SABUR OT
Cybersecurity System

Systemy automatyki

Twoje IT
jest już odpowiednio zabezpieczone.
To bardzo dobrze.

A Twoje OT?
Czy ono także jest bezpieczne?

IEC 62443

Zabezpieczymy Twój system OT na dziś i na przyszłość

Oferujemy pomoc i wsparcie od oceny automatyzacji i infrastruktury OT, poprzez ocenę własnych ryzyk, planowanie konkretnych działań i ustalenie celów aż po wdrożenie i kontrolę.

1. Audyt bezpieczeństwa w warstwie procesowo-organizacyjnej w obszarze OT w oparciu o wybrany standard cyberbezpieczeństwa
2. Inwentaryzacja i ocena bezpieczeństwa elementów w wybranych/ kluczowych instalacjach OT
3. Realizacja analizy konfiguracji bezpieczeństwa wybranej próbki urządzeń OT dla kluczowych instalacji OT
4. Opracowanie rekomendacji dalszych działań mających na celu podniesienie poziomu cyberbezpieczeństwa OT
5. Realizacja zapisów rekomendacji:
   - Dostarczenie rozwiązań (software, hardware)
   - Zalecenia konfiguracji/ konfiguracja urządzeń i systemu zarządzania OT
6. Nadzór nad wdrożeniem
7. Testowanie rozwiązania w środowisku preprodukcyjnym
8. Nadzór nad eksploatacją:
   - Dostarczanie aktualizacji
   - Serwis/ umowa serwisowa
   - Monitoring ruchu w sieci
   - Analiza zdarzeń

8 Kroków do cyber bezpieczeństwa

SABUR OT Cybersecurity System

System IDS (Intrusion Detection System)

- Zarządzanie ryzykiem biznesowym oraz operacyjnym dostarcza wiedzę na temat bieżącej architektury sieci: identyfikuje urządzenia, rysuje mapy sieci, monitoruje krytyczne procesy poprzez analizę ruchu automatyki wspierając proces zarządzania ryzykami oraz ciągłością działania.
- Monitoring systemów automatyki przemysłowej z wykorzystaniem zaawansowanego silnika analitycznego, który z połączeniu z modelami sztucznej inteligencji natychmiast identyfikuje zdarzenia odbiegające od standardowego zachowania sieci przemysłowej.
- Dostosowanie procedur do wymogów prawnychpolega m.in na kwalifikacji zdarzenia w incydent z jednoczesnym zapisaniem historii procesu, podjętych działa, osób odpowiedzialnych oraz kopią ruchu, która dokumentuje przebieg incydentu.

BEZPIECZEŃSTWO OPROGRAMOWANIA

PcVue

- Bezpieczny pakiet instalacyjny
- Uwierzytelnianie i integralność
- Bezpieczne pobieranie
- Szyfrowanie pliku konfiguracyjnego
- Zaawansowane uprawnienia użytkownika
- Integracja z Active Directory
- Przemysłowe zapory sieciowe/VPN
- **Certyfikat zgodności IEC 62443-4-1 i 62443-4-2**

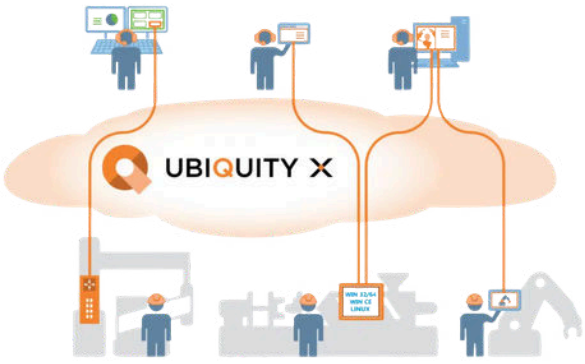
supervisor Saia PCD®

- Uwierzytelnianie użytkowników
- Szyfrowanie danych
- Zarządzanie rolami i uprawnieniami
- Rejestracja zdarzeń w dzienniku audytu

BEZPIECZNY ZDALNY DOSTĘP

UBIQUITY

- Przemysłowe, bezpieczne połączenie VPN
- Protokoły SSL/TLS
- Szyfrowanie asymetryczne
- Certyfikat X509
- Zarządzanie użytkownikami
- Autoryzacja połączeń
- Uwierzytelnienie, także dwuskładnikowe
- Polityka haseł
- **Certyfikat zgodności IEC 62443-3-3 i 62443-4-2**



Cyberbezpieczny system sterowania

BEZPIECZNY SYSTEM STEROWANIA

Saia PCD QronoX

- **Certyfikat zgodności z IEC 62443, SL3+**
- Bezpieczny Webserwer (HTTPS)
- Wbudowany Firewall
- Redundancja
- System operacyjny czasu rzeczywistego QNX
- Zarządzanie użytkownikami
- Szyfrowane protokoły, np. OPC UA

Optimizer Advanced Controller

- **Certyfikat zgodności z IEC 62443** na poziomie projektu i produktu
- Freamwork Niagara
- Obsługa protokołów szyfrowanych
- Opcje separacji sieci komunikacyjnych
- Szyfrowanie danych
- Autoryzacja, uwierzytelnienie

BEZPIECZNA KOMUNIKACJA

M!DGE i RipEX

- Kontrola dostępu oparta na rolach
- RADIUS, VLAN, Firewall L2, L3, L4, NAT
- Szyfrowanie AES-256-CCM (tylko dla RipEX)
- Ipsec, OpenVPN
- Syslog, SNMP, SMS
- FW z podpisem cyfrowym
- Wykrywanie sabotażu sprzętowego – HW Tamper
- Definiowanie użytkowników opartE na rolach
- Ograniczenie dostępu do tylko używanych interfejsów fizycznych i logicznych
- Zdalny dostęp szyfrowany QSSH
- Aktualizacja FW

BEZPIECZNA KOMUNIKACJA

INDUSTRIAL ROUTER RK2X

- Bezpieczny zdalny dostęp do infrastruktury OT przez szyfrowane VPN
- Wbudowana platforma UBIQUITY certyfikowana zgodnie z **IEC 62443**
- Segmentacja i separacja sieci IT/OT
- Zdalny dostęp do urządzeń wyposażonych w interfejsy szeregowe
- Zdalny dostęp do sterowników PLC, HMI i systemów SCADA
- Łączność Ethernet, Wi-Fi i 4G LTE dla rozproszonych instalacji
- Centralne zarządzanie dostępem serwisowym do maszyn i instalacji przemysłowych

Szkolenie - Cyberbezpieczeństwo systemów OT

Wymagania dotyczące cyberbezpieczeństwa przestały być rekomendacją — stały się obowiązkiem. Zwiększ kompetencje swoich zespołów i przygotuj systemy OT do wymogów wynikających z NIS2 i UKSC.

Dla kogo jest to szkolenie?

- dla partnerów wdrożeniowych, integratorów i projektantów systemów automatyki,
- zespołów OT/UR i operatorów instalacji,
- IT / SOC współpracujących z OT,
- przedstawicieli podmiotów ważnych, kluczowych i krytycznych (wg UKSC),
- osób odpowiedzialnych za NIS2/UKSC, IEC 62443 i ciągłość działania.

Najważniejsze daty:

- 3 kwietnia 2026 r. – nowelizacja ustawy o KSC, wchodzi w życie.
- 3 października 2026 r. – upływa termin na złożenie przez podmioty kluczowe i ważne wniosku o wpis do wykazu.
- 3 kwietnia 2027 r. – upływa termin na wdrożenie przez podmioty kluczowe i ważne, obowiązków wynikających z ustawy.
- 3 kwietnia 2028 r. – upływa termin przeprowadzenia pierwszego obowiązkowego audytu cyberbezpieczeństwa.

To takie proste!

1

Rejestracja

Wypełnij formularz, a nasz zespół skontaktuje się z Tobą.

2

Szkolenie

Ucz się od naszych ekspertów, zadawaj pytania, dyskutuj.

3

Certyfikat

Odbierz certyfikat i wykorzystaj zdobytą wiedzę w praktyce!

Co zyskasz dzięki uczestnictwu?

- Jasność, co i w jakiej kolejności wdrożyć w OT.
- Wiedzę niezbędną do opracowania spójnego planu działań — od architektury zabezpieczeń po procedury operacyjne — zgodnie z wymaganiami NIS2/UKSC oraz najlepszymi praktykami IEC 62443.
- Umiejętność rozpoznawania i zabezpieczania kluczowych obszarów OT.
- Nauczysz się, jak w praktyce stosować zasady segmentacji, bezpiecznego dostępu, kontroli uprawnień, monitoringu, obsługi incydentów oraz utrzymania konfiguracji — tak, by realnie zmniejszyć ryzyko w środowisku operacyjnym.
- Zgodność z wymaganiami regulacyjnymi - szkolenie spełnia wymóg podnoszenia kompetencji zespołu oraz obowiązku szkoleniowego dla kadry kierowniczej wynikającego z NIS2. Dzięki temu Twoja organizacja może wykazać należyte działania w zakresie zarządzania ryzykiem i zapewniania cyberbezpieczeństwa OT.

Szczegółowe informacje na temat zakresu i warunków szkolenia:
https://www.sabur.com.pl/szkolenia-ot-cyberbezpieczenstwo-systemow-ot/

Kontakt

SABUR Systemy automatyki

SABUR Sp. o.o.
ul. Puławska 303
02-785 Warszawa

+48 22 549 43 53
sabur@sabur.com.pl
www.sabur.com.pl

NCC-PL · Centrum Projektów Polska Cyfrowa · ECCC · Co-funded by the European Union