

The background features a photograph of a power substation with several tall metal towers and power lines, set against a bright orange and yellow sky. A white diamond-shaped grid pattern is overlaid on the entire image, creating a geometric design. The text is positioned on the left side of the image.

**Кібербезпека, як невід'ємна складова
захисту електромереж та підстанцій
в умовах воєнного часу**

Спікер: Максим Причина
Sales Engineer, ВАКОТЕСН

Найперша кіберзброя: «ядерний удар» Stuxnet або “Ефект Stuxnet” в кібербезпеці

THE WALL STREET JOURNAL. WSJ

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

Computer Worm Hits Iran Power Plant



Computer systems at Iran's first nuclear power plant have been infected with a potent worm capable of taking over their control systems. WSJ's Slobian Gorman discusses with Simon Conrab and Julia Angwin on Digita. Plus: China suffers an iPhone 4 shortage. Just a few days after sales started.

By **SLOBIAN GORMAN**
Updated Sept. 26, 2010 12:01 a.m. ET

AVAILABLE LOCKY

News Programs Opinion Investigations video

Topics: Business & Economy, Tech, Healthcare, Law, Science

Cyber attack 'targeted Iran'

Malignant software discovered on systems around world could have been designed to target Bushehr reactor, experts say.



Experts have suggested that the Bushehr nuclear reactor could have been a target of the virus.

The New York Times

Malware Hits Computerized Industrial Equipment

By **RYA RICHMOND** SEPTEMBER 24, 2010 8:41 PM

The technology industry is being rattled by a quiet and sophisticated malicious software program that has infiltrated factory computers.

The malware, known as Stuxnet, was discovered by VirusBlokAda, a Belarusian computer security company in July, at least several months after its creation.

Security experts say Stuxnet attacked the software in specialized industrial control equipment made by Siemens by exploiting a previously unknown hole in the Windows operating system. The malware is the first such attack on critical industrial infrastructure that sits at the foundation of modern economies.

It also displays an array of novel tactics — like an ability to steal design documents or even sabotage equipment in a factory — that suggest its creators are much more sophisticated than hackers whose work has been seen before. The malware casts a spotlight on several security weaknesses.

The Economist World politics Business & finance Economics Science & technology Culture

The Stuxnet outbreak

A worm in the centrifuge

An unusually sophisticated cyber-weapon is mysterious but important

Sep 30th 2010 | From the print edition

Timekeeper Like 197 Tweet



Tim Marrs

IT SOUNDS like the plot of an airport thriller or a James Bond film. A crack team of experts, assembled by a shadowy government agency, develops a cyber-weapon designed to shut down a rogue country's nuclear programme. The software uses previously unknown tricks to worm its way into industrial control systems undetected, searching for a particular configuration that matches its target—at which point it wreaks havoc by reprogramming the system, closing valves and shutting down pipelines.

BBC NEWS Sign in News Sport Weather Shop Earth Travel

Home Video World UK Business Tech Science Magazine Entertainment &

Technology

Stuxnet 'hit' Iran nuclear plans

○ 22 November 2010 Technology

The Stuxnet worm might be partly responsible for delays in Iran's nuclear programme, says a former UN nuclear inspections official.



Olli Hainonen, deputy director at the UN's nuclear watchdog until August, said the virus might be behind Iran's problems with uranium enrichment.

Discovered in June, Stuxnet is the first worm to target control systems found in industrial plants.

Iran has denied that delays to its nuclear plans were caused by Stuxnet.

SPIEGEL ONLINE INTERNATIONAL Sign in | Register

Front Page World Europe Germany Business Zeitgeist BeyondTomorrow Newsletter

English Site > World > Cyber Threats > Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War

Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War

By **Holger Stark**

The Mossad, Israel's foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet. The first digital weapon of geopolitical importance, it could change the way wars are fought -- and it will not be the last attack of its kind.

1 August 08, 2011 - 03:04 PM

Print

Feedback

Comment

f Share t Twitter @ Email +

The complex on a hill near an interchange on the highway from Tel Aviv to Haifa is known in Israel simply as "The Hill." The site, as big as several soccer fields, is sealed off from the outside world with high walls and barbed wire -- a modern fortress that symbolizes Israel's fight for survival in the Middle East. As the headquarters of Israel's foreign intelligence agency, the Mossad, this fortress is strictly off-limits to politicians and journalists alike. Ordinarily, it is the Mossad that makes house calls, and not the other way around.

From the Magazine

Ukraine's cyber war

BBC NEWS

3/2022, 12:02 AM



Ukraine's cyber war
BBC NEWS

9:06

How Ukraine and Russia are rewriting the rules of cyber war - BBC News
165 тыс. просмотров • 1 месяц назад

BBC News

When Russia began its full-scale invasion of Ukraine, a second less visible battle got underway. Armies of vic

Intro | Kill Milk | NATO websites | Vigilante groups | Hacking | Michael Fedorov | Ukraines cy

RUSSIA CYBER ATTACKS

ACCESS GRANTED

3:47

How important is cyber warfare in the Russia-Ukraine conflict?
6,9 тыс. просмотров • 9 месяцев назад

Forces News

We evaluate what cyber attacks by both Russia and Ukraine have told us about the strateg

UKRAINE WAR CYBER WARFARE

2:58

Ukraine war: A virtual testing ground for cyber-warfare
12 тыс. просмотров • 10 месяцев назад

Al Jazeera English

Experts say the war in Ukraine has become a virtual testing ground for

Industroyer2: How Ukraine avoided another blackout attack

A Black Hat 2022 session explained how the latest attack on Ukraine's energy grid was thwarted this spring, thanks to quick responses and timely sharing of threat data.

The Subpostmasters



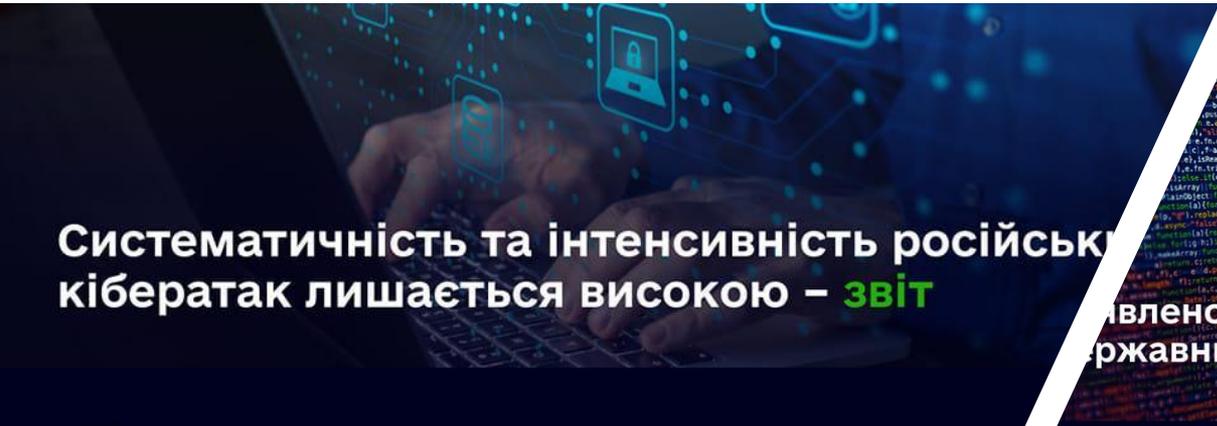
Кабінет Міністрів України ухвалив постанову за 2022 році кількість зареєстрованих об'єктів критичної інфраструктури, потерпілих від кіберінцидентів виросла майже втричі – **звіт**



Державна служба спеціального зв'язку та захисту інформації України



Державна служба спеціального зв'язку та захисту інформації України



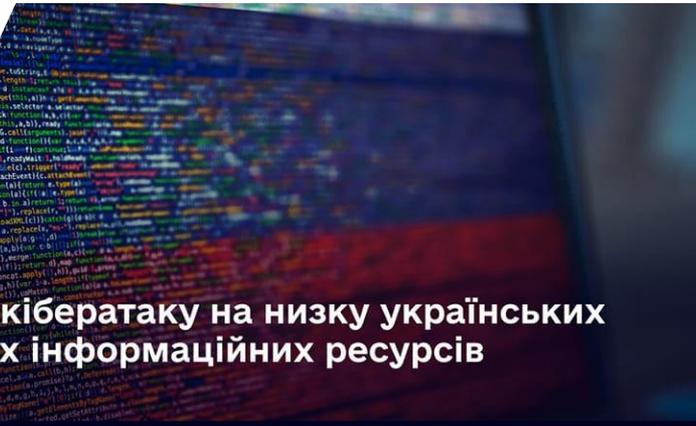
Систематичність та інтенсивність російських кібератак лишається високою – **звіт**



Державна служба спеціального зв'язку та захисту інформації України

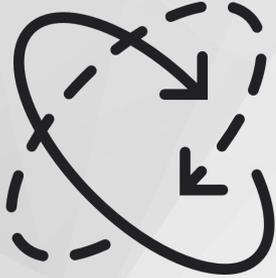


Державна служба спеціального зв'язку та захисту інформації України



Відбулося понад 10 тисяч кібератак на низку українських державних інформаційних ресурсів

3 ключові драйвери кібербезпеки АСУ ТП



OT та IT зближуються

- Уніфікація платформ
- Розвиток віртуалізації
- Зближення інфраструктур
- Збільшена поверхня атаки
- Обмін загрозами



Зловмисники мають високу мотивацію

- Геополітична агресія
- Фінансова вигода (програми-вимагачі)
- Серйозні втрати (імідж)
- Ідеологічні причини
- Хактивізм



АСУ ТП є легкою мішенню

- Недостатній захист периметру
- Слабка або відсутня автентифікація
- Людський фактор
- ІБ у зародковому стані

Чому кіберзахист НЕ є універсальним?

ІТ безпека

Стандартні протоколи на основі IP
(наприклад, TCP/IP, HTTP)

Непередбачувана поведінка
(люди)

Активне сканування
ОК

Схвалюються регулярні виправлення та оновлення ОС

ОТ безпека

Стандартні та власні промислові протоколи
(наприклад, GE SRTP, Siemens S7, IEC)

Передбачувана поведінка
(машина-машина)

Активне сканування призводить до простою

Виправлення спричиняє простої, а оновлення ОС змушують перезаписувати додатки SCADA

Проблема 1:

Як відслідковувати всі загрози в промисловій мережі, і реагувати до того, як вони нанесуть шкоду?





NOZOMI
NETWORKS



Nozomi Networks



Глобальна база клієнтів
7.6K+ впроваджень



82M+ контрольованих пристроїв
у пов'язаних OT/IoT мережах



Масштабна присутність
на 6 континентах



Глобальна експертиза
Всесвітня мережа партнерів і
понад 1500 сертифікованих
професіоналів



Участь в безпеці найбільших організацій світу

9 із Топ 20
Нафта та газ

7 із Топ 10
Фармацевтика

5 із Топ 10
Видобуток

5 із Топ 10
**Енергетичні
послуги**



Хімія



Електроенергетика



Виробництво



Видобування



Нафта та газ



Фармацевтика



Гідроенергетика



Аеропорти



Автомобільна промисловість



Автоматизація будівель



Продукти харчування та
роздрібна торгівля



Логістика



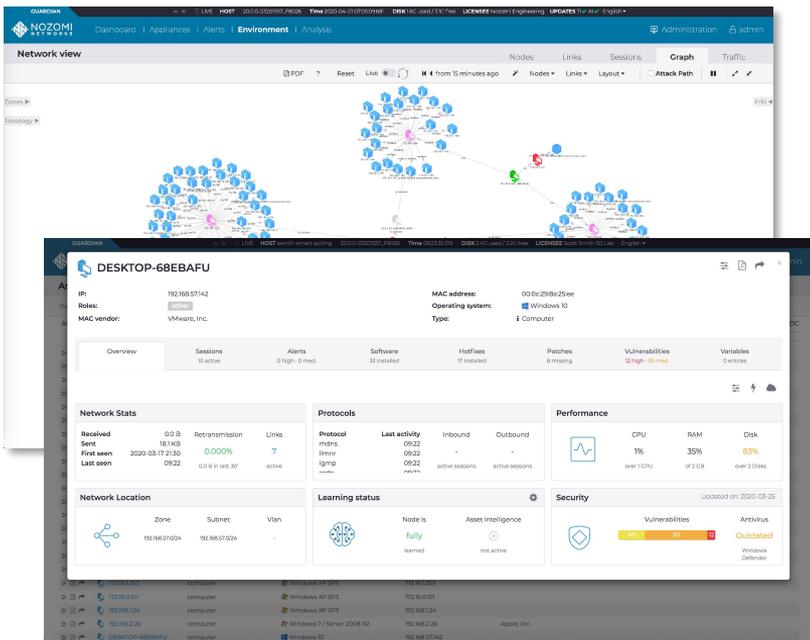
Розумні міста



Перевезення

ВИДИМІСТЬ

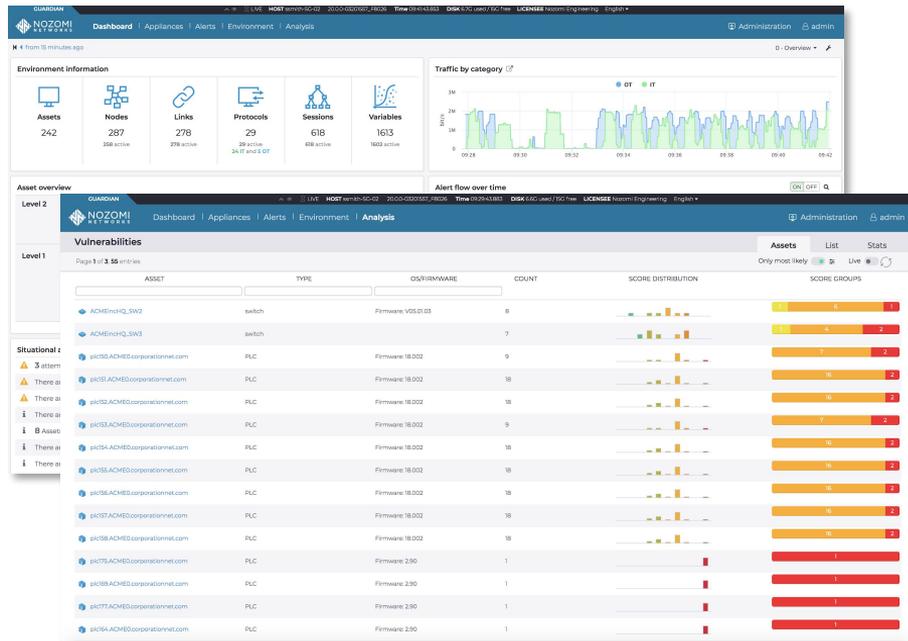
Що є у вашій мережі та як воно працює



- Виявлення активів та візуалізація мережі

ВИЯВЛЕННЯ

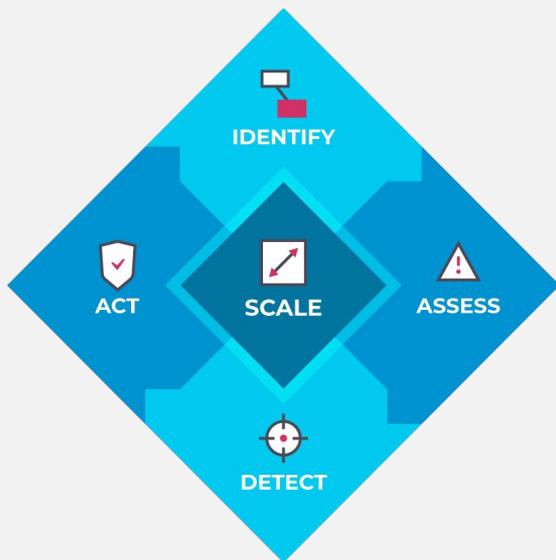
Кіберзагрози, ризики та аномалії для швидшого реагування



- Оцінка вразливості та моніторинг ризиків
- Виявлення аномалій і загроз

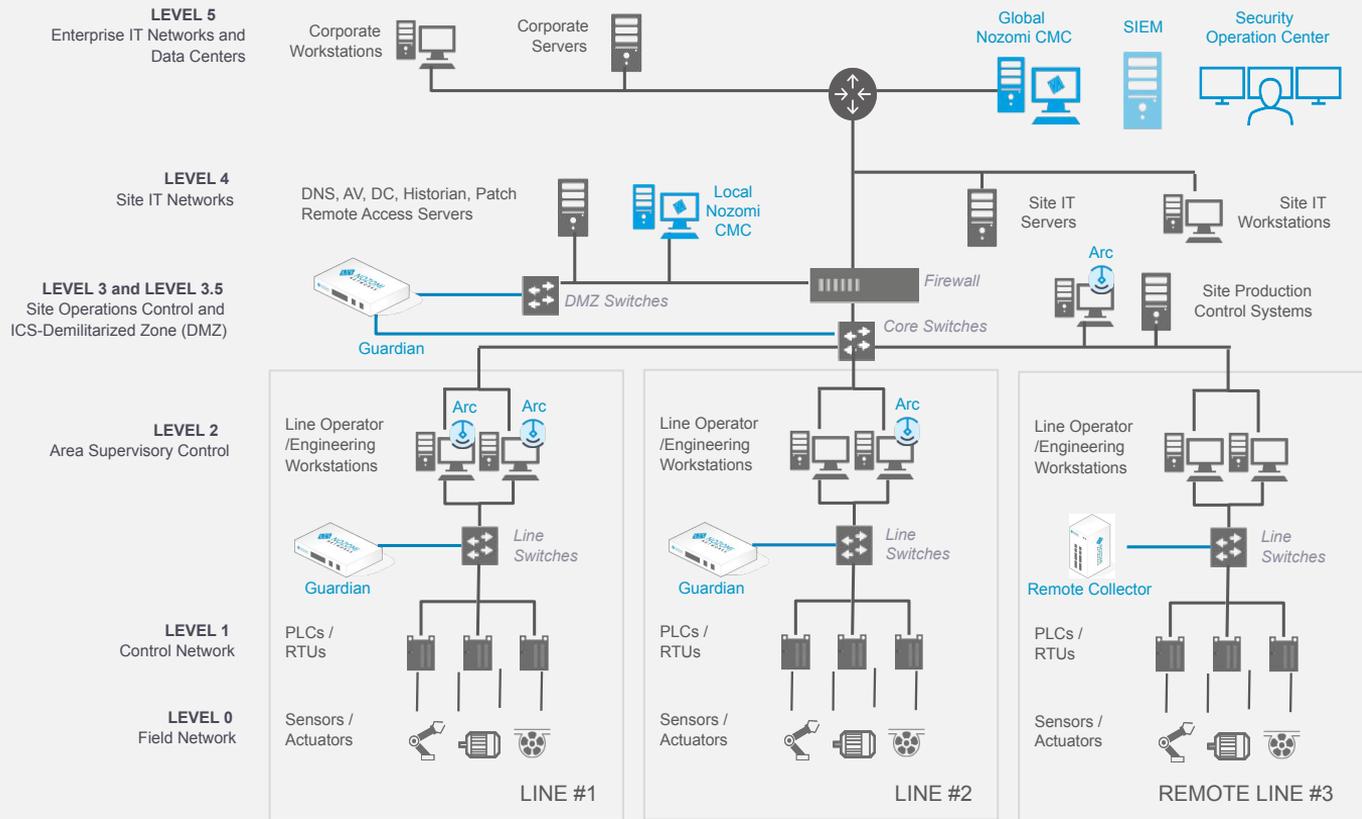
Guardian від Nozomi Networks

Централізована безпека та видимість ОТ та IoT для всіх сайтів Visibility



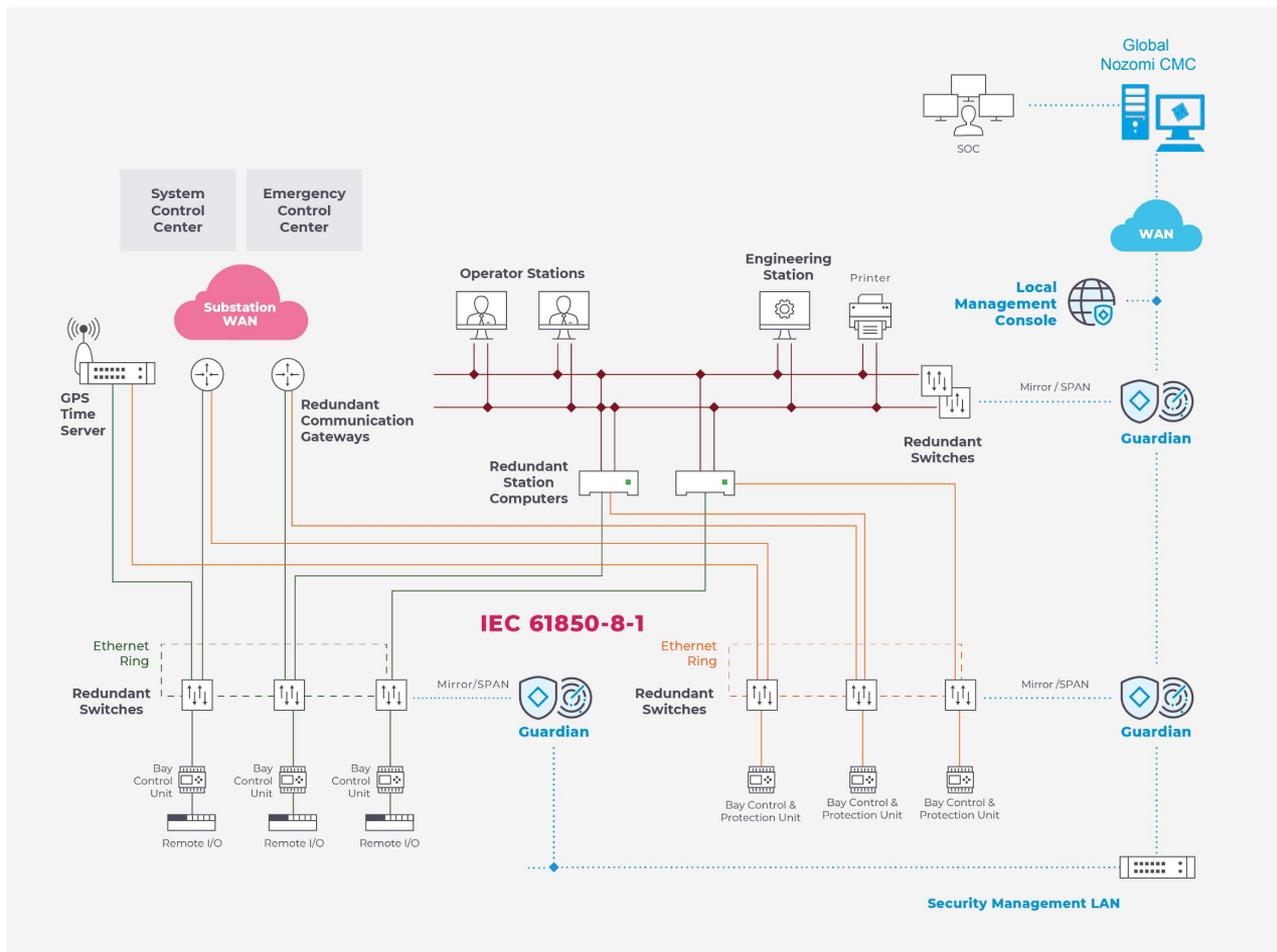
- | | |
|----------------------|--|
| Ідентифікація | Виявлення активів і візуалізація мережі |
| Оцінка | Оцінка вразливості та моніторинг ризиків |
| Виявлення | Виявлення аномалій і загроз |
| Реагування | Інформаційні панелі та інструменти для швидкого розслідування інцидентів |
| Масштабування | Уніфікована безпека для тисяч розподілених точок |

Приклад розгортання

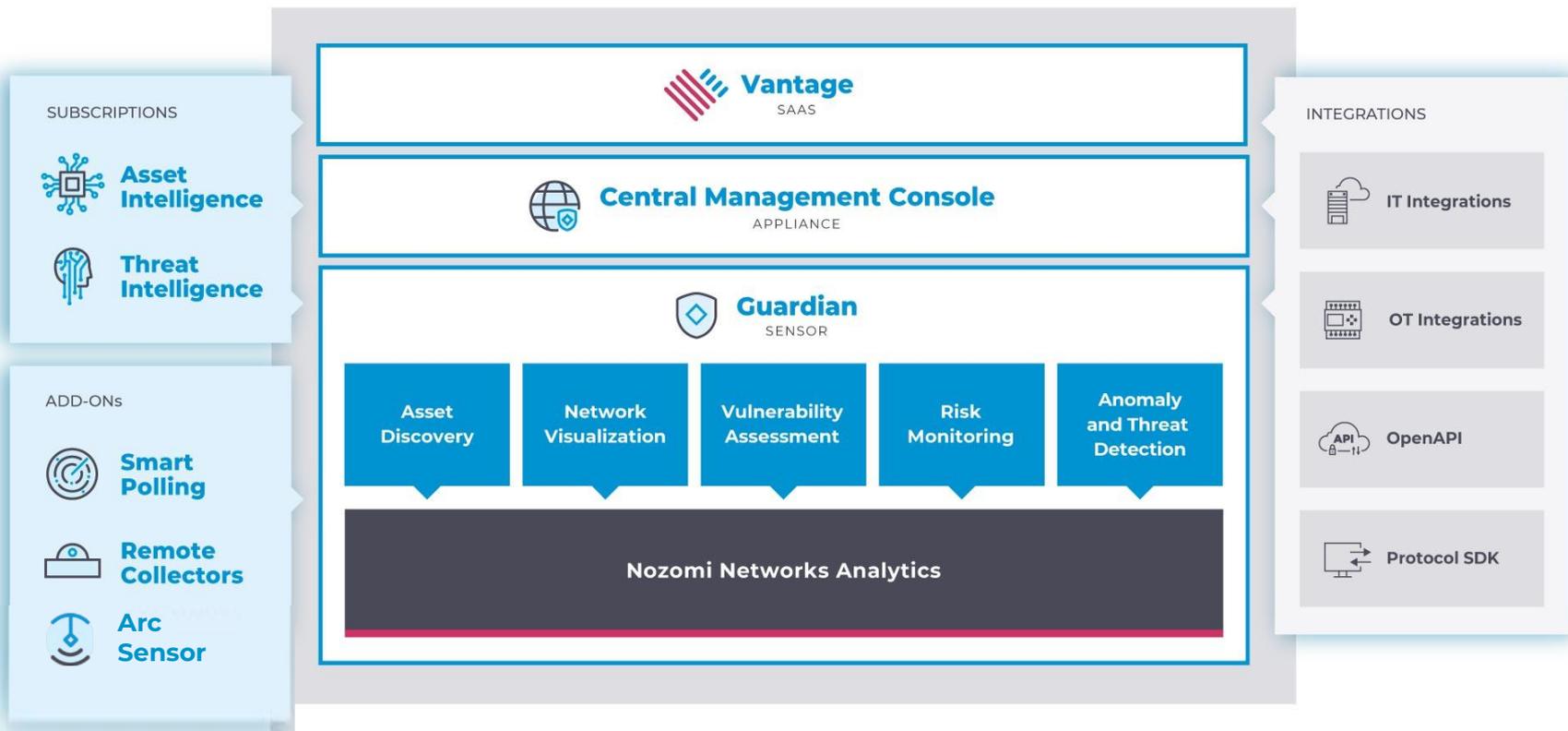


- ✓ **Глобальна центральна консоль керування** для збору сповіщень і інформації про активи, що надходять із різних точок, розповсюджених по всьому світу.
- ✓ **Локальна центральна консоль керування** для єдиного перегляду кожної з точок
- ✓ Пристрій **Guardian** середнього / високого рівня для контролю зв'язку, що проходить через ключові комутатори та DMZ
- ✓ Невеликий/середній пристрій **Guardian** (можливий і захищений формфактор) для моніторингу зв'язку на рівні 2
- ✓ **Колектор** для віддаленого розташування
- ✓ **Примітка:** ефективну кількість і розмір пристроїв можна визначити лише після перегляду топології мережі, що розглядається

Приклад архітектури розгортання в енергетичній інфраструктурі



Nozomi Networks Портфоліо рішень



Проблема 2:

Як безпечно передавати дані з промислової мережі не порушуючи ізоляцію?



Рішення WATERFALL SECURITY

100% ВИДИМОСТІ ЗІ
СТРОГИМ КОНТРОЛЕМ
ДОСТУПУ



Проблематика безпеки ОТ

ІНТЕГРАЦІЯ ІТ/ОТ – ПЕРЕВАГИ ТА РИЗИКИ



Неприйнятні ризики

Хмарне підключення збільшує доступність
Побоювання про безпеку та захист обладнання
Параметри обмежень контролю технічних змін
Фізичні наслідки компрометації

vs.

Бізнес потреби

Прогнозне обслуговування та аналітика великих даних
Нова автоматизація видимості в ОТ
Відповідність програмі безпеки підприємства
Підвищена ефективність та динамічність

Компанія WATERFALL

Заснована в 2007

Продажі та впровадження
в Європі, Америці, Азії

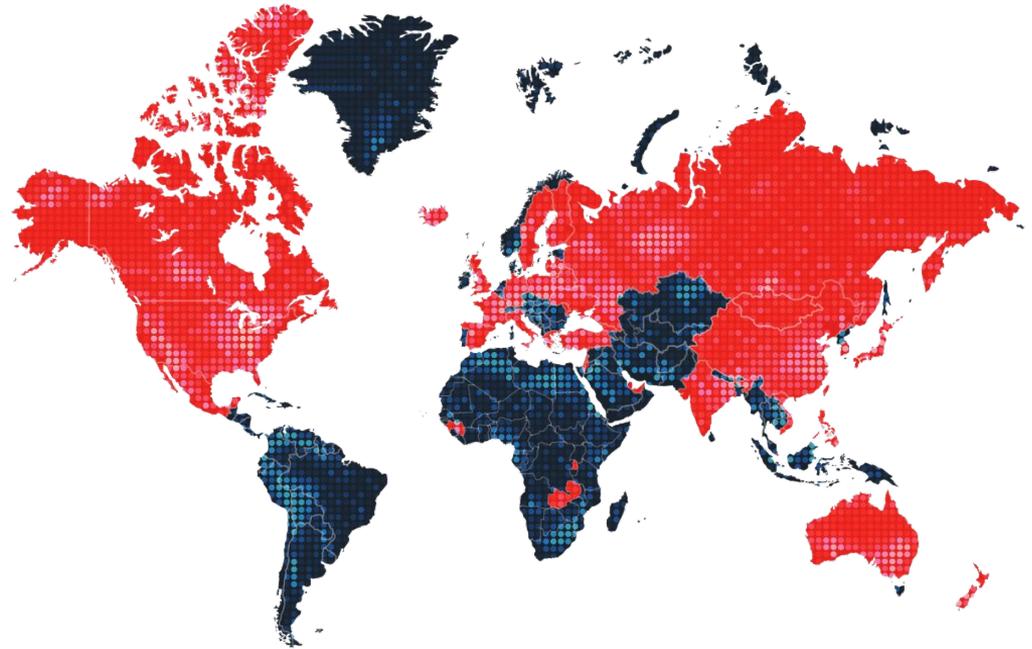
Global Installed Base

Головний офіс в Ізраїлі

Всі види критичної інфраструктури

Співпраця з глобальними партнерами

Зареєстровані патенти в США



ЕЛЕКТРОЕНЕРГЕТИКА



АЕРОПОРТИ



НАФТА ТА АГЗ



ГІДРОЕНЕРГЕТИКА

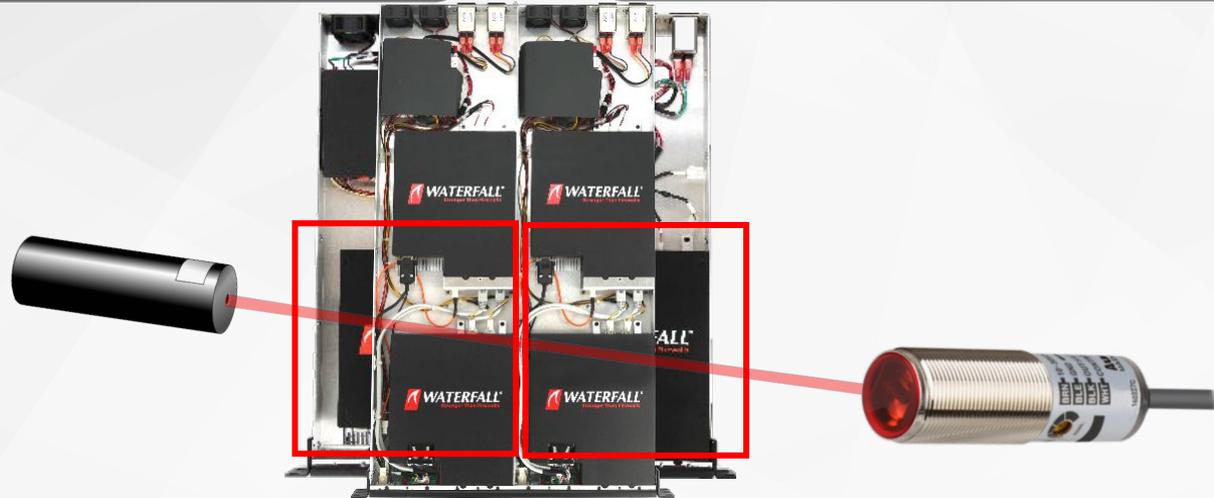
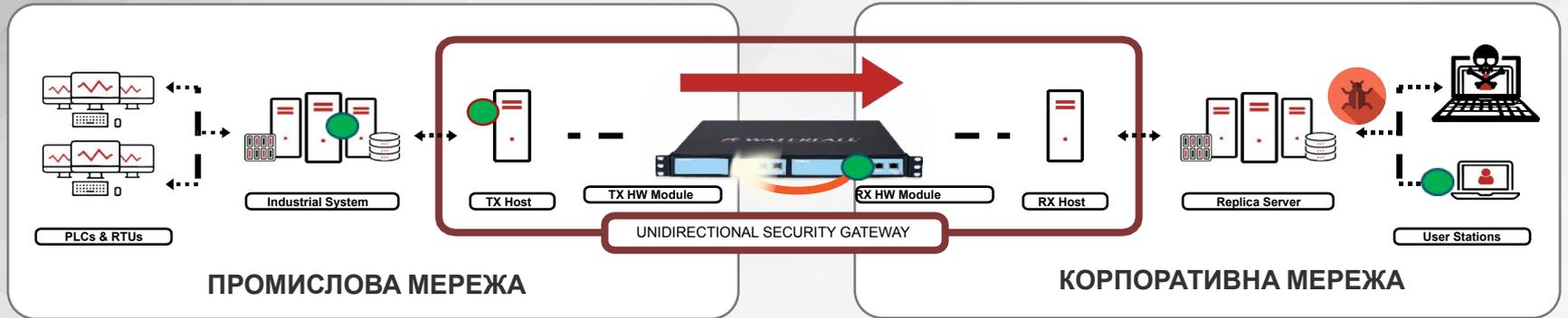


ЗАЛІЗНИЧНІ
СПОЛУЧЕННЯ



ВИРОБНИЦТВО

Однонаправлений шлюз



Однонаправлений шлюз WATERFALL

Модульний, Продуктивний, Гнучкий

- Нуль внутрішніх перехресних з'єднань – надійна та сертифікована односпрямована техніка
- Фізично розділені промислові та корпоративні компоненти
- DIN-рейка та форм-фактори 1U з однаковою потужністю та функціональністю
- Подвійні джерела живлення на кожній стороні відправлення та приймання

Потужні опції – форм-фактори для будь-яких потреб



DIN Rail



WF-500 Compact



WF-500 Standard



1U Rack Mount

ПОРТФОЛІО WATERFALL SECURITY

Waterfall for IDS:

Односпрямовані рішення для систем Intrusion Detection Systems (IDS)

Waterfall FLIP:

Реверсивна односпрямована технологія та віддалений доступ

Remote Screen View:

Безпечна віддалена підтримка односпрямованих захищених мереж

Secure Bypass:

Планова та екстрена підтримка персоналом на місці

Unidirectional CloudConnect:

Безпека для хмарних сервісів

Waterfall BlackBox:

Безпечне сховище журналів



Кіберзагрози та виклики для енергетичного сектору існуватимуть завжди



Автоматизація інвентаризації активів

Створення точної інвентаризації всіх активів АСУ ТП та підтримка її в актуальному стані досить складно, але **НЕОБХІДНО ТА МОЖЛИВО**



Розуміння вразливостей системи

Знання постачальників RTU, PLC та інших пристроїв, що можуть бути під загрозою, допомагає зосередити зусилля з безпеки OT/IoT.



Виявлення крадіжки облікових даних OT/IoT

Щоб запобігти несанкціонованому доступу до мережі, необхідно негайно помічати зловживання обліковими даними та унеможливити преривання в критичну мережу на фізичному рівні.



Вирішення OT/IoT кіберінцидентів

Найкращий спосіб зменшити операційний ризик — швидко виявити випадкові та ненавмисні кіберінциденти.

**ДЯКУЮ ЗА
УВАГУ**