

## **Przykładowe tematy projektów**

Poniższa lista ma charakter orientacyjny. Zachęcam Państwa do zaproponowania własnych tematów projektów związanych z bezpieczną konfiguracją środowisk, elementami przemysłowymi, IoT lub innymi formami automatyzacji. Projekt realizowany jest w grupach 1-4 osoby. Do projektu należy przygotować dokumentację i prezentację która odbędzie się na ostatnich zajęciach lub we wcześniejszym terminie.

### **Temat 1: Analiza Ryzyka i Audyt Systemu SCADA**

Przeprowadzenie kompleksowej analizy ryzyka dla wybranego, fikcyjnego (lub opisanego w literaturze) systemu SCADA w sektorze infrastruktury krytycznej (np. stacja uzdatniania wody, mała elektrownia). Zidentyfikować kluczowe aktywa, przeanalizować potencjalne zagrożenia i podatności oraz ocenić ryzyko. Projekt powinien zawierać propozycję planu audytu bezpieczeństwa opartego na wytycznych normy.

### **Temat 2: Opracowanie Planu Reagowania na Incydenty (IRP)**

Stworzenie szczegółowego planu reagowania na incydenty cybernetyczne dla operatora systemu sterowania przemysłowego (ICS). Plan musi definiować role i obowiązki, procedury detekcji i analizy incydentu, kroki powstrzymywania zagrożenia, odtwarzania systemu oraz komunikacji kryzysowej. Powinien uwzględniać specyfikę systemów OT (np. priorytet ciągłości działania).

### **Temat 3: Projekt Bezpiecznej Segmentacji Sieci OT/IT**

Zaprojektowanie bezpiecznej architektury sieciowej dla przedsiębiorstwa produkcyjnego, integrującego nową linię produkcyjną opartą o urządzenia IIoT z istniejącą siecią korporacyjną (IT). Projekt musi bazować na **Modelu Purdue**, definiować strefy bezpieczeństwa i kanały komunikacji, uwzględniać strefę DMZ (dla np. serwerów Historian) oraz proponować zasady filtrowania ruchu między segmentami.

### **Temat 4: Hardening Stacji Roboczej HMI i Sterownika PLC**

Opracowanie i (w miarę możliwości) przetestowanie w środowisku wirtualnym procedur hardeningu dla typowych komponentów systemu ICS. Stworzyć "check-listę" i skrypty konfiguracyjne do umacniania stacji HMI (opartej np. o Windows) oraz sterownika PLC (np. blokada portów, zarządzanie hasłami, kontrola dostępu). Należy odnieść się do wytycznych NIST lub CIS Benchmarks.

### **Temat 5: Studium Ataku na ICS i Opracowanie Sygnatur Detekcji**

Dogłębna analiza wybranego, rzeczywistego ataku na systemy przemysłowe (np. **Stuxnet**, atak na ukraińską sieć energetyczną, TRITON/TRISIS, itp.). Przeanalizować wektory ataku, wykorzystane podatności i skutki. Kluczowym elementem projektu jest opracowanie na tej podstawie reguł dla systemu IDS (np. Snort/Suricata) lub zapytań dla systemu SIEM, które mogłyby wykryć podobny atak w monitorowanej sieci przemysłowej.

## **Temat 6: Analiza Podatności Przemysłowych Urządzeń IoT**

Identyfikacja i analiza bezpieczeństwa wybranego urządzenia IoT (np. dowolne urządzenie smart) lub IIoT (np. brama Modbus-to-MQTT, inteligentny czujnik przemysłowy, router IIoT) w środowisku testowym. Wykorzystując dostępne narzędzia (np. nmap, shodan, firmware analysis tools), spróbować zidentyfikować otwarte porty, domyślne hasła, znane podatności (CVE) oraz słabości w protokołach komunikacyjnych. Projekt kończy się raportem z podatności i rekomendacjami zabezpieczeń.

## **Temat 7: Bezpieczna Stacja Monitorowania Warunków Pracy (Symulacja IIoT)**

Zbudować (np. przy użyciu Raspberry Pi / ESP32 i czujników) prosty system monitorowania warunków w "hali produkcyjnej, gleby itp." (np. temperatura, wilgotność, itp.). Dane te mają być bezpiecznie przesyłane do centralnego panelu (dashboard).

- **Zadania:**
  - Implementacja czujników i mikrokontrolera.
  - Wybór i bezpieczna konfiguracja protokołu komunikacyjnego
  - Hardening urządzenia brzegowego
  - Stworzenie prostego dashboardu do wizualizacji danych.
- Praktyczne wdrożenie bezpiecznej architektury IoT, zabezpieczanie urządzeń i protokołów.

TLDR;

Dowolna realizacja mini projektu hardware IoT która zbiera i wyświetla różne dane pomiarowe  


## **Temat 9: Analiza Bezpieczeństwa i Podatności Wybranego Urządzenia IoT**

Przeprowadzenie analizy bezpieczeństwa (w kontrolowanym środowisku laboratoryjnym) taniego, komercyjnego urządzenia IoT (np. inteligentne gniazdko, kamera IP, przekaźnik Wi-Fi).

- **Zadania:**
  - Rekonesans sieciowy (skanowanie portów, identyfikacja usług).
  - Analiza komunikacji (przechwytywanie ruchu, np. Wireshark, mitmproxy).
  - Próba ekstrakcji firmware'u i jego podstawowa analiza (np. w poszukiwaniu zaszytych kluczy, haseł).
  - Identyfikacja znanych podatności (CVE).
  - Opracowanie raportu z analizy i rekomendacji (hardening).

## **Temat 10: Stworzenie i Analiza Danych z Honeypota IoT**

Uruchomienie i konfiguracja "honeypota" symulującego popularne, niezabezpieczone urządzenie IoT lub dowolny serwer lub usługę przemysłową (np. otwarty serwer Telnet, niezabezpieczony broker MQTT).

- **Zadania:**

- Wybór i instalacja oprogramowania honeypota (np. Cowrie, lub dedykowany dla IoT/ICS).
- Wystawienie usługi w kontrolowany sposób (lub planu jak usługa można wystawić do sieci).
- Gromadzenie i analiza logów prób ataków (typy ataków, źródła IP, próby logowania) (przykładowe logi można wygenerować samodzielnie).
- Przygotowanie raportu na temat zaobserwowanych zagrożeń ("Threat intelligence").

## **Temat 11: Dogłębna analiza przykładowego ataku na infrastrukturę krytyczną**

Zrozumienie mechaniki realnego incydentu w infrastrukturze krytycznej (IK), łańcucha zdarzeń oraz decyzji obronnych. Efektem ma być raport pokazujący, co się stało, dlaczego, jakie były skutki i jak temu zapobiegać w przyszłości.

Spróbować odpowiedzieć na pytania:

1. Jak wyglądał kontekst organizacyjny i techniczny (architektura, OT/IT, zależności, wymagania ciągłości)?
2. Jakie wektory dostępu zostały wykorzystane (społeczne, procesowe, techniczne) opis ogólny.
3. Łańcuch zdarzeń (timeline): od kompromitacji do wpływu na proces.
4. Skutki: operacyjne, finansowe, prawne, społeczne, wpływ na bezpieczeństwo ludzi/środowiska.
5. Kontrole i luki: co zawiodło (procedury, segmentacja, monitoring, szkolenia, zależności od dostawców)?
6. Dobre praktyki i rekomendacje: co realnie ogranicza podobne ryzyka (organizacyjne, techniczne, procesowe).
7. Wnioski dla IK: które elementy były krytyczne i dlaczego, jak priorytetyzować inwestycje bezpieczeństwa.

### **Metodyka:**

- **Źródła:** oficjalne raporty (CERT/CSIRT, NERC/NIST, firmy reagujące na incydenty), publikacje branżowe, materiały prasowe wysokiej jakości.
- Mapowanie technik: odniesienie do MITRE ATT&CK for ICS (na poziomie taktyk/technik, bez szczegółów eksplotacyjnych).