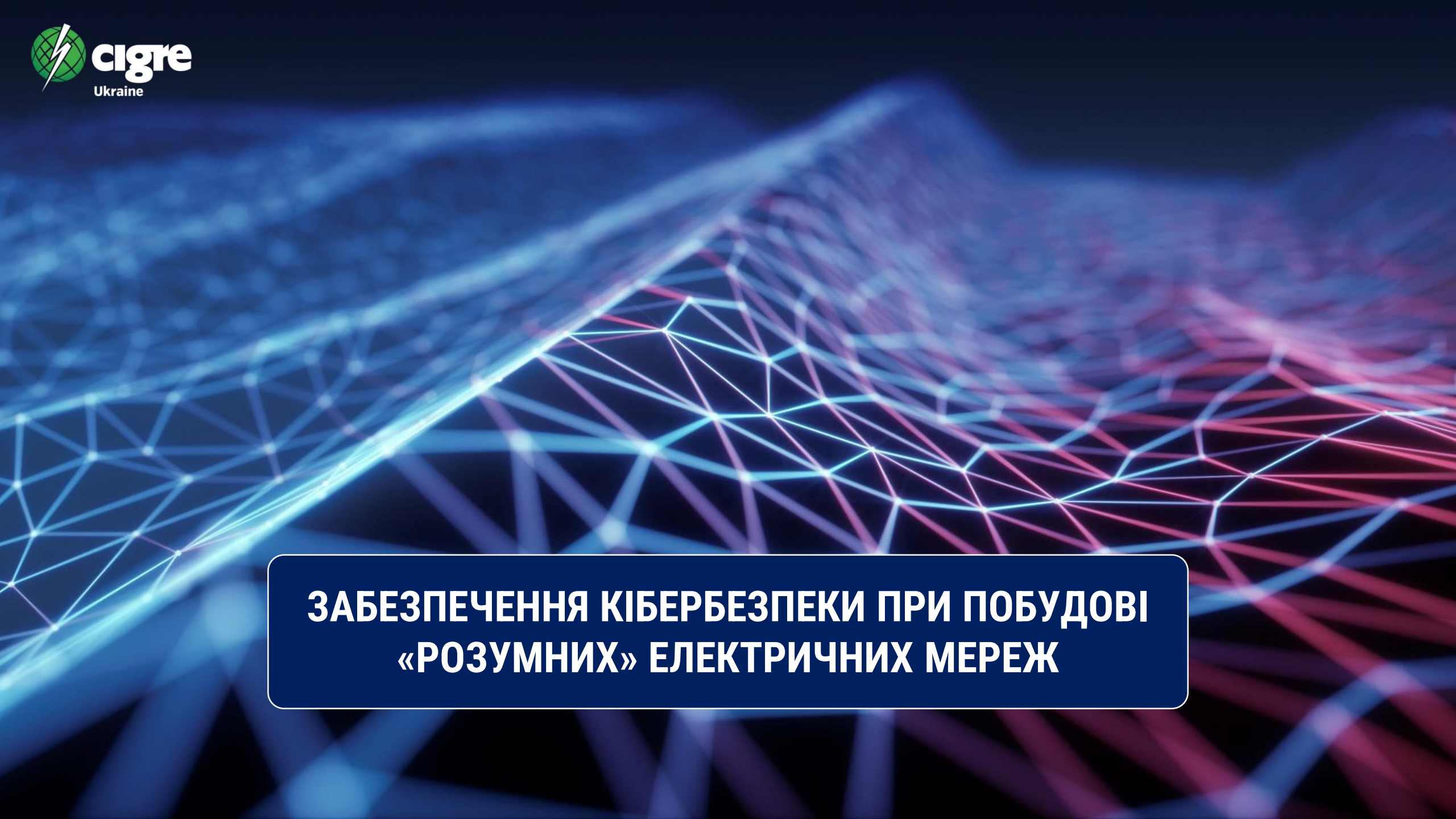

cigre
Ukraine
ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРИ ПОБУДОВІ
«РОЗУМНИХ» ЕЛЕКТРИЧНИХ МЕРЕЖ

СТВОРЕНА РОБОЧА ГРУПА

«КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ЕЛЕКТРОЕНЕРГЕТИЦІ»

ОСНОВНІ ЗАДАЧІ ГРУПИ

- Експертна підтримка і оцінка потенційних загроз та участь у розробці галузевих вимог до організації ефективних процесів кіберзахисту всіма учасниками ринку генерації, розподілу та споживання електроенергії
- Система незалежної оцінки стану технологічної та інформаційної захищеності об'єктів критичної інфраструктури (в першу чергу). Створення на базі СІГРЕ-Україна центру підготовки та професійної сертифікації таких спеціалістів
- Організація взаємодії з національними розробниками систем управління, а також організація тематичної співпраці з провідними університетами України у питаннях підготовки кадрів та підтримки наукових досліджень
- Просвітницька діяльність, публічні та спеціалізовані інформаційні заходи

ВИКЛИКИ СУЧАСНОСТІ

- Користувачі зацікавлені в сталому отриманні енергії певної якості відповідно до поточного попиту та економічної доцільності. Системи типу Microgrid – пріоритетне рішення для цього
- Енергогенеруюче та енергорозподільче обладнання має мережеві інтерфейси, які підключаються до IP-мереж користувача
- Користувач в багатьох випадках не здатен фахово оцінити рішення інсталяторів такого обладнання з точки зору кібербезпеки
- Результати кібератак на інсталяції microgrid Користувачів впливають не тільки на їх роботу, але і можуть спричинити негативні впливи на роботи розподільчих мереж, що забезпечують їх зовнішнім живленням

ЩО РОБИТИ?

- Необхідно створити інститут незалежних консультантів/аудиторів по питаннях оцінки стану кібербезпеки та формуванню рекомендацій по їх вдосконаленню до рівня вимог національних та міжнародних стандартів.
- Організувати профільне підвищення кваліфікації проектантів та інсталяторів систем типу Microgrid

ПОТЕНЦІЙНІ ОБ'ЄКТИ ДЛЯ АТАК

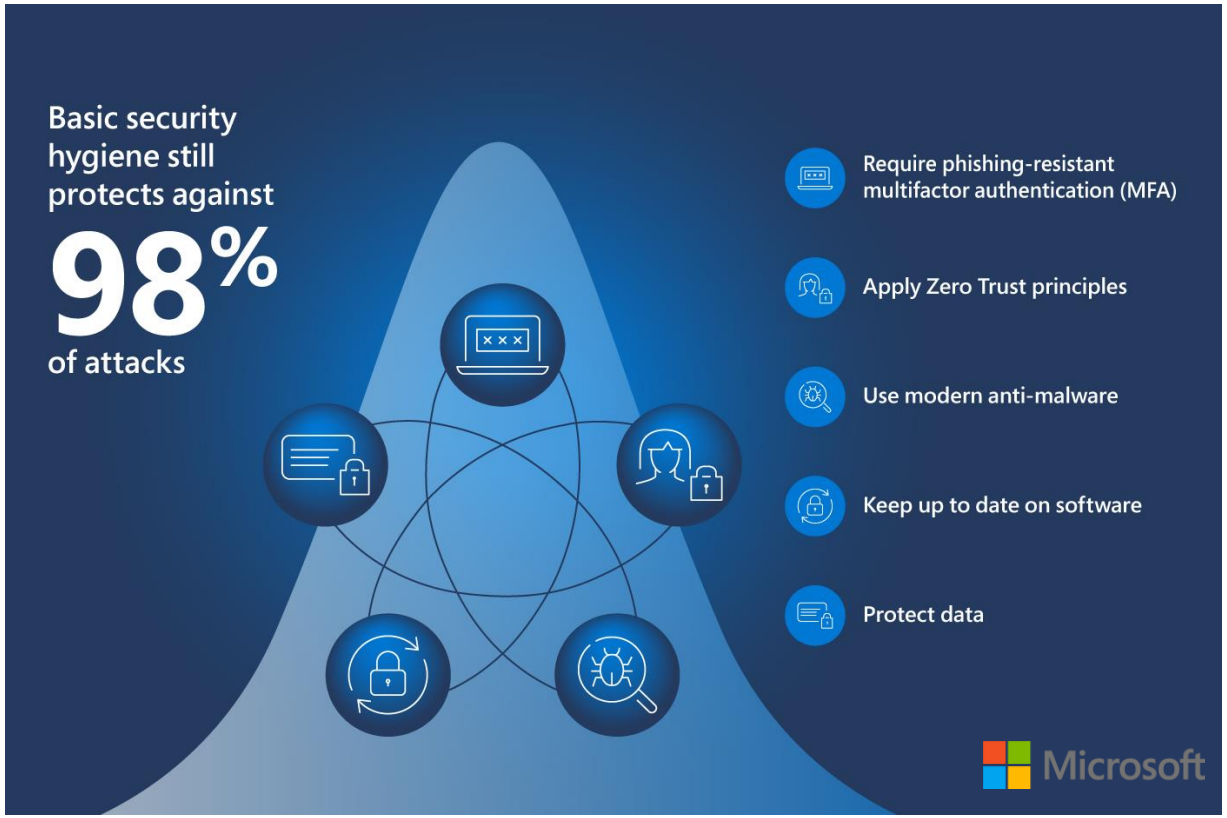
- Інформаційні системи, що Користувач використовує для свої бізнес-процесів
- Системи керування інженерним обладнанням – технологічні процеси, електропостачання, тепло-/холодозабезпечення, водозабезпечення, каналізація, електромеханічне обладнання, тощо
- Системи технічної безпеки – відеоспостереження, контроль доступу, охоронна сигналізація, пожбезпека
- Мережі IoT, які інтегруються з інформаційними та технологічними системами керування
- Мережі публічного доступу до ресурсів Internet на території Користувача

Складність забезпечення кіберзахисту для таких об'єктів полягає в тому, що:

- Для комплексного управління перелічені системи пов'язані між собою певними потоками даних
- Інженерне та технологічне обладнання у своєму складі може мати різні протоколи обміну даним, які інтегруються в IP-мережу через спеціальні шлюзи
- Інтеграція з IoT пристроями через хмарні інтерфейси
- Для ефективного та своєчасного обслуговування активно використовується дистанційний доступ профільних сервіс-інженерів.

ВПРОВАДЖУЙТЕ ПРИНЦИПИ КІБЕРГІГІЄНИ

Кібергігієна - це набір процедур, які зменшують ризик атаки



2022 Microsoft Digital Defense Report

Головні елементи базової кібергігієни на думку MIcrosoft такі:

- Використовуйте багатофакторну аутентифікацію, стійку до фішингу:
- Застосуйте принципи Zero Trust
- Використовуйте сучасні антивіруси
- Регулярно оновлюйте програмне забезпечення, операційні системи та системні прошивки.
- Захищайте дані - Інвентаризуйте та класифікуйте дані, встановлюйте та здійснюйте контроль доступу, виявляйте внутрішні ризики за допомогою відповідних фахівців та навчання користувачів

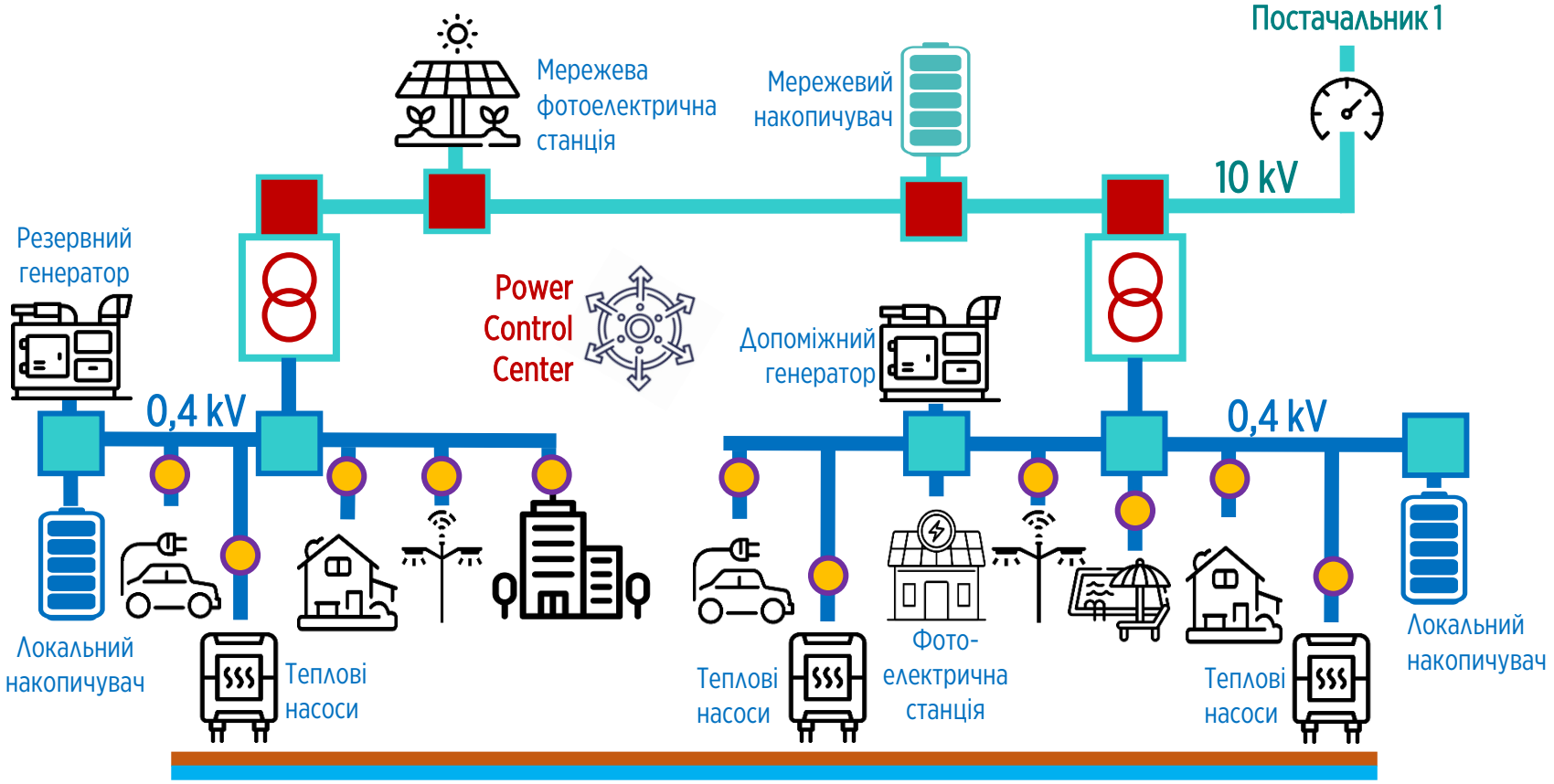
Правила КІБЕРГІГІЄНИ

1. Визначте та задайте пріоритети ключовим послугам, продуктам та їх допоміжних активів.
2. Визначайте, задайте пріоритети та реагуйте на ризики для ключових послуг і продуктів організації.
3. Створіть план реагування на інцидент.
4. Проводьте навчальні та просвітницькі заходи з питань кібербезпеки.
5. Встановіть мережеву безпеку та моніторинг.
6. Контролюйте доступ на основі найменших привілеїв і підтримуйте облікові записи доступу користувачів.
7. Керуйте технологічними змінами та використовуйте стандартизовані безпечні конфігурації.
8. Впроваджуйте керування для захистом та відновленням даних.
9. Запобігайте та відслідковуйте вплив зловмисного програмного забезпечення.
10. Контролюйте кібер ризики, пов’язані з постачальниками та зовнішніми факторами.
11. Виконуйте моніторинг кіберзагроз і вразливостей, виправляйте їх.

ВПРОВАДЖУЙТЕ СТРАТЕГІЇ ЗАХИСТУ

Стратегія ZERO TRUST **адаптована до** ISA/IEC62443 Industrial Security standards

- Інформаційні системи, орієнтовані на бізнес-процеси
- Мережі систем фізичної безпеки
- Мережі публічного доступу
- Хмарні інтерфейси IoT



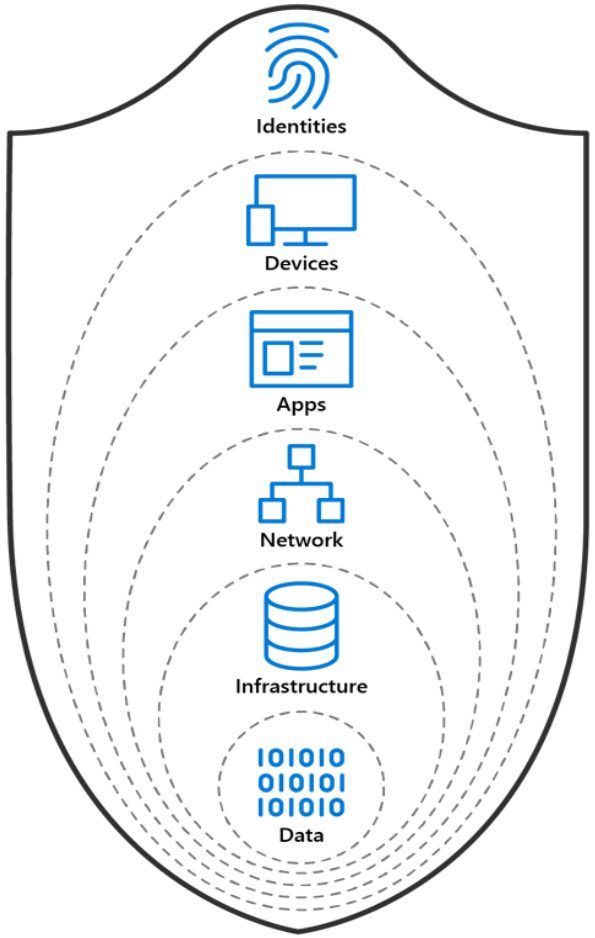
IT

OT+ICS

Стратегія ZERO TRUST

Zero Trust - Ніколи не довіряти, завжди перевіряти.

Передбачається, що зловмисники є як всередині, так і за межами мережі, тому жодним користувачам чи пристроям не можна автоматично довіряти.



Identities - перевірка та контроль ідентифікаційних даних користувачів.

Devices - Контроль усіх пристроїв, які звертаються до інфраструктури компанії

Apps - Пошук тіньових IT у своєму середовищі, контроль прав та привілеїв усередині додатків, організація доступів на основі аналітики в режимі реального часу, відстеження та контролю прав користувачів.

Infostructure - Використання засобів телеметрії, щоб виявляти атаки або аномалії та автоматичне блокування та маркування небезпечних дій; організація доступів з урахуванням мінімальних необхідних привілеїв.

Network - Недовіра до пристроїв та користувачів на підставі того, що вони знаходяться всередині мережі компанії. Організація шифрування всіх каналів обміну даними та обмеження доступу на основі політик компанії.

Data - Перехід із захисту на основі периметра до системи безпеки на основі даних. Використання аналітики для класифікації та маркування даних. Організація шифрування та обмежень доступу з урахуванням політик компанії.

Основи ZERO TRUST

- **ЗАВЖДИ ПЕРЕВІРЯЙ**. Треба завжди верифікувати ідентичність користувачів, приладів, процесів перед наданням їм доступу до ресурсів.
- **НІКОЛИ НЕ ДОВІРЯЙ, ЗАВЖДИ ПЕРЕВІРЯЙ**. Не довіряй автоматично користувачам та приладам, навіть якщо вони всередині периметру мережі. Замість цього перевіряй їх ідентичність та оцінюй рівень ризику перед наданням доступу
- **НАЙМЕНЬШІ ПРИВІЛЕЇ**. Надавай користувачам та приладам мінімальні рівні доступу, що необхідні для їх роботи.
- **МІКРОСЕГМЕНТАЦІЯ**. Поділи мережу на менші сегменти, щоб проблеми одного не вплинули на роботу інших.
- **ПОСТІЙНИЙ МОНІТОРИНГ**. Безперервно контролюй роботу мережі, таким чином можна швидко ідентифікувати та відповісти на загрозу.
- **КЕРУВАННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ**. Запроваджуй надійну ідентифікацію та управління доступом, включаючи мульти-факторну аутентифікацію, щоб бути впевненим, що тільки авторизовані користувачі та прилади мають доступ до ресурсів.

5 кроків побудови ZERO TRUST + ISA/IEC 62443

1. **Визначте поверхню захисту** – всі підключені пристрої, що стосуються технологічного процесу. Визначте критичні цифрові активи і їх зв'язки з фізичними процесами
2. **Відобразіть потоки транзакцій.** На відміну від IT-систем, в OT найголовніше захистити сам технологічний процес: його елемента, потоки даних між ними і як критичні цифрові активи впливають на їх активність.
3. **Побудуйте Zero Trust Architecture.** Ви повинні розуміти фізичний зв'язок між процесами даних і діями в реальному світі, що допоможе спроектувати детерміновану мережеву архітектуру, де технологічний процес, а також критичні цифрові процеси та обладнання захищені.
4. **Створіть політику Zero Trust.** Необхідно створити допоміжні політики Zero Trust, щоб відповісти на питання хто, що, коли, де, чому та як у вашій мережі та політиках.
5. **Контролюйте та підтримуйте мережу.** Слідкуйте за попередженнями та анормальною поведінкою.

ПЕРШІ КРОКИ

1. Аудит існуючої IT+OT/ICS інфраструктури
2. Розробка або адаптація вже існуючої системи кібергігієни
3. Підготовка плану та програми навчання, підвищення кваліфікації фахівців
4. Розробка плану реалізації стратегії Zero Trust

В презентації використані матеріали компаній:
Microsoft, Siemens, Oracle, Palo Alto Networks, Rockwell Automation, Carnegie Mellon University