візуалізація даних;

виявлення загроз на основі поведінкових моделей;

автоматизація реагування на інциденти.

Переваги:

відкритий вихідний код: можливість кастомізації та налаштування під конкретні потреби організації;

висока продуктивність: обробка великих обсягів даних у реальному часі;

інтеграція з elastic stack: використання потужних інструментів для аналізу та візуалізації даних;

широкі можливості кастомізації: гнучкість налаштувань і інтеграція з іншими інструментами.

Недоліки:

необхідність додаткових налаштувань: потребує значних зусиль для впровадження та налаштування;

відсутність повної інтеграції з деякими комерційними інструментами: можуть виникати проблеми з інтеграцією у змішаних середовищах[9].

У цьому підрозділі було проаналізовано кілька рішень для моніторингу безпеки віртуального середовища. Загальний висновок з аналізу показує, що існують різні підходи та інструменти для забезпечення безпеки в IT-інфраструктурі.

Перш за все, різноманіття рішень відображає різний спектр потреб різних організацій. Кожне рішення має свої переваги та недоліки, які необхідно враховувати при виборі оптимального варіанту для конкретної інфраструктури.

VMware AppDefense і Cisco Tetration, наприклад, надають комплексні рішення для моніторингу безпеки, але вони можуть бути дорогими та складними у впровадженні, особливо для малих та середніх підприємств.

Splunk і Elastic Security використовують потужні аналітичні інструменти для моніторингу та виявлення загроз, але вони також вимагають додаткових зусиль для налаштування та інтеграції.

Отже, при виборі рішення для моніторингу безпеки віртуального середовища необхідно ретельно враховувати потреби та можливості організації, а також розглядати вартість, складність впровадження та можливості налаштування.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ МОНІТОРИНГУ БЕЗПЕКИ ВІРТУАЛЬНОГО СЕРЕДОВИЩА НА БАЗІ VMWARE APP DEFENCE

2.1. Призначення та архітектура рішення VMware App Defence

VMware App Defense – це система кібербезпеки, спеціально розроблена для захисту додатків, що працюють у віртуалізованих середовищах VMware. Основна мета цього рішення – забезпечення безпеки шляхом моніторингу поведінки додатків і виявлення відхилень від нормального функціонування, що може свідчити про наявність загроз. VMware App Defense використовує інтеграцію з іншими продуктами VMware для створення комплексного захисного середовища, яке автоматизує багато аспектів безпекових процесів, знижуючи ризики та підвищуючи ефективність захисту.

VMware App Defence призначене для захисту додатків шляхом виявлення та блокування загроз. Основні функції та можливості цього рішення включають:

Виявлення загроз: автоматичне виявлення аномальної поведінки додатків, що може свідчити про наявність загроз.

Автоматичний захист: реагування на виявлені загрози шляхом автоматичного блокування або ізоляції підозрілих дій.

Моніторинг поведінки додатків: постійний моніторинг активності додатків для виявлення відхилень від нормальної поведінки.

Ці функції дозволяють VMware App Defence забезпечити високий рівень безпеки для віртуальних середовищ, мінімізуючи ризики від кіберзагроз.

Архітектура VMware App Defense побудована таким чином, щоб забезпечити ефективне виявлення, моніторинг і реагування на загрози в реальному часі. Вона складається з кількох ключових компонентів, кожен з яких виконує специфічні функції, і всі вони разом утворюють злагоджену систему захисту. Основними компонентами архітектури є: AppDefense Manager, AppDefense Appliance, AppDefense Guest Module.

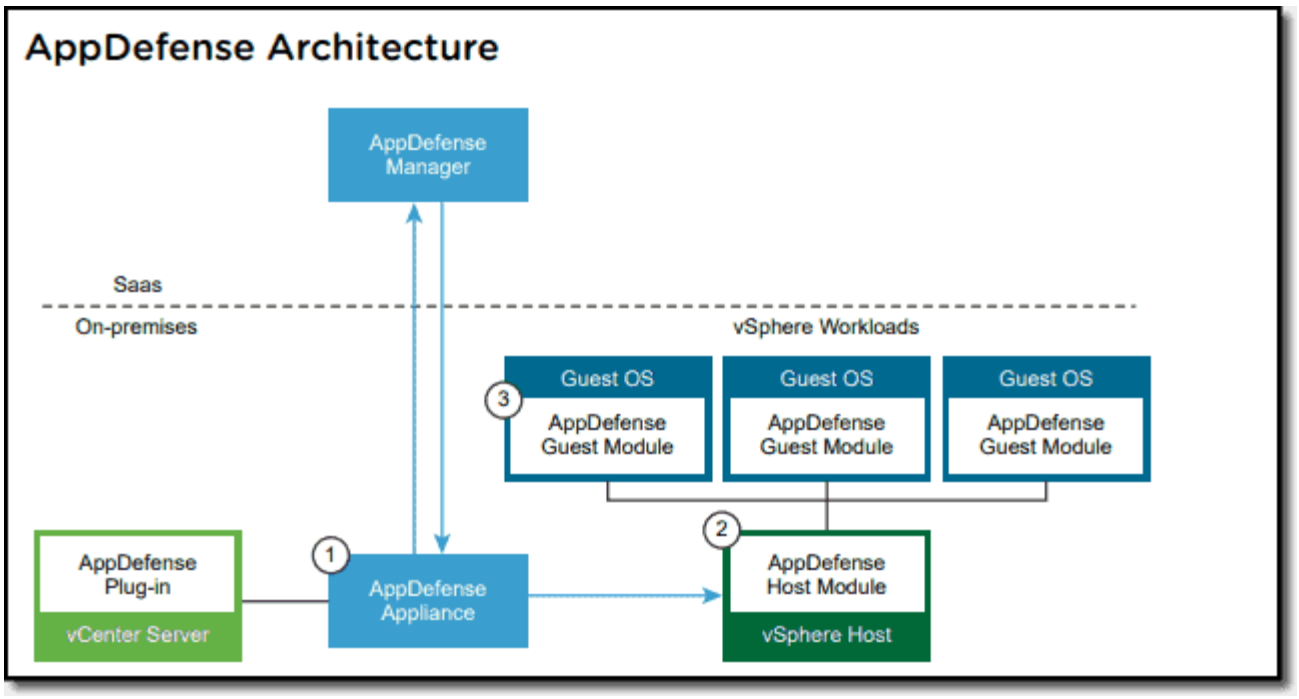

Рис 2.1. Архітектура рішення VMware App Defence [10]

Загальна архітектура VMware App Defense складається з трьох основних компонентів, які взаємодіють між собою та з іншими продуктами VMware, такими як VMware vCenter і vSphere. Кожен компонент виконує специфічні функції, що сприяють загальному захисту додатків[10].

AppDefense Manager – центральний компонент системи, який відповідає за управління політиками безпеки, моніторинг стану системи та реагування на інциденти[10].

AppDefense Appliance – віртуальний пристрій, що забезпечує зв'язок між віртуальними машинами, де встановлений AppDefense Guest Module, та AppDefense Manager[10].

AppDefense Guest Module – агент, який встановлюється на кожну віртуальну машину і здійснює моніторинг активності додатків на рівні операційної системи.

Потік даних в архітектурі VMware App Defense проходить через кілька етапів.

1. Моніторинг – AppDefense Guest Module здійснює постійний моніторинг активності на віртуальних машинах.
2. Передача – Зібрані дані передаються до AppDefense Appliance.

3. Обробка – AppDefense Appliance аналізує дані та передає їх до AppDefense Manager.
4. Аналіз та реагування – AppDefense Manager аналізує дані, виявляє відхилення від нормального функціонування та вживає необхідних заходів для захисту системи[10].

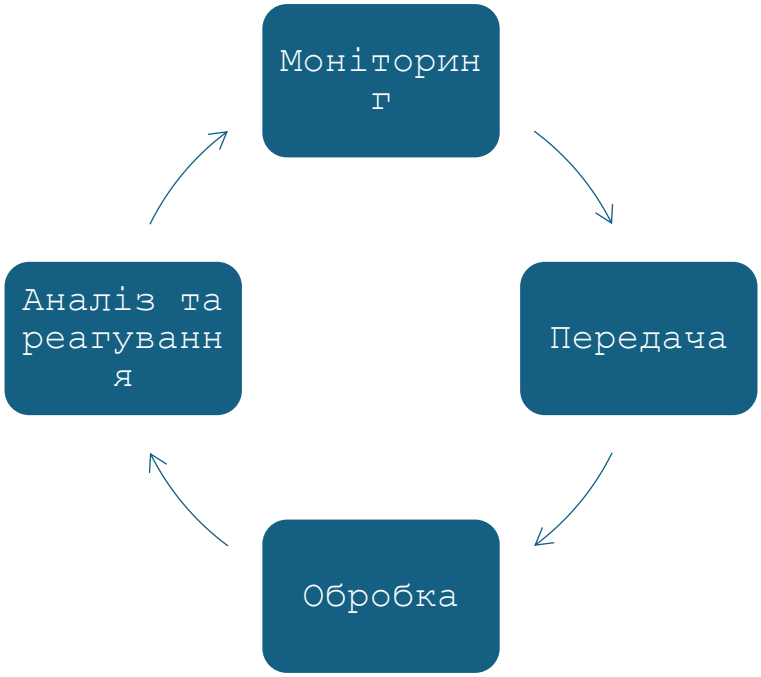

Рис. 2.2. Етапи потоку даних

Інтеграція компонентів VMware App Defense з іншими продуктами VMware, такими як vSphere та vCenter, дозволяє створити єдину систему управління та моніторингу безпеки:

vCenter: Забезпечує централізоване управління віртуальними машинами і інтеграцію з AppDefense Appliance.

vSphere: платформа віртуалізації, на якій працюють віртуальні машини, забезпечує необхідне середовище для роботи AppDefense Guest Module.

В даному підрозділі було розглянуто систему кібербезпеки VMware App Defense, яка спеціально розроблена для захисту додатків у віртуалізованих середовищах VMware. Основна мета VMware App Defense – забезпечення безпеки додатків через моніторинг їх поведінки та виявлення аномалій, що можуть свідчити про загрози. Було детально описано призначення рішення, яке полягає у виявленні

та блокуванні загроз шляхом автоматичного реагування та моніторингу поведінки додатків.

Архітектура VMware App Defense складається з трьох основних компонентів: AppDefense Manager, AppDefense Appliance та AppDefense Guest Module, які забезпечують ефективне виявлення, моніторинг та реагування на загрози в реальному часі. Потік даних проходить через кілька етапів, включаючи моніторинг, передачу, обробку та аналіз, що дозволяє вчасно виявляти та нейтралізувати загрози.

Також було розглянуто інтеграцію VMware App Defense з іншими продуктами VMware, такими як vSphere та vCenter, що створює єдину систему управління та моніторингу безпеки. Це дозволяє підвищити ефективність захисту додатків у віртуалізованих середовищах, знижуючи ризики від кіберзагроз та автоматизуючи багато аспектів безпекових процесів.

2.2. Призначення та основні функції компонентів VMware App Defence

VMware AppDefense складається з кількох ключових компонентів: AppDefense Manager, AppDefense Appliance, Guest Modules, Host Modules та інтеграції з NSX. Кожен з цих компонентів має своє унікальне призначення і виконує важливі функції, що забезпечують комплексний підхід до захисту. У цьому підрозділі ми детально розглянемо призначення та основні функції кожного з компонентів VMware AppDefense.

1. AppDefense Manager

Призначення: AppDefense Manager є центральним елементом рішення, відповідальним за управління політиками безпеки, аналіз поведінки віртуальних машин і координацію реагування на інциденти.

Основні функції:

управління політиками безпеки: створення, редагування та застосування політик безпеки для віртуальних машин і їхніх груп.

аналіз поведінки: збір і аналіз даних про активність віртуальних машин для

виявлення аномалій та потенційних загроз.

інцидент-менеджмент: виявлення, класифікація та реагування на інциденти безпеки, включаючи автоматичне застосування заходів для нейтралізації загроз.

інтеграція з іншими системами: забезпечення взаємодії з іншими інструментами та платформами безпеки для підвищення ефективності моніторингу та захисту.

2. AppDefense Appliance

Призначення: AppDefense Appliance використовується в локальному середовищі датацентру. Це віртуальний пристрій, який контролює весь трафік до і з AppDefense Manager.

Основні функції:

Моніторинг трафіку: віртуальний пристрій контролює весь трафік до і з AppDefense Manager.

Брокер з'єднань: Локальний проксі-пристрій виступає як брокер з'єднань, перенаправляючи трафік до інших компонентів VMware vSphere, таких як vCenter.

Зв'язок з AppDefense Manager: Забезпечує з'єднання з компонентом AppDefense Manager для координації заходів безпеки.

3. Guest Modules

Guest Modules — це модулі, які встановлюються безпосередньо на віртуальні машини для забезпечення детального моніторингу їхньої активності та виявлення аномалій[10].

Основні функції:

збір даних: збір детальної інформації про процеси, мережеву активність і системні виклики віртуальних машин.

виявлення аномалій: аналіз зібраних даних для виявлення відхилень від нормальної поведінки, що можуть свідчити про наявність загроз.

передача даних: надсилання зібраної інформації до AppDefense Manager для подальшого аналізу і прийняття рішень.

забезпечення цілісності: перевірка цілісності програмного забезпечення та конфігурацій віртуальних машин для виявлення несанкціонованих змін.

4. Host Modules (VIB)

Призначення: VIB (vSphere Installation Bundle) розгортається на кожному хості ESXi.

Основні функції:

моніторинг та забезпечення безпеки: модулі на хості та гостьовій системі працюють разом для моніторингу та забезпечення виконання запланованого стану поведінки гостьової системи.

5. Інтеграція з VMware NSX

Призначення: інтеграція з VMware NSX дозволяє забезпечити додатковий рівень мережевої безпеки, використовуючи політики мікросегментації для ізоляції віртуальних машин і захисту мережевих взаємодій[10].

Основні функції:

мікросегментація: створення і застосування політик мікросегментації для обмеження мережевих взаємодій між віртуальними машинами, зменшуючи ризик розповсюдження загроз;

контроль трафіку: моніторинг і контроль мережевого трафіку, що проходить через віртуальні машини, для виявлення підозрілої активності;

автоматична ізоляція: автоматичне ізолювання віртуальних машин у разі виявлення загроз для запобігання їх розповсюдженню;

інтеграція з політиками безпеки: забезпечення узгодженості політик мережевої безпеки з загальними політиками безпеки віртуального середовища.

6. vCenter Server

Призначення: vCenter Server використовується для збору інвентаризаційних даних на місці.

Основні функції:

збір інвентаризаційних даних: інформація використовується для призначення області безпеки, готовності гостьових систем (на основі ос) та призначення гостьових систем до хостів;

виконання заходів по усуненню загроз: використовується для виконання заходів, таких як призупинення роботи віртуальної машини.

Взаємодія між компонентами VMware AppDefense забезпечує комплексний підхід до захисту віртуального середовища. Дані з Guest Modules передаються до AppDefense Manager, де вони аналізуються для виявлення потенційних загроз. У разі виявлення аномалій, AppDefense Manager може взаємодіяти з NSX для ізоляції віртуальної машини або застосування інших заходів безпеки. AppDefense Appliance забезпечує ефективне розгортання та налаштування всіх компонентів, гарантуючи їх безперебійну роботу та взаємодію. Використання vCenter Server дозволяє збирати інвентаризаційні дані та виконувати заходи по усуненню загроз, забезпечуючи цілісність та безпеку всієї інфраструктури.

В даному підрозділі було розглянуто призначення та основні функції компонентів VMware App Defense, які разом забезпечують комплексний підхід до захисту віртуальних середовищ. AppDefense Manager є центральним елементом системи, що відповідає за управління політиками безпеки, аналіз поведінки віртуальних машин та координацію реагування на інциденти. AppDefense Appliance інтегрує рішення з існуючою інфраструктурою, автоматизує розгортання компонентів та забезпечує масштабованість. Guest Modules, встановлені безпосередньо на віртуальні машини, здійснюють детальний моніторинг їхньої активності та виявлення аномалій. Інтеграція з VMware NSX додає додатковий рівень мережевої безпеки, застосовуючи політики мікросегментації для ізоляції віртуальних машин та контролю мережевого трафіку.

2.3. Процеси функціонування рішення VMware App Defense

Рішення VMware App Defense включає в себе декілька ключових процесів, що забезпечують комплексний підхід до захисту. Ці процеси охоплюють всі етапи від розгортання та налаштування системи до постійного моніторингу, аналізу та реагування на інциденти. У цьому розділі ми детально розглянемо основні процеси функціонування рішення VMware App Defense.

1. Розгортання та налаштування

Ініціалізація системи

Процес розпочинається з розгортання AppDefense Appliance у віртуальній інфраструктурі, що забезпечує центральний пункт управління всіма компонентами.

Рис 2.3. Ключові етапи

AppDefense починає з захоплення початкового стану додатку, використовуючи машинне навчання для збирання інформації про стан виконання додатку. Це дозволяє отримати повну картину інфраструктури.

Інсталяція модулів

На кожну віртуальну машину встановлюються Guest Modules, які забезпечують детальний моніторинг діяльності та безпеки.

Налаштування політик:

В AppDefense Manager створюються та налаштовуються політики безпеки, які визначають дозволену поведінку для віртуальних машин і мережевих взаємодій.

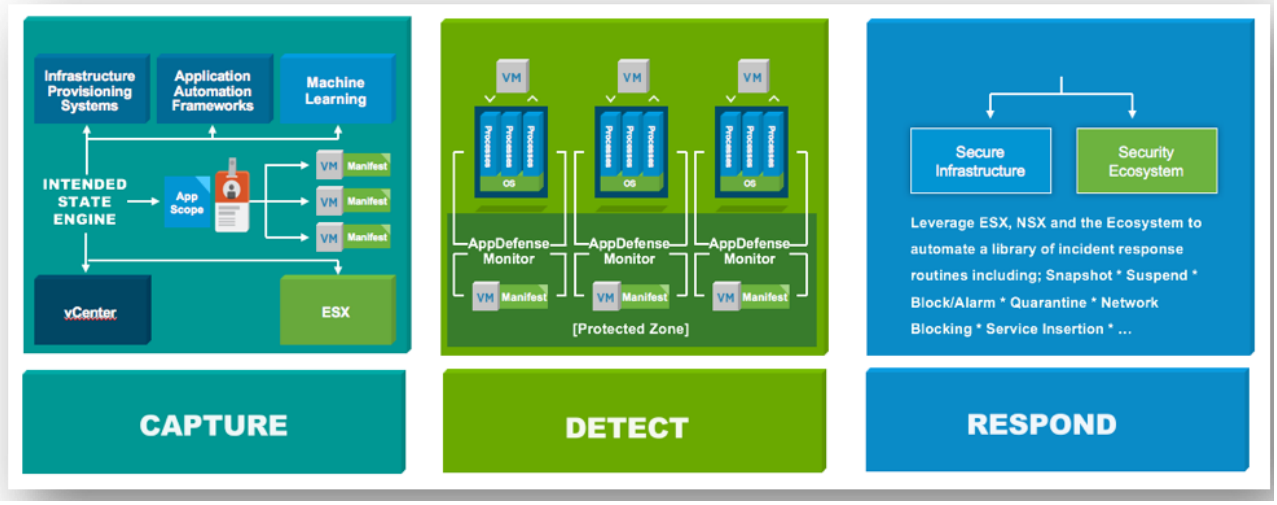

Рис. 2.4. Основні техніки [11]

2. Моніторинг та збір даних

Постійний моніторинг

Guest Modules збирають детальну інформацію про процеси, мережеву активність та системні виклики віртуальних машин у реальному часі.

Використання гіпервізора vSphere для підвищеної видимості додатків. Гіпервізор може бачити як запланований, так і виконуваний стан розгорнутого додатку, що забезпечує детальне уявлення про функціонування додатку[11].

Аналіз поведінки

Зібрані дані надходять до AppDefense Manager, де вони аналізуються для виявлення аномалій та потенційних загроз.

Захоплення і зберігання інформації про запланований і виконуваний стан додатків у захищеному просторі гіпервізора vSphere. Це запобігає несанкціонованому втручанню та дозволяє автоматично сповіщати про неочікувані або непередбачені зміни[11].

Моніторинг гіпервізора та мережевих взаємодій:

AppDefense інтегрується з VMware vSphere для моніторингу стану гіпервізора та забезпечення його безпеки.

Завдяки інтеграції з VMware NSX, здійснюється моніторинг та контроль мережевого трафіку між віртуальними машинами, забезпечуючи виявлення підозрілої активності.

3. Виявлення та реагування на інциденти

Виявлення інцидентів: AppDefense Manager постійно аналізує дані для виявлення аномалій, які можуть свідчити про потенційні загрози. Використовуються методи машинного навчання для покращення точності виявлення.

Використання унікальних властивостей віртуалізації для сильної ізоляції та забезпечення найкращого контексту для виявлення аномалій. AppDefense працює у гіпервізорі, що дозволяє мати окрему довірчу домену та забезпечувати контекст додатку і ізоляцію одночасно.

Класифікація інцидентів виявлені інциденти класифікуються за рівнем критичності, що дозволяє пріоритизувати реагування на них.

Реагування на інциденти в разі виявлення серйозних загроз, AppDefense може автоматично ізолювати віртуальні машини або застосувати інші заходи для нейтралізації загроз.

Використання автоматизації для забезпечення автоматичних відповідей на тривоги, що спрацьовують. Віртуалізована інфраструктура повністю підтримує автоматизацію, що дозволяє AppDefense використовувати такі властивості, як вимикання, призупинення та створення знімків віртуальних машин для усунення шкідливої активності.

Адміністратори отримують повідомлення про виявлені інциденти та рекомендовані дії для їх усунення.

Аналіз інцидентів та розслідування:

Для кожного інциденту збираються всі необхідні дані та журнали, що дозволяє провести детальний аналіз і розслідування.

На основі зібраних даних складаються звіти, які допомагають зрозуміти причини інциденту та розробити рекомендації для запобігання подібним випадкам у майбутньому.

4. Оптимізація та покращення безпеки

Оцінка ефективності

Регулярний аудит: проводяться регулярні аудити системи безпеки для оцінки

ефективності політик та виявлення можливих слабких місць.

Аналіз ефективності заходів: аналізуються результати реагування на інциденти, що дозволяє оцінити ефективність застосованих заходів та внести необхідні корективи.

Регулярний аудит і аналіз ефективності політик та заходів безпеки, з урахуванням додаткових даних, зібраних гіпервізором про запланований і виконуваний стан додатків.

Впровадження покращень

Оновлення політик: на основі висновків аудиту та аналізу інцидентів оновлюються та оптимізуються політики безпеки.

Інтеграція нових технологій: впроваджуються нові технології та методи захисту для забезпечення актуальності та ефективності системи безпеки.

У цьому підрозділі ми розглянули процеси функціонування рішення VMware App Defense, які забезпечують комплексний підхід до захисту віртуальної інфраструктури. Було вивчено основні етапи розгортання та налаштування системи, включаючи ініціалізацію, інсталяцію модулів та налаштування політик безпеки. Це створює надійну базу для подальшого моніторингу та збору даних.

Постійний моніторинг віртуальних машин, здійснюваний Guest Modules та гіпервізором vSphere, забезпечує детальну видимість і контроль над мережевою активністю та системними викликами. Аналіз поведінки додатків дозволяє виявляти аномалії та потенційні загрози, забезпечуючи швидке реагування на інциденти. Інтеграція з VMware NSX додатково покращує можливості моніторингу та контролю мережевого трафіку.

Процес виявлення та реагування на інциденти включає класифікацію загроз за рівнем критичності, автоматизацію відповідей на виявлені загрози та надання адміністраторам рекомендацій щодо їх усунення. Це дозволяє швидко ізолювати підозрілі віртуальні машини та мінімізувати потенційний збиток.

Оптимізація та покращення безпеки здійснюються через регулярні аудити та аналіз ефективності політик і заходів безпеки. Це дозволяє своєчасно вносити корективи та впроваджувати нові технології, забезпечуючи актуальність і високий

рівень захисту віртуальної інфраструктури.

Таким чином, VMware App Defense забезпечує комплексний підхід до захисту віртуальних середовищ, що охоплює всі етапи від розгортання до постійного моніторингу, виявлення та реагування на загрози, а також постійного вдосконалення системи безпеки.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ МОНІТОРИНГУ БЕЗПЕКИ ВІРТУАЛЬНОГО СЕРЕДОВИЩА

3.1. Варіанти впровадження системи моніторингу безпеки віртуального середовища на базі VMware App Defence

Впровадження системи моніторингу безпеки віртуального середовища на базі VMware App Defense може бути здійснене різними способами, залежно від потреб та можливостей організації. В даному підпункті розглянемо основні варіанти впровадження, етапи реалізації, а також їх переваги та недоліки.

Методи впровадження:

1. Локальне впровадження

Локальне впровадження системи моніторингу передбачає встановлення та налаштування VMware App Defense на інфраструктурі, що знаходиться в межах локальної мережі організації. Цей підхід має такі особливості:

для локального впровадження необхідно забезпечити наявність достатніх апаратних ресурсів, включаючи сервери, сховища та мережеве обладнання. Також потрібне програмне забезпечення, включаючи гіпервізор VMware vSphere та інші необхідні компоненти;

локальне впровадження дозволяє організації мати повний контроль над усіма аспектами системи безпеки, включаючи управління даними, політиками безпеки та конфігурацією компонентів.

Недоліки: основними недоліками є високі початкові витрати на обладнання та складність підтримки системи.

2. Хмарне впровадження

Хмарне впровадження передбачає використання хмарних сервісів для розгортання VMware App Defense. Цей підхід має такі особливості:

Інтеграція з хмарними сервісами: Організації можуть використовувати сервіси, такі як VMware Cloud on AWS, для забезпечення моніторингу та безпеки

віртуального середовища.

Гнучкість та масштабованість: хмарне впровадження дозволяє легко масштабувати ресурси відповідно до потреб організації, зменшуючи витрати на обладнання та обслуговування.

Недоліки: основним недоліком є залежність від провайдера хмарних послуг та можливі ризики, пов'язані з безпекою даних.

3. Гібридне впровадження

Гібридне впровадження поєднує локальні та хмарні ресурси, дозволяючи організації використовувати переваги обох підходів. Цей метод має такі особливості:

Комбінація ресурсів: організації можуть розміщувати критично важливі компоненти локально, а менш критичні – у хмарі, забезпечуючи оптимальний баланс між безпекою та гнучкістю.

Управління ресурсами: гібридний підхід дозволяє ефективно керувати ресурсами та забезпечувати високий рівень безпеки, розподіляючи робочі навантаження між локальними та хмарними сервісами.

Недоліки: основним недоліком є складність управління гібридною інфраструктурою та інтеграція між локальними та хмарними компонентами.

Етапи впровадження:

1. Підготовка інфраструктури

Перший етап включає аудит існуючої інфраструктури, оцінку ресурсів та планування впровадження.

Аналіз поточних потреб: визначення вимог до системи моніторингу та обсягу роботи, необхідного для впровадження.

Оцінка ресурсів: перевірка наявності необхідних апаратних та програмних ресурсів, включаючи сервери, мережеве обладнання та ліцензії на програмне забезпечення.

розробка плану впровадження, включаючи етапи роботи, відповідальних осіб та терміни виконання.

2. Інсталяція та конфігурація

На цьому етапі здійснюється встановлення та налаштування VMware App Defense:

Встановлення програмного забезпечення: інсталяція гіпервізора VMware vSphere, AppDefense Appliance, Guest Modules та інших необхідних компонентів.

Конфігурація системи: налаштування політик безпеки, правил моніторингу та інтеграції з існуючими системами управління.

3. Тестування та верифікація

Після встановлення та конфігурації проводиться тестування системи:

тестування всіх компонентів системи, включаючи моніторинг, аналіз даних та автоматичне реагування на інциденти.

перевірка на вразливості та оцінка ефективності впровадженої системи.

внесення необхідних змін та налаштувань на основі результатів тестування.

Локальне впровадження. Його перевагами є повний контроль над системою, що дозволяє забезпечити високий рівень безпеки даних. Крім того, можливість індивідуальних налаштувань дозволяє відповідати конкретним потребам організації. Проте, слід зазначити, що локальне впровадження супроводжується високими початковими витратами, оскільки потрібно інвестувати в обладнання та інфраструктуру. Крім того, складність підтримки та масштабування може стати проблемою в майбутньому.

Хмарне впровадження. Перевагою хмарного впровадження є гнучкість і легкість масштабування. Зменшення витрат на обладнання також є значним плюсом цього підходу. Однак, варто враховувати, що цей метод може стати залежним від провайдера хмарних послуг, що може вплинути на доступність сервісу та призвести до ризиків безпеки.

Гібридне впровадження. Поєднує в собі кращі аспекти обох підходів. Воно забезпечує оптимальний баланс між безпекою та гнучкістю, що дозволяє ефективно управляти ресурсами. Однак, слід відзначити, що складність інтеграції та управління може стати викликом для організацій, які вирішують прийняти цей підхід. Також можуть виникнути проблеми з сумісністю між різними системами, що може ускладнити процес впровадження.

Отже, у даному розділі було ретельно проаналізовано три основні стратегії впровадження системи моніторингу безпеки на базі VMware App Defense: локальне, хмарне та гібридне впровадження. Локальне впровадження, незважаючи на його здатність забезпечити повний контроль над системою, створює значні витрати на початковий етап і потребує складної підтримки в подальшому. З іншого боку, хмарне впровадження пропонує гнучкість та легкість масштабування, але його ефективність залежить від надійності обраного хмарного провайдера і може включати певні ризики безпеки. Гібридне впровадження виявляється оптимальним варіантом, оскільки поєднує переваги обох підходів, забезпечуючи баланс між безпекою та гнучкістю. Тим не менш, воно потребує складного управління та інтеграції для оптимальної роботи. Загальна аналіз дозволяє зробити висновок, що гібридне впровадження є наибільш перспективним із зазначених варіантів, забезпечуючи не лише безпеку, але і гнучкість у використанні технологічних рішень.

3.2. Порядок налаштування та використання засобів моніторингу безпеки віртуального середовища на базі VMware App Defence

Впровадження VMware App Defense для моніторингу безпеки віртуального середовища включає декілька ключових етапів, які допоможуть налаштувати систему та забезпечити її ефективну роботу. У цьому підрозділі розглянемо детальний порядок налаштування та використання засобів моніторингу безпеки на базі VMware App Defense, а також основні кроки для інтеграції та підтримки.

Етап 1: Підготовка до встановлення

Оцінка інфраструктури: Перевірка поточного стану інфраструктури, визначення необхідних ресурсів для впровадження VMware App Defense.

Планування впровадження: Розробка плану впровадження з урахуванням специфіки організації, визначення відповідальних осіб та етапів роботи.

Закупівля та підготовка обладнання

Придбання ліцензій: отримання необхідних ліцензій для VMware App Defense та інших пов’язаних продуктів.

Підготовка апаратних ресурсів: Перевірка наявності необхідного апаратного забезпечення, включаючи сервери, мережеве обладнання та сховища.

Етап 2: Інсталяція VMware App Defense

Інсталяція гіпервізора VMware vSphere: Встановлення гіпервізора, який буде використовуватися для управління віртуальними машинами.

Інсталяція VMware App Defense Appliance: Встановлення та налаштування App Defense Appliance, який буде центральним компонентом системи безпеки.

Інсталяція та налаштування агентів

Інсталяція Guest Modules: Встановлення агентів на кожну віртуальну машину, що буде моніторитися. Ці агенти відповідальні за збір даних та моніторинг діяльності.

Налаштування зв'язку між агентами та Appliance: Забезпечення коректного зв’язку між агентами та центральним компонентом для передачі даних.

Етап 3: Налаштування політик безпеки

Визначення політик безпеки: Створення політик безпеки на основі вимог організації, включаючи правила доступу, поведінкові патерни та аномалії.

Налаштування правил моніторингу: Впровадження правил для виявлення підозрілих дій та аномальної поведінки віртуальних машин.

Тестування та верифікація політик

Тестування політик: Проведення тестів для перевірки коректності роботи впроваджених політик безпеки.

Аналіз результатів: Оцінка результатів тестування, внесення необхідних змін для оптимізації політик.

Етап 4: Моніторинг та управління

Моніторинг діяльності віртуальних машин: Постійний аналіз активності віртуальних машин для виявлення потенційних загроз.

Аналіз логів та подій: Регулярний перегляд логів та подій для виявлення підозрілої діяльності.

Реагування на інциденти:

Автоматичне реагування – використання інструментів автоматичного реагування на інциденти для швидкого усунення загроз.

Ручне втручання – втручання адміністраторів для вирішення складних інцидентів та внесення змін до налаштувань системи.

Рис. 3.1. Етапи впровадження

Етап 5: Підтримка та оновлення

Оновлення програмного забезпечення: Регулярне оновлення VMware App

Defense та інших компонентів для забезпечення актуальності системи.

Впровадження нових політик: Внесення змін до політик безпеки на основі нових загроз та вразливостей.

Навчання персоналу

Тренінги для адміністраторів: Проведення навчальних заходів для адміністраторів з метою підвищення їх компетенцій у роботі з VMware App Defense.

Навчання користувачів: Інформування користувачів про основні правила безпеки та нові політики організації.

У даному підрозділі було ретельно проаналізовано процес налаштування та використання засобів моніторингу безпеки, які базуються на VMware App Defense. Виявлено, що впровадження цих засобів передбачає кілька критичних етапів. По-перше, необхідна підготовка інфраструктури, що включає в себе розгортання необхідних ресурсів та належне налаштування. По-друге, етап інсталяції програмного забезпечення вимагає уважної уваги до деталей та дотримання встановлених процедур. По-третє, налаштування політик безпеки відіграє ключову роль у забезпеченні відповідності системи вимогам безпеки. Далі, етап моніторингу та управління вимагає постійної уваги та реагування на потенційні загрози. Нарешті, підтримка та оновлення системи є важливими аспектами її ефективної роботи та забезпечення безпеки. Кожен з цих етапів передбачає конкретні дії, спрямовані на забезпечення найвищого рівня безпеки та ефективної роботи системи у відповідності до вимог організації.

3.3. Рекомендації щодо застосування методів та засобів моніторингу безпеки віртуального середовища

Моніторинг безпеки віртуального середовища є критичним аспектом забезпечення інформаційної безпеки сучасних IT-інфраструктур, тому ми розробили перелік методичних рекомендацій та практичні приклади щодо ефективного застосування методів та засобів моніторингу безпеки, що допоможуть

організаціям знизити ризики та підвищити рівень захищеності своїх віртуальних середовищ.

Для ефективного застосування методів та засобів моніторингу безпеки віртуального середовища рекомендуємо:

системи виявлення вторгнень (IDS) забезпечують моніторинг мережевого трафіку та системних подій для виявлення підозрілої активності. IDS можуть бути як мережевими (NIDS), так і хостовими (HIDS).

Приклад:

впровадження NIDS у віртуальне середовище для аналізу мережевого трафіку між віртуальними машинами та виявлення аномалій;

встановлення HIDS на кожну віртуальну машину для моніторингу системних логів і процесів.

Впровадження рішень з управління логами та подіями безпеки.

Системи управління інформацією та подіями безпеки. забезпечують централізоване збирання, аналіз та кореляцію логів з різних джерел, що дозволяє швидко виявляти та реагувати на інциденти.

Приклад:

Використання SIEM для збирання логів з гіпервізорів, віртуальних машин та мережевих пристроїв.

Налаштування кореляційних правил для автоматичного виявлення складних атак та аномальної поведінки.

Застосування шифрування та управління ключами.

Шифрування даних є важливим заходом для захисту конфіденційної інформації. Управління ключами забезпечує безпечне зберігання та використання ключів шифрування.

Приклад:

шифрування даних, що зберігаються на віртуальних машинах, з використанням стандартів AES-256.

Використання централізованого сервера управління ключами для автоматичного генерації та ротації ключів.

Забезпечення шифрування офлайн VM образів та резервних копій для захисту конфіденційності та цілісності даних. Для організацій, що використовують зовнішніх постачальників хмарних послуг, забезпечення шифрованих з'єднань та приватного каналу, окремого від звичайного Інтернет-трафіку.

Впровадження механізмів контролю доступу.

Механізми контролю доступу забезпечують обмеження доступу до критичних ресурсів та функцій віртуального середовища, запобігаючи несанкціонованим діям.

Приклад:

Налаштування ролей та привілеїв у VMware vSphere для обмеження доступу адміністраторам та користувачам до певних функцій.

Використання двофакторної аутентифікації для доступу до консолі управління гіпервізором.

Впровадження системи контролю доступу до фізичного середовища, де розміщена інфраструктура, а також до платформи управління гіпервізором та віртуальними машинами. Доступ повинні мати тільки адміністратори та авторизовані користувачі.

Використання віртуальних довірчих платформ.

Віртуальні довірчі платформи забезпечують апаратний рівень захисту для віртуальних машин, включаючи безпечне зберігання ключів та інші криптографічні операції.

Приклад:

Впровадження vTPM на віртуальних машинах для забезпечення апаратного рівня захисту ключів шифрування.

Використання vTPM для підвищення захисту операційних систем та додатків, що працюють у віртуальному середовищі.

Використання віртуальних міжмережевих екранів.

Віртуальні міжмережеві екрани забезпечують сегментацію мережі та контроль доступу між віртуальними машинами, знижуючи ризик внутрішніх атак.

Приклад:

Встановлення віртуальних міжмережевих екранів для сегментації мережі та обмеження трафіку між різними віртуальними машинами.

Налаштування політик безпеки для віртуальних міжмережевих екранів, що обмежують доступ до критичних ресурсів та служб.

Використання довірчих віртуальних доменів.

Довірчі віртуальні домени забезпечують ізоляцію віртуальних машин з різними рівнями довіри, запобігаючи витоку даних між ними.

Приклад:

Налаштування довірчих віртуальних доменів для ізоляції тестових, розробницьких та продуктивних середовищ.

Використання TVD для запобігання витоку конфіденційної інформації між віртуальними машинами з різними рівнями довіри.

Моніторинг і аудит

Реалізація моніторингу та аудиту: впровадження системи моніторингу та логування всього мережевого трафіку та операцій віртуальних машин. Регулярний аудит цих логів для виявлення тенденцій, які можуть свідчити про порушення безпеки[3].

Використання рішень для моніторингу, таких як системи виявлення вторгнень (IDS), та спеціалізованих інструментів для гіпервізорів, таких як віртуальні міжмережеві екрани та інтеграційні системи моніторингу цілісності[2].

Налаштування кореляційних правил у SIEM для автоматичного виявлення складних атак та аномальної поведінки[2].

Використання систем автоматичного оновлення та патч-менеджменту для підтримки актуальності програмного забезпечення та запобігання вразливостям[2. 3].

Шифрування та управління ключами

Шифрування даних. Забезпечення шифрування офлайн VM образів та резервних копій для захисту конфіденційності та цілісності даних. Для організацій, що використовують зовнішніх постачальників хмарних послуг, забезпечення шифрованих з'єднань та приватного каналу, окремого від звичайного Інтернет-

трафіку [2].

Контроль доступу

Доступ до фізичного середовища та гіпервізора.

Впровадження системи контролю доступу до фізичного середовища, де розміщена інфраструктура, а також до платформи управління гіпервізором та віртуальними машинами. Доступ повинні мати тільки адміністратори та авторизовані користувачі [3].

Налаштування ролей та привілеїв у системах управління віртуальними машинами, таких як VMware vSphere, для обмеження доступу до певних функцій і даних[2].

Використання багатофакторної аутентифікації для доступу до консолі управління гіпервізором для додаткового рівня захисту [2].

Загальні рекомендації щодо впровадження та використання методів моніторингу

Постійний аудит та перевірка політик безпеки

Регулярний перегляд та оновлення політик безпеки для забезпечення їх актуальності та ефективності.

Проведення аудитів для виявлення слабких місць та оптимізації налаштувань системи.

Навчання персоналу

Проведення регулярних тренінгів для адміністративного та технічного персоналу з метою підвищення їх компетенцій у галузі безпеки.

Навчання користувачів правилам безпеки та найкращим практикам роботи у віртуальному середовищі.

Використання автоматизованих інструментів.

Застосування автоматизованих засобів для виявлення та реагування на інциденти безпеки.

Використання систем автоматичного оновлення та патч-менеджменту для підтримки актуальності програмного забезпечення.

Інтеграція з існуючими системами управління.

Інтеграція засобів моніторингу безпеки з існуючими системами управління IT-інфраструктурою для централізованого контролю та управління.

Використання API та інших засобів інтеграції для забезпечення безперебійного обміну даними між різними системами.

Використання рішень для управління віртуальними машинами, таких як VMware vSphere, для ефективного управління всією віртуальною інфраструктурою, забезпечуючи належне розподілення ресурсів для віртуальних машин, а також автоматичну установку оновлень та патчів безпеки.

У цьому підрозділі було розглянуто важливі аспекти моніторингу безпеки віртуального середовища, а також надано конкретні рекомендації щодо застосування методів та засобів моніторингу для забезпечення високого рівня захисту інформації.

Перш за все, виявлено, що впровадження системи моніторингу та логування всього мережевого трафіку та операцій віртуальних машин, разом з регулярним аудитом цих логів, є ключовим елементом забезпечення безпеки віртуального середовища. Такий підхід дозволяє оперативно виявляти та реагувати на потенційні загрози та інциденти безпеки.

Далі, рекомендовано використання рішень для моніторингу, таких як системи виявлення вторгнень (IDS) та спеціалізовані інструменти для гіпервізорів, які допомагають виявляти та запобігати атакам на віртуальну інфраструктуру. Це доповнюється налаштуванням кореляційних правил у системах управління інформацією та подіями безпеки (SIEM), що сприяє автоматичному виявленню складних атак та аномальної поведінки.

Щодо шифрування та управління ключами, встановлено, що шифрування даних є ефективним засобом захисту конфіденційної інформації, особливо в офлайн режимі та під час передачі через ненадійні мережі. Крім того, важливим аспектом є ефективне управління ключами для забезпечення безпеки шифрування та запобігання несанкціонованому доступу до зашифрованих даних.

Також контроль доступу до фізичного середовища та гіпервізора є ще одним важливим аспектом безпеки віртуального середовища. Впровадження

систем контролю доступу та налаштування ролей та привілеїв у системах управління віртуальними машинами допомагають обмежити доступ до критичних ресурсів та функцій лише авторизованим користувачам.

Отже, враховуючи ці рекомендації, організації можуть забезпечити ефективний моніторинг та захист віртуального середовища, знижуючи ризики та забезпечуючи високий рівень безпеки своєї інформаційної інфраструктури.

ВИСНОВКИ

У даній дипломній роботі проведено комплексне дослідження проблеми моніторингу безпеки віртуального середовища на базі VMware App Defence. Основна мета роботи полягала у виявленні та аналізі актуальних загроз для віртуальних середовищ, оцінці ефективності існуючих рішень та розробці рекомендацій щодо вдосконалення моніторингу безпеки.

Вивчення проблеми моніторингу безпеки віртуального середовища показало, що зростання популярності віртуалізації супроводжується збільшенням кількості загроз, пов'язаних із безпекою віртуальних інфраструктур. Основні загрози включають шкідливе програмне забезпечення, атаки на гіпервізори та уразливості в конфігураціях віртуальних машин. За результатами аналізу виявлено, що значна частина інцидентів безпеки у віртуальних середовищах обумовлена людськими помилками та неправильними налаштуваннями.

У роботі було проведено аналіз різних підходів до моніторингу безпеки віртуального середовища. Встановлено, що ефективний моніторинг повинен включати постійний збір та аналіз логів, виявлення аномалій та автоматичне реагування на інциденти. Різні методи моніторингу, такі як шифрування, управління ключами, механізми контролю доступу, віртуальні довірчі платформи та віртуальні міжмережеві екрани, відіграють важливу роль у забезпеченні безпеки.

Проведено детальний аналіз існуючих рішень для моніторингу безпеки віртуальних середовищ. Було виявлено, що більшість рішень мають певні переваги та недоліки. Наприклад, деякі системи пропонують високу ефективність у виявленні загроз, але можуть бути складними у налаштуванні та використанні. Інші рішення, навпаки, відзначаються простотою використання, але мають обмежений функціонал.

У другому розділі роботи було розглянуто архітектуру та компоненти рішення VMware App Defence. Це рішення складається з декількох ключових компонентів, кожен з яких виконує специфічні функції для забезпечення безпеки

віртуальних середовищ. Описано їхні основні функції та призначення, що дозволяє краще зрозуміти, як це рішення забезпечує захист віртуальної інфраструктури.

Докладно розглянуто призначення та основні функції компонентів VMware App Defence. Зокрема, було вивчено, як кожен компонент сприяє загальній безпеці системи, які завдання виконує та які технології використовує. Це включає функції збору даних, аналізу загроз, автоматизованого реагування на інциденти та інші важливі аспекти.

Аналіз процесів функціонування рішення VMware App Defence показав, що воно здатне ефективно виявляти та реагувати на загрози у реальному часі. Описано основні процеси, включаючи збір і аналіз даних, виявлення аномалій, генерацію попереджень та автоматичне реагування на інциденти. Ці процеси забезпечують високий рівень безпеки віртуальних середовищ.

У третьому розділі розглянуто різні варіанти впровадження системи моніторингу безпеки на базі VMware App Defence. Обговорено можливі сценарії використання, враховуючи особливості конкретних організацій та їхні вимоги до безпеки. Надано рекомендації щодо вибору оптимального варіанту впровадження.

Описано детальний порядок налаштування та використання засобів моніторингу безпеки на базі VMware App Defence. Ці рекомендації охоплюють всі етапи від первинної інсталяції до щоденного використання та підтримки системи. Наведено приклади налаштувань та кращих практик для забезпечення максимальної ефективності моніторингу.

Надано рекомендації щодо застосування методів та засобів моніторингу безпеки віртуального середовища. Підкреслено важливість регулярного оновлення та адаптації стратегій моніторингу до нових загроз. Рекомендації включають використання передових технологій, інтеграцію різних засобів безпеки та автоматизацію процесів реагування на інциденти, що має призвести до покращення реакції на потенційні загрози.

ПЕРЕЛІК ПОСИЛАНЬ

1. State of Virtualization. URL: https://www.spiceworks.com/sw-marketing/reports/state-of-virtualization/ (дата звернення: 20.04.2024).
2. Virtualization Security Issues and Risks. URL: https://www.relianoid.com/blog/virtualization-security-issues-and-risks/ (дата звернення: 20.04.2024).
3. Virtualization Security Issues and Risks. URL: https://www.liquidweb.com/kb/virtualization-security-issues-and-risks/ (дата звернення: 20.04.2024).
4. Schmidt, K., Phillips, C., Chuvakin, A. (2006), Logging and Log Management.
5. Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K. (2014), Network Anomaly Detection: Methods, Systems and Tools.
6. AppDefense Overview Whitepaper. URL: https://web.archive.org/web/20191218171847/https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-appdefense-overview-whitepaper.pdf (дата звернення: 20.04.2024).
7. Cisco. Tetration Analytics. URL: https://www.cisco.com/c/en_sg/products/data-center-analytics/tetration-analytics/index.html (дата звернення: 20.04.2024).
8. BlueVoyant. Splunk SIEM with Splunk Enterprise Cloud and Splunk ES. URL: https://www.bluevoyant.com/knowledge-center/splunk-siem-with-splunk-enterprise-cloud-and-splunk-es (дата звернення: 20.04.2024).
9. Elastic. What is SIEM? URL: https://www.elastic.co/what-is/siem (дата звернення: 20.04.2024).
10. Seget, V. (n.d.). What is VMware AppDefense? URL: https://4sysops.com/archives/what-is-vmware-appdefense/ (дата звернення: 20.04.2024).

11. Holmes, W. (2017), Ensuring Good AppDefense. URL: https://blogs.vmware.com/networkvirtualization/2017/09/ensuring-good-appdefense.html/ (дата звернення: 20.04.2024).