USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПРОГРАМА МЕНТОРСТВА ТЕХНІЧНИХ ДИРЕКТОРІВ

ТЕМА 5

Ця презентація була підготовлена на замовлення USAID. Її самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цій презентації, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Основи операційних технологій, критично-важлива інфраструктура та IT-інтеграція кібербезпеки

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ЩО ЦЕ?

"Програмовані системи або пристрої, які взаємодіють із фізичним середовищем (або керувати пристроями, які взаємодіють з фізичним середовищем)"

NIST SP 800-37 Версія 2

"Операційні технології (OT) — це апаратне та програмне забезпечення, яке виявляє або викликає зміни шляхом прямого моніторингу та/або контролю виробничого обладнання, активів, процесів і подій"

Гартнер

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ЩО ЦЕ?

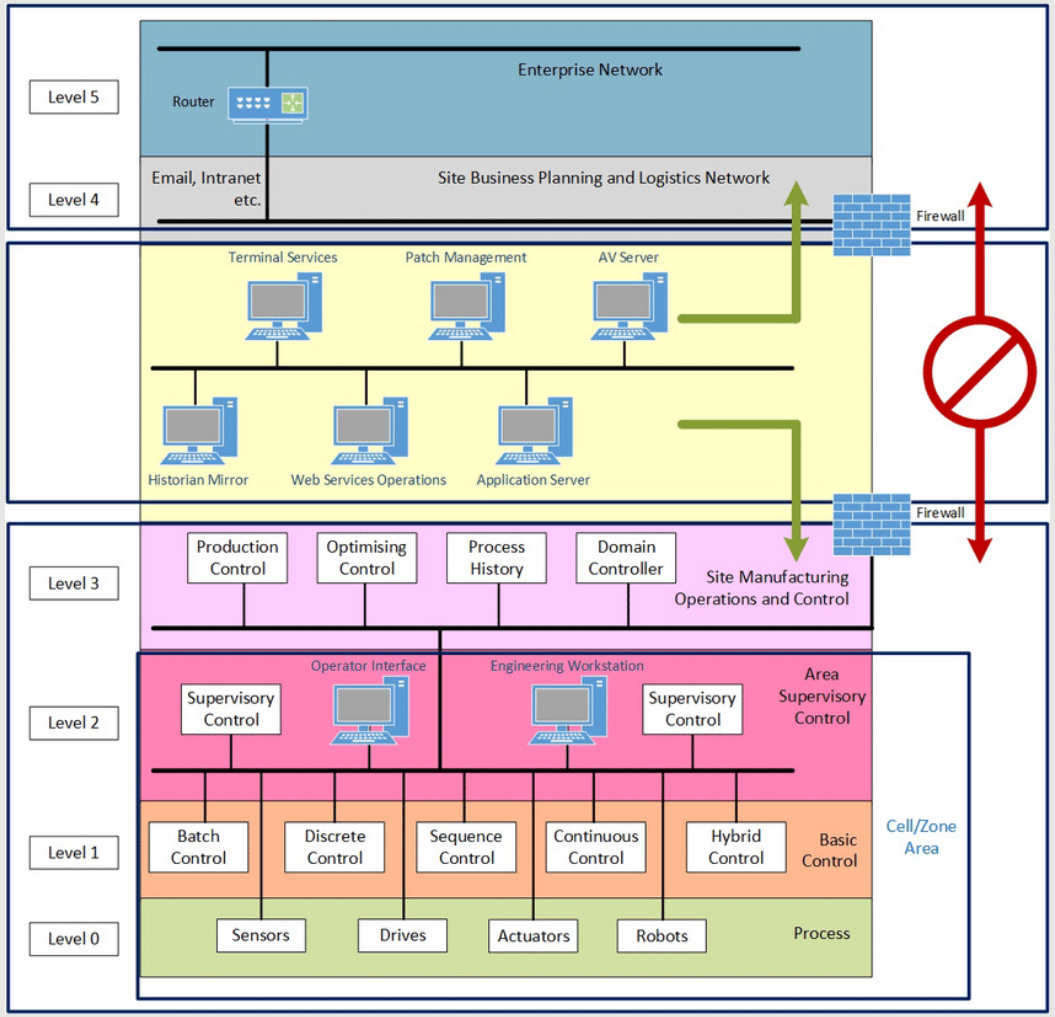
ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ЩО ЦЕ?

Ми всі можемо придумати гарні приклади Операційних технологій. Часто дуже зрозуміло, що щось є Операційною технологією

Коли використовуються визначення, іноді стає важко зрозуміти, де закінчується Операційні технології та починаються Інформаційні технології

Тому нам потрібно класифікувати або систематизувати їх за функціоналом

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – МОДЕЛЬ ПЕРДЬЮ



Модель Пердью можна знайти в ряді стандартів OT

Вона допомагає нам розмістити наші активи на логічних рівнях

Вона дозволяє нам зрозуміти, де можна розмістити елементи контролю, і зрозуміти, як різні варіанти використання можуть призвести до обходу цих елементів керування або забезпечити маршрут для переміщення суб'єкта між цими зонами, щоб досягти своєї мети.

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ЧИМ ВОНИ ВІДРІЗНЯЮТЬСЯ

Багато в чому Операційні технології дуже схожа на Інформаційні технології – ми не повинні вірити тому, що вона не може бути захищеною, і що вона дуже відрізняється імплементацією/впровадженням!

Однак ми повинні розуміти, чим наше середовище відрізняється.

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ТРІАДА ЦДК

Конфіденційність, Цілісність, Доступність

Чому цей порядок неправильний для ОТ? Він означає важливість – часто доступність і цілісність здаються найважливішими в ОТ.

Подумайте про свої власні процеси, що для вас найважливіше

приклад…

Якщо у вас система критично важлива для безпеки, то цілісність є життєво важливою, і ви краще закриєтесь, ніж поставите під загрозу життя

Якщо у вас є електрична мережа, найважливішою може бути доступність

Але всі фактори важливі

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ТРІАДА ЦДК

Що означає конфіденційність у OT?

Вона частіше досягається шляхом обережного поводження з конфіденційними даними, а не за допомогою шифрування.

Шифрування трафіку між сервером SCADA і PLC може бути непрактичним або неможливим.

Рух між точками має бути захищений, навіть якщо він є небезпечним, наприклад, за допомогою тунелю VPN. Це не для припинення втрати даних, а для забезпечення довіри до джерела та кінцевої точки.

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ТРІАДА ЦДК

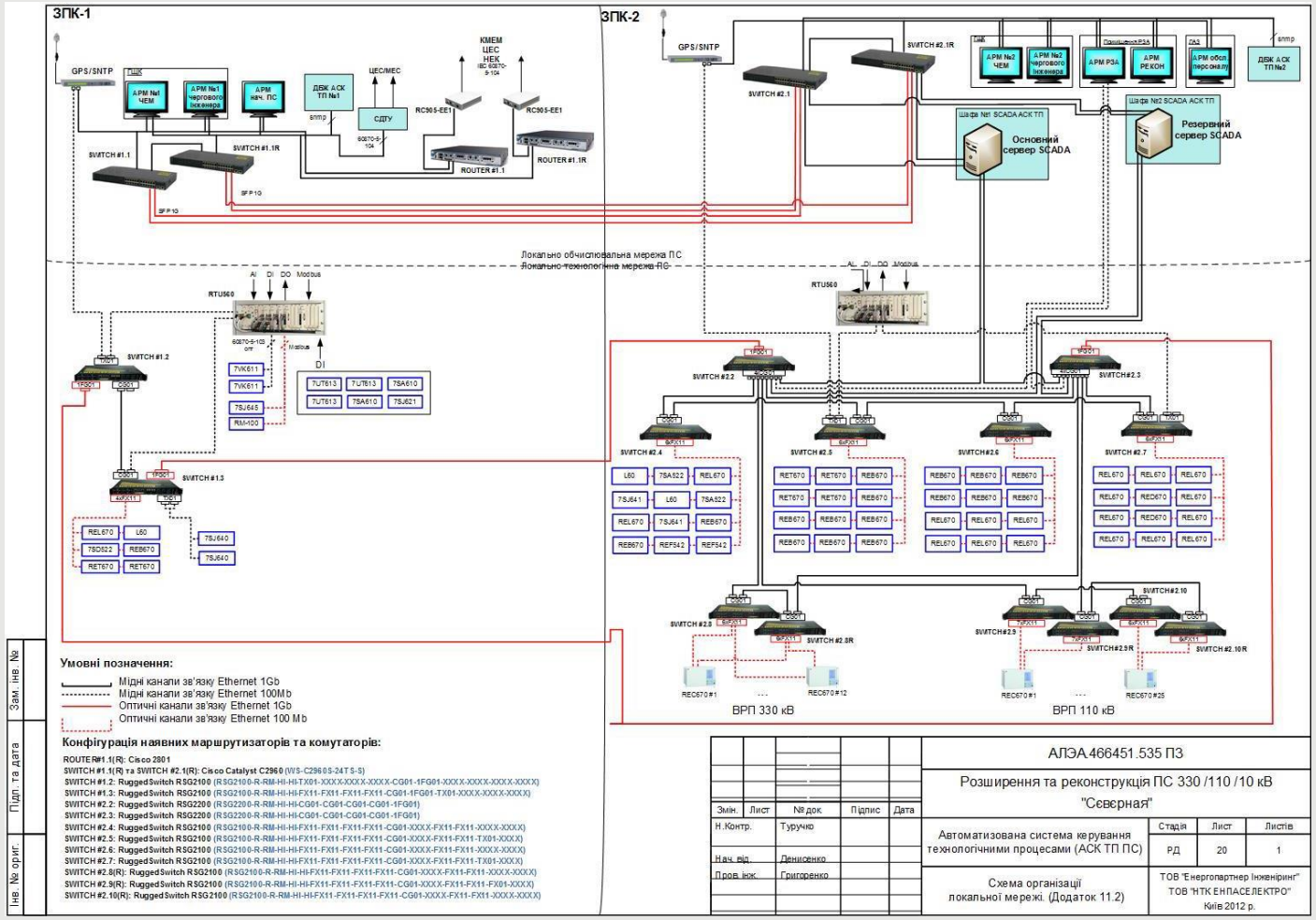
Що означає конфіденційність у ОТ?

Захист конфіденційності повинен бути досягнутий не тільки за допомогою технологій, а й за допомогою людей.

Атака на мережі ОТ, особливо ті, що з хорошим захистом, вимагає розвідки. Не завжди вдається зберегти наполегливість, тому створені атаки означають хороше розуміння цілі.

Але…

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ

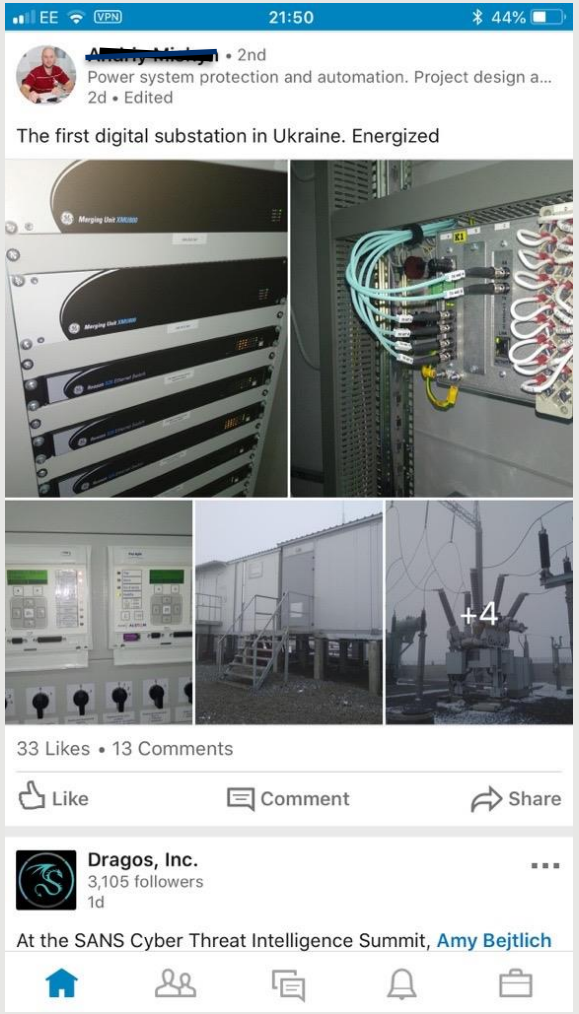


Переконайтеся, що Постачальники не публікують детальну інформацію про проекти, які вони виконують для вас.

Цей рівень інформації повідомляє зловмиснику:

1. Як ваше середовище пов'язане із зовнішнім світом.
2. Як орієнтуватися у вашому середовищі
3. Пристрої та версії програмного забезпечення та їх функції

ОПЕРАЦІЙНІ ТЕХНОЛОГІЇ – ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ



Переконайтеся, що персонал не передає деталі проектів ОТ

Часто гордість і прагнення до визнання роблять соціальні мережі ризикованою зоною

1. Постачальники
2. Розташування
3. Навіть те, як пристрої підключені до Комунікаційних мереж і Систем підстанцій

ЗАКЛЮЧЕННЯ

- Визначте всі свої активи – тримайте надійний інвентар і зберігайте його безпечному місці
- Зрозумійте архітектуру вашої мережі
- Подивіться, куди йдуть потоки даних, як і чому люди перетинають цю межу
- Забезпечте надійне розподілення сервісів
- Визначте засоби керування, які ви можете застосувати в середовищі OT, і зробіть поступові кроки до однакового контролю в усіх сферах

1. Переконайтеся, що ваша програма OSINT включає перевірку інформації про ваші активи OT
2. Переконайтеся, що ваш персонал поінформований про ризики
3. Відстежуйте конкретні загрози
4. Працюйте разом, IT-команди та команди з операційної інженерії працюють разом із самого початку!

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ДЯКУЮ