IT vs OT

Bezpieczeństwo w epoce konwergencji IT i OT

Definicje, różnice, wyzwania i kierunki integracji w kontekście bezpieczeństwa cyfrowego

Spis treści

1. Wprowadzenie

Współczesne organizacje funkcjonują na styku dwóch światów: technologii informacyjnej (IT) oraz technologii operacyjnej (OT). Oba te obszary, choć od lat rozwijane równolegle, coraz częściej się przenikają, co prowadzi do nowych wyzwań związanych z bezpieczeństwem.

Bezpieczeństwo IT koncentruje się na ochronie systemów informacyjnych, danych, użytkowników i aplikacji. Z kolei bezpieczeństwo OT dotyczy ciągłości działania infrastruktury przemysłowej, kontroli procesów fizycznych oraz ochrony ludzi i środowiska. Różnice między tymi domenami nie wynikają jedynie z odmiennych technologii, ale także z innych priorytetów, celów, cykli życia systemów i poziomu akceptacji ryzyka.

W erze cyfrowej transformacji oraz Przemysłu 4.0 zrozumienie tych różnic staje się kluczowe - nie tylko dla specjalistów IT czy inżynierów, ale również dla liderów biznesowych, którzy odpowiadają za całościową odporność organizacji.

2. Podstawowe definicje, kontekst działania i różnice

Technologie IT i OT różnią się w wielu fundamentalnych aspektach – od definicji i głównego przeznaczenia, po priorytety bezpieczeństwa, cykl życia systemów i środowisko działania – jednak pełnią przy tym role komplementarne. IT skupia się na zarządzaniu informacją, wspieraniu procesów biznesowych oraz ochronie danych i użytkowników, funkcjonując głównie w środowisku wirtualnym i logicznym. OT natomiast odpowiada za monitorowanie i sterowanie procesami przemysłowymi w świecie fizycznym, gdzie nadrzędną rolę odgrywa bezpieczeństwo ludzi, niezawodność infrastruktury oraz ciągłość produkcji.

Różnice te sprawiają, że wymagania w zakresie bezpieczeństwa, dostępności oraz sposobu zarządzania systemami znacząco się od siebie różnią – podczas gdy IT opiera się na triadzie CIA (Poufność, Integralność, Dostępność), OT kieruje się zasadą SA (Safety, Availability). W efekcie bezpieczeństwo w obu środowiskach rządzi się odmiennymi zasadami, wynikającymi z różnych priorytetów, modeli ryzyka, architektur systemów i celów operacyjnych. Dla pełnego obrazu poniższa tabela zestawia kluczowe różnice pomiędzy tymi dwiema domenami.

Komentarz techniczny

- **W IT** ważna jest skalowalność i szybkość reakcji – systemy często działają w środowiskach dynamicznych (np. chmura), gdzie priorytetem jest ochrona danych i zgodność z regulacjami.
- **W OT** nadrzędnym celem jest niezawodność i deterministyczne działanie – system musi działać **zawsze**, a jego awaria może mieć bezpośredni wpływ na świat fizyczny (np. wybuch, zalanie, pożar).

Tabela 1

Kluczowe różnice obu technologii

Obszar	Technologie informacyjne IT	Technologie operacyjne OT
Główne cele	Ochrona przed wyciekiem danych, nieautoryzowanym dostępem, naruszeniem prywatności i sabotażem informacyjnym.	Ochrona przed zakłóceniem działania urządzeń, przestojem produkcji, uszkodzeniami fizycznymi i zagrożeniem życia.
Definicja	IT to zbiór technologii służących do przetwarzania, przechowywania, przesyłania i zarządzania danymi cyfrowymi. W jego skład wchodzą m.in. serwery, bazy danych, sieci komputerowe, aplikacje i stacje robocze.	OT to systemy i technologie używane do monitorowania i sterowania procesami fizycznymi w środowiskach przemysłowych, takich jak elektrownie, fabryki, oczyszczalnie czy rafinerie. Przykłady to SCADA, DCS, PLC, HMI, RTU.
Charakter środowiska	Wirtualne, logiczne środowiska – najczęściej chmurowe, sieciowe lub lokalne.	Fizyczne środowiska – sterowanie maszynami, przepływami mediów, regulowanie parametrów procesowych.
Akceptowalność przestoju	Możliwy krótki downtime (planowany lub awaryjny) – w wielu przypadkach łatwy do nadrobienia.	Przestój może powodować ogromne straty finansowe, zagrożenie życia lub katastrofę przemysłową – wymagane działanie w czasie rzeczywistym.
Priorytet bezpieczeństwa (triada CIA vs SA)	Najważniejsze są: Poufność (Confidentiality), Integralność (Integrity) i Dostępność (Availability).	Priorytetem jest: Bezpieczeństwo (Safety) ludzi i maszyn oraz Dostępność (Availability) procesów przemysłowych.
Cykl życia systemów	Krótki – od 3 do 5 lat. Technologie szybko się starzeją i są często wymieniane.	Długi – nawet 15–25 lat. Wiele systemów opiera się na przestarzałych, ale sprawdzonych komponentach (legacy).
Zarządzanie aktualizacjami	Regularne aktualizacje i łatki bezpieczeństwa – często zautomatyzowane.	Aktualizacje rzadkie i trudne – wymagają długiego planowania, testów i często zatrzymania produkcji.

Tabela 1

Kluczowe różnice obu technologii

Obszar	Technologie informacyjne IT	Technologie operacyjne OT
Zarządzanie dostępem	Zaawansowane systemy: Active Directory, LDAP, MFA, role, polityki bezpieczeństwa.	Często lokalne konta, brak centralnego zarządzania, hasła fabryczne – niska kontrola tożsamości.
Protokóły komunikacyjne	Standardowe, szyfrowane protokoły: HTTPS, SMB, SMTP, DNS, RDP.	Przemysłowe protokoły (Modbus, OPC, DNP3, PROFIBUS, PROFINET) – często niezabezpieczone, stworzone bez uwzględnienia cyberzagrożeń.
Wdrażanie zmian	Elastyczne – zmiany można szybko testować i wprowadzać (DevSecOps).	Zmiany wymagają długiego planowania i często fizycznej obecności personelu – konserwatywne podejście.
Zarządzanie ryzykiem	Aktywnie zarządzane przez zespoły SOC, IAM, SIEM	Często manualne, oparte na analizach zagrożeń fizycznych
Użytkownicy	Pracownicy biurowi, administratorzy IT	Inżynierowie, operatorzy maszyn, technicy
Dostęp do sieci	Zwykle połączone z Internetem	Często izolowane lub ściśle kontrolowane
Awaria	Przestój systemu – wpływ na dane lub użytkowników	Przestój – wpływ na bezpieczeństwo ludzi/produkcji
Skutki incydentu	Utrata danych, kradzież informacji, naruszenie RODO	Przestoje produkcji, uszkodzenie sprzętu, zagrożenie życia
Dostępność aktualizacji	Regularne aktualizacje i łatki	Rzadkie i trudne do wdrożenia (ryzyko zatrzymania systemu)
Detekcja zagrożeń	IDS/IPS, EDR, XDR	Monitorowanie sieci przemysłowej (np. Nozomi, Claroty, Dragos)
Przykładowe zastosowania	Systemy ERP, CRM, poczta elektroniczna, bazy danych, systemy płatności.	Linie produkcyjne, turbiny w elektrowniach, systemy dozowania chemikaliów, systemy wentylacji w tunelach.

3. Model Purdue – struktura hierarchiczna systemów OT

Model Purdue (Purdue Enterprise Reference Architecture, PERA) to jedna z najczęściej stosowanych koncepcji opisu architektury systemów przemysłowych. Powstał w latach 90. XX wieku na Uniwersytecie Purdue jako odniesienie dla przemysłu w zakresie planowania i zarządzania systemami produkcyjnymi. Do dziś stanowi fundament wielu standardów i dobrych praktyk w obszarze OT, w tym normy ISA-95 oraz IEC 62443, które szeroko wykorzystują ten podział przy projektowaniu i zabezpieczaniu infrastruktury.

Model składa się z sześciu warstw (od poziomu 0 do 5), które przedstawiają hierarchiczną strukturę systemów przemysłowych – od elementów fizycznych w zakładzie produkcyjnym aż po warstwę biznesową i integrację z rozwiązaniami chmurowymi. Każdy poziom ma swoją specyfikę, cele oraz technologie, które tam dominują:

- Poziom 0 – Proces fizyczny: obejmuje urządzenia wykonawcze i sensoryczne odpowiedzialne za fizyczne działanie procesu, takie jak silniki, zawory, czujniki temperatury, ciśnienia czy przepływu. Na tym poziomie powstają dane pierwotne, które następnie są przesyłane wyżej w strukturze.
- Poziom 1 – Sterowanie: tutaj znajdują się programowalne sterowniki logiczne (PLC) i zdalne jednostki terminalowe (RTU), które bezpośrednio kontrolują procesy fizyczne, zbierają sygnały z czujników i sterują aktuatorami.
- Poziom 2 – Sterowanie nadzorcze: obejmuje systemy SCADA (Supervisory Control and Data Acquisition) oraz interfejsy HMI (Human-Machine Interface). To tutaj operatorzy otrzymują wizualizację procesów i mogą podejmować decyzje na podstawie bieżących danych.
- Poziom 3 – Zarządzanie produkcją: to warstwa systemów MES (Manufacturing Execution Systems), odpowiedzialnych za monitorowanie wydajności produkcji, raportowanie, kontrolę jakości czy planowanie zasobów produkcyjnych w czasie rzeczywistym.
- Poziom 4 – Zarządzanie przedsiębiorstwem: obejmuje systemy typowe dla IT, takie jak ERP (Enterprise Resource Planning) czy CRM (Customer Relationship Management), które wspierają zarządzanie finansami, logistyką, sprzedażą i innymi obszarami biznesowymi.
- Poziom 5 – Połączenie z chmurą i internetem: to warstwa najnowsza, związana z transformacją cyfrową i Przemysłem 4.0. Obejmuje rozwiązania Business Intelligence, zaawansowaną analitykę danych, machine learning, predykcyjne utrzymanie ruchu oraz zdalny dostęp do systemów.

Granica IT/OT tradycyjnie przebiega pomiędzy poziomem 3 a 4 – powyżej znajdują się systemy stricte biznesowe (IT), poniżej zaś warstwy związane bezpośrednio z procesami przemysłowymi (OT). To miejsce jest szczególnie newralgiczne z punktu widzenia cyberbezpieczeństwa, ponieważ stanowi punkt styku dwóch światów o różnych priorytetach i wymaganiach. Atak przechodzący przez tę granicę może z jednej strony zagrozić ciągłości procesów przemysłowych, a z drugiej – narazić na wyciek lub manipulację danymi biznesowymi.

W praktyce Model Purdue służy dziś nie tylko jako schemat organizacji systemów przemysłowych, ale także jako narzędzie projektowania segmentacji sieci, definiowania polityk bezpieczeństwa i planowania obrony w architekturze defense-in-depth. W erze rosnącej konwergencji IT/OT i rozwoju IIoT (Industrial Internet of Things) model ten staje się fundamentem dla wdrażania nowoczesnych standardów bezpieczeństwa w przemyśle.

4. Główne wyzwania w bezpieczeństwie OT

Systemy IT i OT, choć pełnią odmienne role w organizacjach, stoją dziś przed równie poważnymi wyzwaniami w obszarze bezpieczeństwa. IT, będące fundamentem współczesnych procesów biznesowych, odpowiada za przetwarzanie, przechowywanie i ochronę danych, jednak dynamiczny rozwój technologii, chmury i mobilności sprawia, że utrzymanie jego bezpieczeństwa staje się coraz trudniejsze. Z kolei OT, projektowane pierwotnie jako środowiska izolowane i dedykowane wyłącznie do sterowania procesami przemysłowymi, nie uwzględniało w swojej architekturze współczesnych zagrożeń cybernetycznych. W efekcie bezpieczeństwo OT napotyka liczne bariery technologiczne, organizacyjne i kulturowe. Zrozumienie tych różnic i wyzwań jest kluczowe dla budowy skutecznej strategii ochrony całej organizacji.

Obszar wyzwania	IT (Information Technology)	OT (Operational Technology)
Dziedzictwo technologiczne (legacy systems)	Starsze systemy (np. Windows Server 2003/2008, stare ERP), brak wsparcia, trudności w migracji krytycznych aplikacji.	Urządzenia i oprogramowanie działające 10–30 lat, brak aktualizacji od producenta, brak obsługi nowoczesnych mechanizmów bezpieczeństwa.
Segmentacja i architektura sieci	Często brak segmentacji lub Zero Trust, płaskie sieci sprzyjające lateral movement i rozprzestrzenianiu malware.	Brak izolacji między IT i OT, łączenie z Internetem bez DMZ, zagrożenie przenoszeniem ataków z IT do OT.
Aktualizacje i patchowanie	Łatki instalowane z opóźnieniem z powodu kompatybilności, brak testów, problemy z endpointami mobilnymi.	Aktualizacje rzadkie (czasem co kilka lat), wymagają przestojów, brak środowisk testowych, obawy o destabilizację procesów.
Czynnik ludzki / świadomość	Użytkownicy padają ofiarą phishingu, słabe hasła, brak MFA, shadow IT, brak przestrzegania polityk bezpieczeństwa.	Inżynierowie skupieni na ciągłości operacyjnej, niska świadomość cyberzagrożeń, bagatelizowanie ryzyka związanego z siecią.
Narzędzia i polityki bezpieczeństwa	Duża liczba rozproszonych narzędzi (EDR, SIEM, SOAR, DLP), trudna integracja, problemy w środowiskach hybrydowych i chmurowych.	Narzędzia IT (np. EDR, DLP) często niekompatybilne z PLC/RTU/SCADA, mogą zakłócać procesy sterowania.
Standardy i zarządzanie ryzykiem	Brak wdrożenia ISO 27001/NIST CSF, marginalizacja roli CISO, bezpieczeństwo traktowane jako dodatek.	Niewdrożone normy (IEC 62443, NIST SP 800-82), brak polityk bezpieczeństwa OT, brak dedykowanych ról (np. OT Security Officer).
Monitorowanie i detekcja zagrożeń	Alert fatigue w SOC, brak widoczności w chmurze i IoT, ograniczone zasoby kadrowe w IR.	IDS/IPS często nie rozumieją protokołów przemysłowych, brak pełnej widoczności ruchu, trudności w szybkiej reakcji na incydenty.
Priorytet bezpieczeństwa	Triada CIA: Poufność > Integralność > Dostępność.	Model SA: Safety > Availability > Confidentiality.

Podsumowanie wyzwań

Bezpieczeństwo IT i OT, choć mają wspólny cel ochrony organizacji, opiera się na odmiennych priorytetach i wymaga różnego podejścia. W środowisku OT kluczowe znaczenie ma niezawodność systemów, ciągłość operacyjna oraz bezpieczeństwo ludzi i procesów – dlatego nie można wdrażać zabezpieczeń metodą „kopiuj-wklej" z IT. Wymaga to zrozumienia specyfiki infrastruktury przemysłowej, ścisłej współpracy między zespołami i zastosowania narzędzi oraz procedur, które nie zakłócą produkcji. Z kolei bezpieczeństwo IT koncentruje się na ochronie danych i użytkowników, a ze względu na dynamicznie zmieniające się zagrożenia wymaga ciągłej adaptacji, spójnych polityk, świadomych działań personelu i zintegrowanych procesów reagowania. Tylko połączenie obu perspektyw pozwala budować skuteczną i całościową strategię cyberbezpieczeństwa organizacji.

5. Przykładowe incydenty – różne światy, wspólne zagrożenia

Zarówno systemy IT, jak i OT padają ofiarą cyberataków, jednak skutki tych incydentów różnią się zasadniczo. W środowisku IT dominują skutki finansowe, utrata danych i naruszenie prywatności. W OT – skutki są często fizyczne: uszkodzenie infrastruktury, zatrzymanie produkcji, zagrożenie życia i środowiska. Poniżej zestawiono kluczowe przypadki obrazujące te różnice.

Incydenty w środowisku IT

Przypadek	Opis	Skutek
WannaCry (2017)	Globalny atak ransomware wykorzystujący lukę w SMBv1 (EternalBlue). Szyfrował dane i żądał okupu w bitcoinach.	Setki tysięcy komputerów zaszyfrowanych w 150+ krajach. Utrata danych, przestoje systemów szpitalnych (np. NHS UK), szkody finansowe.
Equifax (2017)	Wyciek danych osobowych i finansowych 147 mln Amerykanów po ataku przez lukę w Apache Struts.	Naruszenie prywatności, olbrzymie kary, spadek zaufania do firmy.
SolarWinds (2020)	Zaawansowany atak supply chain – złośliwy kod trafił do aktualizacji oprogramowania Orion.	Infekcja sieci wielu instytucji rządowych i korporacji (USA, Microsoft, FireEye), szpiegostwo, wyciek danych.

Incydenty w środowisku OT

Przypadek	Opis	Skutek
Stuxnet (2009–2010)	Zaawansowany robak stworzony przez USA/Izrael, atakujący irańskie wirówki nuklearne przez złośliwe sterowanie PLC Siemens.	Fizyczne uszkodzenie ponad 1000 wirówek. Pierwszy udokumentowany cyfrowy sabotaż infrastruktury przemysłowej.
Ukraina Blackout (2015, 2016)	Ataki na sieć energetyczną Ukrainy. Hakerzy uzyskali zdalny dostęp do SCADA i wyłączyli zasilanie w wielu regionach.	Brak prądu dla setek tysięcy ludzi. Pokaz możliwości ataku na infrastrukturę krytyczną.
Colonial Pipeline (2021)	Ransomware (DarkSide) zaatakował amerykański system zarządzania ropociągiem. Choć system OT nie został zainfekowany, firma prewencyjnie go wyłączyła.	Zakłócenia w dostawach paliwa na Wschodnim Wybrzeżu USA, panika konsumencka, wzrost cen paliw.

Porównanie skutków

Kryterium	IT	OT
Cel ataku	Dane, pieniądze, reputacja.	Procesy, urządzenia, infrastruktura fizyczna.
Następstwa	Kradzież danych, blokada systemów, wycieki, straty finansowe.	Uszkodzenia fizyczne, przestoje produkcyjne, zagrożenie życia, skażenie środowiska.
Widoczność	Często wykrywane z opóźnieniem, ale śledzone przez SOC.	Trudne do wykrycia w czasie rzeczywistym, brak SIEM lub IDS w wielu zakładach.
Zasięg	Globalny (np. phishing, ransomware).	Regionalny/lokalny, ale z potencjalnie krytycznym wpływem.

Wnioski praktyczne

- Środowiska OT nie są już izolowane – cyberzagrożenia z IT mogą przenikać do systemów sterujących.
- Nawet incydenty IT (np. ransomware) mogą pośrednio spowodować wyłączenie produkcji.
- Potrzebne są scenariusze wspólnych reakcji (IT/OT Incident Response) oraz zintegrowane centra monitoringu (IT/OT SOC).

6. Integracja IT/OT – kluczowe rekomendacje

W miarę jak rośnie stopień cyfryzacji procesów przemysłowych, granice między środowiskami IT i OT coraz bardziej się zacierają. Technologie takie jak IIoT (Industrial Internet of Things), zdalny monitoring, analityka danych w czasie rzeczywistym czy integracja ERP z systemami SCADA powodują, że dawniej odseparowane światy muszą współdziałać.

Ta integracja niesie ze sobą wiele korzyści operacyjnych, ale także nowe zagrożenia. Poniżej przedstawiono zestaw praktycznych rekomendacji, które wspierają bezpieczne połączenie IT i OT, bez narażania infrastruktury krytycznej na cyberataki.

Zastosuj model referencyjny Purdue

Model Purdue dzieli systemy na warstwy (od poziomu fizycznych urządzeń po zarządzanie biznesowe) i umożliwia ich logiczne rozgraniczenie:

- Ułatwia segmentację sieci.
- Pozwala określić, gdzie i jak przepływają dane.
- Pomaga zdefiniować punkty kontroli i granice bezpieczeństwa (trust boundaries).

Kluczowa zasada: nie dopuszczać ruchu bezpośredniego między poziomem IT (warstwy 4/5) a poziomem produkcyjnym (warstwa 0/1).

Wprowadź segmentację i strefy DMZ (Demilitarized Zone)

Zastosuj architekturę sieciową, która rozdziela:

- sieć korporacyjną (IT),
- strefę buforową (DMZ),
- sieć przemysłową (OT).

Strefy te powinny być oddzielone zaporami sieciowymi (firewall) oraz nadzorowane za pomocą list kontroli dostępu (ACL) i reguł inspekcji ruchu.

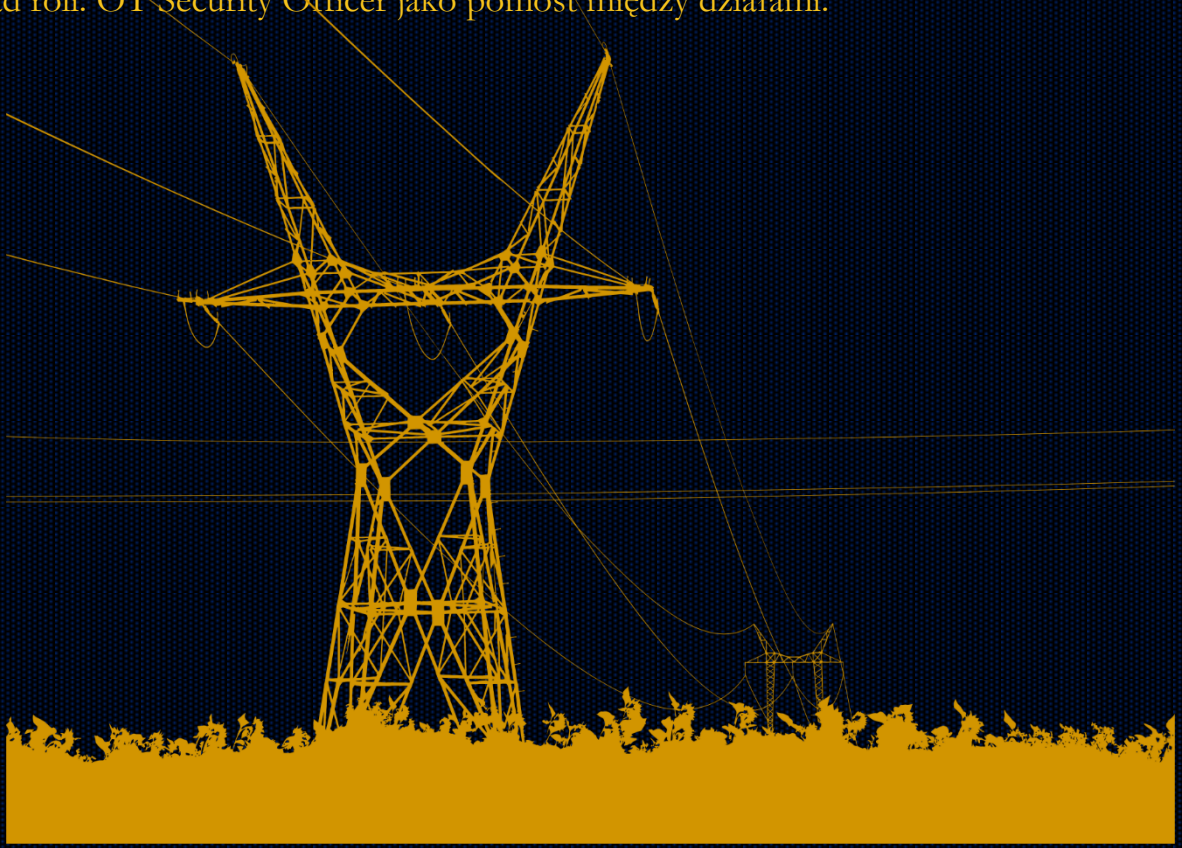
DMZ może zawierać bezpieczne punkty wymiany danych (np. serwery Historian, serwery OPC UA Gateway).

Zbuduj zespół hybrydowy: IT + OT

Stwórz międzydziałowy zespół ds. cyberbezpieczeństwa przemysłowego, który:

- rozumie zarówno wymogi procesów przemysłowych, jak i aktualne zagrożenia cybernetyczne,
- potrafi przetłumaczyć język IT na język inżynierii i odwrotnie,
- wspólnie tworzy polityki bezpieczeństwa oraz plany reagowania na incydenty.

Przykład roli: OT Security Officer jako pomost między działami.



Szkolenie personelu OT z zakresu cyberbezpieczeństwa

Operatorzy, technicy i inżynierowie OT:

- muszą rozumieć podstawowe zagrożenia cyfrowe (phishing, ransomware, USB malware),
- powinni znać zasady „cyberhigieny" – np. politykę haseł, zakaz podłączania nieautoryzowanych urządzeń,
- powinni uczestniczyć w testach i symulacjach (np. tabletop exercises).

Stwórz i wdrażaj wspólne polityki i procedury bezpieczeństwa IT/OT

Dokumenty takie jak:

- polityka dostępu do systemów sterowania,
- polityka aktualizacji w środowisku przemysłowym,
- plan zarządzania incydentem OT (z integracją z IT-SOC),
- plan backupów i odtwarzania środowisk przemysłowych powinny być tworzone wspólnie i uwzględniać ograniczenia oraz wymagania obu domen.

Stosuj uznane standardy i normy bezpieczeństwa

Wdrożenie ram regulacyjnych takich jak:

- IEC 62443 – kompleksowy zestaw norm dla bezpieczeństwa systemów automatyki przemysłowej,
- NIST SP 800-82 – przewodnik dla bezpieczeństwa ICS w środowisku amerykańskim,
- NIST CSF – ogólne podejście do zarządzania ryzykiem, możliwe do adaptacji w OT,
- ENISA Guidelines for ICS/SCADA – europejskie rekomendacje dotyczące systemów przemysłowych

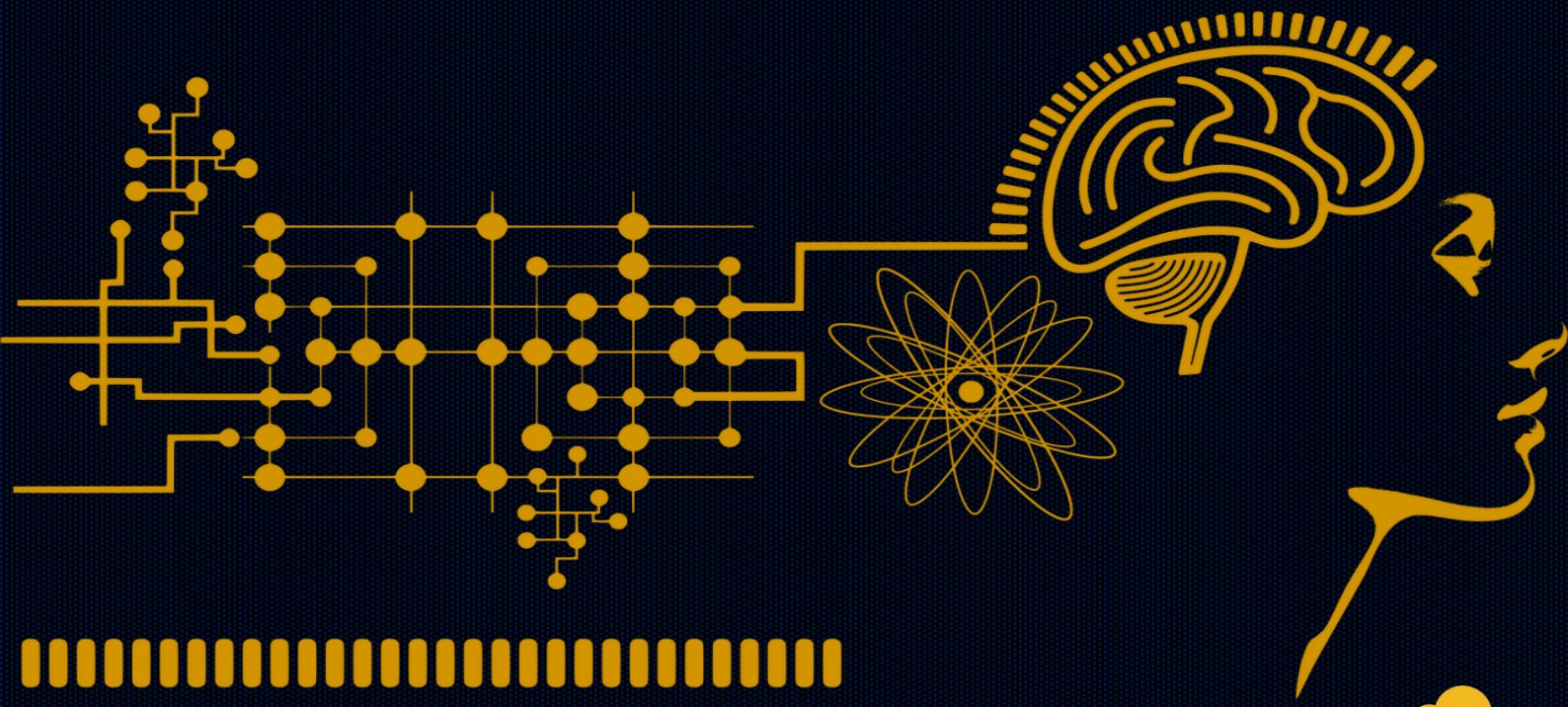
pozwala na standaryzację działań oraz ułatwia audyty, zgodność i rozwój strategii bezpieczeństwa.

Monitoruj, wykrywaj i reaguj – także w OT

- Wdrażaj pasywne systemy IDS (np. Nozomi, Claroty, Zeek dla ICS), które nie zakłócają działania procesów.
- Analizuj anomalia w ruchu przemysłowym.
- Integruj logi z systemów OT z SIEM lub SOC (z odpowiednim filtrowaniem i korelacją).
- Planuj testy penetracyjne i symulacje w kontrolowanym środowisku.

Podsumowanie rekomendacji

Bezpieczna integracja IT i OT to nie jednorazowy projekt – to proces ciągły. Wymaga wspólnej strategii, zrozumienia celów obu środowisk oraz ścisłej współpracy ludzi, technologii i procesów.



7. Zmiana paradygmatu

Relacja między IT a OT uległa w ostatnich latach znaczącej zmianie. To, co dawniej funkcjonowało w odseparowanych silosach, dziś coraz częściej tworzy zintegrowany ekosystem, w którym granice między światem informatyki a automatyką przemysłową zacierają się. Poniższe zestawienie pokazuje, jak ewoluowało podejście do roli i bezpieczeństwa obu obszarów.

Dawniej	Obecnie
IT i OT działały osobno, z minimalną wymianą danych	IT i OT są zintegrowane – dane płyną w obu kierunkach
IT odpowiadało za cyberbezpieczeństwo	Odpowiedzialność rozciąga się na działy techniczne, operacyjne, zarządcze
OT było domeną inżynierów i automatyki	OT staje się częścią cyfrowej transformacji przedsiębiorstwa
Bezpieczeństwo OT było oparte głównie na izolacji	Teraz musi opierać się na aktywnym zarządzaniu ryzykiem

8. Podsumowanie

Choć systemy IT i OT przez lata rozwijały się w odmiennych kierunkach – zarówno technologicznie, jak i organizacyjnie – obecna rzeczywistość biznesowa i przemysłowa zmusza je do współistnienia w coraz bardziej wspólnym, wzajemnie zależnym ekosystemie. Wprowadzenie koncepcji Przemysłu 4.0, cyfrowych bliźniaków (Digital Twin), zdalnego sterowania czy integracji ERP z systemami produkcyjnymi zatarło dawną granicę między danymi a procesami fizycznymi.

W tym nowym układzie:

- IT nie może postrzegać OT jako „zamkniętej czarnej skrzynki", odpornej na cyfrowe zagrożenia.
- OT nie może dłużej ignorować zasad i praktyk cyberbezpieczeństwa, które w IT są standardem.

Bezpieczeństwo informacji, ciągłość działania, ochrona infrastruktury i bezpieczeństwo ludzi są dziś nierozerwalnie powiązane. Dlatego:

- systemy muszą być projektowane, utrzymywane i monitorowane w sposób holistyczny,
- zespoły IT i OT muszą współpracować ponad strukturami organizacyjnymi,
- kierownictwo organizacji musi traktować bezpieczeństwo jako element strategiczny, nie tylko techniczny.

9. Kluczowe wnioski końcowe

- Wiedza o różnicach między IT i OT jest niezbędna do budowania skutecznych systemów bezpieczeństwa.
- Zagrożenia IT coraz częściej wpływają na infrastrukturę przemysłową – ataki ransomware, APT czy exploity systemów SCADA to realne ryzyka.
- Bezpieczeństwo OT nie może być traktowane jako problem wyłącznie technologiczny – to kwestia ciągłości operacji, ochrony życia i reputacji firmy.
- Standaryzacja i współpraca (np. wg IEC 62443, NIST SP 800-82) to fundament do budowania odporności.
- Ludzie, procesy i technologia muszą działać spójnie – bezpieczeństwo to nie produkt, lecz proces.

O autorze

Wojciech Sikorski – inżynier z doświadczeniem w energetyce, który połączył swoją pasję do technologii z cyberbezpieczeństwem. Twórca marki Hacktrick, gdzie świat OT spotyka się z IT, a teoria z praktyką. Autor licznych publikacji na tematy związane z przemysłem oraz cyberbezpieczeństwem. Moim nadrzędnym celem jest uczynić cyberbezpieczeństwo naturalną częścią przemysłu i infrastruktury krytycznej – nie dodatkiem, lecz fundamentem.

Kontakt

Strona: www.hacktrick.pl

E-mail: kontakt@hacktrick.pl

Współpraca

- Chcesz dowiedzieć się, jak bezpiecznie integrować świat IT i OT?
- Szukasz wsparcia w ocenie ryzyka lub wdrożeniu norm bezpieczeństwa?
- Interesują Cię praktyczne narzędzia i frameworki dla OT Security?

Zapraszam do kontaktu - razem możemy zbudować bezpieczniejszą przyszłość przemysłu.