ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ПРОМИСЛОВИХ ІОТ ІЗ ВИКОРИСТАННЯМ CISCO CYBER VISION»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Григоренко Д.Ю.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. Важливість Інтернету речей і промислового IoT різко зросла з розвитком індустріалізації та промисловості 4.0. Через те, що промислові IoT мережі майже повністю автоматизовані, в деяких випадках напівнезалежні або з мінімальним втручанням людини.

У зв'язку з тим, що нові можливості створюють свої проблеми, кібербезпека цих мереж і конфіденційність їхніх користувачів стали важливими аспектами з масивними взаємопов'язаними пристроями IIoT. Якщо відбудеться кібератака від якої не буде змоги захиститися, то це може призвести до поганих наслідків, наприклад зв'язаною з економікою країни.

Наступний рівень технології IoT, яка унікальна тим, що її застосування повністю змінило виробництво. Сучасним компаніям, які шукають конкурентну перевагу, не варто дивитися далі, окрім можливостей, які надає користувачам Інтернет речей – переваги впливають на все: від технічного обслуговування до логістики постачальників, робочих процесів співробітників і доставлення продукції.

Сьогодні IIoT в основному використовується в рамках додатків Інтернету речей за межами споживчого простору та корпоративного ринку IoT, як загальний термін для програм і варіантів використання в кількох промислових секторах.

Охорона здоров'я вже давно використовує розумні пристрої. Медичні працівники можуть віддалено контролювати пацієнтів і отримувати сповіщення про будь-які зміни стану. Це робить охорону здоров'я точнішою та індивідуальнішою. У майбутньому штучний інтелект може допомогти в діагностиці, дозволяючи лікарям лікувати пацієнтів точніше та ефективніше.

У найближчі роки IIoT, ймовірно, змусить більш уніфіковані протоколи та архітектури пристроїв, які дозволять машинам безперебійно спілкуватися та, таким чином, покращити взаємодію.

Об'єкт дослідження – промислові IoT мережі.

Предмет дослідження – технологія забезпечення безпеки мереж IIoT.

Мета роботи – розробити рекомендації по інсталяції та налаштуванню програмного забезпечення щодо безпеки захисту IIoT.

Завдання:

- дослідити проблематику промислових Інтернет речей з зазначеною хронологією кібератак за весь час.
- розглянути рішення Cisco Cyber Vision для захисту промислових IIoT мереж від кіберзагроз,
- дослідити етапи підготовки встановлення і налаштування програмного забезпечення.
- проаналізувати IIoT мережі,
- виконати огляд Cisco Cyber Vision,
- продемонструвати налаштування програмного забезпечення і основних компонентів та визначити значення практичної частини.

Практичне значення одержаних результатів. Результат та рекомендації по встановленню та налаштуванню всіх компонентів Cisco Cyber Vision щодо безпеки промислових Інтернет речей можуть бути використані у сфері забезпечення кібербезпеки інформаційних систем або промислових мереж.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на конференції:

- Всеукраїнська наукова-технічна конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 82-84 с.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ ПРОМИСЛОВИХ IOT МЕРЕЖ ТА ОСОБЛИВОСТІ ЇХ ЗАХИСТУ

1.1 Аналіз поняття промислові IOT

Промисловий Інтернет речей (IIoT) — це використання інтелектуальних датчиків і приводів для вдосконалення виробничих і промислових процесів. Також відомий, як промисловий Інтернет або Індустрія 4.0, IIoT використовує потужність розумних машин і аналітику в реальному часі, щоб скористатися перевагами даних, які «тупі машини» створювали в промислових умовах роками. Філософія, що лежить в основі IIoT, полягає в тому, що розумні машини не тільки краще за людей збирають і аналізують дані в режимі реального часу, але й передають важливу інформацію, яку можна використовувати для швидшого й точнішого прийняття бізнес-рішень.

Підключені датчики та виконавчі механізми дозволяють компаніям швидше виявляти неефективність і проблеми та економити час і гроші, одночасно підтримуючи зусилля бізнес-аналітики. У виробництві, зокрема, IIoT має великий потенціал для контролю якості, стійких і екологічних практик, відстеження ланцюга постачання та загальної ефективності ланцюга постачання. У промисловому середовищі IIoT є ключовим для таких процесів, як прогнозоване обслуговування, розширене обслуговування на місцях, управління енергією та відстеження активів.

IIoT — це мережа інтелектуальних пристроїв, підключених до систем, які відстежують, збирають, обмінюються й аналізують дані. Кожна промислова екосистема IoT складається з:

- підключених пристроїв, які можуть відчувати, передавати та зберігати інформацію про себе;
- державної та/або приватної інфраструктури передачі даних;

- аналітики та програм, які генерують бізнес-інформацію з вихідних даних;
- зберігання даних, які генеруються пристроями IIoT;
- людей.

Ці периферійні пристрої та інтелектуальні активи передають інформацію безпосередньо в інфраструктуру передачі даних, де вона перетворюється на актуальну інформацію про те, як працює певна частина техніки. Цю інформацію можна використовувати для прогнозного обслуговування, а також для оптимізації бізнес-процесів (рис.1.1).

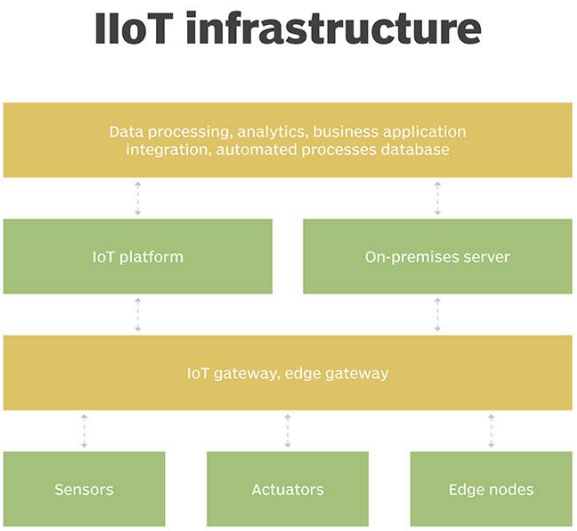

Рис.1.1. Інфраструктура IIoT

Існує незліченна кількість галузей, які використовують IIoT. Одним із прикладів є автомобільна промисловість, яка використовує пристрої IIoT у виробничому процесі. Автомобільна промисловість широко використовує промислових роботів, і IIoT може допомогти завчасно підтримувати ці системи та виявляти потенційні проблеми, перш ніж вони зможуть порушити виробництво.

Сільське господарство також широко використовує пристрої IIoT. Промислові датчики збирають дані про поживні речовини ґрунту, вологість тощо, що дозволяє фермерам вирощувати оптимальний урожай.

Нафтогазова промисловість також використовує промислові пристрої IoT. Деякі нафтові компанії мають флот автономних літальних апаратів, які можуть

використовувати візуальні та тепловізори для виявлення потенційних проблем у трубопроводах. Ця інформація поєднується з даними інших типів датчиків для забезпечення безпечної роботи [1].

1.2 Порівняльний аналіз подібностей та відмінностей між IoT та IIoT

Як правило, IoT зосереджується на зручності споживачів, тоді як IIoT зосереджується на рентабельності інвестицій, щоб компанії отримали найбільшу користь від впровадження IIoT. Якщо порівняти IoT та IIoT з огляду на складність, вартість і вимоги, можна зробити наступне:

Вартість. В основному IoT та IIoT залежать від такого обладнання, як датчики, підключення до Інтернету та вбудованих систем. Але IoT дешевше, ніж IIoT, тому що точність, необхідна для пристроїв IoT, нижча, ніж для пристроїв IIoT. IIoT використовує більш складні пристрої для більшої точності, оскільки IIoT працює в критичних сферах бізнесу, таких як виробництво, моніторинг обладнання тощо.

Складність. Програми IoT є більш просунутими, ніж програми IoT, із зростанням технологічного прогресу зростає і складність. Таким чином, додатки IIoT є більш складними, ніж програми IoT.

Вимоги:

- Кінцевою вимогою до Інтернету речей є зручність для споживача, а кінцевою вимогою до Інтернету речей є рентабельність інвестицій або повернення інвестицій.
- IoT зосереджується на управлінні побутовою технікою, яка підвищує зручність споживачів за коштом економії ресурсів, таких як електроенергія.
- IIoT зосереджується на критично важливих системах, таких як охорона здоров’я, аерокосмічна промисловість, автоматизація виробничого обладнання та об’єднання машин і людей разом з аналітикою даних.
- IIoT хоче, щоб час безвідмовної роботи був вищим, а час простою бізнес-операцій був меншим.

Представлений порівняльний аналіз (табл.1.1.) двох видів промислових мереж [2].

Таблиця 1.1.

Порівняльний аналіз IoT і IIoT

IIOT	IOT
Це описується як використання Інтернету речей у промислових додатках і секторах.	Він описується як фізичні пристрої, такі як мобільні телефони, ПК, побутова техніка та багато інших електронних пристроїв, у які вбудовано датчики, програмне забезпечення та інші технології для передачі даних і спілкування між пристроями через Інтернет.
Приклади: amazon warehouse, smart robotics, Airbus тощо.	Приклади: кондиціонери, датчики, розумні годинники, мобільні телефони тощо.
IIoT працює з великими мережами.	IoT має справу з невеликою мережею.
Пропонує дистанційне програмування на сайті.	Пропонує просте програмування поза сайтом.
Для захисту даних потрібна надійна безпека.	IoT вимагає ідентичності та конфіденційності.
Тривалий життєвий цикл.	Короткий життєвий цикл продукту.
Висока надійність.	Менш надійний.

1.3 Аналіз статистичних даних щодо особливостей розгортання атак на IIoT

Промисловий Інтернет речей, або Індустрія 4.0, покращує операційну ефективність глобальних промислових систем у небачених раніше масштабах. IIoT має великий потенціал для покращення комунікацій, продуктивності, контролю якості, ефективності ланцюга постачання та загального ведення бізнесу. З цим

широким підключенням з’являються нові вектори атак, уразливості та можливості для хакерів.

Збитки від різноманітних кібератак та експлойтів IIoT за останнє десятиліття, вражають. У хронології нижче створено часову шкалу з реальними інцидентами безпеки, щоб продемонструвати масштаби загроз. Багато з них є експлойтами, де вразливість була виявлена та викрита дослідниками та привернула увагу ЗМІ. Наприклад, відомий злом Miller/Valasek Jeep, описаний журналом Wired. Витік даних Target або злом Ukraine Power Grid, який стався в грудні, коли хакери використовували вкрадені облікові дані, щоб отримати віддалений доступ до мережі та відключити енергопостачання понад 200 000 клієнтів.

IIoT охоплює безліч галузей, таких як виробництво, електростанції, енергетичні мережі, напівпровідники, автомобільна, аерокосмічна промисловість і автоматизація комерційних будівель. Тож, незалежно від того, чи йдеться про під’єднання автомобілів, оснащення розумних будівель, створення інтелектуальних міст онлайн чи виробництво на заводах майбутнього, настав час запровадити безпеку в екосистемі Інтернету речей.

Хронологія атак на IIoT.

Stuxnet virus 2005. Цей вірус, який використовувався для атаки на завод зі збагачення урану в Натанзі, Іран, був раннім індикатором вразливості IOT і того, як вони можуть призвести до критичних порушень національної інфраструктури. Дослідники Symantec виявили Stuxnet: рання версія має номер версії в коді, версія 0.5, і, аналізуючи дату реєстрації домену веб-сайту, Stuxnet 0.5, можливо, використовувався ще у 2005 році. Ще одна цікава інформація про цю версію Stuxnet полягає в тому, що він перестав заражати комп’ютери 4 липня 2009 року, за кілька днів до створення версії 1.001.

Hackable heart monitors 2008. Дослідники виявили, що імплантовані серцеві дефібрилятори (ICD) можуть керуватися зовні, дозволяючи зловмисникам перехоплювати медичну інформацію та маніпулювати пристроєм, користуючись перевагами незашифрованих сигналів у вбудованому радіо ICD. Центр безпеки

продемонстрував злам ICD, виготовлений Medtronic, за допомогою ПК, радіообладнання та антени. ІКД на той момент не було у пацієнта.

Puerto rico smart meters 2009. Електроенергопідприємство в Пуерто-Ріко втратило сотні мільйонів доларів після маніпуляції з цифрою споживання електроенергії, що дозволило контролювати інтелектуальні лічильники за допомогою зовнішніх пристроїв, таким чином не точно вимірюючи кількість споживаної електроенергії. ФБР вважає, що відповідальні зламали інтелектуальні лічильники за допомогою оптичного перетворювача, наприклад інфрачервоного світильника, підключеного до ноутбука, який дозволяє інтелектуальному лічильнику спілкуватися з комп'ютером. Після підключення параметри запису споживання електроенергії були змінені за допомогою програмного забезпечення, яке можна завантажити з Інтернету. Також вважалося, що сильні магніти, розміщені на пристроях для уповільнення лічильників, також використовувалися, особливо вночі, у деяких випадках [3].

Medtronic insulin pumps 2011. Програмне забезпечення та спеціальна антена дозволяли дослідникам знаходити та контролювати будь-який пристрій у межах 300 футів через його радіопередавачі, потенційно змушуючи його закачувати надмірну кількість інсуліну в кров.

Water utility system (SCADS) 2011. Хакери знищили водопровід за межами міста Іллінойс, отримавши доступ до промислової системи контролю. Їм вдалося спалити один із помпи комунального підприємства, змусивши систему SCADA, яка керувала помпа, постійно вмикати та вимикати помпу. Зловмисники почали свою атаку з IP-адрес та отримали доступ, спочатку зламавши мережу постачальника програмного забезпечення, яке створює систему SCADA, яку використовує комунальне підприємство. Хакери викрали імена користувачів і паролі, які постачальник підтримував для своїх клієнтів, а потім використовували ці облікові дані для отримання віддаленого доступу до мережі комунального підприємства.

Bashlite Botnet 2014. BASHLITE заразив понад 2 млн пристроїв за два роки. Поширюючись за допомогою грубої сили, BASHLITE зміг запускати кілька типів

великомасштабних DDoS-атак одночасно. Версія 2020 також може розгортати майнінг криптовалюти та зловмисне програмне забезпечення.

University of michigan traffic lights 2014. Дослідники захопили контроль над цілою системою з понад 100 перехресть з однієї точки доступу. Система світлофора, яку легко зламати, використовувала бездротові радіостанції для своєї комунікаційної інфраструктури з простим шифруванням і без пароля. Останнім часом дослідники безпеки виявили чотири нові версії ботнету Bashlite. Вони називаються Backdoor.Linux.BASHLITE.AMF, Troj.ELF.TRX.XXELFC1DFF002 і Trojan.SH.BASHDLOD.AMF. Одна з цих версій використовується для націлювання на пристрої з API WeMo Universal Plug and Play (UPnP).

German steel mill hack 2014. Хакери використали фішинг, щоб проникнути в мережу німецького металургійного заводу та маніпулювати його елементами керування, щоб зламати безліч систем, зокрема промислові компоненти у виробничій мережі та доменну піч, яку не можна було належним чином зупинити, що призвело до значної шкоди. Відповідно до звіту, опублікованого Інститутом SANS, хакери атакували персонал сайту та отримали доступ до мережі металургійного комбінату за допомогою фішингової атаки. Цілком ймовірно, що електронний лист містив вкладений документ, який після відкриття запустив шкідливий код у мережах сталеливарного заводу. Потім, використовуючи вразливі місця в програмах, запущених у цільовій системі, код створив віддалену точку з’єднання для встановлення мосту між зловмисниками та цільовою промисловою мережею. На цьому етапі хакерам вдалося перепрограмувати програмовані логічні контролери (PLC), скомпрометувавши функції печі.

Bmw connected drive system 2015. Дослідники використали вразливість у системі Connected Drive від BMW та імітували сервери BMW, щоб надсилати інструкції щодо дистанційного розблокування автомобілям. Тест використовував функцію дистанційного розблокування, яку можна було запитати через лінію підтримки BMW.

Fiat chrysler remote control 2015. Uconnect, інтелектуальна функція, яка контролює розваги та навігацію автомобілів Fiat Chrysler, виявила вразливість, яка

відкривала мікросхему головного пристрою автомобіля для шкідливого коду, який, своєю чергою, міг використовуватися для надсилання команд для маніпулювання фізичними компонентами, включаючи рульове керування. і гальма.

Ukranian power grid 2015. Хакери скомпрометували внутрішню корпоративну мережу через електронні листи з фішинговими шкідливими програмами. Потім їм вдалося захопити контроль над мережею SCADA і вимкнути підстанції, залишивши без світла 230 тисяч людей. Зловмисне програмне забезпечення також вимикало пристрої контролю IoT, імплантувавши шкідливе програмне забезпечення на пристрої. Вважається, що перша частина атаки спрямована на оновлену версію шкідливого програмного забезпечення BlackEnergy. Шкідливий код було надіслано через електронні листи зі шкідливими вкладеннями, націлені на конкретних осіб у різних енергетичних компаніях, щоб отримати облікові дані адміністратора та отримати доступ до мереж енергетичних підстанцій. Під час другої частини атаки актори активували руйнівну шкідливу програму KillDisk, яка змогла знищити частину жорстких дисків комп'ютерів і запобігти перезавантаженню систем, що зрештою призвело до відключень електроенергії. Зрештою хакери запустили TDoS-атаку (телефонна відмова в обслуговуванні), спрямовану на кол-центр клієнтів, не даючи абонентам повідомити про збій. Інцидент в Україні – це перша публічно визнана атака з використанням цифрової зброї, яка вдарила по електромережі та спричинила перебої в електропостачанні. Це також перший випадок, коли кібератака, яка спричиняє збої в електропостачанні, була здійснена повністю віддалено [4].

Tesla model s reote hack 2016. Дослідники дистанційно зламали немодифіковану Tesla Model S і заволоділи мультимедійною системою та дисплеями приладової панелі, встигаючи вмикати покажчики повороту та відкривати двері без ключа. Також під час руху встигли ввімкнути склоочисники, скласти бокове дзеркало та відкрити багажник.

Miral botnet 2016. Сумно відомий ботнет IoT Mirai скористався перевагами пристроїв IoT зі слабкими паролями або паролями за замовчуванням і отримав контроль над великою кількістю скомпрометованих телевізійних камер і

маршрутизаторів, використовуючи їх для запуску DDoS-атаки, яка паралізувала великі частини Інтернету, включаючи Twitter, Guardian., Netflix, Reddit і CNN. Потім вихідний код було випущено в дику природу.

Nyadrop selfupdating malware 2016. Ця атака грубою силою була спрямована на пристрої 10T шляхом перегляду величезного списку поширених імен користувачів і паролів, доки не було отримано доступ. Потрапивши в систему, NyaDrop скинув інше шкідливе програмне забезпечення на пристрій-жертву. Зловмисне програмне забезпечення було важко діагностувати та видалити, оскільки воно само видалялося та змінювалося кожного разу, коли успішно проникало в систему.

Hajime vigilante botnet 2016. Більш складний, ніж Mirai, Hajime боровся б з конкурентними ботнетами за контроль над пристроєм. Hajime не мав інструментів для DOS-атак, лише способи продовжувати розширювати охоплення та продовжувати боротьбу з іншими ботнетами. Він відомий тим, що залишає химерні повідомлення, наприклад «Будьте обережні!» на скомпрометованих системах.

CCTV botnet 2016. Цей ботнет викрав 25,5 тис. підключених до Інтернету камер відеоспостереження для здійснення мережевих атак на онлайн-магазини. Масштабна операція змогла регулярно заповнювати веб-сайти 35 тисячами HTTP-запитів на секунду. Це може перерости в цунамі з 50 тисяч HTTP-запитів на секунду, якщо не буде вжито захисних заходів.

Fitbit vulnerability 2017. Дослідники виявили, що деякі продукти Fitbit були вразливі до вторгнень, і що повідомлення, що передаються між фітнес-трекерами та хмарними серверами, можуть бути перехоплені. Потрапивши у внутрішню мережу, хакери можуть маніпулювати даними та ділитися ними з третіми особами.

Reaper botnet 2017. Вважається, що ботнет Reaper, який є розвитком Mirai, заразив до 1 мільйона пристроїв, що робить його найбільшим ботнетом IoT в історії. Він взяв під контроль вбудовані пристрої, заражаючи камери, маршрутизатори, ящики для зберігання тощо. Reaper особливо небезпечний, тому що його код можна легко оновити для запуску наступних атак через бот-мережі в черзі. Reaper проводить сканування перед доставкою корисного вантажу. Перша

хвиля складається зі сканування SYN портів TCP у такому порядку: 20480, 20736, 36895, 37151, 22528, 16671, 14340, 20992, 4135, 64288, 45090, 21248, 21504, 31775, 39215, 47. Перша хвиля сканування виконується з ідентичним вихідним IP-адресою та вихідним портом у кожному пакеті SYN. Сканування, ймовірно, є спробою зняти відбитки пальців пристроїв. Коли він знаходить пристрій IoT, його IP-адреса передається робочому процесу експлойту.

Reaper починає свою останню фазу сканування, коли IP-адреса передається процесу експлойту. На відміну від попередніх ботнетів IoT або варіантів Mirai, Reaper не використовує грубу силу Telnet із обліковими даними за замовчуванням, а скоріше використовує HTTP-експлойти відомих уразливостей в IoT. Reaper сканує TCP-порти 80, 8080, 81, 88, 8081, 82, 83, 8060, 10000, 8443, 8880, 3000, 3749, 1080, 84, 8090, 8001 і 1080 і намагається відкрити порт сервера та запустити один з дев'яти експлойтів, включених до ботнету [5].

Amsesia botnet 2017. Amnesia була спрямована на невиправлену помилку виконання коду ret-note у пристроях DVR, вразивши приблизно 227 тис. пристроїв, отримавши повний контроль і дозволивши зловмисникам запускати широкі DDoS-атаки розміру Mirai на цілі по всьому світу.

Persirai botnet 2017. Дотримуючись кроків Mirai, Persirai завантажила програмне забезпечення DDoS на камери з підключенням до Інтернету та заразила понад 120 тисяч пристроїв тисячі різних марок і моделей камер.

Saudi petrol chemical plant attack 2018. Зловмисники отримали віддалений доступ до інженерної робочої станції, розгорнувши шкідливе програмне забезпечення, яке перепрограмувало контролери SIS. Після цього вдалося спровокувати вибух, який завдав фізичної шкоди інфраструктурі заводу.

Thinkphp exploitation 2018. Зловмисники використали CVE-2018-20062, уразливість віддаленого виконання коду (RCE) у китайському фреймворку PHP з відкритим вихідним кодом ThinkPHP, щоб імплантувати різноманітне шкідливе програмне забезпечення, яке використовується для розповсюдження майнерів криптовалюти. Хоча в основному він був націлений на веб-сервери, він також заразив велику кількість пристроїв IoT.

Amazon ring hack 2019. Хакер зміг спостерігати та спілкуватися з 8-річною дівчинкою в Міссісіпі, зламавши камеру Amazon Ring, яку її батьки встановили в її спальні, використовуючи пароль, знайдений в онлайн-базі даних з раніше зламаною інформацією для входу.

Silex linux malware 2019. Хакер використав новий тип шкідливого програмного забезпечення, щоб блокувати до 4K незахищених пристроїв IoT, що працюють на операційних системах Linux або Unix, які мали відомі або вгадані паролі за замовчуванням. Зловмисне програмне забезпечення знищує сховище пристроїв, видаляє брандмауери та мережеву конфігурацію та, зрештою, блокує їх, унеможливлюючи завантаження.

Two million tareovet 2019. Дослідники виявили, що камери безпеки 2M, радіоняні та розумні дверні дзвінки можна використовувати для стеження за їхніми власниками без будь-якої ручної настройки — без відомого виправлення виявленої вади. Метод атаки простежується до двох уразливостей в одноранговому однорангове технологічне рішення iLnkP2P, розроблене Shenzhen Yunni technology.

Philips hue lightbuld 2020. Дослідники показали, як одна розумна лампочка може заразити всю мережу, захопивши контроль і завантаживши її шкідливим програмним забезпеченням, змушуючи її працювати з ладу.

Sweyntooth family 2020. Дослідники помітили сімейство з 12 уразливостей у комплектах розробки програмного забезпечення BLE, що належать 6 основним постачальникам систем на чіпі. Уразливості дозволяють зловмисникам у радіусі радіозв’язку викликати збої, блокування, переповнення буфера та навіть обходити захист. Bluetooth Low Energy (BLE) — це технологія безпроводового зв’язку, спеціально розроблена для подовження терміну служби батареї пристроїв з різним енергоспоживанням і можливостями використання. BLE складається з набору багатьох стандартизованих протоколів, які забезпечують віддалене підключення та безпеку між простим пристроєм (периферійним) і пристроєм користувача (центральним), яким зазвичай є смартфон або ноутбук. Відповідна взаємодія між обома пристроями.

Dark nexus botnet 2020. Dark Nexus швидко розвивається з понад 40 версіями за три місяці, а також містить понад 1,3 тисячі ботів. Його вихідний код повторно використовує компоненти з BASHLITE та Mirai, але цей ботнет також може маскувати зловмисний трафік, який він спрямовує на ціль, щоб виглядати як законний трафік веб-браузера. Отримавши доступ, Dark Nexus виконає команди оболонки, намагаючись запобігти перезавантаженню ураженого пристрою, перш ніж зупинити низку процесів. Потім він підключається до сервера C2, щоб завантажити список IP-адрес для здійснення DDoS-атак. Dark Nexus також має можливість SOCKS, хоча на момент публікації жодного екземпляра Dark Nexus, що використовує цю функцію, не спостерігалося. Можливо, що оператори Dark Nexus мають намір продати цю можливість пізніше, або вона була присутня в коді, взятому з Mirai або Qbot.

Kaiji malware 2020. Дослідники виявили різновид шкідливого програмного забезпечення, спеціально створене для зараження пристроїв IoT і серверів на базі Linux. Ботнет Kaiji закодовано з нуля та виконує атаки методом грубої сили через порти SSH, відкриті в Інтернеті. Хоча спочатку виявлена версія шкідливого ПЗ здається неповною, дослідники уважно стежать за її розвитком [6].

1.4 Виокремлення проблематики щодо захисту IIoT від кіберзагроз

Прийняття IIoT може революціонізувати роботу галузей, але існує проблема, пов’язана з розробкою стратегій для посилення зусиль з цифрової трансформації, зберігаючи при цьому безпеку на тлі розширеного зв’язку.

Можна очікувати, що галузі та підприємства, які працюють з оперативними технологіями, будуть добре обізнані в таких аспектах, як безпека працівників і якість продукції. Однак, враховуючи те, що OT інтегрується в Інтернет, організації бачать впровадження більш інтелектуальних і автоматизованих машин у роботі, що, своєю чергою, запрошує низку нових викликів, які потребуватимуть розуміння внутрішньої роботи IIoT.

При реалізації IIoT необхідно зосередитися на трьох сферах: доступності, масштабованості та безпеці. Доступність і масштабованість вже можуть бути другою натурою промислових операцій, оскільки вони вже можуть бути створені або працювати в бізнесі досить давно. Проте багато хто може спіткнутися під час інтеграції IIoT у свої операції з безпекою. По-перше, багато компаній досі використовують застарілі системи та процеси. Багато з них функціонують десятиліттями й тому залишаються незмінними, що ускладнює впровадження нових технологій.

Крім того, поширення інтелектуальних пристроїв породило вразливість системи безпеки та занепокоєння щодо підзвітності безпеки. Прихильники Інтернету речей несуть фактичну відповідальність за безпеку налаштування та використання підключених пристроїв, але виробники пристроїв зобов'язані захищати своїх споживачів під час випуску своїх продуктів. Виробники повинні мати можливість гарантувати безпеку користувачів і вживати профілактичних заходів або виправлення у разі виникнення проблем із безпекою.

Навіть більше, потреба в кібербезпеці висувається на перший план, оскільки з роками з'являються все більш серйозні інциденти безпеки. Хакери, які отримують доступ до підключених систем, означають не лише наражання бізнесу на серйозний злом, але також означають потенційну зупинку операцій. До певної міри галузі та підприємства, які впроваджують IIoT, повинні планувати та працювати як технологічні компанії, щоб безпечно керувати як фізичними, так і цифровими компонентами.

Користувачі також стикаються з проблемою правильної інтеграції промислових операцій з IT, де як з'єднання, так і інформація повинні бути захищені. Дані користувачів слід обробляти відповідно до чинних норм конфіденційності, таких як Загальний регламент захисту даних (GDPR) Європейського Союзу (ЄС). Хоча зібрані дані відіграють важливу роль у створенні розуміння для пристроїв та інфраструктури, вкрай важливо, щоб особиста інформація була відокремлена від загальних даних журналу. Таку інформацію, як ідентифікаційна інформація (PII), слід зберігати в зашифрованій базі даних.

Зберігання незашифрованої інформації разом з іншою відповідною діяльністю в хмарі може означати, що підприємства ризикують стати жертвою.

Однією з головних проблем, пов'язаних з IoT, є технологічна фрагментація, і IIoT, відповідно, не є винятком зі співіснування різних стандартів, протоколів і архітектур. Різне використання в системах IIoT, наприклад, стандартів і протоколів, таких як Message Queuing Telemetry Transport (MQTT) і Constrained Application Protocol (CoAP), може перешкоджати сумісності систем IIoT.

Ризики для мереж IIoT. Багато проблем безпеки, пов'язаних з IIoT, виникають через відсутність базових заходів безпеки. Прогалини в безпеці, як-от відкриті порти, неадекватні методи автентифікації та застарілі програми, сприяють виникненню ризиків. Поєднавши це з прямим підключенням мережі до Інтернету, і отримують більше потенційних ризиків.

Компанії, можливо, вже знайомі з можливим впливом на бізнес відмова IT-систем через кіберзлочинність або зараження зловмисним програмним забезпеченням. Однак конвергенція IT та OT створює новий значний фактор ризику: реальні загрози, які можуть вплинути навіть на цивільних.

Незахищені системи IIoT можуть призвести до збоїв у роботі та грошових втрат, серед інших значних наслідків. Більше підключених середовищ означає більше ризиків для безпеки, як-от:

1. Уразливості програмного забезпечення, які можна використати для атаки на системи.
2. Загальнодоступні пристрої та системи, підключені до Інтернету.
3. Зловмисна діяльність, як-от хакерство, цілеспрямовані атаки та витік даних.
4. Маніпуляції з системою, які можуть спричинити порушення роботи або саботаж процесів.
5. Збій у роботі системи, який може призвести до пошкодження пристроїв і фізичних об'єктів або травмування операторів або людей поблизу.
6. Системи OT, утримувані для вимагання, як скомпрометовані через IT-середовище.

Сумнозвісним прикладом с компрометації системи OT через IT-середовище є кібератака на енергомережу в Україні в грудні 2015 року, коли зловмисник зміг заразити IT-інфраструктуру, вимкнувши критичні системи та порушивши електропостачання в тисячах домогосподарств [7].

Для кращого розуміння представлена базова еталонна архітектура безпеки в новому середовищі IT/OT (рис.1.2.).

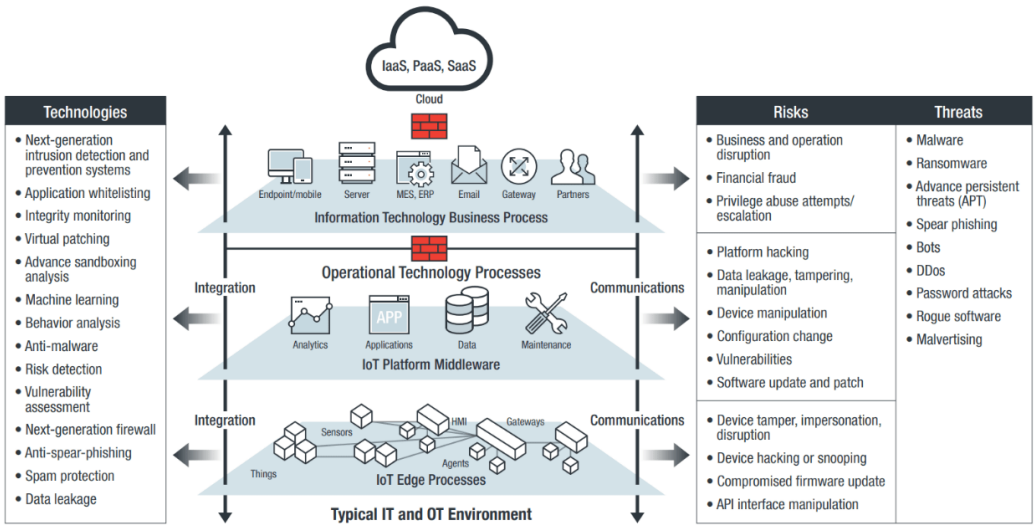

Рис.1.2. Базова еталонна архітектура безпеки в новому середовищі IT/OT

Проблеми з промисловою інтеграцією IoT:

- **Висока інвестиційна вартість.** Однією з найбільш очевидних проблем промислового Інтернету є висока вартість впровадження. Звичайно, одне з головних обіцянок Інтернету речей полягає в тому, що він може зменшити витрати шляхом кращого управління активами, доступу до бізнес-аналітики та підвищення продуктивності. Однак організаціям важко виправдати витрати, коли A: вони не зовсім впевнені, якої рентабельності інвестицій чекати, і B: вони не мають досвіду впровадження підключених систем. Відповідно до звіту Microsoft IoT Signals за 2019 рік, 29% організацій повідомили, що нестача ресурсів була однією з головних причин відкладання впровадження IoT.

- **Безпечне зберігання та керування даними.** Пристрої IoT генерують тонну даних. Згідно з офіційною документацією IDC за 2018 рік, до 2025 року глобально генеруватиметься 160 зетабайт даних частично завдяки зростанню

впровадження пристроїв Інтернету речей промислового рівня. Проблема полягає в тому, що цей величезний обсяг даних потрібно обробляти надзвичайно швидко, щоб виявити закономірності в режимі реальної години. Враховуючи рівень безпеки, якого вимагають технології IIoT, організації повинні розробити план оптимізації моніторингу, управління та зберігання даних, що дозволить швидко реагувати на вхідні загрози. Це означає, що організації повинні планувати безпечні короткострокові рішення для зберігання (наприклад, периферійні обчислення), а також довгострокові рішення (хмара чи центри обробки даних) для довгострокового зберігання. Крім того, статистичні дані в режимі реальної години необхідні для економії коштів і запобігання простою. Наприклад, організація може використовувати датчики для моніторингу продуктивності основного обладнання. У цьому випадку система повинна мати можливість виявляти зношення, що відбувається, дозволяючи користувачам виправляти проблеми до того, як вони призведуть до збоїв у виробництві, що може коштувати організації втрати часу та грошей. Варто також зазначити, що введення всіх цих нових датчиків, пристроїв та програмного забезпечення також може ввести різні типи даних, які організація ще не в змозі обробляти. Наприклад, виробнича компанія може використовувати систему планування ресурсів підприємства (ERP) або систему планування потреб у матеріалах (MRP), яка використовує реляційну базу даних для відстеження запасів, сировини, SKU, ціноутворення та вхідних замовлень. Проблема полягає в тому, що датчики IoT можуть генерувати різнорідні дані, якими керують нереляційні бази даних. А щоб компанії могли отримати максимальну віддачу від підключеної системи, дані ERP, записи про клієнтів та статистичні дані IoT мають бути об'єднані в одному підключеному поданні. Інша ключова проблема IIoT полягає в тому, що навіть якщо організація здатна впровадити всі необхідні датчики, програмне забезпечення та обладнання, її рентабельність інвестицій може бути реалізована лише за умови, що організація має правильні інструменти та досвід.

- **Перебої у з’єднанні.** Одна з ключових промов, яку підприємства повинні врахувати перед тим, як зазнати великої трансформації IIoT, полягає в

тому, що є потреба в постійному безперебійному з'єднанні. Проблема полягає в тому, що навіть якщо просто казати про безперебійну роботу Інтернету, досягти 100% доступності майже неможливо. Незалежно від того, через технічне обслуговування чи інше, в певний момент з'єднання може бути втрачено. Таким чином, організаціям потрібно буде знайти відповідного постачальника для задоволення вимог підключення, щоб уникнути простоїв. На жаль, вимоги відрізняються залежно від галузі. Згідно з дослідженням McKinsey, організаціям необхідно враховувати діапазон, кількість місць (тобто зв'язок між декількома робочими майданчиками/фабриками) та споживання електроенергії. Наприклад, можна звернути увагу на стільниковий зв'язок, якщо система потребує великої пропускної здатності, тоді як малопотужне рішення дальньої дії може бути найкращим вибором для моніторингу активів протягом багатьох років. З IIoT збої створюють кілька факторів ризику, які виходять за межі роздратування тимчасового збою Wi-Fi. Коли датчики використовують для виявлення таких небезпек, як витік газу, збій може бути справді небезпечним для життя чи смерті. Відключення інтелектуальної електромережі можуть знищити електроенергію для цілої громади.

Висновки до першого розділу

Проаналізовано особливості функціонування промислових IoT мереж та особливості їх захисту. Розглянуто поняття промислових інтернет речей. Представлено порівняльний аналіз подібностей та відмінностей між IoT та IIoT.

Наведено статистичне порівняння найбільш відомих атак на IIoT, яке включає в себе такі відомі атаки як: Ukraine Power Grid, Stuxnet virus, Reaper botnet, Dark nexus botnet, German steel mill hack та інші.

Описано проблематику промислових інтернет речей, з виокремленими поняттями високої інвестиційної вартості, безпечне зберігання та керування даними і перебоїв у з’єднанні.

2 ДОСЛІДЖЕННЯ CISCO CYBER VISION ТА ВИРІШЕННЯ ПРОБЛЕМ IIOT

2.1 Огляд рішення Cisco Cyber Vision для захисту промислових IoT мереж від кіберзагроз

Оскільки багато хто переводить свої промислові операції в цифровий формат і розгортає технології Industry 4.0, глибша інтеграція між IT, хмарою та промисловими мережами наражає промислові системи управління (ICS) на кіберзагрози. Потрібне рішення з кібербезпеки, яке допоможе забезпечити безперервність, стійкість і безпеку промислових операцій.

Cisco Cyber Vision надає власникам активів повну видимість їхніх промислових мереж і стану безпеки OT, щоб вони мали інформацію, необхідну для зменшення поверхні атаки, сегментації промислової мережі та застосування політик кібербезпеки. Розширені можливості моніторингу OT також надають інформацію для підвищення ефективності мережі та дозволяють швидше вирішувати проблеми з роботою. Поєднуючи унікальну периферійну архітектуру, яка вбудовує функції безпеки OT у промислову мережу, і глибоку інтеграцію з провідним портфоліо безпеки Cisco. Cisco Cyber Vision можна легко розгорнути в масштабі, щоб дозволити командам IT та OT працювати разом над створенням інноваційних промислових операцій, одночасно захищаючи глобальне підприємство.

Переваги:

• **Збільшує видимість OT у масштабі.** Легко визначає всі промислові пристрої та схеми їх зв’язку. Cyber Vision вбудовано у промислову мережу.

• **Розуміння положення безпеки OT.** Зменшує поверхню атаки. Cyber Vision виділяє пристрої, які потребують негайної уваги, і пропонує рішення.

• **Підвищення ефективності роботи.** Скорочує час простою та підвищує ефективність. Cyber Vision відстежує події OT, виявляє проблеми з мережею та допомагає швидше вирішувати проблеми.

• **Розширення IT-безпеки на OT.** Конвергенція безпеки. Cyber Vision забезпечує інструменти IT-безпеки багатими відомостями про пристрої та події OT.

Основний інструмент для захисту промислових операцій:

Видимість, вбудована у промислову мережу. Cyber Vision вбудовує можливості видимості в промислове мережеве обладнання. Немає потреби купувати спеціалізовані пристрої безпеки та думати про те, як їх встановити. Немає потреби будувати позасмугові мережі, щоб надсилати потоки промислової мережі на центральну платформу безпеки. Менеджери мережі оцінять унікальну простоту та низьку вартість архітектури Cyber Vision.

Незрівнянна видимість усіх підключених активів. Cyber Vision визначає активи, їхні характеристики та шаблони зв’язку шляхом пасивного захоплення та декодування потоків промислових додатків. Цей над безпечний підхід можна покращити за допомогою активного виявлення, яке надсилає запити в семантиці конкретного протоколу ICS. Ці запити надсилаються датчиками, вбудованими в мережеве обладнання, тому їх не блокують брандмауери або межі трансляції мережевих адрес (NAT), допомагаючи забезпечити 100% видимість.

Оперативна інформація для OT. Cyber Vision записує всі потоки додатків у промисловому середовищі, щоб надати інформацію про проблеми мережі, неправильну конфігурацію пристроїв, проблеми зв’язку, несподівані зміни промислових процесів, зловмисний трафік тощо. Це допомагає покращити продуктивність мережі, вирішувати проблеми з виробництвом і вживати заходів для підтримки цілісності системи та скорочення часу простою.

Безпека для IT. Cyber Vision поєднує аналіз протоколів, виявлення вторгнень, виявлення вразливостей і аналіз поведінки, щоб допомогти зрозуміти ідеальну безпеку. Програмний продукт автоматично розраховує показники ризику, щоб власники могли визначити пріоритетність того, що потрібно виправити. Він

також містить вказівки щодо того, що потрібно зробити, щоб була можливість завчасно побудувати процес вдосконалення для усунення ризиків.

Розширення IT-безпеки на OT. Інвентаризація активів Cyber Vision і видимість подій OT мають цінність як для операцій, так і для команд безпеки. Готові інтеграції з портфоліо кібербезпеки Cisco, а також із широким набором рішень сторонніх розробників розширюють знання Cyber Vision на наявні інструменти. Команди безпеки матимуть доступ до IT- і OT-доменів, щоб керувати ризиками та запроваджувати політику безпеки в усьому світі [8].

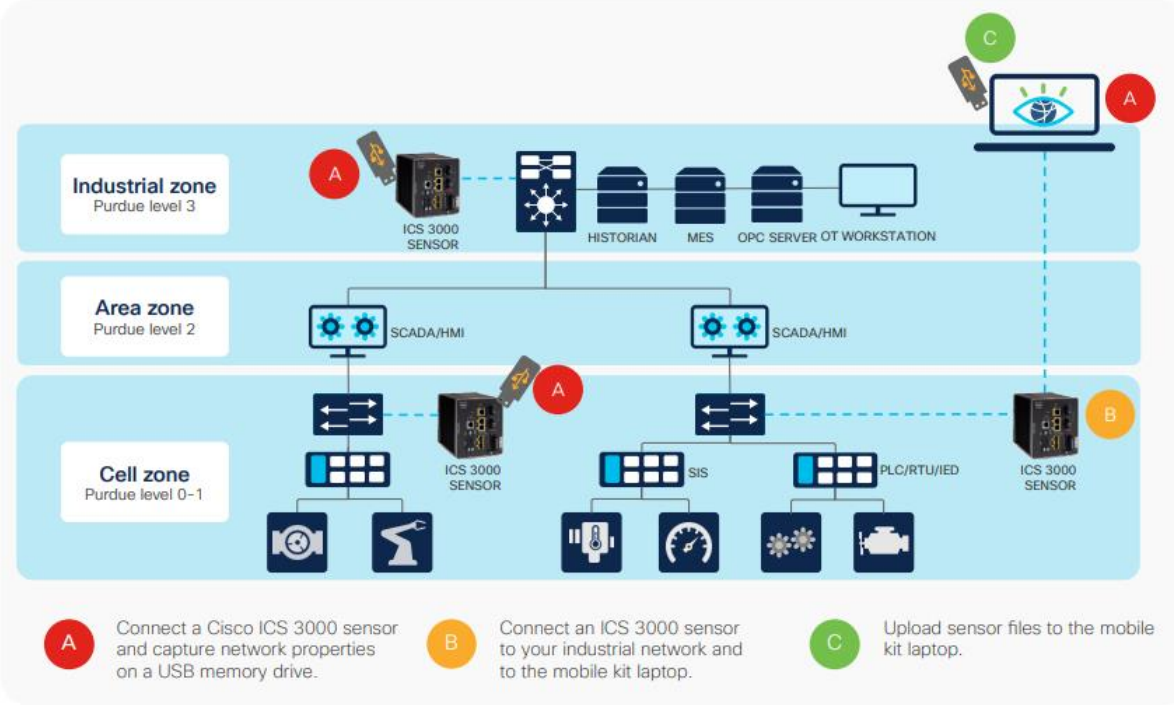

Рис.2.1. Приклад схеми промислової мережі

Пристрої IoT почали відігравати важливу роль у мережах OT (рис.2.1.). IP-камери тепер контролюють критично важливі системи, а розумні датчики у виробничих середовищах передають цінні дані безпосередньо в хмару. Ці розробки покращили якість і зробили процеси швидшими, ніж будь-коли. Однак ці події також несуть ризики, які можуть зробити промислове середовище вразливим[9].

Багато припущень щодо найкращих методів захисту промислових мереж і критично важливих промислових систем управління більше не є дійсними. Традиційні заходи, такі як «безпека через невідомість», розрив повітря або

створення промислової демілітаризованої зони, вже недостатні для захисту промислового середовища. Ізоляція промислових мереж не завжди ефективна, а повітряні проміжки роблять дані недоступними та запобігають зміні конфігурації та виправленню. Правда в тому, що багато з цих так званих систем із повітряним зазором рясніють задніми дверима. Наприклад, подумати лише про постачальників і сторонніх технічних спеціалістів, які налаштували власний віддалений доступ для оновлення систем і пристроїв у середовищах OT. Оскільки кібератаки на промислові середовища стають частішими та складнішими, члени правління та державні регулюючі органи тиснуть на організації, щоб переконатися, що ці ризики контролюються, а критичні для бізнесу мережі IoT/OT належним чином захищені. Виконання цього завдання потребує спільного підходу, у якому IT та OT мають рівноправну позицію.

У багатьох організаціях загальну відповідальність за кібербезпеку несуть керівник відділу інформаційної безпеки (CISO) та IT-команда. Вони володіють інструментами, знаннями та методологіями, необхідними для забезпечення безпеки підприємства, і вони часто контролюють бюджет. Однак IT-персонал і персонал SecOps рідко мають необхідний досвід або розуміння операційних технологій і технологій управління процесами. Ця прогалина в знаннях часто змушує IT-персонал і SecOps припустити, що той самий підхід, який вони використовують для захисту IT, працюватиме в середовищі OT [10].

Рішення Cisco Cyber Vision може мати 2- або 3-рівневу архітектуру, яка складається з:

- Граничних датчиків, що встановлюються в промислову мережу. Ці датчики призначені для захоплення мережевого трафіку, декодування протоколів за допомогою механізму Cisco Deep Packet Inspection і надсилання важливої інформації в Cisco Cyber Vision Center.
- Cisco Cyber Vision Center, центральна платформа, яка збирає дані з усіх периферійних датчиків і діє як платформа моніторингу, виявлення та керування всім рішенням.

- За бажанням, глобального центра третього рівня, до якого підключені всі центри, щоб забезпечити централізований огляд усіх центрів, розгорнутих в організації для оповіщення, звітності та функцій управління.

Під час встановлення Центру є можливість налаштувати синхронізацію даних Центру з Глобальним центром. Однак, якщо користувач вирішить налаштувати глобальну інфраструктуру, потрібно спочатку встановити глобальний центр, потім центри та датчики.

З точки зору Cisco Cyber Vision, три важливі мережі будуть залучені до платформи:

- Мережа адміністрування, яка використовується для доступу до інтерфейсу користувача Center (UI) і взаємодії з авторизованими зовнішніми службами (NTP, DNS, API, SIEM тощо).
- Мережа збору, яка використовується для керування всіма датчиками Cisco Cyber Vision. Ця мережа має бути ізольована від робочого трафіку (відокремлена VLAN/підмережа).
- Мережа збору/промислова мережа, яка використовується для всього трафіку промислових установок і/або розглядається зовнішнього з'єднання, яке буде проаналізовано датчиками (зібраний трафік SPAN) [11].

2.2. Вимоги до інсталяції

Перш ніж інсталювати Cisco Cyber Vision як віртуальну машину потрібно переконатись, що перелічені нижче умови виконано.

Гіпервізор**:**

- VMware vSphere 6.x або новішої версії, або Microsoft Hyper-V Server 2016 або новішої версії.

Слід переконатись, що використовуваний гіпервізор налаштовано з правами, необхідними для створення нової віртуальної машини.

Розмір ВМ (мінімум – до 500 компонентів):

- Процесор: Intel Xeon, 8 ядер

- Оперативна пам'ять: мінімум 16 ГБ
- Зберігання: 500 ГБ SSD

Рекомендовано (для 10 000 компонентів без центральної роздільної здатності):

- Процесор: Intel Xeon, 10 ядер
- Оперативна пам'ять: мінімум 32 ГБ
- Зберігання: мінімум 1 ТБ SSD, RAID-10

Для більш ніж 10 000 компонентів або Center DPI:

- Процесор: Intel Xeon, 16 ядер
- Оперативна пам'ять: мінімум 64 ГБ

Зберігання: мінімум 1 ТБ SSD, RAID-10

Необхідні ресурси:

- Одна або дві IP-адреси, залежно від встановленого центру з одним або подвійним інтерфейсом. Подвійний інтерфейс: один інтерфейс отримує дані протоколу від датчиків (мережевий інтерфейс збору даних), інший використовується для доступу до веб-інтерфейсу та для віддаленого адміністрування SSH (мережевий інтерфейс адміністрування) (недоступно для глобального центру або центру, налаштованого з одним інтерфейсом).

Для розгортання центру з функцією датчика на EXSi потрібен додатковий інтерфейс, призначений для DPI.

- IP-адреса для кожного датчика для підключення (бажано у виділеній LAN або VLAN для з’єднань між датчиками та центром, тобто інтерфейсом промислової мережі) (недоступно до глобального центру).
- NTP-сервер, доступний із центру (час зазвичай отримується на маршрутизаторі).
- Ім’я машини, яке має бути унікальним (або налаштованим у DNS, або на кожному клієнті). Це важливо для налаштування безпеки обміну між клієнтом (людьми або API) і Центром [12].

2.3 Вирішення проблем IIoT

Щоб зменшити кіберризики для критичної інфраструктури, NIST розробив структуру кібербезпеки (Framework for Improving Critical Infrastructure Cybersecurity). Він використовує стандарти, інструкції та найкращі практики, щоб допомогти промисловим організаціям почати свої проєкти безпеки OT.

Перша функція фреймворку кібербезпеки NIST – це функція Identify. Ця функція передбачає ідентифікацію не лише фізичних активів, але й даних, персоналу, пристроїв, систем, можливостей і засобів, які складають організацію. Розробка повної стратегії управління ризиками означає повне розуміння як ресурсів, які підтримують критичні функції, так і відповідних ризиків кібербезпеки.

Захист промислових середовищ вимагає постійної видимості кожного пристрою в середовищі на кожному етапі, від моменту потрапляння в середовище до моменту його видалення. Це допомагає організаціям відстежувати вразливості, віддалений доступ для постачальників і виведені з експлуатації активи.

Процес виявлення включає створення автоматизованої інвентаризації активів, яка визначає марки та моделі пристроїв, мікропрограми, антивірусне програмне забезпечення та інші системні фактори для оцінки вразливості активів. Цей процес виявлення мережі для створення перегляду мережі в реальному часі. Так, наприклад за допомогою вкладки активі, показаних на рис.2.2, можна в прямому ефірі моніторити всі компоненти мережі, спостерігати за всіма потрібними змінами. За бажанням продивитись записану інформацію з сервера, яка допоможе своєчасно виявити загрозу.

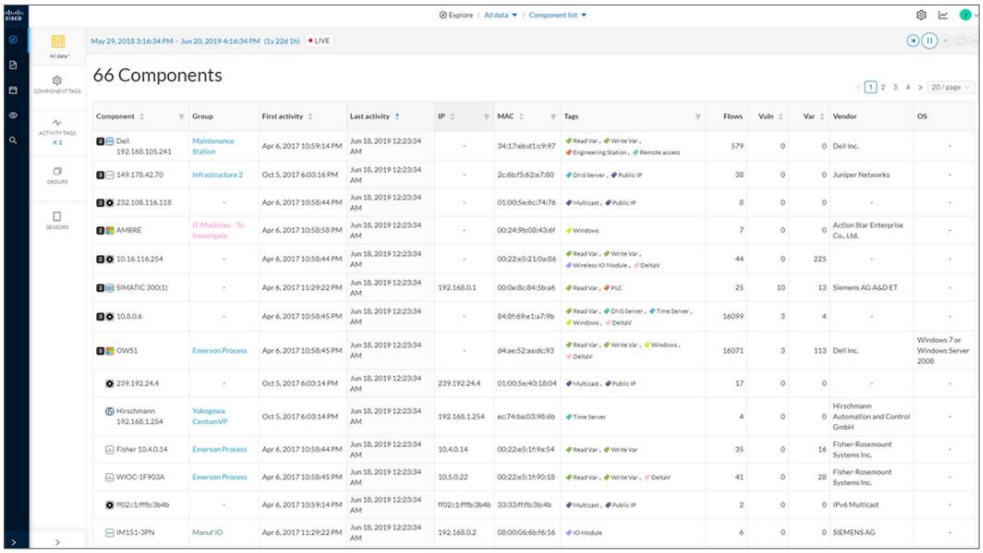

Рис.2.2. Cisco Cyber Vision, що показує детальну інвентаризацію активів

Ключовим результатом є аналіз ризиків для бізнес-процесів. Працюючи разом, команди IT/SecOps і OT можуть розміщувати активи в групи, які представляють ключові процеси, визначати, як ці групи повинні спілкуватися одна з одною, і визначати їх критичність для організації. Завдяки цьому сповіщення про події для кожної групи мають відповідний пріоритет.

Роль OT тут критична. Їм доручено допомогти накласти бізнес-функції та визначити критичність. Команди OT можуть використовувати перегляд мережі OT і активів у режимі реального часу, щоб визначити промисловий вплив на активи, отже, визначаючи пріоритетність подій на основі рівня критичності кожного активу. Цей крок необхідний для побудови ефективної стратегії виявлення та уникнення втоми подій у Центрі безпеки (SOC).

Командам IT/SecOps і OT потрібна комплексна, контекстна картина промислового середовища. Повна та детальна інвентаризація активів, розуміння комунікацій між пристроями та розуміння промислових процесів у реальному часі є життєво важливими, особливо з огляду на мінливе середовище.

Рисунок 2.3, що відображає активи, взаємодії та бізнес-контекст (процеси), дозволяє інженерам OT отримати чітке уявлення про те, як мережа OT працює в різних умовах, краще спланувати безпеку та безперервність виробництва, а також працювати разом із командами IT-кібербезпеки для документування критичних

бізнес-процесів із пов'язаними пристроями. Ці заходи також допомагають командам IT/SecOps розробити дружні до OT процедури та план для кращого захисту та безпеки цих процесів. Передача OT-контексту, розуміння та знань фахівцям з IT/SecOps і аналітикам SOC є фундаментальною для досягнення мети кібербезпеки всієї організації.

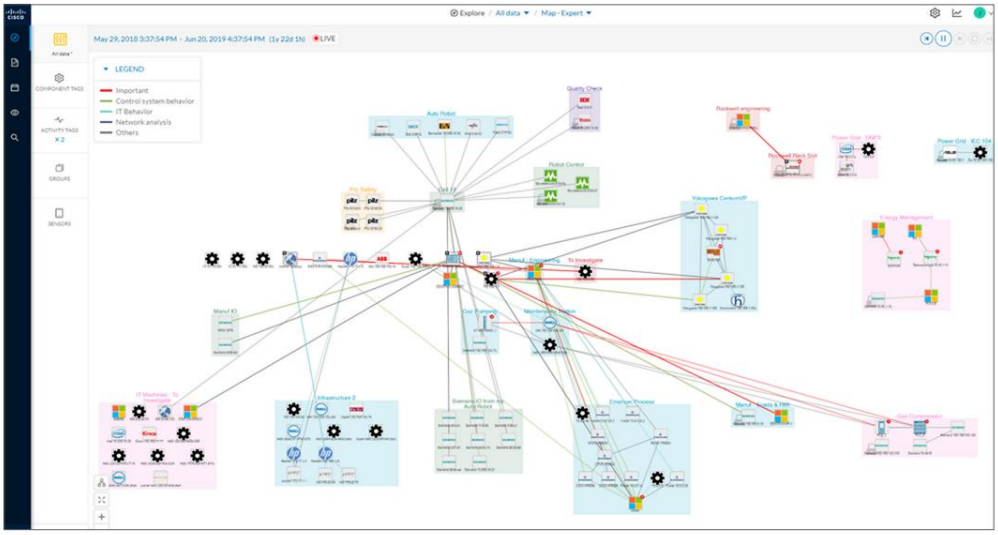

Рис.2.3. Карта мережі Cisco Cyber Vision

Після того, як заходи чітко узгоджені навколо єдиного погляду на мережеві пристрої, процеси та засоби, команди IT/SecOps і OT можуть працювати разом, щоб створити спільну стратегію захисту середовища IoT/OT. Це означає розробку та впровадження відповідних заходів безпеки для забезпечення безперебійної та ефективної роботи промислового середовища.

Функція Protect інфраструктури кібербезпеки NIST підтримує можливість обмежити або стримати вплив потенційної події кібербезпеки. Для цього необхідно розробити мережеву архітектуру, у якій різні елементи промислової мережі розділені на зони, з'єднані між собою за допомогою каналів, як описано в моделі ISA99/IEC 62443.

Типова дія для побудови такої мережевої архітектури включає сегментацію мережі для захисту пристроїв, залучених у критично важливих бізнес-процесах, і для запобігання будь-яким загрозам або зловмисникам від безперешкодного переміщення через мережу. Сегментація дає організаціям можливість ізолювати

загрози та зосереджувати зусилля з виявлення загроз на тих частинах мережі, які є найбільш критичними.

Сегментація за допомогою спеціалізованих промислових рішень, таких як Cisco 3000 Series Industrial Security Appliances (ISA 3000), дозволить IT-спеціалістам і їхнім OT-партнерам створювати локальні правила фільтрації для ізоляції виробничих осередків, промислових зон або комунальних підстанцій, щоб гарантувати, що лише авторизовані пристрої або підключення мали доступ, захищаючи мережу від зловмисних або небажаних дій. Крім того, ці «OT-aware» брандмауери забезпечать рівень захисту для вразливих пристроїв, які просто неможливо виправити.

Сегментацію мережі також можна реалізувати за допомогою контролерів доступу до мережі (NAC), таких як Cisco Identity Services Engine (ISE). Хоча це рішення не пропонує таких можливостей фільтрації чи виявлення загроз, як брандмауери наступного покоління, воно дозволяє організаціям легко впроваджувати політики безпеки, дозволяючи або забороняючи об’єктам можливість спілкуватися один з одним на основі їх ідентифікаційних даних і профілю. Мережеве обладнання автоматично налаштовано для застосування цих політик.

Оскільки цими платформами NAC керує IT, вони не можуть сегментувати промислову мережу без допомоги OT. Профіль кожного з цих промислових активів необхідно додати до платформи, щоб можна було налаштувати політики безпеки. Це можна зробити автоматично, якщо такі продукти, як Cisco Cyber Vision, постійно обмінюються інформацією про активи з інструментом.

Що ще важливіше, розробка OT повинна визначити політику, яку потрібно застосовувати. Саме вони знають, які комунікації слід заборонити, а які потрібні, щоб не порушити виробництво. Цих спільних зусиль між IT і OT можна досягти, сівши разом і вручну визначивши групи активів (зони) і політику зв’язку (проводи). Або OT може використовувати такі інструменти, як Cisco Cyber Vision, щоб налаштувати цю логіку та автоматично надати їй доступ до Cisco ISE, щоб IT-

спеціалісти мали необхідну інформацію для налаштування відповідних політик безпеки.

Функція виявлення системи кібербезпеки NIST передбачає розробку та подальшу реалізацію відповідних заходів для ідентифікації виникнення події кібербезпеки.

Оскільки все більше IT-компонентів розгортається в операційних середовищах, виявлення IT-загроз у промислових мережах стає ще важливішим. Для цього необхідна комбінація захисту кінцевих точок і технологій виявлення та захисту від вторгнень.

Засоби безпеки, які використовуються для сегментації мережі, повинні містити такі можливості, щоб їх можна було використовувати, наприклад, для виявлення зловмисного програмного забезпечення та шкідливого трафіку. Однак, хоча брандмауери нового покоління є ключовими, організаціям потрібні канали аналізу загроз, такі як Cisco Talos і Cisco AMP for Networks, щоб ці брандмауери могли ефективно виявляти широкий спектр відомих і нових загроз.

Організації також повинні запровадити можливості безперервного моніторингу безпеки для контролю цілісності даних. Хоча цілісність даних зазвичай асоціюється з IT-безпекою, вона також застосовна до безпеки OT, коли йдеться про перевірку аномалій процесів шляхом декодування промислового мережевого трафіку та визначення цілісності та легітимності команд у такому трафіку. Організаціям потрібне рішення, яке б розуміло протоколи, що використовуються в цих промислових середовищах, а також знало процеси OT, середовище, активи та правильне використання протоколів.

IT-і OT-персонал повинні працювати разом, щоб визначити, що слід вважати аномалією. Це включає визначення того, яким має бути звичайний промисловий процес, розуміння потенційного впливу аномалії для встановлення рівнів критичності та забезпечення ефективного зв’язку між IT-командами та командами OT, щоб SecOps не потонув у помилкових тривогах під час, наприклад, обслуговування OT.

Під час повсякденної діяльності кожній стороні організації знадобляться різні типи даних і розуміння для оцінки, дослідження та реагування на події безпеки OT. Команди OT стежитимуть за модифікаціями процесу та змінами пристроїв. Команди IT/SecOps відстежуватимуть уразливості та події IDS. А менеджерам SOC знадобиться детальна інформація про активи, представлена на рис.2.4, щоб спростити процес розслідування та налаштування політики.

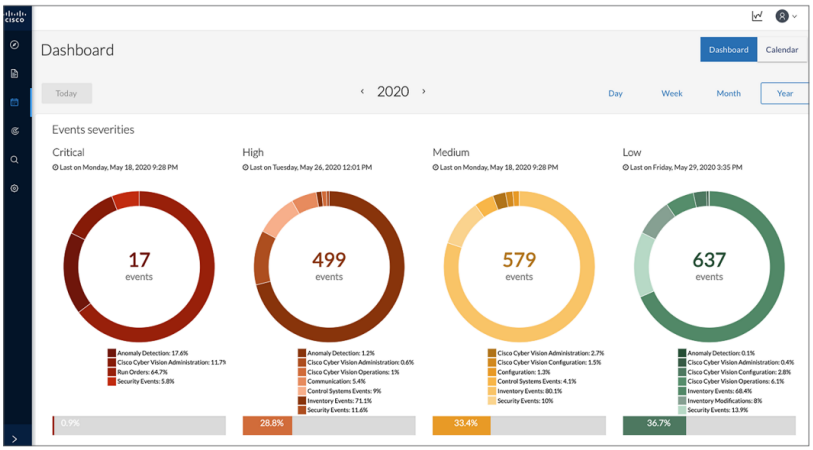

Рис.2.4. Панель подій уразливостей на мережу

Аналітику IT/OT SOC знадобиться повне уявлення про ланцюжок кіберзагроз, який охоплює як IT-мережу підприємства, так і мережу процесів IoT/OT. Контекст OT і здатність тісно інтегрувати IoT/OT в наявні IT.

Інструменти SecOps і SOC дозволять цим командам досягти мети мінімізації кіберризиків для всієї організації. Крім того, однакова детальна інформація, представлена на рис.2.5, часто потрібна для відповідності та нормативних актів, залежно від галузі.

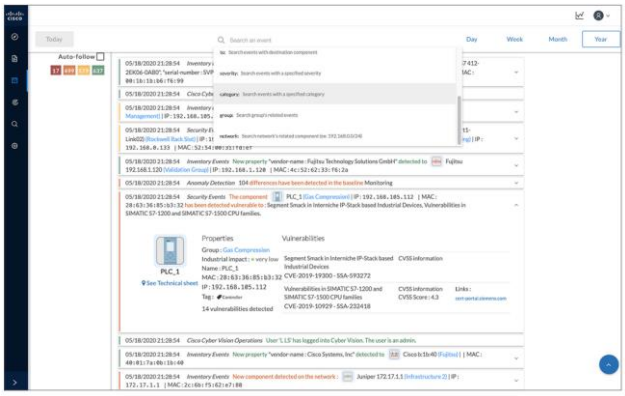

Рис.2.5. Детальна інформація загрози

Унікальна крайова архітектура. Розгортає безпеку IoT/OT у великих масштабах. Датчики Cyber Vision вбудовані в обране мережеве обладнання Cisco, тож не потрібно розгортати спеціальні пристрої чи будувати поза полосну мережу збору SPAN. Cyber Vision також може контролювати промислові мережі, побудовані за допомогою обладнання сторонніх виробників.

Відсутність перевантаження мережі. Нема потреби в додаткових ресурсах мережі. Датчики Cyber Vision декодують промисловий мережевий трафік на межі та надсилають лише легкі метадані до Cyber Vision Center. Ця унікальна архітектура лише додає навантаження на промислову мережу від 2% до 5%.

Глобальний перегляд усіх сайтів. Забезпечує управління та дотримання детальної інформації про безпеку на всіх промислових об’єктах. Глобальний центр Cyber Vision Global Center легко збирає дані з усіх локальних центрів, щоб команди CISO та служби безпеки мали централізовану видимість активів і подій на кожному сайті та між сайтами.

Пасивне та активне відкриття. Cyber Vision відстежує промислові операції шляхом пасивного захоплення та декодування мережевого трафіку за допомогою глибокої перевірки пакетів (DPI) промислових протоколів керування. Більше інформації можна зібрати за допомогою активного виявлення, яке надсилає надзвичайно точні запити без збоїв у семантиці конкретного протоколу ICS.

100% видимість. Лише розподілене граничне активне виявлення Cyber Vision може забезпечити 100% видимість промислової мережі. Він надсилає цільові запити до активів від датчиків, вбудованих у мережеве обладнання, тому ці повідомлення не блокуються брандмауером або межами трансляції мережевих адрес (NAT), що забезпечує 100% видимість.

Динамічна інвентаризація активів. Створює відповідну політику безпеки та підвищує ефективність роботи. Cyber Vision дає детальну картину в режимі реального часу щодо промислових активів, їхніх моделей зв’язку та потоків програм.

Оцінка ризику. Зосереджена на безпосередніх загрозах і визначена пріоритетність дій, щоб швидко покращити рівень безпеки. Cyber Vision

розраховує ризики для кожного пристрою, а також для конкретного сайту, лінії чи будь-якого набору даних. Він навіть містить вказівки щодо того, що можна зробити, щоб завчасно зменшити ризики.

Види карти. Візуалізована діяльність мережі керування. Cyber Vision пропонує кілька типів карт, щоб показати активи та їхні комунікації. Що дозволяє швидко виявляти загрози та аномалії завдяки кольоровому кодуванню.

Документні зони та канали. Легке створення політики безпеки. Cyber Vision дозволяє групувати активи в зони (виробничі клітини, будівлі, підстанції тощо), щоб робочі команди могли обмінюватися логічною мережевою інформацією з IT та створювати політики безпеки відповідно до IEC 62443.

Оперативні інсайти. Скорочення часу простою та підвищить ефективність мережі. Cyber Vision відстежує всі події OT, щоб виявити проблеми з пристроєм до того, як вони порушать виробництво, і допомогти оперативному розв'язувати проблеми швидше. Він визначає проблемні шаблони мережі, щоб IT-спеціалісти могли оптимізувати конфігурації та продуктивність мережі.

OT теги. Одразу зрозуміти роль кожного пристрою та що він робить. Cyber Vision перетворює потоки додатків у зрозумілі людині теги, щоб знати, що відбувається, навіть якщо користувач не експерт з протоколів.

Попередньо встановлені види. Легке ознайомлення із набором даних за допомогою попередньо встановлених і користувацьких переглядів, які виділяють те, що дійсно важливо для користувачів, допомагаючи зосередити свою стратегію виявлення та ділитися цільовою інформацією з колегами.

Статистика безпеки. Швидке визначення поточного стану безпеки, виявлення аномалій і вразливостей та реагує на загрози. Cyber Vision пропонує різні інформаційні панелі, звіти та історії подій, щоб легко виявляти проблеми безпеки та ділитися інформацією з усіма зацікавленими сторонами.

Бортовий самописець OT. Відповідність вимогам відповідності. Cyber Vision зберігає історію всіх подій і потоків додатків, у тому числі доступ до змінних, тож є можливість легко виконувати криміналістичний пошук і створювати звіти про інциденти.

Виявлення вразливостей. Збереження промислових активів в безпеці. Cyber Vision попереджає користувачів про вразливості апаратного та програмного забезпечення, які необхідно виправити.

Виявлення вторгнень (IDS). Розкриття загроз кібербезпеці, що виходять з IT-мережі. Cyber Vision інтегрує механізм Snort IDS, який використовує правила підписки Talos для виявлення відомих і нових загроз, таких як зловмисне програмне забезпечення або шкідливий трафік.

Виявлення аномалії. Виявлення відхилення від нормальної поведінки процесу. Легко створити кілька базових планів, щоб профілювати промислову діяльність або зосередитися на тому, що для користувачів є найбільш критичним (наприклад, на певному активі чи певній поведінці, як-от віддалений доступ). Відхилення негайно викликають сповіщення.

Корелювати події безпеки IT/OT. Покращення практики керування подіями безпеки. Cyber Vision попередньо інтегровано з провідними платформами SIEM і SOAR, такими як IBM QRadar або SPLUNK, і може пересилати події та сповіщення OT до будь-якого іншого інструменту за допомогою Syslog. Щоб уникнути втоми подій, є можливість вибору, до яких типів подій слід надавати спільний доступ.

IT/OT співпраця. Використання знань OT про промислові активи та процеси. Cyber Vision допомагає побудувати спільний робочий процес між IT та OT для ефективного захисту виробництва. OT може повідомляти про події безпеки, надаючи додатковий контекст. IT-спеціалісти можуть додавати власні властивості до активів і груп OT, щоб документувати особливості, залежності та зацікавлених сторін.

Поширення IT-безпеки на OT. Створення уніфікованого OT/IT SOC. Cyber Vision повністю інтегровано з платформами IT-безпеки Cisco (та іншими) і надає їм детальну інформацію про активи та події OT. Створення політик безпеки OT і усунення загроз за допомогою наявних IT-інструментів тепер стало набагато простіше.

Багата інтеграція з IT. Можливість легкого розповсюдження контекстом OT зі IT-інструментами. Cyber Vision попередньо інтегровано з багатьма

рішеннями сторонніх розробників, такими як брандмауери або OT Management від ServiceNow, і має багатий REST API для створення індивідуальної інтеграції. Провідник API допомагає користувачам писати та тестувати виклики API за допомогою дружнього інтерфейсу користувача та містить зразки коду, які допоможуть почати роботу.

Локально або в хмарі. На місці за допомогою апаратного чи віртуального пристрою або в хмарі. Cyber Vision можна встановити на Amazon Web Services або Microsoft Azure [13].

2.4 Порівняння Cisco Cyber Vision

Claroty. Claroty xDome — це модульна платформа промислової кібербезпеки на основі SaaS, яка масштабується, щоб захистити власне середовище та досягти потрібних цілей у міру їх розвитку.

Виявлення активів.

- Неможливо захистити те, чого не видно, тому можливості виявлення активів є основою не лише кібервідмовостійкості, але й усього шляху до промислової кібербезпеки.
- Отримати повну та повністю автоматизовану інвентаризацію активів XIoT
- Використати поглиблені комунікаційні та поведінкові профілі для всіх активів XIoT
- Вибирати між кількома методами виявлення активів, щоб досягти видимості своїм способом

Уразливість і управління ризиками

- Ключова перешкода для кіберстійкості, уразливості поширені в промислових середовищах. Виключати цей бар'єр із власного середовища.
- Автоматично співвідносити активи XIoT з інформацією про вразливість і ризики.

- Розставити пріоритети для відновлення на основі реальних ризиків для діяльності.
- Увімкнути безперервне керування станом безпеки та відповідність.

Захист мережі

- Допомогти підтримувати кіберстійкість, зміцнюючи середовище компонентами ефективного захисту мережі, які складно впроваджувати.
- Початок сегментації мережі з індивідуальними рекомендаціями.
- Застосувати детальний контроль доступу для віддалених внутрішніх і сторонніх користувачів.
- Впровадити архітектуру Zero Trust, щоб мінімізувати кіберризик.

Виявлення загроз

- Оскільки жодне промислове середовище не захищене від загроз, потрібно надати користувачам можливість виявляти їх і реагувати на них негайно й ефективно.
- Постійно відстежувати всі відомі та невідомі загрози.
- Розширити існуючі можливості SOC до свого промислового середовища.
- Пом'якшити кібератаки, перш ніж вони вплинуть на промислові операції.

Виявлення активів

- Операційна стійкість вимагає централізованого, глибокого, завжди актуального інвентаризації всіх активів XIoT, які є основою промислової діяльності.
- Отримувати повну інвентаризацію активів XIoT.
- Використовувати поглиблені профілі для всіх активів XIoT.
- Вибирати між кількома методами виявлення активів для видимості.

Управління змінами

- Надає оптимальне управління змінами для забезпечення безпеки та цілісності процесів на власному шляху до операційної стійкості.

- Розширити можливості програм МоС безперервним моніторингом операцій.
- Скористатись детальними профілями ресурсів XIoT для оптимізації робочих процесів.
- Використовувати ефективні, дуже гнучкі інструменти звітності для відстеження програмного прогресу.

Управління активами

- Інвентаризація активів XIoT, дає користувачу відомості про управління активами, необхідні для зниження операційного ризику.
- Автоматично відстежувати оновлення своїх активів.
- Легко визначати пріоритети необхідних оновлень на основі ризику.
- Оптимізувати процеси дотримання SLA та звітності.

Безпечний віддалений доступ

- Віддалений доступ має вирішальне значення для безперервності роботи, але традиційні методи є ризикованими та неефективними. Підхід забезпечує послідовність без компромісів.
- Усунути потребу у переходових серверах або складних конфігураціях брандмауера.
- Запропонувати ідеальний досвід віддаленого користувача, який зменшує MTTR.

Переваги:

- Чудовий інтерфейс користувача.
- Для Claroty CTD чудово підходить модуль Enterprise.
- Підтримка схвалення доступу (але відсутній глибокий дозвіл на робочий процес), захоплення екрана та передача великих файлів є ключовими темами безпечного віддаленого доступу.

Недоліки:

- Навчання користуванню продуктом орієнтоване на користувальницький інтерфейс або техніку, а не на аналітиків

- Вбудовані посібники в продукт залишають бажати кращого, оскільки запропоновані кроки досить загальні.
- Масове оновлення функцій обмежене - це завадить правильному налаштуванню інформації про активи, включаючи зонування та правила [14].

Dragos Platform. Платформа Dragos — це найбільш надійна технологія кібербезпеки промислових систем керування (ICS), яка забезпечує повну видимість власних активів ICS/OT і загроз, з якими користувач стикаєтесь, із рекомендаціями щодо найкращих практик для реагування до значного компромісу.

Переваги:

- Інвентаризація активів і можливості видимості платформи Dragos забезпечують найповніше та глибоке розуміння середовищ ICS у галузі.
- Повна інвентаризація всіх активів, пристроїв і деталей.
- Швидке сортування інцидентів за допомогою аналізу шкали часу.
- Групувати активи за зонами, щоб визначити неочікуваний трафік.

Недоліки. Здається, націлений на зрілі компанії, які можуть розмістити датчики в ідеальних місцях для захоплення мережевого трафіку OT. Для виробничих компаній, які починають свою кіберподорож у сфері OT, де IT та OT сильно змішані, конкуренти надають більшу цінність комбінованим мережам IT/OT [15].

Переваги управління вразливістю:

- Можливості керування вразливістю платформи Dragos дають клієнтам інформацію, необхідну для зосередження на проблемах найвищого пріоритету, щоб зменшити ризик, мінімізувати час простою та розподілити ресурси кібербезпеки там, де вони найбільше потрібні.
- Найбільш повна та точна доступна база знань про вразливості OT.
- Пріоритетні вказівки з напрямком «Зараз, далі, ніколи», щоб команди знали, з чого почати.
- Продемонструвати відповідність нормативним стандартам і галузевим нормам.

- Розподілити ресурси кібербезпеки там, де вони найбільше потрібні [16].

Характеристики тактик, методів і процедур противника (TTP), які швидко визначають зловмисну поведінку, надають контекстні попередження та сповіщення, а також пов’язані з посібниками з розслідування, щоб допомогти аналітикам ефективно реагувати на загрози

На відміну від методів виявлення загроз, заснованих виключно на аномаліях, аналітика поведінки загроз зменшує кількість сповіщень, які отримують аналітики, зменшує кількість помилкових спрацьовувань і надає контекстне уявлення про загрози для швидшого часу відповіді [17].

Nozomi Networks Guardian

- Високоточна інвентаризація активів усіх комунікаційних пристроїв.
- Розширена інформація про вузол, включаючи назву, тип, серійний номер, версію прошивки та компоненти.
- Статистична інформація щодо оцінки ризиків, включаючи сповіщення про безпеку та надійність, відсутні виправлення та вразливості.

Миттєво побачити всю мережу:

- Миттєва інформація про мережі OT/IoT і «звичайні» моделі активності.
- Отримати доступ до ключових даних, таких як пропускна здатність трафіку, TCP-з’єднання та протоколи.
- Інтуїтивно зрозумілі інформаційні панелі та звіти з макро- та мікро-видами, а також фільтруванням і групуванням.

Швидке визначення, які пристрої ICS, OT та IoT вразливі:

- Ефективне встановлення пріоритетів і виправлення.
- Швидше реагування за допомогою панелей уразливостей, детальної інформації та звітів.
- Базується на національній базі даних вразливостей (NVD) уряду США для стандартизованого найменування, опису та оцінки.

Таблиця 2.1

Порівняльний аналіз платформ промислової кібербезпеки

	Cisco Cyber Vision	Claroty	Dragos Platform	Nozomi Networks Guardian
Platforms Supported	Linux, SaaS	SaaS	SaaS	SaaS
Audience	Команди OT та IT, які хочуть працювати разом, щоб забезпечити безперервність виробництва, стійкість і безпеку	Галузі, яким потрібна платформа кібербезпеки для досягнення повного спектру засобів контролю промислової кібербезпеки	Групи IT-безпеки	Галузі, які шукають рішення для видимості, безпеки та моніторингу для своїх OT, IoT, IT, периферійних і хмарних ресурсів
Support	Робочий час Онлайн		Робочий час Онлайн	Робочий час Онлайн
Pricing	Безкоштовне випробування			
Training	Документація Вебінари Живий онлайн Особисто	Документація Вебінари Живий онлайн	Документація	Документація Вебінари Живий онлайн
Company Information	Заснований: 1984 рік Сполучені Штати www.cisco.com/go/cybervision	Рік заснування: 2015 рік Сполучені Штати claroty.com/comprehensive-platform-overview/	Рік заснування: 2013 рік Сполучені Штати www.dragos.com/platform/	Рік заснування: 2013 рік Сполучені Штати www.nozominetworks.com/products/guardian/

Продовження таблиці 2.1

Categories	Кібербезпека Безпека Інтернету речей SCADA	Кібербезпека Безпека Інтернету речей SCADA	Кібербезпека Виявлення та запобігання вторгненням Безпека Інтернету речей	Безпека Інтернету речей

Постійно контролювати власні мережі та системи автоматизації:

- Постійний моніторинг усіх активів, мережевих комунікацій і підтримуваних протоколів.
- Легкий доступ до узагальненої інформації про ризики ICS, OT та IoT.
- Висвітлює потенційні проблеми з надійністю, наприклад незвичні значення процесу [18].

Проаналізувавши найбільш популярні платформи для захисту промислових IOT, зупинив би свій вибір на Cisco Cyber Vision. Тому що саме він має більше гнучкий функціонал, пробну версію, кожен керівник зможе підібрати саме те, що йому потрібно [19].

Висновки до другого розділу

Оглянуто рішення Cisco Cyber Vision для захисту промислових IIoT мереж від кіберзагроз. Досліджено програмне забезпечення Cisco Cyber Vision, переваги, основні інструменти для захисту промислових операцій та варіант збору мережевих даних.

Зазначено двох або трьох рівневу архітектуру та важливу інформацію вимог до монтажу і необхідних ресурсів, яку потрібно розуміти керівникам при виборі системи для захисту промислових IoT.

Розписано рішення Cisco Cyber Vision по вирішенню проблем промислових інтернет речей, які допоможуть забезпечити основний рівень захисту.

Розглянуто порівняння Cisco Cyber Vision з іншими відомими продуктами таких як: Claroty, Dragos Platform та Nozomi Networks Guardian. Обрано з проаналізованої інформації найбільше відповідний варіант із всіх зазначених недоліків та переваги кожної із систем.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ CISCO CYBER VISION

3.1 Встановлення програмного комплексу Cisco Cyber Vision

Для встановлення віртуального центру, потрібно виконати кілька кроків:

1. Отримати інсталяційний файл Cisco Cyber Vision.
2. Створити віртуальну машину на ESXi та розгорнути файл Cisco Cyber Vision.ova на віртуальній машині. Або створити віртуальну машину на Hyper-V, установити розмір диска, створити та зіставити мережеві інтерфейси.
3. Налаштувати Cisco Cyber Vision Center.

1. Отримання інсталяційного файлу.

Перш ніж почати інсталяцію віртуальної машини, потрібно отримати інсталяційний файл ova віртуальної машини.

Щоб отримати інсталяційний файл віртуальної машини:

1. Отримати доступ до платформи завантаження програмного забезпечення Cisco Cyber Vision.

2. Завантажити файл ova, необхідний для Hyper-V або ESXi, з останньої випущеної версії. Також доступні файли ova з опцією DPI.

Щоб переконатися, що файл, який щойно був завантажений, справний, рекомендується використовувати контрольну суму SHA512, надану Cisco.

Для цього (для користувачів Windows):

3. Перейти на сторінку завантаження Cisco Cyber Vision.

4. Завантажити файл.

5. Відкрити підказку оболонки, наприклад Windows Powershell, і скористатися наведеною командою (рис.3.1), щоб отримати контрольну суму файлу: Get-FileHash.\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> - Алгоритм SHA512 |Формат-список.

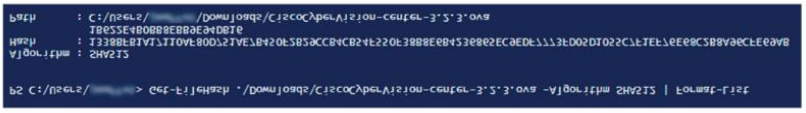

Рис.3.1. Команда для отримання контрольної суми

6. На сторінці завантаження навести курсор миші на файл і скопіювати контрольну суму SHA512 (рис.3.2).

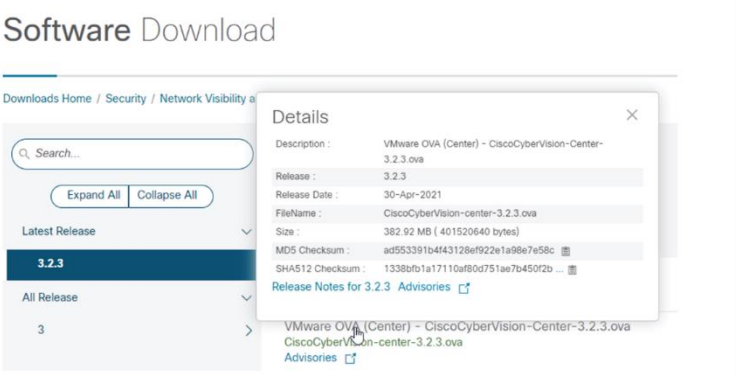

Рис.3.2. Файл на сторінці завантаження

7. Порівняти обидві контрольні суми.

- Якщо обидві контрольні суми ідентичні, це означає, що файл справний.
- Якщо контрольні суми не збігаються, слід спробувати завантажити файл ще раз.
- Якщо після повторного завантаження файлу контрольні суми все ще не збігаються, потрібно звернутись до служби підтримки Cisco.

2. Створити віртуальну машину на ESXi та розгорнути файл Cisco Cyber Vision.ova на віртуальній машині. Або створити віртуальну машину на Hyper-V, установити розмір диска, створити та зіставити мережеві інтерфейси.

Створити віртуальну машину. Перш ніж виконати наведені нижче кроки для створення віртуальної машини на ESXi, *слід встановити два мережеві інтерфейси* (мережеві інтерфейси адміністрування та збору) і третій, якщо розгортати центр із DPI (мережевий інтерфейс DPI), відповідно до інфраструктури мережі. Для цього потрібно звернутись до документації VMware ESXi.

Щоб створити віртуальну машину та розгорнути Cisco Cyber Vision (рис.3.3):

1. Увійти у VMware EXSi.

2. Натиснути «Створити/Зареєструвати віртуальну машину».

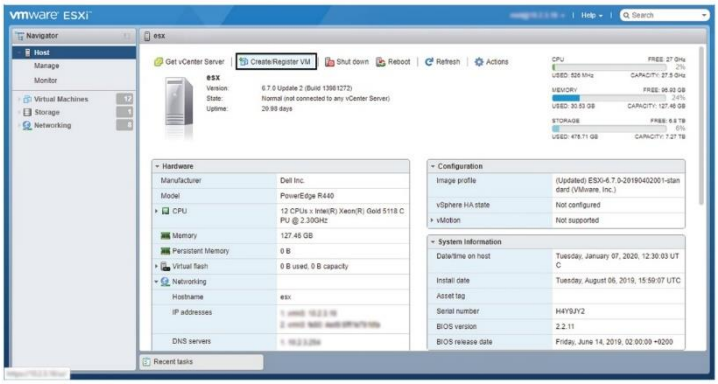

Рис.3.3. Майстер створення

Відкриється майстер створення нової віртуальної машини.

3. Натиснути Розгорнути віртуальну машину (рис.3.4) з файлу OVF або OVA.

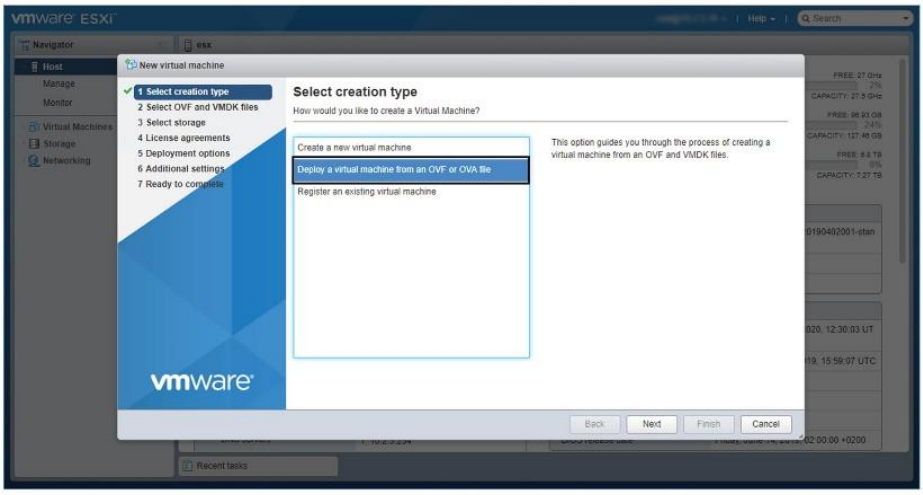

Рис.3.4. Розгортання віртуальної машини

4. Дати назву віртуальній машині (рис.3.5) та вибрати файл (рис.3.6) Cisco Cyber Vision OVA. Потрібно обрати файл DPI.OVA, щоб увімкнути функцію датчика на Center VM.

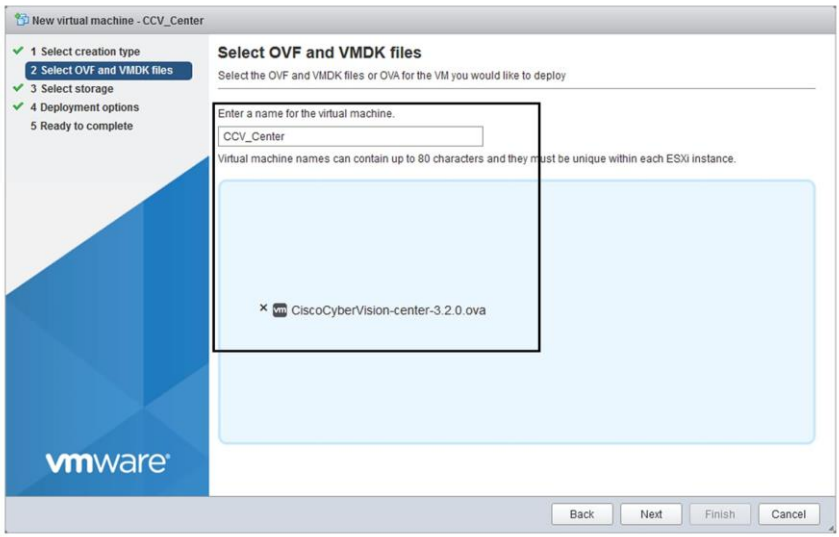

Рис.3.5. Назва віртуальної машини

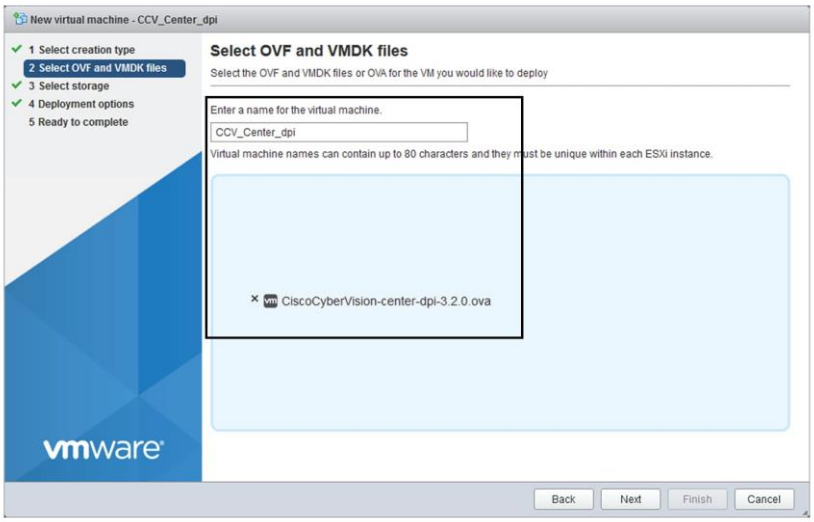

Рис.3.6. Вибір файлу DPI

6. Зіставити мережеві інтерфейси, які раніше були створені, на порти віртуальної машини, як показано нижче:

- Мережевий інтерфейс адміністрування, як eth0.
- Мережевий інтерфейс колекції, як eth1.
- Якщо розгортається центр із DPI, мережевий інтерфейс DPI має значення eth2.

7. Встановити налаштування диска як тонкий.

8. Обрати диск із достатньою пам’яттю (рис.3.7).

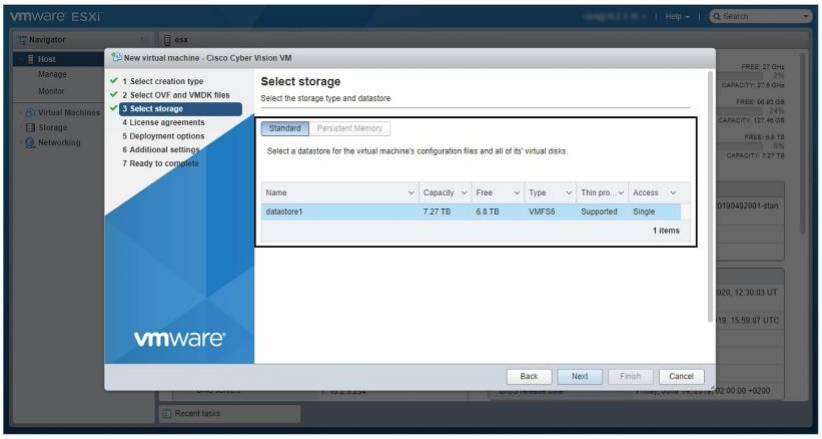

Рис.3.7. Вибір диска

9. Встановити тип розгортання як малий, середній або великий. Розмір розгортання для файлу OVA DPI за замовчуванням — великий.

- Маленький: Intel Xeon, 8 ядер, 16 ГБ оперативної пам’яті.
- Середній: Intel Xeon, 10 ядер, 32 ГБ оперативної пам'яті.
- Великий: Intel Xeon, 16 ядер, 64 ГБ оперативної пам’яті.

10. Вимкнути автоматичний запуск віртуальної машини.

11. Перш ніж натиснути «Готово», слід перевірити параметри нової віртуальної машини (рис.3.8).

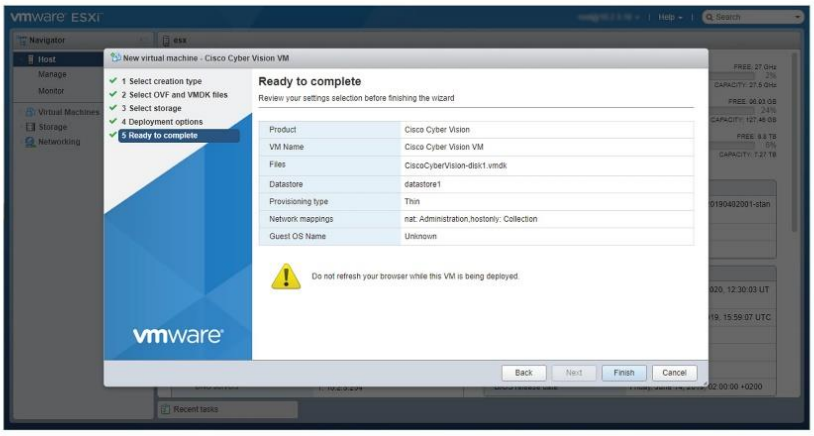

Рис.3.8. Перевірка параметрів

Нова віртуальна машина (рис.3.9) відображається у списку віртуальних машин.

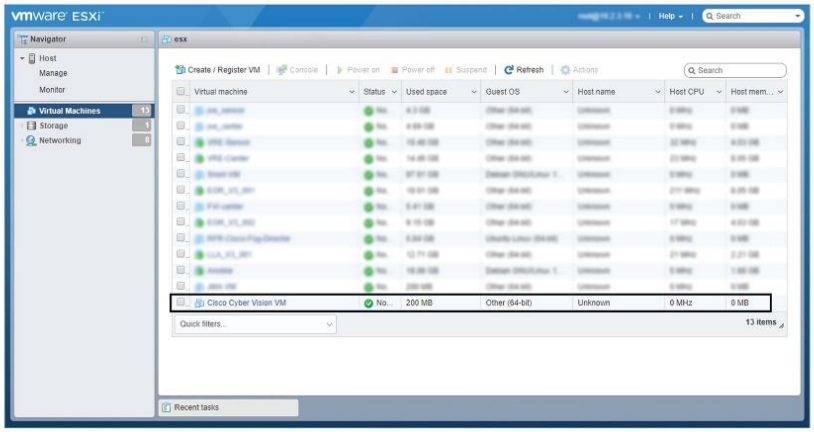

Рис.3.9. Відображення машини у списку

Завантажити віртуальну машину.

Після створення віртуальної машини можна переходити до її першого завантаження (рис.3.10).

1. Натиснути віртуальну машину у списку.
2. Увімкнути віртуальну машину.

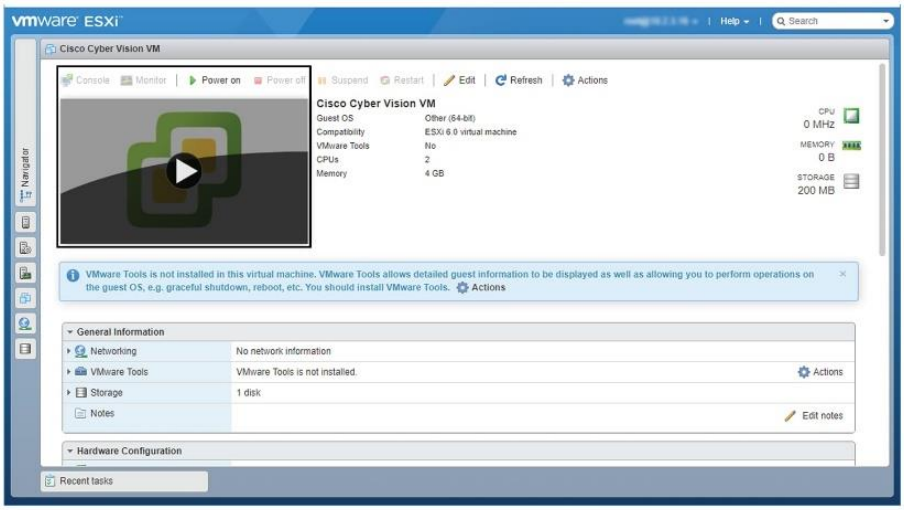

Рис.3.10. Віртуальна машина

3. Зачекати кілька хвилин, поки завершиться ініціація віртуальної машини. Відобразиться такий екран (рис.3.11):

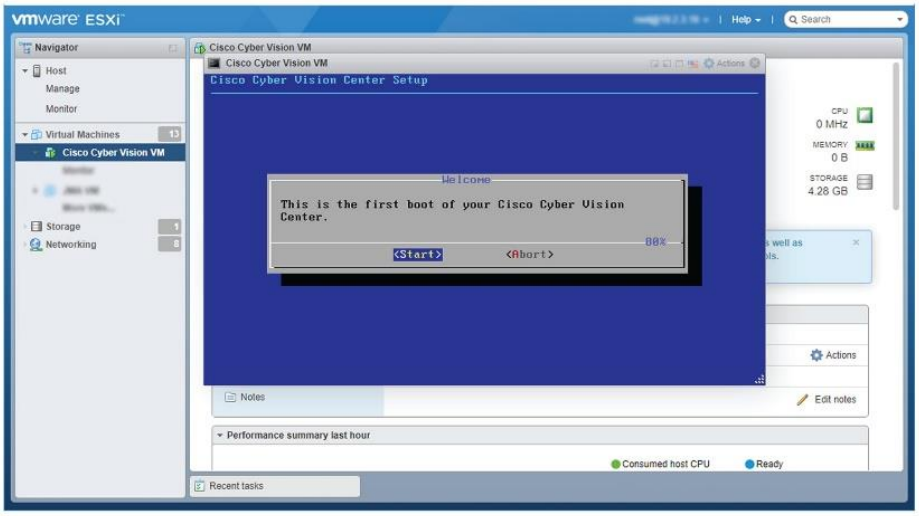

Рис.3.11. Завершення ініціації

4. Натиснути Ctrl+Alt, щоб відновити керування клавіатурою та мишею. Тепер віртуальний центр готовий до базової конфігурації.

Налаштування Hyper-V.

Створення віртуальної машини. Щоб створити нову віртуальну машину:

1. Потрібно відкрити диспетчер Hyper-V (рис.3.12). З'явиться такий головний екран:

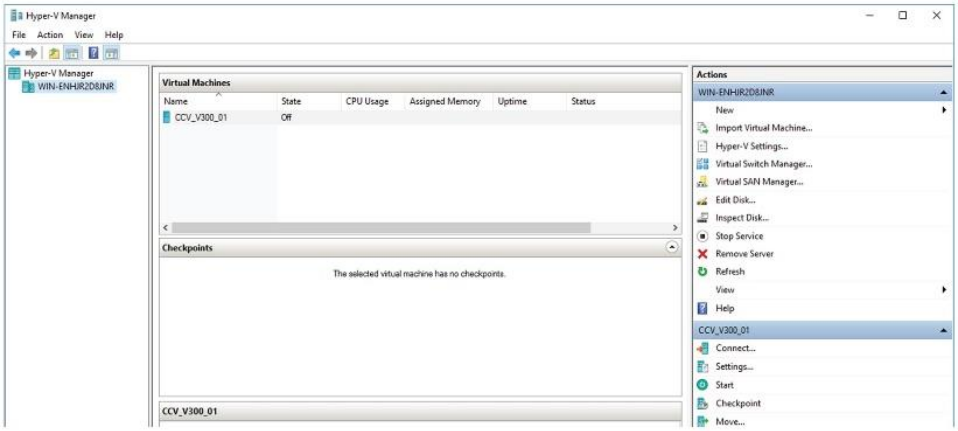

Рис.3.12. Головний екран

2. Відкрити Майстер створення віртуальної машини, натиснувши Дія > Створити > Віртуальна машина (рис.3.13).

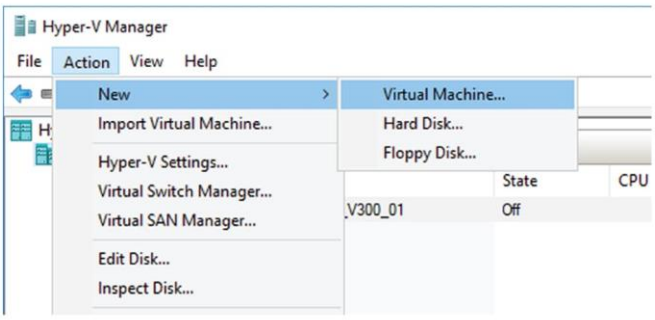

Рис.3.13. Відкриття майстера створення

Відобразиться майстер створення віртуальної машини (рис.3.14).

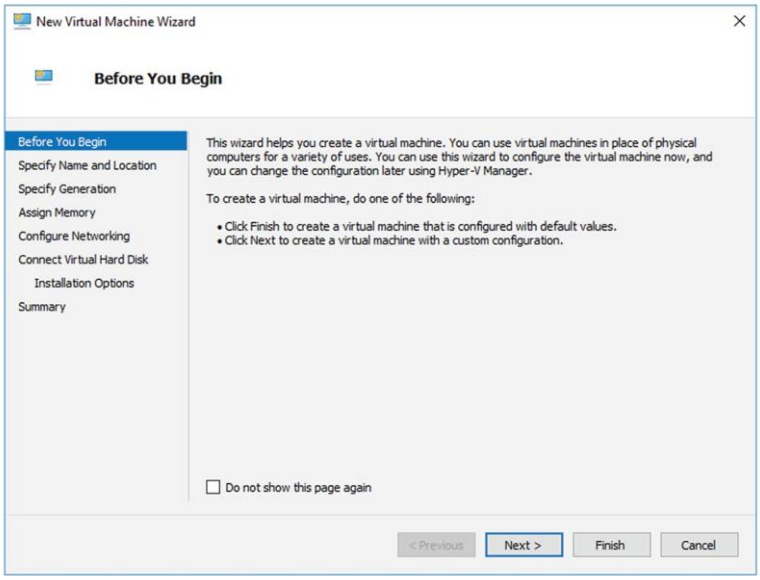

Рис.3.14. Майстер створення

3. Натиснути «Далі», щоб почати.

4. Дати новій віртуальній машині назву (наприклад, «Центр») (рис.3.15).

5. За потреби встановити віртуальному центру інше розташування на сервері, ніж те, що встановлено за замовчуванням. У будь-якому випадку у вибраному розташуванні має бути достатньо вільного місця на випадок, якщо планується створення знімків (тобто резервні копії віртуальної машини).

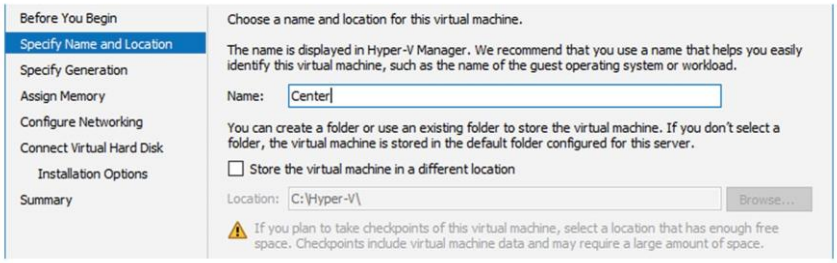

Рис.3.15. Присвоєння назви

6. Встановити для віртуальної машини покоління 1 (рис.3.16).

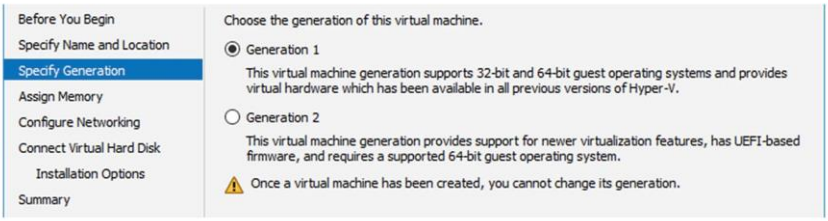

Рис.3.16 Встановлення

7. Призначити пам’ять віртуальній машині (рис.3.17). Мінімальна необхідна конфігурація становить 8192 МБ.

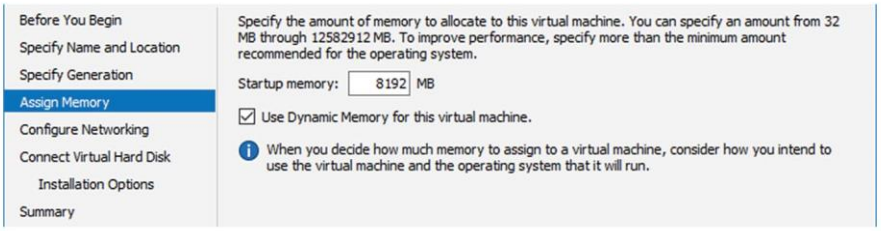

Рис.3.17. Призначення пам’яті

8. Залишити мережеве підключення відключеним (рис.3.18).

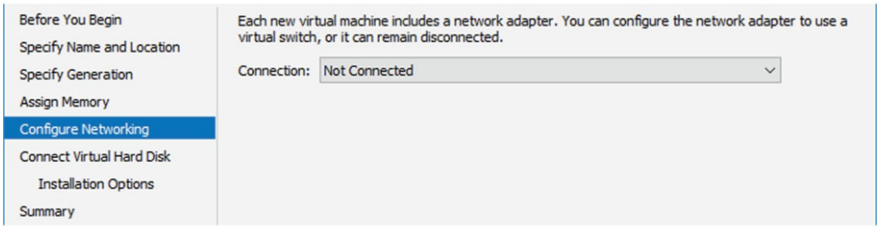

Рис.3.18. Відключена мережа

9. Обрати «Використовувати наявний жорсткий диск» (рис.3.19) і вибрати файл VHDX.

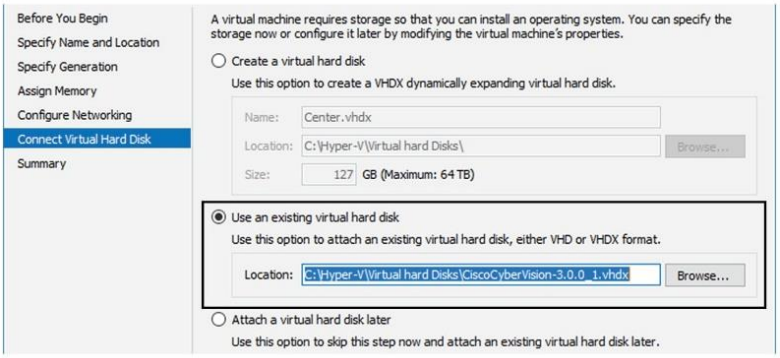

Рис.3.19. Файл VHDX

10. Натиснути «Готово», щоб створити віртуальну машину та закрити майстер (рис.3.20).

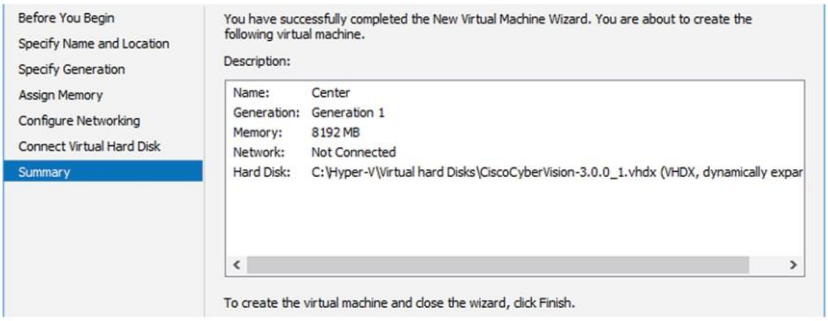

Рис.3.20. Створений віртуальний центр

Створений віртуальний центр відображається на головному екрані Hyper-V Manager.

Налаштувати розмір диска. Щоб налаштувати розмір диска:

1. У диспетчері Hyper-V вибрати Центр.

2. Натиснути Дія > Налаштування (рис.3.21).

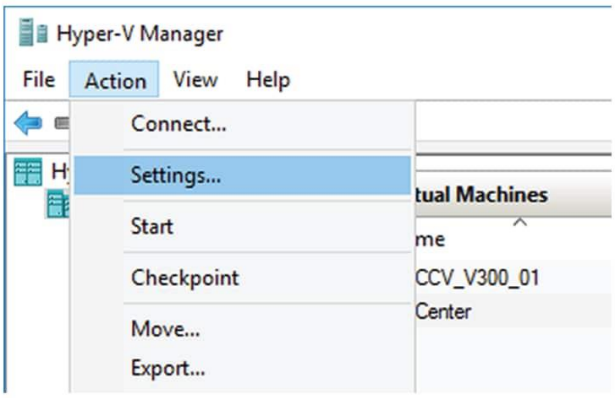

Рис.3.21. Налаштування

3. Натиснути «Жорсткий диск », а потім «Редагувати» (рис.3.22).

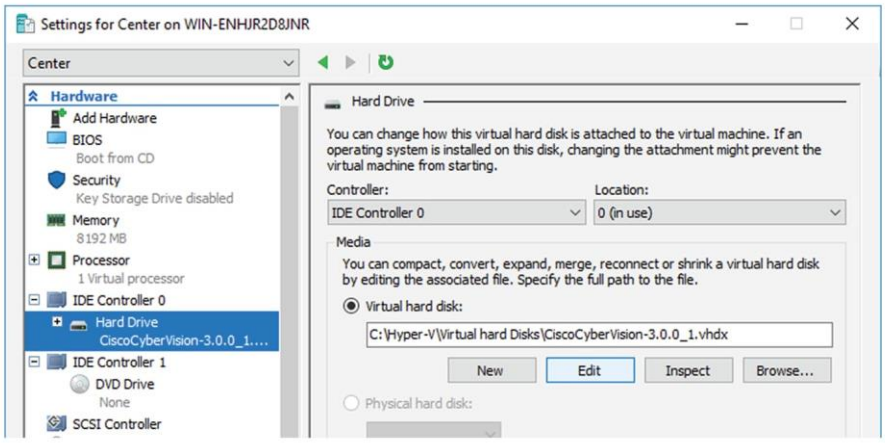

Рис.3.22. Редагування

Відобразиться майстер редагування віртуального жорсткого диска.

4. Натиснути «Далі», щоб перейти до вкладки «Вибрати дію» (рис.3.23).

5. Перебуваючи на вкладці «Вибрати дію», обрати параметр «Розгорнути».

6. Налаштувати новий розмір віртуального жорсткого диска.

Рекомендовано:

- встановлювати мінімальний розмір 100 ГБ для демонстраційної інсталяції з невеликими обсягами даних.
- встановити мінімальний розмір 250 ГБ для картографії.
- встановити мінімальний розмір 800 ГБ для центру із синхронізацією або 1,5 ТБ для глобального центру для робочого середовища.

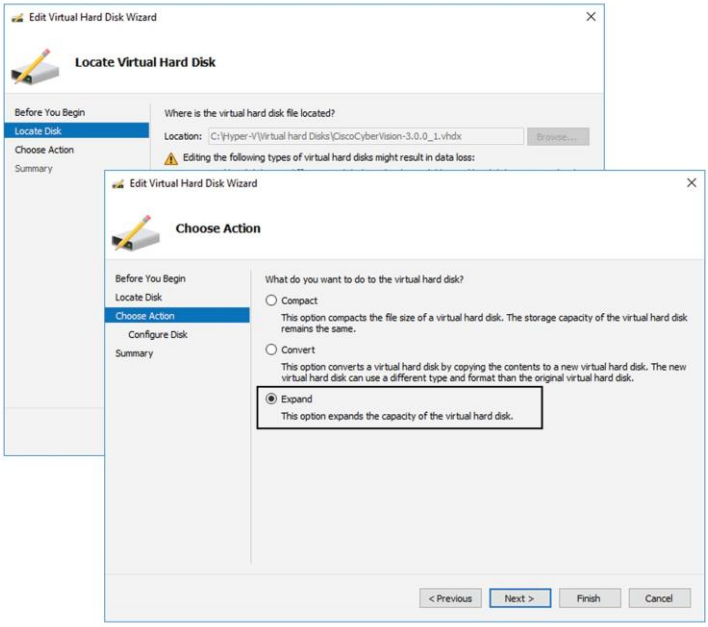

Рис.3.23. Вкладка «Вибрати дію»

Встановлюється мінімальний розмір. Віртуальний диск буде розширюватися, коли дані записуватимуться на віртуальний диск (рис.3.24).

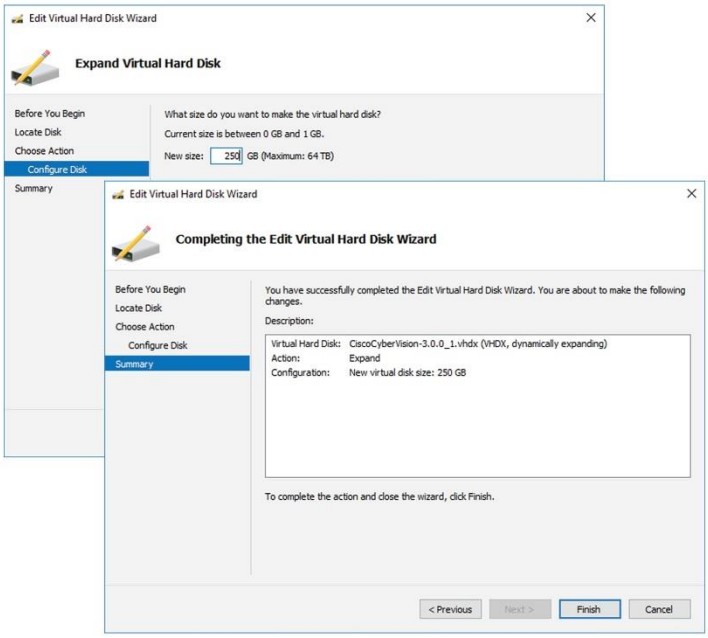

Рис.3.24. Створення віртуального жорсткого диска

7. Натиснути готово.

Створення мережевих інтерфейсів. Щоб створити мережеві інтерфейси адміністратора та колекції:

1. Вибрати Центр.

2. У меню «Дії» відкрити Virtual Switch Manager (рис.3.25).

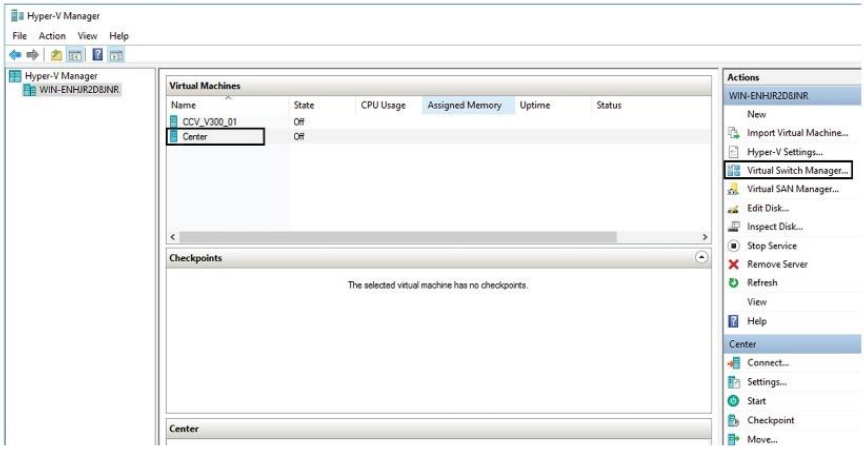

Рис.3.25. Відкриття Virtual Switch Manager

Відкриється диспетчер віртуальних комутаторів (рис.3.26).

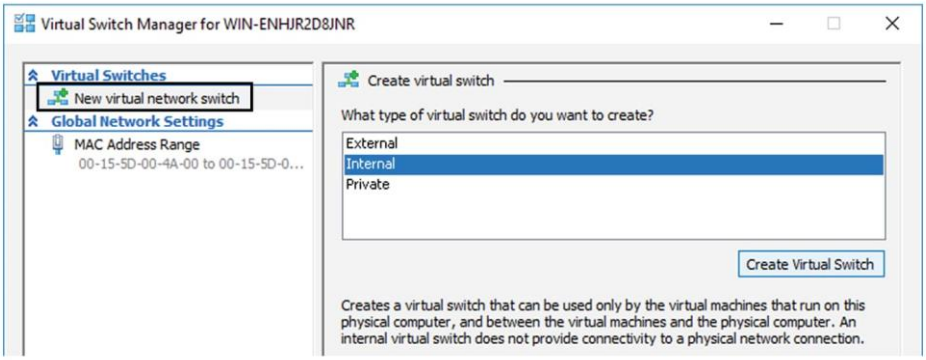

Рис.3.26. Диспетчер

3. Натиснути «Новий комутатор віртуальної мережі».

4. Відобразиться новий віртуальний перемикач.

5. Назвати його «Адміністратор».

6. Вибрати «Внутрішня мережа» (рис.3.27).

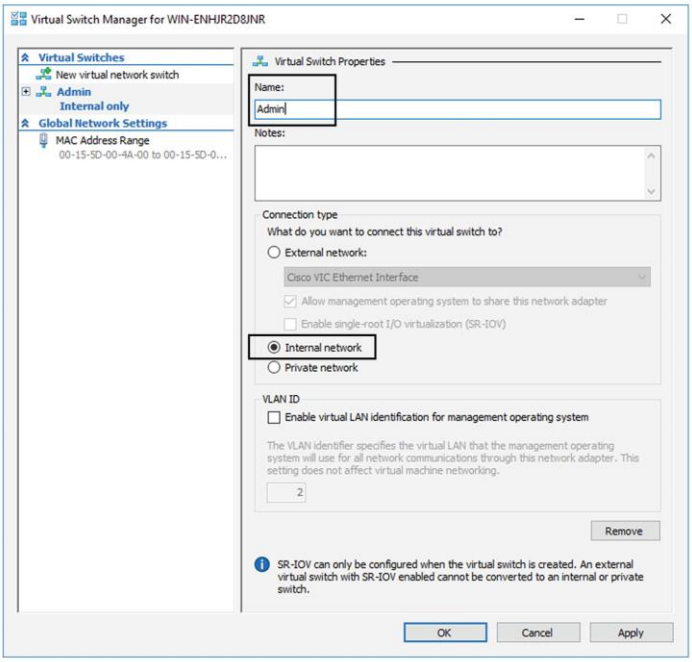

Рис.3.27. Внутрішня мережа

7. Створити другий віртуальний комутатор і назвати його «Колекція» (рис.3.28).

8. Вибрати «Внутрішня мережа».

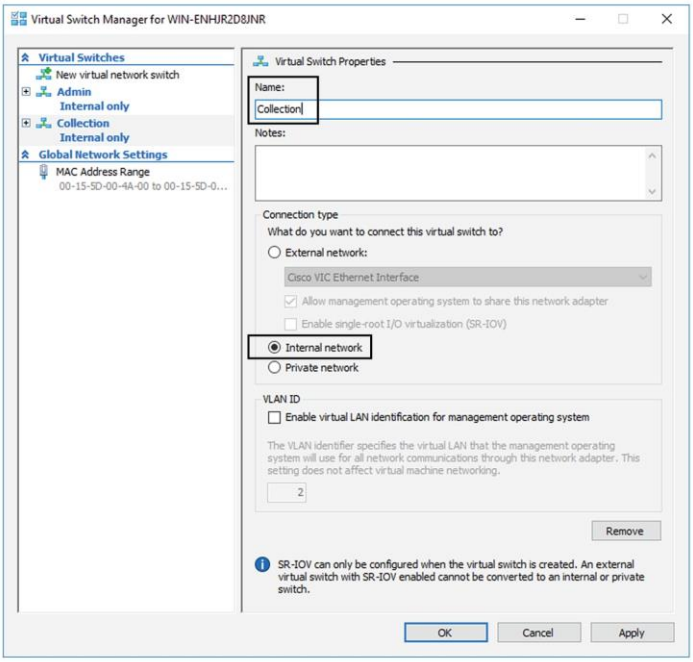

Рис.3.28. Віртуальний комутатор «Колекція»

Зіставити карту мережевих інтерфейсів. Щоб додати мережеву карту: ICS CyberVision потрібні два мережеві адаптери (тобто мережева карта), яким будуть призначені мережеві інтерфейси адміністратора та колекції. Кожна нова віртуальна машина під час створення включає мережеву карту, яка доступна в списку обладнання. Тому потрібно створити ще один мережевий адаптер під час цього кроку.

1. Клацнути правою кнопкою миші Центр і знову натиснути «Налаштування» (рис.3.29).

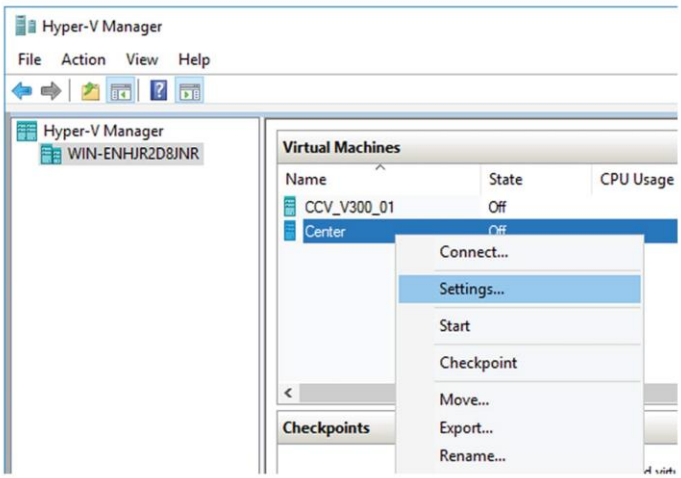

Рис.3.29. Налаштування

Відобразиться вікно налаштувань віртуального центру.

2. Натиснути «Додати обладнання».

3. Обрати «Мережевий адаптер».

4. Натиснути «Додати» (рис.3.30).

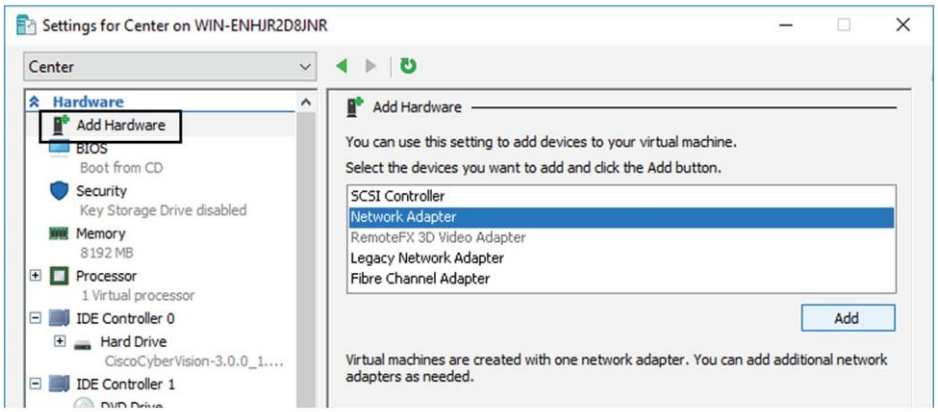

Рис.3.30. Додання мережевого адаптеру

Створено другий необхідний мережевий адаптер. Тепер потрібно зіставити кожен мережевий адаптер з віртуальним комутатором.

Щоб перейти до відображення мережі:

5. Обрати перший мережевий адаптер.

6. Обрати «Адміністратор» як віртуальний комутатор.

Потрібно налаштувати мережеві інтерфейси в порядку появи в списку мереж, щоб уникнути плутанини (рис.3.31):

- Перша мережева карта як мережевий інтерфейс адміністрування (eth0).
- Другий як мережевий інтерфейс колекції (eth1).

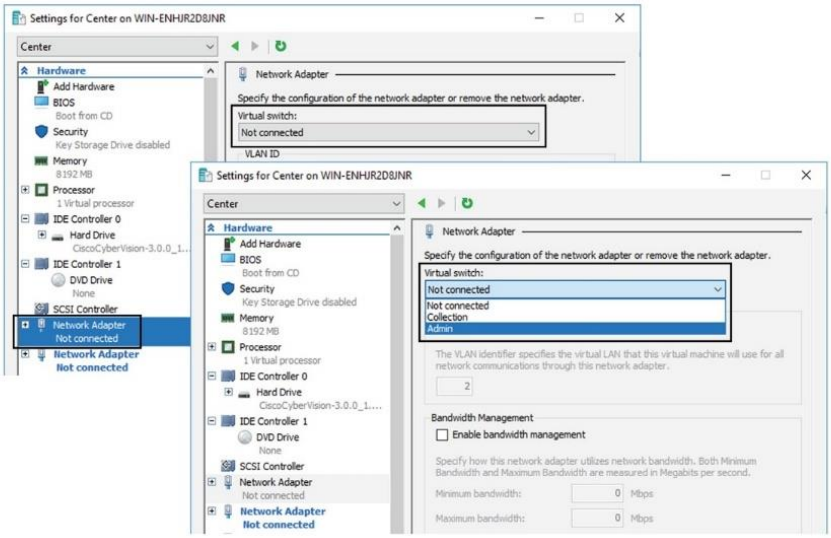

Рис.3.31. Налаштування мережевих інтерфейсів

Повторити попередню дію для другого мережевого адаптера та вибрати «Колекція» як віртуальний комутатор (рис.3.32).

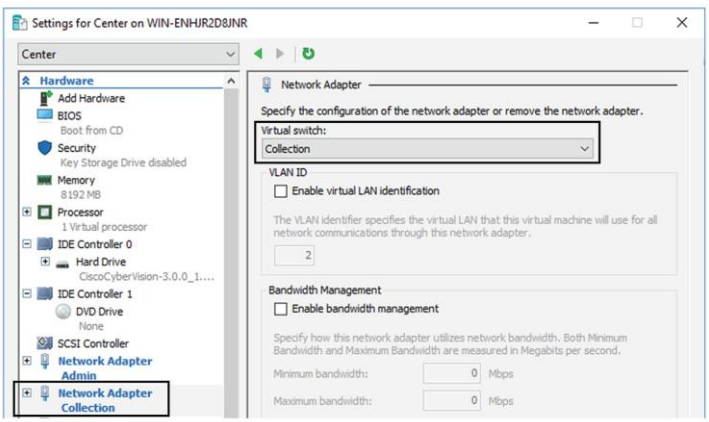

Рис.3.32. Для другого мережевого адаптера

Завантажити віртуальну машину. Тепер можна перейти до першого завантаження віртуального центру.

1. Натиснути «Центр» у диспетчері Hyper-V і натиснути «Підключитися» (рис.3.33).

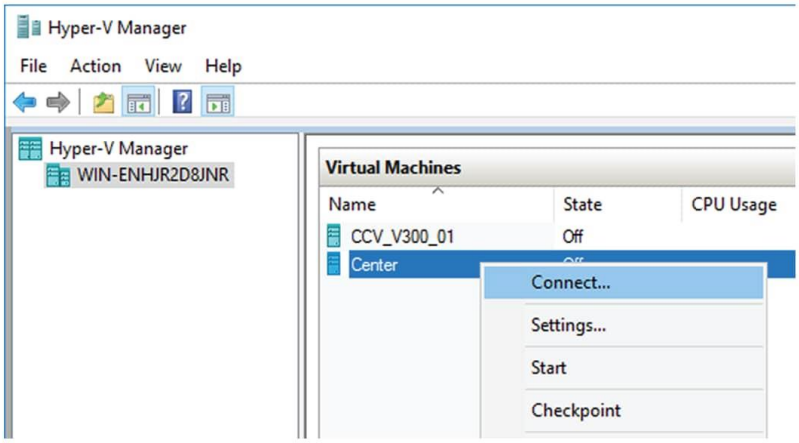

Рис.3.33. Підключення до Центру

2. Запустити віртуальний центр (рис.3.34).

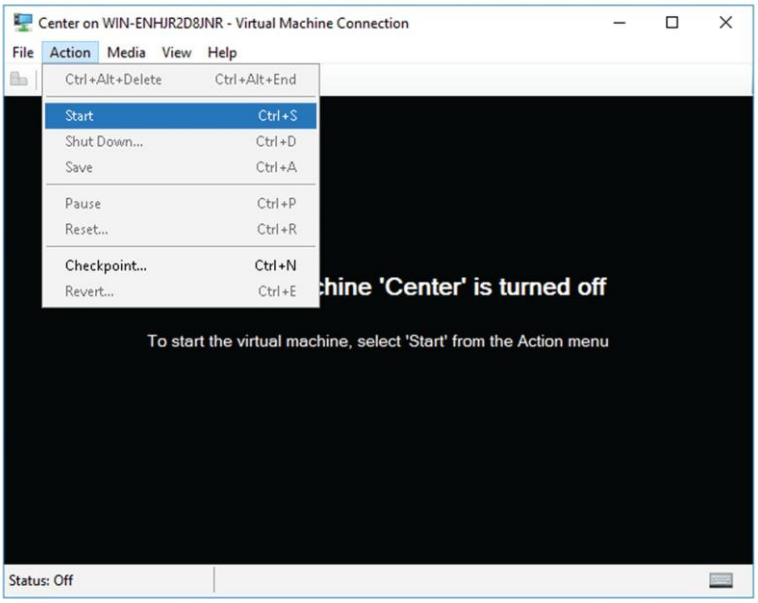

Рис.3.34. Запуск віртуального центру

Після успішного завершення налаштування віртуальної машини з’явиться такий екран (рис.3.35) [20]:

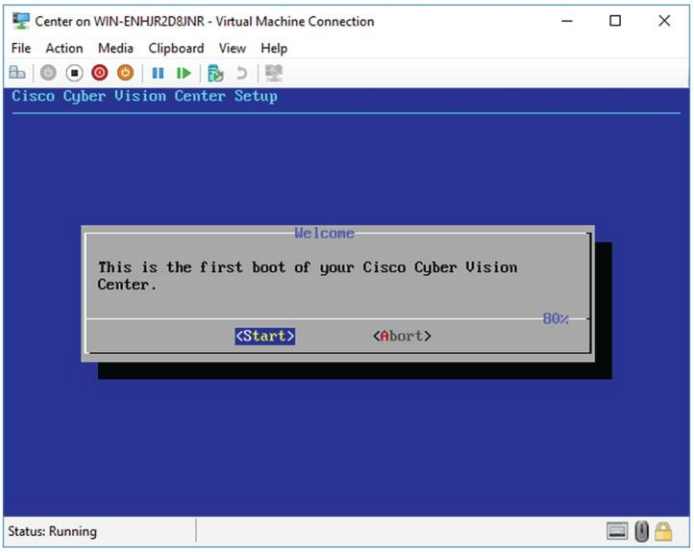

Рис.3.35. Успішне завершення налаштування віртуальної машини

3.2 Налаштування Center

Щоб налаштувати Центр, потрібно виконати два кроки:

1. Основна конфігурація центру за допомогою дисплея VGA та клавіатури або консолі для:

- Встановити пароль центру та датчика.
- Синхронізувати Центр із сервером NTP.
- Налаштувати інтерфейси адміністрування та збирання (не доступно для глобального центру або центру, що використовує один інтерфейс).

2. Конфігурація Cisco Cyber Vision через браузер, щоб:

- Створити обліковий запис адміністратора.
- Налаштувати синхронізацію даних центру.

Базова конфігурація центру. Цей крок дозволить налаштувати параметри мережі Center перед використанням його з інтерфейсом користувача.

Необхідна інформація:

- Локальні IP-адреси NTP і DNS.
- Мережева адреса інтерфейсу колекції (немає даних для глобального центру або центру, що використовує один інтерфейс).

У разі налаштування мережевого інтерфейсу адміністрування вручну:

- Його IP-адреса.
- Його маска мережі (у форматі з двох чисел, наприклад, 192.168.1.0/24).
- Його шлюз за замовчуванням (для доступу до пристроїв, розташованих поза локальною мережею).

Доступ до базової конфігурації Центру.

Майстер Центру відображається на екрані під час увімкнення Центру. Ввести «Пуск», щоб почати налаштування Центру (рис.3.36).

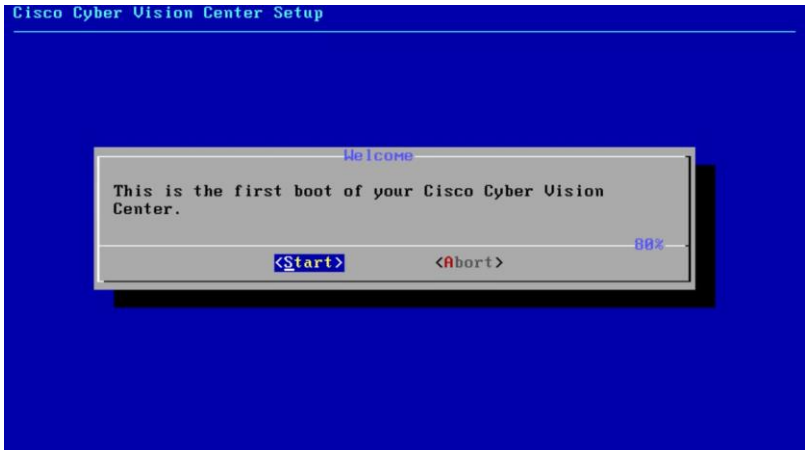

Рис.3.36. «Пуск», для початку налаштування Центру

Обрати мову, яка відповідає клавіатурі. За замовчуванням система налаштована на роботу з американською клавіатурою QWERTY (рис.3.37).

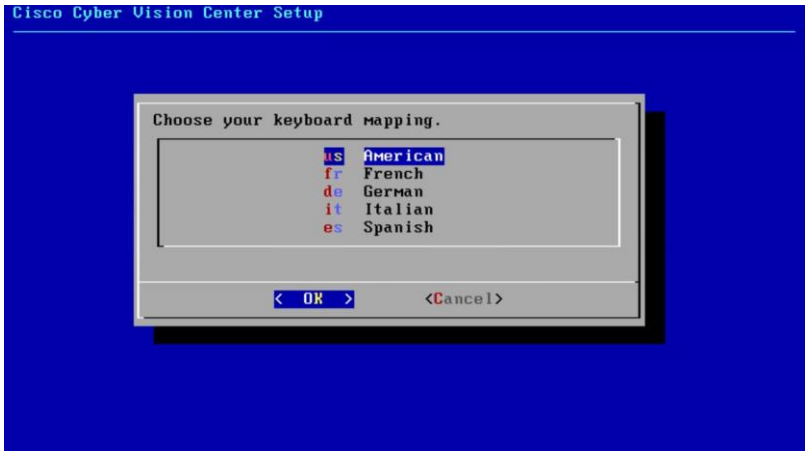

Рис.3.37. Обрання мови

Вибір типу центру. Під час цієї процедури обирається, який тип Центру встановити. Існує три види центрів:

- Центр отримує метадані від датчиків і зберігає їх у внутрішній базі даних (Postrgresql). Цей центр (може бути автономним або з синхронізацією з Глобальним центром) подібний до автономного Центру з функціональної точки зору, за винятком посилання на Глобальний центр. Потрібно встановити центри з синхронізацією після глобального центру. Це дозволить системі розпочати реєстрацію та розпочати надсилання подій до неї.
- Глобальний центр представляє централізовану архітектуру, яка збирає всі промислові ідеї та події з Центрів із Глобальним центром і об'єднує їх у єдиній глобальній точці зору. Це також дозволить керувати базою даних знань (KDB) і оновлювати всю платформу.

Обрати тип Центру, який потрібно встановити (рис.3.38).

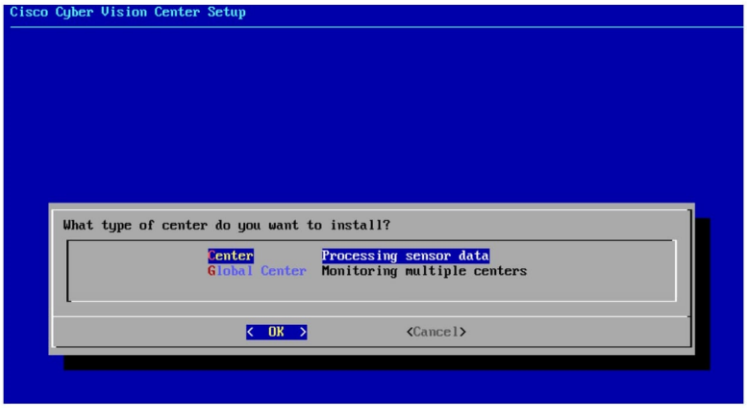

Рис.3.38. Тип центру

Центр. Якщо встановлюється Центр, потрібно обрати перший варіант (рис.3.39).

Тоді буде можливість встановити ідентифікатор центру. Його можна використовувати у випадку відновлення Центру, щоб повторно використовувати той самий ідентифікатор, попередньо встановлений у Глобальному центрі. Таким чином, деякі дані можна отримати.

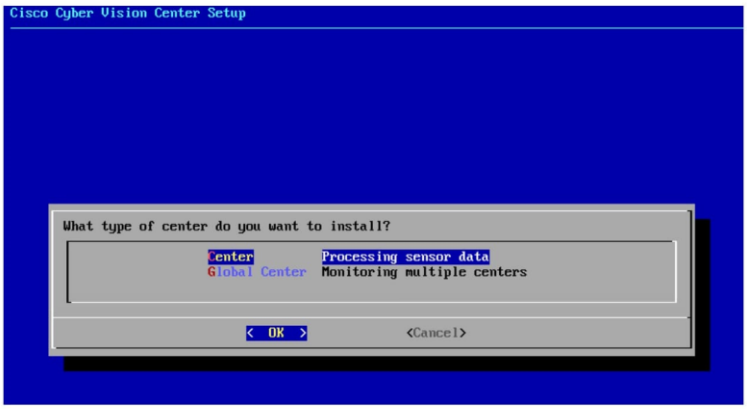

Рис.3.39. Вибір варіанту

Якщо встановлення Центру відбувається вперше, цей ідентифікатор буде згенеровано автоматично. Слід обрати «Ні» (рис.3.40).

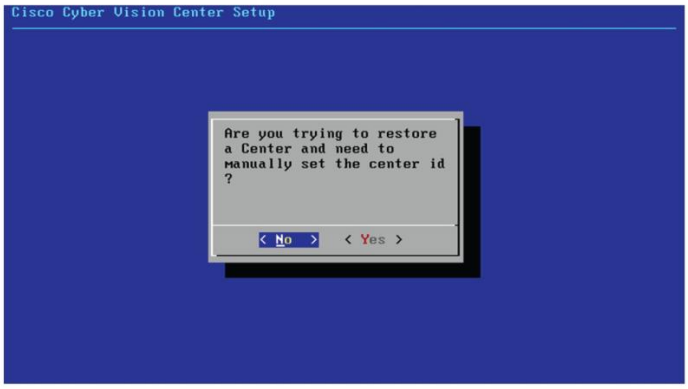

Рис.3.40. Негенерувати автоматично

Якщо перевстановлювати Центр і його потрібно відновити, слід вибрати Так (рис.3.41).

Рис.3.41. Вибір варіанту

Потрібно використати наступну команду з інтерфейсу командної команди Глобального центру, щоб отримати список усіх ідентифікаторів Центру:

sbs-db exec "select name, id from center"

Ввести ідентифікатор у поле UUID базової конфігурації центру (рис.3.42).

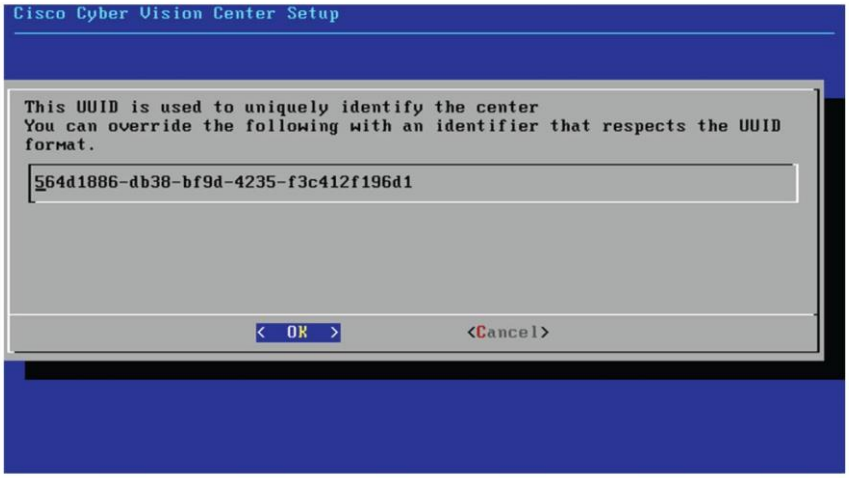

Рис.3.42. Введення ідентифікатора

Натиснути OK та перейти безпосередньо до наступного кроку.

Глобальний центр. Якщо встановлюється глобальний центр, обрати другий варіант (рис.3.43).

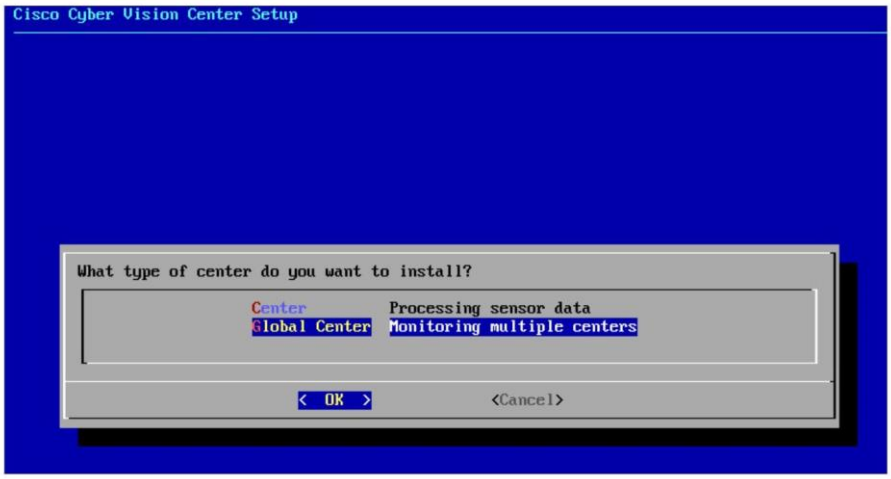

Рис.3.43. Для встановлення глобального центру

Оскільки наступний крок не стосується глобального центру, обрати Ні (рис.3.44).

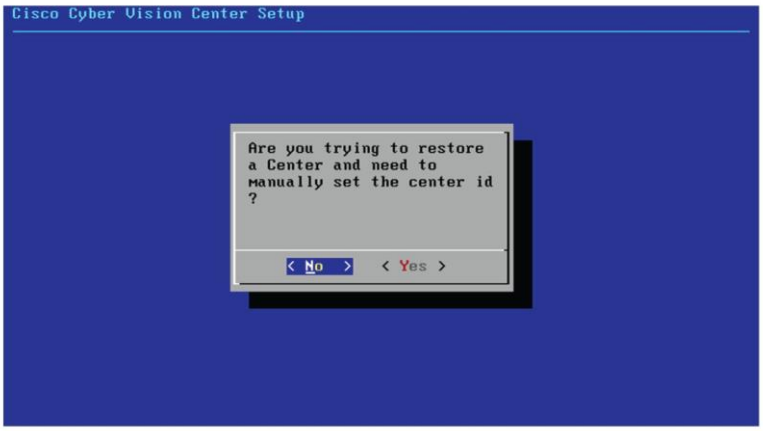

Рис.3.44. Вибір Ні

Налаштувати мережевий інтерфейс адміністрування центру. Центр використовує спеціальну підмережу в інтерфейсі адміністрування. Його можна змінити, якщо стандартний не підходить для середовища, до якого буде підключатися Центр.

Налаштувати мережевий інтерфейс адміністрування можна одним із таких способів:

- Використання DHCP-сервера, якщо він доступний у мережі (рис.3.45).

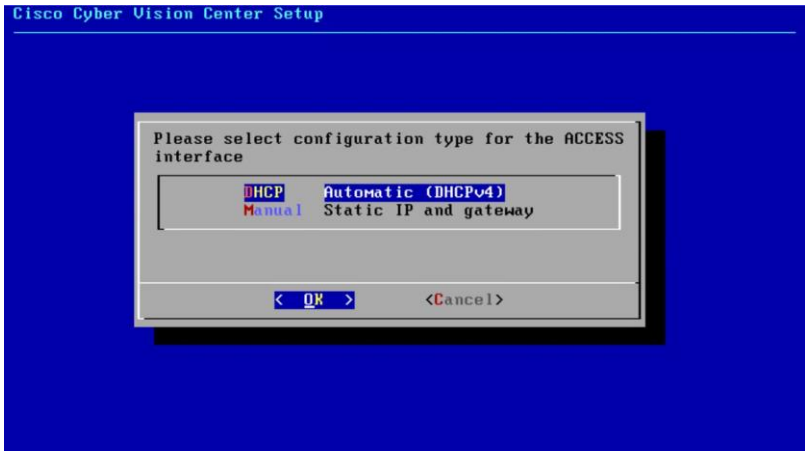

Рис.3.45. Використання DHCP-сервера

У цьому випадку ввести OK. Параметри будуть налаштовані автоматично.

- Вручну (рис.3.46):

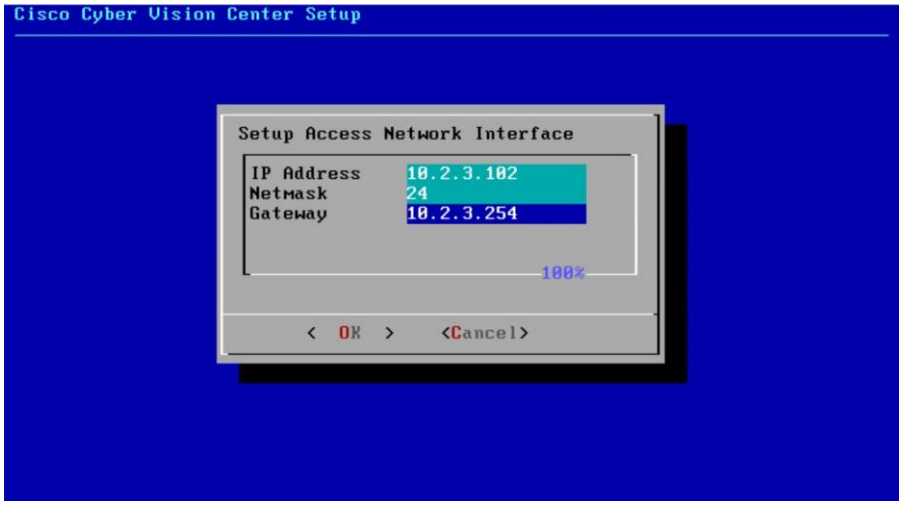

Рис.3.46. Продовження налаштування вручну

Ввести IP-адресу мережевого інтерфейсу адміністрування, маску мережі (у форматі з двох чисел) і шлюз.

Набір інтерфейсів (подвійний або одиничний). Цей крок не застосовується до глобального центру. Обрати Ні.

Що стосується центру, то можна:

- Налаштувати мережеві інтерфейси адміністрування та колекції на двох різних інтерфейсах (рекомендовано для безпеки). У цьому випадку вибирається Так.
- Використовувати єдиний інтерфейс. У цьому випадку обрати Ні (рис.3.47).

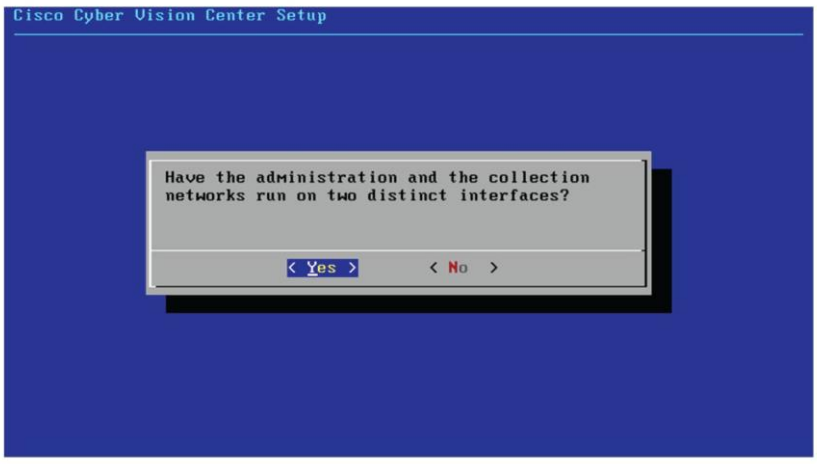

Рис.3.47. Використання єдиного інтерфейсу

Якщо налаштувати подвійний інтерфейс, то буде спрямовано до наступних екранів у підрозділі «Налаштувати мережевий інтерфейс колекції центру».

Налаштування DNS центру. Ввести адресу DNS-сервера та додаткові резервні варіанти (рис.3.48).

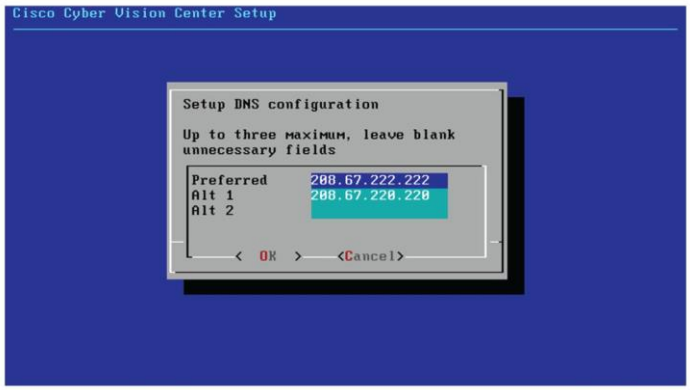

Рис.3.48. Налаштування конфігурації DNS

Синхронізація центр і датчики з NTP-серверами. Ввести IP-адреси локальних або віддалених NTP-серверів (необхідна конфігурація шлюзу), щоб синхронізувати центр і датчики з опорним годинником. Кожна адреса має бути розділена пробілом (рис.3.49).

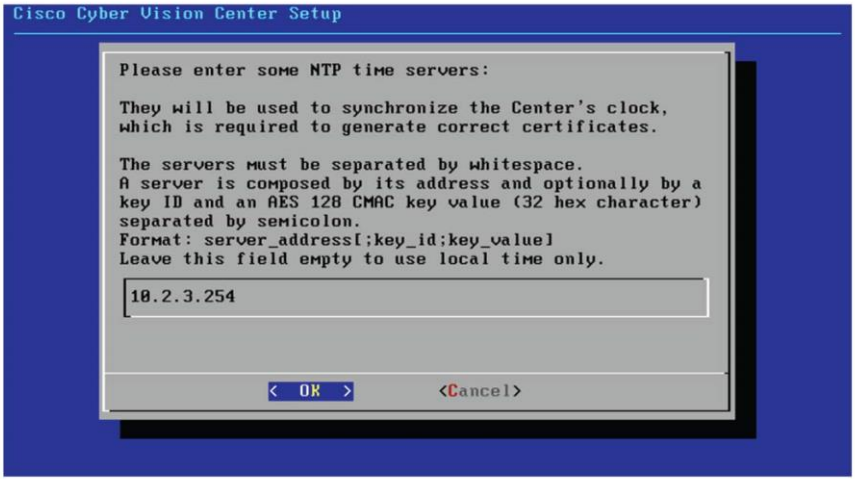

Рис.3.49. Введення IP-адрес

За бажанням можна додати ідентифікатор ключа та значення ключа AES A28 CMAC, розділені крапкою з комою з відповідним сервером NTP.

Синхронізація займає кілька секунд.

Перевірити, чи правильний час, або встановити час вручну (рис.3.50).

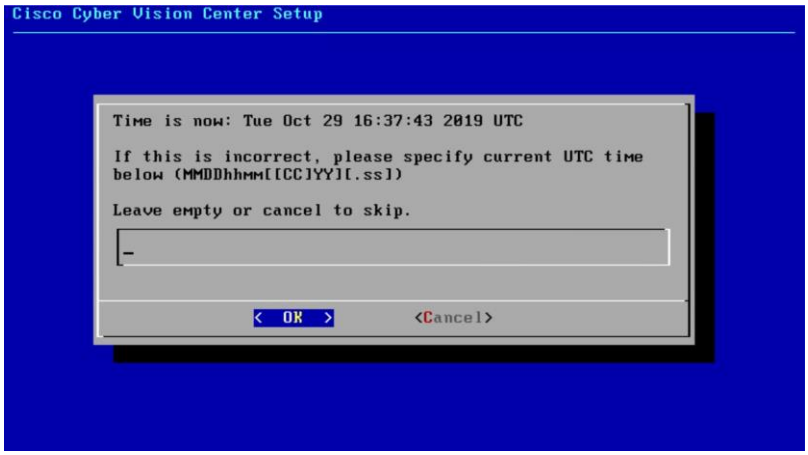

Рис.3.50. Встановлення часу

Дати назву Центру. Це ім'я буде використано в сертифікаті Центру (рис.3.51).

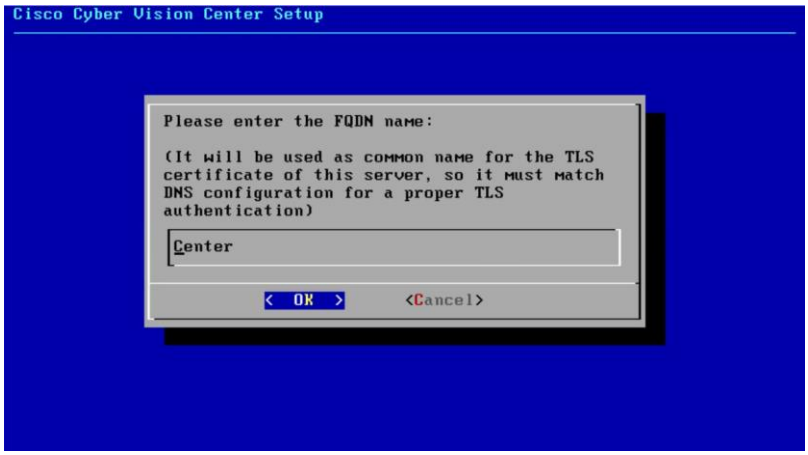

Рис.3.51. Назва Центру

Ввести назву центру, надану адміністратором, або ввести «За замовчуванням», що є безпечним значенням. Це ім’я має відповідати імені DNS, яке використовуватиметься для доступу до Центру через SSH або браузер.

Встановити пароль Центру. З міркувань безпеки необхідно встановити пароль облікового запису адміністратора (cv-admin) Центру (рис.3.52). Це приховано з міркувань конфіденційності.

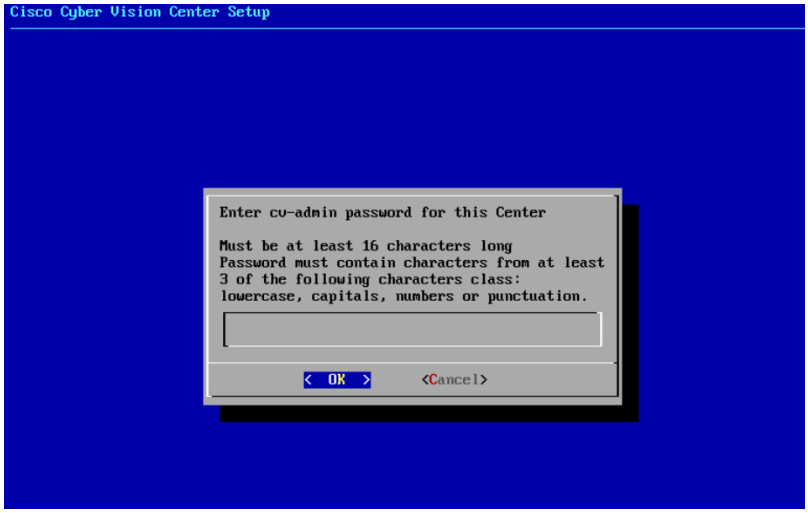

Рис.3.52. Встановлення пароля

Підтвердити пароль (рис.3.53).

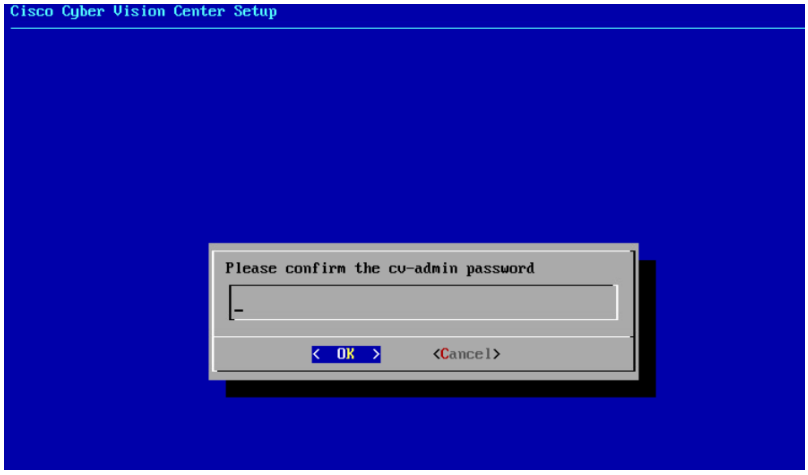

Рис.3.53. Підтвердження пароля

Налаштувати мережевий інтерфейс Центру збору. Стерти мережеву адресу (рис.3.54), запропоновану в полі, щоб вимкнути сервер DHCP, і ввести OK, щоб перейти до наступного кроку.

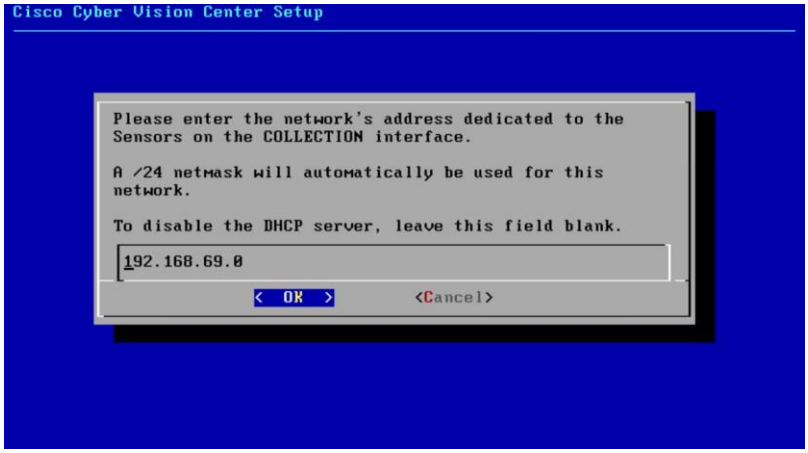

Рис.3.54. Введення IP-адрес

Ввести IP-адресу інтерфейсу промислової мережі (рис.3.55):

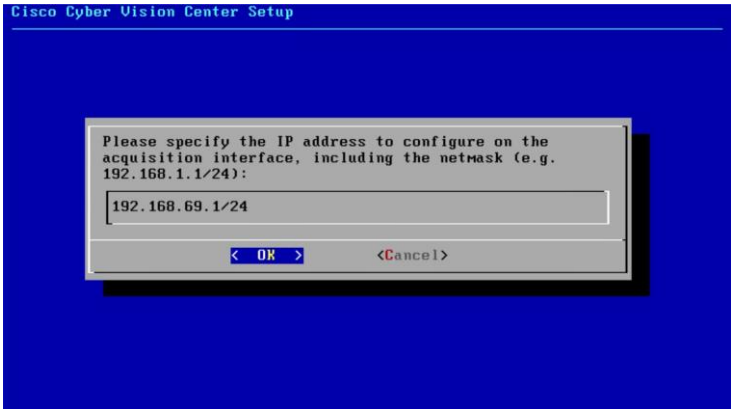

Рис.3.55. IP-адреса інтерфейсу промислової мережі

Налаштувати пароль датчиків. Оскільки цей крок не застосовується під час встановлення глобального центру, наведені нижче екрани не відображатимуться. Натомість буде спрямовано до авторизації мереж.

З міркувань безпеки необхідно встановити root-пароль датчиків (рис.3.56).

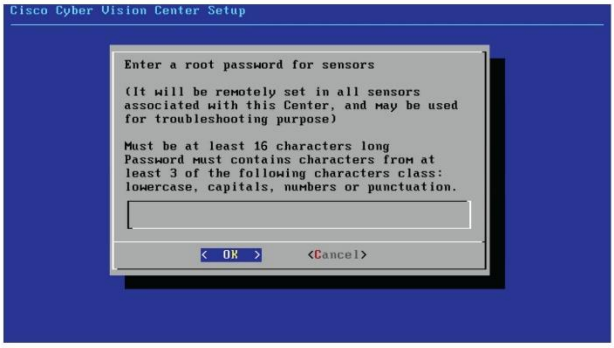

Рис.3.56. Встановлення root-пароля

Цей пароль буде призначено, коли будуть зареєстровані датчики в Центрі. Цей пароль знадобиться для усунення несправностей, діагностики та оновлень. Підтвердити пароль (рис.3.57).

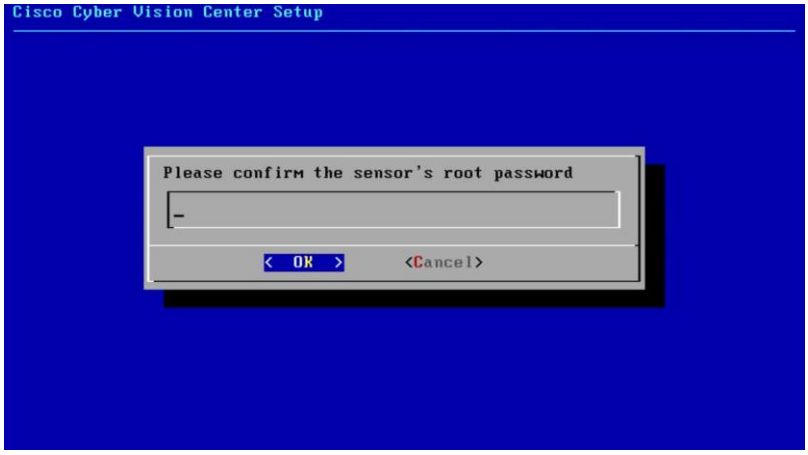

Рис.3.57. Підтвердження пароля

Авторизація мережі. Цей крок дозволяє обмежити IP-адреси, які можуть підключатися до інтерфейсу адміністрування. Якщо IP-адреса не введена, усі мережі авторизовано за замовчуванням (рис.3.58).

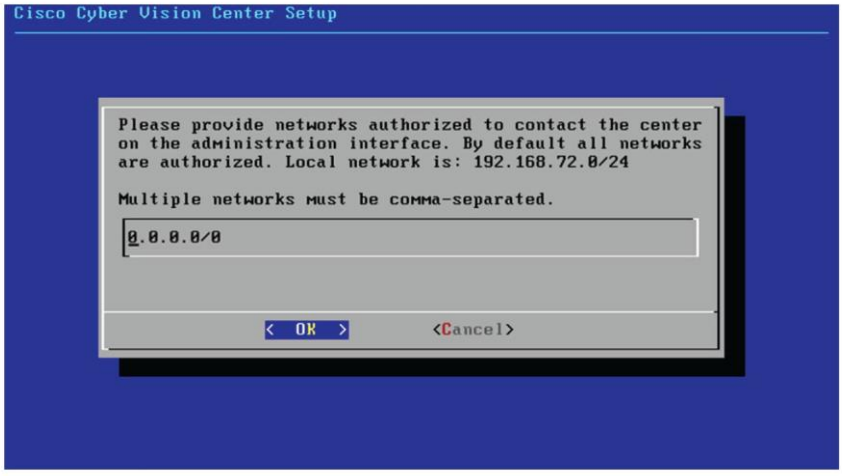

Рис.3.58. Введення IP-адреси

Завершення базової конфігурації Центру. Далі – останній екран базової конфігурації Центру. Він нагадує налаштовані адреси для завантаження сертифіката ЦС і доступу до Cisco Cyber Vision. Краще зберегти десь ці адреси, вони знадобляться пізніше для доступу до інтерфейсу користувача.

Натиснути OK, щоб завершити основне налаштування центру (рис.3.59).

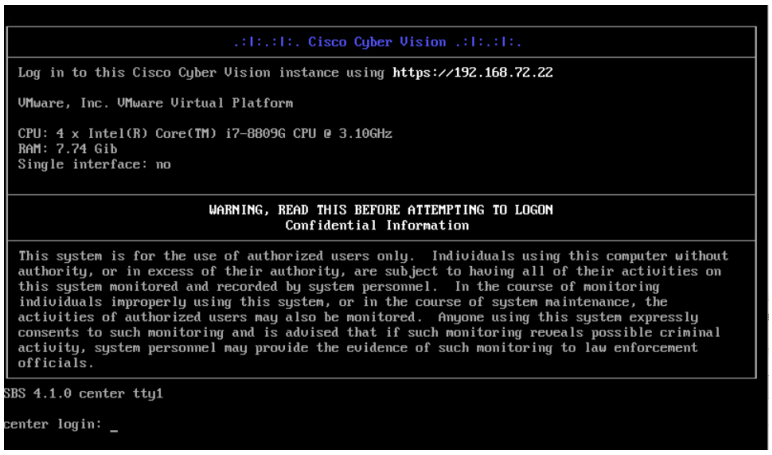

Рис.3.59. Завершення налаштувань

У версії 4.1.0 Cisco Cyber Vision було внесено суттєву зміну щодо доступу до командного рядка центру (CLI) через послідовну консоль або SSH. Корінь користувача більше не можна використовувати для встановлення з'єднання. Необхідно використати нового користувача під назвою «cv-admin». Цей користувач має обмежені права, і багато команд CLI вимагатимуть підвищення прав:

- додати до команди «sudo».
- або відкрити кореневу оболонку за допомогою «sudo –i» та ввести команду.

Закрити вікно конфігурації центру, перш ніж продовжити наступні кроки налаштування Cisco Cyber Vision.

Щоб продовжити налаштування Cisco Cyber Vision, потрібно відкрити браузер і перейти за URL-адресою, вказаною раніше, щоб отримати доступ до інтерфейсу користувача.

Кожен Cisco Cyber Vision Center включає власну PKI (інфраструктуру відкритих ключів) із CA (сертифікаційним центром), який використовуватиметься для встановлення з'єднання TLS із датчиками та клієнтами. Центр сертифікації має бути встановлений у кожному браузері клієнта.

Конфігурація Cisco Cyber Vision. Після завершення налаштування базового центру потрібно підключитися через веб-браузер до URL-адреси, яка

відображається на останньому кроці майстра базового налаштування (тобто IP-адреса центру). З’явиться повідомлення про те, що URL-адреса небезпечна.

- Якщо планується використання самопідписаного сертифіката, потрібно налаштувати браузер, а потім отримати доступ до майстра встановлення інтерфейсу користувача, щоб налаштувати користувачів і датчики.
- Якщо планується використовувати корпоративний сертифікат, слід проігнорувати повідомлення безпеки та виконати наступні дії в такому порядку:

1. Перейти до майстра встановлення інтерфейсу користувача, щоб налаштувати користувачів і датчики.

2. Налаштувати безпеку самого інтерфейсу користувача.

Потім налаштувати синхронізацію даних Центрів (лише для Глобального центру та його центрів).

Вимоги до браузера. Cisco Cyber Vision підтримує Chrome 54, Firefox 49 і новіші версії.

Встановити сертифікат у свій браузер. Це завдання пояснює, як інсталювати самопідписаний сертифікат Cisco Cyber Vision у браузері. Перед тим як почати, слід виконати це завдання, якщо потрібно встановити самопідписаний сертифікат. Якщо планується використовувати корпоративний сертифікат, то перейти безпосередньо до Установіть Cisco Cyber Vision.

1. Відкрити браузер.

2. Ввести «http://<CENTERIPADDRESS>/ca.crt» у рядку пошуку. Сертифікат завантажиться.

3. Зберегти сертифікат на комп’ютері.

4. У браузері перейти до налаштувань.

5. Ввести «сертифікат» (рис.3.60) у рядку пошуку та перейти до меню керування сертифікатами.

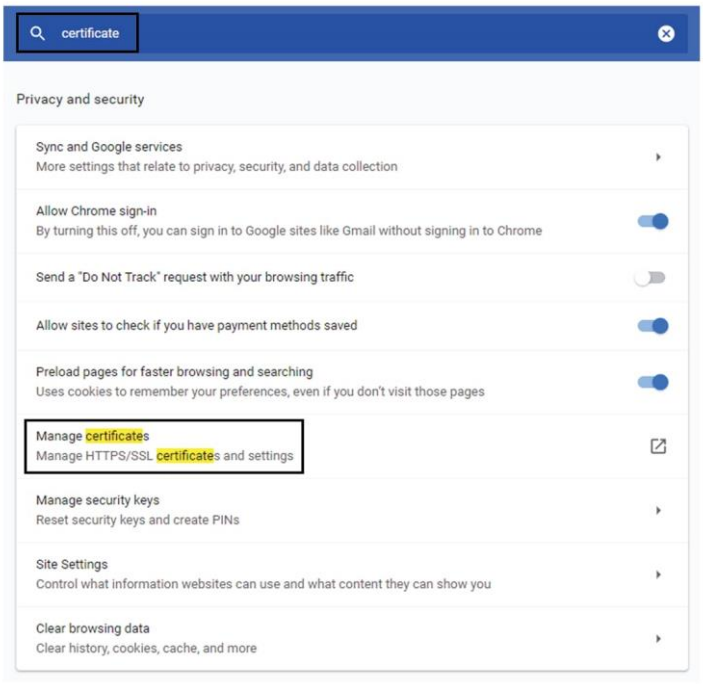

Рис.3.60. Перехід до меню сертифікатів

6. Перейти на вкладку «Довірена коренева сертифікація» та натиснути «Імпортувати». Відкриється майстер імпорту сертифікатів.

7. Перейти до наступного кроку.

8. Знайти сертифікат, який був завантажений раніше.

9. Перейти до наступного кроку.

10. Прийняти значення за замовчуванням (рис.3.61), перейшовши до наступного кроку.

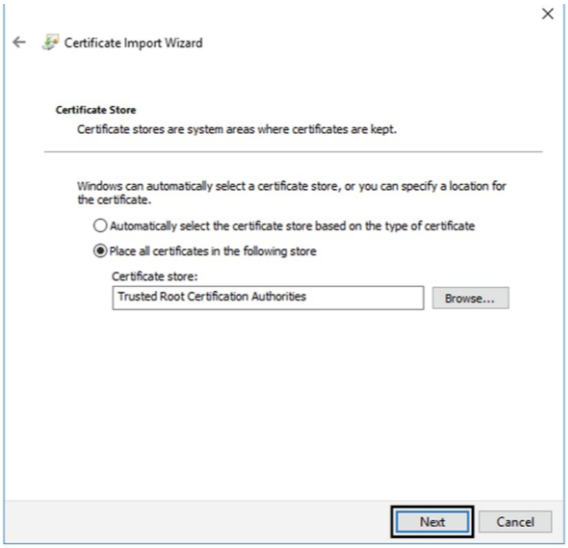

Рис.3.61. Вибір за замовчуванням

11. Сертифікат тепер вважається надійним у браузері(рис.3.62). Його буде імпортовано, щойно буде натиснута клавіша «Готово».

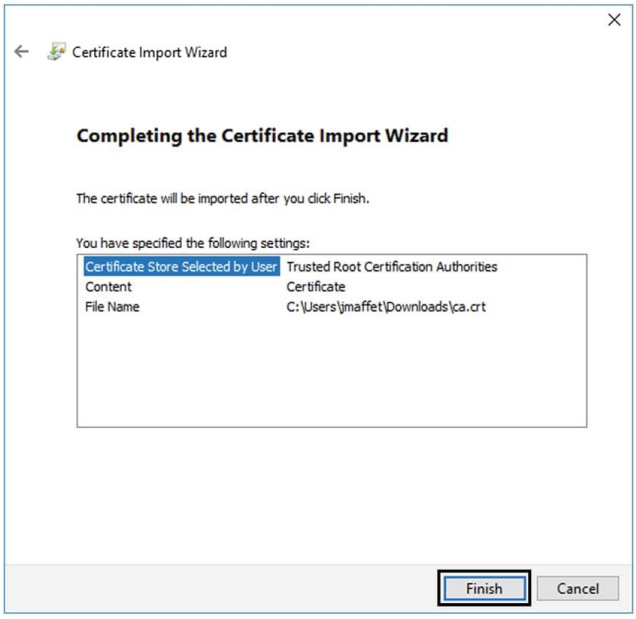

Рис.3.62. Надійність сертифіката

Встановити Cisco Cyber Vision. Доступ до майстра встановлення Cisco Cyber Vision:

1. За допомогою браузера перейти за посиланням https://<CENTERNAME>/.

2. Доступ до Центру за його іменем увімкне безпечний інтерфейс HTTPS. Однак для цього потрібна конфігурація DNS або локального хоста, щоб зв’язати ім’я та IP-адресу. Доступ до центру через його IP-адресу можливий, але з’єднання не є безпечним.

3. Відобразиться майстер налаштування, використаний для першого доступу до Cisco Cyber Vision. Необхідно створити обліковий запис адміністратора (рис.3.63), та ввести необхідну інформацію.

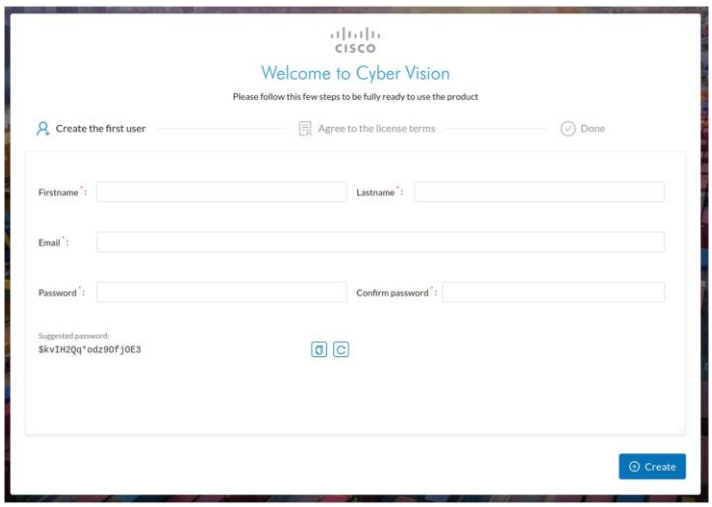

Рис.3.63. Створення облікового запису

Буде запропоновано доступ до електронної пошти для входу. Паролі повинні містити не менше 6 символів і відповідати наведеним нижче правилам.

Паролі:

- Має містити символ нижнього регістру: az.
- Має містити символ верхнього регістру: AZ.
- Має містити цифровий символ: 0-9.
- Не може містити ідентифікатор користувача.
- Має містити спеціальний символ: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

Паролі слід регулярно змінювати, щоб забезпечити цілісність платформи та безпеку промислової мережі. Можна скинути користувачів за допомогою такої команди в CLI Center: sbs-db reset-users

Далі, необхідно прийняти ліцензійну угоду на програмне забезпечення.

Встановлення Cisco Cyber Vision завершено. Якщо потрібно використати корпоративний сертифікат, слід перейти до Налаштування безпеки інтерфейсу користувача. Якщо вже встановлено самопідписаний сертифікат і якщо встановлюється глобальний центр або синхронізований центр, перейти до Налаштування синхронізації даних центру. Якщо вже встановлено самопідписаний сертифікат і якщо встановлюється автономний центр, можна почати встановлення

датчиків. Для цього слід звернутись до відповідних посібників із встановлення датчика Cisco Cyber Vision.

Налаштувати безпеку інтерфейсу користувача. Пояснюється, як налаштувати захист інтерфейсу користувача Cisco Cyber Vision за допомогою сертифіката підприємства. Є можливість завантажити .p12 або створити CSR.

Перед тим як почати слід виконати це завдання, якщо планується використання сертифіката підприємства. Потрібно попередньо встановити Cisco Cyber Vision.

1. Щоб використовувати корпоративний сертифікат, потрібно перейти до Адміністратор > Сертифікат центру (рис.3.64).

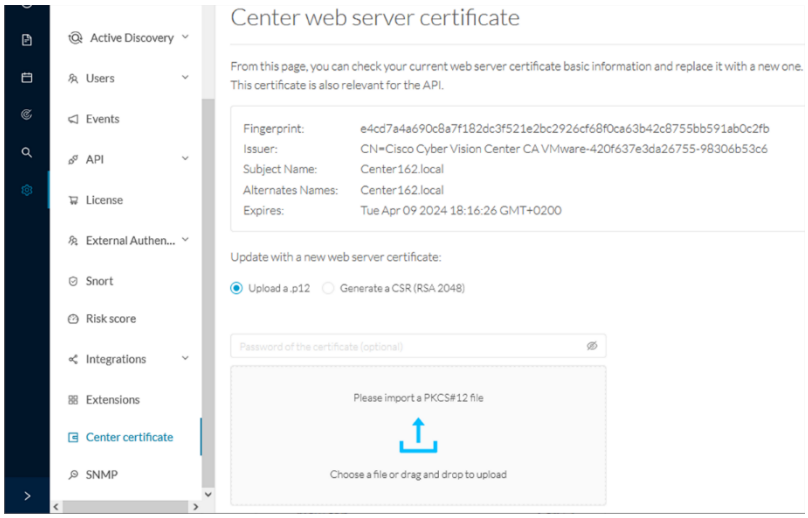

Рис.3.64. Для використання корпоративного сертифіката

2. Можна завантажити .p12 або створити CSR.

Завантажити p12. Перед тим як почати, файл p12 (або Microsoft pfx) має містити закритий ключ, пароль, а поле «Альтернативне ім’я суб’єкта X509v3» має містити DNS-ім’я центру. Вибрати Завантажити .p12 (рис.3.65).

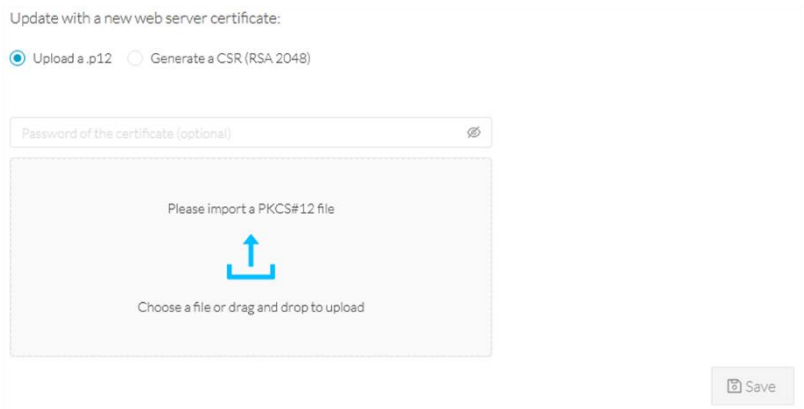

Рис.3.65. Завантаження

Натиснути - імпортувати файл PKCS12 і вибрати файл pfx або p12, створений на сервері сертифікації. Ввести пароль сертифіката. Натиснути кнопку «Імпортувати файл PKCS#12» або перетягнути файл, щоб імпортувати його (рис.3.66).

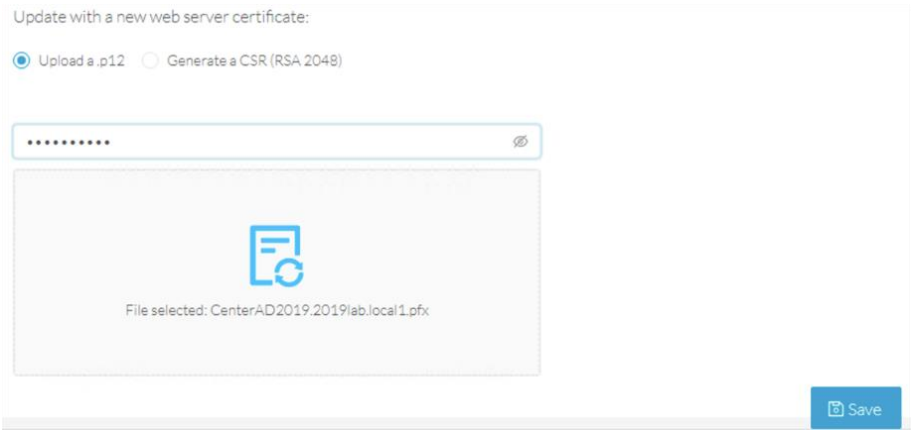

Рис.3.66. Імпортування файлу

Натиснути Зберегти.

З'явиться таке повідомлення (рис.3.67):

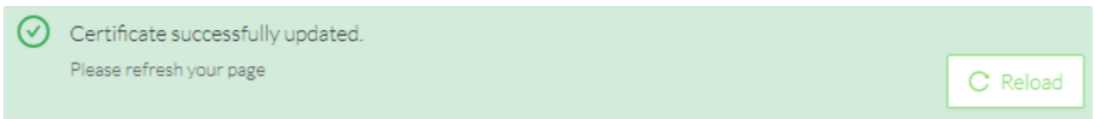

Рис.3.67. Сертифікат збережено

Натиснути Перезавантажити.

У браузері потрібно використовувати ім’я DNS, щоб підключитися до власного екземпляра Cisco Cyber Vision.

Повідомлення про помилку не з’являється, з’єднання безпечне.

Якщо встановлюється глобальний центр або синхронізований центр, потрібно перейти до Налаштування синхронізації даних центру.

Якщо встановлюється автономний центр, можна почати установку датчиків. Для цього слід звернутися до відповідних посібників із встановлення датчика Cisco Cyber Vision.

Створити CSR. Відобразиться повідомлення про те, що CSR було створено.

1. Обрати - Створити CSR (рис.3.68).

Рис.3.68. Створення CSR

2. Ввести центральне FQDN, зареєстроване на DNS-сервері.

3. Натиснути кнопку «Створити та завантажити CSR» (рис.3.69).

Рис.3.69. Кнопка створення та завантаження

4. Натиснути кнопку завантаження (1) (рис.3.70).

Завантажується файл <FQDN>.csr.

5. Використати файл <FQDN>.csr, щоб створити сертифікат pem від центру сертифікації підприємства.

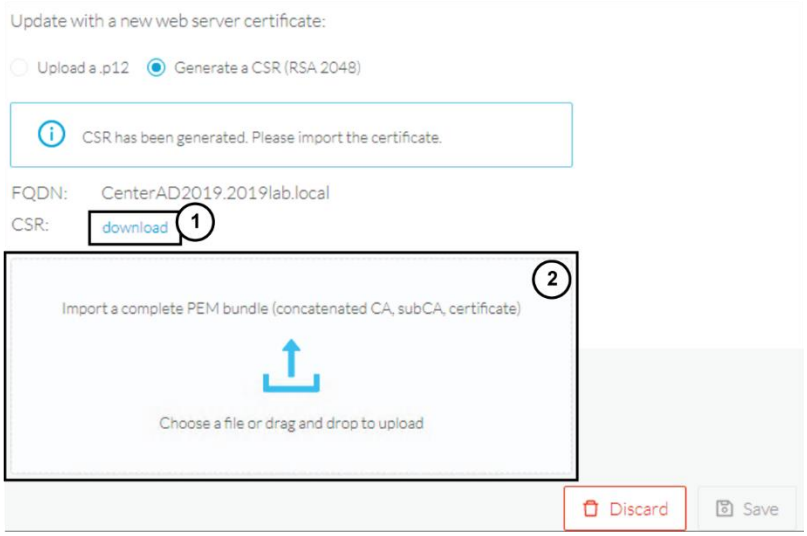

Рис.3.70. Завантаження

6. Після створення сертифіката pem повернутись до Cisco Cyber Vision і натиснути кнопку «Імпортувати повний пакет PEM» (2) або перетягніти його, щоб імпортувати (рис.3.71).

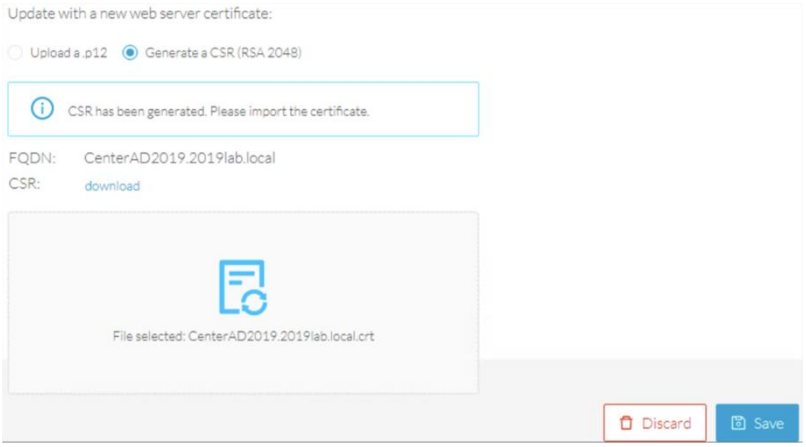

Рис.3.71. Імпортування

7. Натиснути Зберегти.

З'явиться таке повідомлення (рис.3.72):

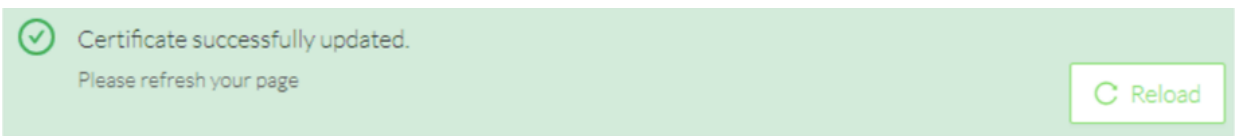

Рис.3.72. Повідомлення про перезавантаження

8. Натиснути Перезавантажити. У браузері використовуйтся ім’я DNS, щоб підключитися до свого екземпляра Cisco Cyber Vision. Повідомлення про помилку не з’являється, з’єднання безпечне.

Якщо встановлюється глобальний центр або синхронізований центр, потрібно перейти до Налаштування синхронізації даних центру. Якщо встановлюєтся автономний центр, можна почати установку датчиків. Для цього слід звернутись до відповідних посібників із встановлення датчика Cisco Cyber Vision.

Налаштувати синхронізацію даних центру. Цей крок застосовується до глобального центру та його синхронізованих центрів. Після встановлення Глобального центру та його синхронізованих центрів потрібно перейти до синхронізації даних, яка складається з реєстрації Центру в Глобальному центрі та реєстрації Центру в Глобальному центрі. Для цього потрібно відкрити графічний інтерфейс Cisco Cyber Vision кожного.

Щоб відрізнити кожен інтерфейс користувача, потрібно перевірити верхній лівий кут «Глобального центру» або «Центру» Cisco Cyber Vision.

У графічному інтерфейсі Cisco Cyber Vision Глобального центру потрібно перейти до Адміністратора > Керування системою > Керування.

Натиснути кнопку Зареєструвати центр.

Відкриється вікно «Реєстрація центру», готове до заповнення. Тепер потрібно отримати доступ до графічного інтерфейсу користувача Центру, щоб отримати його відбиток.

У графічному інтерфейсі користувача Cisco Cyber Vision центру перейти до Адміністратора > Система.

Далі прокрутити униз до розділу Відбиток сертифіката (рис.3.73) та скопіювати його.

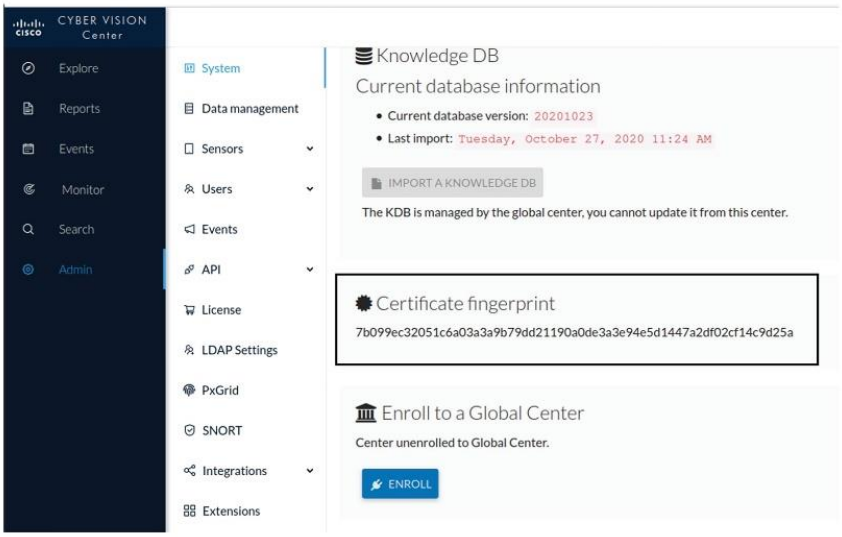

Рис.3.73. Відбиток сертифіката

У графічному інтерфейсі глобального центру дати назву центру та вставити відбиток пальця центру у відповідне поле (рис.3.74).

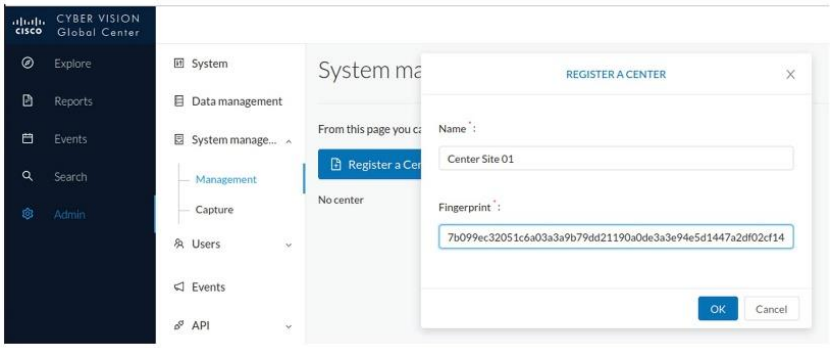

Рис.3.74. Назва центру

Центр відображається в списку як незареєстрований (рис.3.75).

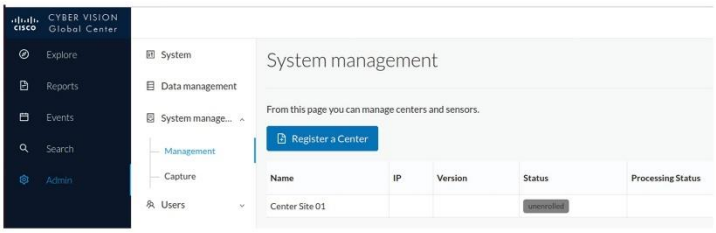

Рис.3.75. Відображення Центру у списку

На цьому етапі потрібно перейти до графічного інтерфейсу користувача Центру та зареєструвати його в Глобальному центрі. У GUI Центрі прокрутити

униз до пункту Зареєструвати глобальний центр і натиснути кнопку Зареєструвати (рис.3.76).

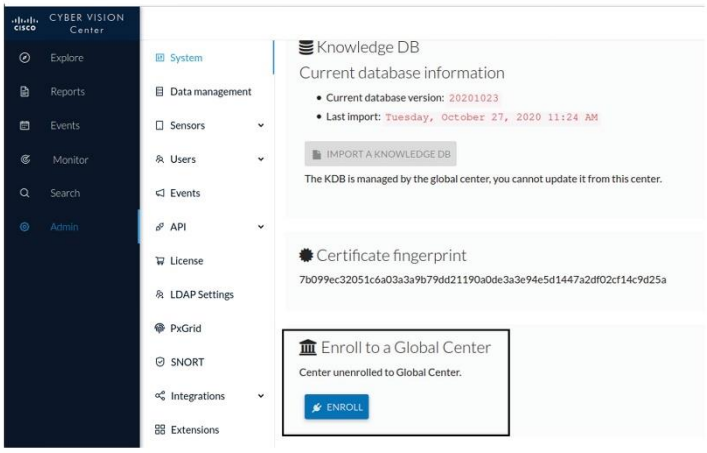

Рис.3.76. Реєстрація глобального Центру

Відкриється вікно реєстрації. Скопіювати відбиток пальця Глобального центру зі сторінки системного адміністрування графічного інтерфейсу користувача (те саме місце, що й Центр). Ввести IP-адресу глобального центру та натиснути «Зареєструватися».

Після завершення синхронізації вказується, що центр зареєстровано в глобальному центрі.

У графічному інтерфейсі глобального центру статус центру змінюється на Підключено (рис.3.77).

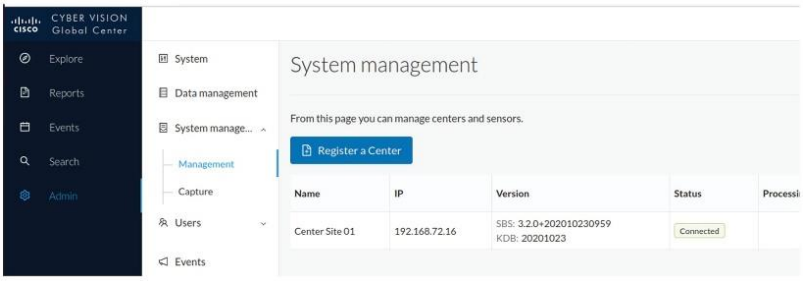

Рис.3.77. Зміна статусу на Підключено

Глобальний центр і Центр успішно підключені. Повторити попередні кроки стільки разів, скільки потрібно для підключення інших центрів. Наступним кроком буде встановлення та реєстрація датчиків. Для цього слід звернутись до відповідних посібників із встановлення сенсорів Cisco Cyber Vision.

Після підключення датчика він з’явиться в графічному інтерфейсі глобального центру, як показано нижче (рис.3.78) [21]:

Рис.3.78. Підключення датчика

3.3 Налаштування центру DPI

Вимоги. Переконатись, що інтерфейс Ethernet доступний для трафіку Center DPI залежно від:

- Якщо сервер має подвійний інтерфейс, тобто інтерфейс адміністрування знаходиться на eth0, а інтерфейс колекції – на eth1, тоді eth2 використовуватиметься для центру DPI.
- Якщо сервер має єдиний інтерфейс, тобто інтерфейси адміністрування та збору знаходяться на одному інтерфейсі, тоді eth1 використовуватиметься для центру DPI.

Налаштування центру DPI.

1. Перейти на сторінку адміністрування датчиків Cisco Cyber Vision (рис.3.79).

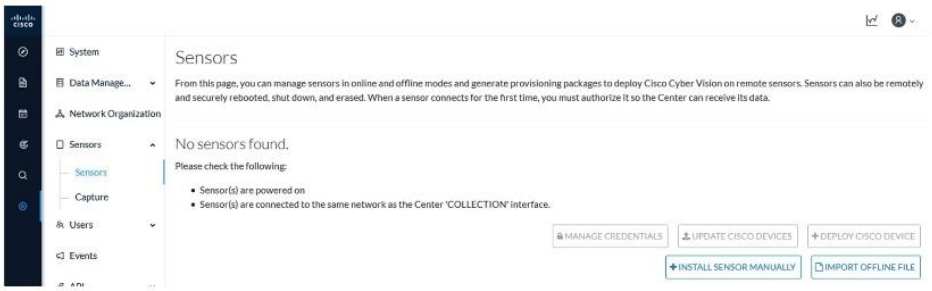

Рис.3.79. Адміністрування датчиків

2. Відкрити запрошення центральної оболонки та ввести таку команду: sbs-netconf (рис.3.80).

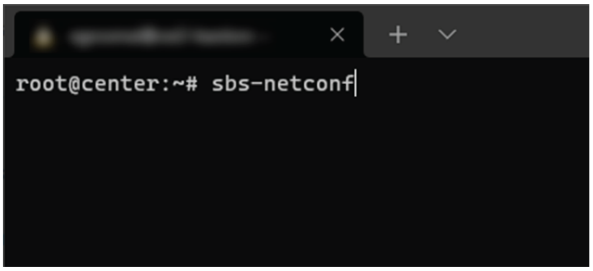

Рис.3.80. Запрошення центральної оболонки

3. У випадку одного інтерфейсу обрати інтерфейс eth1.

У випадку подвійного інтерфейсу обрати eth2 (рис.3.81).

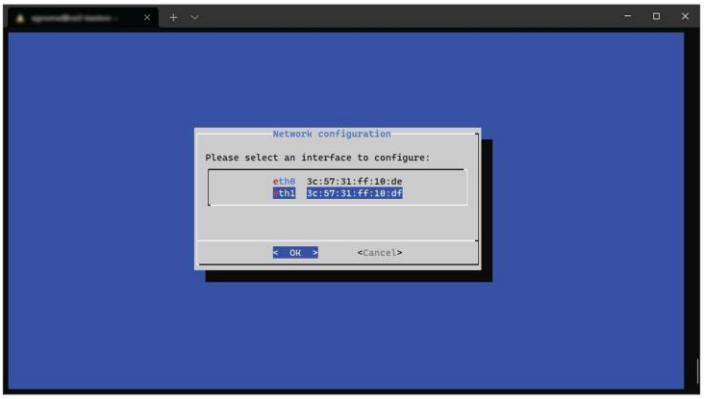

Рис.3.81. Вибір інтерфейсу

4. Обрати інтерфейс як порт DPI+Snort (рис.3.82).

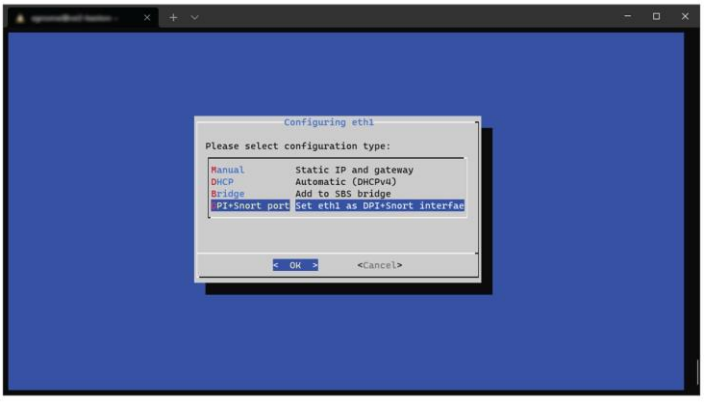

Рис.3.82. Вибір інтерфейсу

5. Налаштувати режим фільтра захоплення. Можна зробити це пізніше на сторінці датчика Cisco Cyber Vision, натиснути кнопку Режим захоплення.

Наприклад, можна ввести «not arp» (рис.3.83).

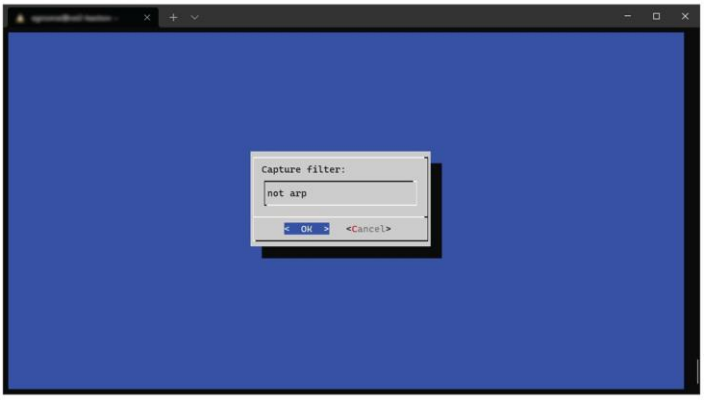

Рис.3.83. Введення «not arp»

На сторінці датчика адміністрування Cisco Cyber Vision з’являється новий віртуальний датчик, який готовий приймати дані (рис.3.84) [22].

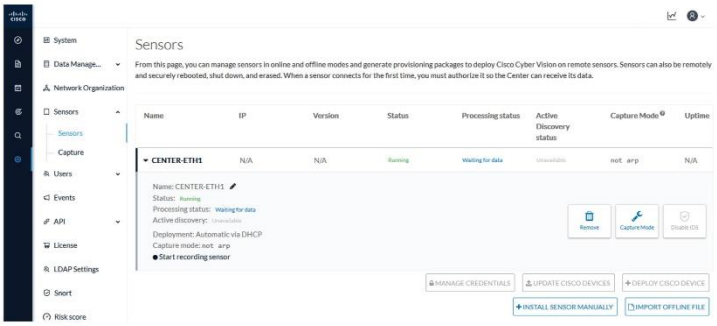

Рис.3.84. Сторінка датчика адміністрування

3.4 Налаштування глобального центру

Функція Cisco Cyber Vision Global Center дозволить синхронізувати кілька центрів в одному репозиторії. Глобальний центр об’єднає Центри в єдину програму та представить підсумок діяльності кількох Центрів.

Після завершення налаштування Центру та Глобального центру можна ініціалізувати синхронізацію Центру з Глобальним центром. Цей процес включає реєстрацію Центру з Глобальним Центром. Коли центр зареєстровано, його дані поступово синхронізуються. Пізніше, за потреби, Центр може бути виписаний. Потім Глобальний центр видалить усі дані з цього конкретного Центру. Центр стане незареєстрованим і буде готовий до майбутньої реєстрації.

Реєстрація центру. Глобальний центр і його центри повинні бути доступними, щоб бути зареєстрованими.

1. Запустити процес в інтерфейсі користувача Центру для синхронізації, перейти до меню адміністратора, на системній сторінці можна знайти відбиток сертифіката (рис.3.85).

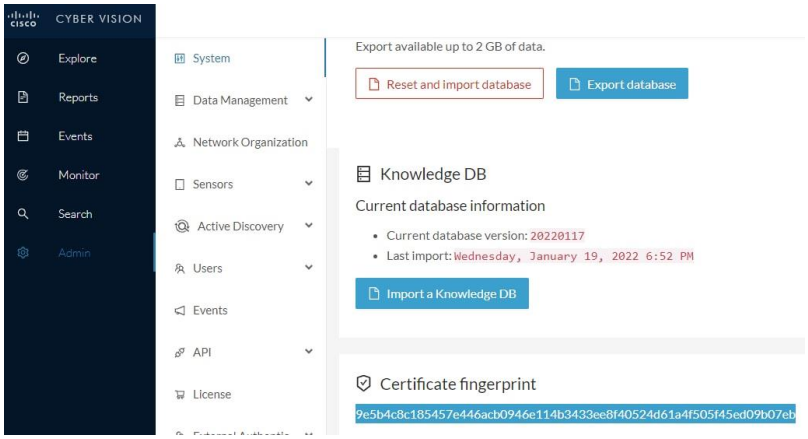

Рис.3.85. Вікно відбитка сертифіката

2. Перейти до інтерфейсу користувача Global Center, меню «Адміністратор», у розділі «Керування системою» перейти до меню «Керування». Натиснути на кнопку Зареєструвати центр:

a. Заповнити поле «Назва» назвою.

b. Вставити скопійований вище відбиток сертифіката (рис.3.86).

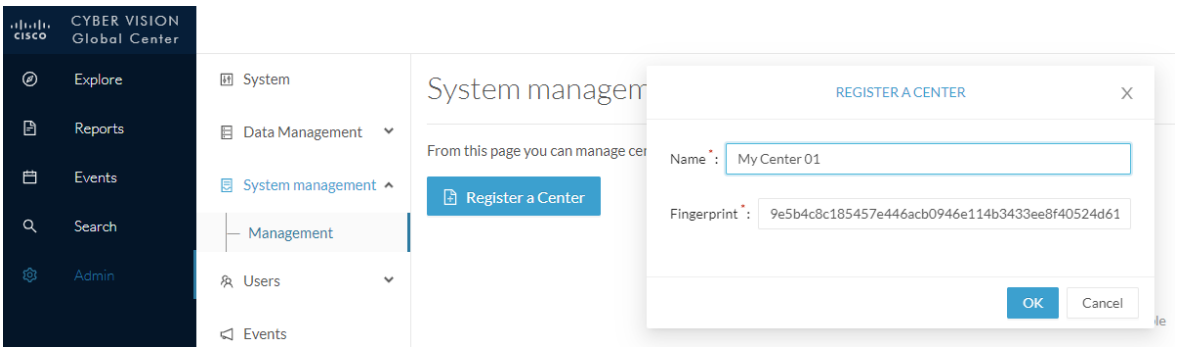

Рис.3.86. Реєстрація центру

3. Залишатися в Глобальному центрі в тому ж меню (Адміністратор - Керування системою - Керування) і скопіювати відбиток Глобального центру (рис.3.87).

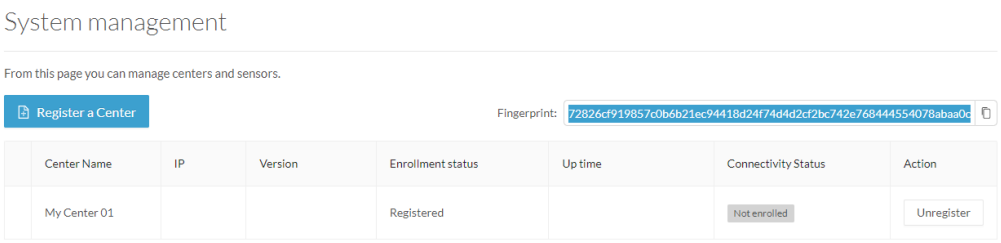

Рис.3.87. Копіювання Відбитка пальця Глобального центру

4. У центрі в меню адміністратора на сторінці «Система» натиснути кнопку «Зареєструватися» та:

a. Додати відбиток глобального центру (вставити його зі значенням, скопійованим вище, у глобальний центр).

b. Додати IP-адресу глобального центру.

c. Натиснути Зареєструватися (рис.3.88).

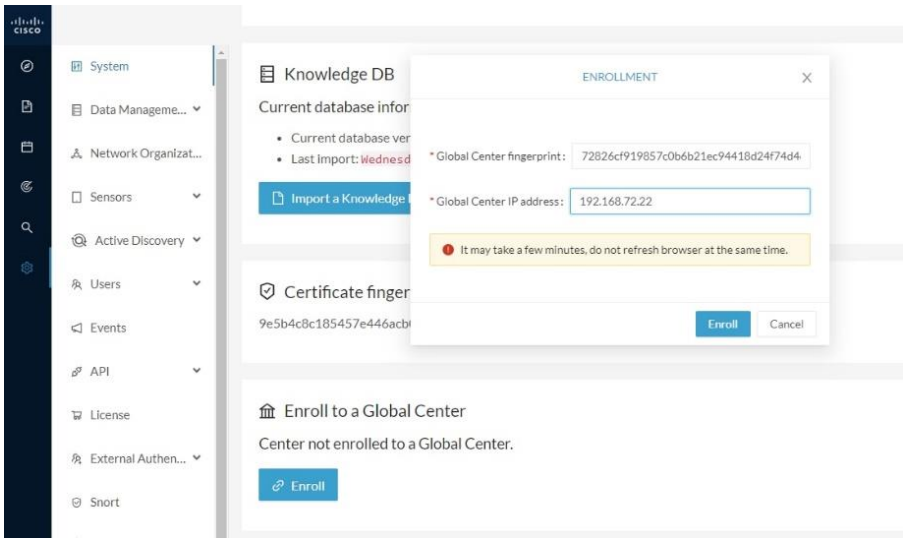

Рис.3.88. Реєстрація

5. Відбудеться перша синхронізація. Центр надішле всю необхідну історичну інформацію. Після завершення з’явиться зелене повідомлення: Реєстрація виконана (рис.3.89).

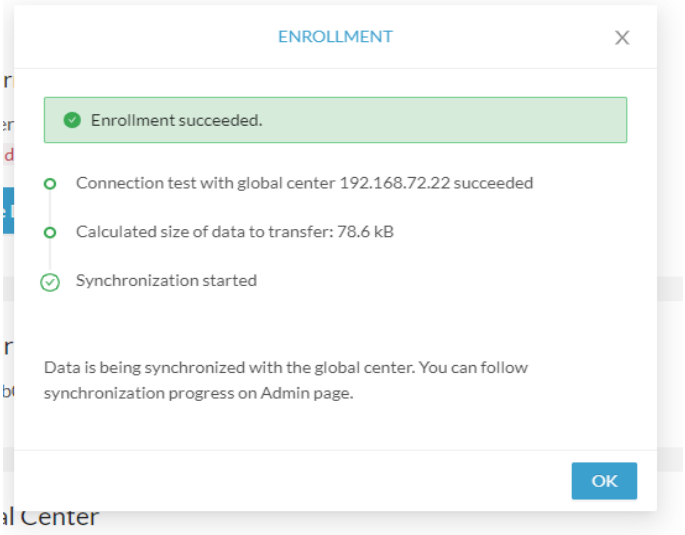

Рис.3.89. Виконана реєстрація

Після реєстрації Центр регулярно синхронізується з Глобальним центром.У глобальному центрі в меню адміністратора сторінка «Керування системою» надає статус усіх синхронізованих центрів та їхніх датчиків (рис.3.90).

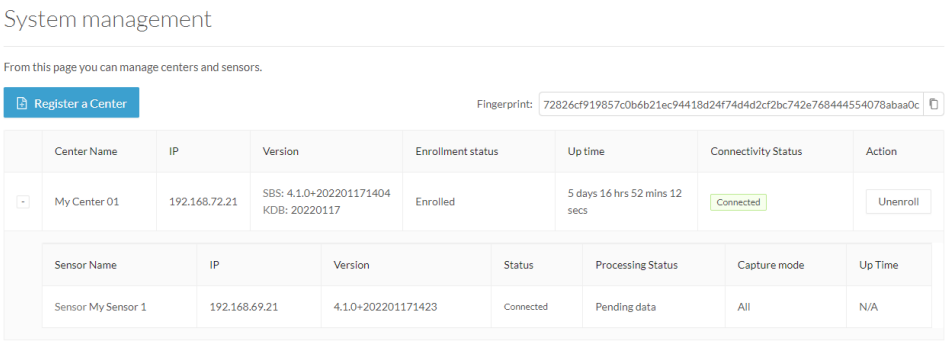

Рис.3.90. Статус усіх синхронізованих центрів та їхніх датчиків

Скасування центру. Центр можна скасувати, коли це необхідно, наприклад, як операцію з технічного обслуговування для заміни Центру або Глобального центру. Це призведе до видалення всіх даних Центру в Глобальному центрі.

1. У Cisco Cyber Vision перейти до Адміністратор > Керування системою > Керування. Перераховано всі центри Глобального центру.

2. Натиснути Скасувати реєстрацію в потрібному центрі (рис.3.91).

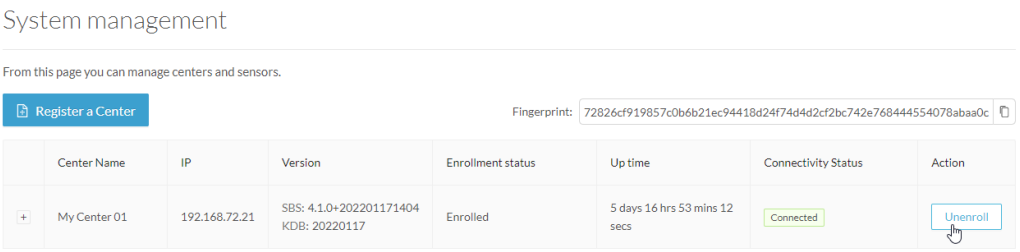

Рис.3.91. Скасування реєстрації

У разі заміни глобального центру потрібно скасувати реєстрацію всіх його синхронізованих центрів.

3. З'явиться спливаюче вікно із запитом підтвердження. Натиснути Скасувати реєстрацію, щоб розпочати процес.

4. Якщо зареєстровано в іншому Глобальному центрі, цей центр залишатиметься в списку свого колишнього Глобального центру як «Не зареєстрований». Можна скористатися кнопкою Скасувати реєстрацію, щоб видалити його зі списку (рис.3.92).

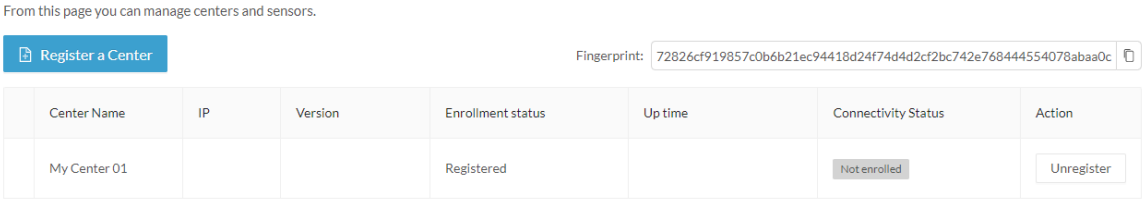

Рис.3.92. Видалення зі списку

Примусово скасувати реєстрацію центру. Якщо Центр із синхронізацією був відключений протягом дуже тривалого часу, наприклад, через збій апаратного забезпечення, його можна скасувати з глобального центру. Це дозволить видалити всі дані Центру та замінити їх.

У Cisco Cyber Vision перейти до Адміністратор > Керування системою > Керування. Перераховано всі центри Глобального центру.

Щоразу, коли центр було відключено протягом тривалого часу, у стовпці «Дія» з'являється червона кнопка «Примусово скасувати реєстрацію».

Використати цю кнопку, щоб видалити всі дані Центру з Глобального центру. Центр буде вилучено зі списку (рис.3.93) [23].

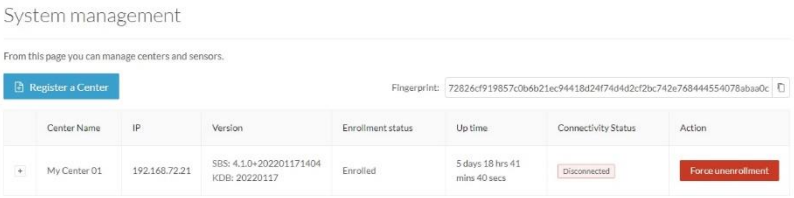

Рис.3.93. Вилучення центру зі списку

3.5 Рекомендації

Нижче наведено поради щодо забезпечення безпеки:

1. Безпека за проєктом. Вбудувати захист у власні системи IIoT якомога раніше, оскільки зміни набагато легше та економічніше вносити на ранніх стадіях життєвого циклу продукту, особливо тому, що належні функції безпеки та конфіденційності рідко коли-небудь «закріплюються».

2. Принципи інформаційної безпеки. Що стосується створення продуктів IoT/IIoT, деякі з основних концепцій інформаційної безпеки включають автентифікацію (автентифікація пристроїв у хмарних службах, між користувачами та пристроями та від речі до речі), шифрування (яке дозволяє приватне спілкування) і дані цілісність (для того, щоб повідомлення можна було довіряти та не було змінено під час передачі).

3. Використовувати перевірені технології та стандарти – поєднання захищеного апаратного забезпечення, наприклад модулів довіреної платформи (TPM) з інфраструктурою відкритих ключів (PKI), забезпечує надійні припущення про ідентифікацію.

4. Використовувати хмару – модель SaaS дозволяє широкомасштабне розгортання сертифікатів без витрат і налаштування локального обладнання.

5. Не йти наодинці – пошук відповідного партнера з безпеки є ключовим фактором для реалізації бізнес-вигод IIoT [24].

Cisco Cyber Vision розроблено для IT-команд і професіоналів із забезпечення контролю виробництва та безпеки. Він допомагає підприємствам розвиватися на висоті, надаючи їм статистичні дані в режимі реального часу та передові системи безпеки другого рівня, а також просту та унікальна модель. Вона також допомагає клієнтам створити базову лінію для моделювання нормального стану для виробництва. API цієї системи може інтегруватися з поточною IT-інфраструктурою, а також може ділитися контекстом OT. Він захищає домен OT шляхом інтеграції з IT SOC. Користувачі можуть розгорнути систему моніторингу безпеки та масштабувати свої проєкти сегментації мережі.

Cisco Cyber Vision — це чудова функція, яка керує, контролює та захищає бізнес. Cisco Cyber Vision відповідає власним промисловим протоколам для відстеження аномалій процесів, модифікацій активів і змін змінних. Він також має вбудовану систему аналізу загроз, яка захищає бізнес. Він також може виправляти вразливості, відомі чи невідомі нові загрози. Користувачі можуть виявити збій пристрою та інші аномалії. Він повністю інтегрований із кіберпортфоліо Cisco та багатьма її рішеннями безпеки. Користувачі можуть захищати атаки від поширення та керувати системою моніторингу. Це усуває потребу в спеціалізованих приладах. Він працює в напрямку підходу, орієнтованого на клієнта, і створює для користувача екологічно чисте та дружнє для бізнесу середовище [25].

Недоліки. У віддалених районах може виникнути проблема з вартістю та розгортанням.

Переваги:

- Покращення результатів бізнес-процесів
- Покращення гнучкості бізнес-процесів
- Створення внутрішньої/операційної ефективності
- Управління витратами
- Стимулювання зростання доходу
- Покращити прийняття рішень
- Стимулювання інновації

Ключові фактори вибору продукту:

- Дорожня карта продукту та бачення майбутнього
- Сильний досвід надання послуг
- Широта послуг
- Фінансова/організаційна спроможність
- Загальна вартість
- Попередні відносини
- Функціональність і продуктивність продукту

Висновки до третього розділу

Проведено детальне встановлення програмного забезпечення, яке складалось з етапів отримання інсталяційного файлу та створення віртуальної машини на ESXi і Hyper-V.

Показано налаштування Cisco Cyber Vision Center і додаткових фунцкій центру DPI та глобального центру, з детальною ілюстрацією процесу.

Досліджено рекомендації щодо забезпечення безпеки, з наведеними порадами таких як: безпека за проєктом, принцип інформаційної безпеки, використання перевірених технології і стандартів, використовння хмари та терміну «Не йдіть наодинці».

ВИСНОВКИ

В магістерській роботі отримано наступні наукові на науково-практичні результати:

1. Проаналізовано головну ідею промислових IoT з представленою інформацією про прорив людини у світі науково-технічних технологій.

2. Створено порівняльний аналіз подібностей та відмінностей між IoT та IIoT, з представленою таблицею порівняння. Виокремлено проблематики щодо захисту IIoT від кіберзагроз,через те, що потреба в кібербезпеці висувається на перший план, оскільки з роками з’являються все більш серйозні інциденти безпеки.

3. Показано огляд рішення Cisco Cyber Vision для захисту промислових мереж від кіберзагроз. Обґрунтовано основні інструменти для захисту промислових операцій, а саме: видимість вбудована у промислову мережу, найкраща видимість усіх підключених активів, оперативна інформація для OT, безпека для IT та розширення IT-безпеки на OT.

4. Продемонстровано основні рішення для вирішення проблематика промислових IoT з представленим інтерфейсом Cisco Cyber Vision. Проаналізовано порівняння Cisco Cyber Vision з популярними конкурентами, таких як: Claroty, Dragos Platform та Nozomi Networks Guardian.

5. Проведено детальне встановлення програмного забезпечення, яке складалось з етапів отримання інсталяційного файлу та створення віртуальної машини на ESXi та Hyper-V. Продемонстровано етапи керуванням глобального центру: реєстрація (для ініціалізації синхронізації Центру з Глобальним центром), скасування та примусове завантаження реєстрації центру. Запропоновано рекомендація, щодо забезпечення безпеки IIoT.

6. Визначено, що зазначені рекомендації встановлення і налаштування всіх компонентів Cisco Cyber Vision щодо безпеки промислових Інтернет речe можуть бути використані у сфері наукового та практичного забезпечення кібербезпеки інформаційних систем або промислових мереж.