Модуль 1. Основи управління кібербезпекою

Лекція 3: Управління ризиками та корпоративне управління в ICS/SCADA

Мета заняття

Методологія оцінки ризиків

Дати широкову методологію оцінки та оброблення ризиків у середовищах **ICS** (Industrial Control Systems — промислові системи керування) і **SCADA** (Supervisory Control and Data Acquisition — диспетчерське керування та збір даних)

Корпоративне управління

Побудувати системне корпоративне управління через **CSMS** (Cybersecurity Management System — система управління кібербезпекою)

Інтеграція безпеки

Поєднати кібербезпеку з функціональною безпекою процесу та з бізнес-цілями

3.1. Процес оцінки ризиків у середовищах ICS/SCADA

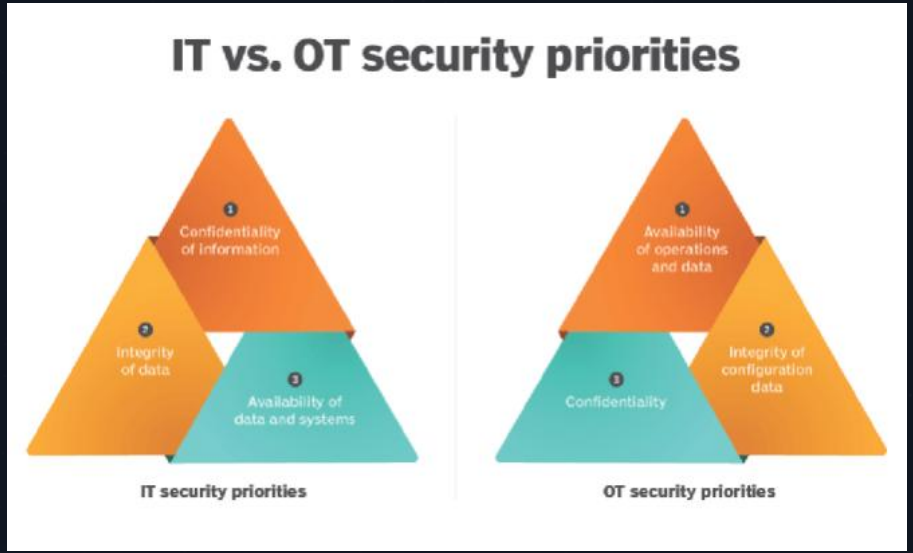
3.1.1 Чому оцінка ризиків в OT відрізняється від IT

Особливості домену

- Кінетичний вплив на людей, довкілля та обладнання
- Довгі життєві цикли систем і залежність від застарілих протоколів
- Висока чутливість до затримок і простоїв реального часу
- Нерідко обмеження на активні сканування і перерви на обслуговування

Режими відмови

- Порушення конфіденційності
- Втрата доступності
- Порушення цілісності даних і керувань



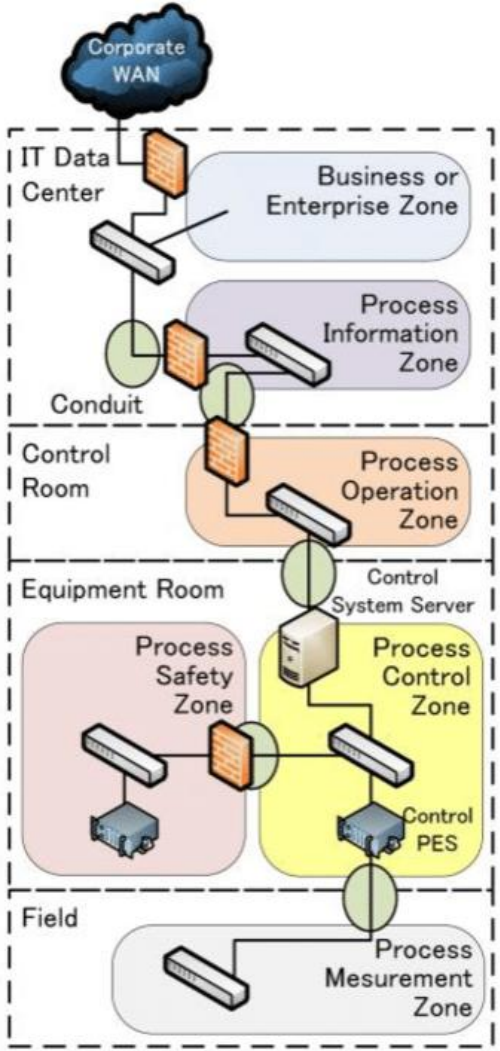
3.1.2 Підготовка до ризик-асесменту за IEC 62443-3-2

Організація процесу

- Формуємо міждисциплінарну команду з OT, IT, інженерії, безпеки процесу, юридичного відділу, HR
- Визначаємо рамки аналізу, рівні допусків до ризику, критерії прийнятності

Артефакти старту

- Політика управління ризиками
- Методика ранжування впливів на безпеку процесу і бізнес
- План збору даних і доступів до майданчиків



3.1.3 Інвентаризація активів та картографування зон і трактів

01

Реєстр активів

- Тип обладнання, модель, серійний номер, версії прошивок і ОС, IP та MAC, відповідач і власник
- Критичність для процесу, допустимий час простою, вимоги реального часу

02

Зони і тракти

- Групуємо активи в зони зі спільними вимогами безпеки
- Визначаємо тракти зв'язку між зонами з чіткими правилами доступу і моніторингом

03

Практичні джерела даних

- Пасивні інструменти OT-візибіліті, креслення від інтеграторів, опитування персоналу, журнали мережевого обладнання

3.1.4 Ідентифікація загроз і вразливостей без шкоди для процесу

Загрози

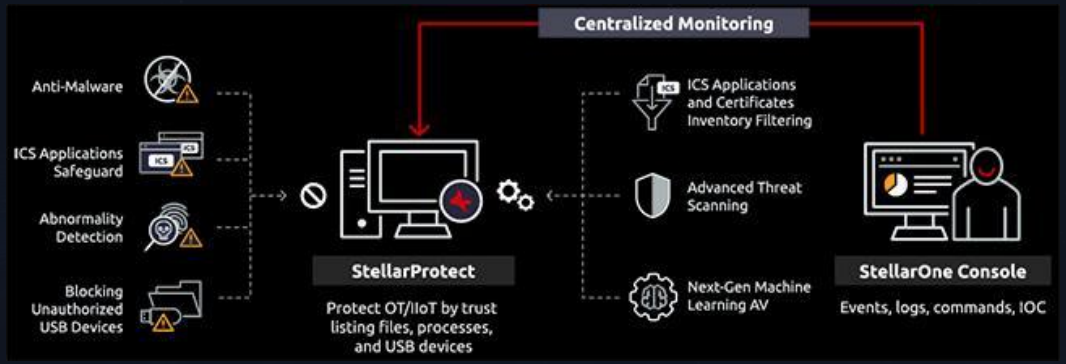
- Ворожі дії, інсайдери, випадкові помилки, структурні відмови, природні події

Вразливості

- Невимкнені служби, застарілі протоколи, слабкі облікові записи, відсутність сегментації, нестача журналювання

Безпечно для ОТ

- Перевага пасивного моніторингу і рев'ю конфігурацій
- Активне тестування лише на стендах та у вікнах планових робіт
- Залучення вендорів для аналізу специфічних уразливостей PLC і HMI



3.1.5 Оцінка ризику і призначення цільових рівнів безпеки SL-T

1

Методика

- Будуємо матрицю впливу і ймовірності з урахуванням безпеки процесу
- Для кожної зони визначаємо SL-T за очікуваною спроможністю противника

2

Вихідні документи

- Пріоритизований реєстр ризиків з власниками і термінами
- Карта зон і трактів з SL-T, контрольними точками моніторингу і вимогами до журналів

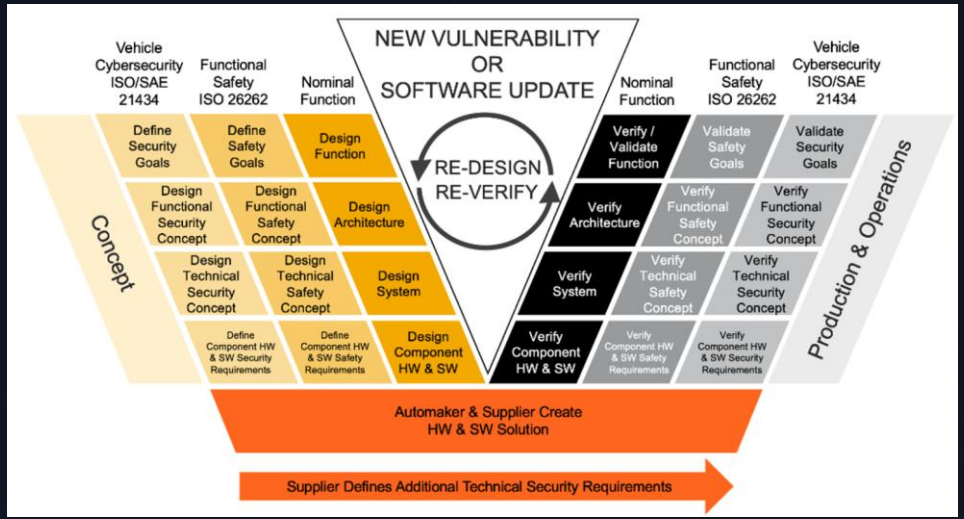
3.1.6 Синхронізація з функціональною безпекою процесу

Спільний аналіз

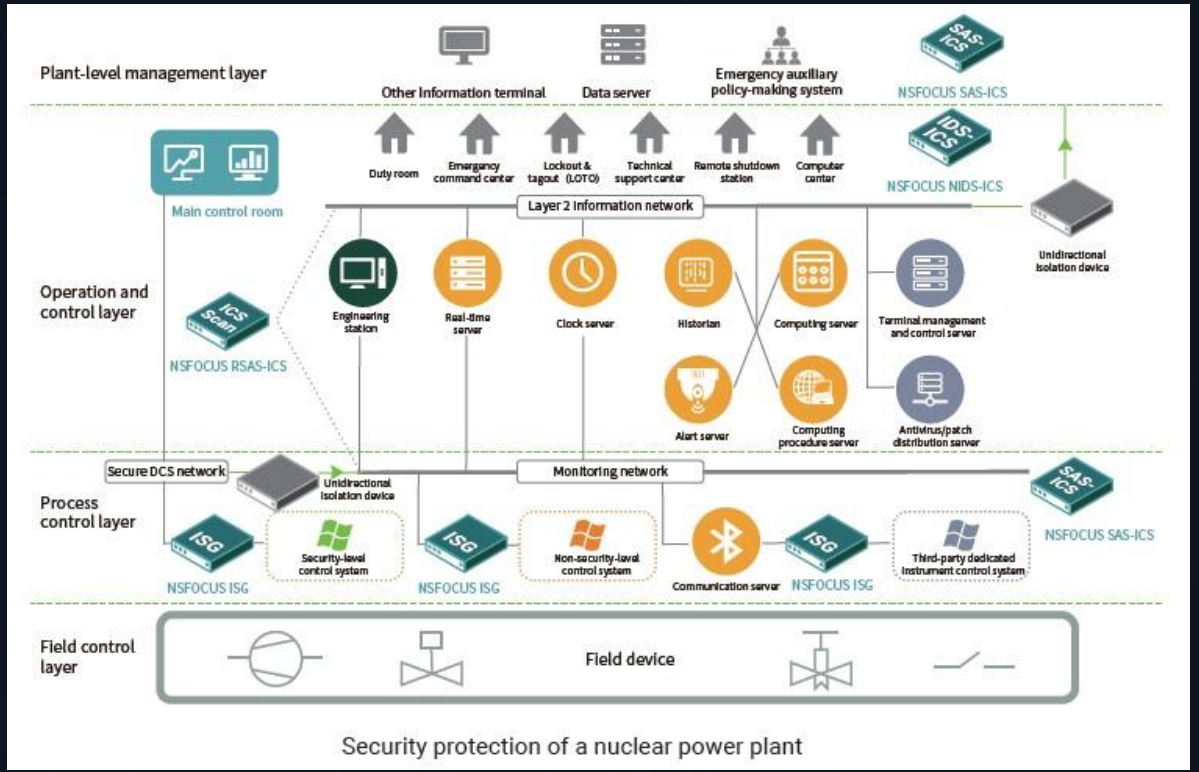
- Кореляція результатів OT ризик-асесменту з аналізом небезпек і аварій
- Перевірка, щоб кібер-контролі не знижували ефективність функцій безпеки

Практика

- Спільні сценарії тестів на стендах
- Подвійне погодження змін, що впливають на захисні функції



3.2. Стратегії управління та політики кібербезпеки ICS



Security protection of a nuclear power plant

3.2.1 CSMS як каркас корпоративного управління OT-кібербезпекою

Що таке CSMS

Система політик, процедур, ролей і метрик для стабільного управління ризиками в IACS

Блоки CSMS за IEC 62443-2-1

- Політика безпеки і ролі
- Управління активами і конфігураціями
- Управління доступом і привілеями
- Сегментація, моніторинг і журналювання
- Управління змінами, патчами і вразливостями
- Реагування на інциденти і відновлення
- Навчання, аудит і досконалення

Узгодження

Синхронізація з **ISMS** за ISO/IEC 27001 та з виробничими регламентами

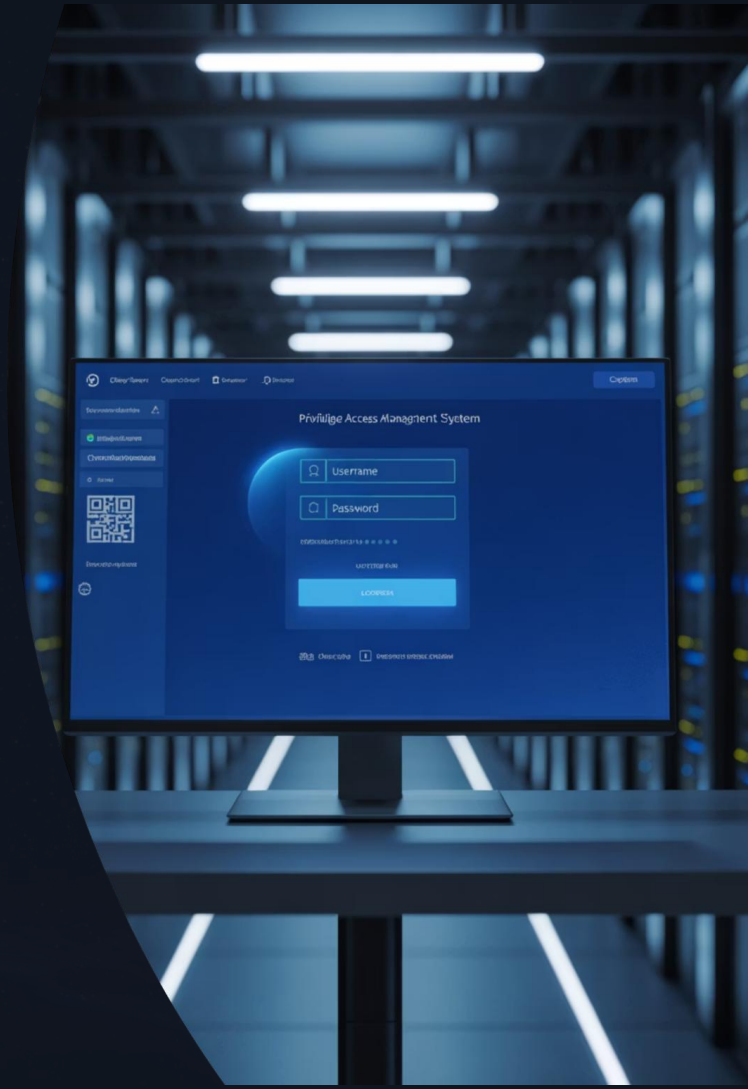
3.2.2 Політики доступу і керування привілеями

Принципи

- Найменші привілеї, розділення обов'язків, контроль сесій і запис дій
- **MFA** для віддаленого і привілейованого доступу
- Тимчасові доступи з автоматичним відкликанням

Технічні засоби

- Bastion-хости і проксі для адміністрування
- Централізоване управління обліковими записами і ключами
- Регулярні перевірки прав та ревізії облікових записів постачальників



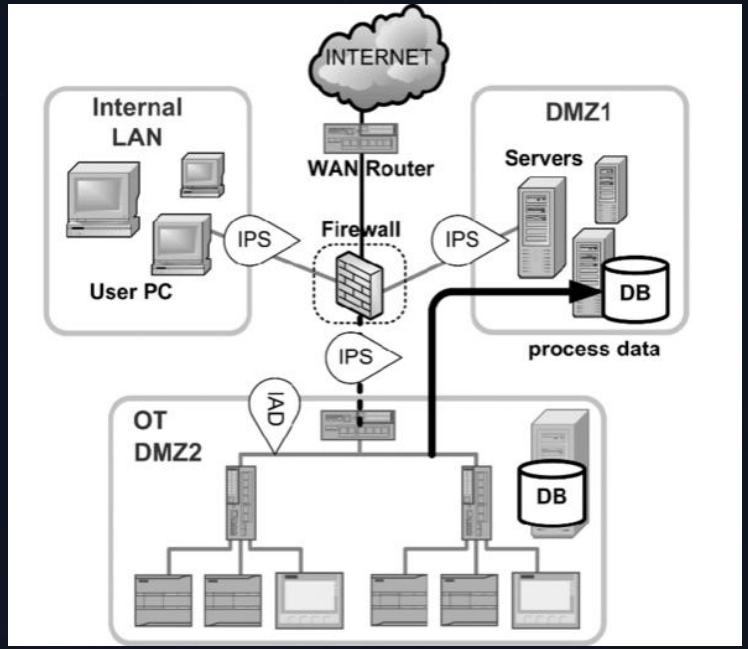
3.2.3 Сегментація мережі, DMZ і правила взаємодії OT з IT

Архітектура

- Виділення промислової **DMZ** між OT та IT
- Заборона безпосереднього доступу з IT у контрольні зони
- Односторонні діоди де можливо, обмеження протоколів до мінімально необхідних

Комунікаційні правила

- Ініціатива зв'язку з боку OT до IT для експорту даних
- Таблиці дозволених потоків, deny by default
- Інспекція OT-протоколів, окремі брандмауери на межах трактів



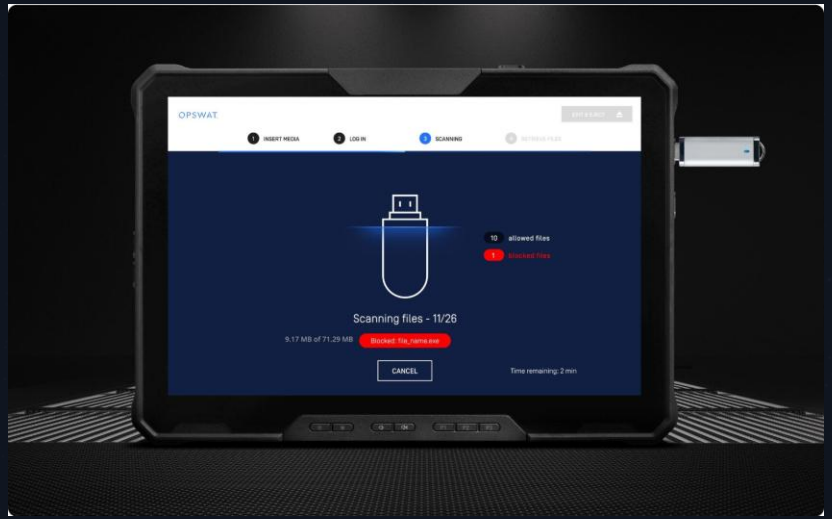
3.2.4 Керування змінними носіями і мобільними пристроями

Політика

- Категоризація носіїв, обов'язкове сканування у виділених кіосках
- Заборона підключення особистих пристроїв до OT мережі
- Фізичне блокування портів, контроль Bluetooth і Wi-Fi

Операційні процедури

- Ведення журналів ввезення-вивезення носіїв
- Перевірка походження файлів і цифрових підписів
- Регулярні навчання щодо ризиків знімних носіїв



2.5 Постачальники і ланцюг поставок у контексті OT

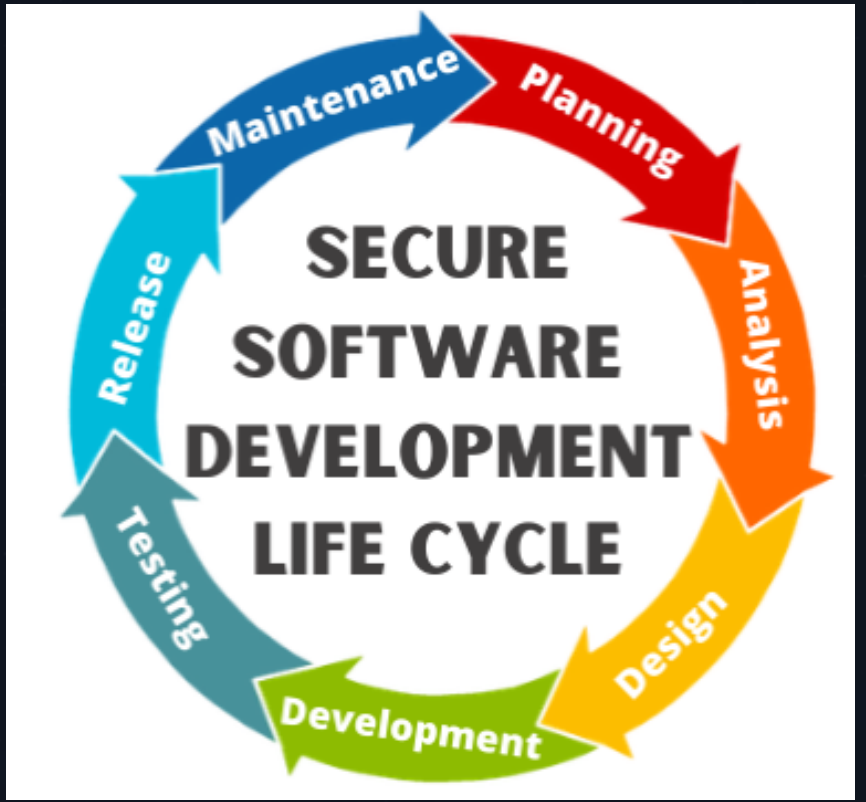
Вимоги до вендорів

- Відповідність **IEC 62443-4-1** життєвому циклу безпечної розробки
- Заявлені можливості компонентів за **IEC 62443-4-2**
- Прозорість щодо вразливостей, бюлетені безпеки, SLA на виправлення

Контракти

- Умови доступу на майданчик, правила віддаленого доступу, вимоги MFA
- Зобов'язання щодо журналювання робіт і надання звітів
- Механізми відкликання доступів і відповідальність за інциденти

3.3. Життєвий цикл кібербезпеки та безперервне вдосконалення



3.3.1. PDCA для IACS. Фаза Plan

01

Дії планування

- Інвентаризація активів і класифікація за критичністю
- Моделювання загроз і оцінка ризиків
- Визначення **SL-T** для зон і трактів
- План контролів, план резервного копіювання і відновлення
- План реагування на інциденти з ролями і контактами

02

Артефакти

- Політики і стандарти побудови конфігурацій
- Карта зон і трактів, матриця доступів, матриця ризиків

3.3.2 PDCA для IACS. Фаза Do

Впровадження

- Сегментація мережі та налаштування брандмауерів
- Впровадження MFA, bastion-хостів, проксі-адміністрування
- Загартовування хостів і HMI, вайтлістинг застосунків
- Налаштування журналювання, синхронізації часу та резервного копіювання
- Розгортання моніторингу IDS і централізації у SIEM

Узгодження з виробництвом

- Вікна робіт, плани повернення, схвалення змін з боку інженерії та безпеки процесу

3.3 PDCA для IACS. Фаза Check

Контроль ефективності

- Постійний моніторинг активів і нових підключень
- Аналіз подій у SIEM, кореляція з технологічними аномаліями
- Перевірка резервних копій відновленням на стендах
- Управління патчами з попереднім тестуванням і поетапним розгортанням
- Перевірка відповідності **SL-A** відносно **SL-T** за результатами тестів і аудитів

Метрики

- MTTR інцидентів, час від виявлення до ізоляції, частка закритих high-risk
- Покриття зон журналюванням і моніторингом, рівень зрілості ML

3.3.4 PDCA для IACS. Фаза Act і підвищення зрілості ML

1

Безперервне вдосконалення

- Розбір інцидентів і навчені уроки
- Оновлення політик, матриць доступу і карт зон
- Підвищення **ML** з фіксацією процесів, внутрішні аудити, автоматизація контрольних перевірок

2

План наступної ітерації

- Нові цілі за метриками, перерозподіл ресурсів, корекція **SL-T** за потреби

3.4. Висновки та рекомендації

Ризик-менеджмент в OT спирається на коректну інвентаризацію, зонування і призначення **SL-T**

CSMS поєднує політики, процеси і технічні контролі та забезпечує керованість на рівні підприємства

Цикл **PDCA** гарантує сталість і поступове зростання зрілості **ML**

Синхронізація з безпекою процесу запобігає конфліктам і знижує операційний ризик

Список використаних джерел

1. Radvanovsky, R., & Brodsky, J. (2016). Handbook of SCADA/Control Systems Security (2nd ed.). CRC Press.

2. Colbert, E. J. M., & Kott, A. (Eds.). (2016). Cyber-Security of SCADA and Other Industrial Control Systems. Springer.

3. Shaw, W. T. (2020). Cybersecurity for SCADA Systems (2nd ed.). PennWell Books.

4. Brooks, C. J., & Craig Jr., P. A. (2022). Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT. Wiley.

5. Kouremetis, M. (2014). Defending a SCADA System with the Snort IDS [Presentation]. ECSSE Department.

6. National Telecom Regulatory Authority (NTRA). (2022). IoT Cyber Security Framework. EG-CERT.

7. Emerson. (2021). Industrial Security in SCADA Systems: IEC 62443-3-3 Certification. Emerson Automation Solutions.

8. Krotofil, M. (2023). Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle. Technical White Paper.

9. UtilSec, LLC. (2024). Getting Started in ICS/OT Cyber Security: Lab Manual. UtilSec.

Дякую за увагу!