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 застосування системи моніторингу Zabbix на кінцевих точках»

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

_____ Олександр ЛОМОВАЦЬКИЙ
(підпис)

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

Керівник д. ф., доцент МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ломовацькому Олександру Вікторовичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо застосування системи моніторингу Zabbix на кінцевих точках»

керівник кваліфікаційної роботи Марченко Віталій, д. ф., доцент
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Zabbix;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми моніторингу кінцевих точок організації.
2. Аналіз методів та засобів моніторингу кінцевих точок організації на базі Zabbix.
3. Розроблення рекомендацій щодо застосування системи моніторингу Zabbix на кінцевих точках організації.
4. Рекомендації щодо застосування методів та програмного забезпечення для аналізу під час використання технології моніторингу.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок організації.	15.04.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз методів та засобів захисту кінцевих точок організації на базі Zabbix.		
4.	Практична реалізація варіанту моніторингу кінцевих точок організації на базі Zabbix.		
5.	Розроблення рекомендацій щодо застосування методів та засобів моніторингу кінцевих точок організації.		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Элександр Ломовацький
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ЛОМОВАЦЬКОГО Олександра
на тему: «Дослідження шляхів та розробка рекомендацій щодо застосування системи моніторингу Zabbix на кінцевих точках»

Актуальність: Забезпечення безпеки кінцевих точок організацій є ключовим для запобігання несанкціонованому доступу, витоку та втраті даних. Системи моніторингу забезпечують безперервний моніторинг кінцевих точок, що дозволяє організаціям мати повну видимість стану безпеки та оперативно реагувати на нові загрози.

Кібератаки, які порушують роботу кінцевих пристроїв організації або ставлять їх під загрозу, можуть призвести до простоїв, що впливає на продуктивність і безперервність бізнесу. Тому тема кваліфікованої роботи актуальна і своєчасна.

Позитивні сторони:

1. На основі аналізу в статті визначається зміст проблеми, моніторингу кінцевих точки організації, визначаються мета і призначення цього типу програмного забезпечення, а також його компоненти.
2. Досліджено методи та засоби моніторингу кінцевих точок організації на базі Zabbix.
3. Запропоновано варіант моніторингу кінцевих точок на базі Zabbix та рекомендації щодо їх застосування.
4. Текст представлений дуже грамотно і зв'язно. Був зроблений чіткий і змістовний висновок. Графічний матеріал розроблений з високою якістю. Перелік науково-технічної літератури свідчить про вміння використовувати матеріали по темі кваліфікованої роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз моніторингу кінцевих точок на прикладі конкретної організації.
2. Запропонований порядок застосування методів та засобів моніторингу кінцевих точок бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“відмінно”**, а здобувач(ка) **ЛОМОВАЦЬКИЙ Олександр** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент:

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

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач ЛОМОВАЦЬКИЙ Олександр до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо застосування системи моніторингу Zabbix на кінцевих точках».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ЛОМОВАЦЬКИЙ Олександр*** обрав тему роботи, метою якої було вивчити шляхи та засоби захисту кінцевих точок організації та розробити рекомендації щодо їх реалізації. Список використовуваних ресурсів демонструє здатність заявника розуміти наукові проблеми та застосовувати їх у дослідженнях Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ЛОМОВАЦЬКИЙ Олександр*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ЛОМОВАЦЬКОГО Олександра*** на оцінку **"відмінно"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ЛОМОВАЦЬКИЙ Олександр** допускається до захисту
даної кваліфікаційної роботи в Екзаменаційній комісії.
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 42 сторінки, 11 рисунків, 10 джерел.

Об'єкт дослідження – об'єктом дослідження є технологія моніторингу Zabbix.

Предмет дослідження – методи та засоби щодо моніторингу кінцевих точок організації за допомогою технології Zabbix.

Мета роботи розробити варіант системи на базі рішення Zabbix та рекомендації щодо застосування методів та засобів моніторингу кінцевих точок організації.

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

Системи моніторингу – це програмні або апаратні засоби, які постійно стежать за станом і роботою різних компонентів IT-інфраструктури. Вони збирають і аналізують дані про продуктивність, безпеку та надійність систем, допомагаючи виявляти та усувати проблеми до того, як вони вплинуть на роботу організації. Системи моніторингу також забезпечують звітування та оповіщення про критичні події і зміни, що дозволяє підтримувати стабільну і безпечну роботу всіх IT-компонентів..

В роботі досліджено проблему моніторингу кінцевих точок організації, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів моніторингу кінцевих точок організації. Досліджено методи та засоби моніторингу кінцевих точок організації на базі Zabbix. Визначено призначення, основні функції та склад рішення Zabbix.

На основі досліджень проведених в роботі запропоновано варіант системи на базі Zabbix. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів захисту кінцевих точок організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, МОНІТОРИНГ, КІНЦЕВІ ТОЧКИ, МОНІТОРИНГ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ МОНІТОРИНГУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CPR - Check Point Research

DoS - denial-of-service

DDoS - distributed denial-of-service attack

ВСТУП

Актуальність дослідження. Важливість вивчення способів впровадження систем моніторингу Zabbix в кінцевих точках і розробки рекомендацій була дуже високою з урахуванням сучасних вимог до безпеки та ефективності IT-інфраструктури. Зростаючі кіберзагрози та складні мережеві середовища вимагають, щоб організації мали надійні інструменти для постійного моніторингу та управління кінцевими точками, такими як сервери, комп'ютери, ноутбуки та мобільні пристрої.

Система Zabbix-це потужне рішення для моніторингу, яке може відстежувати стан та продуктивність різних IT-компонентів у режимі реального часу. Вивчаючи потенціал додатків на кінцевих точках, організації можуть своєчасно виявляти та реагувати на потенційні проблеми, надаючи засоби для підвищення загальної безпеки, зменшення ризику порушення даних та зменшення простоїв системи.

Розробка рекомендацій щодо впровадження та оптимізації Zabbix сприятиме підвищенню ефективності IT-операцій, більш ефективному використанню ресурсів організаціями та підвищенню надійності інформаційних систем. Ця робота також зробить значний внесок у розробку технологій моніторингу, адаптованих до конкретних потреб різних секторів та типів організацій..

Рішення для моніторингу є невід'ємною частиною сучасної IT-інфраструктури і постійно контролюють стан і продуктивність різних компонентів системи. Їх основна мета-виявити, проаналізувати та запобігти потенційним проблемам, які можуть вплинути на стабільність та безпеку інформаційних технологій організації.

Рішення для моніторингу забезпечують всебічний збір даних про можливості серверів, комп'ютерів, мережевих пристроїв та інших кінцевих точок. Ці дані включають показники продуктивності, використання ресурсів, стан безпеки та виявлення аномалій та потенційних загроз. На основі зібраної інформації система моніторингу може створювати звіти, відправляти повідомлення при виявленні відхилень від нормальної роботи і автоматично вживати заходів для усунення

виявлених проблем.

У практичних додатках рішення для моніторингу використовуються для забезпечення стабільної роботи IT-інфраструктури, зниження ризику простоїв і втрати даних, а також для забезпечення високого рівня кібербезпеки. Це дозволяє адміністраторам та IT-фахівцям швидко реагувати на інциденти, оптимізувати використання ресурсів, планувати оновлення та розширення системи, а також забезпечувати відповідність стандартам і нормативним вимогам.

Загалом, рішення для моніторингу необхідні для ефективного управління IT-ресурсами, що сприяє підвищенню ефективності, безпеки та надійності інформаційних систем, які стикаються зі зростаючими вимогами та загрозами в сучасному цифровому середовищі.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів моніторингу кінцевих точок організації на базі Zabbix.

Об'єкт дослідження – Об'єктом дослідження є технологія моніторингу.

Предмет дослідження – методи та засоби щодо аналізу дій зловмисника за допомогою технології Zabbix.

Мета роботи розробити варіант системи на базі рішення Zabbix та рекомендації щодо застосування методів та засобів моніторингу кінцевих точок організації.

Наукові завдання:

дослідити сутність проблеми моніторингу кінцевих точок організації;

проаналізувати методи та засоби моніторингу кінцевих точок організації на базі Zabbix;

запропонувати варіант системи захисту кінцевих точок організації на базі Zabbix;

розробити рекомендацій щодо застосування методів та засобів моніторингу кінцевих точок організації.

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 кінцевих точок організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ДІЙ ЗЛОВМИСНИКА ПІД ЧАС КІБЕРАТАКИ

1.1. Поняття кібератака

Кібератака - це будь-яка навмисна спроба викрасти, розкрити, змінити, вивести з ладу або знищити дані, програми чи інші активи шляхом несанкціонованого доступу до мережі, комп'ютерної системи або цифрового пристрою.

Суб'єкти загрози починають кібератаки з різних причин, від дрібних крадіжок до військових дій. Вони використовують різні тактики, такі як атаки шкідливих програм, шахрайство з використанням соціальної інженерії та викрадення паролів, щоб отримати несанкціонований доступ до своїх цільових систем.

Кібератаки можуть порушити, пошкодити і навіть знищити бізнес. Середня вартість витоку даних становить 4,35 мільйона доларів США. Ця ціна включає в себе витрати на виявлення та реагування на порушення, простої та недоотриманий дохід, а також довгострокову репутаційну шкоду для бізнесу та його бренду.

Але деякі кібератаки можуть бути значно дорожчими за інші. Атаки з використанням програм-вимагачів призвели до виплати викупу в розмірі 40 мільйонів доларів США. Шахрайство з компрометацією ділової електронної пошти (BEC) викрало у жертв до 47 мільйонів доларів США за одну атаку. Кібератаки, які компрометують особисту інформацію клієнтів, можуть призвести до втрати довіри клієнтів, штрафів з боку регуляторних органів і навіть судових позовів. За однією з оцінок, до 2025 року кіберзлочинність коштуватиме світовій економіці 10,5 трильйонів доларів США [1].

Чому відбуваються кібератаки?

Мотиви кібератак можуть бути різними, але можна виділити три основні категорії:

- Кримінальні
- Політичні
- Особисті

Зловмисники з кримінальними мотивами прагнуть отримати фінансову вигоду через крадіжку грошей, даних або порушення роботи бізнесу. Кіберзлочинці можуть зламати банківський рахунок, щоб безпосередньо викрасти гроші, або використовувати соціальну інженерію, щоб обманом змусити людей надсилати їм гроші. Хакери можуть викрасти дані та використати їх для крадіжки персональних даних, продати їх у темній мережі або утримувати з метою отримання викупу.

Вимагання - ще одна тактика, яка використовується. Хакери можуть використовувати програми-вимагачі, DDoS-атаки або інші тактики, щоб утримувати дані або пристрої в заручниках, поки компанія не заплатить. Згідно з Індексом розвідки загроз X-Force, 27% кібератак мають на меті вимагання грошей у своїх жертв [2].

Добавлено примечание ([MS1]): Не так посилання. Крапка вкінці так як нижче

Особисто вмотивовані зловмисники, такі як незадоволені нинішні або колишні співробітники, в першу чергу прагнуть відплати за якусь уявну дрібницю. Вони можуть забрати гроші, викрасти конфіденційні дані або вивести з ладу системи компанії.

Політично вмотивовані зловмисники часто асоціюються з кібервійною, кібертероризмом або "хактивізмом". У кібервійнах національні держави часто націлені на урядові установи або об'єкти критичної інфраструктури своїх супротивників. Наприклад, з початком російсько-української війни обидві країни зазнали низки кібератак на життєво важливі установи (посилання знаходиться за межами ibm.com). Хакери-активісти, яких називають "хактивістами", можуть не завдавати значної шкоди своїм цілям. Замість цього вони зазвичай прагнуть привернути увагу до своїх дій, роблячи свої атаки відомими громадськості [3].

Менш поширеними мотивами кібератак є корпоративне шпигунство, коли хакери викрадають інтелектуальну власність, щоб отримати несправедливу перевагу над конкурентами, та хакери-месники, які використовують вразливості системи, щоб попередити про них інших. Деякі хакери займаються зломом заради спорту, насолоджуючись інтелектуальним викликом.

Злочинні організації, державні суб'єкти та приватні особи можуть розпочати кібератаки. Один із способів класифікувати суб'єктів загроз - це розділити їх на

зовнішні та внутрішні загрози.

Зовнішні загрози не мають дозволу на використання мережі або пристрою, але все одно вдираються в неї. До зовнішніх суб'єктів кіберзагроз належать: організовані злочинні угруповання, професійні хакери, державні структури, хакери-аматори та хактивісти.

Внутрішні загрози - це користувачі, які мають санкціонований і законний доступ до активів компанії і навмисно або випадково зловживають своїми привілеями. До цієї категорії належать: працівники, бізнес-партнери, клієнти, підрядники та постачальники, які мають доступ до системи.

Хоча недбалі користувачі можуть наражати свої компанії на ризик, кібератака відбувається лише тоді, коли користувач навмисно використовує свої привілеї для здійснення зловмисних дій. Працівник, який необережно зберігає конфіденційну інформацію на незахищеному диску, не вчиняє кібератаки, але незадоволений працівник, який свідомо робить копії конфіденційних даних з метою особистої вигоди, вчиняє кібератаку.

Зловмисники зазвичай вдираються в комп'ютерні мережі, тому що вони переслідують певну мету. Найпоширеніші цілі включають: гроші, фінансові дані підприємств, списки клієнтів, дані клієнтів, включаючи особисту інформацію, або інші конфіденційні персональні дані, адреси електронної пошти та облікові дані для входу в систему, інтелектуальна власність.

У деяких випадках кібератаки взагалі не хочуть нічого красти. Вони просто хочуть вивести з ладу інформаційні системи або IT-інфраструктуру, щоб завдати шкоди бізнесу, державним установам чи іншим цілям.

1.2. Різновиди кібератак та статистика їх застосування

Кіберзлочинці використовують багато складних інструментів і методів для здійснення кібератак на корпоративні IT-системи, персональні комп'ютери та інші цілі. Деякі з найпоширеніших типів кібератак включають:

- Шкідливе програмне забезпечення - це шкідливе програмне забезпечення,

яке може вивести заражені системи з ладу. Шкідливе програмне забезпечення може знищити дані, викрасти інформацію або навіть стерти файли, важливі для роботи операційної системи. Шкідливе програмне забезпечення буває різних форм, зокрема:

- Троянські програми маскуються під корисні програми або ховаються в легальному програмному забезпеченні, щоб обманом змусити користувачів встановити їх. Троянський троян для віддаленого доступу створює на пристрої жертви секретний чорний хід, а троян-"крапельниця" встановлює додаткове шкідливе ПЗ після того, як закріпиться на ньому.
- Програми-вимагачі - це складні шкідливі програми, які використовують стійке шифрування, щоб утримувати дані або системи в заручниках. Потім кіберзлочинці вимагають оплату в обмін на звільнення системи та відновлення її функціональності. Згідно з Індексом розвідки загроз X-Force компанії IBM, програми-вимагачі є другим найпоширенішим типом кібератак, на який припадає 17% атак [2].
- Програми залякування використовують фальшиві повідомлення, щоб налякати жертву і змусити її завантажити шкідливе програмне забезпечення або передати шахраєві конфіденційну інформацію.
- Шпигунські програми - це тип шкідливих програм, які таємно збирають конфіденційну інформацію, наприклад, імена користувачів, паролі та номери кредитних карток. Потім воно надсилає цю інформацію назад хакеру.
- Руткіти - це пакети шкідливих програм, які дозволяють хакерам отримати доступ на рівні адміністратора до операційної системи комп'ютера або інших активів.
- Черв'яки - це самовідтворюваний шкідливий код, який може автоматично поширюватися між програмами та пристроями.
- Соціальна інженерія - атаки соціальної інженерії маніпулюють людьми, змушуючи їх робити те, чого вони не повинні робити, наприклад, ділитися інформацією, якою вони не повинні ділитися, завантажувати програмне забезпечення, яке вони не повинні завантажувати, або надсилати гроші злочинцям.

- Фішинг - одна з найпоширеніших атак соціальної інженерії. Згідно зі звітом Cost of a Data Breach, це друга найпоширеніша причина витоку даних [4]. Найпростіші фішингові атаки використовують підроблені електронні листи або текстові повідомлення для викрадення облікових даних користувачів, витоку конфіденційних даних або розповсюдження шкідливого програмного забезпечення. Фішингові повідомлення часто виглядають так, ніби вони надходять з легітимного джерела. Зазвичай вони спонукають жертву натиснути на гіперпосилання, яке веде на шкідливий веб-сайт, або відкрити вкладення в електронному листі, яке виявляється шкідливим програмним забезпеченням.
- Кіберзлочинці також розробили більш складні методи фішингу. Списовий фішинг - це вузькоспрямована атака, яка має на меті маніпулювання конкретною особою, часто з використанням деталей з публічних профілів жертви в соціальних мережах, щоб зробити обман більш переконливим. Китовий фішинг - це різновид фішингу зі списом, який спеціально націлений на високопосадовців компаній. Під час компрометації ділової електронної пошти кіберзлочинці видають себе за керівників, постачальників або інших ділових партнерів, щоб обманом змусити жертву переказати гроші або поділитися конфіденційними даними.
- Атаки на відмову в обслуговуванні (DoS) та розподілені атаки на відмову в обслуговуванні (DDoS) переповнюють ресурси системи шахрайським трафіком. Цей трафік перевантажує систему, перешкоджаючи відповідям на законні запити та знижуючи продуктивність системи. Атака на відмову в обслуговуванні може бути як самоціллю, так і підготовкою до іншої атаки.

Різниця між DoS-атаками та DDoS-атаками полягає в тому, що DoS-атаки використовують одне джерело для генерації шахрайського трафіку, тоді як DDoS-атаки використовують декілька джерел. DDoS-атаки часто здійснюються за допомогою бот-мережі - мережі підключених до Інтернету, заражених шкідливим програмним забезпеченням пристроїв, що перебувають під контролем хакера. Ботнети можуть включати ноутбуки, смартфони та пристрої Інтернету речей. Жертви часто не знають, коли ботнет захопив їхні пристрої.

- Компрометація облікового запису - це будь-яка атака, під час якої хакери

викрадають обліковий запис законного користувача для зловмисної діяльності. Кіберзлочинці можуть зламати обліковий запис користувача різними способами. Вони можуть викрасти облікові дані за допомогою фішингових атак або купити викрадені бази даних паролів з темної мережі. Вони можуть використовувати інструменти для злому паролів, такі як Hashcat і John the Ripper, щоб зламати шифрування паролів або влаштувати атаку грубої сили, в якій вони запускають автоматизовані скрипти або ботів, щоб генерувати і тестувати потенційні паролі до тих пір, поки один з них не спрацює.

- Атака «людина посередині» - під час атаки "людина посередині", яку також називають "атакою підслуховування", хакер таємно перехоплює комунікацію між двома людьми або між користувачем і сервером. Атаки «людина посередині» зазвичай здійснюються через незахищені публічні мережі Wi-Fi, де зловмисникам відносно легко підглядати за трафіком.

Check Point Research (CPR) опублікувала нові дані про тенденції кібератак у 2022 році. Дані сегментовані за глобальним обсягом, галуззю та географією. У 2022 році кількість глобальних кібератак зросла на 38% порівняно з 2021 роком. Таке зростання кількості кібератак зумовлене діями менших і спритніших хакерських угруповань, які зосередилися на використанні інструментів спільної роботи, що застосовуються в умовах роботи з дому, та націлилися на навчальні заклади, які перейшли на електронне навчання після COVID-19. Таке зростання глобальних кібератак також зумовлене інтересом хакерів до організацій охорони здоров'я, на які припадає найбільше зростання кібератак у 2022 році порівняно з усіма іншими галузями. CPR попереджає, що зрілість технологій штучного інтелекту, таких як CHATGPT, може прискорити кількість кібератак у 2023 році.

Компанія Check Point Research (CPR) опублікувала нові дані про минулорічні тенденції кібератак. Дані сегментовані за глобальним обсягом, галузями, континентами та країнами.

Основні статистичні дані:

Глобальний обсяг кібератак досяг історичного максимуму в 4 кварталі - в середньому 1168 щотижневих атак на одну організацію

Топ-3 найбільш атакованих галузей у 2022 році - освіта/дослідження, уряд та охорона здоров'я

Географія Африки зазнала найбільшої кількості атак - 1875 щотижневих атак на організацію, за нею слідує ATP з 1691 щотижневою атакою на організацію

Північна Америка (+52%), Латинська Америка (+29%) та Європа (+26%) продемонстрували найбільше зростання кількості кібератак у 2022 році порівняно з 2021 роком

У США загальна (рисунок 1.1) кількість кібератак у 2022 році зросла на 57%, у Великобританії - на 77%, а в Сінгапурі - на 26%.

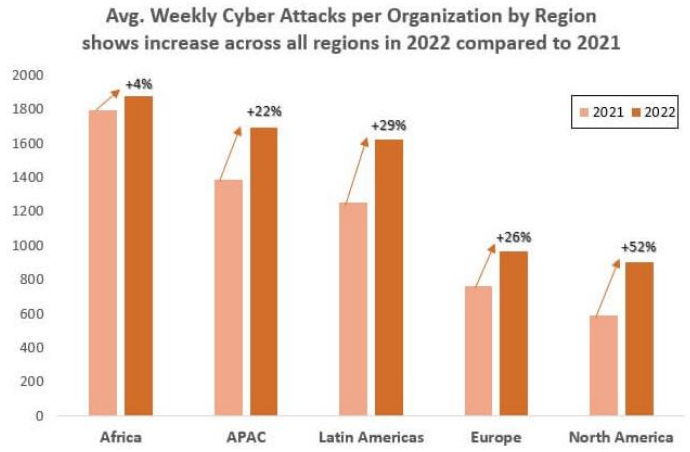

Рис. 1.1 Приріст кількості кібератак в 2022 році до 2021 року

Кількість кібератак зростає в усьому світі: у 2022 році на 38% більше кібератак на корпоративні мережі щотижня порівняно з 2021 роком. Відбувається одразу кілька тенденцій кіберзагроз.

По-перше, екосистема програм-вимагачів продовжує розвиватися і розростатися за рахунок менших і спритніших злочинних груп, які об'єднуються для того, щоб уникати правоохоронних органів. По-друге, хакери розширюють свої цілі, націлюючись за допомогою фішингових експлойтів на інструменти бізнес-співпраці, такі як Slack, Teams, OneDrive і Google Drive. Вони є багатим джерелом

конфіденційних даних, враховуючи, що більшість працівників організацій продовжують працювати віддалено.

По-третє, академічні установи стали популярним середовищем для кіберзлочинців після швидкої оцифровки, яку вони здійснили у відповідь на пандемію COVID-19. Фактично, сектор освіти/досліджень став галуззю номер один у світі, яка зазнала найбільше атак у 2022 році - на 43% більше, ніж у 2021 році, із середнім показником 2 314 атак на одну організацію щотижня. Багато навчальних закладів виявилися погано підготовленими до несподіваного переходу на онлайн-навчання, що створило широкі можливості для хакерів проникати в мережі будь-якими способами. Школи та університети також стикаються з унікальною проблемою роботи з дітьми та молодими людьми, багато з яких користуються власними пристроями, працюють у загальних місцях і часто підключаються до громадського Wi-Fi, не замислюючись про наслідки для безпеки.

Озираючись на кібератаки (рисунок 1.2) на сектор охорони здоров'я у 2022 році, медичні організації в США зазнали в середньому 1410 щотижневих кібератак на організацію, що на 86% більше, ніж у 2021 році, при цьому сектор охорони здоров'я посідає друге місце серед усіх секторів за кількістю кібератак у США.

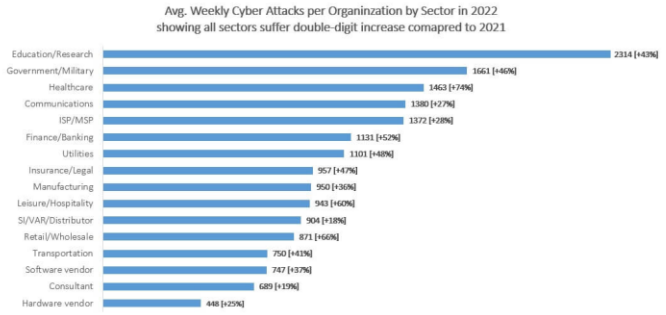

Рис. 1.2 Порівняння середньо тижневої кількості кібератак 2022 до 2021 року

Хакери полюбляють атакувати лікарні, оскільки вважають, що їм не вистачає ресурсів для забезпечення кібербезпеки, а невеликі лікарні є особливо вразливими, оскільки вони не мають достатнього фінансування та персоналу, щоб впоратися зі

складними кібератаками.

Сектор охорони здоров'я є настільки прибутковим для хакерів, що вони прагнуть отримати інформацію про медичне страхування, номери медичних карток і, іноді, навіть номери соціального страхування за допомогою прямих погроз з боку банд, що вимагають викуп, які вимагають оплату під загрозою оприлюднення медичних карток пацієнтів. Банди вимагачів також вважають, що увага, яку вони отримують від нападу на лікарню, є привабливим плюсом до їхньої репутації.

На жаль, ми очікуємо, що активність кібератак буде тільки зростати. Завдяки загальнодоступним технологіям штучного інтелекту, таким як ChatGPT, хакери можуть генерувати шкідливий код та електронні листи швидше та автоматизованіше

Щоб захистити себе, необхідно в першу чергу думати про профілактику, а не про виявлення. Існує кілька найкращих практик і заходів, які організація може вжити, щоб мінімізувати свій ризик наступної атаки або зламу, наприклад, навчання з кібербезпеки, оновлення патчів і впровадження технології захисту від програм-вимагачів" [5].

1.3 Побудова моделі дій зловмисника

Перш за все, необхідно визначити поняття інформації, даних і "моделі порушника". Інформація - це відомості про об'єкти та явища довкілля, їхні параметри, властивості та стани, які зменшують ступінь невизначеності, неповноти знань про них. Теоретична інформатика розглядає інформацію як концептуально пов'язані відомості, дані, поняття, що змінюють уявлення про будь-яке явище або об'єкт навколишнього світу. Поряд з інформацією в інформатиці часто використовують поняття даних. Дані можна розглядати як атрибути або записані спостереження, які з якихось причин не використовуються, а тільки зберігаються. У тому випадку, коли з'являється можливість використати ці дані для визначення невизначеності чого-небудь, дані перетворюються на інформацію [6]. Тобто інформація - це дані, які використовуються.

Модель порушника - це опис можливих дій порушника, який ґрунтується на аналізі типу порушника, його рівня повноважень, знань, теоретичних і практичних можливостей. Порушників зазвичай ділять на зовнішніх і внутрішніх. До внутрішніх порушників належать співробітники, користувачі інформаційної системи, які можуть завдати шкоди інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі та приміщення (електрики, сантехніки, прибиральники тощо); персонал, який обслуговує технічні засоби (інженери, техніки). Зовнішні порушники - це сторонні особи, які перебувають за межами контрольованої території організації або не мають повноважень на використання даної комп'ютерної системи. Це означає, що вони не мають облікового запису в системі і, згідно з політикою безпеки системи, взагалі не можуть працювати в ній. Прикладами зовнішніх порушників є: відвідувачі, які можуть заподіяти шкоду навмисно або через незнання наявних обмежень; досвідчені хакери; особи, найняті конкурентами для одержання необхідної інформації; порушники перепусток.

Під час розроблення моделі порушника необхідно визначити, що і якою мірою має відображати отримана модель. Для цього необхідно визначити необхідний ступінь деталізації моделі порушника.

Можна запропонувати такі ступені деталізації:

- змістовна модель порушників - відображає причини і мотивацію дій порушників, цілі, які вони переслідують, і загальний характер дій у процесі підготовки та реалізації порушення інформаційної безпеки. Побудувавши змістовну модель, адміністратори безпеки можуть визначити цілі порушника, його рівень знань, кваліфікацію, місцезнаходження тощо.
- сценарії впливу порушника - визначають класифіковані типи порушень із зазначенням алгоритмів і етапів, а також способів дій на кожному етапі. Розробивши сценарії впливу, адміністратори безпеки отримають можливу послідовність дій зловмисника з нанесення шкоди інформаційним ресурсам.
- Математична модель впливу порушника - це формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушника, кількісних

значень, що параметрично характеризують результати дій, та функціональних (аналітичних, числових чи алгоритмічних) залежностей, що описують процеси взаємодії порушників з елементами об'єкта та системи безпеки. Цей тип моделі слід використовувати для кількісних оцінок уразливості об'єкта та ефективності системи безпеки.

Для того щоб модель порушника найточніше і найдокладніше характеризувала порушників, алгоритм їхніх дій і давала кількісні оцінки вразливості об'єкта та ефективності захисту, рекомендується розробляти комплексну модель, що враховує всі ступені деталізації.

Під час побудови моделі порушника насамперед необхідно проаналізувати всіх користувачів системи, розподілити їх за категоріями і виділити найбільш критичних. Користувачів таких категорій прийматимуть як можливих внутрішніх порушників системи. Далі необхідно визначити, які категорії відвідувачів можуть бути зовнішніми порушниками.

Усіх можливих порушників необхідно класифікувати за різними ознаками, щоб надалі скласти модель порушника. Нижче перелічено можливі типи класифікацій:

- Класифікація порушників інформаційної безпеки за метою проникнення. Класифікація за метою проникнення проводиться для визначення мотивів порушника. Залежно від мети, дії порушника можуть бути спрямовані як на інформаційні, так і на матеріальні носії. Знаючи мету порушника, адміністратори безпеки орієнтуватимуться, на захист яких ресурсів слід звернути увагу насамперед.
- Класифікація порушників інформаційної безпеки за рівнем знань про автоматизовані системи. Кожен порушник має певний рівень кваліфікації та обізнаності щодо організації функціонування лабораторії зовнішніх і внутрішніх мереж інформаційно-обчислювального комплексу. Залежно від рівня знань, якими володіє порушник, може бути завдано певної шкоди інформаційним ресурсам організації. Класифікація враховує знання можливого порушника і його практичні навички роботи з комп'ютерними системами та інформаційними технологіями.

- Класифікація порушника за місцем розташування. Цю класифікацію проводять для визначення місця розташування порушника щодо організації під час спроби несанкціонованого доступу до інформаційного ресурсу.
- Класифікація порушників за використовуваними ними методами і технологіями. Порушник може отримати конфіденційну інформацію та інформацію обмеженого доступу, використовуючи різні методи і засоби. Порушення може бути скоєно як з використанням певних засобів отримання інформації, так і без них. Методи можуть бути різними: дозволеними або забороненими. Під дозволеними розуміється отримання інформації без порушення прав власності. Прикладом може слугувати використання методів соціальної інженерії [7].
- Класифікація порушників за рівнем можливостей, що надаються їм автоматизованою системою і комп'ютерними засобами. Внутрішні порушники можуть бути класифіковані за наданим рівнем повноважень у системі. Адже чим більше повноважень, тим більше можливостей отримати доступ до інформації з обмеженим доступом [8].
- Класифікація порушників за мотивами порушень. Зловмисники можуть порушувати інформаційну безпеку з різних причин. Порушення можна розділити на дві групи - навмисні та ненавмисні. Особи, які ненавмисно завдають шкоди інформаційним ресурсам шляхом порушення конфіденційності, цілісності або доступності інформації, не складають план дій, не мають мети та спеціальних методів і засобів реалізації планованого порушення. Ненавмисні порушення найчастіше реалізуються внаслідок недостатньої кваліфікації, неуважності персоналу. Порушники, які завдають шкоди інформаційним ресурсам навмисне, мають певну мету, готують план реалізації атаки на інформаційний ресурс. Умисні порушення інформаційної безпеки здійснюються з метою завдання шкоди організації (матеріальної або моральної), для власного збагачення за рахунок отриманої інформації, а також для нейтралізації конкурентів.

Практично кожна інформаційна система містить таку інформацію, розкриття якої неуповноваженим особам може завдати шкоди її власнику або особі, до якої

ця інформація належить. Питання інформаційної безпеки стає особливо актуальним на підприємствах, в організаціях, що займаються обробкою інформації з обмеженим доступом. Одним з етапів побудови комплексної системи захисту інформації є розробка моделі зловмисника. Що точніше буде визначено образ, алгоритм дій ймовірного порушника, то простіше адміністраторам безпеки буде розробити комплекс заходів для запобігання успішних атак. Вибір класифікацій порушників відіграє важливу роль у розробленні моделі порушника. Отже, для найточнішого визначення можливих порушників, втрати від яких будуть максимальними, необхідно класифікувати всі типи суб'єктів, потенційно здатних взаємодіяти з інформаційними ресурсами, за всіма можливими для системи показниками, що значно спростить процедуру організації ефективної системи інформаційної безпеки.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД КІБЕРАТАК ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ МОНІТОРИНГУ

2.1. Технологія моніторингу та її різновиди

Моніторинг - це ключова частина управління та підтримки інформаційних систем і технологій. Існує кілька видів моніторингу, кожен з яких має свої особливості та значення для конкретних цілей і потреб.

Якщо ми відкриємо статтю моніторинг у Вікіпедії, то прочитаємо, що моніторинг або спостереження - це система безперервного спостережень за явищами та процесами, що відбуваються в навколишньому середовищі, суспільстві, результати яких використовуються для обґрунтування управлінських рішень щодо забезпечення безпеки людей та об'єктів/суб'єктів (наприклад, економіки). У широкому сенсі моніторинг - це процес безперервного або регулярного (періодичного) збирання інформації про стан тих чи інших параметрів об'єкта або суб'єкта спостереження (моніторингу). Метою моніторингу може бути як накопичення інформації для її подальшого аналізу та прийняття управлінських рішень, так і постійне відстеження стану об'єкта спостереження без збереження попередньої інформації про об'єкт з метою своєчасного реагування у разі певних кількісних або якісних змін об'єкта. Моніторинг може бути автоматизованим: у разі автоматичного моніторингу здійснюють приймання та оброблення інформації про стан об'єкта/суб'єкта та зовнішнього середовища стану об'єкта/суб'єкта та зовнішнього середовища для виявлення подій, що визначають управлінські дії.

Таблиця 2.1

Види моніторингу

Вид моніторингу	Ціль моніторингу
Системний моніторинг	Оцінка продуктивності, надійності та ефективності системи, виявлення аномалій та проблем для швидкого реагування.
Мережевий моніторинг	Забезпечення безпеки, виявлення і вирішення проблем у мережевій інфраструктурі.
Додатковий моніторинг	Оцінка роботи додатків, виявлення та усунення проблем, покращення відповідності до вимог користувачів.
Безпековий моніторинг	Забезпечення безпеки, виявлення та запобігання кібератак, захист від несанкціонованого доступу.
Журналювання	Забезпечення можливості аналізу та виявлення незвичайної активності, вирішення проблем та безпеки

Різниця між цими видами моніторингу полягає в тому, що кожен із них спрямований на відстеження та аналіз певних аспектів системи та її екосистеми. Системний моніторинг фокусується на апаратній і програмній частині системи, мережевий моніторинг - на мережевій інфраструктурі, доповнення - на мережевій інфраструктурі, доповнення до програмного забезпечення - на програмних доповненнях, безпека - на виявленні та захисті від загроз, а протоколювання - на записі та зберіганні подій для подальшого аналізу. аналізу. Ці види моніторингу однаково важливі для забезпечення ефективності, надійності та безпеки систем і доповнень.

Системний моніторинг - це комплексний процес автоматичного або ручного спостереження, аналізу та оцінки параметрів і функцій конкретної системи, або групи систем. Цей процес організовується для отримання повної та об'єктивної інформації про стан системи в реальному часі або на певних етапах її функціонування. У процесі оцінки стану системи в реальному часі або на певних етапах її функціонування. Основна мета - своєчасне виявлення та реагування на проблеми або відхилення в роботі системи для забезпечення її стабільності та ефективності. Системний моніторинг - ключовий елемент управління та

забезпечення ефективності інформаційних технологій у сучасному бізнес-середовищі.

Ми пам'ятаємо, що цей процес містить у собі систематичний нагляд за функціональністю, продуктивністю та надійністю IT-систем, що дає змогу забезпечити безперебійну роботу інфраструктури й уникнути багатьох проблем у бізнесі за відносно невеликих витрат. Зупинимося на принципах збирання даних під час системного моніторингу, які охоплюють такі аспекти:

Таблиця 2.2

Аспекти моніторингу

изначення ключових метрик	сновні параметри та метрики для моніторингу ожуть включати такі показники, як родуктивність, швидкість реакції, завантаження истеми та обсяги даних.
ибір засобів моніторингу	беріть інструменти та програмне забезпечення ля збору, аналізу та візуалізації даних. Це можуть ути як спеціалізовані системи моніторингу, так і пасноруч розроблені рішення.
алаштування моніторингу	Конфігуруйте інструменти моніторингу для бору даних за обраними метриками та араметрами. Встановіть правила та порогові начення для виявлення аномалій.
бір та агрегація даних	истематично збирайте дані з обраного спектру етрик, що можуть включати інформацію про есурси системи, вхідні та вихідні дані, а також ідгуки користувачів.
наліз та інтерпретація даних	роводьте аналіз зібраних даних для виявлення номалій, прогнозування проблем і визначення ожливих шляхів вирішення. Порівнюйте езультати з ключовими показниками ективності та пороговими значеннями.
ізуалізація результатів	икористовуйте графіки, діаграми та інші засоби ізуалізації для наочного представлення езультатів моніторингу. Це полегшить розуміння тану системи та сприятиме прийняттю бґрунтованих рішень.
вітність та документація	едіть детальну документацію процесу оніторингу, результатів аналізу та прийнятих

	ішень. Це стане важливим джерелом інформації ля подальших удосконалень та оптимізацій.
втоматизація та оптимізація	озгляньте можливість автоматизації процесу оніторингу для підвищення ефективності та очності збору даних. Вдосконалюйте стратегію оніторингу та параметри аналізу на основі езультатів аналізу.

Системний моніторинг включає в себе наступні елементи:

Таблиця 2.3.

Елементи моніторингу

Збір даних	Включає збір інформації про різноманітні параметри системи, такі як продуктивність, використання ресурсів, стан мережі, потенційні загрози та інші важливі параметри.
Аналіз та обробка даних	Отримані дані аналізуються з метою виявлення аномалій, тенденцій, прогалин у продуктивності та ознак потенційного Проблеми або поліпшення ефективності системи.
Візуалізація та звітність	Результати аналізу даних представлені у вигляді зрозумілих графіків, діаграм і корисних інформаційних панелей Операторам і адміністраторам легше зрозуміти стан системи і приймати правильні рішення.
Сповіщення та автоматизація	Моніторинг системи може включати процес автоматичного сповіщення про виявлені проблеми або аномалії. Він може швидко реагувати на негативні явища і запобігати можливості виходу з ладу.
Оцінка та оптимізація	Отримані результати аналізу використовуються для оцінки ефективності системи і прийняття по ній рішень Оптимізація, підвищення продуктивності та забезпечення стабільності.

Сучасні інформаційні технології є невід'ємною частиною діяльності підприємств і організацій у всіх сферах. У цьому контексті необхідний системний

моніторинг. Важливо забезпечити надійність, ефективність та безпеку цих технологічних екосистем.

2.2 Переваги та недоліки технології моніторингу

Перш за все, система моніторингу дозволяє швидко реагувати на будь-які проблеми, які можуть виникнути у вашій IT-інфраструктурі. Вони не тільки дозволяють нам виявляти проблеми в режимі реального часу, але й пропонують швидкі рішення для них ще до того, як вони стануть критичними. Це забезпечує постійну доступність і надійність наших клієнтів, крім того, система моніторингу допомагає оптимізувати використання ресурсів. Можливість виявляти перевантаження і ефективно розподіляти ресурси підвищує продуктивність системи і знижує витрати. Крім того, не можна мінімізувати роль систем спостереження в забезпеченні безпеки. Вони допоможуть вам своєчасно виявляти та реагувати на потенційні загрози безпеці, а також запобігати можливим кібератакам та несанкціонованому доступу до ваших систем. Але крім всієї своєї корисності, система моніторингу має і недоліки. Впровадження та обслуговування можуть бути дорогими, що може призвести до перевантаження інформацією та помилкових спрацьовувань. Розглянемо переваги та недоліки систем моніторингу в IT.

Переваги:

- Підвищення доступності і надійності: Системи моніторингу дозволяють оперативно виявляти проблеми в IT-інфраструктурі, такі як відмови обладнання чи програмне забезпечення. Це допомагає попередити можливі відмови, що забезпечує більшу доступність і надійність систем.
- Швидка реакція на проблеми: Автоматизовані системи моніторингу здатні виявляти проблеми в реальному часі і надсилати сповіщення адміністраторам системи. Це дозволяє оперативно реагувати на проблеми і швидко виправляти їх перед тим, як вони стануть критичними.

- Оптимізація ресурсів: Моніторинг дозволяє виявляти перевантаження ресурсів, такі як процесор, пам'ять, мережевий трафік тощо. Це дозволяє ефективно розподіляти ресурси і уникати перевантажень, що сприяє підвищенню продуктивності системи.
- Планування майбутнього розвитку: Шляхом аналізу зібраних даних про використання ресурсів та пропускну здатність мережі, можна зробити висновки про необхідність масштабування системи чи покращення інфраструктури.
- Підвищення безпеки: Моніторинг дозволяє виявляти ненормальну активність в мережі, атаки або спроби несанкціонованого доступу до системи. Це допомагає вчасно виявляти та реагувати на загрози безпеці.

Недоліки:

- Витрати на впровадження та підтримку: Реалізація і підтримка систем моніторингу може бути дорогим процесом, який включає в себе витрати на обладнання, програмне забезпечення, навчання персоналу та підтримку системи.
- Перевантаження інформацією: Великий обсяг зібраної моніторингової інформації може призвести до перевантаження та ускладнення аналізу даних. Це може затримати виявлення та реагування на критичні проблеми.
- Фальшиві позитиви: Деякі системи моніторингу можуть генерувати фальшиві або непотрібні сповіщення про проблеми, що може викликати втомлення адміністраторів та зниження ефективності моніторингу.
- Недостатня адаптивність: Деякі системи моніторингу можуть бути обмежені у своїй здатності адаптуватися до нових технологій або середовищ.
- Приватність і конфіденційність: Збір і аналіз даних моніторингу може порушувати приватність та конфіденційність користувачів, якщо не вжиті відповідні заходи забезпечення конфіденційності.

2.3 Методи аналізу кібератак за допомогою технології моніторингу

У сучасному цифровому світі кібербезпека стала однією з найважливіших сфер для компаній будь-якого розміру. Зі збільшенням кількості та складності

кіберзагроз виникає необхідність покращити спосіб виявлення та аналізу кібератак. Однією з перспективних областей у цьому відношенні є використання технологій спостереження для виявлення та аналізу потенційних загроз.

Виявлення аномальних моделей поведінки. Технологія моніторингу дозволяє відстежувати мережеву активність і виявляти відхилення від типових моделей поведінки. Наприклад, надмірна активність або ненормальні запити до сервера можуть вказувати на можливість шкідливого доступу. Алгоритми машинного навчання можуть застосовуватися для аналізу великих обсягів даних і виявлення найдрібніших аномалій.

Моніторинг потоку інформації. Аналіз потоку інформації-ще одне важливе міркування при виявленні кібератак. Технології відстеження дозволяють збирати дані про вхідні та вихідні повідомлення та переглядати відомі схеми атак або з'єднання з відомими зловмисниками. Це корисно при виявленні атаки за допомогою зовнішнього сервера або ботнету для виконання атаки.

Використання технології моніторингу в реальному часі. Одним з найважливіших аспектів ефективного виявлення кібератак є можливість аналізу даних у режимі реального часу. Завдяки миттєвому моніторингу мережі ви можете швидко реагувати на потенційні загрози, навіть якщо вони виникають у вигляді нових раніше невідомих атак. Технології штучного інтелекту, зокрема системи автоматичного виявлення загроз, допомагають у цьому процесі, швидко і точно реагуючи на можливі кібератаки. Аналіз та відновлення подій

Одним з ключових етапів боротьби з кібератаками є виявлення системи і аналіз подій після відновлення. Технології відстеження дозволяють збирати дані про інциденти, їх характеристики та способи їх злому. Це допоможе розробити стратегії активного захисту в майбутньому та уникнути подібних інцидентів у майбутньому.

Як результат, технологія спостереження відіграє важливу роль у виявленні та аналізі кібератак. Це дозволяє компаніям швидко реагувати на загрози та ефективно захищати свою інформацію та інфраструктуру від кіберзлочинців. Правильне впровадження та використання цих технологій може значно підвищити

рівень кібербезпеки в організації.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО АНАЛІЗУ КІБЕРАТАК ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ МОНІТОРИНГУ

3.1 Реалізація технології моніторингу за допомогою системи Zabbix

Zabbix – це потужне рішення для моніторингу мереж і систем, яке надає користувачам можливість відстежувати стан мережевого обладнання, серверів, додатків та інших IT-ресурсів в реальному часі. Zabbix є відкритим програмним забезпеченням з розширеною функціональністю, що включає збір і аналіз даних, оповіщення про інциденти, а також можливості візуалізації даних через веб-інтерфейс. Zabbix широко використовується в різних галузях, включаючи фінансовий сектор, телекомунікації, урядові установи та IT-послуги, забезпечуючи високу надійність і безпеку моніторингу IT-інфраструктури [9].

- Архітектура

Zabbix складається з декількох основних програмних компонентів, функції яких викладено нижче.

- Сервер

Zabbix сервер є основним компонентом, якому агенти повідомляють інформацію про доступність і цілісність та статистику. Сервер є головним сховищем, у якому зберігаються всі дані конфігурації, статистики, а також оперативні дані.

- База даних

Вся інформація про конфігурацію, а також дані, зібрані Zabbix, зберігаються в базі даних.

- Веб-інтерфейс

Для легкого доступу до Zabbix з будь-якого місця і з будь-якої платформи, поставляється інтерфейс на основі Веб. Інтерфейс є частиною Zabbix сервера і зазвичай (але не обов'язково) працює на тій же самій фізичній машині, що і сервер.

- Проксі

Zabbix проксі може збирати дані про продуктивність і доступність від імені Zabbix сервера. Проксі є опціональною частиною Zabbix; однак він може бути корисним, щоб розподілити навантаження одного Zabbix сервера.

- Агент

Zabbix агенти розгортаються на спостережуваних системах для активного моніторингу за локальними ресурсами і додатками, і для надсилання зібраних даних Zabbix серверу або проксі. Починаючи з версії Zabbix 4.4, є два типи агентів: Zabbix агент (легкий, підтримується на великій кількості платформ, написаний мовою C) і Zabbix агент 2 (особливо гнучкий, легко розширюваний за допомогою плагінів, написаний мовою Go).

- Потік даних

Крім того, важливо зробити крок назад і поглянути на весь потік даних у Zabbix. Для того щоб створити елемент даних, який буде збирати дані, ви повинні спочатку створити вузол мережі. Переміщаючись в інший кінець спектра Zabbix, у вас повинен бути елемент даних, щоб створити тригер. У вас має бути тригер, щоб створити дію. Отже, якщо ви хочете отримувати сповіщення про занадто високе завантаження CPU на Сервері X, ви спершу маєте створити запис про вузол мережі для Сервера X, потім елемент даних для спостереження за CPU, потім тригер, який спрацює, якщо завантаження CPU буде занадто високим, а потім дію, яка надішле вам e-mail. Хоча може здатися, що потрібно занадто багато кроків, при використанні шаблонів насправді це не так. Тим не менш, така побудова системи дозволяє створювати дуже гнучкі інсталяції.

Також наведено короткий перелік можливостей системи Zabbix:

- Zabbix - високоінтегроване рішення для моніторингу мережі, що пропонує безліч функцій в одному пакеті.
- Збір даних

Перевірки доступності та продуктивності, підтримка моніторингу з використанням SNMP (і траппери, і поллери), IPMI, JMX, VMware, користувацькі перевірки, збір бажаних даних із використанням користувацьких інтервалів виконуються сервером/проксі та агентами.

- Гнучкі визначення порогів

Ви можете задавати дуже гнучкі пороги проблем, звані тригерами, посилаючись на значення з бази даних

- Безліч налаштувань сповіщень

Надсилання сповіщень може бути налаштоване з використанням розкладу ескалацій, одержувачів, способів сповіщень, сповіщення можна зробити інформативними та корисними з використанням змінних макросів, автоматичні дії, що включають в себе віддалені команди.

- Побудова графіків у режимі реального часу

За допомогою вбудованого функціоналу побудови графіків відразу ж доступні графіки за спостережуваними елементами даних

- Можливості веб-моніторингу

Zabbix може імітувати натискання мишкою на веб-сайті, перевіряти працездатність і час відповіді.

- Широкі можливості візуалізації

Можливість створювати користувацькі графіки, що дає змогу комбінувати безліч елементів даних в одному місці, карти мережі, слайд-шоу в огляді в стилі панелі, звіти, високорівневе (бізнес) представлення спостережуваних ресурсів.

- Зберігання даних історії

Зберігання даних у базі даних, історія, що налаштовується, вбудована процедура очищення історії.

- Просте налаштування

Додавання спостережуваних пристроїв у вигляді вузлів мережі, щойно вузли мережі з'являються в базі даних, вони відразу готові до моніторингу, застосування шаблонів до спостережуваних пристроїв.

- Використання шаблонів

Групування перевірок у шаблонах, шаблони можуть успадковуватися від інших шаблонів

- Мережеве виявлення

Автоматичне виявлення мережевих пристроїв, автоматична реєстрація агентів, виявлення файлових систем, мережевих пристроїв і SNMP OID'ів.

- Швидкий веб-ітерфейс

Веб-інтерфейс, заснований на мові PHP, доступний з будь-якого місця, зручна навігація, журнал аудиту.

- Zabbix API

Zabbix API надає програмований інтерфейс до Zabbix для масових маніпуляцій, інтеграції стороннього програмного забезпечення та інших цілей.

- Система прав доступу

Безпечна аутентифікація користувачів можливість обмеження доступу окремим користувачам до конкретних сторінок

- Повнофункціональний і легко розширюваний агент

Розгортається на спостережуваних машинах можна розгорнути як на Linux, так і на Windows

- Бінарні демони

Написані мовою Сі, мають високу продуктивність і використовують невеликий обсяг пам'яті легко переносяться.

- Готовність до складних середовищ

Простий віддалений моніторинг з використанням Zabbix проксі

Встановлення Zabbix:

- Завантажуємо .ovf файл для Zabbix з офіційного сайту - https://www.zabbix.com/ru/download_ appliance
- Імпортуємо .ovf файл у VirtualBox (рисунок 3.1)

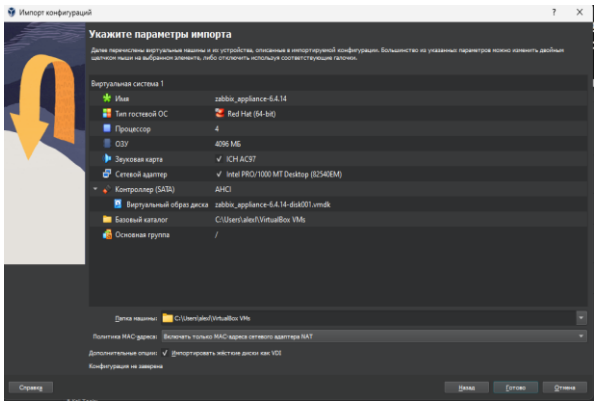

Рис. 3.1. Налаштування VirtualBox

Запускаємо віртуальну машину й входимо до системи з налаштуваннями по замовченню (root/zabbix) (рисунок 3.2)

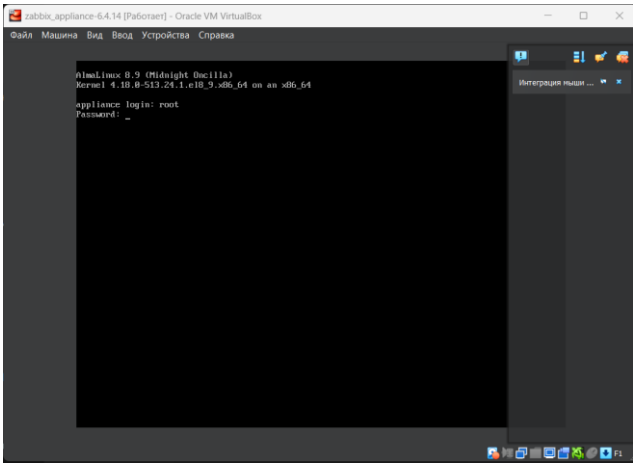

Рис. 3.2. Автентифікація Zabbix

- Тепер вводимо команду ip addr, та отримуємо IP адресу віртуальної машини (рисунок 3.3)

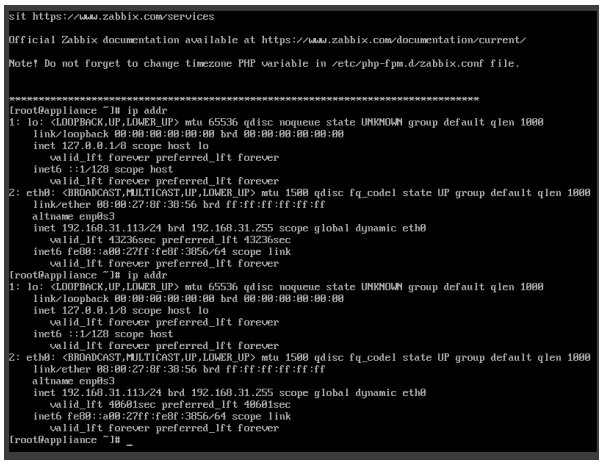

Рис. 3.3. IP адреса Zabbix

- Й в кінці заходимо по IP адресі віртуальної машини й бачимо веб-інтерфейс Zabbix (рисунок 3.4). Встановлення серверу пройшло успішно.

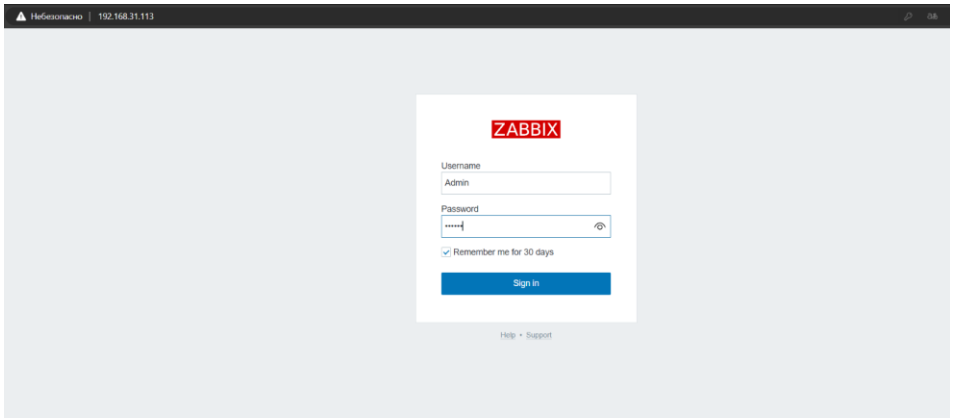

Рис. 3.4. Вхід у веб інтерфейс Zabbix

Тепер встановимо windows агент. Для цього заходимо по посиланню https://www.zabbix.com/ru/download_agents й завантажуємо агент під потрібну операційну систему. У моєму випадку це windows

- Відкриваємо завантажений архів й модифікуємо файл zabbix_agentd.conf (рисунок 3.5). У полі сервер потрібно вписати IP адресу машини, де встановлено Zabbix сервер.

Рис. 3.5. Модифікація файлу zabbix_agentd.conf

- В командному рядку, відкритому від імені адміністратора виконуємо команди: C:\zabbix\bin\zabbix_agentd.exe --config C:\zabbix\conf\zabbix_agentd.conf –-install та запускаємо службу командою C:\zabbix\bin\zabbix_agentd.exe --start (рисунок 3.6)

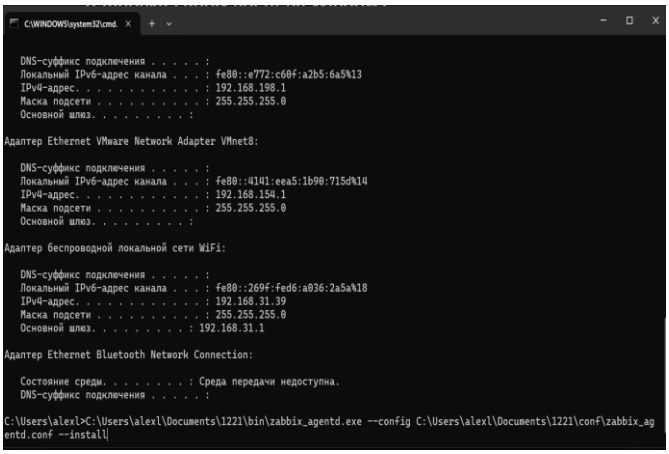

Рис. 3.6. Встановлення та запуск агенту Zabbix

- Наступним кроком, через Powershell, запущеному від імені адміністратора, відкриваємо порти для коректного функціонування агенту моніторингу командами: New-NetFirewallRule -DisplayName 'Zabbix agent_inb' -Profile 'Any' -Direction Inbound -Action Allow -Protocol TCP -LocalPort 10050 New-NetFirewallRule -DisplayName 'Zabbix agent_out' -Profile 'Any' -Direction Outbound -Action Allow -Protocol TCP -LocalPort 10050 (рисунок 3.7).

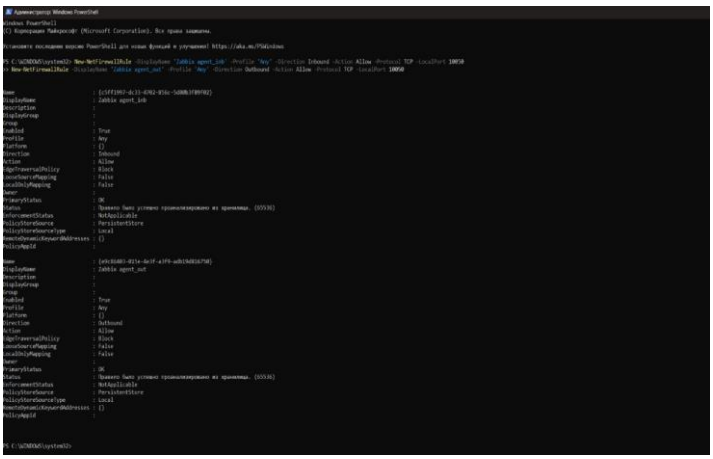

Рис. 3.7. Модифікація налаштувань брандмауера

- Після цього заходимо у веб інтерфейс Zabbix й налаштовуємо параметри нового вузла мережі (рисунок 3.8)

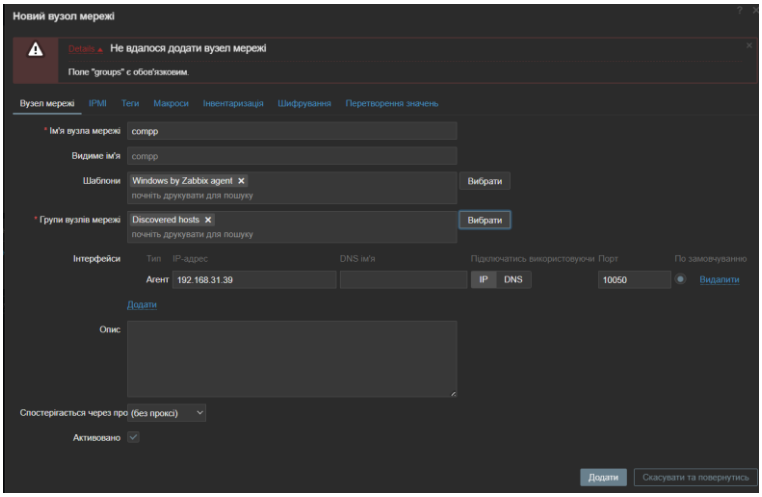

Рис. 3.8. Налаштування вузла мережі в Zabbix

- Й під кінець перевіряємо правильність налаштування системи, після того як логи почнуть надходити до Zabbix (рисунок 3.9)

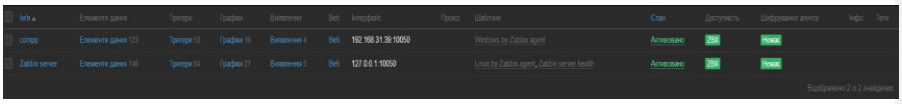

Рис. 3.9. Статус агента у Zabbix

3.2 Збір та аналіз зловмисних дій за допомогою системи Zabbix

В умовах сучасної кібербезпеки важливо не тільки виявляти, але й оперативно реагувати на зловмисні дії в IT-інфраструктурі. Система моніторингу Zabbix пропонує потужні інструменти для збору, аналізу та оповіщення про зловмисні дії. Для ефективного моніторингу важливо встановити агент Zabbix на всі критичні сервери та робочі станції. Агент збирає дані про системні метрики, мережевий трафік та інші важливі параметри, які можуть бути індикаторами зловмисних дій. Системні логи є цінним джерелом інформації про діяльність користувачів та системні події. Zabbix дозволяє налаштувати збір логів з різних

джерел, таких `/var/log/syslog` або `/var/log/auth.log`. Це дозволяє виявляти підозрілі події, такі як невдалі спроби входу або зміни конфігурації системи. Моніторинг мережевого трафіку є ключовим елементом виявлення зловмисної діяльності. Zabbix підтримує різні протоколи моніторингу мережі, такі як SNMP, IPMI та JMX, що дозволяє відстежувати обсяг трафіку, кількість відкритих з'єднань та активність портів. Одним із основних інструментів виявлення зловмисних дій є тригери. Наприклад, тригер для виявлення великої кількості невдалих спроб входу може бути налаштований таким чином:

{host:log[/var/log/auth.log].str(/Failed password for root).count(5m)} > 10

Цей тригер спрацьовує, якщо більше 10 невдалих спроб входу відбуваються за останні 5 хвилин.

Для виявлення аномальної поведінки системи можна використовувати тригери для системних параметрів. Наприклад, тригер для високого навантаження процесора:

{host:system.cpu.util[,user].avg(5m)} > 90

Цей тригер спрацьовує, якщо середнє завантаження процесора перевищує 90% за останні 5 хвилин.

Аномальна мережева активність може свідчити про зловмисні дії. Тригери для мережевого трафіку можуть бути налаштовані наступним чином:

{host:net.if.in[eth0].avg(5m)} > 100M

Цей тригер спрацьовує, якщо вхідний трафік на інтерфейсі eth0 перевищує 100 Мб за 5 хвилин.

Zabbix надає потужні інструменти для аналізу зібраних даних. Графіки, звіти та спеціальні панелі дозволяють виявляти тенденції та аномалії, які можуть свідчити про зловмисну діяльність. Аналіз зібраних даних допомагає своєчасно виявляти загрози та приймати обґрунтовані рішення.

Оперативне оповіщення є ключовим елементом виявлення та реагування на зловмисні дії. Zabbix дозволяє налаштувати оповіщення через різні канали, такі як електронна пошта, SMS, месенджери та інші. Налаштування ескалації оповіщень для критичних інцидентів забезпечує негайне інформування відповідальних осіб.

Для комплексного захисту інфраструктури важливо інтегрувати Zabbix з іншими системами безпеки, такими як Security Information and Event Management та Intrusion Detection and Prevention Systems. Використання API Zabbix дозволяє автоматизувати обробку інцидентів та обмін даними з іншими системами.

Також нижче наведені деякі приклади використання Zabbix для збору та аналізу зловмисних дій:

- **Відстеження невдалих входів до системи:** Zabbix може збирати та аналізувати журнали входів до системи, щоб виявити спроби несанкціонованого доступу, такі як використання неправильних паролів або атаки методом перебору паролів.
- **Аналіз журналів брандмауера:** Zabbix може аналізувати журнали брандмауера, щоб виявити заблоковані спроби доступу, які можуть свідчити про спроби сканування або атаки.
- **Відстеження змін конфігурації:** Zabbix може відстежувати зміни конфігураційних файлів, щоб виявити підозрілу активність, яка може свідчити про те, що зловмисник намагається отримати доступ до вашої системи.
- **Виявлення зараження шкідливим програмним забезпеченням:** Zabbix може сканувати системні файли на наявність відомих вірусів, троянів та інших типів шкідливого програмного забезпечення.
- **Відстеження змін цілісності файлів:** Zabbix може відстежувати хеш-суми системних файлів, щоб виявити зміни, які можуть свідчити про те, що файл був пошкоджений або замінений шкідливим програмним забезпеченням.
- **Аналіз використання дискового простору:** Zabbix може аналізувати використання дискового простору, щоб виявити підозрілі файли, які можуть бути великими за розміром або швидко зростати.
- **Виявлення несанкціонованих процесів:** Zabbix може відстежувати активні процеси та виявляти ті, які не є частиною вашої стандартної операційної системи або програмного забезпечення.

- **Відстеження ресурсів процесора та пам'яті:** Zabbix може відстежувати використання ресурсів процесора та пам'яті, щоб виявити процеси, які споживають занадто багато ресурсів і можуть бути шкідливими.
- **Аналіз мережевої активності процесів:** Zabbix може аналізувати мережеву активність процесів, щоб виявити підозрілу активність, наприклад, надсилання даних на невідомі сервери. [10]

3.3 Рекомендації щодо аналізу дій зловмисника за допомогою системи Zabbix

Zabbix - це потужний інструмент моніторингу, який може бути використаний для збору та аналізу даних про безпеку, що може допомогти вам виявити та дослідити зловмисні дії. Ось кілька рекомендацій щодо використання Zabbix для аналізу дій зловмисника:

Першим кроком є збір відповідних даних про моніторинг. Це може включати:

- **Мережевий трафік:** Моніторинг мережевого трафіку може допомогти вам виявити підозрілу активність, таку як сканування портів, атаки типу "відмова в обслуговуванні" або несанкціонований доступ до даних.
- **Журнали:** Збір та аналіз журналів з різних джерел, таких як веб-сервери, брандмауери та системи баз даних, може допомогти вам виявити зловмисні дії, такі як спроби проникнення або зараження шкідливим програмним забезпеченням.
- **Системні файли:** Моніторинг системних файлів може допомогти вам виявити зміни, які можуть свідчити про те, що зловмисник отримав доступ до вашої системи, наприклад, зміни конфігураційних файлів або завантаження шкідливого програмного забезпечення.

Системні процеси: Моніторинг системних процесів може допомогти вам виявити підозрілі процеси, які можуть бути шкідливим програмним забезпеченням або іншими зловмисними програмами.

Zabbix пропонує широкий спектр функцій візуалізації даних, які можуть допомогти вам швидко та легко зрозуміти дані про моніторинг. Використовуйте графіки, діаграми та панелі моніторингу, щоб візуалізувати тенденції, аномалії та інші важливі дані.

Zabbix може виявляти аномалії в даних про моніторинг, що може допомогти вам виявити зловмисні дії. Наприклад, ви можете встановити базові лінії для трафіку, журналів або системних файлів і отримувати сповіщення, коли дані виходять за межі цих базових ліній.

У сучасному світі кібербезпеки ефективний моніторинг та аналіз дій зловмисників є критично важливими для забезпечення захисту IT-інфраструктури. Система моніторингу Zabbix пропонує потужні інструменти для збору, аналізу та оповіщення про зловмисні дії. У цій статті розглядаються методи використання Zabbix для виявлення та аналізу потенційних загроз, а також рекомендації щодо ефективного використання цієї системи для аналізу дій зловмисника.

Забезпечення безпеки IT-інфраструктури є критично важливим завданням для будь-якої організації. Кіберзагрози постійно зростають, тому організації повинні мати ефективні інструменти для виявлення та аналізу зловмисних дій. Система Zabbix є потужним рішенням для моніторингу, яке допомагає організаціям здійснювати цілодобовий моніторинг своїх систем, збирати та аналізувати дані, а також реагувати на потенційні загрози.

Zabbix може моніторити продуктивність серверів, включаючи використання процесора, пам'яті та дискового простору. Наприклад, можна створити тригери для виявлення високого завантаження процесора:

{host:system.cpu.util[,user].avg(5m)} > 90

Цей тригер спрацює, якщо середнє завантаження процесора перевищить 90% за останні 5 хвилин, що може свідчити про проблеми з продуктивністю.

Для моніторингу робочих станцій можна використовувати ті ж принципи, що й для серверів. Наприклад, моніторинг використання дискового простору:

{host:vfs.fs.size[/,pused].last()} > 80

Цей тригер спрацює, якщо використання дискового простору на головному розділі перевищить 80%.

Zabbix підтримує моніторинг мережевих пристроїв, таких як маршрутизатори, комутатори та точки доступу. Наприклад, моніторинг вхідного та вихідного трафіку:

net.if.in[eth0]

net.if.out[eth0]

Ці параметри дозволяють відслідковувати кількість вхідного та вихідного трафіку на інтерфейсі eth0.

Завдяки моніторингу мережевого трафіку можна виявляти аномалії, що можуть свідчити про мережеві атаки. Наприклад, тригер для великої кількості невдалих спроб підключення:

{host:net.tcp.port[port_number].count(5m)} > 100

Цей тригер спрацює, якщо кількість підключень до порту перевищить 100 за останні 5 хвилин.

Zabbix може моніторити продуктивність баз даних, таких як MySQL, PostgreSQL та інших. Наприклад, моніторинг кількості активних з'єднань до бази даних:

{host:db.connections[mysql].last()} > 100

Цей тригер спрацює, якщо кількість активних з'єднань до MySQL перевищить 100.

Моніторинг довготривалих запитів до бази даних може допомогти виявити проблеми з продуктивністю. Наприклад, тригер для виявлення запитів, що виконуються більше ніж 5 секунд:

{host:db.query_time[mysql].avg(5m)} > 5000

Цей тригер спрацює, якщо середній час виконання запитів перевищить 5 секунд за останні 5 хвилин.

Zabbix може перевіряти доступність веб-сайтів шляхом надсилання HTTP-запитів. Наприклад, моніторинг статусу HTTP-відповіді:

{host:web.page.get[example.com,,response_code].last()} <> 200

Цей тригер спрацює, якщо HTTP-відповідь від example.com не дорівнює 200 (OK).

Моніторинг часу відповіді веб-сайтів та веб-додатків може допомогти виявити проблеми з продуктивністю. Наприклад, тригер для виявлення довготривалого часу відповіді:

{host:web.page.perf[example.com,,response_time].avg(5m)} > 3000

Цей тригер спрацює, якщо середній час відповіді перевищить 3 секунди за останні 5 хвилин.

Моніторинг стану апаратного забезпечення допомагає попередити можливі відмови. Наприклад, моніторинг температури процесора:

{host:system.hw.temp[coretemp].last()} > 80

Цей тригер спрацює, якщо температура процесора перевищить 80°C.

Моніторинг стану жорстких дисків може допомогти виявити можливі проблеми до того, як вони призведуть до втрати даних. Наприклад, тригер для виявлення помилок S.M.A.R.T.:

{host:vfs.fs.s.mart[/dev/sda].str(ERROR)} = 1

Цей тригер спрацює, якщо на диску /dev/sda буде виявлено помилку S.M.A.R.T.

Інтеграція Zabbix з SIEM-системами дозволяє здійснювати кореляцію подій та виявляти комплексні атаки. Наприклад, Zabbix може надсилати дані до Security Information and Event Management систем для подальшого аналізу та кореляції з іншими джерелами даних.

Використання Intrusion Detection and Prevention Systems у поєднанні з Zabbix дозволяє підвищити рівень захисту мережі. Наприклад, Zabbix може автоматично реагувати на події, виявлені Intrusion Detection and Prevention Systems, шляхом створення тригерів для певних дій.

API Zabbix дозволяє автоматизувати процеси моніторингу та реагування. Наприклад, можна створити кастомні скрипти для автоматичного додавання нових хостів до моніторингу або для створення кастомних звітів.

Система Zabbix є потужним інструментом для моніторингу різних аспектів IT-інфраструктури. Від моніторингу серверів та мережевого обладнання до інтеграції з іншими системами безпеки, Zabbix забезпечує гнучкість та масштабованість, що робить його незамінним у забезпеченні стабільної та безпечної роботи організації. Використання прикладів та рекомендацій, наведених у цій статті, допоможе організаціям ефективно використовувати Zabbix для виявлення, аналізу та реагування на зловмисні дії.

ВИСНОВКИ

У ході дослідження було розглянуто ефективність застосування системи моніторингу Zabbix на кінцевих точках IT-інфраструктури. Зокрема, було виявлено, що Zabbix надає широкі можливості для моніторингу продуктивності серверів, робочих станцій, мережевих пристроїв та баз даних. Використання цієї системи дозволяє своєчасно виявляти та аналізувати зловмисні дії, а також запобігати можливим інцидентам завдяки налаштуванню тригерів і автоматизації оповіщень.

Розроблені рекомендації щодо збору та аналізу даних з кінцевих точок за допомогою Zabbix включають:

- Встановлення та налаштування агента Zabbix на всі критичні елементи інфраструктури для забезпечення комплексного моніторингу.
- Моніторинг системних параметрів, логів та мережевого трафіку для виявлення аномалій та підозрілих дій.
- Налаштування тригерів для автоматичного виявлення потенційних загроз та оперативного оповіщення про них.
- Аналіз зібраних даних за допомогою графіків, звітів та інструментів для виявлення аномалій.
- Інтеграція з іншими системами безпеки, такими як SIEM та IDS/IPS, для підвищення рівня захисту та ефективного реагування на інциденти.

Практичне застосування цих рекомендацій дозволяє значно підвищити рівень безпеки IT-інфраструктури та забезпечити надійний захист від зловмисних дій. Система Zabbix демонструє високу гнучкість та масштабованість, що робить її незамінним інструментом для моніторингу в сучасних умовах постійно зростаючих кіберзагроз. Подальше дослідження шляхів оптимізації налаштувань Zabbix та інтеграції з новими технологіями безпеки допоможе ще більше підвищити ефективність використання цієї системи у різних сферах діяльності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cybercrime threatens business growth. URL: https://www.zdnet.com/article/cybercrime-can-be-the-biggest-threat-to-business-growth (дата звернення 01.05.2024).

2. IBM X-Force Threat Intelligence. URL: https://www.ibm.com/reports/threat-intelligence (дата звернення 01.05.2024).

3. The cyber war between Ukraine and Russia: An overview. URL: https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10 (дата звернення 01.05.2024).

4. Cost of the data breach 2023. URL: https://www.ibm.com/reports/data-breach (дата звернення 01.05.2024).

5. Increase of the cyberattacks in 2022. URL: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (дата звернення 01.05.2024).

6. Богуш В.М., Юдін О.К. Інформаційна безпека держави. –К.: «МК-Прес», 2005. -432с.

7. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації d автоматизованій системі.

8. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

9. Zabbix appliance manual. URL: https://www.zabbix.com/documentation/6.0/ru/manual/appliance (дата звернення 01.05.2024).

10. Manual for Zabbix. URL: https://www.zabbix.com/documentation/6.0/ru/manual (дата звернення 01.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)