

# Vectra AI та CrowdStrike Falcon Next-Gen SIEM

## Ключові Виклики

Видимість є основою ефективного виявлення кібератак до того, як вони стають критичними для бізнесу. Це особливо важливо в умовах, коли інфраструктура організацій поєднує локальні та хмарні середовища. Застарілі системи керування журналами подій і традиційні інструменти виявлення та реагування перевантажені шумом і складністю, що ускладнює роботу аналітиків і сповільнює реагування на загрози. Крім того, витрати на зберігання та обробку даних у таких системах стрімко зростають, особливо з огляду на необхідність аналізу великих обсягів даних.

## Огляд рішення

Інтеграція Vectra AI з Falcon Next-Gen SIEM від CrowdStrike дозволяє подолати ці обмеження завдяки об'єднанню мережевої телеметрії та масштабованого аналізу даних. Falcon Next-Gen SIEM забезпечує обробку та аналіз великих обсягів даних із різних джерел, включаючи хмарні сервіси, кінцеві пристрої, системи ідентифікації та мережеву інфраструктуру. Vectra AI доповнює це високоточним виявленням атак на основі штучного інтелекту. У результаті команди центру операцій безпеки отримують повний контекст інцидентів, швидше проводять розслідування та можуть оперативнo зупинити атаки до того, як вони вплинуть на бізнес.

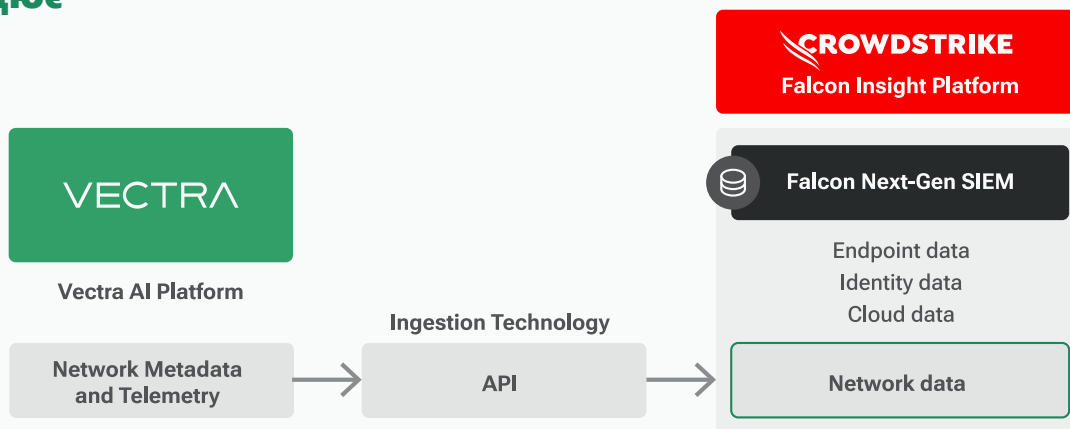
## Компоненти рішення:

- Vectra AI Platform with Attack Signal Intelligence
- Vectra NDR
- CrowdStrike Falcon Next-Gen SIEM

## Ключові переваги:

- Єдине представлення пріоритетів для мережевих виявлень на платформі Vectra AI -з урахуванням хостів, облікових записів і джерел даних.
- Плавний перехід між платформою Vectra AI та CrowdStrike Falcon Next-Gen SIEM для проведення глибших розслідувань.
- Швидке керування журналами подій та аналітика в режимі реального часу для мережі, кінцевих пристроїв, хмарних середовищ і систем ідентифікації.
- Пріоритизація загроз за рівнем критичності та поведінковими ознаками атаки.
- Прискорення розслідування інцидентів команди центру операцій безпеки завдяки об'єднанню мережевих даних і телеметрії з кінцевих пристроїв.

## Як це працює



- 1 Network Detection and Response від Vectra AI передає мережеві метадані та телеметрію до Falcon Next-Gen SIEM від CrowdStrike.
- 2 Далі користувачі можуть одним кліком перейти від виявленої загрози до Falcon Next-Gen SIEM CrowdStrike, щоб виконати детальніше розслідування стану безпеки своєї організації.
- 3 Візуалізація даних і блискавично швидкі запити до логів у Falcon Next-Gen SIEM прискорюють розслідування та дозволяють оперативнo вжити заходів ще до того, як атака переросте у повноцінний інцидент.

## Ключова цінність інтеграції

### Повна видимість

Платформа Vectra AI забезпечує глибоку видимість атак у мережі та в різних середовищах — публічній хмарі, хмарних застосунках, системах ідентифікації, мережевій інфраструктурі та на кінцевих пристроях — передаючи високоякісні сигнали до системи керування подіями та інформацією безпеки Falcon Next-Gen SIEM.

### Чіткість

Завдяки аналізу загроз на основі штучного інтелекту та кореляції телеметрії команди центру операцій безпеки отримують менше шуму сповіщень і чітко визначення пріоритетів критичних інцидентів.

### Контроль

Аналітики можуть швидко перейти від виявлення загрози до глибшого розслідування у Falcon Next-Gen SIEM та оперативно вжити заходів для зупинки атаки.

## Про Vectra AI

Vectra AI є лідером у розвитку Attack Signal Intelligence на основі штучного інтелекту. Компанія нативно надає телеметрію гібридних атак у публічній хмарі, хмарних застосунках, системах ідентифікації та мережах у межах єдиної платформи. Платформа Vectra AI допомагає командам безпеки швидко визначати пріоритети, проводити розслідування та реагувати на найскладніші кібератаки у гібридному середовищі. Vectra AI має 35 патентів у сфері виявлення загроз на основі штучного інтелекту та є одним із найбільш цитованих постачальників у фреймворку MITRE D3FEND. Організації по всьому світу використовують платформу Vectra AI та сервіси MXDR, щоб діяти зі швидкістю та масштабом сучасних гібридних атак. Більше інформації: [www.vectra.ai](http://www.vectra.ai).

## Про CrowdStrike

CrowdStrike, глобальний лідер у сфері кібербезпеки, переосмислив сучасний підхід до захисту завдяки передовій хмарній платформі, що забезпечує захист ключових зон корпоративного ризику: кінцевих пристроїв, хмарних навантажень, систем ідентифікації та даних. Платформа CrowdStrike Falcon®, побудована на базі CrowdStrike Security Cloud та технологій штучного інтелекту, використовує індикатори атак у режимі реального часу, аналітику загроз, знання про тактики і техніки зловмисників та збагачену телеметрію з усієї інфраструктури. Це забезпечує високоточне виявлення загроз, автоматизований захист і відновлення, проактивний пошук загроз та чітко визначення пріоритетів вразливостей. Більше інформації: [www.crowdstrike.com](http://www.crowdstrike.com).



**iIT Distribution** забезпечує дистрибуцію та просування ексклюзивних рішень для побудови IT-інфраструктури та забезпечення кібербезпеки в Україні, Азербайджані, Казахстані, Узбекистані, Польщі, Латвії, Литві, Естонії, а також надає професійну підтримку в їх проєктуванні та впровадженні.

Щоб отримати консультацію, звертайтеся за контактами: +38 (044) 339 91 16, [cs@iitd.io](mailto:cs@iitd.io)

Більше інформації: <https://iitd.io/>