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

Спікер: Максим Причина
Sales Engineer, BAKOTECH

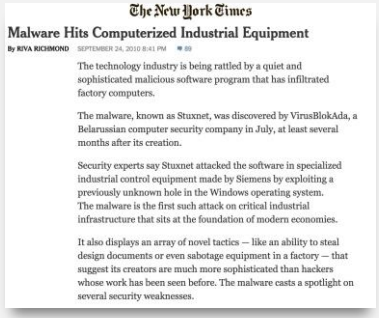
Найперша кіберзброя: «ядерний удар» Stuxnet або “Ефект Stuxnet” в кібербезпеці


THE WALL STREET JOURNAL.

Computer Worm Hits Iran Power Plant


Cyber attack 'targeted Iran'

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


The New York Times

Malware Hits Computerized Industrial Equipment

By RIVA 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 Belarussian 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.


BBC NEWS

Technology

Stuxnet 'hit' Iran nuclear plans

22 November 2010 | Technology

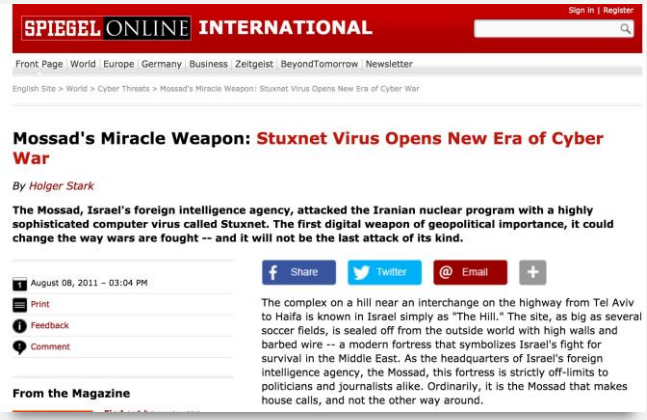
The Stuxnet worm might be partly responsible for delays in Iran's nuclear programme, says a former UN nuclear inspections official.

Olli Heinonen, 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.

Iran has always denied that Stuxnet has caused delays to its nuclear power plans


SPIEGEL ONLINE INTERNATIONAL

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.

August 08, 2011 – 03:04 PM

Print

Feedback

Comment

Share 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


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.

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 vi

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

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 strate

Ukraine war: A virtual testing ground for cyber-warfa

12 тыс. просмотров • 10 месяцев назад

Al Jazeera English

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

3/2022, 12:02 AM

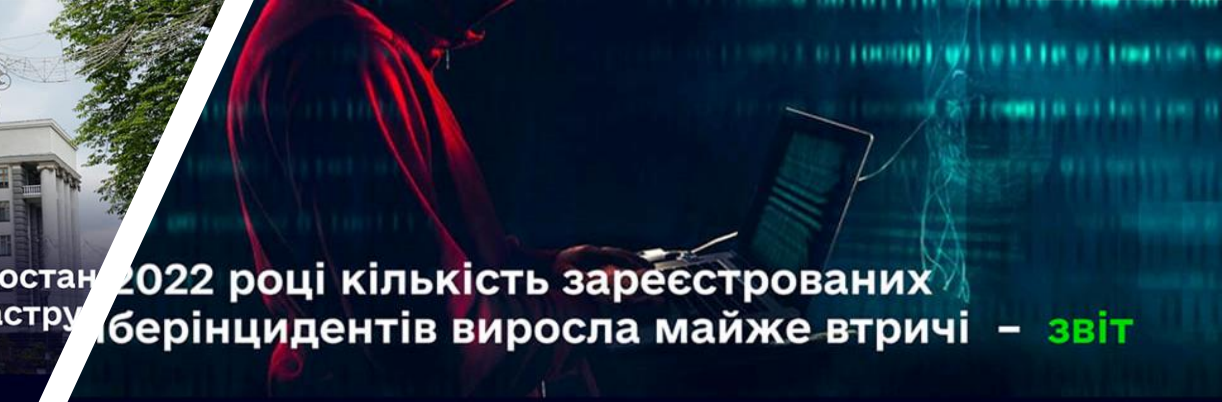
NEWS

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.

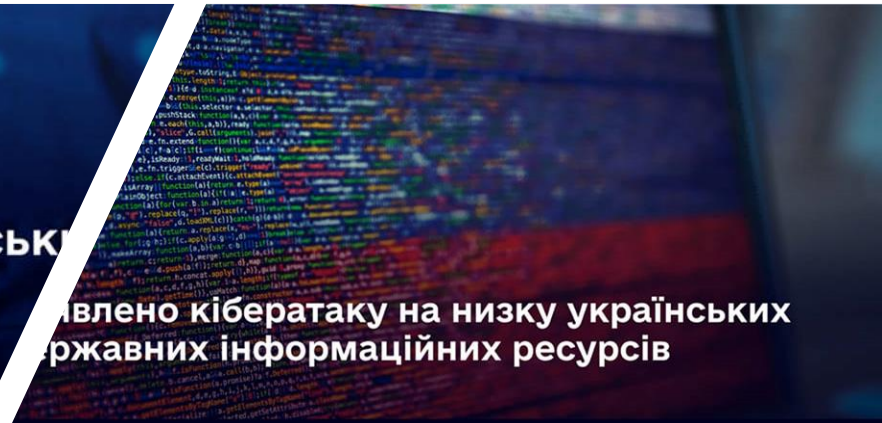
The Subpostmasters

Державна служба
спеціального зв'язку та захисту
інформації України



Державна служба
спеціального зв'язку та захисту
інформації України

Державна служба
спеціального зв'язку та захисту
інформації України



Державна служба
спеціального зв'язку та захисту
інформації України

3 ключові драйвери кібербезпеки АСУ ТП

ОТ та ІТ 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?

IT безпека	OT безпека
Стандартні протоколи на основі IP (наприклад, TCP/IP, HTTP)	Стандартні та власні промислові протоколи (наприклад, GE SRTP, Siemens S7, IEC)
Непередбачувана поведінка (люди)	Передбачувана поведінка (машина-машина)
Активне сканування ОК	Активне сканування призводить до простою
Схвалюються регулярні виправлення та оновлення ОС	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

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

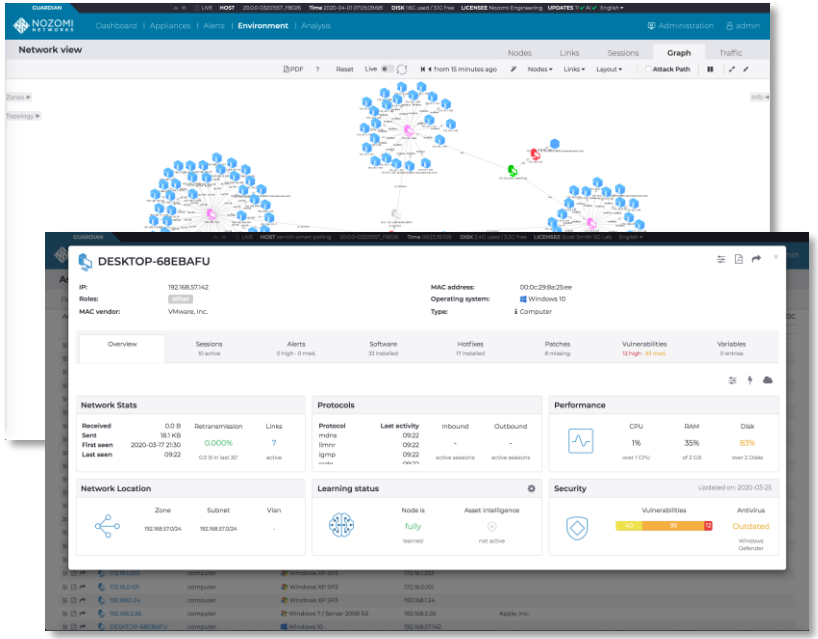

Логістика


Розумні міста


Перевезення

ВИДИМІСТЬ

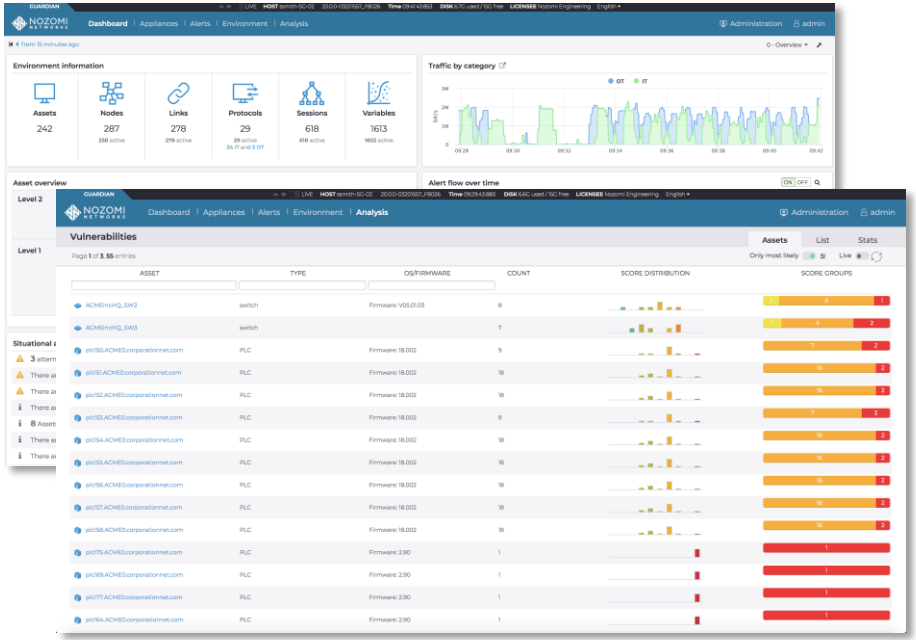
Що є у вашій мережі та як воно працює



- Виявлення активів та візуалізація мережі

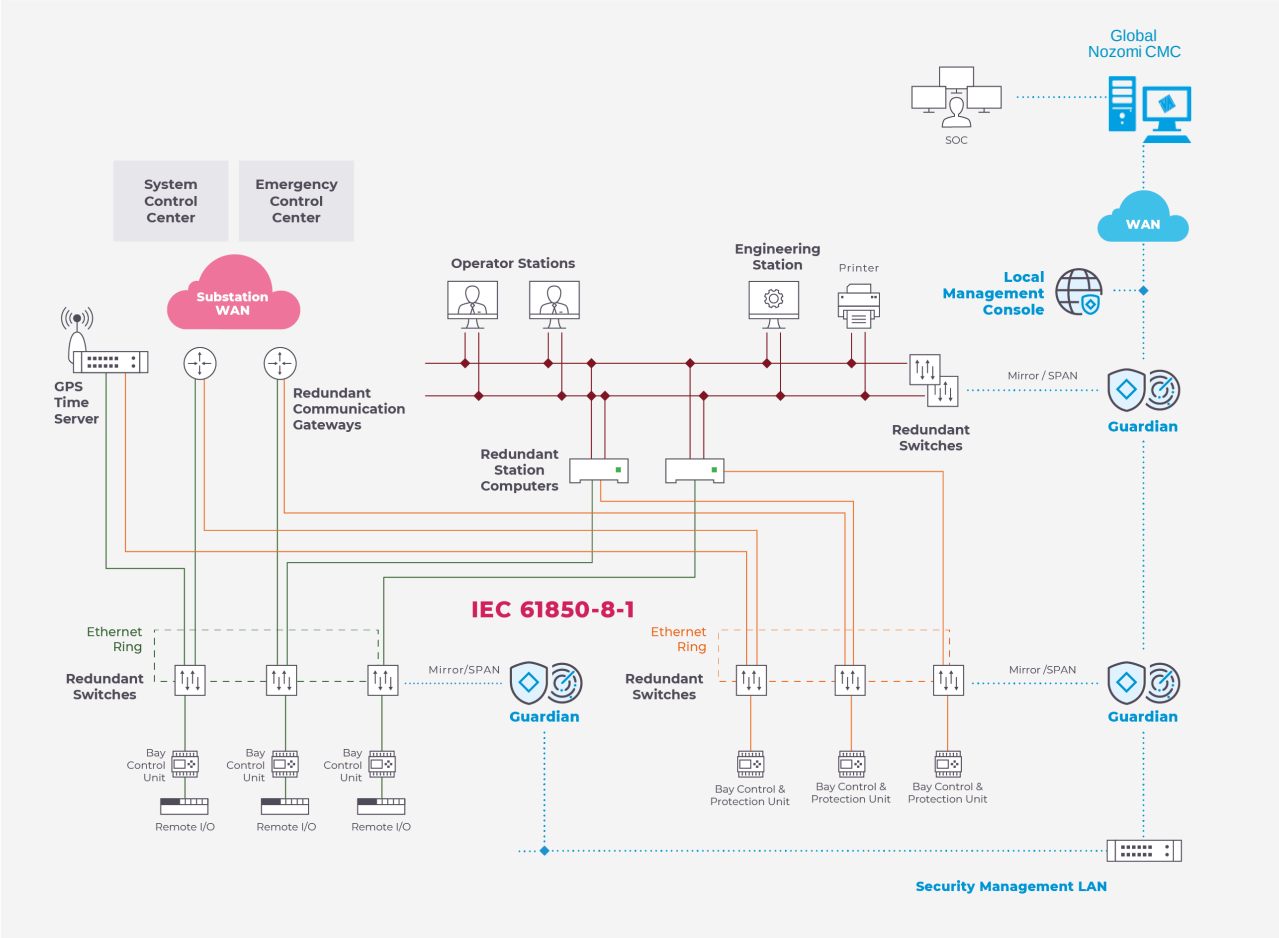
ВИЯВЛЕННЯ

Кіберзагрози, ризики та аномалії для швидшого реагування

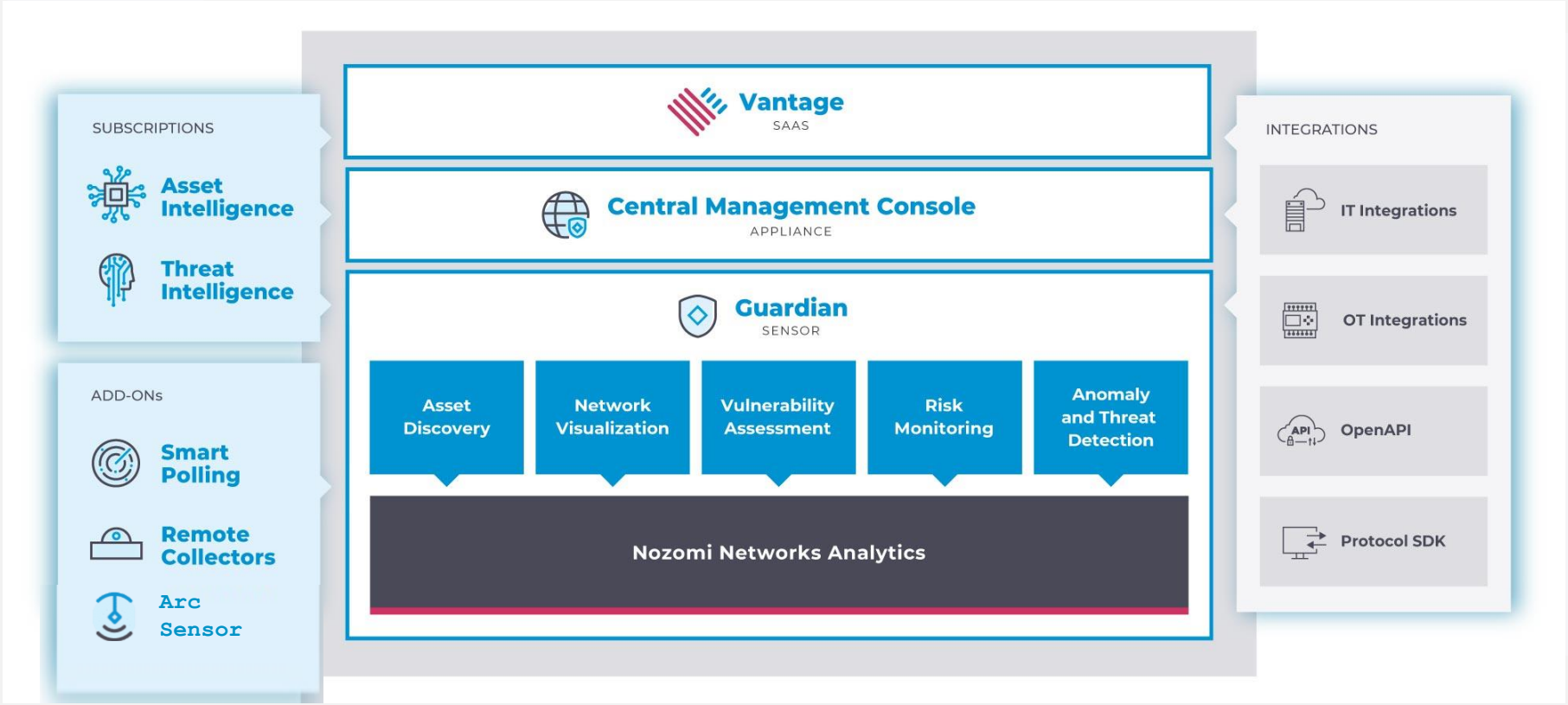


- Оцінка вразливості та моніторинг ризиків
- Виявлення аномалій і загроз

Приклад архітектури розгортання в енергетичній інфраструктурі



Nozomi Networks Портфоліо рішень



Проблема 2:
Як безпечно передавати дані з промислової мережі не порушуючи ізоляцію?

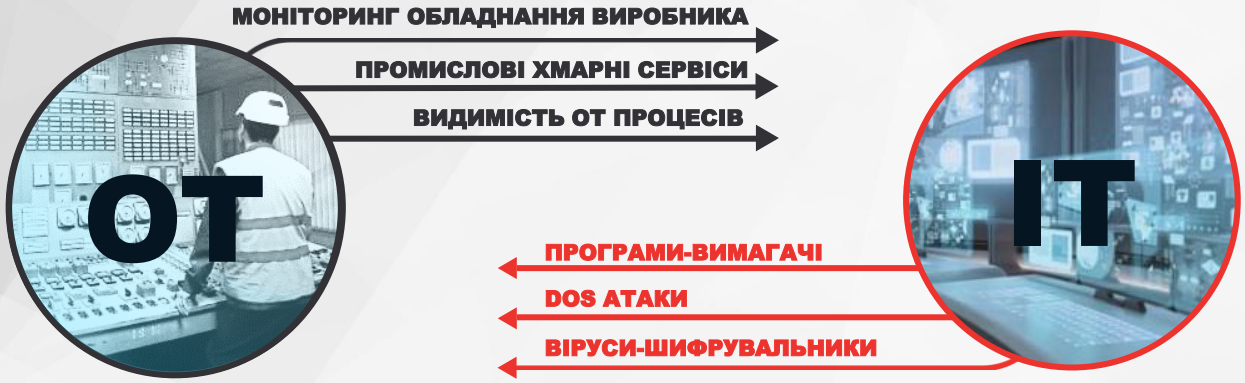
WATERFALL®
Stronger Than Firewalls

Рішення WATERFALL SECURITY

100% ВИДИМОСТІ ЗІ СТРОГИМ КОНТРОЛЕМ ДОСТУПУ

Проблематика безпеки ОТ

ІНТЕГРАЦІЯ IT/OT – ПЕРЕВАГИ ТА РИЗИКИ



Неприйнятні ризики

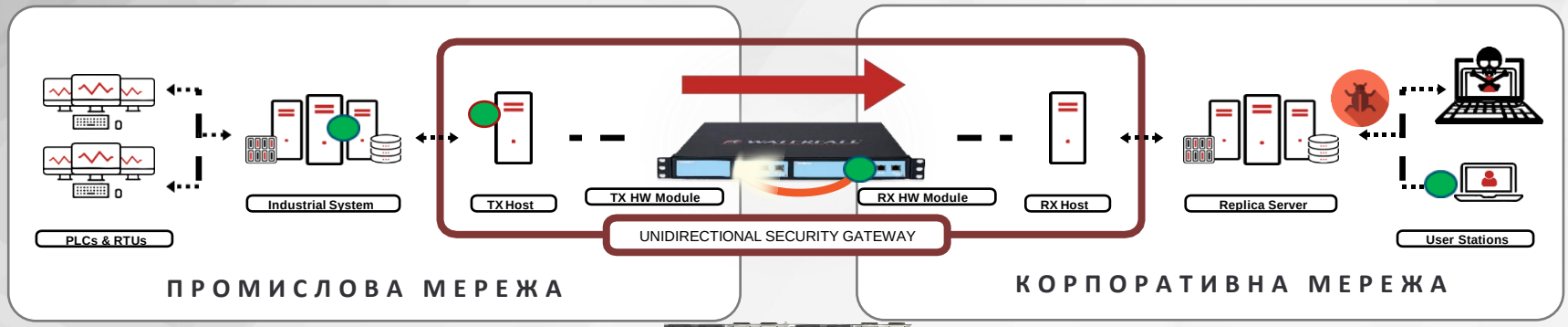
Хмарне підключення збільшує доступність
Побоювання про безпеку та захист обладнання
Параметри обмежень контролю технічних змін
Фізичні наслідки компроментації

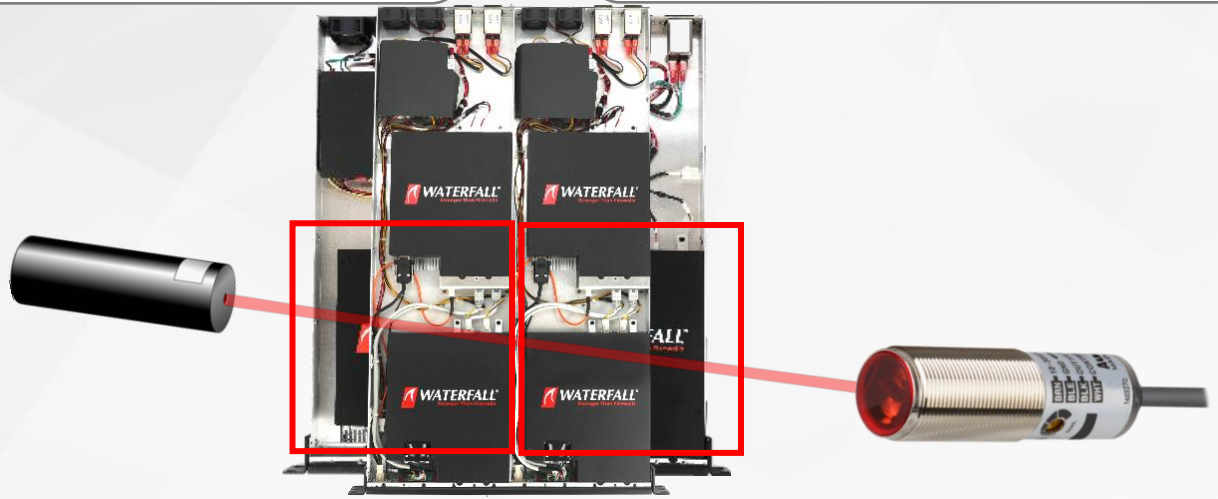
VS.

Бізнес потреби

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

Однонаправлений шлюз





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

WATERFALL®
Stronger Than Firewalls

Кіберзагрози та виклики для енергетичного сектору існуватимуть завжди

Автоматизація інвентаризації активів

Створення точної інвентаризації всіх активів АСУ ТП та підтримка її в актуальному стані доволі 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 проникнення в критичну мережу на фізичному рівні.

Вирішення OT/IoT кіберінцидентів

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

ДЯКУЮ ЗА УВАГУ