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)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Розробка системи безпеки для IoT з використанням SIEM технологій

Виконав: студент VI курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) *Маслій Р.Б.* (прізвище та ініціали)

Керівник (підпис) *Скарга-Бандурова І.С.* (прізвище та ініціали)

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

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

Рецензент (підпис) (прізвище та ініціали)

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 Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Маслію Ростиславу Богдановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка системи безпеки для IoT з використанням SIEM технологій

Керівник роботи Скарга-Бандурова Інна Сергіївна, д.т.н., проф., проф. кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_25_» _листопада__ 2022 року № _4/7-966_____

2. Термін подання студентом завершеної роботи 14 грудня 2022р.

3. Вихідні дані до роботи Наукові публікації про загрози хмарної безпеки та проблем безпеки хмарних середовищ

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ, 1 Аналіз предметної області та постановка задачі , 1.1 Аналіз стану безпеки IoT систем, 1.2 Архітектура IoT систем, 1.3 Технології зв'язку та проколи обміну даними, 1.4 Висновок до першого розділу, 2 Дослідження технологій управління інформаційною безпекою, 2.1 Аналіз архітектури SIEM – технології, 2.2 Splunk, 2.3 McAfee Enterprise Security Manager, 2.4 IBM QRadar, 2.5 Elastic Stack 2.6 Висновок до другого розділу, 3 Розробка системи безпеки для IoT з використанням SIEM технологій, 3.1 Особливості управління інформаційною безпекою для IoT систем, 3.2 Розгортання SIEM-рішення, 3.3 Тестування системи безпека SIEM для IoT за допомогою Elastic 3.4 Висновок до третього розділу
4 Охорона праці та безпека в надзвичайних ситуаціях
4.1 Охорона праці, 4.2 Безпека в надзвичайних ситуаціях, Висновки, Перелік використаних джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., старший викладач з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 14 листопада 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	14.11.2022-15.11.2022	*Виконано*
2.	Підбір наукових джерел про мережу інтернет речей	16.11.2022-20.11.2022	*Виконано*
3.	Переклад та опрацювання наукових джерел про		
	захист мережі інтернету речей	21.11.2022-23.11.2022	*Виконано*
4.	Виконання дослідження щодо аналіз інструментів для		
	організації інфраструктури та безпеки системи IoT	24.11.2022-27.11.2022	*Виконано*
5.	Оформлення розділу «Аналіз предметної області та		
	постановка задачі»	28.11.2022-30.11.2022	*Виконано*
6.	Оформлення розділу «Дослідження технологій		
	управління інформаційною безпекою»	01.12.2022-04.12.2022	*Виконано*
7.	Оформлення розділу «Розробка системи безпеки для	05.12.2022-07.12.2022	*Виконано*
	IoT з використанням SIEM технологій»		
8.	Виконання завдання до підрозділу «Охорона праці»	08.12.2022-09.12.2022	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чай них ситуаціях»	10.12.2022-11.12.2022	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2022-13.12.2022	*Виконано*
11.	Нормоконтроль	14.12.2022-15.12.2022	*Виконано*
12.	Перевірка на плагіат	9.12.2022	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.12.2022	*Виконано*
14.	Захист кваліфікаційної роботи	.12.2022	

Студент _____ Маслій Р.Б.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Скарга-Бандурова І.С
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка системи безпеки для IoT з використанням SIEM технологій // Qualification work of the educational level “Master” Degree Thesis // Маслій Ростислав Богданович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2022 // С. 58, рис. – 20, табл. – 4, додат. – 1, бібліогр. – 28.

Ключові слова: СИСТЕМА БЕЗПЕКИ, МЕРЕЖА ІНТЕРНЕТУ РЕЧЕЙ, SIEM, IOT, ТЕХНОЛОГІЯ

Метою роботи є дослідження технологій управління інформаційною безпекою та розробка системи безпеки для IoT на підставі SIEM технології.

Основні результати роботи: досліджено площу діяльності новітніх IoT пристроїв та їх передачу даних через проколи, що в свою чергу дозволило краще визначити переваги та недоліки для розробки власної системи. Проаналізовано декілька технологій управління інформаційної безпекою, серед доступних на ринку. Аналіз проводився в першу чергу, для того, щоб обрати підходящу систему для конкретних пристроїв та обслуговування системи було дешевим і водночас якісним порівняно з конкурентами. На підставі проведеного досліження створено безпеки для IoT за допомогою Elastic Stack SIEM.

У першому розділі описується сучасний стан безпеки IoT систем, а також технологій зв’язку, протоколів передачі даних та архітектуру IoT систем.

У другому розділі проаналізовано найбільш актуальні SIEM системи, описано їхні недоліки та переваги.

Третій розділ – практична частина. У ньому описано деталі розробки системи безпеки пристроїв мережі Інтернет речей. Система здатна самостійно аналізувати та сповіщати користувача про події, які можуть загрожувати безпеці. Завдяки цьому моніторингу, можливо швидко реагувати на інциденти та побачити їх у вигляді візуалізації на панелі адміністратора мереж.

У четвертому розділі описано інструкції з охорони праці при роботі з комп’ютером та фактори виробничого середовища і їх вплив на життєдіяльність людини.

В розділі " Безпека в надзвичайних ситуаціях " описано питання здоров’я працівників,додано поради щодо його покращення та як воно впливає на професійну діяльність.

ANNOTATION

Development of a security system for IoT using SIEM technologies // Master's Degree Thesis / Masliy Rostyslav Bogdanovych // Ternopil National Technical University named after Ivan Pului, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group SBm-61 // Ternopil, 2022 // P. 58, Fig. 20, Tables 4, Supplement 1, Bibliog. 28.

Keywords: SECURITY SYSTEM, INTERNET OF THINGS NETWORK, SIEM, IOT, TECHNOLOGY

The purpose of the work is to study information security management technologies and develop a security system for IoT based on SIEM technology.

The main results of the work: the area of activity of the latest IoT devices and their data transmission through the punctures were investigated, which in turn allowed to better determine the advantages and disadvantages for the development of their own system. Several information security management technologies available on the market were analyzed. The analysis was carried out primarily in order to choose a suitable system for specific devices and to ensure that the system maintenance was cheap and at the same time of high quality compared to competitors. Based on the conducted research, security for IoT using Elastic Stack SIEM was created.

The first section describes the current state of security of IoT systems, as well as communication technologies, data transfer protocols and architecture of IoT systems.

The second section analyzes the most relevant SIEM systems, describes their disadvantages and advantages.

The third section is a practical part. It describes the details of developing a security system for Internet of Things devices. The system is able to independently

analyze and notify the user about events that may threaten security. Thanks to this monitoring, it is possible to quickly respond to incidents and see them in the form of visualization on the network administrator panel.

The fourth section describes occupational safety instructions when working with computers and factors of the production environment and their impact on human life.

The section "Safety in Emergency Situations" describes the health of employees, adds tips for its improvement and how it affects professional activities.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IOT - Internet of Things

OS - Operating System

OSI - Open Systems Interconnection

RFID – Radio Frequency Identification

SEM - Security Event Management

SIM - Security Information Management

SIEM - Security Information and Event Management

ЗМІСТ

ВСТУП

Актуальність теми. З появою Інтернету людське життя кардинально змінилось. Завдячуючи створенню не дорогих мікросхем і телекомунікацій з великою пропускною здатністю, Інтернет дав можливість приєднувати пристрої одне до одного. Це означає, що речі, які ми використовуємо кожного дня, такі як, зубні щітки, телевізори, холодильники або автомобілі, можуть використовувати датчики для збору даних і розумного реагування на дії користувачів. Всі ці речі можуть об'єднуватись між собою і саме ця мережа з'єднань називається IoT (Internet of Things).

IoT є відносно новітньою технологією у нашому житті, але сфера застосування вже стала настільки великою, що вплинула на взаємодії між людиною та технікою. Наприклад, у розумному будинку після натискання кнопки будильника, автоматично включиться кавоварка і відкриються штори, холодильник може автоматично замовити продукти у разі їх малої кількості в ньому. Всі ці дані потрібно обробити та проаналізувати, для того, щоб отримати з них корисну інформацію. Дані проходять декілька етапів збору, підготовки, обробки, перевірки і зберігання. Але на жаль, вся процедура не є повністю захищеною, що робить її ідеальною мішенню для зловмисників. В зв'язку з цим розробка та використання систем моніторингу при обробці даних стає необхідною.

Системи моніторингу використовуються для отримання інформації про стан даних в режимі реального часу. Вони також використовуються не тільки для знаходження та попередження збоїв і атак, а також для візуалізації даних. Самі ж атаки часто бувають саме там де, моніторинг не контролює область або не коректно працює. Для цього, щоб вирішити цю проблему компанії використовують SIEM (Security Information and Event Management). SIEM – це керування інформаційною безпекою і подіями. Існує безліч компаній, які надають свої найсучасніші послуги в цій області. Зазвичай рішення SIEM

побудовані на ієрархічній схемі, де рівень представлення включає в себе графічні панелі для різних подій, які чудово налаштовані для спостереження операційного центру безпеки (SOC).

Отже, **метою** даної роботи є дослідження технологій управління інформаційною безпекою та розробка системи безпеки для IoT на підставі SIEM технології.

Для отримання поставленої мети, необхідно виконати низку наступних **задач**:

- провести аналіз стану безпеки IoT систем, а також технологій зв'язку, протоколів передачі даних та архітектуру IoT систем;

- дослідження технологій управління інформаційною безпекою;

- реалізувати систему безпеки для IoT за допомогою Elastic Stack SIEM;

- оцінити якість реалізованої системи з точки зору покращення моніторингу системи.

Об'єкт дослідження – технології управління інформаційною безпекою.

Предмет дослідження – SIEM технологія, що інтегрована у IoT систему.

Наукова новизна одержаних результатів дипломної роботи полягає у тому, що розроблено систему безпеки для IoT з використанням Elastic Stack SIEM, за рахунок, чого відбувається реагування на інциденти безпеки IoT пристроїв та запобігання вторгнень зловмисників в мережу.

Практичне значення одержаних результатів. Удосконалено систему моніторингу безпеки IoT пристроїв, що в свою чергу дозволяє вчасно виявити загрози та користувачу або оператору центру безпеки швидше прийняти необхідні дії, щоб зменшити вірогідність потрапляння зловмисника у мережу.

Апробація результатів магістерської роботи. Окремі результати проведених досліджень доповідались на X науково-технічна конференція «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 7 – 8 грудня 2022 р.

Публікації. За темою роботи з викладенням її основних результатів опубліковано 1 наукова праця, що являє собою тези в збірнику матеріалів науково-практичних конференцій (див. Додаток А).

РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ВПРОВАДЖЕННЯ IOT СИСТЕМ

1.1 Аналіз стану безпеки IoT систем

Інтернет речей, як і будь-яка швидкорозвиваюча технологія має ряд проблем росту, серед яких найбільш проблемною є безпека. Чим більше розумних пристроїв підключається до мережі, тим більше ризиків пов'язаних з несанкціонованим доступом в IoT-систему і використання її зловмисниками. Сьогодні багато компаній і організацій в сфері IT зосереджені на пошуку рішень, які дозволять мінімізувати загрози.

За даними порталу Statista у 2017 році нараховувалось більше 20 млрд пристроїв, а до кінця 2025 очікується не менше 75 млрд [1]. Для них всіх безпека полягає перш за все в цілісності коду, перевірці користувачів, встановленню правил, а також відбиттю атак. Але по факту більшість пристроїв не мають вбудованих систем захисту, мають стандартні паролі та всі признаки веб- вразливостей.

У 2016 році ботнет Mirai способом підбору комбінацій стандартних паролів і логінів отримав доступ до великої кількості камер і роутерів, які пізніше були використані для потужної DDoS атаки на провайдерів мереж UK Postal Office, Deutsche Telekom, TalkTalk, KCOM [2]. Але найбільш резонансною була атака націлена на DNS оператора DYN. Під час цієї атаки доступ до Інтернету втратила майже половинна населення США. Для атаки був обраний найлегший шлях через встановленні стандартні логіни і паролі пристроїв. Вище перераховані події чудово показують важливість передбачення вразливостей IoT. Зрозуміло, що несанкціонований доступ до чийогось розумного годинника або фітнес-трекера сильної шкоди не принесуть, але проникнення через IoT в критичну інфраструктуру загрожує непередбаченими подіями.

Існуюча проблема безпеки виникла не через технічні не доопрацювання, а через поспіх. Завдання компанії як найшвидше випустити свій продукт на ринок, адже це дає перевагу перед конкурентами,але, на жаль, не проводиться достатня кількість тестувань.

1.2 Архітектура IoT системи

Завдяки можливостям, які обіцяє IoT, все більше компаній прагнуть добавити ці технології у свою роботу. Але коли справа доходить до реальності, виникає багато питань та труднощів, з огляду на кількість пристроїв та умов необхідних для того, щоб об'єднати весь робочий процес. Ця мережева система складається з численних елементів, таких як датчики, хмарні сервіси, протоколи і рівні архітектури. Різні рівні дозволяють адміністраторам оцінювати, контролювати і підтримувати одноголосність системи. [3] План проектування системи детально інтегрується з наявною інфраструктурою компанії для отримання максимального ефекту. Крім того, система включає в себе рівні архітектури IoT, які допомагають відстежувати процеси. Ці рівні повинні бути створені ще до початку формування мереж і загальна архітектура буде складатись з трьох основних шарів:

Рівень IoT пристроїв – це клієнто-орієнтований рівень, який отримує дані від користувача.

Мережевий рівень – серверно-орієнтований рівень, який підключає пристрої до розумних об'єктів, серверів або мережевих девайсів.

Прикладний рівень – рівень, на якому користувач отримує кінцевий додаток, який з'єднує оператора і клієнта.

Ці рівні забезпечують повну функціональність, маштабування, доступність і ремонтопридатність архітектури IoT.

Але як тільки їх отримуємо, потрібно перейти до наступних чотирьох етапів створення архітектури.

- Прикладний рівень
- Рівень обробки даних
- Мережевий рівень
- Сенсорний рівень

Рисинук 1.1 — Рівні моделі OSI для IoT пристроїв

Прикладний рівень. Прикладний рівень визначає всі додатки у яких розгорнуто IoT. Це інтерфейс між кінцевими пристроями та мережею. Він має повноваження надавати послуги програмам. Послуги можуть бути різними для кожного додатку, оскільки вони ґрунтуються на інформації, яку зібрали датчики.

Інформація транслюється через спеціальний додаток на стороні пристро Наприклад, на комп'ютері саме браузер виступає прикладним рівнем. Найбільш відомою загрозою на прикладному рівні є міжсайстовий скриптинг. Цей тип порушення комп'ютерної безпеки зазвичай зустрічається у веб-додатках, який дозволяє зловмисникам добавляти свої правила зі сторони клієнта використовуючи мову програмування JavaScript. Таким чином зловмисник може повністю змінити веб-сторінку відповідно до своїх потреб.

Рівень обробки даних. В трьохрівневій архітектурі дані напряму відправлялись на мережевий рівень. Через це збільшується вірогідність їх втрати або пошкодити. В чотирьохрівневій архітектурі ці дані відправляються з рівня обробки даних. Цей рівень має два обов'язки: він підтверджує, що дані відправляються справжнім користувачем, а також він запобігає загрозам.

Автентифікація - це найбільш часто використовуваний метод перевірки користувача та даних. Вона застосовується за допомогою наперед розділених ключів та паролів для кожного користувача. Другий обов'язок цього рівня це передача інформації на мережевий рівень. Спосіб передачі цих даних може бути, як провідний, так і безпровідний. Тут теж є дві основні вразливості, які використовують зловмисники:

DoS-атака: зловмисник відправляє величезну кількість даних, щоб зробити мережевий трафік перевантаженим. Таким чином, величезне споживання системних ресурсів виснажує IoT-систему і позбавляє користувача доступу до системи.

Зловмисна внутрішня атака: виконується зсередини середовища IoT-систему для отримання доступу до приватної інформації. Здійснюється авторизованим користувачем для доступу до інформації іншого користувача.

Мережевий рівень. Цей рівень також відомий, як рівень передачі. Він виступає у якості місту, який передає дані, зібрані з фізичних об'єктів за допомогою датчиків. Середовище може бути бездротовим або дротовим. Рівень з'єднує мережеві пристрої та мережі між собою, саме тому він надзвичайно чутливий до атак з боку зловмисників. Мережевий рівень має важливі питання безпеки щодо цілісності та автентичності даних, які передаються в мережу, серед найбільш відомих є:

1. Атака типу Main-in-the-middle.

MiTM-атака - це атака, при якій зловмисник приватно перехоплює і модифікує комунікацію між відправником і одержувачем, які припускають, що вони безпосередньо спілкуються один з одним. Це призводить до серйозної

загрози безпеці в Інтернеті, оскільки дає зловмиснику можливість перехоплювати і контролювати дані в режимі реального часу.

2. Атаки на сховища.

Важлива інформація користувачів зберігається на пристроях зберігання даних або в хмарі. Як пристрої зберігання даних, так і хмара можуть бути атаковані зловмисником, а інформація користувача може бути змінена на некоректні дані.

3. Експлойт-атака.

Експлойт - це будь-яка неетична або незаконна атака у вигляді програмного забезпечення, блоків даних або послідовності команд. Вона використовує недоліки безпеки в додатку, системі або апаратному забезпеченні. Зазвичай відбувається з метою отримання контролю над системою та викрадення інформації, що зберігається в мережі. Встановлення всіх виправлень для програмного забезпечення, випусків безпеки та всіх оновлень для вашого програмного забезпечення - це лише деякі профілактичні заходи проти атаки.

Сенсорний рівень. Сенсорний рівень відповідає за розпізнавання предметів і збір даних про них. Існує багато типів датчиків, підключених до об'єктів для збору інформації, таких як RFID, сенсори та 2-D штрих-код. Датчики вибираються відповідно до вимог додатків. Дані, які збираються цими датчиками, можуть бути про місцезнаходження, зміни в повітрі, навколишньому середовищі тощо. Однак саме вони є основною метою зловмисників, які бажають використати їх для заміни датчика на свій власний.

1.3 Технології зв’язку та протоколи обміну даними

Протоколи та стандарти IoT часто не беруться до уваги, коли технологи досліджують Інтернет речей (IoT). Частіше за все, увага індустрії прикута до

зв'язку. І хоча взаємодія між пристроями, датчиками IoT, шлюзами, серверами і призначеними для користувача додатками має важливе значення, але без правильних протоколів IoT зв'язок не буде ефективним.

Існує кілька десятків протоколів Інтернету речей, кожен з яких пропонує певні можливості або комбінації можливостей, що робить його кращим в порівнянні з іншими варіантами для конкретних розгортань Інтернету речей. Кожен протокол IoT забезпечує зв'язок між пристроєм і пристроєм, пристроєм і шлюзом або пристроєм і хмарою/центром обробки даних - або комбінації цих зв'язків. Такі фактори, як географічне і особливе розташування, потреби в енергоспоживанні, можливості роботи від батареї, наявність фізичних бар'єрів і вартість, визначають, який протокол є оптимальним для розгортання IoT.[4]

Зазвичай при розробці обирають з декількох протоколів зв'язку при побудові мережі для обслуговування своєї екосистеми IoT. До найбільш поширених відносяться наступні.

Bluetooth - це технологія бездротового зв'язку малого радіусу дії, яка використовує короткохвильові, надвисокочастотні радіохвилі. Вона найчастіше використовувалася для потокової передачі аудіо, але також стала важливим засобом для бездротового зв'язку і підключення пристроїв. Як наслідок, цей варіант підключення з низьким енергоспоживанням і малим радіусом дії є основним як для персональних мереж, так і для розгортання IoT.[5]

Інший варіант - *Bluetooth Low Energy*, відомий як Bluetooth LE або BLE, який є новою версією, оптимізованою для з'єднань IoT. Відповідно до своєї назви, BLE споживає менше енергії, ніж стандартний Bluetooth, що робить його особливо привабливим у багатьох випадках використання, таких як фітнес-трекери і пристрої для розумного будинку на стороні споживача і для навігації в магазинах на комерційній стороні.[5]

Стільниковий зв'язок є одним з найбільш широко доступних і відомих варіантів для додатків Інтернету речей, і це один з найкращих варіантів для

розгортання, де зв'язок поширюється на великі відстані. Хоча застарілі стандарти стільникового зв'язку 2G і 3G в даний час поступово відмовляються від використання, телекомунікаційні компанії швидко розширюють сферу застосування нових високошвидкісних стандартів, а саме 4G/LTE і 5G. Стільниковий зв'язок забезпечує високу пропускну здатність і надійний зв'язок. Він здатний передавати великі обсяги даних, що є важливою можливістю для багатьох розгортань IoT. Проте ці функції мають свою ціну: вищу вартість і енергоспоживання в порівнянні з іншими варіантами.[6]

LoRa - це бездротова технологія, яка, як випливає з її назви, пропонує можливості зв'язку на великі відстані. Вона має низьке енергоспоживання і забезпечує безпечну передачу даних для додатків M2M і розгортання IoT. Це запатентована технологія, яка тепер є частиною радіочастотної платформи Semtech. [7]

Враховуючи його поширеність в домашніх, комерційних і промислових будівлях, *Wi-Fi* є часто використовуваним протоколом IoT. Він забезпечує швидку передачу даних і здатний обробляти великі обсяги даних. Wi-Fi особливо добре підходить для роботи в локальних мережах на коротких і середніх відстанях. Крім того, безліч стандартів Wi-Fi - найпоширенішим з яких є 802.11n. Однак багато стандартів Wi-Fi, в тому числі той, який зазвичай використовується в будинках, занадто енергоємні для деяких випадків використання IoT, особливо для пристроїв з низьким енергоспоживанням/живленням від батареї. Це обмежує використання Wi-Fi в якості опції для деяких розгортань. [8]

Zigbee - це протокол мережі, який був розроблений для застосування в будівництві та домашній автоматизації, і є одним з найпопулярніших протоколів в середовищі IoT. Протокол Zigbee з невеликим радіусом дії і низьким енергоспоживанням може бути використаний для розширення зв'язку між декількома пристроями. Він має більший радіус дії, ніж BLE, але має

нижчу швидкість передачі даних, ніж BLE. Zigbee пропонує гнучку, самоорганізуючу сітку, наднизьке енергоспоживання і бібліотеку додатків.

Ще одна запатентована опція, *Z-Wave* - це протокол бездротового зв'язку в мережі, побудований на радіочастотній технології з низьким енергоспоживанням. Як Bluetooth і Wi-Fi, Z-Wave дозволяє смарт-пристроям обмінюватися даними з шифруванням, забезпечуючи тим самим рівень безпеки розгортання IoT. Він широко використовується для продуктів домашньої автоматизації та систем безпеки, а також в комерційних додатках, таких як технології управління енергією. Він працює на радіочастоті 908,42 МГц в США; хоча його частоти варіюються в різних країнах.[9]

Скорочено від *Advanced Message Queuing Protocol* - це відкритий стандартний протокол, який використовується для більш орієнтованого на повідомлення проміжного програмного забезпечення. Таким чином, він забезпечує взаємодію обміну повідомленнями, незалежно від платформ на яких розміщені системи IoT. Він забезпечує безпеку, а також надійність на відстані або через погане з’єднання мереж. Його особливість у тому, що він підтримує зв’язок навіть тоді коли обидві системи не доступні одночасно.

CoAP (Constrained Application Protocol), розроблений для роботи з системами Інтернету речей на основі протоколу HTTP. CoAP покладається на User Datagram Protocol для встановлення безпечного зв'язку і забезпечення передачі даних між декількома точками. Часто використовуваний для додатків типу "машина-машина" (M2M), CoAP дозволяє пристроям з обмеженими можливостями приєднатися до середовища IoT, навіть при наявності пристроїв з низькою пропускною здатністю, низькою доступністю і/або низьким енергоспоживанням.

Object Management Group (OMG) розробила службу розподілу даних для систем реального часу. OMG описує DDS як "протокол проміжного програмного забезпечення і стандарт API для підключення, орієнтованого на

дані. Він інтегрує компоненти системи разом, забезпечуючи підключення даних з низькою затримкою, надзвичайну надійність і масштабовану архітектуру, необхідну для бізнес-додатків і критично важливих додатків IoT. Цей стандарт M2M забезпечує високопродуктивний і масштабований обмін даними в режимі реального часу.

Протокол управління пристроями, розроблений для мереж і вимог середовища *M2M*. Цей протокол зв'язку створений спеціально для віддаленого управління пристроями і телеметрії в середовищах IoT та інших додатках M2M; як такий, він є хорошим варіантом для малопотужних пристроїв з обмеженими можливостями обробки і зберігання даних.

MQTT. Спрощений мережевий протокол, який орієнтований на обмін повідомленнями між пристроями по принципі “публікація - підписка”. Він був розроблений для роботи в умовах низької пропускної здатності, наприклад, для датчиків і мобільних пристроїв в малопотужних мережах. Ця можливість робить його загальноприйнятим варіантом для підключення пристроїв з невеликим кодом, а також для бездротових мереж з різним рівнем затримок, що виникають через обмеження пропускної здатності або ненадійних з'єднань.

XMPP зараз використовується для M2M-зв'язку в легкому проміжному програмному забезпеченні та для маршрутизації XML-даних. XMPP підтримує обмін структурованими, але розширюваними даними в режимі реального часу між декількома об'єктами в мережі, і найчастіше використовується для розгортання IoT, орієнтованих на споживача, таких як розумні прилади. Це протокол з відкритим вихідним кодом, який підтримується Фондом стандартів XMPP.

Жоден протокол зв'язку IoT не є найкращим, і жоден з них не підходить для кожного випадку розгортання.

Скоріше, корпоративні технологи повинні визначити, який протокол буде найкращим для їх організацій, виходячи з унікальних обставин запланованого впровадження IoT.[8]

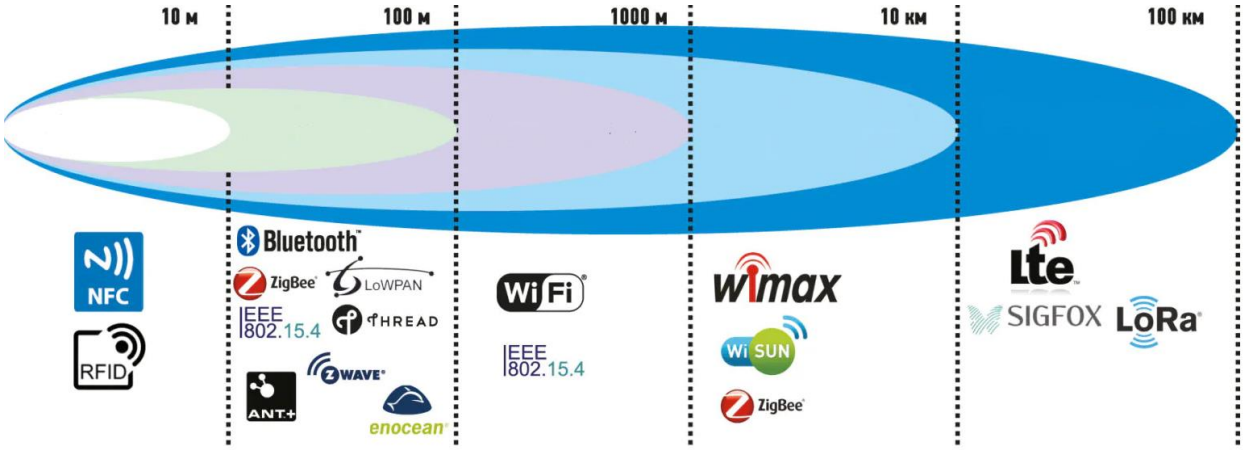

Рисунок 1.2 Радіус дії проколів

Ці рішення повинні враховувати цілий ряд факторів, від потреб в електроживленні підключених пристроїв і розташування цих пристроїв, до географічного розміру і особливостей місця розгортання, а також вимог до безпеки розгортання.

1.4 Висновок до першого розділу

В першому розділі описаний стан безпеки IoT пристроїв, їхня кількість та застосування у світі. Також розглянуто найбільш відомі атаки та їхні наслідки.

Досліджено архітектуру та принципи роботи пристроїв, основні рівні моделі OSI, принцип роботи, функції які вони виконують та вразливості, якими може скористатись зловмисник на певному рівні. Також охарактеризовані протоколи мережі інтернету речей, радіус дії та сфера застосування.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Аналіз архітектури SIEM-технології

SIEM - це підхід, який існує вже більше десяти років.

У минулому SIEM вимагали ретельного управління на кожному етапі конвеєра даних - отримання даних політик, перегляді оповіщень та аналізі аномалій.

З плином часу SIEM систематизуються і стають розумнішими в об'єднанні даних і використанні методів штучного інтелекту, щоб зрозуміти, який тип поведінки є інцидентом безпеки. SIEM працює шляхом збору даних журналів і подій, які генеруються хост-системами, мережею, пристроями безпеки і додатками. Вони роблять це, розгортаючи колекцію агентів по всій технологічній інфраструктурі організації, а потім вони збирають всі дані на централізованій платформі. Програмне забезпечення SIEM ідентифікує ці дані (мережеві аномалії, антивірусні події, інциденти безпеки інциденти, журнали брандмауера) і сортує їх за категоріями, такими як невдалі та успішні входи в систему, активність шкідливого програмного забезпечення та інша потенційно зловмисна активність. Коли програмне забезпечення ідентифікує події, які можуть становити загрозу для організації, оповіщення генеруються сповіщення, які вказують на можливу проблему безпеки. Сповіщення можуть бути встановлені з різними рівнями пріоритету за допомогою набору заздалегідь визначених правил.

Рішення SIEM складається з декількох компонентів, які збирають дані журналів і подій з систем і перетворюють їх на дієві знання про безпеку. Для виконання цього завдання SIEM спирається на наступні елементи та дії:

1. Агрегація даних: збирає та агрегує дані з хост-систем, мережевих пристроїв тощо.
2. Канали розвідки загроз: об'єднує внутрішні дані про загрози та вразливості.
3. Кореляція та моніторинг безпеки: пов'язує події з інцидентами та загрозами.
4. Аналітика: використовує машинне навчання і статистичні моделі для виявлення взаємозв'язків між даними.
5. Сповіщення: аналізує події та надсилає сповіщення при виявленні аномалії.
6. Інформаційні панелі: створює візуалізації для відображення ситуації з даними в реальному часі і допомагає адміністраторам виявляти закономірності та аномалії.
7. Відповідність вимогам: збирає дані журналів з різних стандартів безпеки і генерує звіти.
8. Збереження: зберігає довгострокові історії даних.
9. Криміналістичний аналіз: дозволяє аналізувати дані та оповіщення, щоб виявити деталі інцидентів безпеки.
10. Полювання на загрози: дозволяє адміністраторам виконувати запити до даних журналів і подій для виявлення загроз.
11. Реагування на інциденти: допомагає виявляти і реагувати на інциденти безпеки.
12. Автоматизація SOC: автоматично реагує на інциденти, організовуючи системи безпеки.

Рис.2.1 представляє логічну архітектуру SIEM, показуючи не тільки компоненти, але й дії, що визначають, як вона функціонує.

Як згадувалося раніше, SIEM-рішення збирають дані з різних систем, пристроїв і додатків в єдиний загальний формат. Ці дані нормалізуються, а потім запускаються через механізм політик.

Рисунок 2.1 — Основні процеси утворення SIEM архітектури

Рішення SIEM, як правило, будуються за ієрархічною схемою.

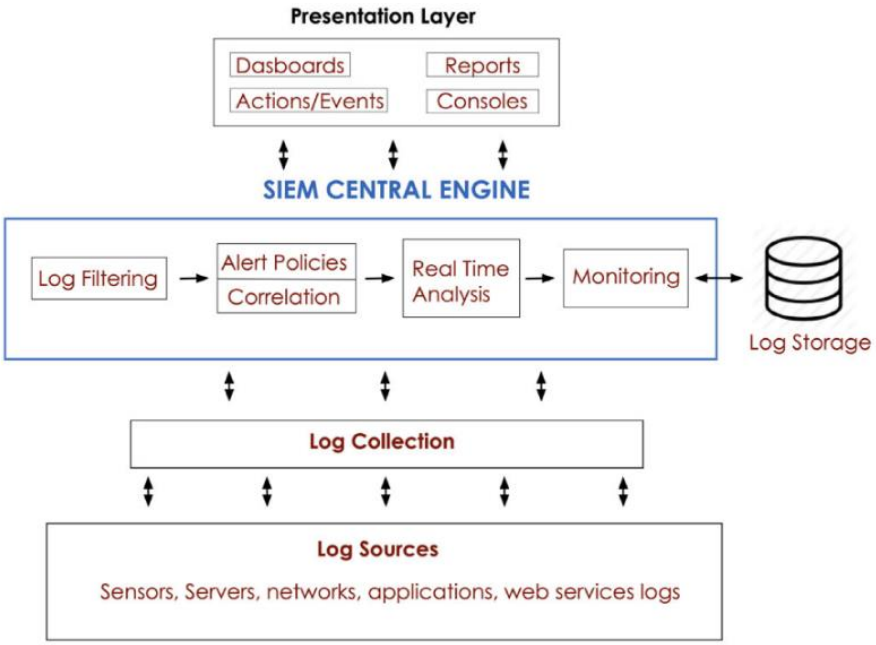

Рисунок 2.2— Фізична архітектура SIEM

Як показано на рис.2.2, центральний модуль SIEM - це частина, що відповідає за фільтрацію, аналіз, моніторинг журналів, застосуванням політик і створенням оповіщень. Крім того, модуль відправляє журнали в сховище і доставляє отриману інформацію на рівень представлення (Presentation Layer), де вона візуалізується і аналізується користувачами:

- Джерело логів: тобто джерело журналів - це будь-який пристрій, який може збирати інформацію і здатний генерувати журнали. Це можуть бути датчики, маршрутизатори, комутатори, сервери тощо.

- Збір журналів: процес, при якому всі записи відправляються в центральну базу даних SIEM.

- Фільтрація журналів: процес, в якому всі записи нормалізуються в загальний формат.

- Політики оповіщень - кореляція: процес, в якому оповіщення генеруються і пов'язуються з подіями з урахуванням певних політик, які дозволять уникнути створення помилкових тривог.

- Аналіз в режимі реального часу: процес, в якому записи аналізуються по мірі їх надходження.

- Моніторинг: заключна фаза роботи центрального ядра SIEM. Після того, як всі записи зібрані і оброблені, ця фаза дозволяє отримати доступ до збереженої інформації, а також сприяє розробці політик безпеки, які дозволять витягувати інформацію з подій, що обробляються.

- Зберігання журналів: журнали зберігаються в базі даних. Залежно від кількості, вони можуть зберігатися на різних вузлах, що утворюють кластер.

З роками SIEM стала чимось більшим, ніж інструменти управління журналами, які їй передували, тому обрати SIEM-рішення – не просте завдання. Є кілька моментів, які слід враховувати і, в основному, вибір буде залежати від сценаріїв використання, де воно буде застосовуватися.

На сучасному ринку існує велика кількість SIEM рішень. Для прикладу у 2018 році був опублікований квадрант Гартнера. Квадрант Гартнера - це результат досліджень на конкретному ринку, що дає змогу отримати широке уявлення про відносні позиції конкурентів на ринку.

Рисунок 2.3— Квадрант Гартнера відносно ринкових SIEM-систем

На рис.2.3 зображується лідери серед SIEM-рішень. Деякі з цих рішень будуть описані та порівняні для того, щоб вирішити, яке з них найкраще відповідає потребам цієї роботи.

2.2 Splunk

Splunk - це платформа для збирання, зберігання, опрацювання та аналізу машинних даних, тобто логів. На сьогоднішній день є вкрай популярною в США і в Європі і поступово виходить на інші ринки. Однією з головних особливостей платформи є те, що вона може працювати з даними практично будь-яких пристроїв, і тому список можливих застосувань системи дуже широкий. У більшості випадків розбирає вхідні дані на поля та значення і надалі обробляє їх. Обробка відбувається за допомогою SPL запитів (спеціальна мова від Splunk), за допомогою якої можна будувати різні вибірки і таблиці, сортувати, фільтрувати, агрегувати, будувати звіти, створювати поля, що обчислюються, звертатися як до внутрішніх, так і до зовнішніх довідників, створювати візуалізації, з широким спектром візуалізації та робити сповіщення. Усе це можна упакувати у свій персональний за стосунок, як показанона рисунку 2.4.

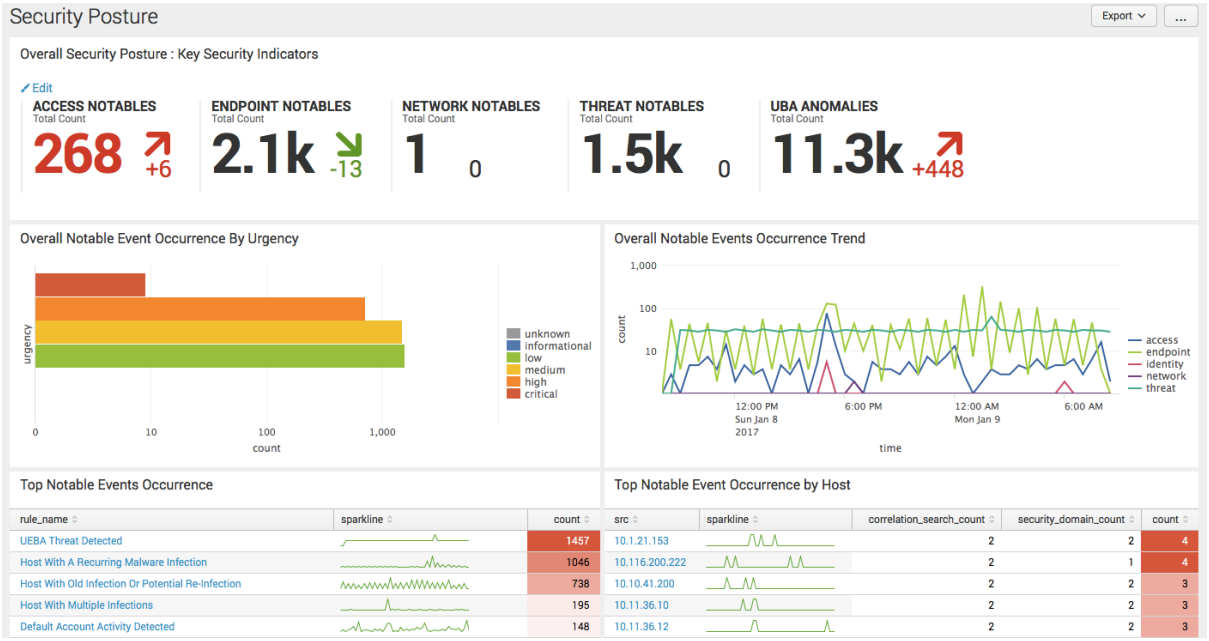

Рисунок 2.4 — Приклад візуалізації Spunk

Таблиця 2.1 – Переваги та недоліки технології управління інформаційною безпекою Splunk

Переваги	Недоліки
Потужний додаток для аналізу даних	Деякі запити можуть працювати повільно
Відмінна і дуже інформативна панель приладів	Складний процес налаштування, у випадку, якщо логи не зберігаються в загальнодоступних місцях
Аналізатор полів дуже простий у використанні	Висока вартість
Ефективно аналізує велику кількість даних	Призначений для великих компаній
OS: Windows and Linux	

2.3 McAfee Enterprise Security Manager

Рішення від компанії McAfee постачається не тільки у вигляді фізичних і віртуальних пристроїв, а також програмного забезпечення. Воно складається з декількох модулів, які можуть застосовуватися як разом, так і окремо.

Рис.2.5 Приклад візуалізації McAfee Enterprise Security Manager

Enterprise Security Manager забезпечує постійний моніторинг корпоративної IT-інфраструктури, збирає інформацію про загрози та ризики, дає змогу поставити пріоритети для загроз та швидко проводити розслідування. McAfee ESM добре інтегрується з продуктами сторонніх розробників без використання API, що робить продукт сумісним з багатьма іншими популярними рішеннями в галузі безпеки. Також у нього є підтримка платформи McAfee Global Threat Intelligence, яка розширює традиційну функціональність SIEM. Завдяки їй, ESM отримує постійно оновлювану інформацію про загрози з усього світу.[9] На практиці це дає, наприклад, можливість виявляти події, пов'язані з підозрілими IP-адресами.

Таблиця 2.2 – Переваги та недоліки технології управління інформаційною безпекою McAfee Enterprise Security Manager

Переваги	Недоліки
Можливість співвідносити різні події з різних платформ	Велика кількість помилок
Присутній адаптивний режим самонавчання	Споживає занадто багато комп'ютерних ресурсів

Хороша технічна підтримка	Призначений для середніх і великих компаній
OS: Windows and Mac	

2.4 IBM QRADAR

SIEM-платформа від технологічного гіганта IBM є однією з найбільш просунутих на ринку: навіть у квадранті лідерів Gartner вона стоїть вище за конкурентів, причому потрапляє туди вже 10 років поспіль. Продукт складається з декількох інтегрованих між собою систем, які разом забезпечують максимальне охоплення подій, що відбуваються в мережі, а безліч функцій працюють з перших базових налаштувань. Інструмент вміє збирати дані з різноманітних джерел, наприклад, операційних систем, пристроїв безпеки, баз даних, застосунків і багатьох інших.

Таблиця 2.3 – Переваги та недоліки технології управління інформаційною безпекою IBM QRadar.

Переваги	**Недоліки**
Має більше 400 вбудованих типів джерел журналів	Не може бути інтегровано з TSM
Редактор DSM. Можливий аналіз подій за вимогою користувача	Деякі пошукові запити не дуже інтуїтивно зрозумілі
Інтеграція з менеджментом вразливостей та ризик-менеджером	Неможливо експортувати звіти з менеджера уразливостей доповнення
Вбудовані правила, порушення та звіти	OS: Windows

Одна з головних особливостей IBM QRadar Security Intelligence - виявлення і розставляння пріоритетів на основі ризиків з використанням розширеного аналізу і кореляції між активами, користувачами, мережевою активністю, наявними вразливостями, аналізом загроз тощо. IBM Qradar може пов'язувати події в один ланцюжок, створюючи для кожного інциденту окремий процес.

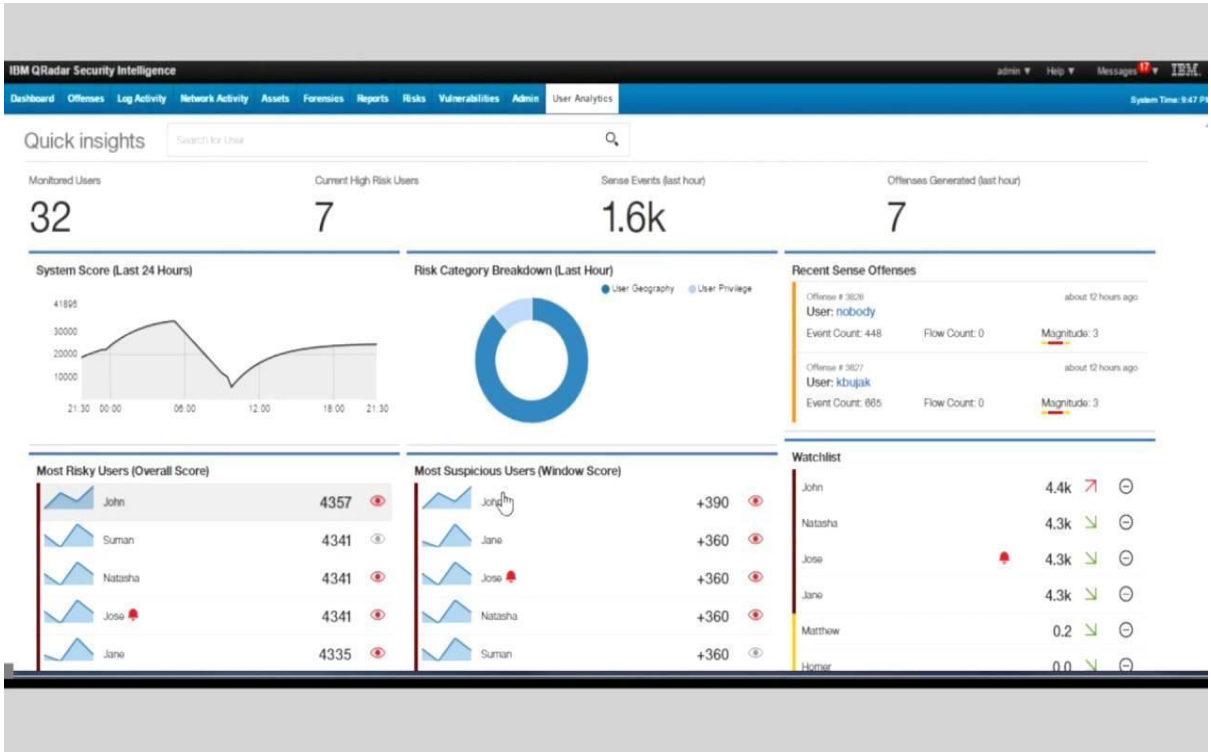

Рис.2.6 Приклад візуалізації IBM QRadar

2.5 ELASTIC STACK

Elastic Stack – це група продуктів з відкритим вихідним кодом, призначених для допомоги користувачам у пошуку, аналізі та візуалізації даних, що надходять з різних джерел у режимі реального часу. Він складається з пошукової системи, генератора журналів, веб-інтерфейсу користувача та колекції відправників. Всі ці компоненти мають відкритий вихідний код.

У червні 2019 року Elastic Stack додав до свого сімейства нового члена - Elastic SIEM. Це офіційне SIEM-рішення, представлене компанією Elastic, яке дозволяє аналізувати події безпеки, пов'язані з хостом і мережею, в рамках розслідувань за допомогою сповіщень або інтерактивного їх пошуку. Через свою пізню появу на сучасному ринку, його не включено в квадрант Гартнера, наведений вище.

Великою перевагою Elastic Stack є їхня розробка продуктів, які швидкі у роботі, не потребують потужних ресурсів ПК та логічно зрозумілі для звичайних користувачів. А саме :

- Logstash - виступає сервером і консолідатором логів.

- Elasticsearch - інструмент пошуку, який ідеально підходить для аналізу лог-файлів.

- Beats - агент передачі даних зі спеціалізованим варіантом для логових даних.

- Kibana - інструмент для перегляду та аналізу даних, що використовується в якості інтерфейсу для Elastic Stack і здатний приймати дані від інших інструментів збору даних.

Logstash, Beats та Kibana мають відкриті вихідні коди і є безкоштовними для використання. Лише Elasticsearch є платним. Кожна одиниця в Elastic Stack може бути використана в поєднанні з іншими інструментами, виробленими третіми сторонами. Особливо широко використовується Kibana.

Рисунок 2.7 – Візуалізація подій за допомогою Kibana

Пакет Elastic Stack є безкоштовним для використання, як локальне програмне забезпечення з більш платними планами, які включають професійну підтримку. Система Elastic SIEM є доповненням до Kibana. Всі продукти Elastic доступні, як хмарні SaaS-рішення, для яких не існує безкоштовної версії.

Таблиця 2.4 – Переваги та недоліки системи Elastic SIEM

Переваги	Недоліки
Компоненти можуть бути встановлені окремо	Не всі компоненти мають відкритий вихідний код
Має потужну пошукову систему	Безкоштовна версія не має служби підтримки
Може бути встановлений на сервері або ПК	
OS: Windows, Linux та Mac	

2.6 Висновок до другого розділу

Після порівняння декількох найпопулярниіших SIEM рішень, складно зупинитись на одній. Кожна система має свої переваги та недоліки, які беруться до уваги. Ключовим моментом є саме середовище, в якому вони будуть застосовуватись, та від проблеми, які вони повинні вирішити. В даній роботі я обрав останню SIEM модель, тобто Elastic Stack. Оскільки Elastic Stack має модульну архітектуру, то це означає, що для роботи можуть бути встановлені окремі компоненти. Також велика перевага в тому, що платні ліцензійні додатки я можу замінити на безкоштовні аналоги з відкритим кодом, без впливу на роботу та решту IoT системи.

РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ БЕЗПЕКИ ДЛЯ IOT З ВИКОРИСТАННЯМ SIEM ТЕХНОЛОГІЙ

3.1 Особливості управління інформаційною безпекою для IoT систем

Дана робота буде виконуватись за на основі The Elastic Stack, так як він чудово підходить для моніторингу, аналізу системних журналів, конфігураційних файлів та подій безпеки. Ці дії стануть можливі за допомогою Beats,Filebeat.[10] Середовище буде складатись з різних хотів,на кожному з яких буде вставлений певний компонент з Elastic Stack.

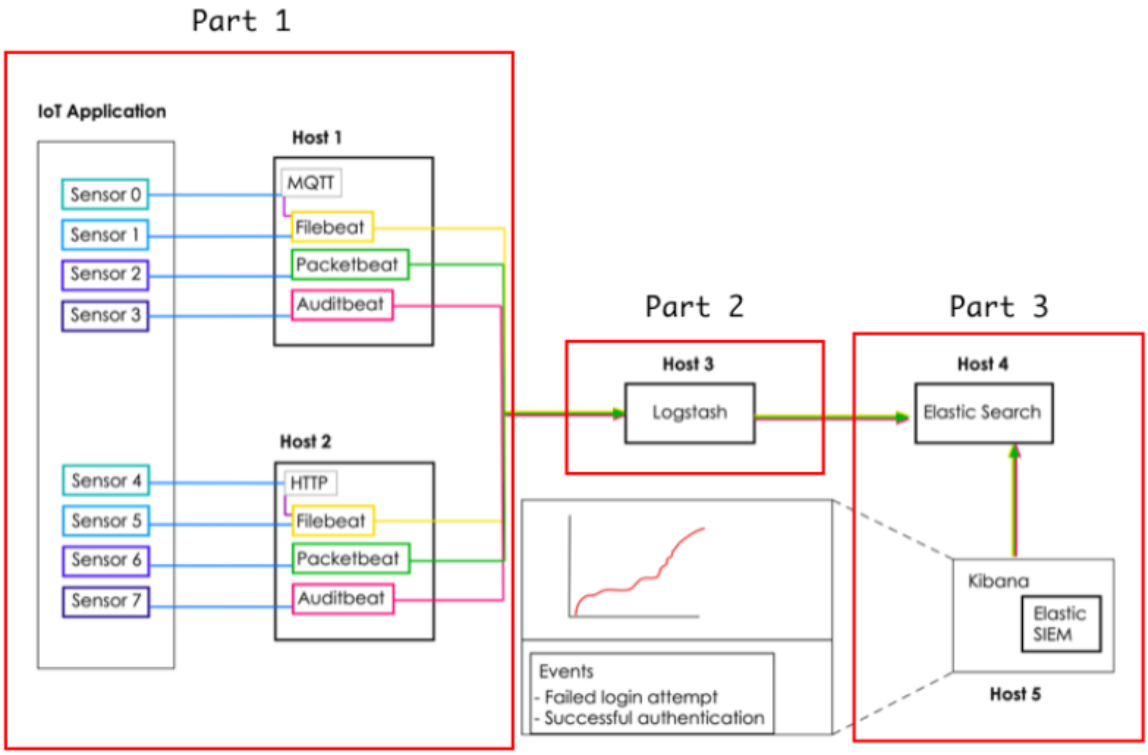

Рисунок 3.1 Архітектура поелементної системи моніторингу безпеки, яка використовується в даній роботі

Частина 1. Складається з IoT додатку, MQTT-блоку, HTTP-сервера та Beats. Додаток є одним з найціннішим елементом системи,так як завдяки йому аналізується інформація.[11] Блок MQTT формує вхідні дані та погоджує процес обробки. FIlebeat виконує роль генерування лог файлів для подальшої

їхньої відправки у Logstash. Packectbeat – мережевий аналіз пакетів,який стежить декодує трафік, розшифровує протоколи та записує дані кожної транзакції. Auditbeat використовується для аудиту активності користувачів і процесів на Linux-сервері та ідентифікаї порушень.[12] HTTP-сервер отримує запити від клієнтів, обробляє їх, генерує логи. Ця частина виступає у якості джерела збору, після якої дані відправляються на наступний етап, де вони будуть оброблятись.

Частина 2. Як згадувалось раніше, Logstash це генератор журналів, який здатен отримувати дані з кількох джерел і перетворювати їх в однорідний набір полів. Так як це другий етап,тут фільтруються та аналізуються дані,щоб відправитись до місця зберігання.[13]

Частина 3. Тут зосереджено Elasticsearch, Kibana та Elastic SIEM. Враховуючи,що дані зберігаються саме у третій частині,ми можемо з легкістю шукати їх завдяки Elasticsearch. Kibana - це інструмент візуалізації, який дозволяє бачити дані в графічному вигляді. Використовуючи кругові діаграми, карти або діаграми розсіювання, дані можуть бути представлені для вивчення та аналізу. [14]Elastic SIEM є частиною Kibana, він показує події безпеки та оповіщення, пов'язані з оброблюваними даними. Це завершальна стадія SMS, де дані перетворюються в інтерактивну форму і відображаються для того, щоб адміністратори могли дізнатися про них.

3.2 Розгортання SIEM-рішення.

Для імітації IoT пристроїв був розроблений симулятор датчиків.[15] Цю роботу створив викладач іспанського політехнічного університету у Мадриді Рамон Лопес. Я обрав саме цю симуляцію пристроїв,так як вона дозволяє моделювати системи,які включаюсь в мебе виконавчі механізми. Поточна реалізація надає абстрактне визначення контролера та реалізовано два

додаткових контролери: один для mqtt та інший для роботи у якості шлюзу для повідомлень, отриманих від брокера MQTT.[16]

Дана робота проводилась на пристрої MacBook Air з процесором M1 та 8ГБ пам’яті ,який виконував роль віртуального хоста середовища для розробки системи. Робота складається з трьох віртуальних машин,які взаємодіють між собою та є об’єктами імітації.

Для віртуалізації трьох хостів використовувався гіпервізор Oracle VM VirtualBox Manager 6.0.8. На хостах з іменами elk, mosquitto та apache встановлена 64-розрядна операційна система Ubuntu Server 16.04.06 LTS і налаштовані наступним чином: elk (4GB оперативної пам’яті, 20GB постійної пам’яті, 2 мережевих адаптери та IP адресса 178.20.156.90). Mosquitto (1GB оперативної пам’яті, 20GB постійної пам’яті, 2 мережевих адаптери та IP адресса 192.168.58.110). Apache (1GB оперативної пам’яті, 20GB постійної пам’яті, 2 мережевих адаптери та IP адресса 192.168.58.110)
Для встановлення Elasticsearch потрібно виконати наступні команди:

```
sudo apt install elasticsearch
```

Рисунок 3.2 – Процес встановлення Elasticsearch

Після успішної установки Elasticsearch, приступимо до налаштування програми.[17] Відкриємо файл конфігурації elasticsearch.yml за шляхом *vim /etc/elasticsearch/elasticsearch.y* у редакторі nano та прописуємо наступне:

```
node.name: "node-1
```

```
network.host: 0.0.0.0
http.port: 9200
discovery.seed_hosts: ["127.0.0.1]
cluster.initial_master_nodes:["node-1]
```

Elasticsearch використовує порт 9200.[18] Щоб обмежити доступ та підвищити рівень безпеки, потрібно знайти рядок з параметром network.host, розкоментувати його та змінити значення в ній на localhost:
Також нам потрібно встановити комплект JRE/JDK за допомогою команди network.host: localhost.

Рисунок 3.3 Редактор Elasticsearch

Для того, щоб запустити Elasticsearch, виконуємо команду:

```
sudo systemctl start elasticsearch
```

Для активації Elasticsearch при кожному завантаженні сервера необхідно виконати команду:

```
sudo systemctl enable elasticsearch
```

Рисунок 3.4– Процес запуску Elasticsearch

```
sudo apt install kibana
```

```
sudo systemctl enable kibana sudo systemctl start kibana
```

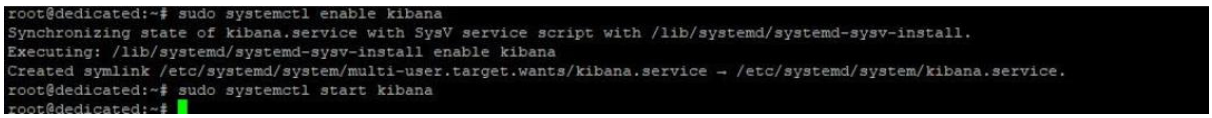

Рисунок 3.5 – Процес встановлення Kibana

Для початку потрібно створити обліковий запис адміністратора Kibana, тобто логін та пароль. Це можна зробити з командою:

```
echo "freehostadmin:`openssl passwd -apr1`" | sudo tee -a/etc/nginx/htpasswd.users
```

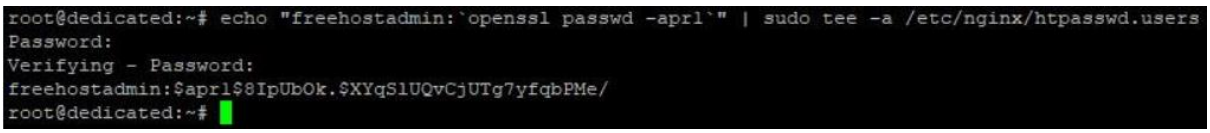

Рисунок 3.6 – Процес налаштування облікового запису

Після всіх кроків, додаток Kibana буде доступна у веб-браузері за адресою https://178.20.156.90/status. Попередньо, необхідно ввести вручну ваші облікові дані у діалоговому вікні введення.

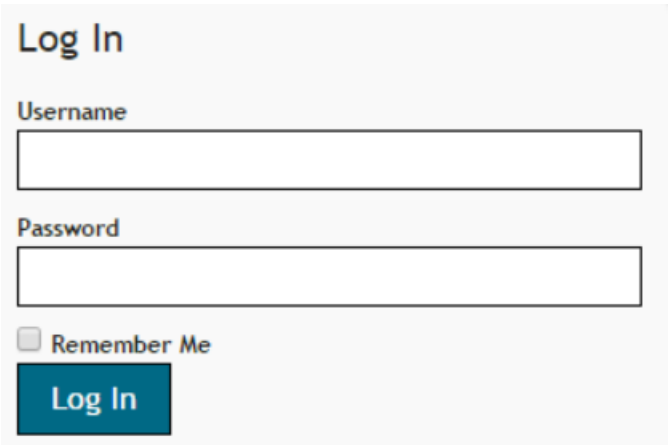

Рисунок 3.7 Поля вводу логіну та паролю для входу в Elasticsearch

Після проходження авторизації отримуємо повноцінний доступ до Elastic, як зображено на рисунку 3.8..

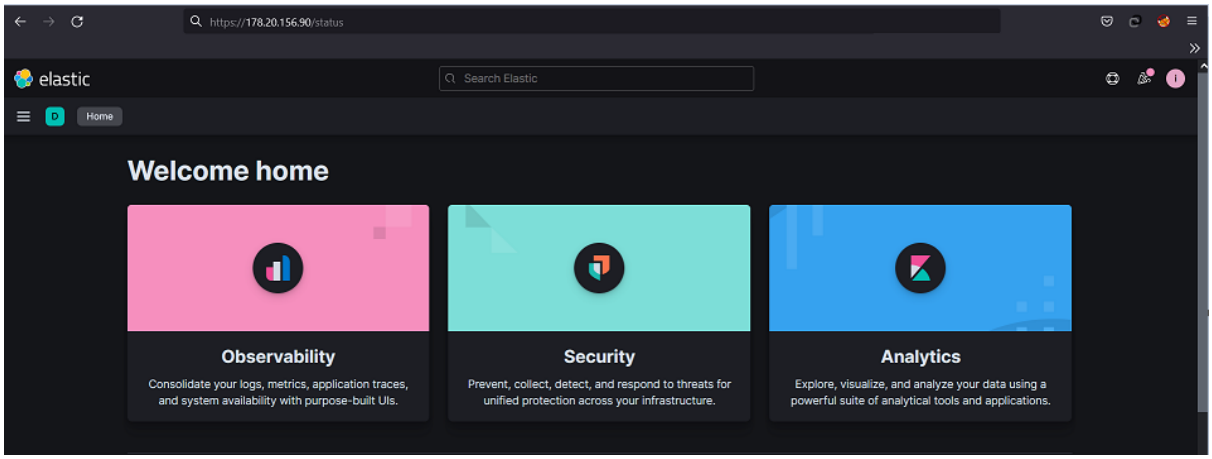

Рисунок 3.8 – Вікно Elasticsearch у браузері

3.3 Тестування системи безпеки SIEM для IoT за допомогою Elastic.

Усі описані вище кроки створюють хорошу систему моніторингу IoT пристроїів.

Для перевірки правильної роботи проведемо тестування.

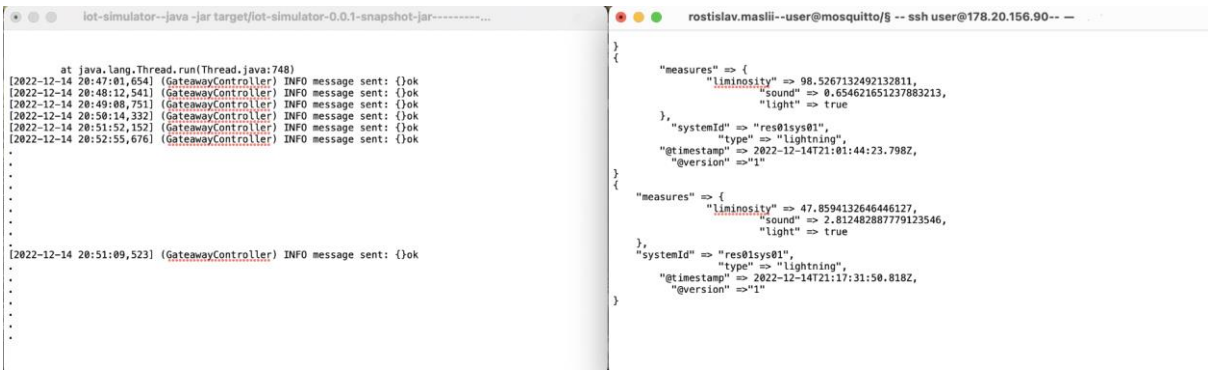

Рисунок 3.6 – Надсилання та отримання повідомлення

Як показано на рисунку 3.9, успішно виконано надсилання повідомлення та його отримання. Також ці дані надіслані до Elasticsearch і можуть бути візуалізовані, як на рисунках 3.10 та 3.11.

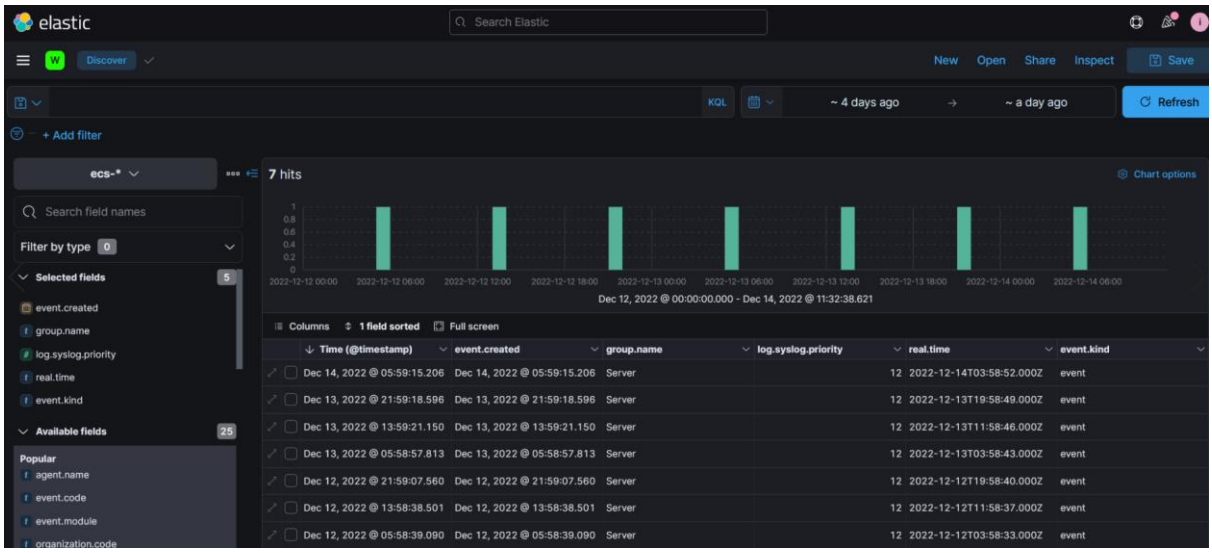

Рисунок 3.10 – Відтворення подій у Elasticsearch

Також ми можемо представити усі події за допомогою графіків.Рис.3.8.

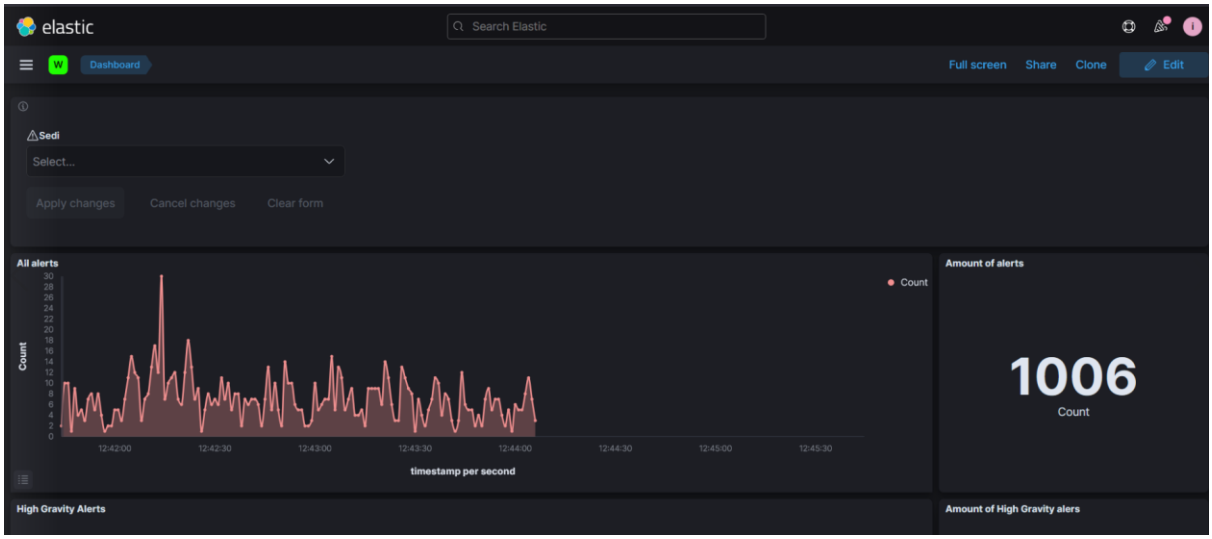

Рисунок 3.11 – Графічна візуалізація даних

3.4 Висновок третього розділу

В даному розділі проведено налаштування та тестування системи, показано її здатність виявляти та графічно візуалізувати сповіщення для кращої обробки адміністраторами системи.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Сучасний розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. Сьогодні, напевно, важко уявити компанію, господарська діяльність в якій здійснювалась би без використання комп'ютерної техніки. Через масовий характер робіт, що виконуються працівниками за допомогою комп'ютера, законодавством України чітко врегульовано норми та вимоги до використання комп'ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп'ютером.[19]

Згідно з нормативними актами про охорону праці (НПАОП 0.00-7.15-18) є такі вимоги безпеки до робочих місць працівників з електронними пристроями:

- Площа, відведена на одне робоче місце має становити не менше 6 кв.м., а об'єм – не менше 20 куб.м.[20]
- Конструкція робочого місця повинна забезпечувати підтримання оптимальної робочої пози, тобто такої, яка дозволяє працівникові виконувати роботу з мінімальним напруженням тіла, і яка дозволяє уникнути перевтоми в ході і після закінчення робочого процесу.
- Для забезпечення безпеки та захисту здоров'я працівників усе випромінювання від екранних пристроїв має бути зведене до гранично допустимого рівня (вплив на людину факторів довкілля - шуму, вібрації, забруднювачів, температури тощо, який не спричиняє соматичних або психічних розладів, а також змін стану здоров'я, працездатності, поведінки,що виходять за межі пристосувальних реакцій) з погляду безпеки та охорони здоров'я працівників.[21]

- Організація робочого місця працівника з екранними пристроями має забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним, антропологічним, психофізіологічним вимогам, а також характеру виконуваних робіт.[22]
- Освітлення робочого місця працівника з екранними пристроями має створювати відповідний контраст між екраном і навколишнім середовищем (з урахуванням виду роботи) та відповідати вимогам ДСанПІН 3.3.2.007-98.
- Мікроклімат приміщень з робочими місцями працівників з екранними пристроями має підтримуватись на постійному рівні та відповідати вимогам Санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року No 42.[23]

Вимоги щодо розміщення ІТС

Приміщення, в яких планується установка та подальша робота з комп'ютером, повинні відповідати проектній документації будинку, погодженій з уповноваженими державними органами. Крім того, роботодавець повинен враховувати санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення, а також характеристики електромагнітного, ультрафіолетового та інфрачервоного полів. Робочі місця, обладнані персональними комп'ютерами, заборонено облаштовувати у підвальних або цокольних приміщеннях будівель.[24] При обладнанні приміщень забороняється використання полімерних матеріалів, що виділяють шкідливі хімічні речовини.

Природне і штучне освітлення

Згідно документу ДБН В.2.5-28:2018 "Природне і штучне освітлення" приміщення з постійним перебуванням людей повинні мати природне освітлення. Природне освітлення поділяється на бокове, верхнє і

комбіноване. Що до штучного освітлення воно поділяється на робоче, аварійне, охоронне і чергове.[25]

Для загального штучного освітлення доцільно використовувати розрядні та світлодіодні джерела світла, які за однакової потужності з тепловими джерелами мають більшу світлову віддачу та більший термін експлуатації.

Види інструктажів з охорони праці

Працівники, під час прийняття на роботу та періодично, повинні проходити на підприємстві інструктажі з питань охорони праці, надання першої медичної допомоги потерпілим від нещасних випадків, а також з правил поведінки та дій при виникненні аварійних ситуацій, пожеж і стихійних лих.

За характером і часом проведення інструктажі з питань охорони праці (далі - інструктажі) поділяються на вступний, первинний, повторний, позаплановий та цільовий.)

Вступний інструктаж

Проводиться:

- з усіма працівниками, які приймаються на постійну або тимчасову роботу, незалежно від їх освіти, стажу роботи та посади;

- з працівниками інших організацій, які прибули до організації і беруть безпосередню участь у робочому процесі або виконують інші роботи для підприємства;

Вступний інструктаж проводиться спеціалістом служби охорони праці або іншим фахівцем відповідно до наказу (розпорядження) по організації, який в установленому типовим положенням порядку пройшов навчання і перевірку знань з питань охорони праці.[26]

Первинний інструктаж.

Первинний інструктаж проводиться до початку роботи безпосередньо на робочому місці з працівником:

- новоприйнятим (постійно чи тимчасово) до організації або до фізичної особи, яка використовує найману працю;

- який переводиться з одного структурного підрозділу організації до іншого;

Повторний інструктаж

Повторний інструктаж на робочому місці індивідуально з окремим працівником або групою працівників, які виконують однотипні роботи, за обсягом і змістом переліку питань первинного інструктажу.

Повторний інструктаж проводиться в терміни, визначені нормативно-правовими актами з охорони праці, які діють у галузі, або роботодавцем (фізичною особою, яка використовує найману працю) з урахуванням конкретних умов праці, але не рідше:

- на роботах з підвищеною небезпекою - 1 раз на 3 місяці;

- для решти робіт - 1 раз на 6 місяців.

Позаплановий інструктаж.

Позаплановий інструктаж проводиться з працівниками на робочому місці або в кабінеті охорони праці:

- при введенні в дію нових або переглянутих нормативно-правових актів з охорони праці, а також при внесенні змін та доповнень до них;

- при порушеннях працівниками вимог нормативно-правових актів з охорони;

- праці, що призвели до травм, аварій, пожеж тощо;

- при перерві в роботі виконавця робіт більш ніж на 30 календарних днів для робіт з підвищеною небезпекою, а для решти робіт - понад 60 днів.

Цільовий інструктаж.

Цільовий інструктаж проводиться з працівниками:

- при ліквідації аварії або стихійного лиха;

- при проведенні робіт, на які відповідно до законодавства оформлюються наряд-допуск, наказ або розпорядження.

Цільовий інструктаж проводиться індивідуально з окремим працівником або з групою працівників. Обсяг і зміст цільового інструктажу визначаються залежно від виду робіт, що виконуватимуться.

4.2 Безпека в надзвичайних ситуаціях

Здоров'я людини грунтується на основі генетичних факторів, способу життя та екологічних умов. Однак певною мірою воно залежить також від свідомого ставлення людини до себе та оточуючого середовища. Здоров'я людини — стан повного соціально-біологічного комфорту коли функція всіх органів і систем організму виважені з природним і соціальним середовищем, відсутні будь-які хвилювання, хворобливі стани та фізичні дефекти. Критерій здоров'я визначається комплексом показників. Однак за найзагальнішими рисами здоров'я індивідуума можна визначити як природний стан організму, що хактеризується повною зрівноваженістю будь-яких виражених хворобливих змін. Слід пам'ятати, що здоров'я залежить від багатьох факторів які об'єднуються в одне інтегральне поняття —здоровий спосіб життя. Його метою є навчити людину розумно ставитися до свого здоров'я, фізичної та психічної культури, загартовувати свій організм, вміло організовувати працю і відпочинок.

До основних складових здорового способу життя належать декілька основних чинників.

Спосіб життя має велике значення для здоров'я людини і складається з чотирьох категорій:

- Економічної (рівень життя).
- Соціологічної (якість життя).
- Соціально-психологічної.
- Соціально-економічної.

Отже, до способу життя людини належать: активна участь людини в процесі формування умов життя, її адекватна реакція на зміну умов навколишнього середовища, а також праця, побут, задоволення матеріальних і духовних потреб у суспільному житті, норми і правила поведінки.

Слід пам'ятати, що людина — суб'єкт і одночасно — головний результат своєї діяльності. Культура з цієї точки зору — це самосвідоме ставлення до самого себе. Однак люди дуже часто нехтують своїм здоров'ям, ведуть неправильний спосіб життя, не дотримуються режиму переїдають, курять. Тому для здоров'я потрібні знання, які увійшли б у повсякденну звичку людини.

Не завжди в житті людини здоров'я займає перше місце порівняно з речами та іншими матеріальними благами. У результаті це призводить до шкоди не лише своєму здоров'ю, а й здоров'ю майбутніх поколінь. Отже, здоров'я повинно займати перше місце в ієрархії потреб людини.

На превеликий жаль, ціну здоров'я більшість людей усвідомлює лише тоді, коли воно значно похитнулось. Лише тоді виникає прагнення вилікувати захворювання, стати здоровим.

Нерозумне і довге випробовування стійкості свого організму нездоровим способом життя (алкоголь, нікотин). Тільки через певний час спрацьовують зворотні зв'язки у людини, коли вона полишає шкідливі звички, проте, часто запізно.

Джерелом навичок з цього питання є, передусім, приклад батьків, допомагає також і санітарна освіта. Важливим фактором, що визначає реакцію людини на екстремальну ситуацію, є її психофізичні якості та загальний стан. Вони проявляються через чутливість людини до виявлення сигналів небезпеки перед реакцією на них. Показники, які зумовлюють можливості людини виявити небезпечну ситуацію та адекватно відреагувати на неї, залежать від її індивідуальних особливостей, зокрема від її нервової системи. На поведінку людини у небезпечній ситуації впливає й її психічний та фізичний стан.

Відомо, що 80 % більшості хвороб мають психосоматичний характер, тобто значною мірою залежить від стану душі людини, який визначає її безпечну поведінку.

Сучасна людина зустрічається з багатьма факторами ризику, що негативно впливають на стан й нервової та серцево-судинної систем, знижує опірність організму. При цьому виникає стресова реакція організму. Так, наприклад, психічна травма, отримана внаслідок конфлікту, виводить людину з нормального психічного стану, що може призвести до суттєвих змін у виконанні професійних функцій і загального функціонального стану. У перекладі «стрес» означає «напруження», тобто відповідь організму на поставлену перед ним проблему.

Велике значення для розвитку стресового стану має поведінка в екстремальних умовах (аварія, кримінальна ситуація, стихійне лихо). Неправильна поведінка у таких ситуаціях найчастіше є причиною шкідливих наслідків стресу. Вона зумовлює результат стресу більше, ніж фактори зовнішнього середовища. У цих випадках стрес може виявитись у вигляді паніки, суєти, істерики.

Це захисна реакція організму на зовнішні надзвичайні подразники і ситуації, тривалі негативні емоції. Він супроводжується підвищеним серцебиттям, виснаженням і зривом адаптаційних і імунних систем організму та іншими змінами. До певної межі стрес сприяє вирішенню людиною певних завищених завдань і навантажень. Однак, у разі перевищення цієї межі в організмі людини виникають порушення механізмів саморегуляції, відбувається погіршення трудової діяльності і стануться зриви, які призводять до виникнення небезпечних ситуацій. При стресових ситуаціях різко підвищується вміст адреналіну у крові, посилюється робота серця, звужуються кровоносні судини, підвищується температура тіла і рівень глюкози у крові. У результаті в організмі виникають фізіологічні порушення, розлади нервової, серцево-судинної систем та ін. До цих розладів належать нервовість,

роздратованість, тривога, агресивність, втома, загострення хворобливих станів.

Тривала стресова ситуація призводить до багатьох психосоматичних захворювань: психозів, неврозів, захворювань мозку, серцево-судинних захворювань, інфаркту, гіпертонічної хвороби, шлунково-кишкових захворювань, зниження імунітету, онкологічних захворювань.

4.3 Висновок до четвертого розділу

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи.

Також розглянуто питання здорового способу життя та його вплив на професійну діяльність, структури системи БЖД, елементів теорії, що відповідають моделі безпеки життєдіяльності.

ВИСНОВКИ

Причиною обрання даної теми стало швидке зростання технологій, особливо Інтернету речей, але, на жаль, їхня безпека бажає кращого. Додатки Інтернету речей є найціннішим активом у сучасному технологічному світі. Той факт, що вони задіяні майже в кожному аспекті життя людини, робить їх більш бажаними. Сьогодні вони стали виробниками даних номер один, несучи з собою приватні, конфіденційні, важливі та безцінні дані, які можуть бути використані проти самих же власників пристроїв. Здебільшого ці дані не обробляються, не переміщуються та/або не зберігаються у безпечний спосіб, що робить її вразливою та ідеальною мішенню для зловмисників. Головне завдання цієї роботи - це автоматизувати систему, в якій люди прийматимуть мінімальну участь. В свою чергу, це зменшує витрати на персонал та мінімізує ризики.

Детально розкрито призначення мережевих рівнів моделі OSI для пристроїв IoT, описано їхнє призначення та найбільш вразливі місця. Охарактеризовано найпопулярніші проколи, описано можливості роботи, принцип дії, сфери застосування.

В даній роботі проведено аналіз і порівняння найбільш популярних SIEM рішень, для того, щоб вирішити яку технологію обрати. Після вивчення декількох платформ, я обрав The Elastic Stack SIEM, яка є найбільше підходить під потреби даної роботи, та візуалізує в режимі реального часу.

Було продемонстровано процес налаштування та інтеграції The Elastic Stack SIEM в симулятор IoT, яке успішно себе показало. Адже з перших секунд роботи запит був отриманий системою, що в свою чергу, передано до візуалізації Kibana.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gunter D. Internet of Things [Електронний ресурс] / Davide Gunter – Режим доступу до ресурсу: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot.
2. A. Gupta: The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, 2019. С. 1
3. Рівні моделі OSI [Електронний ресурс] – Режим доступу до ресурсу: http://petroonline.ho.ua/OSI.html.
4. Top 12 most commonly used IoT protocols and standards [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/iotagenda/tip/Top-12-most-commonly-used-IoT-protocols-and-standards.
5. A Complete Guide to IoT Protocols & Standards In 2022 [Електронний ресурс] – Режим доступу до ресурсу: https://www.nabto.com/guide-iot-protocols-standards/.
6. IoT Communication Protocols—IoT Data Protocols [Електронний ресурс] – Режим доступу до ресурсу: https://www.allaboutcircuits.com/technical-articles/internet-of-things-communication-protocols-iot-data-protocols/.
7. What is SIEM? [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/topics/siem.
8. Splunk: what it is, why companies need it [Електронний ресурс] – Режим доступу до ресурсу: https://news.beta80group.it/en/splunk-what-it-is-why-companies-need-it.
9. McAfee Enterprise Security Manager Reviews & Product Details [Електронний ресурс] – Режим доступу до ресурсу: https://www.g2.com/products/mcafee-enterprise-security-manager/reviews.

10. IBM QRadar Tutorial [Електронний ресурс] – Режим доступу до ресурсу: https://mindmajix.com/ibm-qradar-tutorial.
11. What is Elasticsearch? [Електронний ресурс] – Режим доступу до ресурсу: https://www.elastic.co/what-is/elasticsearch.
12. The heart of the free and open Elastic Stack [Електронний ресурс] – Режим доступу до ресурсу: https://www.elastic.co/elasticsearch/.
13. Централізований збір та обробка логів за допомогою Elasticsearch, Logstash та Kibana [Електронний ресурс] – Режим доступу до ресурсу: https://freehost.com.ua/ukr/faq/articles/tsentralizovannij-sbor-i-obrabotka-logov-s-pomoschju-elasticsearch-logstash-i-kibana/.
14. IoT - Simulator [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/rlopezv/iot-simulator/blob/master/README.md.
15. Importance of having a good monitoring system [Електронний ресурс] – Режим доступу до ресурсу: https://pandorafms.com/blog/why-you-need-a-monitoring-system/.
16. Elastic SIEM Review & Alternatives [Електронний ресурс] – Режим доступу до ресурсу: https://www.comparitech.com/net-admin/elastic-siem-review-alternatives/.
17. Iot based monitoring and control system for appliances [Електронний ресурс] – Режим доступу до ресурсу: https://www.ripublication.com/acst18/acstv11n1_04.pdf.
18. Z-Wave Technical Basics [Електронний ресурс] – Режим доступу до ресурсу: https://www.domotiga.nl/attachments/download/1075/Z-Wave%20Technical%20Basics-small.pdf.
19. RFID-технології та магнітні мітки. [Електронний ресурс] – Режим доступу до ресурсу: http://allta.com.ua/what-is-rfid.
20. The Basics of Bluetooth Low Energy (BLE) [Електронний ресурс] – Режим доступу до ресурсу: https://www.novelbits.io/basics-bluetooth-low-energy/.

21. Wi-Fi HaLow (IEEE 802.11ah) [Електронний ресурс] – Режим доступу до ресурсу: https://www.ixbt.com/news/2016/01/05/wi-fi-halow-ieee-802-11ah.html.
22. Наказ Міністерства соціальної політики України «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0508-18.
23. Закон України «Про охорону праці» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2694-12.
24. Наказ Міністерства внутрішніх справ України «Про затвердження Правил пожежної безпеки в Україні» [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0252-15.
25. Державний комітет ядерного регулювання України. Проект від 01.03.2008 р. Консультації щодо підвищення безпеки джерел іонізуючого випромінювання в Україні. Київ, 2008.
26. Білявський Г.О, Бутченко Л.І., Навроцький В.М. Основи екології: Теорія і практикум: Навч. Посібник. Київ, 2002. 352

Додаток А – Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

УДК 004.056
Р. Маслій
(Тернопільський національний технічний університет імені Івана Пулюя,Україна)

СИСТЕМА БЕЗПЕКИ ДЛЯ ІОТ З ВИКОРИСТАННЯМ SIEM ТЕХНОЛОГІЙ

UDC 004.056
R. Maslii

SECURITY SYSTEM FOR IOT USING SIEM TECHNOLOGIES

Вже зараз технологія IoT (Internet of Things) застосовується у широкому побутовому колі та сферах бізнесу, починаючи від розумних будинків, закінчуючи пристроями в космічній промисловості. Кожного разу, коли в систему додається можливість підключення нових пристроїв, збільшуються ризики. На сьогодні немає повністю прийнятної архітектури безпеки IoT систем. Виробники часто жертвують заходами безпеки заради того, щоб як найшвидше вийти на ринок, що може призвести до серйозних проблем у майбутньому для кожного окремого користувача.[1]

SIEM (Security Information and Event Management) є ключовим компонентом корпоративної інфраструктури. Термін SIEM комбінує в собі два управління: керування мережею та керування безпекою. SEM (управління подіями безпеки) здійснює аналіз журналів і кореляції подій (часто в режимі реального часу) для протидії загрозам безпеки та інцидентам. А SIM (управління інформацією про безпеку) – збір та керування журналами та звітність для внутрішніх аудитів або дотримання вимог.

Завдяки програмному забезпеченню SIEM можливо використовувати утиліти, які допомагають оцінити вразливості згідно стандартів. Перш ніж користувач обере той чи інший інструмент для роботи, він повинен розуміти основні принципи роботи моніторингу, наприклад, інструмент повинен відокремлювати нешкідливі невдалі спроби входу від цільових атак. Адже ключовими моментами є:

1. аналіз даних у реальному часі та автоматичне оповіщення користувача;
2. ведення журналу подій;
3. інтелектуальне виявлення загроз на основі архівних даних.

Всі ці дані повинні бути доступні для пошуку та фільтрації, щоб користувачі могли легко і швидко приймати рішення стосовно подальшої роботи. Графіки та лічильники наочно представляють те, що відбувається в системі, саме тому останнім часом більш популярною стає візуалізація даних.

Більшість хмарних постачальників, які надають рішення для IoT (MS Azure, Amazon Web Services, IBM Watson IoT і т.д.), надають надійний набір API та зовнішніх сховищ даних, що можуть бути легко інтегровані в кращі в своєму роді SIEM-рішення. [2] Тобто на етапі проектування в IoT систему можна легко інтегрувати існуючу архітектуру SIEM, що зрештою покращить і надасть додаткову цінність рішенню.

Література

1. Безпека IoT починається з ідентифікації. URL: https://iot-ssl.com.ua/iot_secure.html.
2. IoT and SIEM Integration. URL: https://medium.com/@dtembe/iot-and-siem-integration-pt-1-6645a012bdc.