Модуль 3. Основні принципи мережевого захисту для ICS/SCADA та інтеграції промислових систем в IT-інфраструктуру

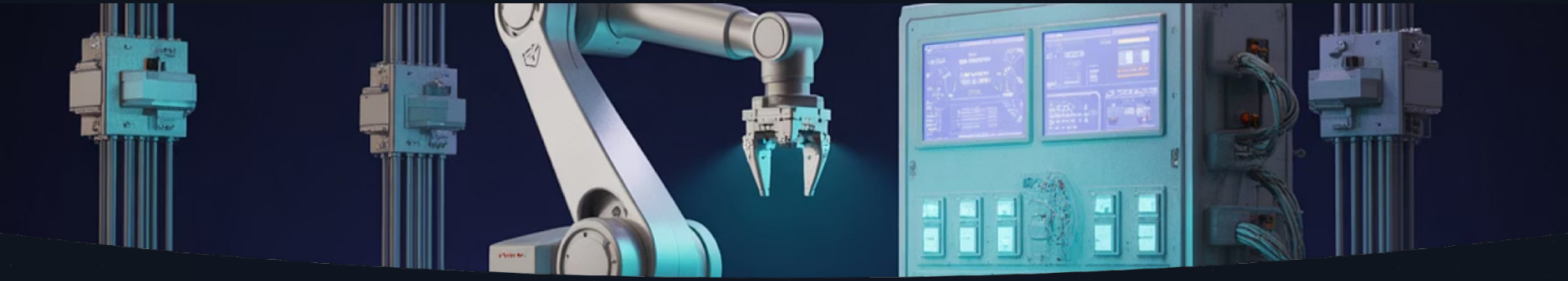
Лекція 4: Управління патчами та контроль конфігурації

Мета лекції

Сформувати практичне розуміння управління патчами та контролю конфігурації в ICS/SCADA для збереження доступності процесу, зниження ризиків і підвищення стійкості

Основні завдання

- Пояснити виклики патчування в OT середовищі з довгим життєвим циклом і вимогою безперервної роботи
- Відпрацювати ризик-орієнтовану оцінку патчів та їх тестування у пісочниці з подальшим контрольованим розгортанням через DMZ сервер оновлень
- Визначити процес і ролі для планування вікон робіт, відкату, журналювання та постійного перегляду процедур
- Розкрити принципи управління конфігураціями за baseline підходом NIST SP 800-53 CM-2 з актуалізацією схем, параметрів і дозволених потоків
- Забезпечити контроль цілісності ПЗ та прошивок, резервне копіювання і регулярні перевірки відновлення
- Показати значення повної інвентаризації активів для пріоритизації патчів, сумісності та швидкого реагування на інциденти



4.1. Виклики управління патчами в ICS

Управління патчами в промислових системах керування є значно складнішим завданням, ніж у традиційних IT-середовищах. Основна причина цієї складності полягає в необхідності забезпечення безперервної роботи та високої доступності систем.

Пріоритети ICS/IACS

Доступність → Цілісність → Конфіденційність

Життєвий цикл

ICS: 15-25 роківIT: 3-5 років

Обмеження ресурсів

Застарілі процесори та обмежені обчислювальні можливості

4.1.1. Конфлікт між безперервністю та безпекою

Традиційний підхід

Компанії, що використовують системи промислової автоматизації, оновлюють програмне забезпечення лише під час планових відключень системи. Це пов'язано з тим, що застосування патчів може призвести до:

- Непередбачуваних збоїв
- Простоїв виробництва
- Проблем з сумісністю
- Порушення критичних процесів

Однак така методологія не відповідає сучасним вимогам кібербезпеки, які вимагають можливості встановлення патчів безпеки у проміжки часу між запланованими відключеннями.

Неприйнятність простоїв у критичних промислових процесах створює дилему між безпекою та операційною ефективністю

4.1.2. Потенційні проблеми з сумісністю

В ICS/OT-середовищах використовуються застарілі системи з тривалим життєвим циклом, що створює унікальні виклики для управління патчами.

1

Несумісність патчів

Патчі для сучасних ОС можуть бути несумісними зі старим обладнанням

2

Неповні оновлення

Часткові патчі можуть стати джерелом нових вразливостей

3

Неправильна конфігурація

Незнання операторами належних налаштувань безпеки

> Приклад проблеми: Патч для усунення вразливості FTP може бути неактуальним для пристрою, де FTP вже вимкнено. Більше того, новий патч може внести нові вразливості, збільшивши загальний ризик.

4.2. Розробка ефективних стратегій патчингу (тестування, пісочниці)

4.2.1. Рекомендації щодо управління патчами

01

Збалансований підхід

Враховувати як вимоги безпеки, так і необхідність безперервної роботи

02

Індивідуальні стратегії

Розробляти стратегії патчингу з глибокою оцінкою сумісності

03

Чіткі процеси

Мати процедури для встановлення патчів між запланованими відключеннями

04

Довгострокове планування

Враховувати тривалий життєвий цикл ICS-систем

4.2.2. Розробка ефективних стратегій патчингу

Ефективна стратегія патчингу в ICS-середовищах починається з ретельної оцінки кожного потенційного патча перед його встановленням у систему.

Визначення релевантності

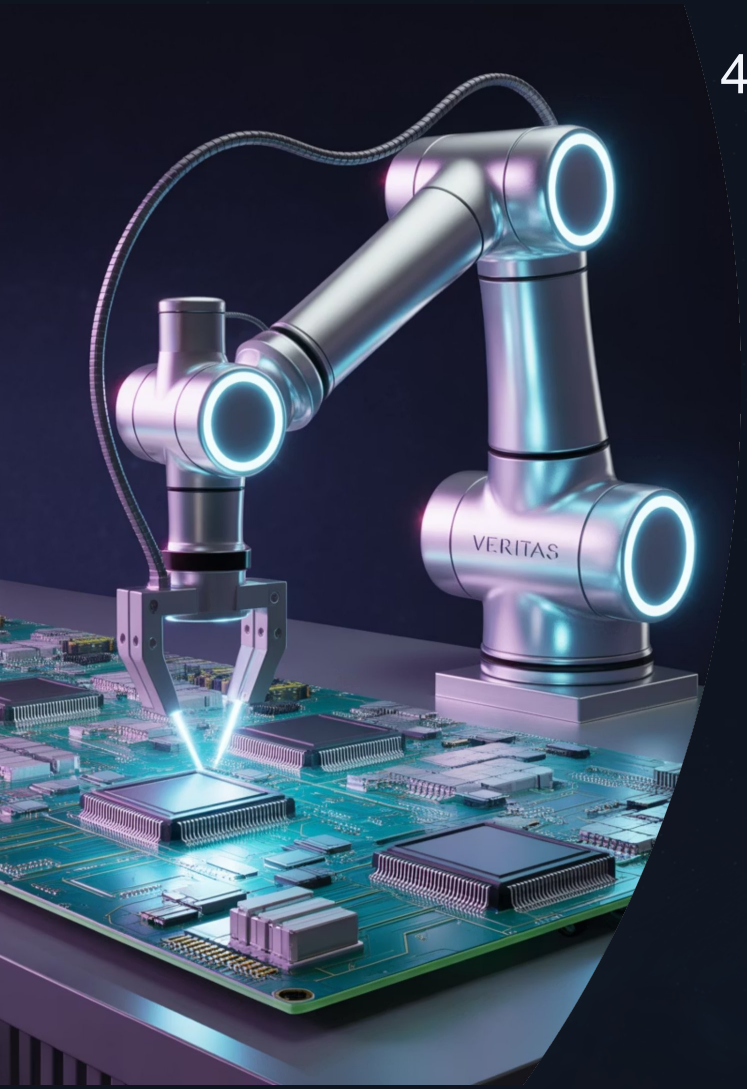
Перевірка, чи патч дійсно стосується існуючої вразливості в конкретній системі промислової автоматизації. Якщо патч усуває вразливість у функції, яка не використовується, його встановлення може бути непотрібним і потенційно ризикованим.

- Аналіз використовуваних функцій
- Оцінка актуальності вразливості
- Перевірка необхідності патча

Аналіз ризиків

Аналіз нового патча для визначення, чи не призведе він до появи нових вразливостей або збільшення ризику для системи більше, ніж та вразливість, яку він покликаний усунути.

- Оцінка потенційних нових ризиків
- Порівняння з існуючими загрозами
- Визначення загального впливу



4.2.3. Тестування в ізольованому середовищі

Одним з найважливіших етапів розробки ефективної стратегії патчингу є тестування патчів в ізольованому середовищі - "пісочниці" (sandbox).

Мета тестування

Ідентифікація файлів, змінених патчем, і перевірка їхнього впливу на функціональність та стабільність системи

Мінімізація ризиків

Тестування дозволяє виявити проблеми до розгортання у виробничому середовищі

Оптимізація процесу

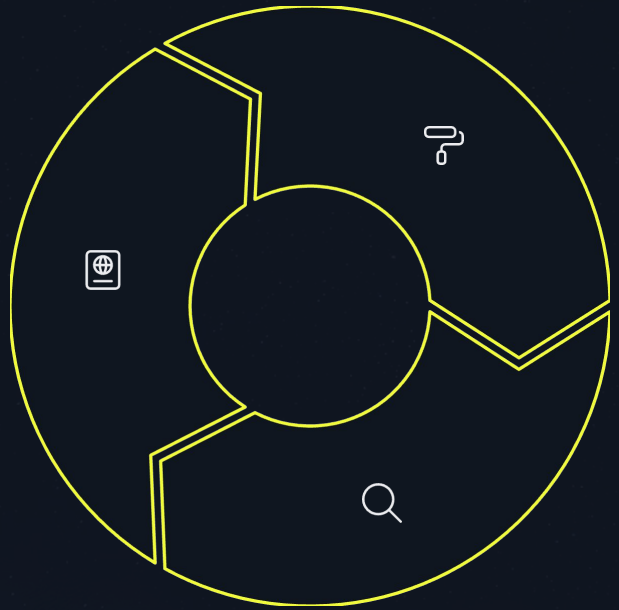
Дотримання принципів патчингу ICS зводить проблеми до мінімуму

Результат: Якщо дотримуватися цих фундаментальних принципів патчингу ICS, проблеми, пов'язані з оновленням, зводяться до мінімуму, що знижує ризик і підвищує безпеку системи.

4.2.4. Постійний перегляд та документування

Регулярний перегляд

Точно визначений процес перегляду програмного забезпечення для виправлення вразливостей



Технічне обслуговування

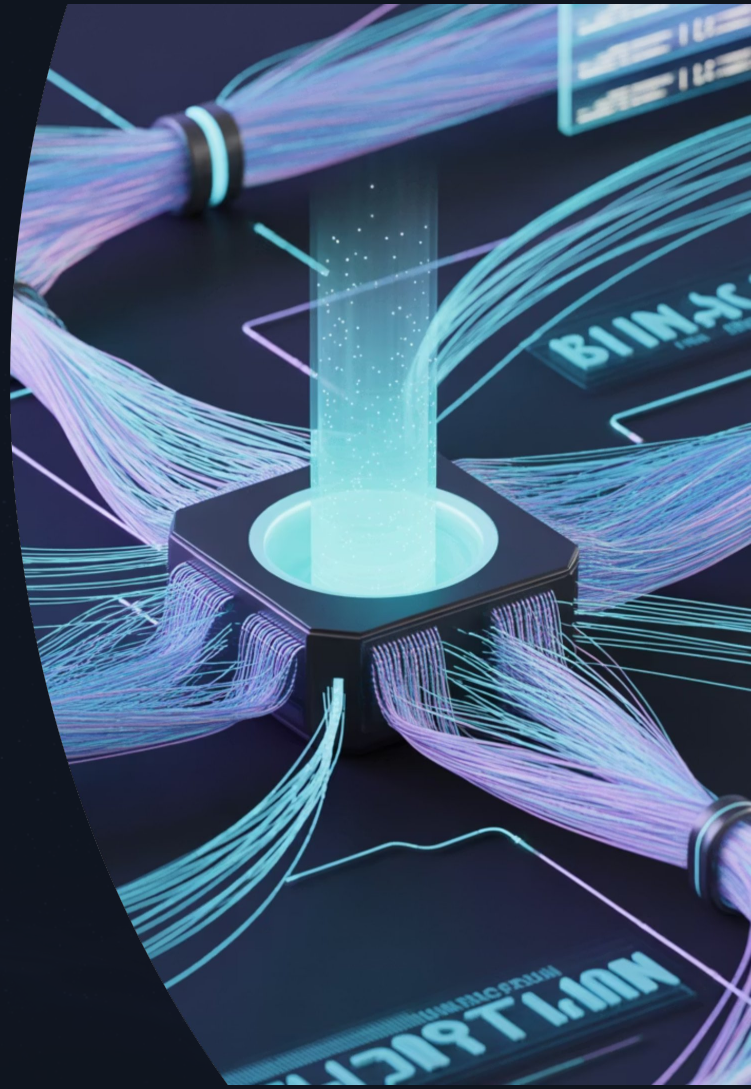
Частина фази технічного обслуговування життєвого циклу кібербезпеки IACS

Постійне вдосконалення

Аналіз уроків від інцидентів та проведення періодичних аудитів

Програмні патчі для обладнання зазвичай завантажуються з підприємства на патч-сервер, який знаходиться в межах демілітаризованої зони (DMZ) між підприємством та мережею керування.

4.3. Управління конфігурацією та цілісністю (програмне забезпечення, бази даних, налаштування мережі)



4.3.1. Управління конфігурацією та цілісністю

Управління конфігурацією є критично важливим аспектом кібербезпеки ICS/OT, оскільки неправильна конфігурація може призвести до втрати функціональності або компрометації системи.

> Цей процес включає розробку, документування та підтримку актуальних базових конфігурацій для інформаційних систем та їх компонентів.

4.3.2. Базові конфігурації за NIST SP 800-53

NIST SP 800-53 CM-2 підкреслює необхідність розробки, документування та підтримки актуальних базових конфігурацій інформаційних систем.

1

Компоненти системи

Стандартні програмні пакети, номери версій, інформація про патчі, налаштування

2

Мережева топологія

Логічне розміщення компонентів в архітектурі системи

3

Актуалізація

Створення нових базових конфігурацій у міру змін інформаційних систем

Базові конфігурації є офіційно перевіреними та погодженими наборами специфікацій для інформаційних систем або елементів конфігурації в цих системах.

4.3.3. Цілісність програмного забезпечення

Інженерні застосунки

Сучасні ICS-виробники пропонують спеціалізовані застосунки для централізованого управління інженерними процесами та зберігання документації. Доступ до таких застосунків значно зменшує зусилля зловмисника для розуміння процесу.

Контроль цілісності

Моніторинг та контроль цілісності прикладної програми та прошивки є критично важливим. Спеціалізовані системи можуть повністю контролювати:

- Версію прошивки (FW)
- Оновлення системи
- Цілісність прикладної програми
- Факт зміни будь-яким чином

4.3.4. Резервне копіювання та відновлення

Компанії з IACS зазвичай мають внутрішні керівництва або політики, які визначають процес резервного копіювання системи.

Елементи для резервного копіювання

Визначення критичних компонентів системи, що потребують регулярного збереження

Інтервал та кількість копій

Встановлення частоти створення резервних копій та їх кількості для зберігання

Місця зберігання

Визначення безпечних локацій для зберігання резервних копій

Вимоги до підписання коду

Забезпечення цілісності резервних копій через цифрові підписи

Важливо: Як резервне копіювання, так і відновлення слід регулярно перевіряти для забезпечення їх ефективності.

4.3.5. Контроль налаштувань мережі

Неправильні або небезпечні конфігурації, модифіковані з початкових налаштувань або адаптовані до середовища замовника, є значною загрозою.

1. **Ідентифікація ризиків**

   Виявлення неправильних конфігурацій та небезпечних налаштувань

2. **Навчання персоналу**

   Власники/оператори повинні бути обізнані з правильними конфігураціями безпеки

3. **Постійний моніторинг**

   Регулярна перевірка та корекція налаштувань мережевого обладнання

4.3.6. Управління змінами в системі

Будь-які зміни в системі вимагають не тільки фіксації в системній документації, а й відповідних змін у самій документації.

Додавання/видалення модулів

Контроль змін у складі системних компонентів

Зміна мережевої конфігурації

Документування всіх мережевих модифікацій

Заміна пристроїв

Фіксація заміни обладнання та оновлення документації

Формальний процес

Запровадження процедур для ефективного прийняття рішень та впровадження

4.3.7. Фізичні механізми контролю

На програмованих логічних контролерах (PLC) фізичний ключ-перемикач контролює режими роботи, що є формою контролю доступу до функціоналу пристрою.

Режим "Програма"

Дозволяє модифікацію логіки контролера

Режим "Виконання"

Блокує зміни та забезпечує стабільну роботу

Це допомагає контролювати можливість віддаленого оновлення прошивки та програмування, забезпечуючи додатковий рівень фізичної безпеки.

4.4. Важливість інвентаризації активів

Ведення точного та повного списку всіх пристроїв/додатків є фундаментальним для кібербезпеки ICS/OT.

> Реєстр активів (Asset Register) – це детальний, централізований список усіх активів у середовищі, що включає технічні та операційні деталі. Він забезпечує основу для управління загрозами та вразливостями, а також ефективного реагування на інциденти.

4.4.1. Роль інвентаризації в управлінні безпекою

Управління патчами

Процес значно спрощується при наявності повного списку пристроїв. Знаючи точну версію ПЗ та прошивки, можна ефективніше визначати релевантні патчі та їх ризики.

Реагування на інциденти

У випадку кіберінциденту актуальний реєстр дозволяє швидко ідентифікувати скомпрометовані системи, їхнє розташування, залежності та відповідальних осіб.

Це прискорює процес стримування, викорінення та відновлення, мінімізуючи вплив інциденту на виробничі процеси.

4.4.2. Зміст інвентаризації активів

Повний реєстр активів повинен містити детальну інформацію про кожен компонент системи для забезпечення ефективного управління безпекою.

Ідентифікаційні дані

IP-адреси, MAC-адреси, унікальні ідентифікатори пристроїв

Розташування

Фізичне місцезнаходження, зона безпеки, логічне розміщення в архітектурі

Мережева топологія

Документування мережевої структури та логічного розміщення компонентів

Технічні характеристики

Постачальники, моделі, версії прошивок/ОС, інформація про встановлені патчі

Відповідальність

Контактні дані відповідальних осіб за обслуговування та управління

Комунікаційні з'єднання

Точний список LAN-з'єднань між SCADA та системами за межами електронного периметра

4.4.3. Методи побудови реєстру активів

Реєстр активів можна побудувати за допомогою різних методів, кожен з яких має свої переваги та обмеження.

Пасивне прослуховування мережі

Використання інструментів, таких як Wireshark, для збору ARP-таблиць, DNS-запитів та аналізу промислового трафіку без втручання в роботу системи.

Активне сканування

Інструменти на зразок Nmap для пінг-сканування, ARP-сканування, переліку DNS, сканування портів та виявлення ОС/сервісів. Використовується переважно в IT/тестових середовищах.

Виявлення через конфігурації

Аналіз конфігурацій мережевих пристроїв (наприклад, комутаторів Cisco) для ідентифікації DHCP-пулів та ідентифікаторів клієнтів.

Аналіз трафіку

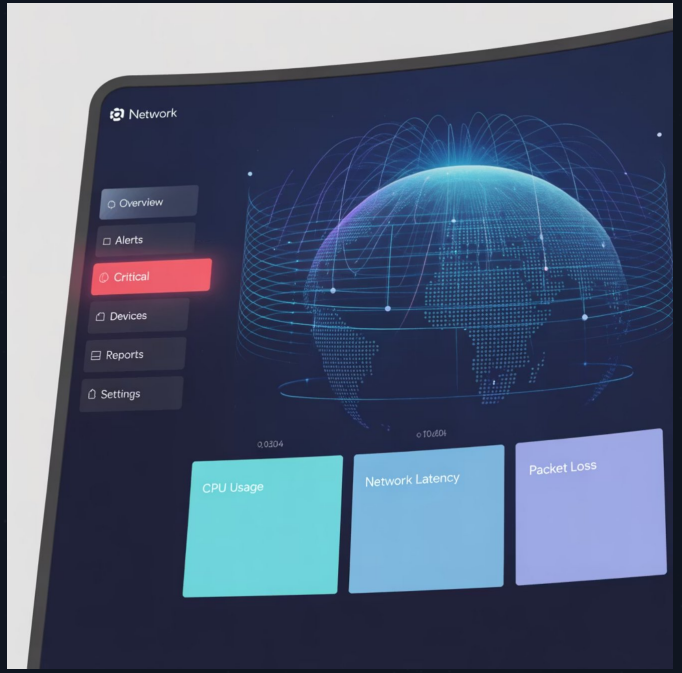
Використання спеціалізованих інструментів, таких як Modbus Poll, для збору та аналізу Modbus/TCP пакетів та інших промислових протоколів.

4.4.4. Переваги пасивного моніторингу

Безпечність для виробництва

Пасивне прослуховування не створює додаткового навантаження на мережу та не ризикує порушити роботу критичних систем. Це особливо важливо в промислових середовищах, де будь-яке втручання може призвести до простоїв.

- Відсутність ризику для виробничих процесів
- Неможливість виявлення зловмисниками
- Збір реальних даних про трафік
- Можливість тривалого моніторингу



Пасивний моніторинг дозволяє отримати точну картину мережевої активності без ризику для стабільності системи

4.4.5. Активне сканування: обережність у OT

Активне сканування може бути корисним інструментом, але в OT-середовищах потребує особливої обережності.

Ризики активного сканування

Може призвести до перевантаження старих пристроїв, порушення роботи протоколів або навіть відмови обладнання

Рекомендовані умови

Використовувати тільки в тестових середовищах або під час планових відключень виробництва

Попередні заходи

Обов'язкове тестування на ізольованих системах перед застосуванням у виробничому середовищі

4.4.6. Аналіз промислових протоколів

Спеціалізований аналіз промислових протоколів дає унікальну інформацію про активи та їх функціональність.

Modbus/TCP

Аналіз Modbus-трафіку для виявлення пристроїв та їх функцій

EtherNet/IP

Моніторинг промислового Ethernet для ідентифікації активів

PROFINET

Виявлення пристроїв через аналіз PROFINET-комунікацій

DNP3

Ідентифікація активів через протокол DNP3

Кожен промисловий протокол містить специфічну інформацію про пристрої, їх функції та стан, що дозволяє створити детальний профіль активів.

4.4.7. Підтримка актуальності реєстру

Створення реєстру активів - це лише початок. Підтримка його актуальності є постійним процесом, критично важливим для ефективності програми кібербезпеки.

Постійний моніторинг

Автоматизоване виявлення нових пристроїв та змін у мережі

Регулярні оновлення

Планові перевірки та актуалізація інформації про активи

Валідація даних

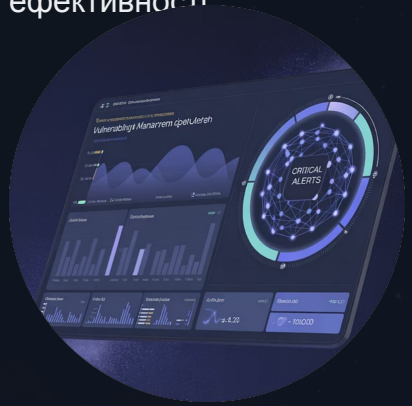
Перевірка точності та повноти інформації в реєстрі

Управління змінами

Інтеграція з процесами управління змінами для автоматичного оновлення

4.4.8. Інтеграція з процесами безпеки

Реєстр активів повинен бути інтегрований з усіма ключовими процесами кібербезпеки для максимальної ефективності



Управління вразливостями

Автоматичне співставлення виявлених вразливостей з активами в реєстрі для пріоритизації заходів

Реагування на інциденти

Швидкий доступ до інформації про скомпрометовані активи та їх залежності

Аудит та комплаєнс

Використання реєстру для демонстрації відповідності регулятивним вимогам

4.5. Висновки та рекомендації

Інвентаризація активів є наріжним каменем ефективної програми кібербезпеки в ICS/OT середовищах.

100%

Покриття активів

Всі пристрої повинні бути включені в реєстр

24/7

Постійний моніторинг

Безперервне відстеження змін у мережі

90%

Зменшення часу реагування

Прискорення процесів управління інцидентами

> Ключові рекомендації: Постійно підтримувати актуальний, деталізований реєстр усіх активів, використовуючи комбінацію пасивних та безпечних методів виявлення. Це не тільки спрощує управління патчами та реагування на інциденти, але й забезпечує фундаментальне розуміння того, що саме потрібно захищати.

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!