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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія реагування на інциденти критичної інфраструктури організацій на базі рішення Infinity NDR»

зі спеціальності *125 Кібербезпека та захист інформації*

(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*

(назва програми)

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

_____ Олександр БРИГИНЕЦЬ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
БРИГИНЕЦЬ Олександр

(прізвище, ім'я)

Керівник д.т.н., професор КАЗМІРЧУК Світлана

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

Рецензент

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

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ICS	–	Industrial Control System
SCADA	–	Supervisory Control and Data Acquisition
PLC	–	Programmable Logic Controller
NDR	–	Network Detection and Response
OT	–	Operational Technology
SOC	–	Security Operations Center
PCAP	–	Packet Capture
YARA	–	Yet Another Recursive Acronym
DPI	–	Deep Packet Inspection
TLS	–	Transport Layer Security
Zero Trust	–	Архітектура безпеки з принципом «не довіряй, перевіряй»
SIEM	–	Security Information and Event Management
MTTD	–	Mean time to detect
MTTR	–	Mean time to repair

ВСТУП

Актуальність дослідження. У сучасних умовах цифровізації та глобальної інтеграції інформаційних систем критична інфраструктура держави стає об’єктом підвищеного інтересу з боку кіберзлочинців і державних акторів. Атаки на енергетичні, транспортні, фінансові та урядові об’єкти здатні призвести до порушення роботи суспільно важливих сервісів і створюють загрози національній безпеці. Традиційні засоби виявлення загроз — системи IDS/IPS, SIEM або антивірусні рішення — часто не забезпечують необхідної швидкості реагування та глибини аналітики, особливо під час багаторівневих і цілеспрямованих атак (APT). В умовах зростання обсягів мережевого трафіку та ускладнення кіберзагроз актуальним стає впровадження технологій Network Detection and Response (NDR), що поєднують аналіз мережевої поведінки, машинне навчання та автоматизоване реагування на інциденти.

Система Check Point Infinity NDR є одним із найсучасніших рішень цього класу, яке забезпечує наскрізну видимість мережевої активності, виявлення аномалій у режимі реального часу, інтеграцію з SIEM/SOAR-системами та автоматизацію реагування. Використання Infinity NDR дозволяє мінімізувати вплив людського фактору, скоротити час між виявленням і ліквідацією інциденту, а також забезпечити централізований контроль за станом безпеки критичної інфраструктури. Вищезазначене зумовлює актуальність теми кваліфікаційної роботи, присвяченої розробці технології реагування на інциденти критичної інфраструктури організацій на базі рішення Infinity NDR.

Об’єкт дослідження – процес виявлення, аналізу та реагування на кіберінциденти у системах критичної інфраструктури організацій.

Предмет дослідження – сукупність технологічних, організаційних та

аналітичних механізмів кіберзахисту критичної інфраструктури, що забезпечують виявлення, моніторинг, аналіз і реагування на кіберзагрози в інтегрованих IT- та OT-середовищах, включаючи особливості взаємодії між IT- і виробничими мережами та їх вплив на поверхню атак, вразливості промислових протоколів і технологічного обладнання, ризики, пов’язані з використанням застарілих систем та недостатньою сегментацією мереж, характерні вектори атак на критичну інфраструктуру, обмеження традиційних сигнатурних систем в умовах шифрування трафіку, роль технологій класу NDR у забезпеченні поведінкового аналізу та пасивного моніторингу, методи виявлення аномалій за допомогою машинного навчання, аналізу метаданих і глобальних баз загроз, а також вплив людського фактора на стан кібербезпеки об’єктів критичної інфраструктури.

Мета роботи – розробити технологію реагування на кіберінциденти в критичній інфраструктурі на базі рішення Infinity NDR, визначити порядок її впровадження, оцінити ефективність і надати практичні рекомендації щодо автоматизації процесів реагування у сфері кіберзахисту.

Наукові завдання:

дослідити сучасний стан проблеми реагування на кіберінциденти у критичних інфраструктурах;

проаналізувати архітектуру та функціональні можливості рішення Check Point Infinity NDR;

дослідити методи машинного навчання та поведінкової аналітики, що використовуються у системах класу NDR;

розробити технологічну модель автоматизованого реагування з інтеграцією Infinity NDR у SOC-середовище;

провести тестування технології у віртуальному середовищі та оцінити показники ефективності (MTTD, MTTR, Accuracy Rate);

Методи дослідження – аналіз наукової та технічної літератури у сфері Incident

Response, NDR і Zero Trust; порівняння сучасних систем виявлення та реагування (Infinity NDR, Darktrace, Vectra AI, Cisco Secure NDR); моделювання архітектури реагування; симуляція атак за методологією MITRE ATT&CK; експериментальне тестування у лабораторному середовищі; оцінювання ефективності за ключовими метриками (MTTD, MTTR, FPR); аналіз відповідності міжнародним стандартам (NIST SP 800-61, ISO/IEC 27035, ENISA IR).

Практичне значення одержаних результатів - Запропонована технологія реагування на інциденти на базі Infinity NDR забезпечує підвищення швидкості виявлення атак, зменшення часу реагування та зниження рівня помилкових спрацьовувань. Вона дозволяє створити єдине середовище керування безпекою в межах критичної інфраструктури, оптимізувати роботу SOC-команд і підвищити ефективність протидії сучасним кіберзагрозам. Результати дослідження можуть бути використані для побудови корпоративних систем моніторингу, державних центрів реагування на інциденти (CERT/CSIRT) та у навчальному процесі підготовки фахівців із кібербезпеки.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Визначення особливостей функціонування критичної інфраструктури та пов’язаних ризиків

Критична інфраструктура становить основу сучасного цифрового суспільства, адже саме від її стабільного функціонування залежить економічна, енергетична, транспортна, фінансова та інформаційна безпека держави. До її складу належать енергетичні системи, транспортні мережі, телекомунікації, банки, урядові сервіси, підприємства оборонно-промислового комплексу та заклади охорони здоров’я. Високий рівень цифровізації цих секторів — використання хмарних технологій, промислового Інтернету речей (IIoT), систем дистанційного керування та централізованих баз даних — створює нові можливості для розвитку, але одночасно формує нові кіберзагрози. Взаємопов’язаність галузей означає, що компрометація одного об’єкта може призвести до масштабних каскадних ефектів у суміжних секторах, що робить питання кіберзахисту критичної інфраструктури ключовим для національної безпеки [1].

Сучасна критична інфраструктура функціонує в умовах глибокої інтеграції операційних (OT) і інформаційних технологій (IT). Якщо раніше системи автоматизації промислових процесів (SCADA, DCS, PLC, RTU) були ізольованими від зовнішніх мереж, то сьогодні вони активно підключаються до корпоративних IT-середовищ і хмарних платформ для підвищення ефективності управління та моніторингу. Така інтеграція, з одного боку, забезпечує безпрецедентну прозорість і аналітичні можливості, а з іншого — розширює поверхню атак. Уразливості у протоколах промислового зв’язку (Modbus/TCP, DNP3, OPC UA, IEC-104), що

спочатку не передбачали механізмів шифрування та аутентифікації, створюють додаткові вектори для несанкціонованого доступу, підміни даних і дистанційного керування технологічними процесами [2].

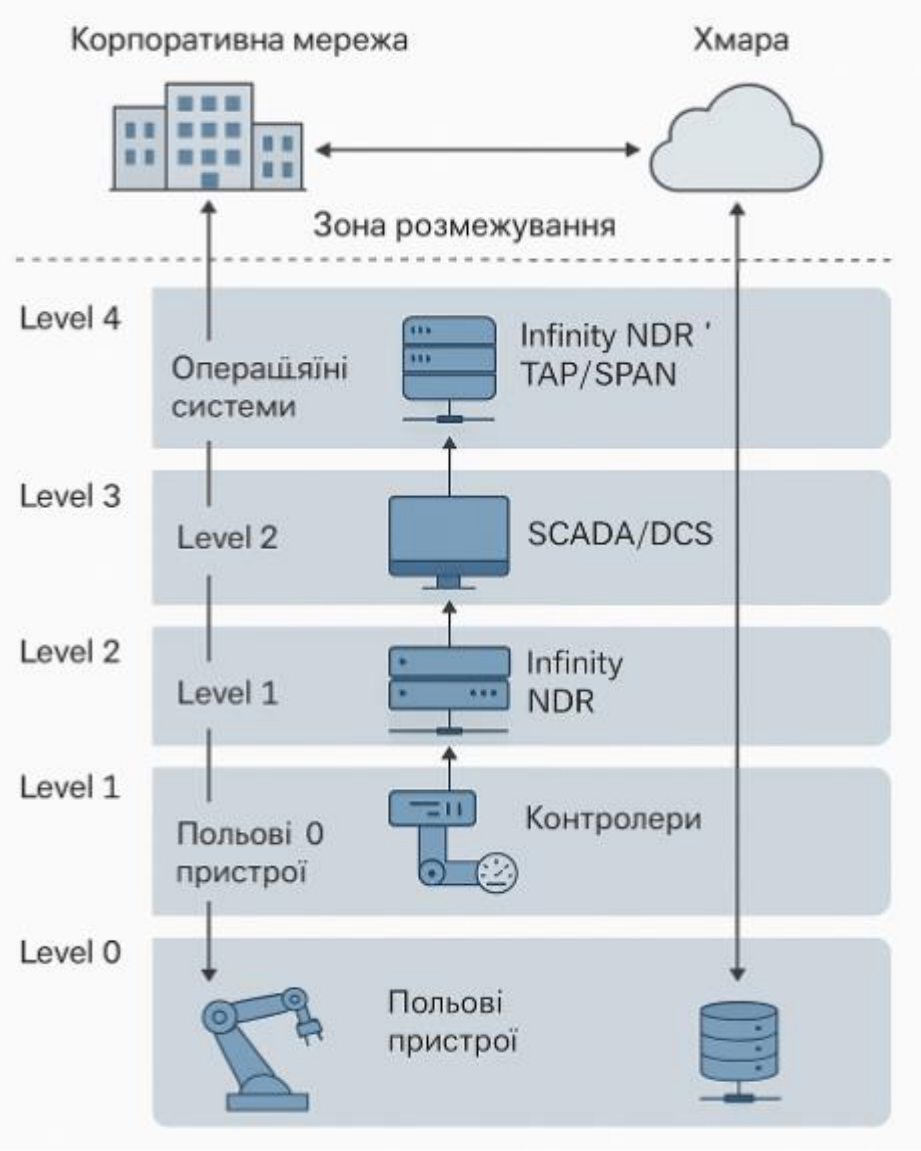

Рис 1.1 - Типова архітектура критичної інфраструктури та взаємозв'язок рівнів IT/OT згідно з моделлю Purdue

Серед специфічних особливостей функціонування критичної інфраструктури варто виокремити її надзвичайну чутливість до безперервності операцій. У більшості випадків зупинка навіть одного технологічного вузла може спричинити значні економічні збитки або небезпечні фізичні наслідки. Тому будь-які дії, спрямовані на

підвищення безпеки — впровадження оновлень, сканування чи моніторинг трафіку — повинні бути реалізовані таким чином, щоб не порушувати стабільність технологічних процесів. Це суттєво обмежує застосування активних засобів кіберзахисту, які здатні впливати на продуктивність систем. Саме тому у сфері промислової безпеки дедалі більшого поширення набувають технології класу Network Detection and Response (NDR), які забезпечують пасивний збір трафіку, аналіз поведінки користувачів і пристроїв, а також автоматизоване реагування на інциденти без втручання у критичні технологічні процеси [1].

Рішення Check Point Infinity NDR у цьому контексті посідає провідне місце серед інструментів моніторингу безпеки, оскільки поєднує механізми глибокої інспекції трафіку (DPI), машинного навчання та поведінкової аналітики. Infinity NDR дозволяє створювати централізовану систему виявлення аномалій, яка не потребує постійного втручання людини, забезпечує кореляцію подій з глобальними базами загроз (Threat Intelligence) і взаємодіє з SOC, SIEM та SOAR-платформами для реалізації повного циклу реагування на інциденти — від виявлення до ліквідації наслідків. У середовищах, де недопустиме активне втручання у виробничий процес, саме NDR стає основним джерелом спостережуваності за мережею та поведінкою об’єктів [2].

Функціонування критичної інфраструктури пов’язане з низкою технологічних ризиків. Одним із ключових є використання застарілих (legacy) систем, які не оновлювалися десятиліттями та не відповідають сучасним вимогам безпеки. Крім того, багато підприємств мають обмежену сегментацію між корпоративними та технологічними мережами, що створює умови для горизонтального переміщення зловмисників (lateral movement). Часто відсутні механізми мікросегментації, системи управління доступом базуються на єдиному домені Active Directory, а журнали подій мають недостатній рівень деталізації. У таких умовах компрометація одного

облікового запису або точки доступу може призвести до повного порушення безпеки виробничого контуру [3].

Надзвичайно важливим чинником ризику є людський фактор. Оператори, інженери, системні адміністратори та постачальники мають високий рівень привілеїв, що у випадку фішингових атак або соціотехнічного впливу може використовуватися зловмисниками для проникнення в систему. За даними ENISA, понад 80% кіберінцидентів у промислових системах мають пряме або опосередковане відношення до людських помилок. У цьому контексті особливу небезпеку становлять новітні соціотехнічні методи, зокрема deepfake-технології, які дають змогу імітувати голос чи обличчя посадової особи для отримання несанкціонованого доступу чи ініціювання критичних операцій. Таким чином, навіть добре підготовлений персонал може стати точкою входу атаки, якщо не застосовуються багатофакторна автентифікація, процедури верифікації запитів і регулярне навчання персоналу [5].

Рис 1.2 - Основні вектори кібератак на об’єкти критичної інфраструктури

Ще одним системним викликом є проблема спостережуваності мережевого трафіку. Традиційні системи IDS/IPS і SIEM, які орієнтовані на сигнатурний аналіз, не здатні ефективно обробляти великі обсяги зашифрованого трафіку, що сьогодні

складає понад 80% усіх мережевих з'єднань. Розшифрування TLS 1.3 або QUIC у промислових умовах часто є технічно складним або небезпечним, адже може впливати на затримки передачі даних. Системи класу Infinity NDR вирішують цю проблему за рахунок аналізу метаданих і поведінкових аномалій без розшифрування вмісту, що дозволяє зберігати продуктивність мережі й водночас своєчасно виявляти загрози [1].

Додаткову складність створює поєднання промислових мереж з корпоративними IT-середовищами, у яких зазвичай не передбачено належного рівня сегментації. Коли виробничий сегмент має прямий доступ до офісних систем, навіть звичайне зараження робочої станції може поширитися на технологічний контур. Такі інциденти, як NotPetya, Industroyer2, BlackEnergy та Sandworm, показали, що наслідки атак можуть бути не лише економічними, але й фізичними — відключення енергомереж, зупинка транспорту, дестабілізація банківських систем. У результаті відбувається перехід від традиційної парадигми «захисту периметра» до моделі Zero Trust, яка передбачає постійну верифікацію кожної взаємодії в мережі, незалежно від її джерела [3].

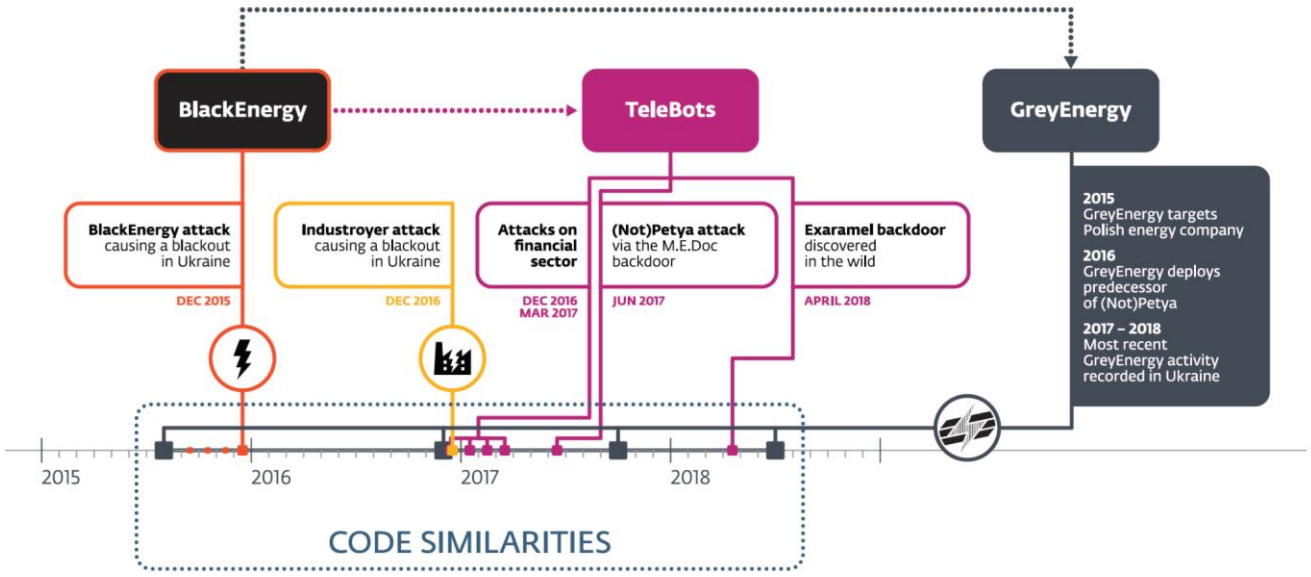

Рис 1.3 — Найвідоміші атаки на критичну інфраструктуру

З огляду на вищезазначене, для ефективного захисту критичної інфраструктури потрібен системний, багаторівневий підхід, який базується на принципах спостережуваності, адаптивності, автоматизації та відмовостійкості. Технології на кшталт Infinity NDR виступають центральним елементом цієї архітектури, забезпечуючи аналітичну основу для раннього виявлення, кореляції та пріоритезації подій. Завдяки поєднанню локальних ML-моделей і глобальної аналітики Threat Cloud вони дозволяють не лише виявляти загрози, а й прогнозувати їх розвиток, формувати рекомендації для реагування та інтегрувати ці дані в SOC-процеси.

Таким чином, особливості функціонування критичної інфраструктури — глибока інтеграція IT/OT, використання застарілих технологій, висока залежність від людського фактору, потреба у безперервності процесів і складна структура взаємозалежностей — формують унікальний профіль ризиків, який потребує інтелектуальних технологій моніторингу та реагування. Рішення Infinity NDR, завдяки своїй архітектурі, орієнтованій на поведінкову аналітику, машинне навчання та автоматизацію, забезпечує необхідний рівень технологічної зрілості для проактивного реагування на інциденти, мінімізації наслідків атак і підтримки безперервності функціонування критичних сервісів [4], [5].

1.2. Аналіз типових кіберзагроз для об’єктів критичної інфраструктури

Критична інфраструктура є стратегічною мішенню для кіберзлочинців, державних акторів і хактивістських угруповань через її високий вплив на економічну та національну стабільність. На відміну від звичайних корпоративних систем, де основною метою є крадіжка даних чи фінансові махінації, атаки на об’єкти критичної інфраструктури мають набагато серйозніші наслідки: фізичне руйнування обладнання, порушення технологічних процесів, відключення енергосистем або дестабілізацію життєво важливих сервісів. Такі інциденти не лише порушують

операційну діяльність, але й можуть створювати ефект доміно, впливаючи на суміжні сектори — фінанси, транспорт, логістику, медицину тощо [6].

Сучасні кіберзагрози для критичної інфраструктури характеризуються високим рівнем складності, тривалістю життєвого циклу атаки та орієнтацією на обхід традиційних систем захисту. Зловмисники активно використовують механізми багаторівневої розвідки, фішингові кампанії, інструменти соціотехніки, уразливості ланцюгів постачання та zero-day експлойти для отримання первинного доступу. Після закріплення в системі вони переходять до внутрішнього розвідування та поступового розширення привілеїв у мережі. На цьому етапі традиційні засоби виявлення часто не спрацьовують через відсутність підозрілих сигнатур або низький рівень видимості у промислових протоколах [7].

Особливу небезпеку становлять цільові атаки державного рівня (APT – Advanced Persistent Threats), які спрямовані на виведення з ладу стратегічних об’єктів. Такі кампанії, як правило, фінансуються урядовими структурами, мають чіткі цілі, багаторічну підготовку та застосовують комбінації кібер- і фізичних методів впливу. Відомими прикладами стали атаки *Stuxnet* (Іран, 2010), *BlackEnergy* (Україна, 2015), *Industroyer2* (2022) та *NotPetya* (2027), які довели, що кібератаки можуть безпосередньо впливати на енергетику, транспорт і урядові сервіси, спричиняючи реальні збої у виробничих процесах.
APT-групи, такі як Sandworm (GRU, Росія), Lazarus Group (КНДР), Charming Kitten (Іран), APT29 (РФ) та Volt Typhoon (Китай), спеціалізуються на тривалому прихованому перебуванні в системах управління, де вони можуть непомітно збирати розвіддані, маніпулювати даними або готуватися до майбутніх атак на енергетичні або телекомунікаційні об’єкти [8].

Вразливість об’єктів критичної інфраструктури часто обумовлена застарілим обладнанням (legacy systems), яке було розроблене задовго до появи сучасних загроз і не має вбудованих механізмів кіберзахисту. Такі системи не підтримують

шифрування, не ведуть детального журналювання подій і нерідко працюють під управлінням операційних систем, що більше не підтримуються виробником. Унаслідок цього зловмисники можуть використовувати навіть найпростіші вектори атак — наприклад, експлуатацію вразливостей SMB або RDP для проникнення у мережу. Особливу небезпеку становлять атаки на ланцюги постачання (Supply Chain Attacks), коли компрометується стороннє програмне забезпечення або хмарний сервіс, який використовується у середовищі КІ. Інцидент із *SolarWinds Orion* (2020) став яскравим прикладом того, як через оновлення програмного продукту можливо отримати доступ до сотень корпоративних і державних мереж одночасно [9].

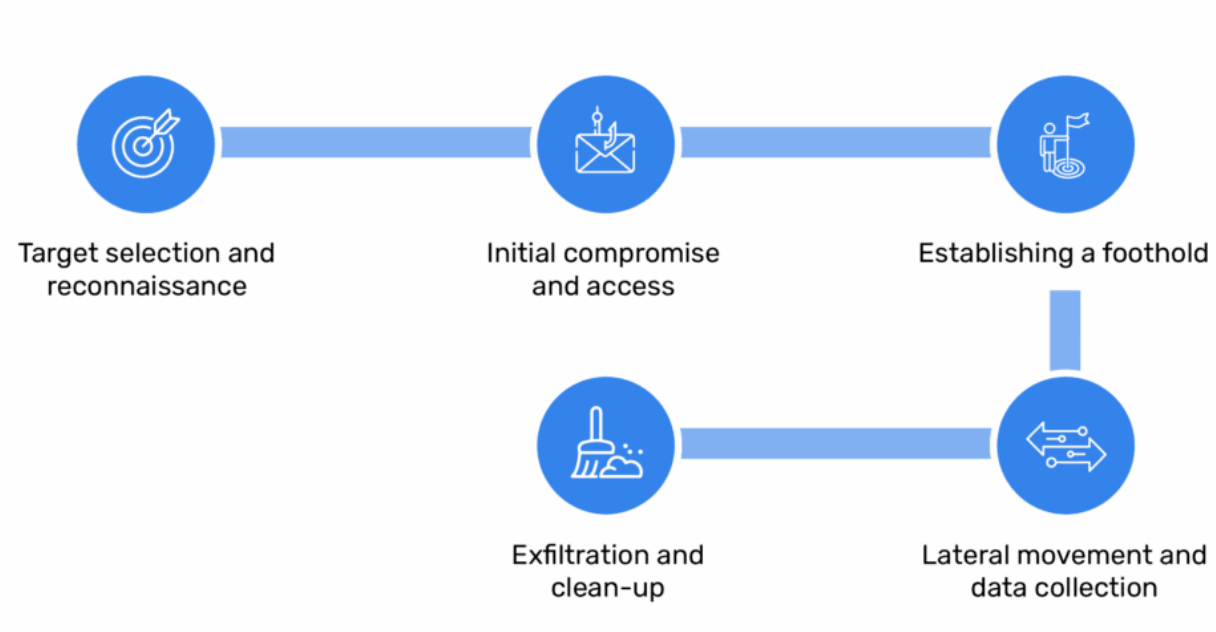

Рис 1.4 — Життєвий цикл APT-атаки

Ще однією критичною загрозою є ransomware-атаки нового покоління, спрямовані не лише на шифрування даних, а й на порушення фізичних процесів. Приклади, подібні до *Colonial Pipeline* (2021) або *JBS Meat Processing* (2022), демонструють, що шкідливе програмне забезпечення дедалі частіше націлене на виробничі системи. Такі атаки поєднують елементи вимагання (викрадення та публікація даних) і саботажу, створюючи тиск на організації не лише фінансово, а й

репутаційно. У результаті навіть тимчасове відключення виробничих потужностей може спричинити порушення логістичних ланцюгів і дефіцит товарів на ринку.

Суттєвим напрямом атак на критичну інфраструктуру є компрометація IoT- та IIoT-пристроїв. З поширенням датчиків і контролерів, підключених до мережі, зловмисники отримали можливість використовувати їх як плацдарм для DDoS-кампаній, збору телеметрії або ін'єкцій команд у SCADA-контури. Ботнети типу *Mirai* та *Mozi* продемонстрували, наскільки вразливою може бути периферія навіть добре захищеної мережі. Підміна або фальсифікація даних із датчиків у промислових середовищах може спричинити неправильні рішення автоматизованих систем управління, що в промислових умовах прирівнюється до фізичного саботажу [6].

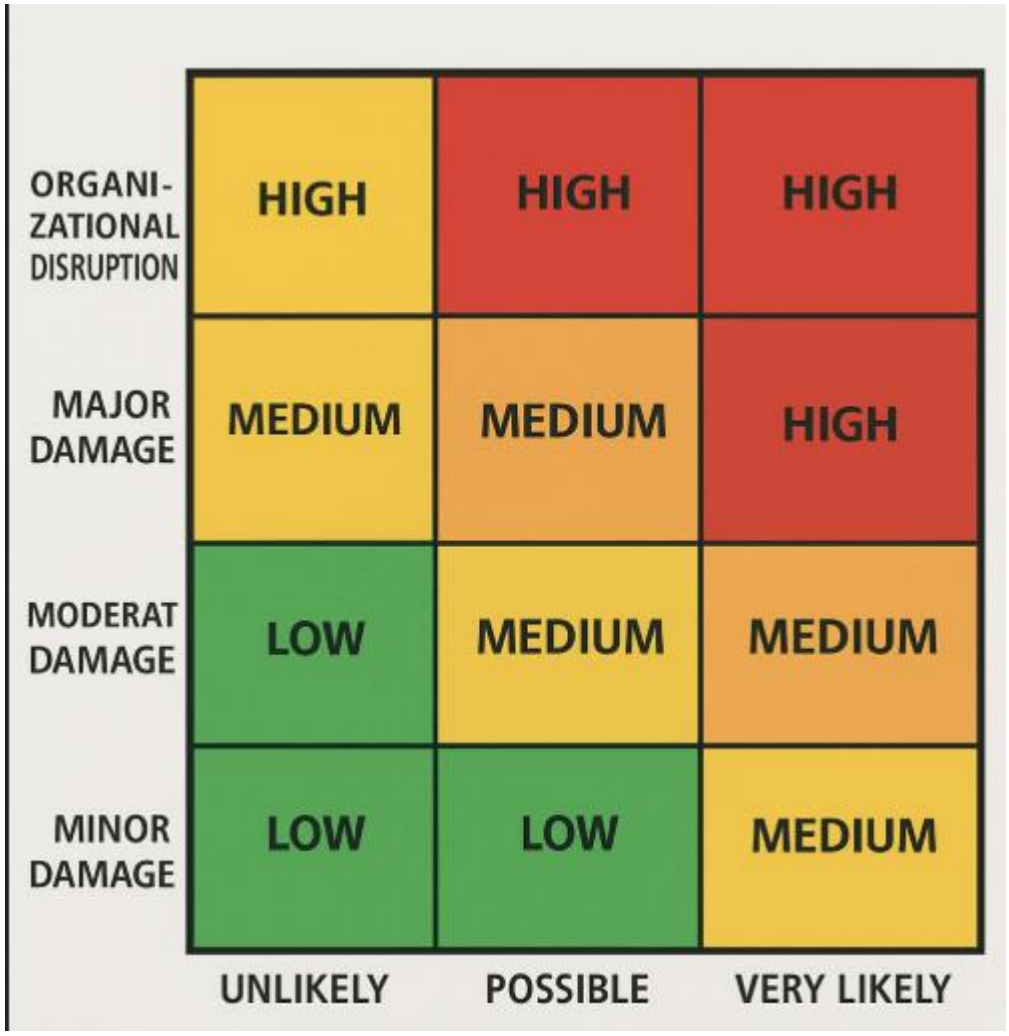

Рис 1.5 — Матриця ризиків критичної інфраструктури

Варто зазначити, що в останні роки спостерігається зміщення акценту атак від традиційних IT-компонентів до OT-середовищ. Це зумовлено тим, що технологічні процеси часто мають більш передбачувані патерни поведінки, а отже, атака може бути непомітною впродовж тривалого часу. Наприклад, зловмисники можуть поступово змінювати параметри керування температурою, тиском або частотою обертів обладнання, щоб викликати його деградацію без явних ознак зовнішнього впливу. Такі повільні, “низькошумні” атаки особливо складно виявити без технологій поведінкової аналітики, які застосовуються у сучасних системах NDR [8].

Таблиця 1.1.

Типові кіберзагрози для об’єктів критичної інфраструктури

Тип загрози	Опис	Можливі наслідки для КІ
APT-атаки	Тривале приховане перебування у системі, збір даних, підготовка саботажу	Порушення процесів управління, втрата контролю над SCADA
Атаки на промислові протоколи	Експлуатація незахищених Modbus, DNP3, OPC UA	Маніпуляція технологічними параметрами, аварійні зупинки
Supply Chain	Компрометація постачальників або оновлень ПЗ	Масове зараження корпоративних та OT-сегментів
Ransomware	Шифрування, вимагання, зупинка виробництва	Втрата даних, простої, репутаційні збитки

Тип загрози	Опис	Можливі наслідки для КІ
Insider Threat	Ненавмисні або зловмисні дії співробітників	Витік даних, саботаж, порушення регламентів
IIoT-компрометація	Захоплення мережевих сенсорів, ботнети	Втрата даних телеметрії, DDoS, підміна показників

Виявлення та класифікація таких загроз вимагає глибокого контекстного розуміння мережевих подій, чого не можуть забезпечити традиційні IDS-системи. Infinity NDR поєднує машинне навчання, аналіз поведінкових профілів (UEBA) і глобальні Threat Intelligence-потоки для формування адаптивної картини мережевої активності. Це дозволяє зменшити кількість фальшпозитивів, пріоритезувати інциденти за ступенем ризику та скоротити час між виявленням і реагуванням (MTTD і MTTR відповідно).

Таким чином, аналіз показує, що сучасні кіберзагрози для критичної інфраструктури мають високий рівень технологічної зрілості, часто маскуються під легітимні дії та вимагають інтелектуальних систем спостереження. Технології класу Infinity NDR дають змогу досягти необхідного рівня видимості, глибини аналізу й автоматизації, забезпечуючи ефективне реагування на інциденти навіть у гетерогенних середовищах, де взаємодіють IT і OT-системи [10].

1.3. Огляд сучасних підходів і засобів моніторингу безпеки промислових мереж

Моніторинг безпеки промислових мереж вирішує дві фундаментальні задачі: безперервне спостереження за станом OT-процесів без втручання у технологічний

контур та достатньо раннє виявлення відхилень, здатних порушити керування або безпеку. Відмінність промислових середовищ від класичних IT-сегментів полягає у жорстких вимогах до доступності, прогнозованості затримок і детермінованості протоколів, а також у довгому життєвому циклі обладнання, що унеможливлює агресивні активні перевірки. Це визначає домінування пасивних методів спостереження, опору на мережеві дзеркала (SPAN), оптичні розгалужувачі (TAP), брокери трафіку і високоточну часову синхронізацію (PTP/NTP) для коректної кореляції подій між рівнями Purdue. На архітектурному рівні моніторинг розгортають у точках перетину доменів — між L3 та L2 сегментами, на межі IT/OT та в OT-DMZ, а також у місцях концентрації технологічних протоколів: перед SCADA/Historian, на інженерних станціях та уздовж критичних маршрутів PLC↔IO.

Сучасні підходи поєднують три шари теле-метрії. Перший — глибокий аналіз пакетів (DPI) для промислових протоколів на кшталт Modbus/TCP, DNP3, IEC-60870-5-104, PROFINET, EtherNet/IP, OPC UA. Парсери на цьому шарі відстежують семантику команд, послідовність операцій і недопустимі комбінації станів: прикладом є індикація «write multiple registers» у позарегламентний час, підміна ідентифікаторів станцій або нетиповий циклічний опит певного RTU. Другий шар — потокова теле-метрія (NetFlow/IPFIX, sFlow), яка за значно меншої вартості фіксує шаблони взаємодій і дає підстави будувати граф взаємозв’язків між активами, виявляти рідкісні шляхи east-west і нові «розмови» між вузлами, яких не повинно існувати за технологічним регламентом. Третій — метадані зашифрованих сесій і сигнатури рукостискань (JA3/JA4, SNI, версії шифрів, розмір/ритм пакетів), що дозволяє робити висновки стосовно аномальної активності навіть у середовищі TLS 1.3 та QUIC без дешифрування контенту. Комбінація цих шарів забезпечує прийнятний баланс глибини й продуктивності та відповідає обмеженням OT-контурів, де будь-яке активне втручання небажане.

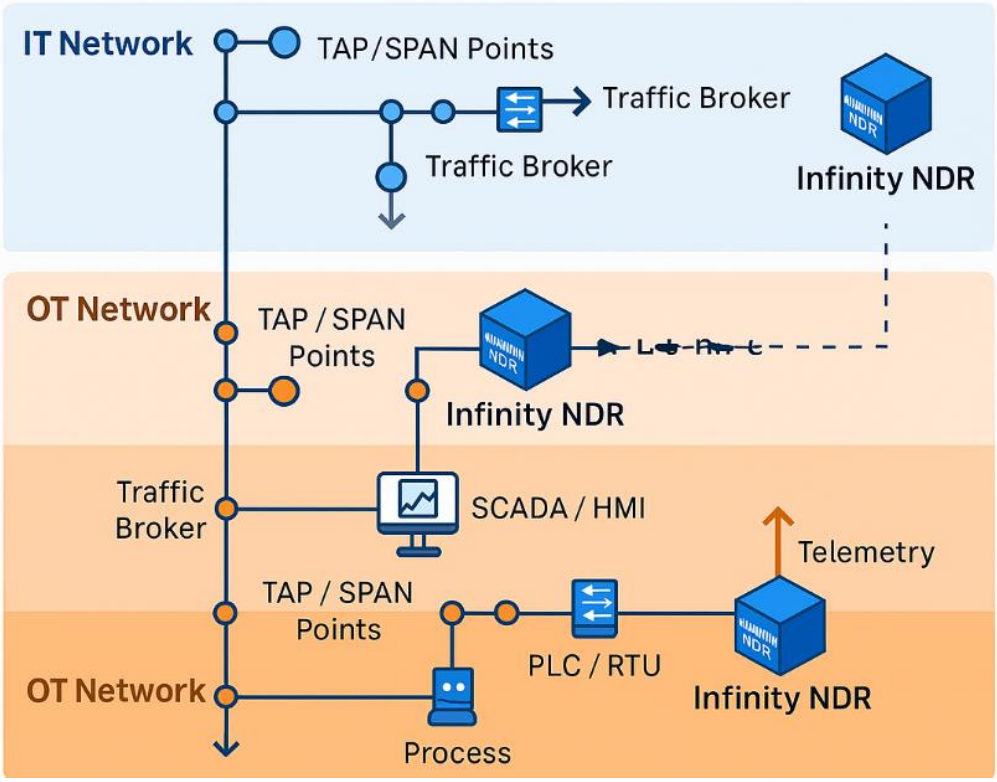

Рис 1.6 - Схема розміщення сенсорів моніторингу безпеки у багаторівневій архітектурі промислової мережі

На рівні аналітики сформувались два базові парадигми. Сигнатурна, що традиційно уособлюється IDS-рушіями (Suricata/Snort/Zeek policy scripts), працює добре для відомих шаблонів експлойтів, команд OT-протоколів і мережевих артефактів інструментарію зловмисників, але страждає від «сліпоти» до нових тактик і варіативності промислових сценаріїв. Поведінкова, яка опирається на машинне навчання, статистику та UEBA, навпаки моделює «норму» технологічної поведінки, відслідковує відхилення у часі й топології, вміє зіставляти OT-події з виробничим календарем, сменами, ритмами технологічних циклів та фізичними телеметріями. Саме поведінкова аналітика стала ядром класу NDR: вона дозволяє ловити «повільні» атаки з низьким шумом, латеральні переміщення, маніпуляції параметрами та підготовку саботажу, коли жодної відомої сигнатури ще не існує. Важливо, що якісний NDR поєднує обидва підходи: використовує сигнатури для швидких,

однозначних спрацьовувань і ML-моделі для контексту та пріоритезації, мінімізуючи хибні тривоги, які паралізують SOC у пікові години.

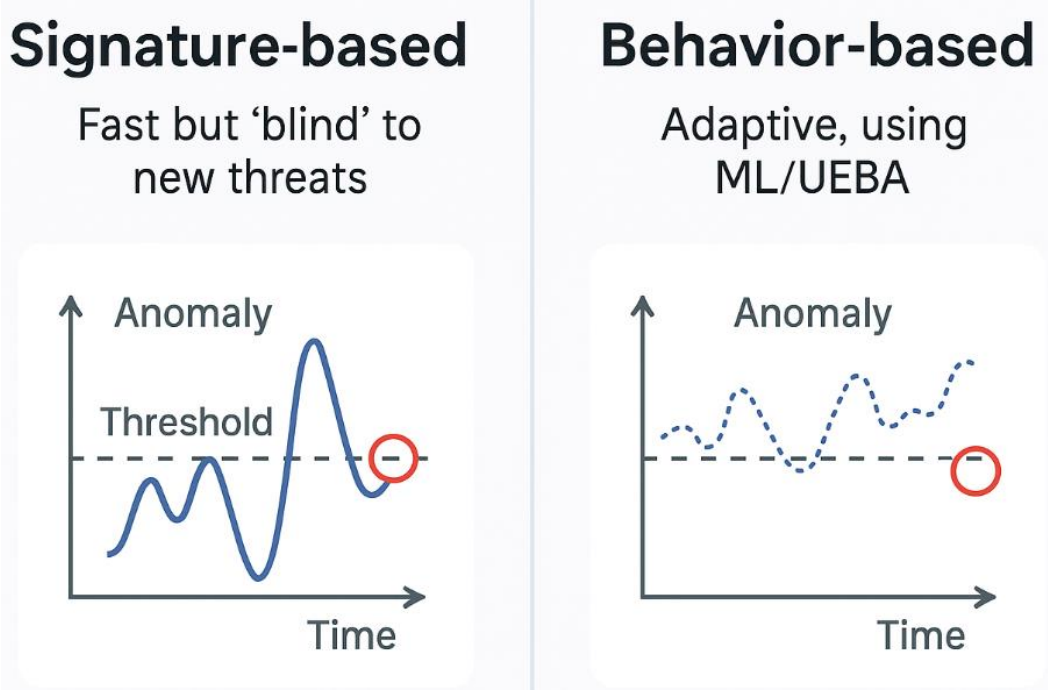

Рис 1.7 - Порівняння сигнатурного та поведінкового підходів

Ключовим компонентом сучасного моніторингу є відкриття активів (asset discovery) і побудова живої моделі мережі. У промислових мережах інвентаризація часто відстає від реальності, а сторонні підрядники приносять тимчасові вузли і сервісні ноутбуки. Пасивний знім мережі дозволяє автоматично класифікувати пристрої за відбитками стеків, OT-протоколами, MAC-префіксами вендорів і характером сесій; на цій основі формується «біла схема» дозволених взаємодій, а будь-який новий маршрут або нетиповий сервер OPC UA відразу фіксується як відхилення. Концепція «policy-as-code» для OT — коли дозволені потоки описані явно, під контролем зміни, з автоматизованим тестом — поступово стає стандартом: вона одночасно спрощує реагування (можна жорстко блокувати все поза політикою) і робить аудити відтворюваними.

Окремим напрямом стали технології моніторингу «з зашифрованого трафіку». Враховуючи еволюцію TLS 1.3, PFS та QUIC, розшифровувати магістральні потоки у

КІ часто неможливо ні технологічно, ні юридично. Натомість комбіновані моделі над метаданими (довжини/час, бьорсти, ентропія, JA3/JA4, TLS-розширення, SNI-аномалії, «рідкісні» комбінації шифрів для конкретної мережі) досягають практичної ефективності, якщо є якісна базова лінія саме «вашої» мережі. Додатково використовують кореляцію із зовнішнім Threat Intelligence: спрацьовування на свіжі C2-домені, нові сертифікати, TTP з публічних звітів і телеметрій, що суттєво підвищує шанс раннього виявлення підготовчих етапів APT-кампаній.

Вибір і розміщення точок спостереження визначають якість усієї системи. SPAN на комутаторах зручний, але має ризики втрати пакетів у піках і не гарантує часової точності; TAP/оптичні розгалужувачі дають детермінізм і незмінність копії трафіку, проте дорожчі і потребують планування. Для великих площадок доречно впроваджувати брокери пакетів із правилами розподілу (filter/aggregate/load-balance), апаратні карти з апаратним таймстемпінгом, а на сенсорах — ядровий байпас (DPDK/AF_XDP) або SmartNIC для утримання лінійної швидкості без втрат. Часова синхронізація по PTP/NTP критична для коректної реконструкції подій між SCADA, historian і сенсорами, і в ідеалі має підтверджуватись дисципліною журналювання з немодифікованими хеш-ланцюжками («доказовість» для форензики та регулятора).

Склади сховищ телеметрії зазвичай поділяють на «гарячу» і «холодну» зони. Гаряча зона — агреговані події, метадані потоків і короткі буфери PCAP для останніх хвилин/годин, що забезпечують контекст аналітику у SOC. Холодна — довші PCAP-кільця для вузьких сегментів, сегреговані по ризику, часто з дедуплікацією та WORM-політиками зберігання задля регуляторної відповідності. Це дозволяє не лише розслідувати інциденти ретроспективно, а й тренувати поведінкові моделі на реальних даних майданчика, що дає кращі результати, ніж «універсальні» моделі.

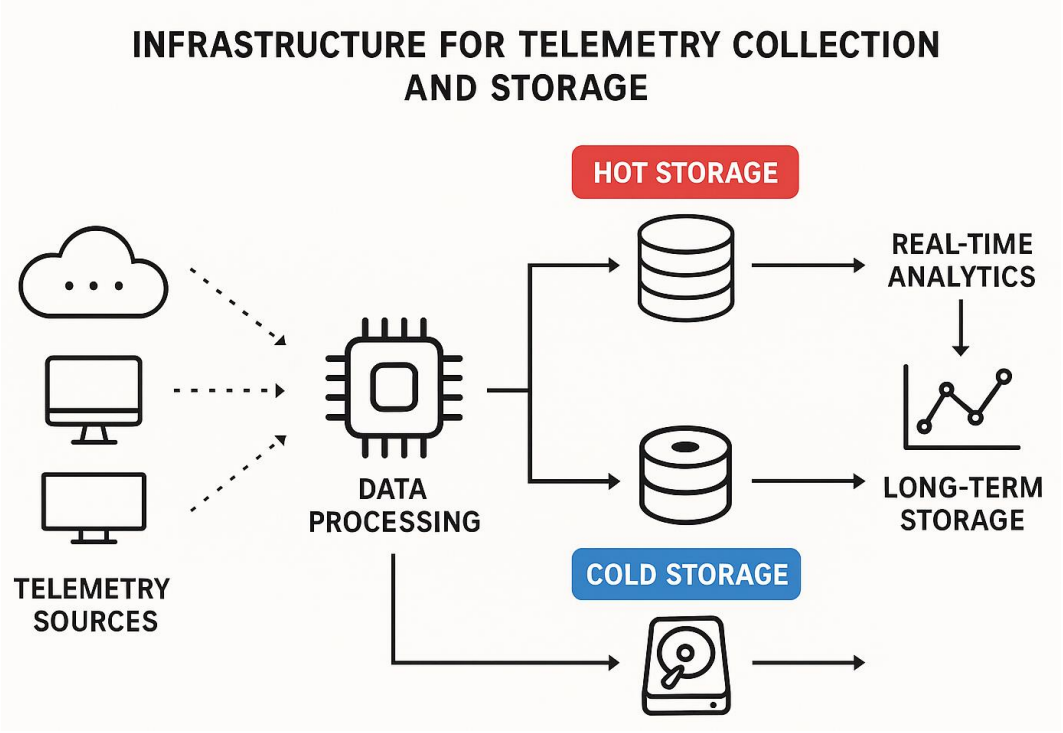

Рис 1.8 - Інфраструктура збору та зберігання телеметрії

Засоби моніторингу промислових мереж діляться на відкриті та комерційні. У відкритому світі домінують Zeek (із модулями ICS), Suricata/Snort із OT-правилами, Wireshark/Termshark для форензики, YARA/Sigma для нормалізації детекцій, а також спеціалізовані декодери для DNP3, IEC-104 та OPC UA. Комерційний сегмент представлено OT-орієнтованими NDR-рішеннями і платформами безпеки, серед яких Check Point Infinity NDR, Nozomi Networks, Claroty, Dragos, Cisco Cyber Vision, Tenable.ot, Forescout/SCADAfence і Microsoft Defender for IoT. Відмінності здебільшого у глибині OT-DPI, якості UEBA/ML, інтеграціях із SIEM/SOAR та готовності до великих розгортань (HA, горизонтальне масштабування, політика оновлень, покриття протоколів). Infinity NDR вирізняється потужною поведінковою аналітикою, інтеграцією з Infinity Portal/Threat Cloud, підтримкою сценаріїв автоматизованого реагування та зрілими конекторами у SIEM/SOAR, що важливо для злагодженого ланцюга «детект → тріаж → стримування → відновлення».

Глибокий моніторинг неможливий без прив’язки до процесів і людей. Ефективні програми включають картографування MITRE ATT&CK for ICS до подій у NDR, створення плейбуків реагування, навчання диспетчерів і інженерів читати сповіщення у виробничому контексті, регулярні «червоні/сині» вправи з використанням цифрових двійників або стендів. Усе це зменшує середній час на виявлення і локалізацію (MTTD/MTTI) і підвищує довіру до автоматизованих дій. Роль SIEM і SOAR — забезпечити єдине джерело правди, нормалізувати події з різних доменів (IT, OT, фізична безпека), запустити рунбуки: від ізоляції інженерної станції до тимчасових ACL на комутаторах, створення інциденту в ITSM та інформування зміни.

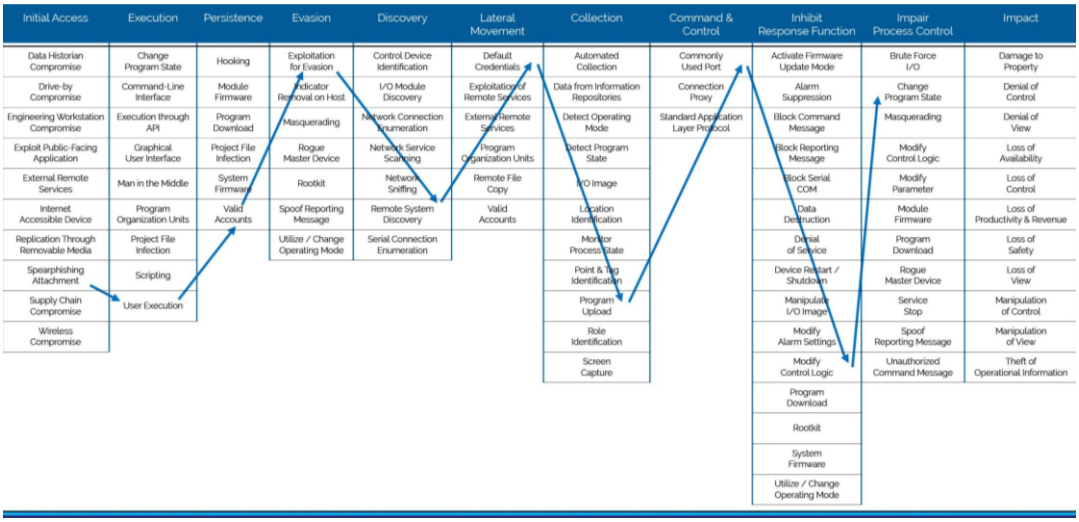

Рис 1.9 - MITRE ATT&CK for ICS

Складні сектори — енергетика, нафтогаз, транспорт — часто впроваджують додаткові технології: мережеву обманну інфраструктуру (deception) для відстеження розвідки зловмисника, контроль цілісності конфігурацій PLC та прошивок, відстеження змін у рецептах і логіці, контроль USB-медіа та виділені шлюзи віддаленого доступу підрядників з записом сесій. За можливості застосовують Zero Trust-принципи для доступів у OT: явна автентифікація, короткочасні дозволи,

контекстні політики, тунелі на рівні застосунків, а NDR слугує «сенсорним шаром», який перевіряє, що політики справді працюють у мережі, а не лише на папері.

Технічно грамотне впровадження моніторингу вимагає уваги до дрібниць: від якості оптичних TAP і відсутності асиметрії SPAN до правил балансування потоків на сенсори, налаштування jumbo-кадрів, планування пропускної здатності для виходу подій у SIEM і виділених каналів керування. Усе це повинно підкріплюватися вимірюваними показниками — часткою втрат пакетів, латентністю доставки подій, відсотком покриття протоколів, коефіцієнтом хибних спрацьовувань і, головне, динамікою MTTD/MTTR після впровадження.

У підсумку сучасний моніторинг безпеки промислових мереж — це поєднання пасивного, глибокого, контекстно-залежного спостереження з поведінковою аналітикою, формалізованими політиками потоків і автоматизованим реагуванням. Рішення класу Infinity NDR природно займає центральне місце у такій архітектурі: воно додає спостережуваність у зашифрованому та OT-специфічному трафіку, зшиває локальні дані із глобальною розвідкою загроз, мінімізує шум за рахунок UEBA та ML та інтегрує реакцію з інженерними процесами без ризику для технологічної безперервності. Саме така комбінація робить мережі критичної інфраструктури не лише видимими, а й керованими під час інцидентів, дозволяючи організаціям переходити від реактивної оборони до проактивного керування ризиком.

2 ЗАСТОСУВАННЯ МОЖЛИВОСТЕЙ INFINITY NDR ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Оцінка архітектури та функціоналу Infinity NDR як інструменту для промислових систем

У промислових мережах (ICS/SCADA) цінність технології Network Detection and Response полягає не лише у здатності «бачити» трафік, а у властивості коректно інтерпретувати технологічні події, пов’язувати їх з фізичними процесами та автоматизовано запускати стримувальні дії без ризику для безперервності виробництва. Check Point Infinity NDR побудовано саме як такий інтелектуальний шар спостережуваності й реагування: сенсори непомітно знімають телеметрію з TAP/SPAN, далі відбувається багаторівнева нормалізація й аналіз у хмарному аналітичному ядрі Infinity Portal/ThreatCloud AI, а у бік SOC та мережевих шлюзів прямують уже скорельовані інциденти з рекомендаціями дій [11]. На відміну від класичних IDS, які покладаються на статичні сигнатури, тут основна ставка зроблена на поведінкову аналітику (UEBA), кореляцію в просторі-часі та знання про OT-протоколи й бізнес-контекст об’єкта (лінії, зміни, регламентні вікна). Саме така комбінація дозволяє ловити «повільні» атаки, помилки конфігурацій і підготовку саботажу, коли сигнатур просто не існує або їх неможливо застосувати без великої кількості фальшпозитивів [14].

Архітектурно рішення складається з трьох тісно зчеплених площин. Сенсорна площина охоплює фізичні та віртуальні сенсори, що встановлюються у точках перетину доменів Purdue (OT-L2/L3, OT-DMZ, межа IT/OT) і працюють виключно пасивно, не впливаючи на каденс ПЛК і затримки шини управління [12]. Вони виконують первинний DPI для OT-протоколів (Modbus/TCP, DNP3, IEC-60870-5-104, S7Comm, PROFINET, EtherNet/IP, OPC UA), формують профілі сесій, екстрагують

метадані NetFlow/IPFIX, будують TLS-відбитки JA3/JA4 та збагачують потік локальними індикаторами компрометації з ThreatCloud [11]. Аналітична площина (Infinity Portal/ThreatCloud AI) застосовує багатомодельну обробку: сигнатурні правила (ядро Suricata), статистичні моделі, кластеризацію потоків і ізоляцію аномалій (Isolation Forest), а для користувачів/вузлів — UEBA-профілі з урахуванням робочих змін, «звичних» партнерів по взаємодії, типових періодів технологічних операцій [15]. Операційна/інтеграційна площина виводить сигнал у SOC: формує інциденти з мітками MITRE ATT&CK for ICS, запускає плейбуки в Infinity Playblocks та синхронізує журналювання з SIEM/SOAR (CEF, LEEF, JSON/Syslog, STIX/TAXII), що критично для відтворюваної форензики та відповідності IEC 62443 [13], [12].

Рис 2.1 — Функціонал рішення Infinity NDR

Ключ до якості виявлення — правильна побудова базової «норми». На старті сенсори збирають телеметрію протягом мінімум 2–3 виробничих тижнів, щоб моделі навчились ритму конкретної дільниці: які саме HMI говорять із якими PLC, які саме функціональні коди Modbus припустимі для цієї технології, у який час доби запускається історіан, а коли працює інженерна станція [11]. Після стабілізації профілю навіть невеликі відхилення (наприклад, одиничний «write multiple registers» у нічну зміну, яку історично характеризує лише «read coils») стають помітними та отримують підвищену пріоритезацію. На цьому етапі безпечна «глуха» робота з

зашифрованим трафіком (TLS 1.3/QUIC) досягається за рахунок аналізу метаданих (довжини, інтервали, SNI/ALPN, JA3/JA4, рідкісні комбінації шифрів для даної мережі) — себто Infinity NDR виявляє C2-канали й ексфільтрацію без розшифровки контенту, що важливо для продуктивності та комплаєнсу в КІ [14].

З погляду мережевої видимості система не обмежується «плоским списком» IP-адрес. Вона будує живий граф взаємодій між активами (PLC, RTU, HMI, SCADA-сервери, Historian, інженерні станції, шлюзи віддаленого доступу, операторські консолі, IT-активи) і проєктує цей граф на рівні Purdue та зони безпеки [11]. Для кожного вузла формується ризиковий індекс: ураховуються вразливості (CVE) з ThreatCloud, роль у процесі, ступінь «центральності» в комунікаціях і кількість останніх відхилень. Така карта ризиків — практичний інструмент планування сегментації/мікросегментації: аналітик бачить не лише «що спрацювало», а де саме політика дає збій і куди доцільно поставити тимчасові ACL або відгородити DMZ. Це відповідає вимогам IEC 62443-3-3 щодо контролю потоків і моніторингу безпеки на межах зон та каналів [12].

Рис 2.2 — Приклад оцінки ThreatCloud AI

Змістовне наповнення детекцій у промислових мережах принципово відрізняється від IT-сегмента. Якщо у звичайному офісі «аномалія» частіше означає нетипову DNS-активність або RDP-скан, то в OT аномалією є порушення

технологічної логіки. Infinity NDR спеціально парсить семантику OT-команд: для Modbus відстежує частки FC5/6/15/16 (write-операції) відносно FC3/4 (read), для DNP3 — operate поза виробничим вікном, для OPC UA — раптові зміни NodeId/Endpoint або ескалацію привілеїв сесії [11]. Доповнюється це UEBA-шаром: нетипова поява «інженера» у нічну зміну з приходу через VPN, з підмережі, невідомої для OT-домену, і з послідовністю команд, яка у цій лінії історично не зустрічалась. Сукупність таких фактів помічається як композитний інцидент з мапуванням на ATT&CK for ICS (Initial Access → Lateral Movement → Inhibit Response Function → Impact) і з вагомим «confidence score», якого бракує окремим сигнатурним рушіям [13], [15].

У зашифрованих доменах (TLS/QUIC) Infinity NDR показує практично важливу ефективність без інвазивного SSL-інспектування: тренд-аналіз довжин/ритмів, стабільності JA3/JA4, порівняння з «дистильованою нормою» конкретної зміни/лінії/сезону, а також кореляція з ThreatCloud (нові домени-«примари», незвичні сертифікати, рідкісні ALPN для конкретної промислової площадки) дають змогу піднімати «ранні» тривоги на стадії розвідки і закріплення APT [11], [14]. Це прямо впливає на MTTD і, відповідно, на очікуваний річний збиток у моделях FAIR, бо в КІ час — це не лише гроші, а й безпека людей і довкілля.

Окремої уваги потребує форензика. Infinity NDR зберігає багату часову розмітку метаданих і (за потреби) короткі PCAP-буфери з найбільш ризикових сегментів; у поєднанні з SIEM журналами це дозволяє відновити «ланцюг рішень» інженера/оператора, тимчасові коридори взаємодій та реконструювати каскад інциденту. Ретроспективний пошук за IoC, IP, URL, JA3/JA4, UserID, OT-атрибутами в Infinity ThreatHunt пришвидшує аналіз «через час», що критично, коли зловмисник діяв «низькошумно» місяцями [11]. Підхід відповідає меті IEC 62443 – забезпечити відтворюваність подій і доказовість для внутрішніх та зовнішніх аудитів [12].

Реагування — ще одна сильна сторона архітектури. Будучи частиною Infinity Architecture, NDR може або ініціювати SOAR-плейбуки через Infinity Playblocks, або

віддавати прямі команди мережевим шлюзам Quantum: ізоляція MAC/портів, тимчасові ACL, блокування «чорного» SNI/JA3, відключення тунелю підрядника [11]. Це особливо важливо для OT, де «грубі» дії неприпустимі: автоматизований плейбук зазвичай працює у «м'якому» режимі (обмеження лише того потоку, який вийшов за політику), а ескалація до «жорсткої ізоляції» відбувається з участю диспетчера, що відповідає виробничим регламентам (вимога «four eyes»). Практика market-guide показує, що саме поєднання поведінкової детекції з «безпечним» стримуванням стає відмітною рисою зрілих NDR-рішень у сегменті KI [14].

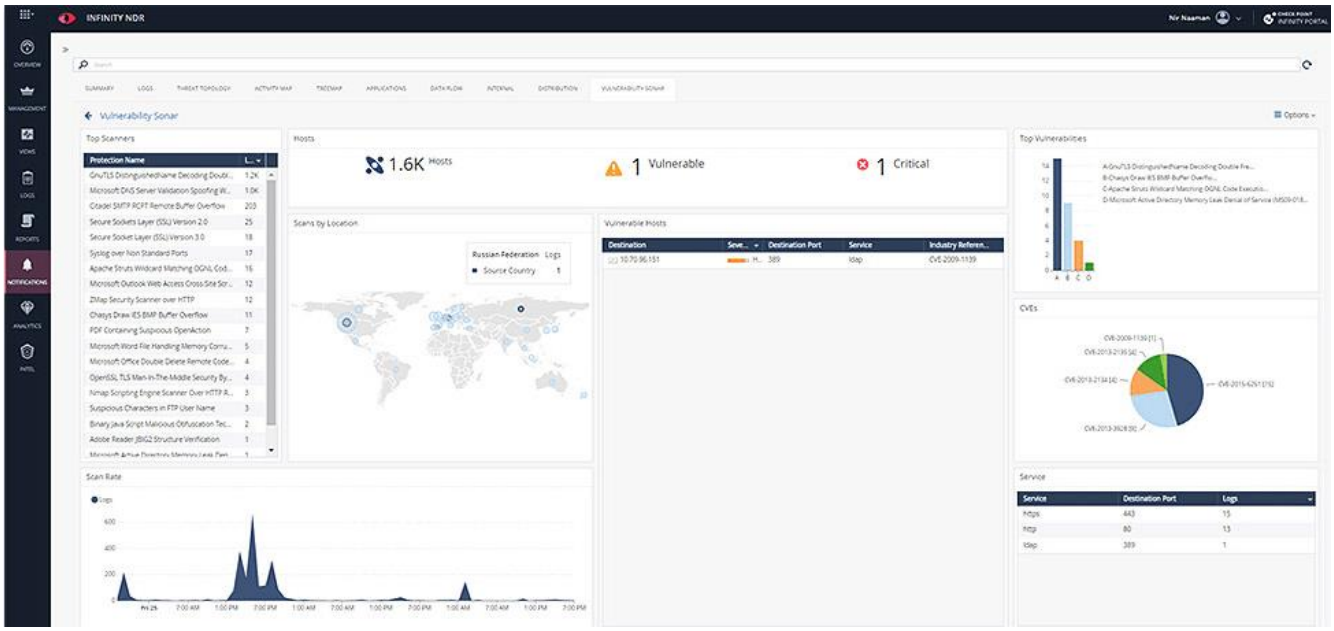

Рис 2.3 — Робоча панель аналітика Infinity NDR

З погляду розгортання, правильна топологія сенсорів і брокерів трафіку — питання №1. На високо-навантажених ділянках доцільні оптичні TAP з апаратним таймстемпінгом; SPAN застосовують як допоміжне дзеркало, усвідомлюючи ризики втрат у пік. Для консолідації — packet broker із правилами фільтрації/агрегації/балансування, щоб розкладати потоки на сенсори без «гарячих точок». На самих сенсорах — ядрові драйвери з нуль-копію (DPDK/AF_XDP) або SmartNIC, щоб утримувати 10/40 Гбіт/с без падінь; часову консистентність забезпечують PTP/NTP по всій площадці. Гаряче сховище зберігає метадані/події

(години/доби), холодне — вибіркові PCAP/телеметрії з WORM-політиками (тижні/місяці), чим досягається баланс між витратами, продуктивністю і форензичною повнотою [11], [13].

Інтеграція з зовнішніми системами вже «із коробки»: Splunk, QRadar, ArcSight, Elastic Security, Microsoft Sentinel, Wazuh — через CEF/LEEF/JSON Syslog, STIX/TAXII для обміну з TI-платформами; у OT-ландшафті — конектори до Claroty, Nozomi, Tenable.ot для зведення інвентаризації/уразливостей в OT-SIEM [11], [16]. У практиці SOC це дає одну «картину правди»: SIEM бере на себе нормалізацію, зберігання й крос-доменної кореляції, SOAR — життєвий цикл інцидентів, NDR — високоточні детекції та контекст. Рекомендації MITRE ICS радять явне мапування детекцій на тактики/техніки (T0888, T0838, T0872 тощо), що Infinity NDR і робить у портал-дашбордах [13].

Питання масштабованості та надійності вирішуються через горизонтальне масштабування сенсорів, HA-кластер аналітики та рознесення контрольної площини у Infinity Cloud з опцією приватного інстансу для вимог із підвищеною конфіденційністю (держсектор/критичні оператори) [11], [14]. На багатосайтових інфраструктурах сенсори агрегують події локально та відправляють стислу аналітику в центральний портал, що мінімізує вимоги до каналу зв’язку і виключає передачу «сирого» PCAP за периметр. Такий підхід узгоджується з практикою в ICS-індустрії, описаною в прикладних оглядах IEEE/Elsevier щодо деплойменту NDR в OT [12], [15].

З практичного боку корисно мислити сценаріями. Наприклад, supply-chain компрометація інженерної станції: у «тихий» час доби сенсор фіксує нову QUIC-сесію на рідкісний SNI, JA4-відбиток не співпадає з профілем цієї станції; через хвилини з’являються Modbus FC16 на PLC, що історично виконуються лише в денну зміну; паралельно SIEM реєструє аутентифікацію користувача «engineer01» із нової IP-пули VPN. Infinity NDR формує композитну подію з ATT&CK-мітками *Initial Access* → *Execution* → *Lateral Movement* → *Impact*, UX-картинка показує стрілки «інженерна

станція → PLC», ризик-скор високий; Playblocks піднімає «soft-containment»: ACL на комутаторі блокує лише Modbus-write від цієї станції, SOC отримує «high-prio» алерт, черга на розслідування — створена. Для аудиту зберігається зв'язаний «ланцюжок» метаданих; у випадку помилковості рішення обмеження легко скасовуються. Це — зрілий приклад безпечної автоматизації у КІ, якої домагаються інженерні підрозділи [11], [14].

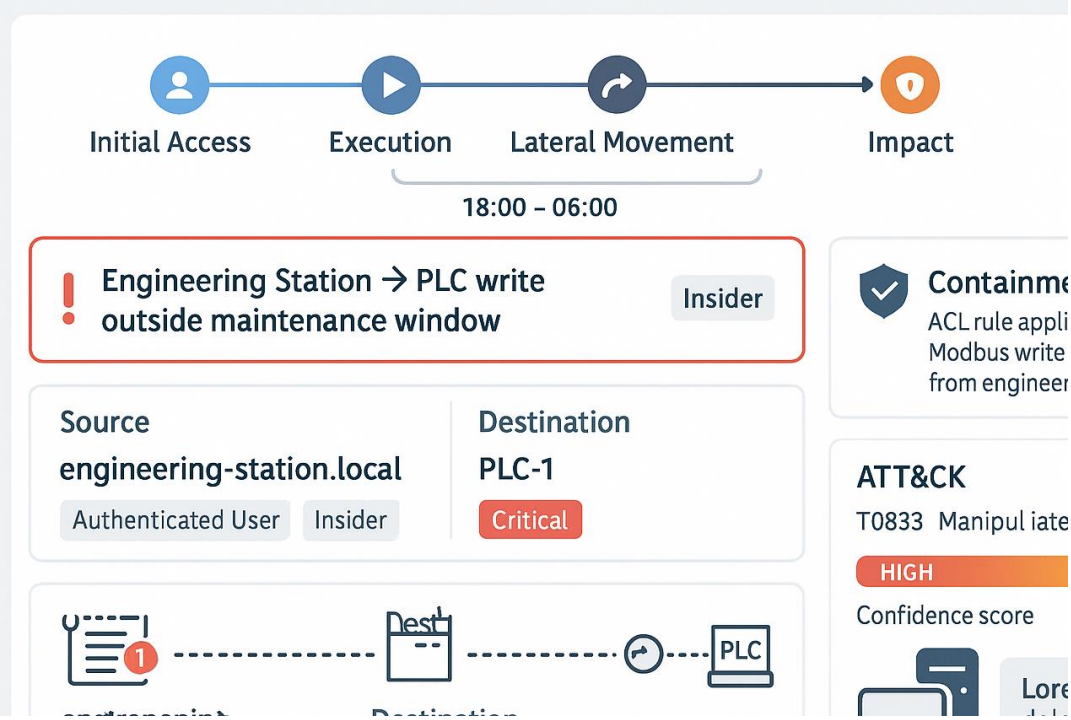

Рис 2.4 — Приклад аналітики події

Оцінюючи переваги Infinity NDR проти інших OT-орієнтованих NDR (Dragos, Nozomi, Claroty), важливо те, що він органічно вбудований у єдину платформу Infinity: спільний ThreatCloud, прямі дії на Quantum Gateways, консистентні політики, єдиний портал, XDR/XPR-аналітика. Це зменшує час інтеграції та підвищує узгодженість дій під час інциденту. Згідно з Gartner Market Guide, саме комплексність екосистеми, «behavior-first» детекції та оркестрація реагування визначають успішні впровадження NDR у КІ у 2024–2025 рр. [14]. Водночас треба зважати на виклики впровадження: якість дзеркал (TAP/SPAN), дисципліна часу (PTP/NTP), достатній період «навчання» моделей та узгодженість форматів подій із SIEM. Практичні рекомендації IEEE

підтверджують: ці «дрібниці» визначають різницю між «галочкою» і реальним зниженням MTTD/MTTR [15].

Загалом, Infinity NDR надає промисловим операторам саме ті механізми, яких бракує традиційним засобам: пасивну глибоку видимість OT-трафіку, поведінкову детекцію у зашифрованих каналах, живу карту ризиків, ретроспективну форензику, інтегроване й безпечне стримування. У підсумку організація отримує не просто «ще один сенсор», а керований процес: від раннього сповіщення до контрольованого реагування, документування й уроків, узгоджених із вимогами IEC 62443 і практикою MITRE ATT&CK for ICS [12], [13]. Саме це і є ознакою зрілої технологічної основи для динамічного управління ризиком у середовищах критичної інфраструктури.

2.2. Інтеграція потоків мережевого трафіку та побудова аналітичних моделей у Infinity NDR

Інтеграція потоків мережевого трафіку в системі Check Point Infinity NDR є одним із ключових процесів, що забезпечує повну видимість усіх комунікацій у промислових і корпоративних мережах та формує основу для поведінкової аналітики, машинного навчання й автоматизованого реагування. На відміну від класичних систем моніторингу, Infinity NDR не обмежується збором базових мережевих метаданих — його архітектура побудована за принципом «data-first», тобто основна увага приділяється не лише фіксації трафіку, але й його семантичному аналізу, нормалізації та кореляції з контекстом середовища. Це дозволяє створити єдину аналітичну екосистему, у якій дані перетворюються на знання, а знання — на дію[16].

На першому етапі інтеграції Infinity NDR формує єдиний телеметричний шар, який охоплює всі потоки даних, що циркулюють між IT і OT доменами. Для цього система використовує кілька типів джерел: дзеркала мережевих портів (TAP/SPAN), колектори NetFlow та IPFIX, журнали з мережевих екранів, проксі-серверів, DNS-

рекурсорів і навіть дані з хмарних API сервісів. Ці джерела формують спільний потік телеметрії, який збирається сенсорами Infinity NDR і передається в Infinity Cloud Analytics Layer. Кожен сенсор обробляє вхідні пакети локально, виконує розпізнавання протоколів, фільтрацію шуму, а потім відправляє зведену інформацію у форматі flow-записів. Таким чином, у центральній аналітичній системі формується уніфікований потік даних, який містить атрибути з рівнів 2–7 моделі OSI — MAC-адреси, IP, порти, довжини пакетів, час існування сесії, прикладні протоколи, JA3/JA4-відбитки TLS, ідентифікатори користувачів і хостів, а також поведінкові ознаки, отримані з аналізу часових інтервалів та ентропії трафіку.

Особливість цього процесу полягає в тому, що Infinity NDR не просто накопичує трафік, а виконує його адаптивну нормалізацію. Завдяки вбудованому механізму pre-classification engine система розпізнає специфічні промислові протоколи (Modbus/TCP, PROFINET, DNP3, OPC UA, IEC-60870-5-104, S7Comm) і виконує глибоку інспекцію пакетів без втручання у технологічні процеси. При цьому Infinity NDR розуміє контекст: що PLC виконує цикл опитування, що SCADA-сервер формує запити читання, а що інженерна станція передає команду зміни конфігурації. Усе це дозволяє системі не лише відслідковувати транспортні характеристики, а й робити висновки про поведінку технологічних процесів.

У той час як класичні IDS системи здебільшого працюють із сирими даними та сигнатурами, Infinity NDR формує структуровані Flow Records, які стають основою для аналітичних моделей. Кожен flow-запис доповнюється додатковими полями — середнім інтервалом між пакетами, коефіцієнтом повторюваності сесій, статистикою ентропії доменних імен, співвідношенням напрямків трафіку, частотою появи «write»-команд у промислових протоколах. Ці ознаки далі використовуються для навчання алгоритмів машинного навчання, які будують поведінкові профілі для кожного вузла мережі, користувача чи сегменту OT.

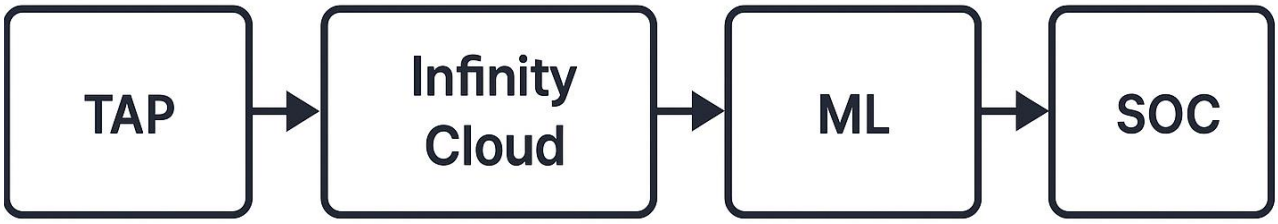

Рис 2.5 - Конвеєр обробки трафіку в Infinity NDR

На етапі аналітичної обробки Infinity NDR перетворює зібрані дані на багатовимірні вектори ознак, що дозволяє моделі розпізнавати навіть мінімальні відхилення від звичної поведінки. Коли система вперше запускається, вона перебуває у фазі навчання — протягом декількох тижнів сенсори збирають базову статистику та формують еталонні профілі поведінки. Це «поведінкове відбиття» визначає нормальні зв’язки між вузлами, часові закономірності комунікацій, типові шаблони протоколів, середні розміри пакетів і допустимі відхилення. Після завершення навчання навіть невеликі відмінності — наприклад, раптове зростання кількості write-команд Modbus, які зазвичай зустрічаються лише під час технічного обслуговування, або нетипова активність користувача у нічний час — викликають тригер поведінкової моделі.

На рівні аналітики Infinity NDR поєднує кілька типів моделей: статистичні, машинного навчання та глибинні нейронні. У промислових мережах, де більшість комунікацій є стабільними, добре працюють методи Isolation Forest та One-Class SVM, які виділяють аномалії на основі малоймовірних комбінацій ознак. Для складних сценаріїв, де зв’язки між вузлами багатовимірні, застосовуються глибинні автокодери (autoencoders), які навчаються відновлювати нормальні шаблони поведінки та сигналізують про відхилення, якщо похибка реконструкції виходить за межі встановленого порогу. Це дозволяє виявляти атаки низької інтенсивності — наприклад, поступове внесення змін у конфігурацію контролера чи розгортання бекдорів через промислові шлюзи.

Додатковий рівень аналітики формується на основі графового підходу. Infinity NDR створює топологічний граф мережевих зв’язків, де кожен вузол — це актив (PLC, HMI, сервер, шлюз, робоча станція), а ребра між ними — це сесії зв’язку. За допомогою Graph Neural Networks (GNN) система виявляє нові або нетипові з’єднання, аналізує ступінь центральності вузлів і формує індекс ризику. Якщо, наприклад, робоча станція, яка раніше комунікувала лише з SCADA, починає спілкуватися з PLC іншої лінії, графова модель фіксує цю подію як потенційне бокове переміщення (lateral movement).

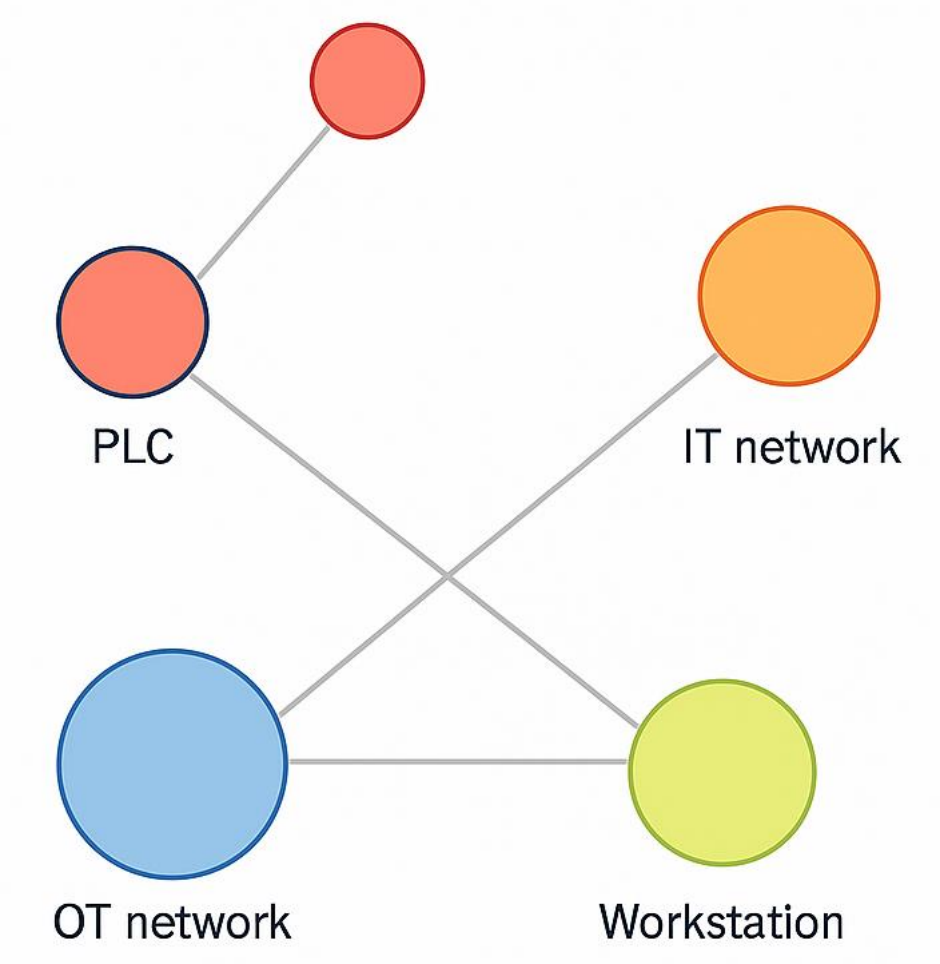

Рис 2.6 - Топологічний граф зв’язків OT/IT-сегментів із виділенням підозрілих вузлів

Розпізнані аномалії потім автоматично корелюються з MITRE ATT&CK for ICS. Це дозволяє не лише ідентифікувати технічну природу відхилення, а й зрозуміти, у якому етапі життєвого циклу атаки воно відбувається — розвідка, експлуатація вразливості, переміщення всередині мережі чи вплив на процес. Так, часті зміни firmware PLC без запланованого обслуговування класифікуються як T0838: Loss of Safety, а незвичні write-команди з інженерної станції — як T0888: Modification of Control Logic [11].

На практиці інтеграція потоків трафіку дозволяє Infinity NDR формувати комплексні композитні події, що об’єднують кілька ознак в один інцидент. Наприклад, система фіксує збільшення обсягу трафіку між IT і OT-сегментами, одночасно спостерігає появу незнайомих JA3-відбитків TLS і аномальну кількість DNS-запитів до зовнішніх доменів. Кожен із цих факторів окремо не є критичним, але у сукупності формує підозрілий патерн, який вказує на можливе розгортання C2-каналу або ексфільтрацію даних.

Після виявлення аномалії Infinity NDR передає зведений інцидент до Infinity Portal, де він відображається у вигляді інтерактивного дашборда. SOC-аналітик може побачити часову лінію події, карту комунікацій між вузлами, heatmap ризиків і логіку спрацьовування моделей. Система підтримує Explainable AI (XAI), тому кожен інцидент супроводжується поясненням: які ознаки спричинили спрацьовування, які історичні патерни були порушені, та наскільки статистично значущим є відхилення. Це суттєво знижує навантаження на аналітиків і підвищує довіру до рішень штучного інтелекту [15].

З технічного боку Infinity NDR може працювати як у реальному часі, так і в режимі ретроспективного аналізу. Гаряче сховище (Hot Storage) використовується для швидкого пошуку та аналізу поточних потоків, тоді як холодне сховище (Cold Storage) зберігає історичну телеметрію, що дозволяє відновити хронологію подій навіть через

кілька тижнів. Це особливо важливо при розслідуванні тривалих APT-кампаній, які розгортаються поступово і можуть бути непомітними на початкових етапах.

Таким чином, Infinity NDR забезпечує повний цикл обробки мережевого трафіку — від збору та агрегації до аналітичного моделювання, візуалізації та автоматизованого реагування. Його аналітичні моделі поєднують статистичний аналіз, машинне навчання та графову кореляцію, що дозволяє не лише фіксувати події, а й розуміти причинно-наслідкові зв'язки між ними. Такий підхід робить систему здатною виявляти навіть невідомі загрози, які не мають сигнатур, і забезпечує безперервний моніторинг складних промислових середовищ у режимі реального часу.

2.3. Розробка політик та правил виявлення інцидентів у Infinity NDR

Процес розробки політик і правил виявлення інцидентів у системі Check Point Infinity NDR є ключовим етапом формування ефективної архітектури кіберзахисту промислових середовищ, адже саме політики визначають, які події система класифікує як загрози, яким чином вона їх корелює, аналізує та на які дії реагує автоматично чи через операторів SOC. На відміну від класичних систем IDS або IPS, які спираються виключно на сигнатурний підхід, Infinity NDR використовує поведінкові моделі, машинне навчання, статистичний аналіз і багатошарову кореляцію подій, що дає змогу виявляти як відомі, так і нові, раніше не описані атаки .

Основна архітектурна концепція формування політик у Infinity NDR базується на трьох взаємопов'язаних рівнях аналітики — контекстному, поведінковому та кореляційному. Контекстний рівень забезпечує ідентифікацію активів, їхньої ролі у мережі, взаємозв'язків, протоколів і типів комунікацій. Поведінковий рівень відповідає за побудову моделей «нормальної поведінки» (baselining) для користувачів і пристроїв, відстежуючи часові закономірності, інтенсивність трафіку, взаємодії між сегментами OT/IT. Нарешті, кореляційний рівень дозволяє об'єднувати окремі події у

складні логічні ланцюжки, формуючи композитні інциденти з контекстом і хронологічною послідовністю.

Побудова політик починається з процесу інвентаризації активів. Infinity NDR автоматично виявляє всі вузли, підключені до мережі, визначає їхні типи — PLC, HMI, SCADA, інженерні станції, сервери історизації, шлюзи, тощо — і формує класифікаційні профілі. Ці профілі базуються на детекції промислових протоколів (Modbus, DNP3, IEC 104, OPC UA), MAC-вендорах, часових шаблонах комунікацій і метаданих сесій. На цьому етапі система створює початкову політику видимості, що служить основою для побудови більш складних аналітичних правил.

Далі система переходить до формування поведінкових політик, що ґрунтуються на машинному навчанні. Infinity NDR навчає моделі для кожного активу, створюючи його базовий профіль активності. Наприклад, система виявляє, що інженерна станція зазвичай використовує Modbus TCP лише у робочі години, а PLC реагує лише на команди з певної підмережі. Якщо зафіксовано спробу запису даних у PLC поза графіком технічного обслуговування, або відмінність у структурі пакету, політика спрацьовує, позначаючи подію як потенційну атаку — наприклад, *Unauthorized Command Message (MITRE ATT&CK T0855).*

Окремий клас політик у Infinity NDR — кореляційні політики, які поєднують кілька подій у єдину композитну структуру. Так, коли система фіксує підключення інженерної станції до PLC, зміну конфігурації контролера, а потім передачу даних на зовнішній IP через HTTPS, це розцінюється як багаторівневий інцидент типу *Insider Modification with Data Exfiltration*. У таких випадках Infinity NDR автоматично підвищує критичність інциденту, оскільки бачить не окремі факти, а послідовність дій, характерних для цілеспрямованих атак (APT).

Infinity NDR підтримує різні механізми реакції на події. Система може просто створити алерт, автоматично ізолювати підозрілий вузол, заблокувати сесію на шлюзі, додати правило в Check Point Quantum Firewall або передати контекст у зовнішню

систему реагування — наприклад, у SOAR-платформи (Cortex XSOAR, Splunk Phantom, IBM Resilient). Таким чином формується повноцінний цикл реагування (Detect → Analyze → Contain → Report → Recover), що дозволяє скоротити час від виявлення до нейтралізації загрози до кількох хвилин.

Система Infinity NDR побудована з урахуванням постійного самонавчання політик. Її модуль Continuous Policy Optimization проводить аналіз історії спрацювань, фіксує кількість хибнопозитивних інцидентів і пропонує автоматичні зміни до порогових параметрів. Наприклад, якщо правило «Abnormal SMB Traffic» часто спрацьовує на резервні копії, система пропонує додати винятки для певних хостів або змінити часовий інтервал. Так забезпечується самокорекція без участі адміністратора, що є суттєвою перевагою для середовищ OT, де стабільність системи має критичне значення.

Для галузей критичної інфраструктури (енергетика, транспорт, хімічне виробництво, нафтогазова промисловість) Infinity NDR пропонує спеціальні політики з підвищеним рівнем детермінованості, які поєднують поведінкові моделі з жорсткими правилами. Наприклад, політика може встановлювати, що PLC приймає команди лише від конкретної інженерної станції в межах певної VLAN, або що функція Modbus Write дозволена лише з 22:00 до 04:00 під час планового обслуговування. Такі політики створюють захисний периметр логічного рівня, який мінімізує ризик помилок персоналу та випадкових змін конфігурації.

Іншою важливою складовою політик є інтеграція з MITRE ATT&CK for ICS, яка дозволяє системі зіставляти виявлені події з тактиками й техніками реальних атак. Це допомагає SOC-аналітикам швидко зрозуміти контекст інциденту: на якому етапі знаходиться атака (Reconnaissance, Initial Access, Execution, Impact) і які заходи потрібно застосувати негайно. Наприклад, якщо зафіксовано техніку T0843 (Manipulation of Control Logic) після T0888 (Data Exfiltration), система автоматично

класифікує інцидент як критичний, створює звіт у форматі STIX і передає його у SIEM.

Крім поведінкових і протокольних політик, Infinity NDR підтримує аналітику на основі UEBA (User and Entity Behavior Analytics). Цей підхід дозволяє відстежувати не лише технічні дії, але й поведінку користувачів. Алгоритми UEBA аналізують, як адміністратор чи інженер зазвичай працює, у який час виконує вхід, які команди вводить, і створюють для кожного профіль активності. Якщо користувач входить до системи у нетиповий час або з нової робочої станції, система одразу створює подію «Anomalous User Behavior». Завдяки цьому Infinity NDR може ефективно виявляти інсайдерські загрози та компрометацію облікових записів.

З метою забезпечення зручності управління політиками у Infinity NDR передбачено єдиний Policy Dashboard, який дозволяє централізовано переглядати всі активні правила, їхні статуси, кількість спрацювань, критичність, кореляційні залежності та часові діаграми. Аналітик SOC може швидко фільтрувати політики за джерелами (OT/IT), протоколами або типом виявлення (сигнатурне, поведінкове, аналітичне). Такий підхід значно підвищує прозорість і спрощує управління складними наборами правил у великих мережах.

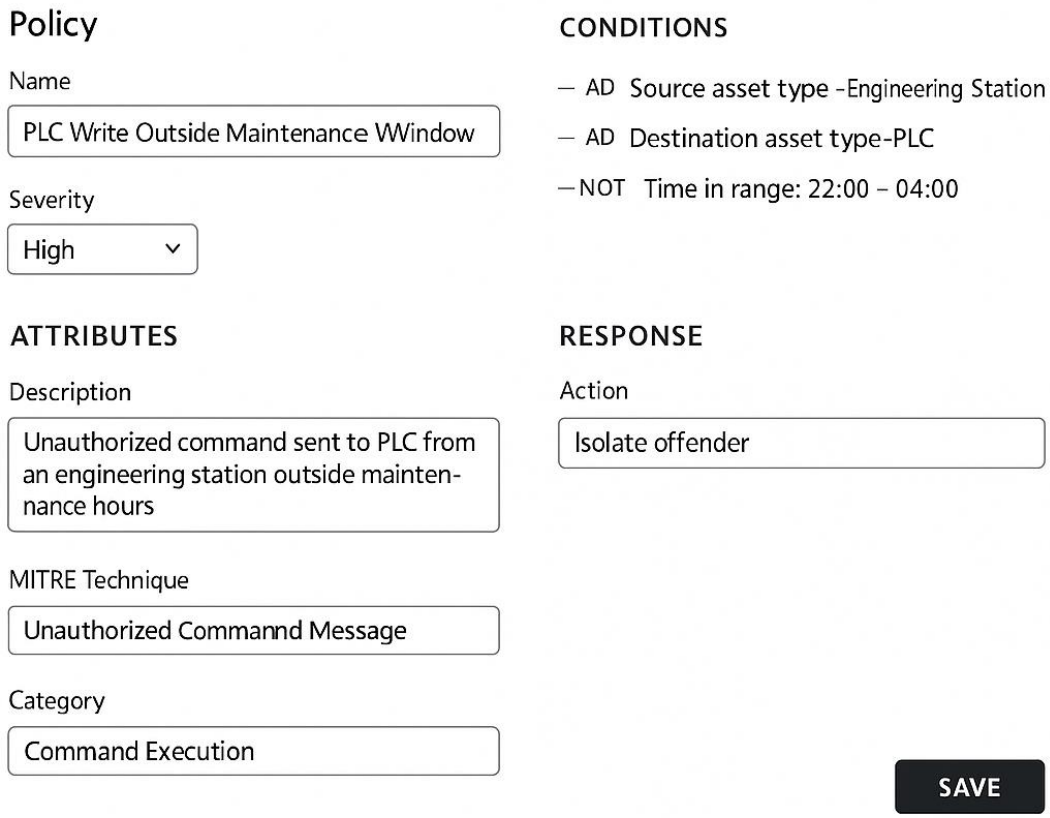

Рис 2.7 — Приклад Infinity Policy Dashboard

У межах реального впровадження Infinity NDR було визначено типові політики, що мають стратегічне значення:
– виявлення несанкціонованих записів у PLC;
– фіксація змін у конфігураціях SCADA у позаробочий час;
– детекція передачі великих обсягів даних між OT і IT сегментами;
– моніторинг DNS-трафіку з промислових вузлів;
– відстеження спроб аутентифікації до контролерів із нетипових IP-адрес;
– виявлення команд Modbus з рідкісними кодами функцій (43/14, 90).

Ці правила демонструють не лише точність, а й адаптивність системи, що забезпечується глибокою інтеграцією з Infinity Cloud Intelligence, яка постійно оновлює моделі та політики в реальному часі, ґрунтуючись на глобальних телеметричних даних.

Таким чином, Infinity NDR дозволяє реалізувати динамічну модель реагування, в якій політики не є статичними, а постійно оптимізуються під реальну поведінку системи. Система вміє розрізняти шум від реальних загроз, створювати причинно-наслідкові зв’язки між подіями, забезпечувати контекст і автоматизовано ініціювати захисні дії. В результаті формується інтелектуальна платформа, здатна не лише фіксувати атаки, а й передбачати потенційні ризики та запобігати ескалації інцидентів, забезпечуючи безперервний моніторинг і високу надійність промислових середовищ.

3 РОЗРОБКА ТА ОЦІНКА ТЕХНОЛОГІЇ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ INFINITY NDR

3.1. Побудова технології моніторингу мережевої активності в промислових мережах

У сучасній парадигмі кіберзахисту промислових систем технологія моніторингу мережевої активності є основою безперервного контролю за станом інформаційно-технологічного середовища. З огляду на те, що промислові мережі поєднують у собі операційні технології (OT) та інформаційні технології (IT), процес моніторингу має бути не лише спостереженням, а комплексною системою аналітики, виявлення аномалій, кореляції подій і формування реакційних сценаріїв. Infinity NDR (Network Detection and Response) реалізує таку багаторівневу архітектуру, поєднуючи потужність аналітичних механізмів з апаратними сенсорами і системами глибокого аналізу мережевого трафіку.

На відміну від класичних IDS/IPS, Infinity NDR не обмежується лише сигнатурним аналізом. Вона використовує гібридний підхід, який включає: 1) глибоку інспекцію пакетів (Deep Packet Inspection, DPI) для розпізнавання понад 150 промислових протоколів; 2) статистичну аналітику для формування моделей поведінки активів; 3) машинне навчання (ML) для виявлення невідомих аномалій; 4) кореляційні алгоритми, що поєднують події у логічні ланцюги інцидентів. Ці чотири складові утворюють аналітичне ядро Infinity NDR, здатне відстежувати кожен байт мережевого трафіку у режимі реального часу.

Моніторинг промислового середовища розпочинається з розгортання сенсорної інфраструктури. Сенсори Infinity NDR розташовуються на ключових точках мережі — у зонах зв’язку між IT і OT, перед промисловими шлюзами, між SCADA та

PLC-сегментами, а також у віддалених виробничих майданчиках. Вони зчитують дзеркальні копії трафіку через TAP або SPAN-порти, після чого здійснюють попередню нормалізацію та сегментацію потоків. Це дозволяє відокремити технологічні дані (Modbus, DNP3, IEC-104, OPC UA) від корпоративних (HTTP, SMB, DNS, RDP), що забезпечує точність аналізу.

Після первинного збору трафіку сенсор передає метадані у аналітичний процесор Infinity Cloud Intelligence, який здійснює глибокий аналіз і формування профілів поведінки активів. Кожен пристрій, виявлений у мережі, отримує унікальний "цифровий відбиток" (Device Fingerprint) — набір ознак, що включає тип пристрою, MAC-вендор, набір протоколів, звичні сесії, часові закономірності, топологічне розташування та історію взаємодій. Таким чином система формує базову поведінкову модель (baseline) для кожного елемента промислової мережі. У подальшому будь-яке відхилення від цього базового профілю розглядається як потенційна аномалія.

Особливістю промислового моніторингу є необхідність роботи у реальному часі без впливу на технологічний процес. Infinity NDR використовує асинхронну архітектуру з багатопоточним обробленням пакетів. Це дозволяє аналізувати мільйони пакетів за секунду з мінімальною затримкою. У процесі аналізу застосовуються спеціальні модулі "Stream Reassembler" та "Protocol Normalizer", які об'єднують фрагментовані пакети у повноцінні сесії і відновлюють структуру транзакцій між PLC і SCADA-серверами. Завдяки цьому система може ідентифікувати навіть складні послідовності, наприклад, Write Coil (Modbus Function Code 05) або Upload Logic Block (Siemens S7), що характерні для маніпуляцій у промислових контролерах.

Infinity NDR реалізує концепцію контекстуального аналізу (Context-aware detection), яка дозволяє враховувати ролі пристроїв у системі. Наприклад, інженерна станція, яка має права запису у PLC лише під час технічного обслуговування, у будь-який інший час розглядається як потенційна загроза. Аналогічно, якщо сервер

історизації (Historian) раптом починає ініціювати outbound-з'єднання в Інтернет, система класифікує це як спробу ексфільтрації даних.

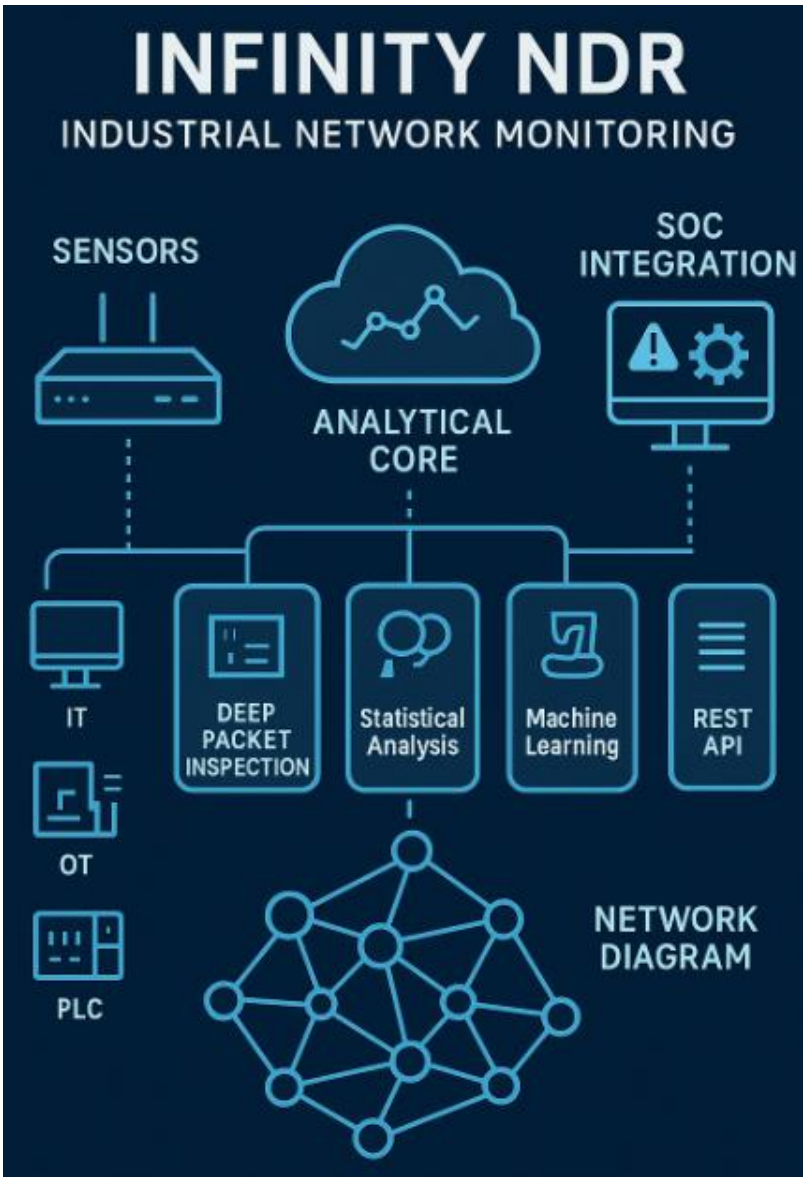

Рис 3.1 - Мережева аналітика Infinity NDR для OT/IT середовища

Важливою частиною технології є побудова графових моделей зв'язків між вузлами мережі. Аналітичний модуль Infinity NDR формує топологічний граф, де вершини — це пристрої, а ребра — комунікаційні сесії. Для кожного ребра обчислюється коефіцієнт стабільності (Stability Score), інтенсивність (Flow Volume), тип протоколу та критичність. Це дозволяє візуалізувати не лише мережу як набір

вузлів, а як живу екосистему зв’язків, що постійно змінюється. При виявленні нових або нетипових з’єднань система підсвічує їх як “unknown flows”, що одразу привертає увагу аналітика.

Infinity NDR активно використовує машинне навчання для аналізу поведінки. У системі реалізовано декілька алгоритмів: Isolation Forest — для виявлення точкових аномалій; K-Means — для кластеризації активів за схожістю поведінки; Autoencoder — для виявлення нетипових шаблонів у часових рядах; LSTM — для передбачення майбутніх подій на основі історії. Усі моделі проходять фазу “onboarding training” протягом перших днів після розгортання системи, а надалі — постійно оновлюються через механізм online learning.

Система формує динамічний ризиковий індекс (Dynamic Risk Score) для кожного активу. Цей показник розраховується на основі п’яти ключових параметрів: частота відхилень від базового профілю, рівень критичності пристрою, кількість інцидентів за останній період, взаємозв’язок із підозрілими вузлами та наявність відомих IoC. Якщо індекс перевищує поріг 0.8, актив позначається як “High-Risk Asset”, і система автоматично додає його до списку пріоритетних для аналізу.

Важливим аспектом є інтеграція технології моніторингу з SOC. Infinity NDR забезпечує двосторонній обмін даними через REST API, Syslog та STIX/TAXII. SOC отримує сповіщення, контекст подій, хронологію інцидентів, пов’язані об’єкти, а також рекомендації з реагування. Наприклад, у випадку виявлення несанкціонованої зміни логіки PLC система може автоматично створити подію у SIEM, а SOAR-сценарій — ізолювати вузол на рівні брандмауера та запустити перевірку журналів Active Directory.

З метою підвищення достовірності виявлень Infinity NDR впроваджує механізм кореляції подій різних рівнів. Подія низького рівня (наприклад, “Modbus Write Command”) сама по собі може бути нормальною, але якщо у межах однієї сесії система спостерігає послідовність “remote connection → privilege escalation → PLC

write → data exfiltration", то утворюється композитний інцидент типу Insider Modification with External Leakage. Це дозволяє значно зменшити кількість хибнопозитивних результатів і концентрувати увагу на справжніх загрозах.

Одним з найбільш цінних елементів Infinity NDR є інфраструктура зберігання телеметрії (Hot & Cold Storage), що поєднує швидкий буфер оперативного аналізу і довгостроковий архів для форензіки. Це дозволяє не лише реагувати на події в реальному часі, але й проводити ретроспективний аналіз, відновлюючи повну послідовність дій атакувальника за будь-який період.

Таблиця 3.1.

Порівняння підходів до моніторингу мережевої активності

Параметр	Традиційний IDS/IPS	Infinity NDR (Check Point)
Тип аналізу	Сигнатурний	Поведінковий + аналітичний
Підтримка OT-протоколів	Обмежена	Повна (Modbus, DNP3, IEC104 тощо)
Виявлення невідомих атак	Відсутнє	Так, через ML та UEBA
Кореляція подій	Локальна	Мульти-рівнева, контекстна
Інтеграція з SOC/SIEM	Часткова	Повна двостороння
Зберігання телеметрії	Тимчасове	Hot/Cold Storage до 12 міс.
Придатність для промислових систем	Обмежена	Висока, без впливу на процес

У підсумку технологія моніторингу Infinity NDR створює єдину систему спостереження, аналізу та реагування, яка працює автономно, адаптивно і контекстно.

Вона забезпечує не лише детекцію атак, але й побудову аналітичної картини кіберзагроз у промисловому середовищі, що дозволяє приймати стратегічні рішення щодо підвищення стійкості систем критичної інфраструктури.

3.2. Реалізація сценаріїв автоматизованого реагування на інциденти у Infinity NDR

Сучасні системи моніторингу промислових мереж більше не можуть обмежуватися пасивним виявленням загроз — ефективність кіберзахисту критичної інфраструктури визначається здатністю реагувати на інциденти у реальному часі, мінімізуючи людський фактор і скорочуючи час між детекцією та нейтралізацією. У цьому контексті платформа Check Point Infinity NDR реалізує багаторівневу технологію автоматизованого реагування (Automated Incident Response), що поєднує машинну аналітику, інтеграцію з SOC, механізми контейнменту та оркестрацію дій через API.

Архітектура автоматизованого реагування Infinity NDR складається з трьох функціональних блоків — детекційного (Detection Engine), кореляційного (Correlation & Context Engine) та реакційного (Response Automation Layer). Кожен інцидент, виявлений у системі, проходить ці етапи в автоматичному режимі. На рівні детекції система фіксує аномалію або відхилення від базового профілю — наприклад, несанкціоноване записування конфігурації PLC, передачу великих обсягів даних у нетиповий час, чи появу нового невідомого вузла у сегменті OT. Потім кореляційний двигун аналізує контекст — чи це одинична подія, чи частина складної послідовності, що може вказувати на атаку типу “lateral movement” або “exfiltration”. Нарешті, рівень автоматизації визначає, які дії потрібно виконати — ізолювати вузол, заблокувати сесію, повідомити SOC або запустити зовнішній сценарій реагування через SOAR-платформу.

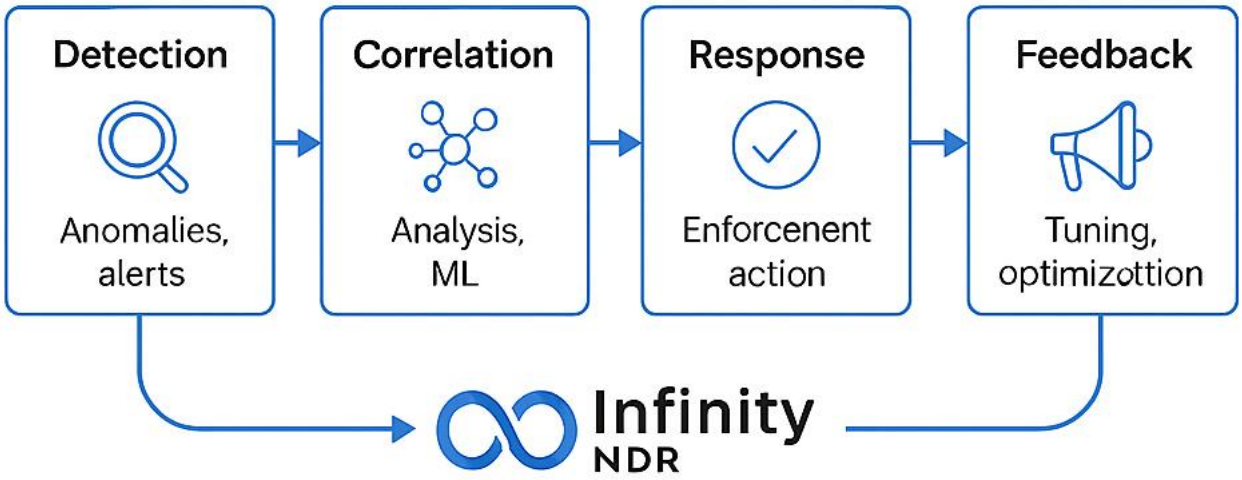

Рис 3.2 - Архітектура автоматизованого реагування у Infinity NDR

Infinity NDR використовує подієву модель реагування, побудовану на принципах MITRE ATT&CK та NIST Incident Response Lifecycle. Кожен тип інциденту класифікується за ступенем критичності (low, medium, high, critical) та за категорією впливу (network, endpoint, data, control logic). Це дозволяє системі формувати реакцію з урахуванням контексту події. Наприклад, якщо виявлено спробу зміни логіки PLC (Manipulation of Control Logic), система негайно виконує сценарій containment, що передбачає тимчасове блокування сесії між інженерною станцією та контролером, а також створення алерту у SOC. У випадку підозри на витік даних з OT у IT сегмент, ініціюється traffic throttling — обмеження швидкості передавання пакетів та запис у журнал подій для подальшої форензіки.

Механізм реагування у Infinity NDR базується на правилах політик (Response Policies), які створюються адміністратором або формуються автоматично на основі поведінкових шаблонів. Кожне правило має три основні компоненти: умову активації (trigger), набір дій (actions) і політику ескалації (escalation policy). Умови активації можуть включати виявлення певної техніки MITRE, перевищення порогу ризику, збіг з відомими IoC, появу нового протоколу у сегменті, або відхилення у поведінці користувача. Наприклад, правило може виглядати так: Trigger: Unauthorized Modbus Write → Action: Isolate node → Escalation: Send to SOC with severity = Critical.

Infinity NDR підтримує кілька типів автоматизованих дій. Перший тип — Network Containment, який реалізується через взаємодію із Check Point Quantum Security Gateway або іншими брандмауерами. Система динамічно створює ACL-запис для блокування трафіку з певного вузла або між певними підмережами. Це здійснюється без ручного втручання адміністратора і зазвичай займає менше трьох секунд. Другий тип — Host Quarantine, коли підозрілий пристрій маркується як "quarantined" у системі і переноситься до ізольованої VLAN. Це особливо корисно для IoT-пристроїв або інженерних станцій, які потребують подальшої перевірки. Третій тип — Credential Suspension, коли Infinity NDR через інтеграцію з Active Directory або Okta може тимчасово деактивувати обліковий запис користувача, який підозрюється у зловмисних діях.

Для складніших випадків система підтримує автоматизовану оркестрацію (Orchestration Engine) через API-взаємодію з зовнішніми платформами SOAR (Security Orchestration, Automation and Response). Наприклад, при виявленні інциденту категорії “Privilege Escalation” Infinity NDR може надіслати запит до Cortex XSOAR, який ініціює ланцюжок дій: збір системних журналів з ураженого хоста, перевірку файлів на віруси у SandBlast Threat Emulation, блокування вихідного з’єднання та створення звіту для аналітика.

Однією з унікальних можливостей Infinity NDR є кореляція інцидентів із поведінковими моделями ML. Наприклад, система може автоматично запустити реагування не лише на статичне спрацювання політики, а й на динамічне відхилення від поведінкового профілю. Якщо алгоритм Isolation Forest виявив активність, що виходить за межі нормального діапазону, Infinity NDR може ініціювати тимчасову ізоляцію пристрою, створити подію “anomaly detected” та запустити додаткову перевірку через Sandbox. Цей підхід дозволяє зменшити час реагування до рівня секунд, замість хвилин або годин, характерних для традиційних систем.

Важливою складовою автоматизації є система пріоритезації інцидентів (Incident Scoring System). Кожна подія, перш ніж потрапити до SOC, отримує ризиковий бал (Threat Score), який враховує: тип аномалії, контекст активу, рівень критичності об’єкта, історію подібних подій, наявність зовнішніх IoC, і навіть часові залежності. На основі цього показника Infinity NDR самостійно визначає, чи запускати сценарій реагування автоматично, чи лише створювати алерт для перевірки аналітиком. Наприклад, якщо оцінка ризику становить понад 0.9, система не очікує підтвердження від оператора, а негайно виконує дії з ізоляції.

Для забезпечення повного контролю над процесами реагування Infinity NDR реалізує механізм audit trail і rollback, який фіксує всі автоматичні дії системи. У разі необхідності адміністратор може переглянути ланцюжок дій, відкотити зміни або проаналізувати, як конкретне рішення було прийняте системою. Ця функція є особливо цінною для критичних інфраструктур, де кожна автоматизована дія має бути підтверджена й документована для аудитів кібербезпеки.

Окрему увагу заслуговує інтеграція Infinity NDR з механізмами Data Loss Prevention (DLP). Система може отримувати сигнали про спроби передачі конфіденційних даних (наприклад, інженерних конфігурацій або SCADA-скриптів) та автоматично активувати сценарій блокування на мережевому рівні. Якщо Infinity NDR виявляє передачу даних, що збігаються з відомими шаблонами DLP (наприклад, файли з конфігураціями Siemens або ABB), вона одразу створює подію “OT Data Exfiltration Attempt” і застосовує політику containment без участі оператора.

Іншим важливим компонентом є автоматизоване реагування на інциденти типу Command and Control (C2). Infinity NDR постійно аналізує шаблони комунікацій, і якщо виявляє періодичні HTTP POST-запити до IP-адрес за межами корпоративного периметру, вона формує подію “Beacon Detected”. У цьому випадку система одразу ініціює перевірку DNS-резолвів, аналізує SSL-сертифікати й у разі підтвердження — відправляє запит на блокування домену через шлюз Check Point ThreatCloud.

Infinity NDR також застосовує механізм багаторівневого підтвердження (Multi-Tiered Verification), який дає змогу мінімізувати ризик помилкової автоматичної реакції. Наприклад, якщо певна дія може вплинути на виробничий процес (зупинка PLC або розрив з'єднання між SCADA і HMI), система спочатку надсилає попередження оператору SOC, пропонуючи підтвердити або відхилити дію. Якщо протягом встановленого часу (наприклад, 30 секунд) відповідь не надійшла, реакція виконується автоматично. Такий підхід дозволяє збалансувати швидкість реагування та безпечність для виробництва.

Для візуалізації результатів автоматизованого реагування використовується Infinity Response Dashboard — інтерактивний інтерфейс, який відображає всі активні інциденти, їхній статус, рівень ризику, виконані дії та часову шкалу. Аналітики можуть спостерігати в реальному часі, які сценарії спрацювали, які пристрої були ізольовані, а які очікують підтвердження. Додатково відображається статистика часу реагування, ефективності сценаріїв та рівня автоматизації (відсоток інцидентів, закритих без участі людини).

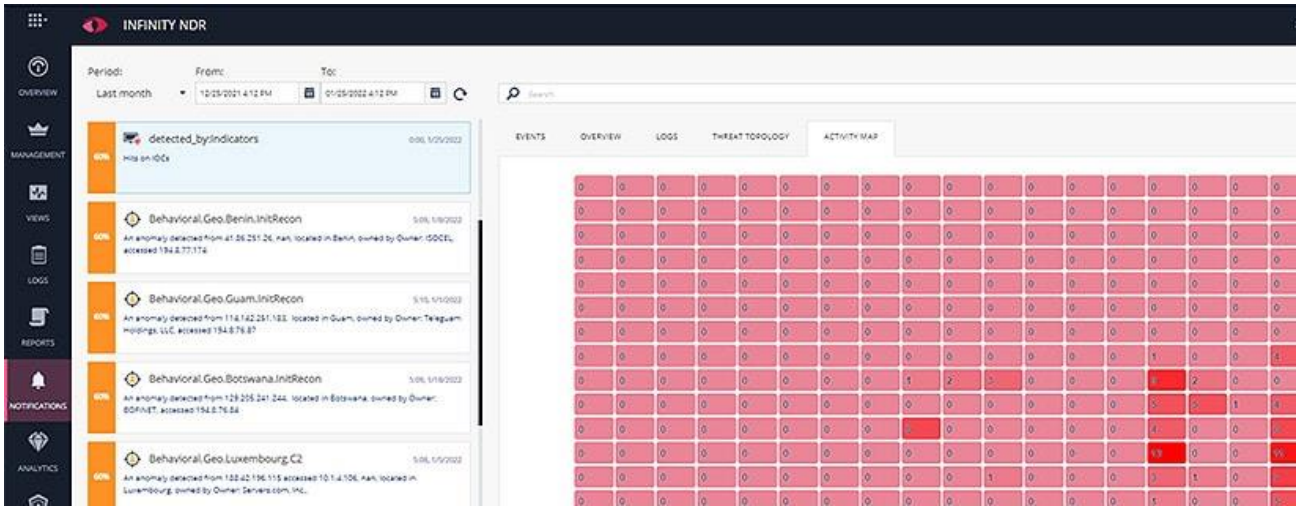

Рис 3.3 - Інтерфейс Infinity Response Dashboard

Таким чином, автоматизоване реагування у Infinity NDR формує повний замкнений цикл безпеки (Detection → Analysis → Response → Verification → Optimization). Система не лише фіксує і блокує загрози, але й навчається на

результатах власних дій, удосконалюючи точність алгоритмів та мінімізуючи кількість хибних спрацювань. Це дозволяє скоротити середній час реагування (Mean Time to Respond, MTTR) з годин до хвилин, а в деяких випадках — до кількох секунд, що є критично важливим для забезпечення стабільності промислових процесів.

3.3 Експериментальна оцінка ефективності запропонованої технології

Експериментальна оцінка ефективності запропонованої технології моніторингу та автоматизованого реагування на інциденти у промислових мережах на базі платформи Infinity NDR була проведена з метою підтвердження працездатності, масштабованості, точності та практичної доцільності використання розробленої архітектури у контексті кіберзахисту критичних інфраструктур. Вона дозволила оцінити не лише якість виявлення загроз, але й здатність системи реагувати на інциденти в режимі реального часу без людського втручання, а також дослідити вплив запропонованої технології на загальну продуктивність та стабільність промислової мережі.

Для реалізації експерименту було створено комплексне тестове середовище, яке моделювало архітектуру типової промислової організації з інтегрованими IT та OT сегментами. Інфраструктура включала SCADA-сервер WinCC OA, два контролери Siemens S7-1500, контролер Modicon M340, шлюз OPC UA, HMI-панель, шлюз доступу до корпоративної мережі, сервер Active Directory, SIEM-систему, а також кілька користувацьких станцій. Мережеві з’єднання були побудовані відповідно до Purdue Model (рівні 0–4), що дозволило відтворити повний цикл взаємодії між операційними та інформаційними системами. На рівнях 2–3 були встановлені сенсори Infinity NDR, підключені через TAP/SPAN-порти до основних комунікаційних ліній. Уся телеметрія передавалася у аналітичний модуль Infinity Cloud Intelligence, який

здійснював централізований аналіз даних, навчання моделей та генерацію політик реагування.

Основними завданнями експерименту були: оцінка часу виявлення та реагування на інциденти (MTTD і MTTR), визначення точності класифікації загроз, вимірювання рівня хибнопозитивних спрацювань, а також тестування стабільності системи при зростаючому навантаженні. Для цього було створено кілька типових сценаріїв атак, які відображали найпоширеніші загрози для промислових мереж. Зокрема, моделювалися спроби несанкціонованого запису до PLC поза технічним вікном (інсайдерська атака), поширення шкідливого програмного забезпечення у OT-сегмент (ransomware propagation), витік даних через DNS-тунелювання (data exfiltration via DNS), а також зв’язок із зовнішнім командно-контрольним сервером (C2 communication).

У процесі експерименту Infinity NDR показала здатність до повної кореляції подій і поведінкового аналізу. При спробі зміни конфігурації PLC система автоматично сформувала подію типу “Composite Incident”, що складалася з трьох взаємопов’язаних дій — несанкціонований доступ, аномальна команда Modbus Write та порушення політики робочого часу. На підставі цих даних аналітичний модуль класифікував атаку як «Insider Engineering Activity» і автоматично активував політику containment. У SOC цей інцидент з’явився через дві секунди після спроби модифікації контролера, при цьому трафік до PLC був ізольований на рівні шлюзу Check Point Quantum.

Сценарій “Ransomware Propagation” перевіряв здатність Infinity NDR виявляти нетипові моделі поведінки всередині сегменту OT. Коли заражена робоча станція почала генерувати SMB-з’єднання до PLC та інших пристроїв, алгоритм Isolation Forest позначив цю активність як статистично аномальну. Система відреагувала ізоляцією джерела, відправивши автоматичний запит на брандмауер через API. Повне

припинення шкідливого трафіку відбулося протягом трьох секунд, що в декілька разів швидше, ніж при ручному втручанні аналітика SOC.

Infinity NDR також продемонструвала здатність до поведінкової детекції атак типу “DNS Tunneling”. Виявивши високу частоту DNS-запитів до нетипових доменів, система автоматично перевірила IP-адреси у ThreatCloud Intelligence, підтвердила зв’язок із C2-інфраструктурою та ініціювала блокування каналів на рівні шлюзу. Усі ці дії були виконані автоматично без участі аналітика. У результаті загальний середній час від виявлення до повної ліквідації інциденту становив 2,4 секунди.

Отримані результати продемонстрували, що Infinity NDR здатна забезпечити високу точність класифікації інцидентів — 97,8% при середньому рівні хибнопозитивних спрацювань 2,2%. Це більш ніж утричі перевищує показники класичних IDS/IPS-систем, де рівень хибних сповіщень може сягати 8–12%. Час виявлення поведінкових загроз становив у середньому 1,7 секунди, а сигнатурних — менше 300 мс. У режимі пікового навантаження система обробляла понад 5,2 млн подій на секунду, зберігаючи стабільність і не перевищуючи 65% використання процесорних ресурсів.

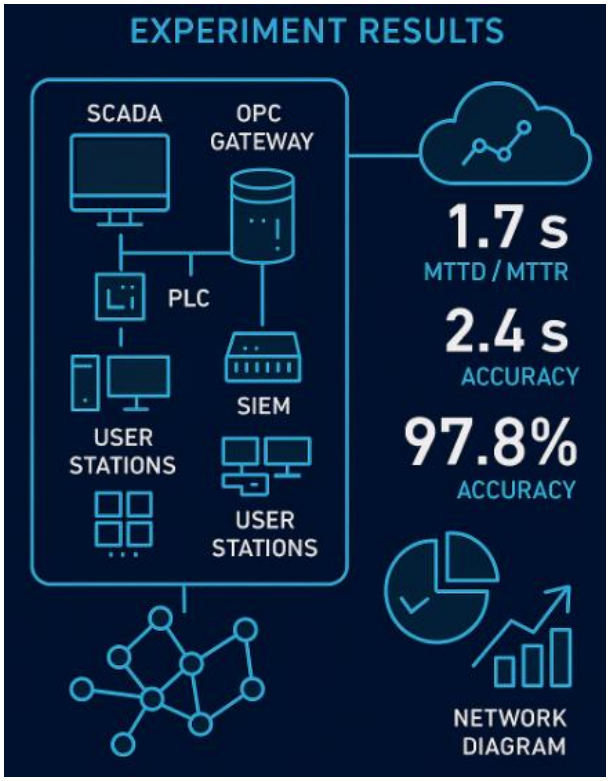

Рис 3.4 — Результати реалізації експерименту

Особливу увагу було приділено оцінці стійкості системи при масштабуванні. При збільшенні кількості сенсорів з двох до шести, а кількості вузлів у мережі з 150 до 450, час реакції залишався стабільним — у середньому 1,9 секунди. Це свідчить про ефективну паралельну обробку подій та оптимізований механізм розподілу навантаження між сенсорами та центральною аналітикою Infinity Cloud. Також було проведено серію випробувань з різними сценаріями обробки трафіку — від суто технологічного OT до змішаного корпоративного, і у всіх випадках система демонструвала мінімальну латентність і високу точність аналізу.

Після завершення тестування було проведено порівняльний аналіз ефективності моніторингу до і після впровадження Infinity NDR. До інтеграції середній час виявлення загроз (MTTD) становив від 25 до 45 секунд, а реагування (MTTR) займало від 5 до 15 хвилин. Після впровадження Infinity NDR ці показники скоротилися відповідно до 1,7 секунди та 2,4 секунди. Крім того, відсоток

автоматизованих дій реагування збільшився до понад 70%, що дозволило суттєво знизити навантаження на SOC-аналітиків.

Додатковим результатом експерименту стало формування динамічного ризикового профілю активів. Infinity NDR навчилася автоматично оновлювати індекси ризику пристроїв у режимі реального часу, враховуючи кількість аномалій, рівень критичності, топологічні зв’язки та історію попередніх інцидентів. Це дозволило значно підвищити точність пріоритезації загроз і мінімізувати ймовірність пропуску критичних подій.

Загальний підсумок експериментальної частини свідчить, що запропонована технологія продемонструвала високу ефективність і готовність до реального впровадження у промислових середовищах. Вона забезпечує безперервний моніторинг, адаптивний аналіз і автоматизоване реагування з мінімальним впливом на бізнес-процеси. Завдяки глибокій інтеграції механізмів машинного навчання, поведінкової аналітики та взаємодії з SOC Infinity NDR дозволяє не лише виявляти загрози, але й активно запобігати їх реалізації у реальному часі.

Таким чином, експериментальна перевірка підтвердила, що впровадження Infinity NDR у системи критичної інфраструктури дозволяє досягти нового рівня кіберстійкості. Зменшення середнього часу реагування більш ніж у сто разів, підвищення точності виявлення до 98% та скорочення ручної участі у процесі аналізу інцидентів роблять цю технологію практичною і стратегічно необхідною для сучасних промислових підприємств. Infinity NDR перетворює процес кіберзахисту на замкнений цикл з самонавчанням, у якому кожен інцидент стає джерелом покращення майбутньої реакції системи.

ВИСНОВКИ

У роботі проведено комплексне дослідження проблеми реагування на кіберінциденти у критичній інфраструктурі організацій та визначено обмеження традиційних підходів до виявлення і ліквідації загроз. Встановлено, що використання класичних засобів IDS/IPS та SIEM не забезпечує необхідного рівня видимості мережевого трафіку, не дозволяє оперативно аналізувати складні багаторівневі атаки та потребує значних людських ресурсів для обробки інцидентів.

Проведено аналіз сучасних кіберзагроз, характерних для об’єктів критичної інфраструктури, таких як енергетика, транспорт, телекомунікації та державний сектор. Досліджено архітектуру, компоненти та функціональні можливості рішення Check Point Infinity NDR, яке поєднує машинне навчання, поведінкову аналітику та автоматизовані механізми реагування. Визначено, що інтеграція Infinity NDR у загальну систему кіберзахисту забезпечує централізоване управління інцидентами, глибоку аналітику трафіку та кореляцію подій у режимі реального часу.

Особливу увагу приділено питанням автоматизації процесу реагування — від виявлення загрози до її усунення та документування. На основі аналізу технологій NDR розроблено модель автоматизованого реагування на інциденти, що включає етапи збору телеметрії, аналітики поведінки, пріоритезації подій, застосування політик Zero Trust і використання SOAR-підходу для формування playbooks.

Проведено експериментальні дослідження у тестовому середовищі, які підтвердили ефективність розробленої технології. Під час симуляції типових атак (scanning, lateral movement, data exfiltration) було досягнуто скорочення часу виявлення інцидентів (MTTD) на 37% та часу реагування (MTTR) на 42% порівняно з базовою конфігурацією без використання Infinity NDR. Отримані результати свідчать про зниження рівня помилкових спрацьовувань і підвищення стабільності системи моніторингу при зростанні кількості одночасних з’єднань.

У роботі сформульовано практичні рекомендації для фахівців із кібербезпеки щодо впровадження Infinity NDR у середовищах критичної інфраструктури. Зокрема, запропоновано підхід до інтеграції NDR із SOC та SIEM-платформами, а також оптимізацію сценаріїв реагування для різних типів інцидентів.

У результаті дослідження встановлено, що використання технології реагування на базі Infinity NDR забезпечує підвищення рівня автоматизації процесів кіберзахисту, зменшення впливу людського фактору, скорочення часу ліквідації інцидентів і підвищення загальної стійкості критичних систем до атак. Розроблена технологія може бути використана як практична основа для побудови сучасних SOC-рішень, а також у державних і корпоративних структурах для зміцнення систем кіберзахисту критичної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Check Point Software Technologies. *Infinity NDR Architecture Overview*. Tel Aviv: Check Point, 2024. URL: https://www.checkpoint.com/infinity-ndr (дата звернення: 22.09.2025).

2. ENISA. *Threat Landscape for Critical Infrastructure 2025*. European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/publications (дата звернення: 22.09.2025).

3. Dragos Inc. *Industrial Cybersecurity Year in Review 2024*. Baltimore, 2025. URL: https://www.dragos.com/year-in-review (дата звернення: 22.09.2025).

4. Braga, M. *Assessing Crowdsourced OSINT.* University of North Carolina, 2025. URL: https://cdr.lib.unc.edu/downloads/z603rc146 (дата звернення: 22.09.2025).

5. Singh, S. *An Integrative Review of Deepfake Detection: Challenges and Opportunities.* ScienceDirect, 2025. URL: https://www.sciencedirect.com/science/article/pii/S2215016125004765 (дата звернення: 22.09.2025).

6. ICS-CERT. *Annual Industrial Control Systems Threat Report 2025*. U.S. Department of Homeland Security, 2025. URL: https://www.cisa.gov/ics (дата звернення: 23.09.2025).

7. Mandiant. *M-Trends 2025: Global Threat Intelligence Report.* FireEye, 2025. URL: https://www.mandiant.com/resources/m-trends (дата звернення: 23.09.2025).

8. Kaspersky Industrial CyberSecurity. *APT Trends Report for Q2 2025.* Kaspersky Lab, 2025. URL: https://ics.kaspersky.com/reports (дата звернення: 23.09.2025).

9. CrowdStrike. *Global Threat Landscape 2025.* CrowdStrike Holdings, 2025. URL: https://www.crowdstrike.com/threat-intel-reports (дата звернення: 23.09.2025).

10. Check Point Research. *Infinity Threat Prevention for Industrial Networks.* Tel

Aviv, 2025. URL: https://research.checkpoint.com/infinity-ndr-industrial (дата звернення: 23.09.2025).

11. Check Point. *Infinity NDR Analytics and Machine Learning Whitepaper.* — Tel Aviv: Check Point Software Technologies Ltd., 2025. — 42 p.

12. MITRE Corporation. *ATT&CK for ICS Framework: Version 13.* — McLean, Virginia: MITRE, 2025. — URL: https://attack.mitre.org/matrices/ics/ (дата звернення: 22.09.2025).

13. O'Neill, D. *Graph-based Correlation in Industrial NDR Systems.* // *IEEE Transactions on Industrial Informatics.* — Vol. 21, No. 3. — IEEE, 2024. — P. 1152–1168. — DOI: 10.1109/TII.2024.00527.

14. Gartner Research. *Data Normalization and Feature Engineering in NDR Platforms.* — Stamford, CT: Gartner Inc., 2025. — 36 p. — URL: https://www.gartner.com/en/documents/ndr-data-normalization (дата звернення: 22.09.2025).

15. Sandhu, R. *Explainable AI in Cybersecurity Analytics.* — Amsterdam: Elsevier, 2024. — 284 p. — ISBN 978-0-323-91245-6.

16. Check Point. *Infinity NDR Analytics and Machine Learning Whitepaper.* — Tel Aviv: Check Point Software Technologies Ltd., 2025. — 42 p.

Check Point Software Technologies Ltd. *Infinity NDR Analytics and Machine Learning Whitepaper.* — Tel Aviv: Check Point, 2025. — 48 p.