Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *"Аудит захищеності пристроїв інтернету речей з допомогою AWS IoT Device Defender"*

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Горішний М.О.
підпис (прізвище та ініціали)

Керівник *Марценюк В.П.*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б.*
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент *Дячук С.Ф.*
підпис (прізвище та ініціали)

м. Тернопіль – 2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«_____» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Горішному Михайлу Орестовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аудит захищеності пристроїв інтернету речей з допомогою AWS IOT DEVICE DEFENDER

Керівник роботи Марценюк В.П., д.т.н, проф. каф. кібербезпеки
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 23 » 03 2022 року № 4/7-177

2. Термін подання студентом завершеної роботи 16.06.2022

3. Вихідні дані до роботи Параметри системи з використанням пристроїв IoT

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Огляд літературних джерел. 1.1 Загрози безпеки пристроїв IoT.
1.2 Ключові критерії захищеності пристроїв IoT. 1.3 Засоби для аудиту безпеки IoT-пристроїв. 1.4 Загальна характеристика IoT Device Defender. 1.5 Постановка задачі.
2. Теоретичні основи аудиту захищеності пристроїв інтернету речей.
2.1 Основні визначення та вимоги до аудиту інформаційних систем.
2.2 Обгрунтування вибору набору вразливостей, щодо яких здійснюється аудит.
3 Практична частина. Планування та проведення аудиту безпеки пристроїв IoT.
3.1 Визначення обсягу та цілей аудиту безпеки пристроїв IoT. 3.2 Налаштування ролей та політик для дослідження. 3.3 Проведення аудиту безпеки за допомогою IoTDeviceDefender.
3.4 Аналіз результатів аудиту та вибір найкращих практик.
4 Безпека життєдіяльності, основи хорони праці Висновки. Перелік використаних джерел

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титулка. 2. Мета, задачі дослідження. 3. Життєвий цикл та структура ідентифікатора пристрою IoT. 4. Екосистема AWS IoT Core та послідовність аудиту. 5. Атрибути політик доступу AWS IoTCore. 6. Налаштування перевірок аудиту AWS IoT Device Defender.
7. Рівнікритичностівразливостей в AWS IoT. 8. Рівні реєстрації ведення журналів через AWS IoT 9. Звіти про аудити IoT Device Defender. 10 Найкращі практики AWS IoT.
11. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Пулька Ч.В., професор кафедри МТ		

7. Дата видачі завдання 24.01.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2022 р.	*Виконано*
2.	Підбір джерел щодо аудиту захищеності	04.01 – 30.01	*Виконано*
3.	Опрацювання джерел в галузі дослідження	31.01 – 06.02	*Виконано*
4.	Виконання дослідження щодо аудиту захищеності		
	пристроїв інтернету речей за допомогою		
	IoTDeviceDefender	07.02 – 13.02	*Виконано*
5.	Опрацювання результатів аудиту	14.02 – 06.03	
6.	Оформлення розділу «Огляд літературних джерел»	07.03 – 20.03	*Виконано*
7.	Оформлення розділу «Теоретичні основи аудиту		
	Захищеності інтернету речей»	21.03 – 03.04	*Виконано*
8.	Оформлення розділу «Практична частина. Планування		
	та проведення аудиту безпеки пристроїв IoT»	04.04 – 17.04	*Виконано*
9.	Виконання завдання до розділу «Безпека		
	життєдіяльності, основи хорони праці»	18.04 – 01.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	02.05 – 15.05	*Виконано*
11.	Нормоконтроль	16.05 – 22.05	*Виконано*
12.	Перевірка на плагіат	03.06.2022 р.	*Виконано*
13.	Попередній захист кваліфікаційної роботи	06.06.2022 р.	*Виконано*
14.	Захист кваліфікаційної роботи	17.06.2022 р.	

Студент *Горішний М.О.*

(підпис) (прізвище та ініціали)

Керівник роботи *Марценюк В.П.*

(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аудит захищеності пристроїв інтернету речей з допомогою AWS IoT Device Defender// Кваліфікаційна робота ОР «Бакалавр» // Горішний Михайло Орестович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБсз-41 // Тернопіль, 2022 // С. 53 , рис. – 9, табл. – 2, додат. – 2 .

Ключові слова: КІБЕРЗАГРОЗА, АТАКА, ІНТЕРНЕТ РЕЧЕЙ, ПОЛІТИКА БЕЗПЕКИ, ВРАЗЛИВІСТЬ, АУДИТ БЕЗПЕКИ.

Кваліфікаційна робота присвячена дослідженню сучасних засобів аудиту захищеності пристроїв інтернету речей. В роботі проведений порівняльний аналіз існуючих програмних засобів, які дозволяють проводити аудит безпеки пристроїв IoT та обґрунтовано вибір AWS IoT Device Defender для проведення періодичних налаштовуваних віддалених аудитів пристроїв інтернету речей. Розроблено програму аудиту, налаштовано ролі та політики доступу.

В роботі також проведено дослідження впливу рівня деталізації набору відомих вразливостей, щодо яких здійснюється перевірка. Встановлено, що недостатня деталізація приводить до низької чутливості засобу аудиту та може привести до реалізації ризиків безпеки. На основі аналізу результатів аудиту обрано найкращі практики, яких слід дотримуватися при конфігуруванні систем інтернету речей.

ANNOTATION

Audit of Internet of Things devices security by means of AWS IoT Device Defender // Qualification thesis of educational level "Bachelor" // Horishnyy Mykhailo Orestovych // Ternopil National Technical University named after Ivan Puluj, Faculty of Computer Information Systems and software engineering, Department of Cybersecurity, СБсз-41 group // Ternopil, 2022 // P.53, figures - 9, tables - 2, appendices - 2.

Keywords: CYBERTHREAT, ATTACK, INTERNET OF THINGS, SECURITY POLICY, VULNERABILITY, SECURITY AUDIT.

The qualification work is devoted to the study of modern means of the security auditing of the Internet of Things devices. Available software for security audits of IoT devices is characterised and the choice of AWS IoT Device Defender for periodic customizable remote audits of IoT devices is justified. Audit programs are developed, access roles and policies are set up.

The study examines the impact of the detailization level of the known vulnerabilities set which is used for the audit specification. It is shown that insufficient detail leads to low sensitivity of the audit tool and can lead to the realization of security risks. Based on the analysis of the audit results, the best practices to be followed when configuring the Internet of Things are selected.

ЗМІСТ

ЗМІСТ.....6
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ.....7
ВСТУП.....8
1 ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ.....9
1.1 Загрози безпеки пристроїв IoT.....9
1.2 Ключові критерії захищеності пристроїв IoT.....11
1.3 Засоби для аудиту безпеки IoT-пристроїв.....15
1.4 Загальна характеристика IoT Device Defender.....16
1.5 Постановка задачі.....17
2 ТЕОРЕТИЧНІ ОСНОВИ АУДИТУ ЗАХИЩЕНОСТІ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ.....18
2.1 Основні визначення та вимоги до аудиту інформаційних систем.....18
2.2 Обгрунтування вибору набору вразливостей, щодо яких здійснюється аудит.....19
3 ПРАКТИЧНА ЧАСТИНА. Планування та проведення аудиту безпеки пристроїв іоТ.....25
3.1 Визначення обсягу та цілей аудиту безпеки пристроїв IoT.....25
3.2 Налаштування ролей та політик для дослідження.....26
3.3 Проведення аудиту безпеки за допомогою IoT Device Defender.....33
3.4 Аналіз результатів аудиту та вибір найкращих практик.....40
4 Безпека життєдіяльності, основи хорони праці.....41
4.1 Застосування ризик орієнтовного підходу для побудови структурно-логічних моделей виникнення надзвичайних ситуацій.....41
4.2 Соціальне значення охорони праці.....44
ВИСНОВКИ.....47
СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ.....48
ДОДАТКИ.....51

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AWS	AmazonWebServices
CA	certificateauthority
CLI	CommandLineInterface
COBIT	ControlObjectivesforInformationandRelatedTechnology
DDoS	(Distributed) Denial-of-serviceattack
IAM	Identityand Access Management
IoT	InternetofThings
MQTT	messagequeuingtelemetrytransport
OEM	Originalequipmentmanufacturer
OWASP	OpenWebApplicationSecurity Project
UUID	universallyuniqueidentifier

ВСТУП

Програмне забезпечення пристроїв інтернету речей надзвичайно вразливе до атак, оскільки воно контролює і доступ до даних (часто особистих або чутливих) і підключені пристрої. Безпечний Інтернет речей грунтуєтсья на ідентифікації пристроїв і датчиків, забезпечення доступу до даних і взаємодії між пристроями у надійній екосистемі.

Для більшості застосувань інтернету речей рекомендованим підходом є надійна екосистема авторизованих пристроїв і авторизованих служб. У надійній екосистемі неавторизовані пристрої чи служби не можуть взаємодіяти з авторизованими пристроями чи службами. Це запобігає несанкціонованому доступу до важливих служб і даних. Надійність екосистеми повинна регулятно підтверджуватися шліхом аудиту за певним набором критеріїв безпеки.

Метою даної роботи є дослідження процесу аудиту безпеки системи інтернету речей за допомогою служби IoTDeviceDefender платформи AmazonIoTCore та виявлння її переваг і недоліків.

Для досягнення поставленої мети потрібно розв'язати наступні завдання:

- Проаналізувати основні вразливості та критерії безпеки пристроїв інтернету речей.
- Проаналізувати відомі засоби аудиту безпеки інтернету речей.
- Обрати засіб та розробити методику дослідження.
- Дослідити вплив повноти набору критеріїв на чутливість аудиту.
- Зробити висновки щодо переваг та недоліків обраного засобу для аудиту систем інтернету речей.

1 ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1.1 Загрози безпеки пристроїв IoT

Інтернет речей (InternetofThings, IoT) вже сьогодні змінив виробництво та побут. Підключені пристрої постійно комунікують один з одним та хмарою за допомогою різних протоколів зв'язку. Хоча такий тип підключення становить основну перевагу додатків IoT, він також може відкривати можливості для неавторизованих користувачів і спричиняти ненавмисне розкриття інформації.

Щоб галузі, які використовують Інтернет речей, могли розвиватися, кінцеві пристрої повинні мати можливість постійно спілкуватися один з одним, користувачами та службами [1]. Оскільки ці нові постачальники послуг розробляють нові та інноваційні послуги для певних сегментів ринку [2, 3], вони можуть не знати про загрози, з якими може зіткнутися їхній сервіс. У деяких випадках постачальник послуг, можливо, раніше не розробляв послугу, яка підключалася до мережі зв'язку або Інтернету, і вони можуть не мати доступу до навичок та досвіду, щоб зменшити ризики, пов'язані з підключенням до Інтернету на своїх пристроях. Навпаки, їхні супротивники розуміють слабкі місця в технології та безпеці, швидко користуючись перевагами, якщо виявляться вразливі місця. Існує ряд атак, які призвели до скомпрометованих пристроїв. Зламані пристрої можуть вилучити дані, атакувати інші пристрої або спричинити збій у роботі пов'язаних чи непов'язаних служб.

Незважаючи на те, що багато постачальників послуг, таких як автомобілебудування, охорона здоров'я, побутова електроніка та муніципальні послуги, можуть вважати свої особливі вимоги безпеки унікальними для свого ринку, це, як правило, не так [4, 5]. Майже всі послуги Інтернету речей створені з використанням компонентів кінцевих пристроїв і сервісної платформи, які містять технології, подібні до багатьох інших комунікаційних, обчислювальних та IT-рішень [6, 7]. На додаток до цього, загрози, з якими стикаються ці різні служби, і потенційні рішення для пом'якшення цих загроз зазвичай дуже схожі,

навіть якщо мотивація зловмисника та вплив успішних порушень безпеки можуть відрізнятися. Щоб Інтернет речей був надійним та ефективним, необхідно постійно вирішувати проблеми безпеки, притаманні його розвитку, та забезпечувати [8]:

- Доступність: забезпечення постійного підключення між кінцевими точками та їх відповідними службами;
- Ідентифікація: автентифікація кінцевих точок, служб і клієнта або кінцевого користувача, що керує кінцевою точкою;
- Конфіденційність: зменшення потенційної шкоди для окремих кінцевих користувачів;
- Безпека: забезпечення того, що цілісність системи може бути перевірена, відслідкована та відслідкована.

Щоб захистити користувачів, пристрої та компанії, пристрої IoT мають бути безпечними та захищеними. Фундамент безпеки IoT лежить в контролі, управлінні та з’єднаннях між пристроями. Належний захист допомагає зберегти конфіденційність даних, обмежує доступ до пристроїв і хмарних ресурсів, пропонує безпечні способи підключення до хмари та відстежує поведінку пристрою. Стратегія безпеки IoT зменшує небажані події за допомогою таких служб і функцій, як аудит, управління ризиками та виявлення загроз.

Пристрої IoT дуже часто записують та передають конфіденційні дані [5, 7]. Системи безпеки (камери, двері), принтери і будь-який тип пристроїв з Wi-Fi зазвичай інтегровано в бізнес-мережі, цим можуть легко скористатися кіберзлочинці. Як тільки кіберзлочинець отримує доступ до пристрою IoT, він може завдати шкоди. Кіберзловмисники можуть використовувати пристрої інтернету речей у ботнеті для атак DdoS, щоб порушити нормальний трафік цільового сервера або мережі. Мікроконтролери та датчики Інтернету речей зазвичай повинні інтегруватися в існуючий пристрій, щоб він міг збирати й надсилати вимірювання (наприклад, тиск, вібрація чи температура) або активувати щось (наприклад, увімкнути світло чи відкрити вікно). Через це пристрої IoT малі та мають обмежені ресурси, що може призвести до експлуатації неавторизованими користувачами. Для розробників вбудованих

систем підтримувати безпечне хмарне з'єднання може бути складно. Дуже важливо, щоб рішення було безпечним і добре спроектованим однак для бідь-якого рішення постійний контроль та захист становлять ще більш нагальну потребу.

1.2 Ключові критерії захищеності пристроїв IoT

Для того, щоб кінцевий пристрій IoT функціонував в екосистемі продукту або сервісу Інтернету речей, він повинен бути здатним безпечно ідентифікувати себе для інших і служб. Цей критичний і принциповий аспект технології IoT гарантує, що послуги та однорангові мережі можуть гарантувати, куди і кому доставляються дані.

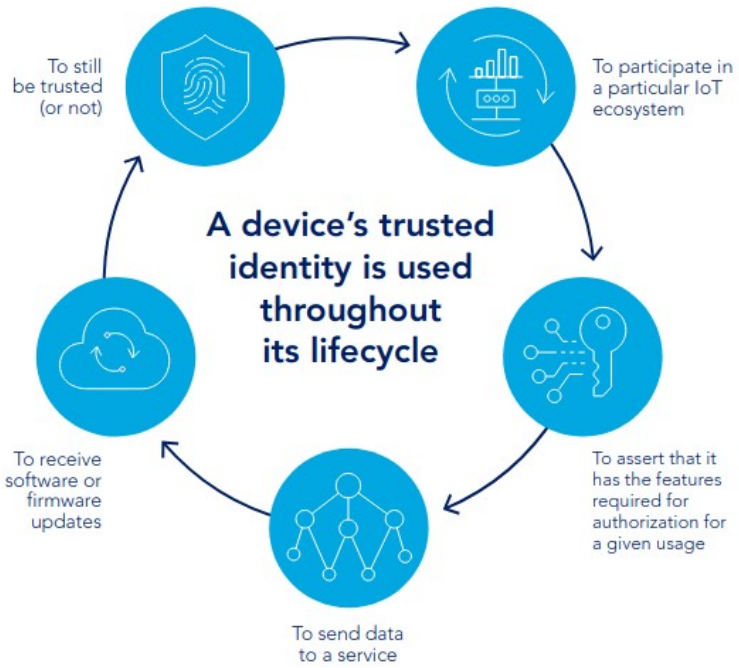


Рисунок 1.1 – Життєвий цикл ідентифікатора пристрою IoT [9]

Хоча взаємна автентифікація є базовою вимогою, пристрої також потребують унікальної ідентифікації [9]. Це дозволяє пристрою виконувати різні операцій і описує, чим він є і що уповноважений робити. На Рисунку 1.1 показано, як ідентифікатор пристрою використовується протягом його життєвого циклу. Хоча одного криптографічного ключа або сертифіката

відкритого ключа може бути достатньо для простих програм, більшість програм потребує складнішої структури даних, яка включає в себе метадані, оператори авторизації та криптографічні облікові дані. Типовий ідентифікатор пристрою показаний на Рисунку 1.2.

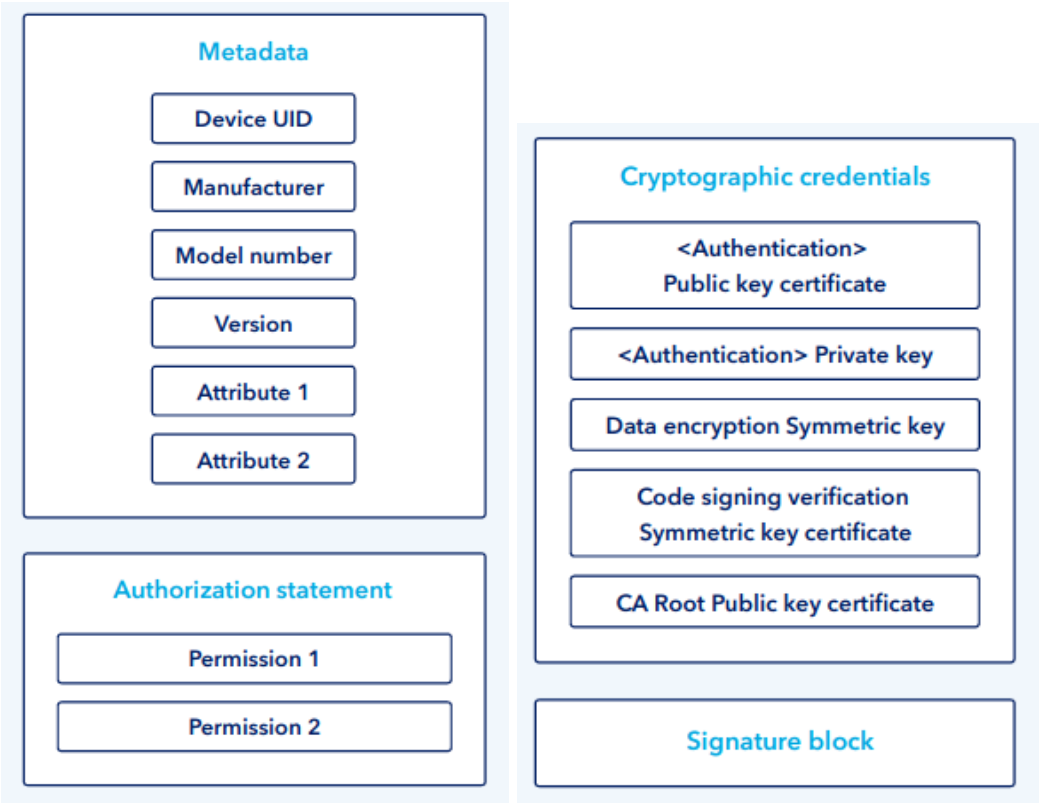


Рисунок 1.2 – Структура ідентифікатора пристрою IoT [9]

Метадані містять описову інформацію про тип пристрою, виробника, модель і номер версії, а також можуть включати атрибути, що описують його функціональність [10, 11]. Оператори авторизації — це дозволи, які описують, що дозволено робити пристрою. Деякі багатофункціональні пристрої можуть використовувати лише частину своїх можливостей для певних випадків використання. Наприклад, відеозапис камери може бути заборонений з правових причин у деяких установках, але фотографування може бути дозволено.

Пристрою може знадобитися кілька типів криптографічних ключів і сертифікатів [12, 13]. Наприклад, йому можуть знадобитися ключі для: аутентифікації служб, шифрування даних або перевірки підписів коду. Усі сертифікати (криптографічні ключі та ключі аутентифікації) зазвичай будуть прив’язані до унікального кореневого сертифіката, виданого центром

сертифікації (CA). Деякі сертифікати в пов’язану ієрархію сертифікатів можуть бути включені, щоб перевірити ідентичність служб, з якими взаємодіє пристрій.

Щоб запобігти фальсифікації, вся ідентифікація пристрою захищена цифровим підписом [14]. Оскільки ідентифікатор пристрою може містити конфіденційну інформацію, таку як закриті ключі та кореневі сертифікати CA, він потребує надійного захисту. Це робиться шляхом доставки ідентифікаційних даних на пристрій через безпечний канал із автентифікацією. Потрапивши на пристрій, конфіденційні матеріали або весь ідентифікатор пристрою потрібно буде надійно зберігати; наприклад, в апаратній підтримці.

Процес присвоєння пристрою ідентифікатором називається наданням (provisioning). Загалом існує два підходи до надання ідентифікаційних даних пристроїв: ініціалізація на заводі та надання послуг у хмарі. При заводській ініціалізації ідентифікатори пристроїв прив’язуються до пристрою на заводі під час виробничого процесу. Основна причина фабричного ініціалізації полягає в тому, що можна скористатися перевагами безпечного обладнання. Багато сучасних наборів мікросхем мають спеціальні апаратні функції, такі як одноразова програмована пам’ять (електричні запобіжники) та інші вбудовані сховища, які можна використовувати для безпечного зберігання криптографічних ключів. Отримання ключів у апаратному забезпеченні – це процес, відомий як введення ключів. Але, залежно від чіпсета, можуть бути обмеження на кількість або типи ключів, які можуть бути введені в чіп.

Як правило, постачальники послуг IoT працюватимуть з виробниками OEM, які, у свою чергу, співпрацюють з виробниками чіпсетів. Цей ланцюжок поставок може ускладнити процес надання, оскільки надання ідентифікаційних даних пристрою може відбуватися в будь-якій точці цього ланцюга постачання.

Доступ до інформації та послуг – не єдине питання, безпосередньо пов'язане з ідентичністю. Важливими є також питання [15-17]:

- Чи може користувач, який керує кінцевою точкою, бути прямо пов’язаний з ідентифікатором кінцевого пристрою?

- Як служби та однорангові партнери можуть перевірити ідентичність кінцевого користувача, перевіривши ідентичність кінцевого пристрою?

- Чи можуть шахрайські служби служби видавати себе за авторизовані?

- Як ідентичність пристрою захищена від фальсифікації чи маніпуляцій?

- Як кінцевий пристрій та мережа можуть гарантувати, що послуга IoT має доступ до кінцевого пристрою?

Конфіденційність не можна розглядати як доповнення до наявних продуктів і послуг. Оскільки на фізичний світ безпосередньо впливають дії, що здійснюються в цифровому світі, конфіденційність має бути розроблена в продуктах з нуля (bydesign), щоб гарантувати, що кожна дія авторизована і кожна особистість перевіряється, гарантуючи, що ці дії та пов'язані метадані є не передаються стороннім особам. Цього можна досягти лише шляхом визначення належної архітектури для продукту чи послуги, і його надзвичайно важко та дорого виконати заднім числом. Медичні пристрої, автомобільні рішення, промислові системи керування, домашня автоматизація, будівельні та охоронні системи тощо – все це безпосередньо впливає на фізичне життя людей.

Для проведення аудиту важливо розглянути питання [17, 18]:

- Чи може кінцевий пристрій або служба IoT виявити, чи є аномалія в її конфігурації або застосуванні?

-Як кінцеві пристрої відстежуються на предмет аномалій, які вказують на шкідливу поведінку?

- Як автентифікація та ідентифікація пов'язані з процесом безпеки продукту чи послуги?

- Чи можна оновити або виправити програмне забезпечення кінцевих пристроїв, щоб усунути вразливості?

1.3 Засоби для аудиту безпеки IoT-пристроїв

Обмеженням в існуючих інструментах аудиту безпеки є відсутність їх адаптації для пристроїв IoT [17]. Пристрої IoT є більш різноманітними, ніж традиційні пристрої. Вони можуть мати дуже обмежені ресурси, і вони можуть бути неоднорідними за своєю природою. Крім того, безпека може бути включена в апаратну архітектуру IoT, драйвер а також програмне забезпечення. Це

зумовлює особливості існуючиз засобів аудиту пристроїв інтернету речей [18]. На даний час, доступною є дуже обмежена кількість таких засобів. Слід відзначити FirmwareAnalysisToolkit (https://github.com/attify/firmware-analysis-toolkit), створений, щоб допомогти дослідникам безпеки в ручному режимі аналізувати та виявляти вразливості вбудованих пристроїв. Для відомої версії драйвера, яка використовується як аргумент сценарію, FirmwareAnalysisToolkit відобразить IP-адреси, призначені створеним мережевим інтерфейсам та емульовано прошивку для подальшого дослідження.

PENIOT (https://github.com/yakuza8/peniot) – це інструмент тестування на проникнення для пристроїв інтернету речей, який допомагає вам перевірити пристрої, тестуючи їх підключення до Інтернету за допомогою різних типів атак (як активних, так і пасивних) на основі протоколів. Після визначення цільового пристрою та необхідної інформації (або параметрів) цього пристрою можна виконувати активні атаки безпеки, як-от зміна/споживання системних ресурсів, відтворення дійсних комунікаційних одиниць тощо. Крім того, можна здійснювати пасивні атаки безпеки, такі як порушення конфіденційності важливої інформації або доступ до аналізу трафіку. Завдяки PENIOT всі ці операції можуть бути напівавтоматичними або навіть повністю автоматизованими. Однією з найважливіших особливостей PENIOT є можливість розширення. За замовчуванням він має кілька поширених протоколів IoT і численні атаки безпеки, пов’язані з цими протоколами.

ByteSweep (https://gitlab.com/bytesweep) – це безкоштовне програмне забезпечення для аналізу безпеки Інтернету речей. Ця платформа дозволяє виробникам пристроїв Інтернету речей проводити повністю автоматизовані перевірки безпеки перед постачанням мікропрограми. До недоліків цієї платформи слід віднести [19] недостатню активну екосистему, що не дозволяє платформі слідувати тенденціям розвитку інтернету речей. Зокрема, на gitlab її бібліотеки не поновлювалися понад рік. Незважаючи на переваги вільного програмного забезпечення, це ставить під сумнів ефективність аудиту IoT пристроїв.

AWS IoTDeviceDefender (https://aws.amazon.com/iot-device-defender) є найбільш потужним та налаштовуваним інструментом для аудиту пристроїв інтернету речей, базується на хмарному сервісі, не потребує розгортання в інфраструктурі користувача. Також AWS IoTDeviceDefender дозволяє проводити різноманітні аудити періодично, автоматично і незалежно від користувача, надсилаючи замовнику аудиту звіти про аудит та рекомендації з покращення безпеки. Саме через ці переваги для аудиту було обрано AWS IoTDeviceDefender.

1.4 Загальна характеристика IoTDeviceDefender

Оскільки використання підключених домашніх пристроїв продовжує зростати, все більше і більше даних передається в хмару, де новітні технології IoT і машинного навчання дають змогу впроваджувати нові інновації в додатках підключеного дому.

AWS IoT дозволяє легко створювати масштабовані програми IoT, які збирають, обробляють, аналізують та діють на основі даних, створених підключеними домашніми пристроями, без необхідності керувати будь-якою інфраструктурою. Це допоможе створити новий клас підключених домашніх додатків, які взаємодіють із фізичним світом.

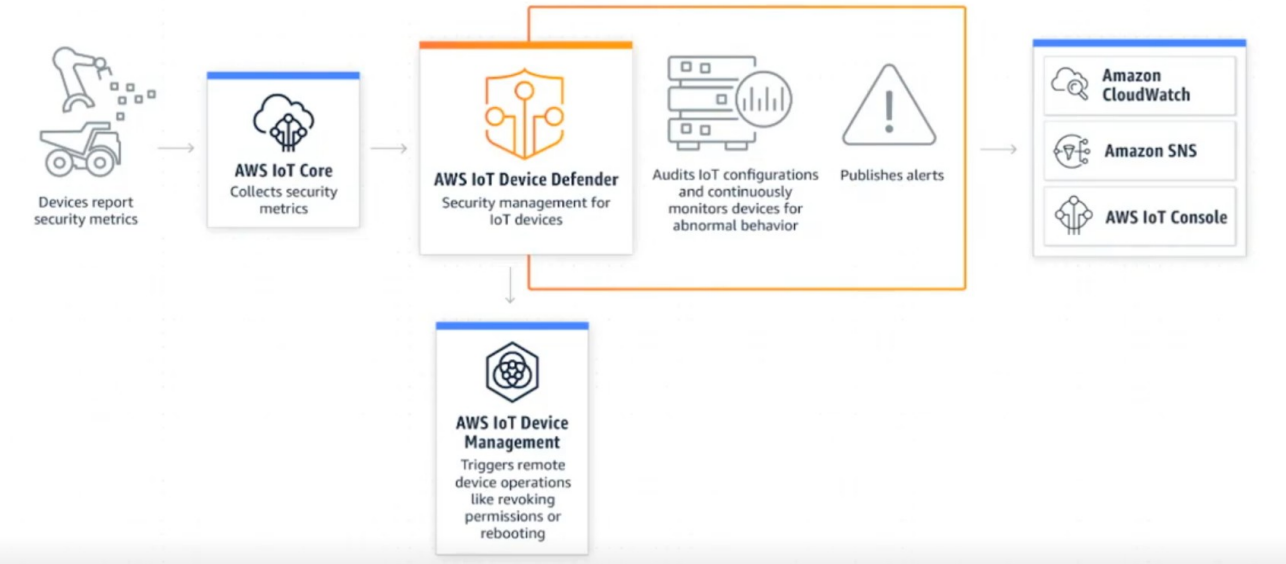


Рисунок 1.3 – Екосистема AWS IoTCore

AWS IoTDeviceDefender – це повністю керована служба, яка допомагає вам захистити ваш парк пристроїв IoT. AWS IoTDeviceDefender постійно перевіряє ваші конфігурації IoT, щоб переконатися, що вони не відхиляються від найкращих методів безпеки.

1.5 Постановка задачі

Оскільки проведення аудитів систем на основі пристроїв інтернету речей набуває все більшої актуальності, основними завданнями цієї роботи було визначено проведення аналізу AWS IoTDeviceDefender як засобу аудиту безпеки пристроїв інтернету речей та дослідити вплив повноти набору критеріїв на чутливість аудиту. Набір критеріїв повинен базуватися на проведеному аналізі основних вразливостей та критеріїв безпеки пристроїв інтернету речей. На основі отриманих результатів слід зробити висновки щодо переваг та недоліків обраного засобу для аудиту систем інтернету речей та розробити рекомендації з аудиту пристроїв IoT.

2 ТЕОРЕТИЧНІ ОСНОВИ АУДИТУ ЗАХИЩЕНОСТІ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Основні визначення та вимоги до аудиту інформаційних систем

Багато організацій вже почали впроваджувати IoT, тому нагальною необхідністю стає аудит пристроїв IoT, щоб забезпечити впевненість у тому, що ризики безпеки, пов’язані з IoT, контролюються належним чином. Захист інформації повинен запобігти можливим її витокам по різнонанітних каналах комунікації та блокуванню цих каналів, отже ця діяльність включає як встановлення можливості витоку інформації певними каналми, так і планування та проведення конкретних заходів з метою запобігання витоків. Відомості та дані, які підпадають під дію Закону України «Про інформацію», є об'єктом технічного захисту. Інформація – це актив, який є важливим для організації і, отже, потребує належного захисту [20]. До систем, в яких зберігається, обробляється чи передається чутлива інформація, застосовують методи тестування та моніторингу, які є змістом аудиту. Відповідно до стандарту ISO 27001, аудитом є систематичний, незалежний і документований процес для визначення ступеня виконання певних критеріїв. Для інформаційних систем, які включають пристрої IoT, цими критеріями, які повинні забезпечити конфіденційність, цілісність та доступність інформації, яка нележить кінцевому користувачу, є стійкість та контроль та усунення відомих вразливостей. Тестування та моніторинг належать до найважливіших заходів системи захисту інформації, які передбачають:

- неперервний аналіз технологій обробки та передавання інформації;
- виявлення загроз в режимі реального часу;
- збір, опрацювання, аналіз та відповідну реєстрацію даних аудиту;
- коригування конфігурації системи та її окремихелементів.

Безперервність захисту та дотримання кращих практик щодо конфігурування системи дозволяють мінімізувати ризики, які неможливо повністю усунути.

Процеси моніторингу та тестування щодо вразливостей безпеки включають:

- розробку ефективних методів, засобів та процедур тестування;
- розробка процедур та метрик для контролю якості системи захисту інформації;
- розробку або вибір –програмного забезпечення для тестування.

В ході аудиту обов'язково перевіряють:

- конфігурування системи;
- компоненти додатків, що можуть містити відомі вразливості;
- елементів контролю автентифікації та доступу до послуг IoT.

Методи аудиту повинні відповідати вимогам міжнародних стандартів, зокрема:

- ISO/IEC 27001:2018, який забезпечує підтримку рішень на основі бібліотек IT інфраструктури, зокрема в сфері IoT)
- COBIT (Задачі інформаційних і суміжних технологій) – відкритий IT-стандарт щодо аудиту IT та оптимізації IT-безпеки);
- ISO/IEC 27007:Guidelinesforinformationsecuritymanagementsystemsauditing.

Політики безпеки, пов'язані з пристоями IoT, повинні мінімізувати ризики безпеки та забезпечити неперервність бізнесу, який використовує пристрої IoT.

2.2 Обгрунтування вибору набору вразливостей, щодо яких здійснюється аудит

В якості програмної платформи для проведення аудиту пристроїв інтернету речей було обрано AmazonWebServices завдяки її налаштовуваності, комплексності та достатній універсальності. Аудит AWS IoTDeviceDefender перевіряє налаштування облікового запису та пристроїв IoT , щоб переконатися, що застосовуються найкращі методи безпеки, а ризики безпеки зведені до

мінімуму. Аудит застосовує попередньо визначені критерії пошуку, які відображають найкращі методи безпеки AWS IoT. Користувач може вибрати, які перевірки використовувати у конкретному обліковому записі для кожного конкретного запланованого аудиту. Наприклад, можна виявити, коли кілька пристроїв ідентифікаються за допомогою тих же облікових даних, використовуються надмірно лояльні політики або використовуються сертифікати, термін дії яких скоро закінчиться. Вмикати та вимикати перевірки можна на рівні облікового запису, проте рекомендовано задіювати усі перевірки, щоб гарантувати найкращі методи безпеки AWS.

Аудити можна запускати за потребою (аудити на вимогу) або планувати їх періодичний запуск (планові аудити). Коли ввімкнено одну або кілька перевірок, збір даних починається негайно. Час, який це займає, залежить від кількості пристроїв та кількості перевірок, що виконуються. Крім того, коли для облікового запису ввімкнено перевірки, автоматично створюється щоденна перевірка, яка переглядає всі ввімкнені перевірки.

На Рисунку 2.1 наведена діаграма, яка конкретизує процес аудиту. Служба DeviceDefender здійснює перевірку задіяних політик та налаштувань окремих пристроїв IoT та груп пристроїв, пормує звіт про аудит на надсилає його через консоль AWS IoTCore та службу повідомлень (якщо вона використовується) до користувача, який повинен змінити скомпрометовані політики. Відповідно до моделі SharedResponcibility, актуальність та відповідність політик та налаштувань IoT компонентів а також актуальність програмного забезпечення є компетенцією користувача. Виняток становлять політики, керовані AWS (так звані керовані, managedpolicies), зміни в яких застосовуються автоматично до всіх пристроїв, яким ці політики призначені.

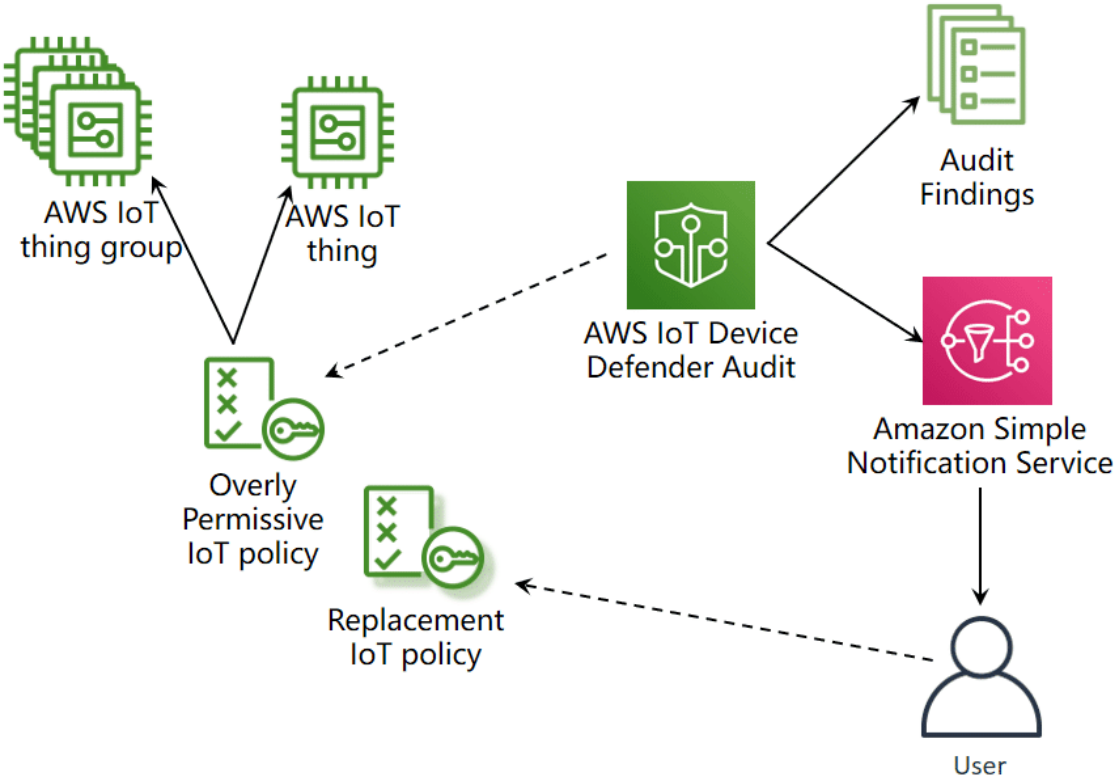


Рисунок 2.1– Ілюстрація послідовності аудиту AWS IoTDeviceDefender

Перевірки аудиту класифікуються за серйозністю як критичні, високого, середнього та низького ступеня ризику. Відповідно до завдань роботи ми виділимо перевірки критичних вразливостей та перевірки високого ступеня ризику та сформулюємо їх характерні ознаки а також способи запобігання.

Критичні:

- Аутентифікована роль має надмірний рівень прав доступу.
- Неавтентифікована роль має надмірний рівень прав доступу.
- Спільний сертифікат використовується кількома пристроями.
- Політика IoT надто лояльна.
- Відкликаний сертифікат пристрою все ще активний.

Високого рівня ризику:

- Спільний ідентифікатор використовується кількома пристроями.
- Аутентифікована роль має надмірний рівень прав доступу

Вважається, що політика для автентифікованої ролі надає надмірний дозвіл, коли вона надає дозвіл на керування або зміни стосовно пристроїв IoT, даних, не пов'язаних із пристроями, або ресурсів, не пов'язаних із пристроями. Також вважається надмірним, коли політика надає дозвіл на читання пов'язаних з пристроями адміністративних даних, змінення тіньових даних або змінення даних виконання завдань. Якщо автентифікованароль скомпрометована, вона може використовувати адміністративні дії, щоб змінити налаштування облікового запису, видалити ресурси або отримати доступ до конфіденційних даних. Політика, додана до аутентифікованої ролі пулу ідентифікаційних даних, має надавати лише ті дозволи, які необхідні для виконання роботи пристрою. Для нейтралізації цієї вразливості слід виконати такі дії:

1. Створити нову відповідну роль.

2. Створити пул ідентифікаційних даних і приєднати до нього відповідну роль.

3. Переконатися, що авторизовані користувачі мають доступ до AWS IoT за допомогою нового пулу.

4. Приєднати підтверджену роль до пулу ідентифікаційних даних , який було позначено як невідповідний.

Подібно, політика для неавтентифікованої ролі вважається надто дозволеною, коли вона надає дозвіл керувати або змінювати пристрої, дані, не пов'язані з пристроями, або ресурси, не пов'язані з пристроями. Також вважається надмірнимм, коли політика надає дозвіл на читання пов'язаних з пристроями адміністративних даних, змінення тіньових даних або змінення даних виконання завдань. Неавтентифікованікористувачі становлять більший ризик, ніж автентифіковані. Якщо неавтентифікований ідентифікатор скомпрометований і він має надмірно дозволену політику, він може використовувати свої дозволи, щоб скомпрометувати весь парк пристроїв або запустити розподілену атаку відмови в обслуговуванні (DDoS). Як вже було вказано, політика має надавати лише ті дозволи, які необхідні для виконання роботи пристрою. Для нейтралізації цієї вразливості слід виконати такі ж дії, як і щодо попередньої вразливості.

Варто підкреслити небезпечність ситуації, коли спільний сертифікат використовується кількома пристроями. Це відбувається, коли кілька одночасних підключень використовують один і той самий сертифікат X.509 для автентифікації за допомогою AWS IoT. Кожен пристрій повинен мати унікальний сертифікат для аутентифікації. Дотримуючись цієї найкращої практики, якщо кілька пристроїв використовують той самий сертифікат, це може означати, що пристрій зламано. Наприклад, його ідентифікатор міг бути клонований для подальшої компрометації системи. Для нейтралізації цієї вразливості слід переконатися, що сертифікат пристрою не зламано. Якщо так трапилося, слід

1. Надати нові та унікальні сертифікати та приєднати кожен сертифікат до окремого пристрою.

2. Переконатися, що нові сертифікати дійсні та пристрої можуть використовувати їх для підключення.

3. Використовувати UpdateCertificate, щоб позначити старий сертифікат як відключений в AWS IoT.

4. Від'єднати старий сертифікат від кожного з пристроїв.

Політика AWS IoT, яка надає занадто широкі або необмежені дозволи, не відповідає найкращій практиці найменших привілеїв [21]. Наприклад, політика може надавати дозвіл на надсилання або отримання повідомлень MQTT для широкого набору пристроїв. Загалом, політика IoT повинна надавати доступ лише до ресурсів, пов'язаних із цим пристроєм, і жодним іншим або до кількох інших пристроїв. За деякими винятками, використання символу підстановки (наприклад, *) для визначення ресурсів у такій політиці вважається занадто широким або необґрунтованим. Надмірно лояльна політика AWS IoT може вплинути на безпеку всього облікового запису. Зловмисник може використовувати такий широкий доступ для читання або зміни тіньових копій, завдань або стану виконання завдань для всіх пристроїв користувача. Крім того, зловмисник може використовувати скомпрометований сертифікат для підключення шкідливих пристроїв або запуску DDoS-атаки на мережу

користувача. Щоб виправити невідповідні правила, які прив'язані до пристроїв IoT, груп пристроїв або інших об'єктів, слід:

1. Використати CreatePolicyVersion , щоб створити нову, сумісну версію політики. Установити прапорець setAsDefault на true. Це робить цю нову версію доступною для всіх організацій, які використовують політику.

2. Використати CreatePolicyVersion ListTargetsForPolicy, щоб отримати список цілей (сертифікатів, груп речей), до яких прикріплено політику. Визначити, які пристрої входять до груп або які використовують сертифікати для підключення.

3. Переконатися, що всі пов'язані пристрої можуть підключатися до AWS IoT. Якщо пристрій не може підключитися, слід скористатися SetPolicyVersion, щоб відкотити політику за замовчуванням до попередньої версії, переглянути політику та повторити спробу.

Наступною критичною вразливістю є відкликаний сертифікат пристрою, який все ще є активним. Сертифікат пристрою зазвичай відкликається, оскільки він був зламаний. Цілком можливо, що його ще не було скасовано в AWS IoT через помилку чи недогляд. Тому треба перевірити, чи не зламано сертифікат пристрою. Якщо так, необхідно здійснити ту ж послідовність кроків, яка відповідає випадку, коли спільний сертифікат використовується кількома пристроями.

До вразливостей високого ступеня ризику належить та, коли спільний ID використовується кількома пристроями. Це відбувається, коли кілька пристроїв підключаються за допомогою одного ідентифікатора клієнта. Пристрої з конфліктуючими ідентифікаторами змушені постійно повторно підключатися, що може призвести до втрати повідомлень або до того, що пристрій не зможе підключитися. Це може означати, що пристрій або облікові дані пристрою були скомпрометовані і може бути частиною DdoS-атаки. Треба зареєструвати кожен пристрій як унікальний в AWS IoT і використовувати пристрою речі як ідентифікатор клієнта для підключення. Також можна використовувати універсальний унікальний ідентифікатор (UUID) як ідентифікатор клієнта під час підключення пристрою через MQTT.

Для системи, яка досліджується у цій кваліфікаційній роботі, доцільно зосередитися на таких вразливостях: спільний сертифікат використовується кількома пристроями, надмірно лояльні політики IoT, відкликаний сертифікат пристрою, який все ще є активним.

3 ПРАКТИЧНА ЧАСТИНА. ПЛАНУВАННЯ ТА ПРОВЕДЕННЯ АУДИТУ БЕЗПЕКИ ПРИСТРОЇВ IOT

3.1 Визначення обсягу та цілей аудиту безпеки пристроїв IoT

Плануючи використання AWS IoTDeviceDefender, необхідно слідувати найкращим практикам безпеки IoT:

- При наданні прав на будь-яку послугу або пристрій IoT дотримуватися принципу найменших привілеїв і надавати лише необхідні права.
- Де можливо, використовувати керовані політики AWS IAM. Застосовуючи цю практику, клієнтське рішення автоматично отримує оновлені дозволи, коли вдосконалення виходять для відповідної функціональної області.

Важливо постійно проводити аудит стосовно свогопарку IoT пристроїв, щоб гарантувати, що налаштування та заходи безпеки діють належним чином. Аудит AWS IoTDeviceDefender перевіряє налаштування облікового запису, ресурси Інтернету речей та активність пристрою. Аудит допомагає виявити будь-які розбіжності з найкращими методами безпеки або політиками доступу. Приклади критеріїв аудиту включають:

- Політики, які надають дозвіл на читання або оновлення даних на кількох пристроях.
- Пристрої, які мають спільну ідентифікацію (сертифікат X.509).
- Сертифікати, термін дії яких закінчується або були відкликані, але все ще активні та інші, перелічені в п. 2.2.

Консоль керування AWS IoTCore надає зручні інструменти для налаштування та відображення результатів аудитів безпеки. Крім графічного інтерфейсу користувача, можливе використання терміналу. Оскільки завданням роботи є дослідження можливостей платформи AWS та її засобу DeviceDefender стосовно полегшення прийняття рішень в галузі кібербезпеки, використаємо консоль користувача як більш візуальний інструмент придатний для ширшого кола користувачів.

3.2 Налаштування ролей та політик для дослідження

Кілька необхідних дозволів дозволяють AWS IoTDeviceDefender збирати дані, публікувати сповіщення та дозволяти обліковому запису виконувати команди аудиту. Щоб виконати будь-яку з цих дій, потрібно вказати роль IAM, яка включає політику дозволів і політику довіри. Під час використання керованої політики або створення дозволів через AWS ManagementConsole обидві політики створюються та об'єднуються в процесі створення ролі (ці ролі також можна створити через інтерфейс командного рядка, скориставшись командою UpdateAccountAuditConfiguration).

Для збору даних через AWS IoTDeviceDefender потрібно оновити дозволи аудиту облікового запису. Розроблена та наведена у Додатку А політика керованих дозволів надає AWS IoTDeviceDefender доступ до даних облікового запису під час аудиту. Політика довіри (Додаток Б) не потребує модифікацій і надає AWS IoTDeviceDefender дозволи на виконання необхідної ролі. На рисунках 3.1- 3.5 показані етапи налаштування ролей та політик для IoT пристроїв. При цьому, необхідно насамперед створити роль для сервісів AWS (Рисунок 3.1), надати необхідні дозволи (Рисунок 3.2). Опційно, можна встановити межі дозволів, щоб контролювати максимальні дозволи, які може мати певна роль. Це налаштування можна використовувати, щоб делегувати керування дозволами іншим. Слід наголосити що необґрунтоване надання дозволів може привести до компрометації системи. Наступним кроком, слід вказати назву аудиту, додати його опис, дозволи та теги (Рисунок 3.3), за допомогою яких можливий пошук, сегментування, більш детальний аналіз та тонке налаштування інструментарію аудиту безпеки пристроїв, підключених до AWS IoTCore.

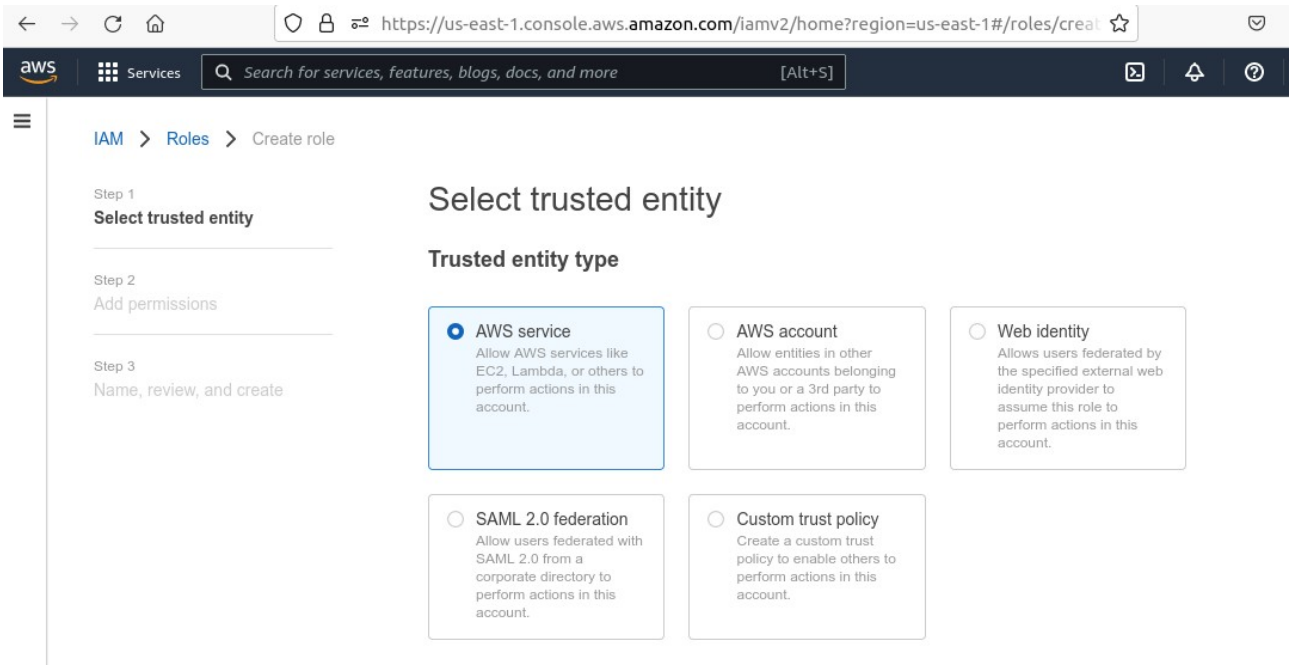


Рисунок 3.1 – Створення ролі для сервісів AWS

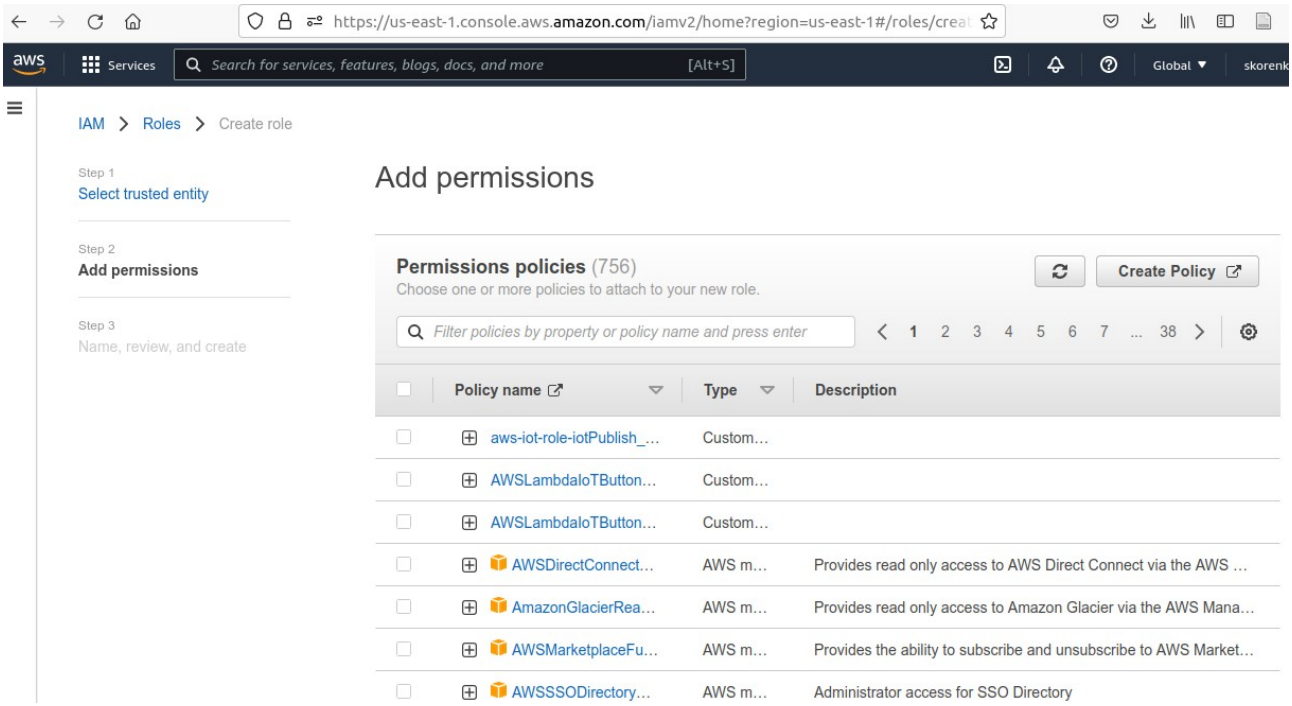
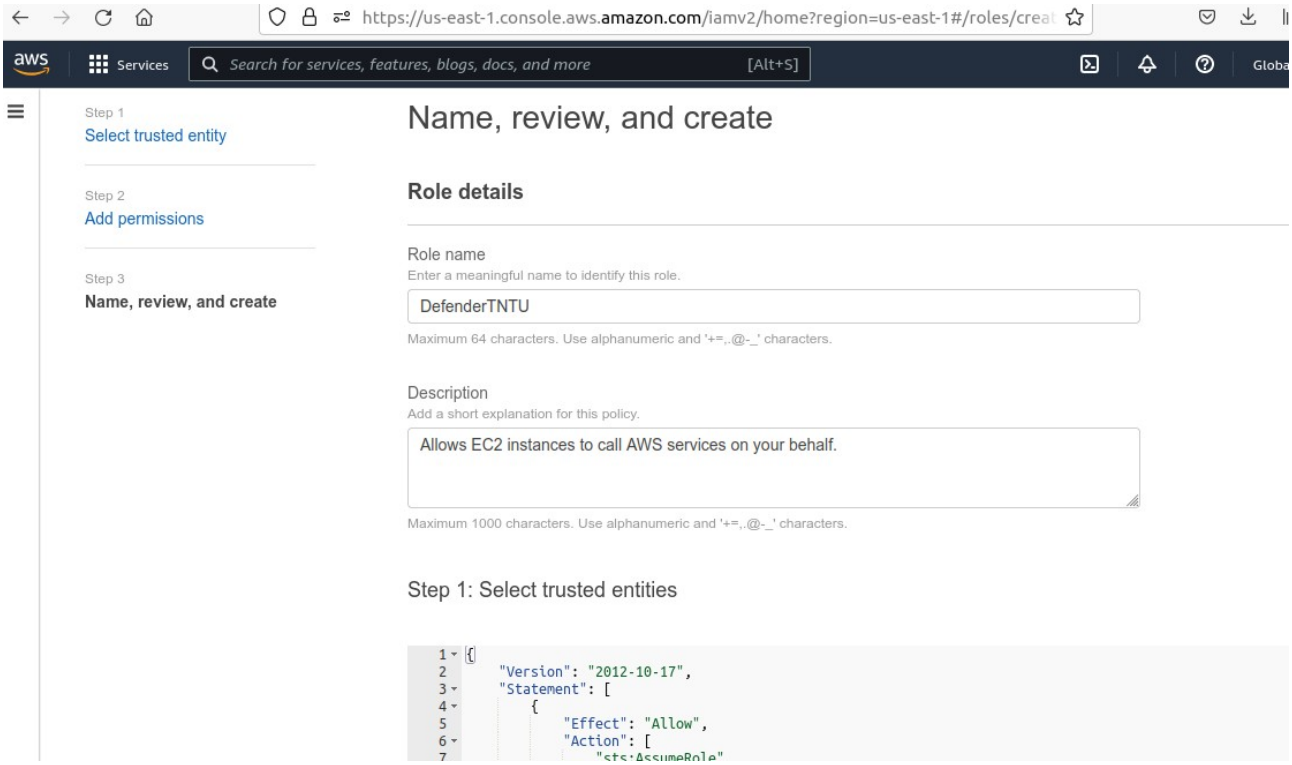


Рисунок 3.2 – Надання дозволів для сервісів AWS



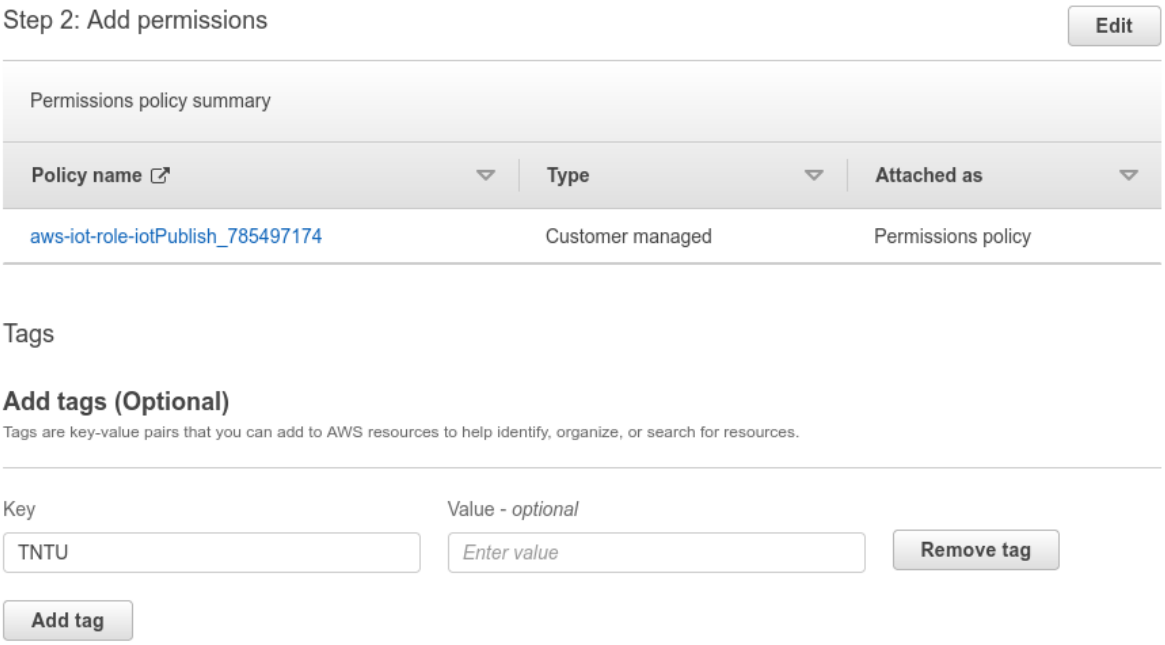


Рисунок 3.3 – Визначення атрибутів – ім’я, опис, дозволи та теги

Використовуючи менеджер доступу, слід приєднати політики безпеки (Рисунок 3.4) до конкретної системи (при цьому не важливо, чи до системи є

фізичний доступ — можна використовувати її віртуальний двійник — shadowthings).

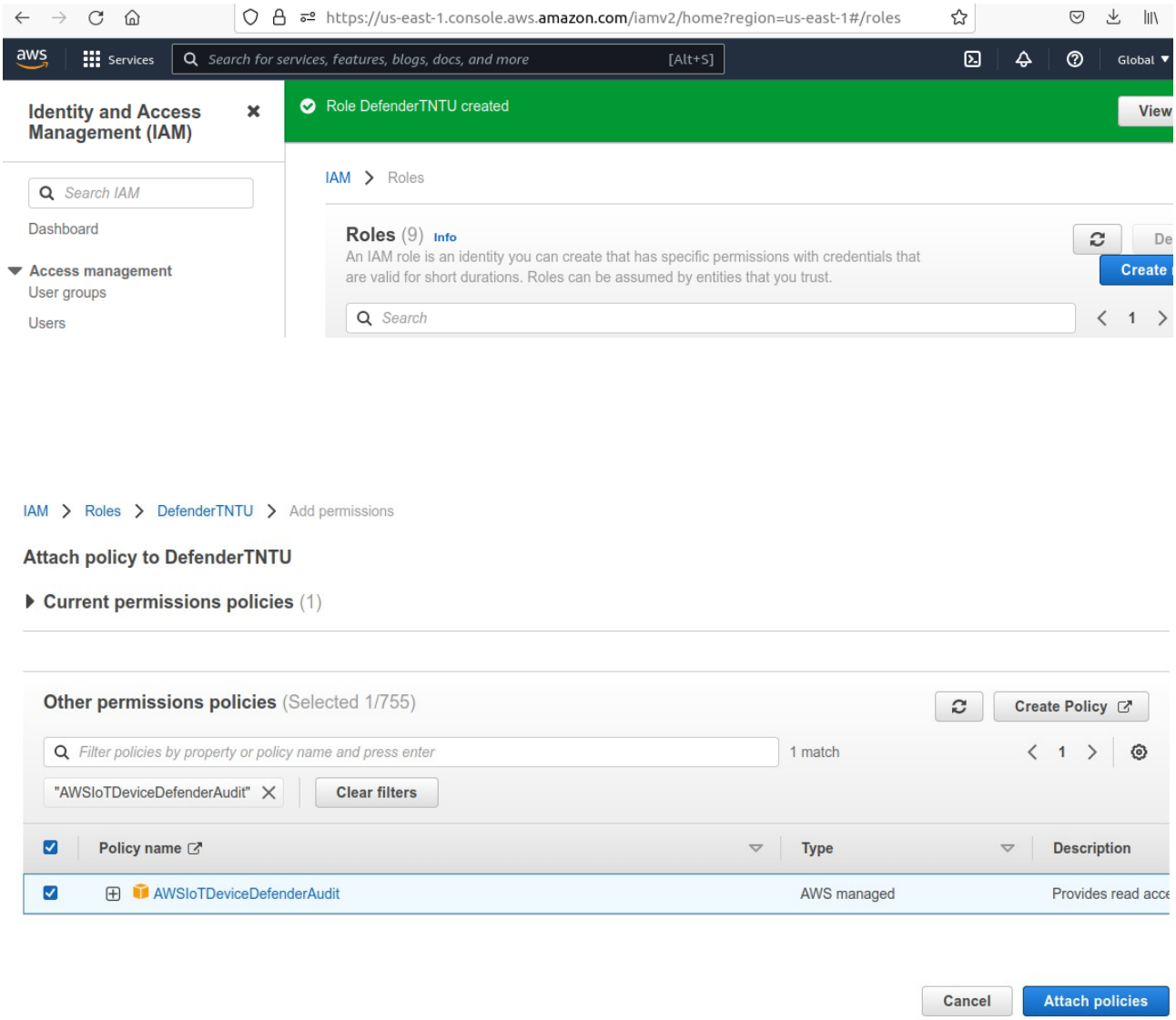


Рисунок 3.4 – Додавання політики безпеки

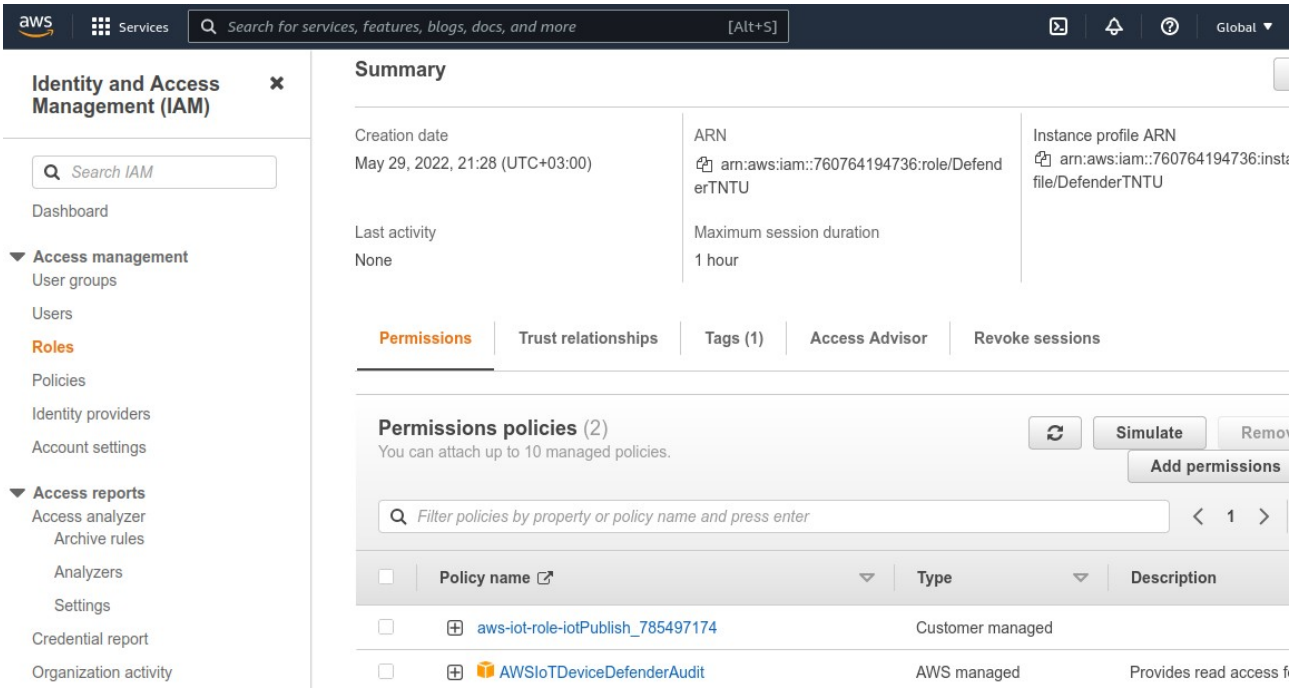


Рисунок 3.5 – Підтвердження статусу політики доступу

Після виконання цих процедур IAM роль створено, до неї приєднано політики, з них одна – керована AWS (Рисунок 3.5). Тепер слід надати дозволи клієнту IoT для запуску аудиту. Спочатку створимо політику яка дозволяє клієнту оновлювати конфігурацію акаунту. Для цього треба додати до політики додаткову інформацію – ID облікового запису та ARN ролі яка надає права цьому IoT клієнту для аудиту:

```
ID облікового запису  760764194***

arn:aws:iam::760764194***:role/DefenderTNTU
```

(останні цифри ідентифікатора облікового запису, використаного для дослідження, не відображені з міркувань приватності)

Варто від самого початку створювати кілька різних політик (в меню IAM >Policies через опцію “Створити політику”), щоб призначати їх для різних користувачів у майбутньому, навіть якщо на момент створення ці користувачі не парадбачені, для відповідності принципу найменших можливих прав. Друга політика буде стосуватися необхідних дозволів прав запиту для клієнта. Третя політика дозволить клієнту планувати та оновлювати графіки аудиту.

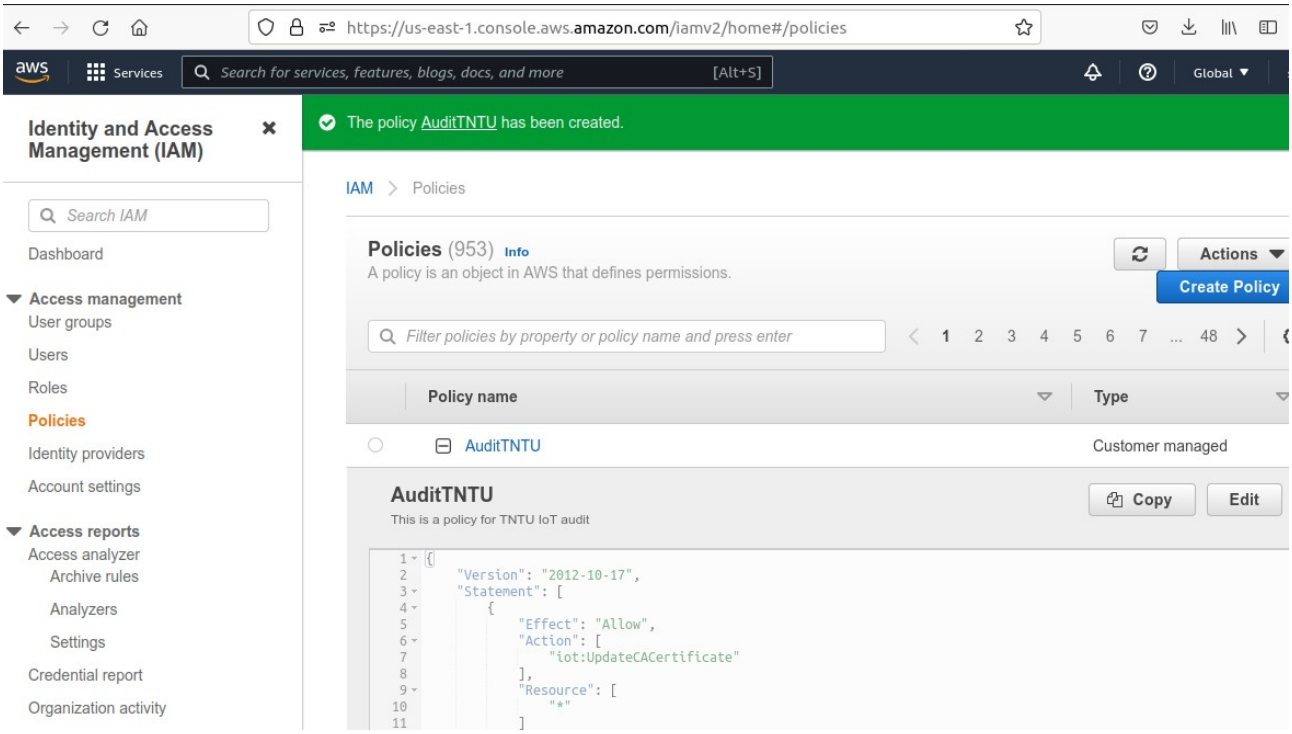


Рисунок 3.6 – Фіналізація створення політики

Аналогічно створюємо політики TNTU_IoTAuditConfigQuery та TNTUAuditSchedule.

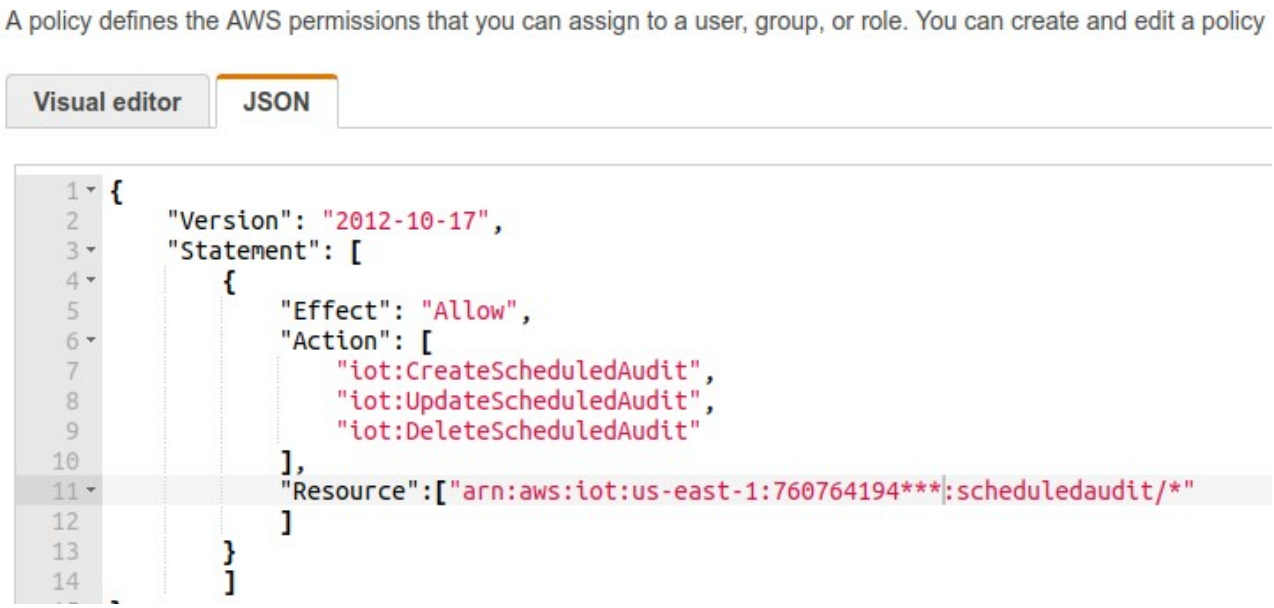


Рисунок 3.7– Редагування політики

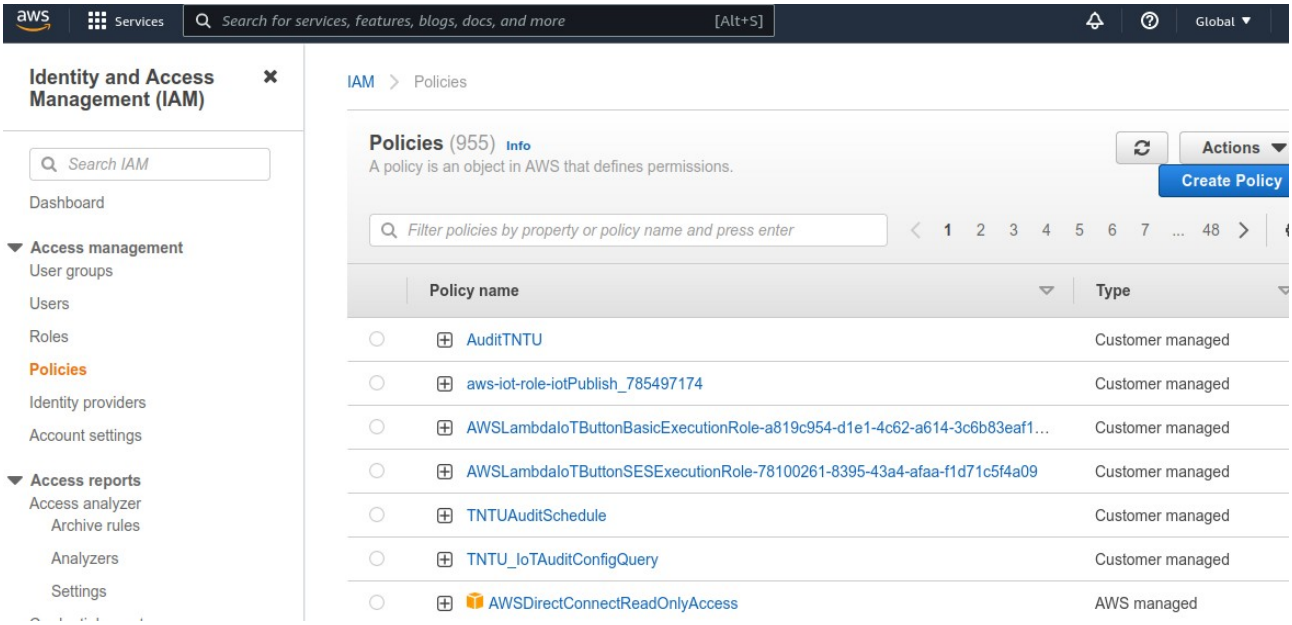


Рисунок 3.8 – Вибір політик

Наступним кроком слід застосувати політики до клієнта (Рисунок 3.9).

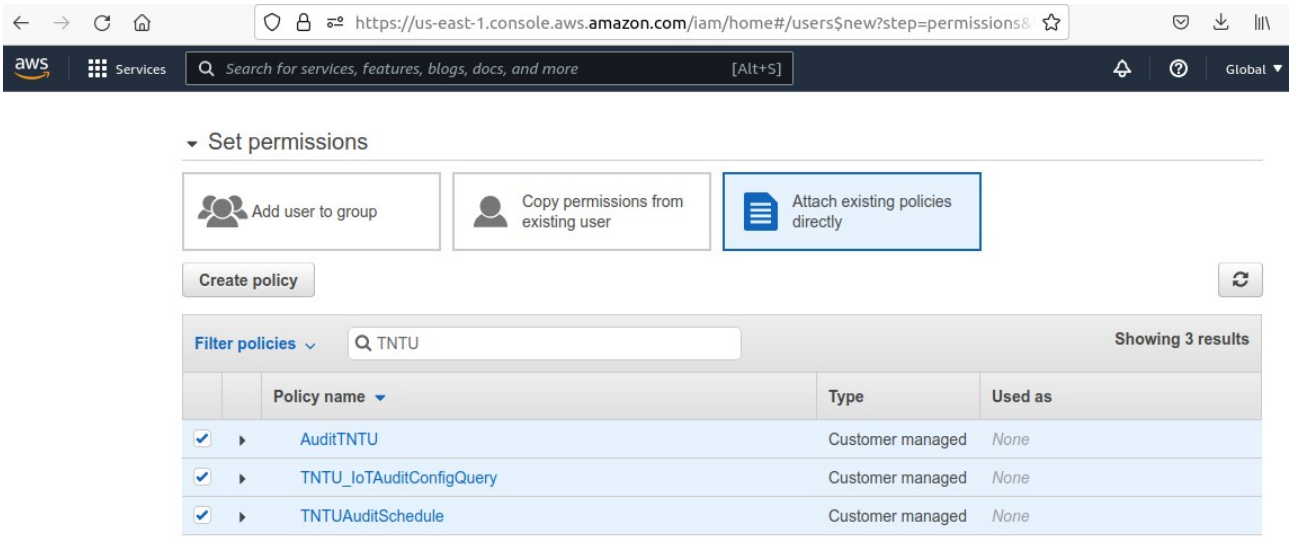


Рисунок 3.9 – Застосування політик

Всі три політики слід застосовувати лише до клієнта з адміністративними правами, для інших – відповідно до їх прав доступу.

Наступним кроком слід встановити параметри логування у IoTCore>Settings

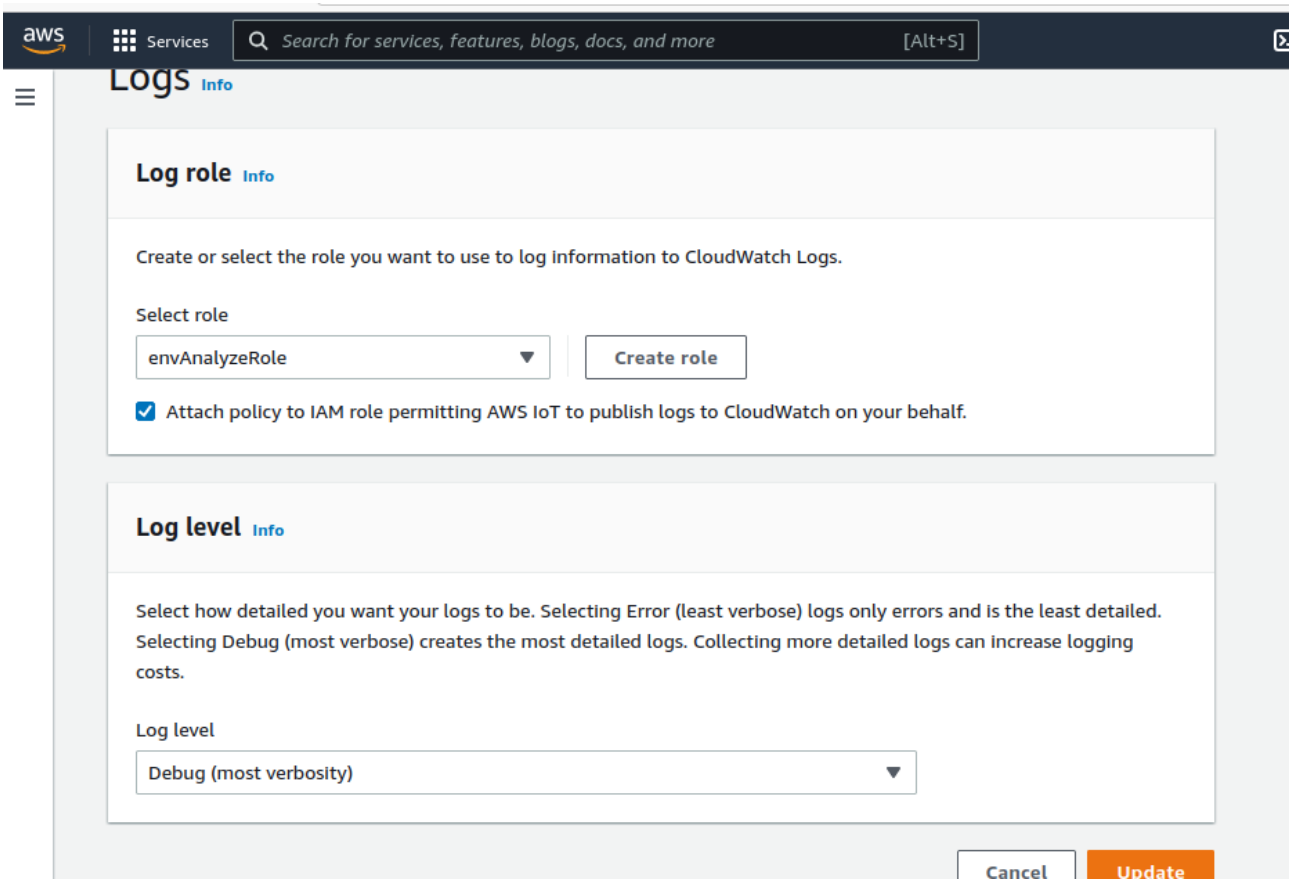


Рисунок 3.10 – Налагодження логування

Таким чином, мети досягнуто, необхідні політики створено, можна переходити до налаштування та проведення аудиту.

3.3 Проведення аудиту безпеки за допомогою IoTDeviceDefender

Для проведення аудиту безпеки налаштувань пристроїв IoT засобами AWS IoTDeviceDefenderслід перш за все вибрати типи аудиту (перевірки) у меню AWS IoT>DeviceDefender>Audit а також визначити роль, яка буде авторизована для проведення аудиту. В нашому випадку це буде роль AuditorIoT_TNTU, для якої визначимо (лістинги 3.1 та 3.2) наступні дозволи.

Лістинг 3.1 – Приклад налаштування дозволів для ролі аудитора

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "iot.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Лістинг 3.2 – Приклад налаштування довіреного доступу для ролі аудитора

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "iot:GetLoggingOptions",
                "iot:GetV2LoggingOptions",
                "iot:ListCACertificates",
                "iot:ListCertificates",
                "iot:DescribeCACertificate",
                "iot:DescribeCertificate",
                "iot:ListPolicies",
                "iot:GetPolicy",
                "iot:GetEffectivePolicies",
                "iot:ListRoleAliases",
                "iot:DescribeRoleAlias",
                "cognito-identity:GetIdentityPoolRoles",
```

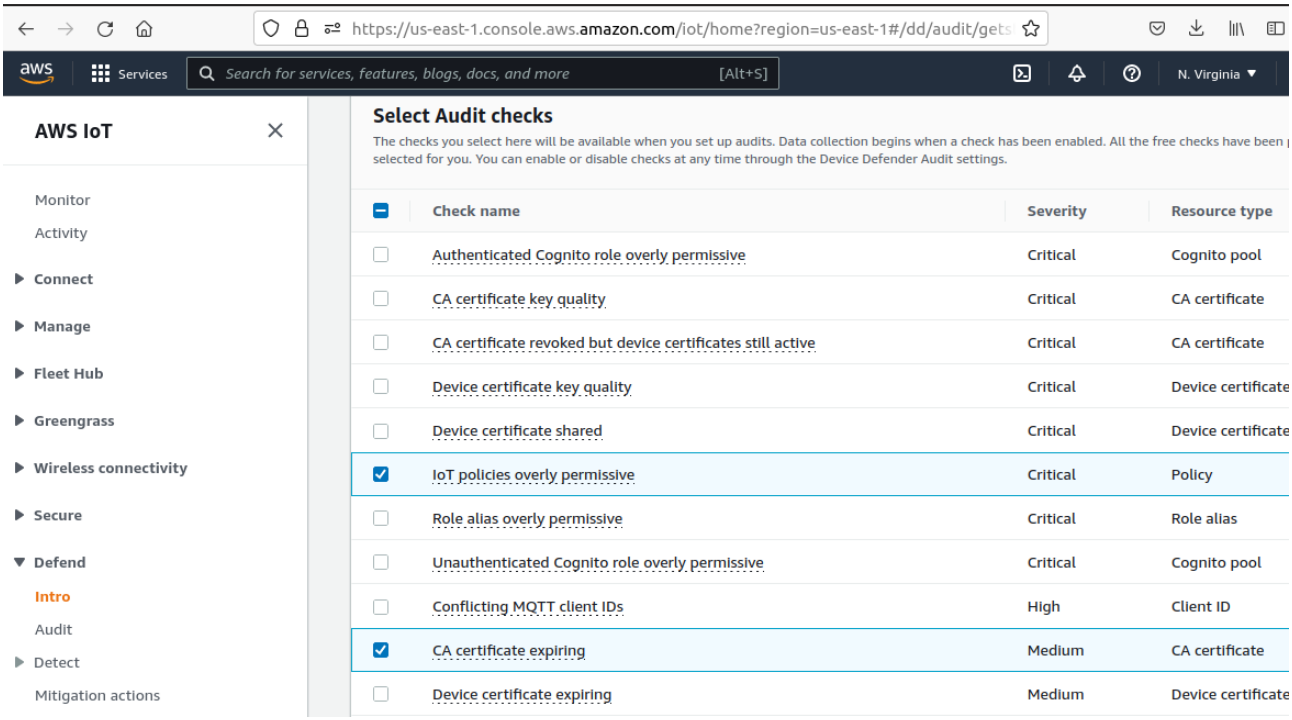


Рисунок 3.11– Інтерфейс для вибору перевірок аудиту

Аудит AWS IoTDeviceDefender перевіряє налаштування та політики, пов’язані з обліковим записом і пристроєм, щоб переконатися, що заходи безпеки діють належним чином. Аудит може допомогти вам виявити будь-які відхилення від політик налаштування доступу (наприклад, кілька пристроїв, які використовують той же ID, або надмірно ліберальні політики, які дозволяють одному пристрою читати й оновлювати дані для багатьох інших пристроїв). Аудит можна запускати за потребою (аудити на вимогу) або планувати їх періодичний запуск (планові аудити).

Аудит AWS IoTDeviceDefender виконує набір попередньо визначених перевірок для поширених найкращих методів безпеки IoT і вразливостей пристроїв. Приклади попередньо визначених перевірок включають політики, які надають дозвіл на читання або оновлення даних на кількох пристроях, пристроях, які мають спільну ідентифікацію (сертифікат X.509), або сертифікати, термін дії яких закінчується або були відкликані, але все ще активні.

Серйозність виявленої проблеми вказує на рівень занепокоєння, пов’язаний з кожним виявленим випадком невідповідності, і рекомендований час для усунення (Табл. 3.1).

Таблиця 3.1 – Рівнікритичностівразливостей вAWSIoT

Рівні	Опис
Critical	Проблеми, якіпотребуютьневідкладноїуваги. Критичніпроблеми часто дозволяютьзловмисникам без інсайдерськихзнаньчиспеціальнихобліковихданихотримати доступ до пристроївIoTабо контроль над ними.
High	Потребуютьтерміновогорозслідування та плануваннявиправленняпіслявирішеннякритичних проблем. Як і критичніпроблеми, проблемивисокогорівня часто надаютьзловмисникам доступ до пристроївIoTабо контроль над ними. Однакпроблемивисокоїсерйозності часто важчевикористовувати. Для них можутьзнадобитисяспеціальніінструменти, інсайдерськізнанняабоспеціальніналаштування.
Medium	Проблеми, які потребують уваги в рамках постійного підтримання стану безпеки. Проблеми середньої тяжкості можуть спричинити негативний вплив на роботу, наприклад, незаплановані відключення через несправність засобів контролю безпеки. Ці проблеми також можуть надавати зловмисникам обмежений доступ до IoT-пристроїв або контроль над ними або можуть сприяти частково їх зловмисним діям.
Low	Вказують на те, щоналаштуваннябезпекибулипропущеніабовиконанінедбало. Хоча вони самі по собіможуть не завдатинегайноговпливу на безпеку, цимипомилкамиможутьскористатисязловмисники.

	Як і проблемисередньоїтяжкості, проблеминизькогорівнявимагаютьуваги як частинипостійногопідтриманнябезпеки.

Налаштування параметрів запуску аудиту можна також виконати в режимі командного рядка. При цьому слід зважати на квоти, які впливають на розрахунок загальної вартості обслуговуванння облікового запису AWS.

Лістинг 3.3 – Виклик планувальника аудиту в CLI

```
aws iot create-scheduled-audit --frequency DAILY --target-check-
names DescribeAccountAuditConfiguration --scheduled-audit-name
AWSIoTDeviceDefenderDailyAudit
```

Залежно від кількості інформації, яка вважається корисною для відображення, можна налаштувати рівні реєстрації ведення журналів через AWS IoT, перелічені у Табл. 3.2

Таблиця 3.2 – Рівні реєстрації ведення журналів через AWSIoT

Рівні реєстрації	Опис
DISABLED	вказує на те, щовсіжурналивимкнено, а інформація не збирається через AmazonCloudWatch. Цезначеннязазамовчуваннямдля AWS IoT Core.
ERROR	Журналипомилокпоказують будь-яку помилку, яка спричиняєзбійоперації. Ціжурналивключатимутьлишеінформаціюпропомилку
WARN	Журнали попереджень показують все, що потенційно може спричинити невідповідність у системі, але не може призвести до збою операції. Ці журнали містять інформацію про помилки та попередження.
INFO	Інформаційніжурналипоказуютьінформаціювисокогорівня проперебіг речей. Ціжурналимістятьінформаціюпро ERROR, WARN та INFO.

DEBUG	Журналиналагодженняпоказуютьінформацію, яка може бути корисноюпід час налагодженняпроблеми. Ціжурналимістятьінформацію про ERROR, WARN, INFO та DEBUG.

Після завершення перевірки можна переглянути її результати. Якщо було налаштовано сповіщення Amazon SNS, то буде отримано push-повідомлення про завершення перевірки.

Можна також переглянути результати за допомогою консолі керування AWS або через командний рідок (термінал) AWS. Тут використано інтерфейс консолі (рисунок 3.12).

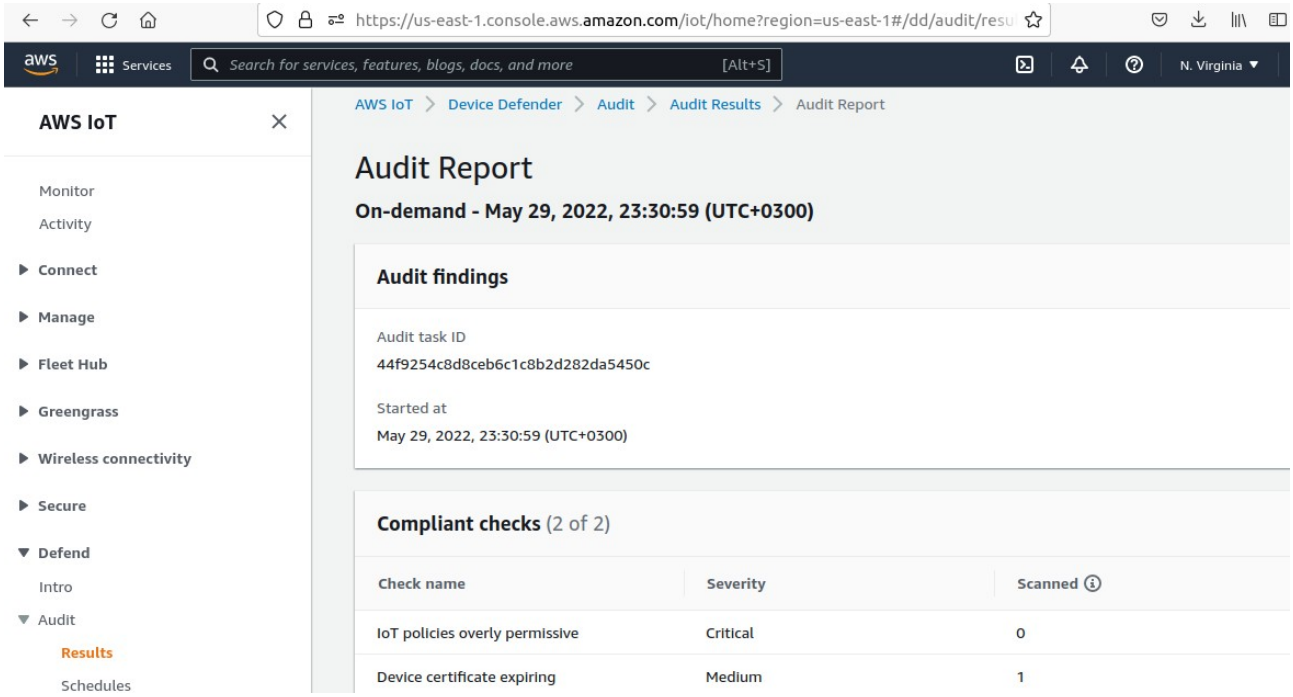


Рисунок 3.12– Звіт про перший аудит

Як бачимо, проведення аудиту з малою кількістю параметрів для перевірки не виявило жодних вразливостей. Змінимо набір критеріїв аудиту, використавши всі доступні опції, як показано на рисунку 3.13 та проведемо його повторно, для цього використаємо меню Audit>Schedules з параметром “Once (ondemand)”.

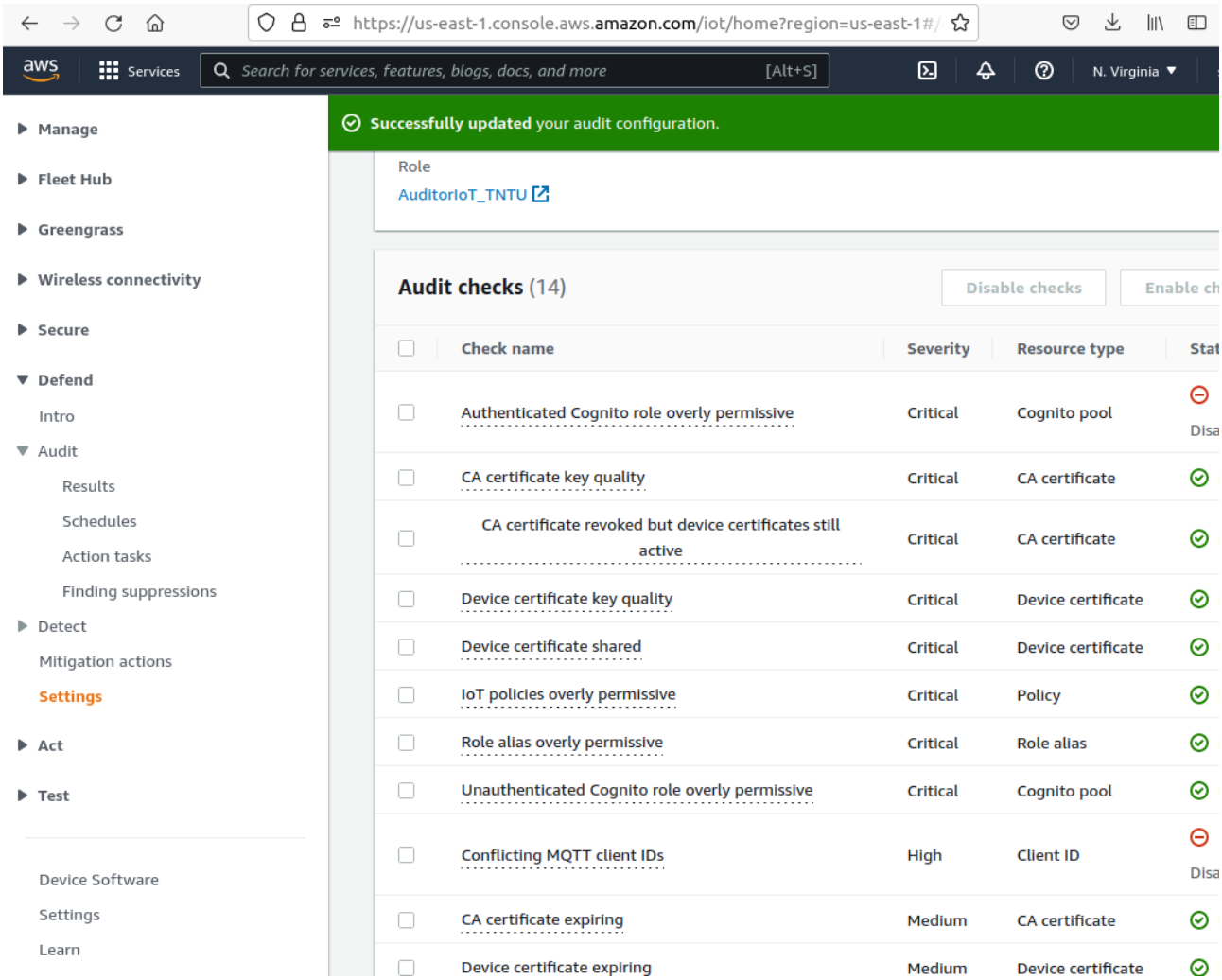


Рисунок 3.13– Зміна набору перевірок для більш детального аудиту

Загальна інформація про всі проведені аудити може бути отримана за допомогою вкладки “AuditResults” (Рисунок 3.14), а деталізовані звіти — за допомогою меню “AuditFindings” (Рисунки 3.15, 3.16).

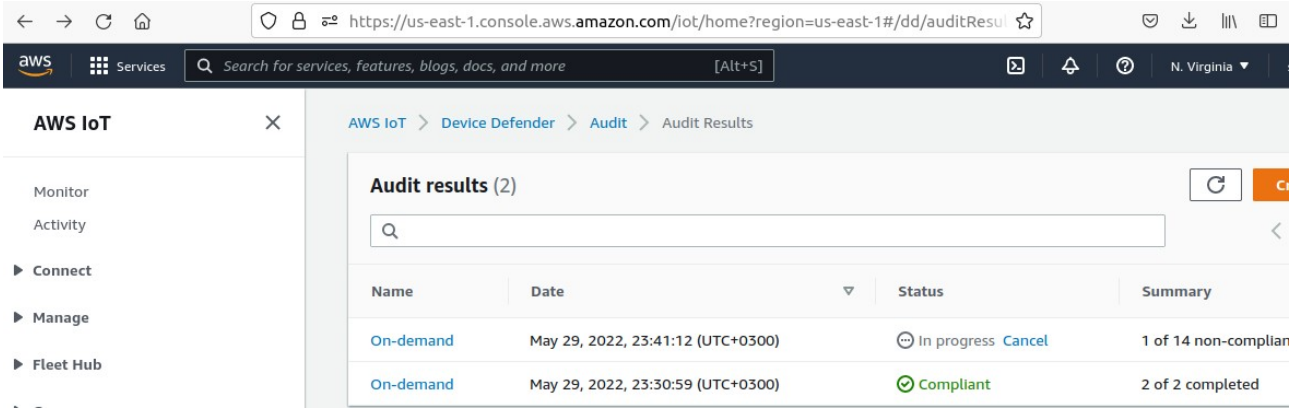


Рисунок 3.14– Зведена інформація про два проведені аудити

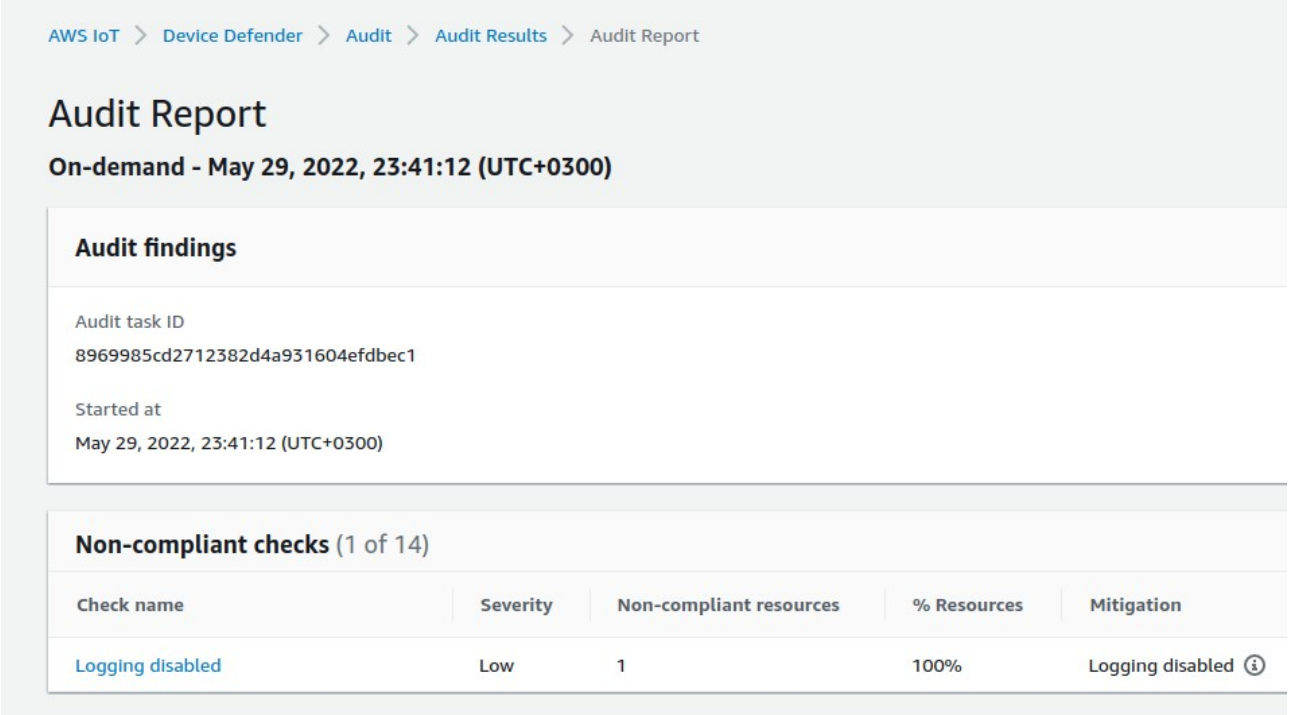


Рисунок 3.15– Звіт про повторний аудит

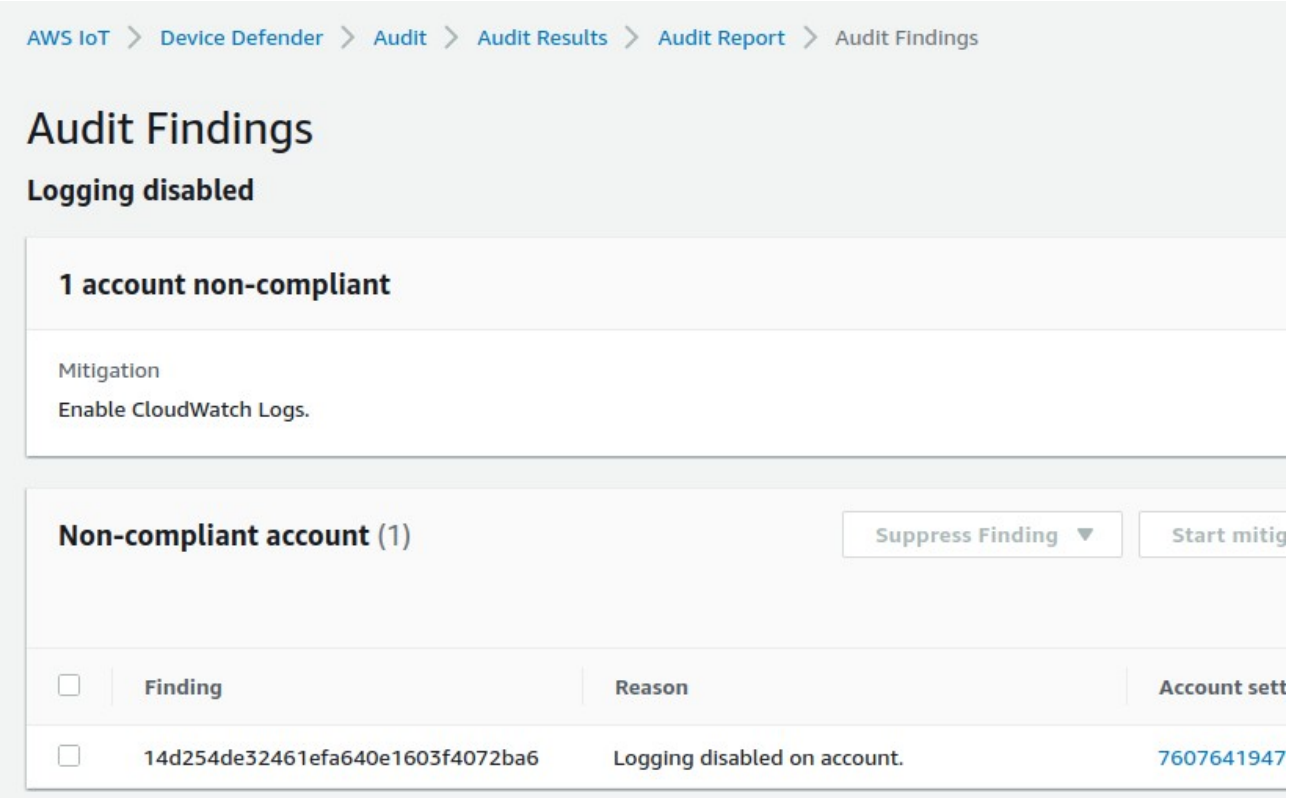


Рисунок 3.16– Результат повторного уадиту — знайдено вимкнене логування

3.4 Аналіз результатів аудиту та вибір найкращих практик

Повторний аудит, який проводився з більш широким (деталізованим) набором вразливостей для пошуку, показав недолік конфігурації, який полягає у відсутності налаштування системного журналу (Рисунок 3.16).

Отже політики були налаштовані відповідним чином а для облікового запису, використаного в дослідженні, слід передбачити ведення логів.

Плануючи та проводячи аудити з допомогою AWS IoTDeviceDefender, доцільно забезпечити дотримання кращих практик [14, 21]:

• Слід активувати всі доступні перевірки аудиту AWS IoTDeviceDefender та запускати аудит щодня.

• Варто увімкнити та відповідним чином налаштувати службу AmazonSimpleNotificationService, щоб отримувати сповіщення, коли перевірка аудиту завершена а її результати готові до перегляду.

• Слід переглядати результати аудиту щодня, щоб вчасно реагувати на нові ризики безпеки у своєму рішенні інтернету речей.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ХОРОНИ ПРАЦІ

4.1 Застосування ризик орієнтовного підходу для побудови структурно-логічних моделей виникнення надзвичайних ситуацій

Важливою характеристикою небезпеки є шкода — якісна або кількісна оцінка збитків, заподіяних небезпекою [22]. Кожний окремий елемент шкоди має своє кількісне вираження: чисельність загиблих, кількість поранених чи хворих, площа ураженої території, вартість пошкоджених транспортних засобів тощо. Універсальною одиницею виміру шкоди є збитки у грошовому еквіваленті. Небезпека сама по собі вказує лише на потенційну можливість спричинення шкоди. Для оцінки її імовірності та тяжкості прояву застосовують поняття ризику. Згідно з ДСТУ 2293-99 «ризик - це ймовірність заподіяння шкоди з урахуванням її тяжкості». Чисельно ризик визначається за формулою $R = PA$, деP - ймовірність виникнення небезпеки; A - очікуваний розмір шкоди (збитку), що,може завдати реалізована небезпека. Оскільки ймовірність - величина безрозмірна, ризик має вимірюватися в одиницях шкоди (збитку), заподіяної небезпекою.

Ризик-орієнтований підхід (РОП) у галузі безпеки ґрунтується на положенні, що будь-які небезпеки (у виробничій сфері, у повсякденному житті й побуті), незважаючи на їх різноманіття, мають однакову природу виникнення і однакову логіку розвитку подій. Основними завданнями РОП є створення наукових основ забезпечення надійності складних технічних систем для безпеки людей і довкілля, розроблення методів оцінювання ступеня небезпеки промислових об'єктів та наукових засад концепції прийнятного ризику. Зниження ризику наразитися на небезпеку потребує певних витрат і пов'язане з інвестуванням природної, техногенної та соціальної сфер. Залежність сумарного (технічний плюс соціально-економічний) ризику від загальних витрат суспільства на безпеку описується кривою, яка має мінімум у разі досягнення оптимального співвідношення між інвестиціями у природну, технічну й соціальну сфери. Зона прийнятного ризику знаходиться в межах мінімуму залежності сумарного ризику наразитися на небезпеку від загальних витрат суспільства, спрямованих на безпеку. Управління

ризиком полягає у пошуку компромісу між витратами на зменшення імовірності виникнення небезпечної події або збитку від неї і тією вигодою, яку приносить використання небезпечних технологій, матеріалів, продуктів тощо. Очікуване значення результату небезпечної (ризикованої) діяльності єсередньовиваженим усіх можливих результатів і розраховується за формулою $E = \sum P_i X_i$, де P_i , X_i, - відповідно ймовірність і значення і-го результату.

Основними складовими ризик орієнтованого підходу в питаннях управління безпекою [23] є процес порівняння існуючого ризику з припустимим (прийнятним), а також зроблені на підставі цього відповідні висновки та прийняті до виконання рішення. В якості основної методології РОП використовується відповідний аналіз безпеки та можливих витрат і збитків. Існує два шляхи встановлення гранично припустимого (прийнятного) ризику – це декларативний та обґрунтований. У разі декларативного підходу, значення припустимого (прийнятного) ризику встановлюється відповідно до нормативно- правових актів – законів, стандартів, правил, норм, якими визначені гранично допустимі (максимальні чи мінімальні) параметри певних шкідливих та небезпечних чинників. У разі обґрунтованого підходу, значення припустимого (прийнятного) ризику визначається шляхом порівняння окремих видів ризику з рівнями існуючих природних ризиків. Кінцеве значення оптимального гранично припустимого (прийнятного) ризику, як правило, корегується в процесі аналізу тих витрат, які необхідно нести для підтримання зазначеного рівня безпеки, а також в процесі порівняння цих витрат із можливими збитками із-за існуючих ризиків.

Жоден вид людської діяльності і жодна, особливо штучна, система не можуть гарантовано вважатися абсолютно безпечними, тобто вільними від ризику. Безпека є відносним поняттям, яка припускає, що в "безпечній системі" наявність чинників ризику вважається прийнятною ситуацією.

Фундаментальна база аналізу ризиків R(t) формується на основі досліджень в галузі соціальних, природних і технічних наук в трьох основних сферах життєдіяльності - соціальній (N), природній (S) і техногенній (T), що складають

єдину складну систему "людина-природа-середовище" (СЛПС), яка функціонує у часі t:

$$R(t)= Fr\{Rn(t), Rs(t), R_T(t)\}; \quad (4.1)$$

Узагальнена модель вказаної складної системи з визначенням ролі її основних компонентів N, S, T будується у величинах базових параметрів ризиків *R*(t) - ймовірності виникнення *P*(t) несприятливих процесів і подій (небезпек, викликів, загроз, криз, катастроф) і супутніх їм збитків U(t):

$$R(t) = Fr\ \{P(t), U(t)\} \quad (4.2)$$

$$P(t) = F_p\ \{R_N(t), Rs(t), Rt(t)\} \quad (4.3)$$

$$U(t) = Fu\ \{U_N(t), Us(t), Ut(t)\} \quad (4.4)$$

Сценарії несприятливих подій в складній системі і кількісна оцінка ризиків *R*(t) визначаються через параметри головних ініці-юючих і вражаючих чинників - потоки небезпечних енергій E(t), речовин W(t) і інформації I(t):

$$R(t)= Fr\ \{E(t), W(t), I(t)\}\ . \quad (4.5)$$

На основі співвідношень (4.1) - (4.5) по величинах ризиків *R*(t) фахівцями розробляються основи визначення категорій надзвичайних ситуацій, високоризикових об'єктів і небезпечних процесів.

Визнання неможливості уникнути ризику небезпек повністю обумовлює необхідність введення контролю ризику всіма досяжними засобами. Запровадження кількісних та якісних методів оцінки техногенних і природних ризиків є одним із стратегічних напрямів досягнення (наприклад, у державі) прийнятного рівня безпеки для населення, навколишнього природного середовища та об'єктів економіки. Концепція ризику, як системний підхід, дозволяє отримати з урахуванням заданого, і в той же час достатньо гнучкого алгоритму, та деталізованості всіх етапів аналізу, хоча не ідеальні, але достатньо ясні і адекватні результати, та, головне, в придатному для швидкого ухвалення управлінських рішень вигляді.

Об'єктами визначення ризиків є складні системи типу "люди-на-система-середовище", в яких враховуються впливи людського чинника, надійності системи, зовнішніх факторів небезпек на інтегральний рівень безпеки. В основі управління безпекою лежить системний підхід до виявлення джерел небезпеки і контролю чинників ризику на користь зведення до мінімуму людських жертв, матеріального збитку, а також фінансових, екологічних і соціальних втрат.

Крім вказаних необхідно використовувати для аналізу ризику (рівня безпеки) наступні принципи:

- принцип безумовного пріоритету безпеки і збереження здоров'я над будь-якими іншими елементами умов і якості життя членів суспільства;
- принцип прийнятного ризику (небезпеки), відповідно до якого встановлюються нижній (допустимий) і верхній (бажаний) рівні безпеки і в цьому інтервалі - прийнятний рівень ризику і безпеки з урахуванням соціально-економічних чинників;
- принцип мінімальної небезпеки, відповідно до якого рівень ризику встановлюється настільки низьким, наскільки він є реально досяжним;
- принцип послідовного наближення до абсолютної безпеки. Застосування показника ризику дозволяє порівнювати дію шкідливих та небезпечних чинників різної природи і різного виду, визначати з урахуванням внеску кожного окремого чинника інтегральний ступінь небезпеки будь-якого об'єкту, системи, технології, проекту, діяльності, процесу тощо.

Проводячи порівняння ризиків, наприклад, пов'язаних з промисловою діяльністю, з повсякденними побутовими ризиками, слід брати до уваги, що одні небезпеки приймаються суспільством добровільно (наприклад, проїзд на автомобілі), а інші - ні. Вельми важливо, що питання про сприйняття ризику істотно залежить від тих реальних вигод, які надає та або інша діяльність.

4.2 Соціальне значення охорони праці

Соціальне значення охорони праці полягає, насамперед, в сприянні росту ефективності суспільного виробництва шляхом безперервного вдосконалення і поліпшення умов праці, підвищення їх безпеки, зниження виробничого травматизму і профзахворювань [22, 23]. Соціальне значення охорони праці проявляється в зростанні продуктивності праці, збереженні трудових ресурсів і збільшенні сукупного національного продукту. Зростання продуктивності праці відбувається в результаті збільшення фонду робочого часу завдяки скороченню внутрішньо-змінних простоїв шляхом ліквідації мікротравм або зниження їх кількості, а також завдяки запобіганню передчасного стомлення шляхом раціоналізації і покращення умов праці та введенню оптимальних режимів праці і відпочинку та інших заходів, які Сприяють підвищенню ефективності використання робочого часу. Збереження трудових ресурсів і підвищення професійної активності працюючих відбувається завдяки покращенню стану здоров'я і подовженню середньої тривалості життя шляхом покращення умов праці, що супроводжується високою трудовою активністю і підвищенням виробничого стажу. Підвищується професійний рівень також завдяки зростанню кваліфікації і майстерності. Збільшення сукупного національного продукту відбувається завдяки покращенню перелічених показників та їх складових компонентів.

Ефективність заходів щодо поліпшення умов і охорони праці оцінюється, в першу чергу, за показниками соціальної ефективності, які передбачають створення умов праці, що відповідають санітарним нормам і вимогам правил безпеки. Покращення умов і охорони праці призводить до зменшення кількості виробничих травм, загальної і професійної захворюваності; до скорочення чисельності працівників, що працюють в умовах, які не відповідають санітарно-гігієнічним нормам; зменшення кількості випадків виходу на пенсію за інвалідністю внаслідок травматизму чи професійної захворюваності; скорочення плинності кадрів через незадовільні умови праці тощо. Соціально-економічна ефективність розраховується з метою:

- економічного обґрунтування планових заходів, необхідних для вибору оптимальних варіантів технологічних, ергономічних та організаційних рішень;

- визначення фактичної ефективності заходів щодо поліпшення умов і охорони праці; - оцінки результатів управління виробництвом на різних рівнях;

- розрахунку необхідних витрат для приведення умов праці на робочих місцях у відповідність до нормативних вимог;

- визначення раціональних розмірів матеріального стимулювання працівників підприємства, науково-дослідних, конструкторських і проектних організацій за розробку і запровадження працеохоронних заходів.

Оцінка соціально-економічної ефективності працеохоронних заходів здійснюється на підприємствах усіх форм власності, у тому числі на робочому місці, дільниці, в цеху Вона може визначатися також по галузі та в державі в цілому. Показники соціальної і соціально-економічної ефективності розраховуються як відношення величин соціальних або соціально-економічних результатів до витрат, необхідних для їх здійснення. Такі показники характеризують кількість умовних одиниць сукупного об'єму соціального чи соціально-економічного результату в розрахунку на одиницю витрат. Показники соціальної і соціально-економічної ефективності використовуються для визначення фактичного рівня питомих витрат, необхідних для зменшення кількості працюючих у незадовільних умовах, зниження рівня травматизму, захворюваності, плинності кадрів на різних підприємствах та в економіці в цілому. Оцінювати економічні аспекти охорони праці слід за допомогою методів оцінки соціальної й економічної ефективності заходів по створенню умов праці, що відповідають чинним нормативним актам з охорони праці.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи було проведено літературний аналіз джерел в галузі аудиту захищеності пристроїв інтернету речей та виділено ключові вразливості, стосовно яких повинен проводитися періодичний аудит, щоб забезпечити конфіденційність, цілісність та доступність інформаційних ресурсів організації. Було проведено порівняльний аналіз сучасних програмних засобів, як безкоштовних із відкритим кодом, так і доступних на умовах підписки, виявлено їх переваги та недоліки й обрано засіб для проведення аудиту системи на основі IoT.

З метою реалізації програми аудиту захищеності в роботі:

- проведено вибір та формування набору вразливостей, стосовно яких проводити аудит критично важливо;
- сформовано типові політики доступу для системи IoT пристроїв;
- проаналізовано сучасні засоби аудиту безпеки інтернету речей;
- обрано засіб та розроблено методику аудиту захищеності системи;
- досліджено вплив повноти набору критеріїв на чутливість аудиту;
- на основі аналізу результатів аудиту обрано кращі практики налаштування конфігурації пристроїв інтернету речей.

Крім цього, в роботі у розділі "Безпека життєдіяльності, основи охорони праці" описано застосування ризик-орієнтованого підходу до побудови імовірнісних структурно-логічних моделей виникнення та розвитку надзвичайних ситуацій а також соціальне значення хорони праці.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. N. Zagorodna, I. Kramar. Economics, Business and Security: Review of Relations. Business Risk in Changing Dynamics of Global Village BRCDGV-2020: Monograph / Edited by Pradeep Kumar, Mahammad Sharif. India, Patna: Novelty&Co., AshokRajpath, 446 p., pp.25-39, 2020.

2. Y. Skorenkyy, R. Kozak, N. Zagorodna, O. Kramar, I. Baran. Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. Journal of Physics: Conference Series, Vol. 1840, Issue 1, 012026, 2021.

3. O. Kramar, Y. Drohobytskiy, Y. Skorenkyy, O. Rokitskyi, N. Kunanets, V. Pasichnyk, O. Matsiuk. Augmented Reality-assisted Cyber-Physical Systems of Smart University Campus. 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 - Proceedings : Institute of Electrical and Electronics Engineers Inc., Vol. 2, pp. 309-313, 2020.

4. GSM AssociationOfficialDocument CLP.11 - IoTSecurityGuidelinesOverviewDocument, 53p., 2020. [Електроннийресурс] – Режим доступу до ресурсу: https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf

5. I. Bodnarchuk, O. Duda, O. Matsiuk, N. Kunanets, V. Pasichnyk. Choicemethodofanalyticalplatformforsmartcities. CEUR WorkshopProceedings, 2732, pp. 116-127, 2020.

6. A. Kharchenko, I. Halay, N. Zagorodna, I. Bodnarchuk. Optimization of software architecture selection for the system under design and reengineering. 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 - Proceedings, pp. 1245–1248, 2018.

7. Y. Drohobytskiy, V. Brevus, Y. Skorenkyy. Spark structured streaming: Customizing kafka stream processing. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 9204304, pp. 296-299, 2020.

8. P. Vervierand Y. Shen, Beforetoastersriseup: A viewintotheemergingIoTthreatlandscape,Proceedingsofthe 21th InternationalSymposiumonResearchinAttacks, IntrusionsandDefenses, pp. 556–576, 2018.

9. CreatingsecureIoTdeviceidentities. WhitePaper, Intertrust Technologies Corporation, 15 p., 2021. [Електроннийресурс] – Режим доступу до ресурсу: https://www.intertrust.com/pki-for-iot/

11. C. Baudoin, E. Bournival, E. Clauer. GlobalIndustryStandardsforIndustrialIoTAnIndustrialInternetConsortiumWhitePaper. [Електроннийресурс] – Режим доступу до ресурсу: https://www.iiconsortium.org/pdf/IIC_Global_Standards_Strategy_Whitepaper.pdf

12. T. Kamiya, A. Kolesnikov, B. Murphy, K. Watson, N. Widell. CharacteristicsofIIoTInformationModelsAnIndustrialInternetConsortiumWhitePaper. [Електроннийресурс] – Режим доступу до ресурсу: https://www.iiconsortium.org/pdf/Characteristics-of-IIoT-Information-Models.pdf

13. S. Carielli, M. Eble, F. Hirsch, E. Rudina, R. Zahavi. IoTSecurityMaturityModel (SMM): DescriptionandIntendedUseAnIndustrialInternetConsortiumWhitePaper. 2020. [Електроннийресурс] – Режим доступу до ресурсу: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf

14. TheOpenWebApplicationSecurity Project (OWASP). IoTSecurityGuidance. [Електронний ресурс] – Режим доступу до ресурсу: https://www.owasp.org/index.php/IoT_Security_Guidance

15. GSM Association. IoTSecurityAssessment, [Електронний ресурс] – Режим доступу до ресурсу: https://www.gsma.com/iot/iot-security-assessment/

16. I. Cooke. AuditingDataPrivacy.ISACA Journal, Vol. 3, 2018. [Електроннийресурс] – Режим доступу до ресурсу: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/is-audit-basics-auditing-data-privacy.

17. S. Majumdar, D. Bastos, A. Singhal. Securityauditingofinternetofthingsdevicesin a smarthome. In: Peterson, G., Shenoi, S. (eds) AdvancesinDigitalForensics XVII. DigitalForensics 2021. IFIP AdvancesinInformationandCommunicationTechnology, Vol. 612, 2021. Springer, Cham. [Електронний ресурс] – Режим доступу до ресурсу: https://doi.org/10.1007/978-3-030-88381-2_11

18. SecurityAuditToolsforIoT – Introduction[Електронний ресурс] – Режим доступу до ресурсу: https://www.kics.edu.pk/project/index/260]

19. bytesweep-old | A FreeSoftwareIoTFirmwareSecurityAnalysisPlatform[Електроннийресурс] – Режимдоступудоресурсу:https://kandi.openweaver.com/shell/bytesweep/bytesweep-old

20. International StandardISO/IEC 27000:2018.Informationtechnology — Securitytechniques — Informationsecuritymanagementsystems — Overviewandvocabulary, 2018, 34 p.[Електроннийресурс] – Режимдоступудоресурсу: https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf

21. C. Bellman, P. vanOorschot. BestpracticesforIoTsecurity: Whatdoesthatevenmean? arXiv: 2004.12179, 2020. [Електроннийресурс] – Режим доступу до ресурсу: https://arxiv.org/abs/2004.12179

22. Я.І. Бедрій Безпека життєдіяльності: Навч.посібн. – К.: Вид-во Кондор, 2009.

23. В.П. Цапко Безпека життєдіяльності: Навч.посібн. – К.: Знання-Прес, 2003.

ДОДАТКИ

ДОДАТОКА. ПОЛІТИКА ДОЗВОЛІВ


```
{
 "Version":"2012-10-17",
 "Statement":[
   {
    "Effect":"Allow",
    "Action":[
       "iot:GetLoggingOptions",
       "iot:GetV2LoggingOptions",
       "iot:ListCACertificates",
       "iot:ListCertificates",
       "iot:DescribeCACertificate",
       "iot:DescribeCertificate",
       "iot:ListPolicies",
       "iot:GetPolicy",
       "iot:GetEffectivePolicies",
      "iot:DescribeAccountAuditConfiguration",
       "iot:DeleteAccountAuditConfiguration",
       "iot:StartOnDemandAuditTask",
       "iot:CreateScheduledAudit",
       "iot:UpdateScheduledAudit",
       "iot:DeleteScheduledAudit",
       "iot:CancelAuditTask",
       "iot:DescribeAuditTask",
       "iot:ListAuditTasks",
       "iot:ListAuditFindings",
       "iam:ListRolePolicies",
       "iam:ListAttachedRolePolicies",
       "iam:GetPolicy",
        "iam:GetRolePolicy"
    ],
    "Resource":[
        "arn:aws:iot:region:account-id:scheduledaudit/scheduled-audit-name"
    ]
   }
 ]
}
```

ДОДАТОКБ. ПОЛІТИКА ДОВІРИ

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```