МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист інформації в спеціалізованих ІТС

Практичне заняття №4

Порівняльний аналіз архітектурно-функціональних властивостей платформ кіберзахисту спеціалізованих ОТ-систем в промисловості

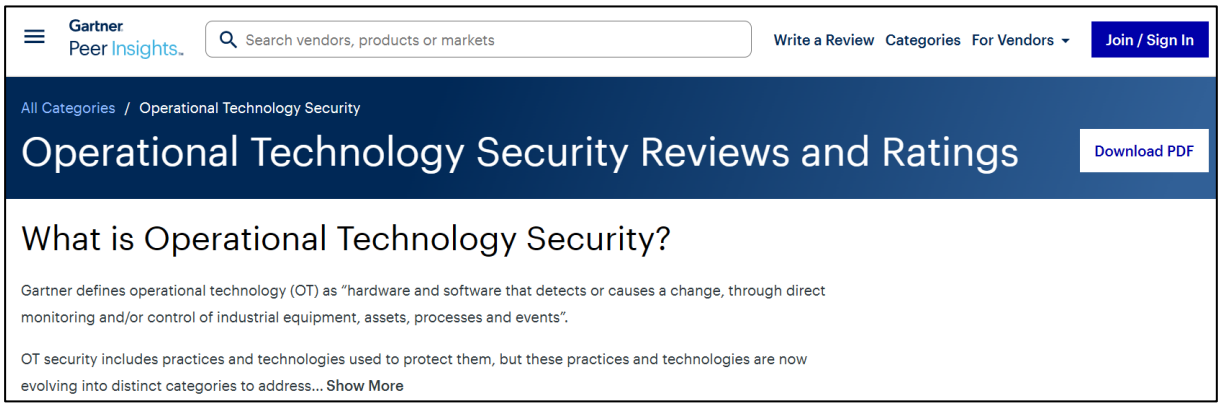
Перевірив:
Зубок В. Ю.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2025

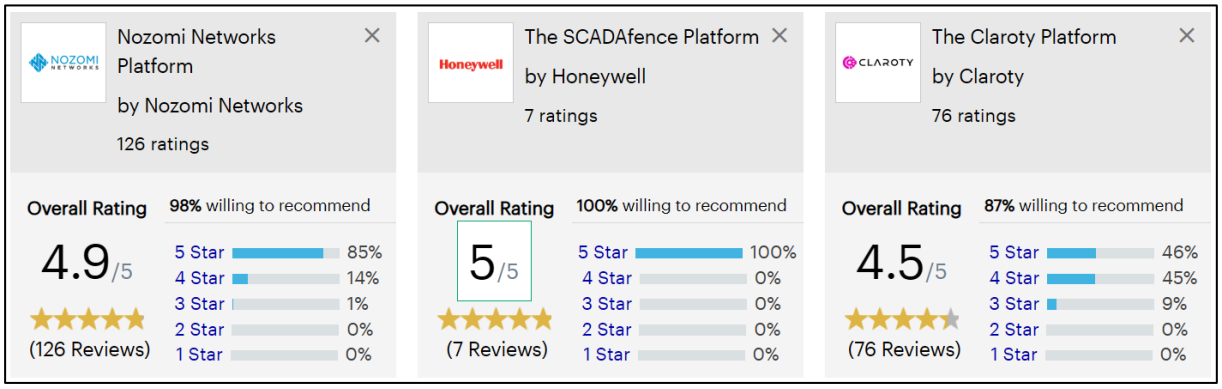
Завдання до виконання:

1. Ознайомитись з матеріалами “Operational Technology (OT) Security Reviews and Ratings” на веб-сайті “Gartner Peer Insights”, зокрема, з методикою оцінювання платформ IAD.
   - **How Categories and Markets Are Defined**
   - **Market Guide for Operational Technology Security**



2. Обрати групу платформ для порівняння в залежності від варіанту.

№ за списком групи	Платформа 1	Платформа 2	Платформа 3
17.	The Claroty Platform	Nozomi Networks Guardian	SCADAfence Platform



3. Обрати групу з не менш ніж 3 критеріїв (краще 5+), які, на вашу думку, є найбільш значущими в умовах, викладених в вашому варіанті. Повний перелік критеріїв відкривається під час порівняння самих платформ (“Compare”). Коротко аргументувати ваш вибір критеріїв.

№ за списком групи	Умови, в яких відбуватиметься розгортання та експлуатація платформ
2,5,8,11,14,17, 20,23,26,29,32	Підприємство критичної інфраструктури, яке власних спеціалістів з кібербезпеки не має, проте водночас повинно зробити проект IAD з детальною сегментацією мереж.

- **Критерій 1: Ease of Deployment** – За відсутності OT/ICS-фахівців важливо, щоб IAD-рішення швидко інтегрувалось у діючу інфраструктуру з мінімальними вимогами до налаштування, щоби швидше досягнути операційної стійкості.

- **Критерій 2: Network segmentation** – Функціональність платформи повинна підтримувати ізоляцію критичних вузлів мережі шляхом зонування (сегментації).

- **Критерій 3: Quality of Technical Support** – За відсутності внутрішнього експертного ресурсу, будь-яке питання потребуватиме оперативної підтримки зі сторони вендора, тому необхідно, щоб вона була якісною та компетентною.

- **Критерій 4: Timeliness of Vendor Response** – Чим швидше платформа оновлюється, виправляє вразливості або надає відповіді, тим менше буде ризиків.

- **Критерій 5: Use of real-time security intelligence and intervention** – Кібербезпека в умовах відсутності локального SOC потребує автоматизованих механізмів моніторингу та розвідки загроз. Отже, платформа має бути здатна мінімізувати час між виявленням та відповіддю, навіть без залучення окремих спеціалістів.

4. Зробити порівняння оцінок зазначених платформ IAD за обраними критеріями. Результат порівняння відобразити у вигляді таблиці.

Назва платформи / Назва критерію	The Claroty Platform	Nozomi Networks Guardian	SCADAfence Platform
Ease of Deployment	4,4	4,7	5,0
Network segmentation	4,4	4,6	4,8
Quality of Technical Support	4,4	4,7	4,9
Timeliness of Vendor Response	4,4	4,7	4,9
Use of real-time security intelligence and intervention	4,3	4,8	4,7
Середня оцінка	**4,4**	**4,7**	**4,9**

5. Запропонувати відображення результатів в інфографічному вигляді (діаграма тощо) за допомогою будь-яких засобів візуалізації.