OT CYBER CHALLENGE – INSTRUKCJA PRZESYŁANIA ZGŁOSZEŃ

1. Zgłoszenie należy złożyć za pośrednictwem formularza zgłoszeniowego umieszczonego na stronie https://www.gov.pl/web/cyber-nccpl/ot-cyber-challenge do 10 maja 2026 r. (do godziny 23:59).
2. Zgłoszenie przesłane w inny sposób niż określony w pkt 1 nie będzie rozpatrywane.
3. Przed przystąpieniem do wypełniania formularza zgłoszeniowego uprzejmie prosimy o sprawdzenie, czy spełniają Państwo wymagane warunki:
    a) jesteście autorami rozwiązania w obszarze cyberbezpieczeństwa OT/ICS,
    b) macie siedzibę na terenie Polski,
    c) udział kapitału polskiego w waszej organizacji wynosi co najmniej 51%,
    d) prowadzicie od co najmniej 1 roku działalność polegającą na oferowaniu lub opracowywaniu rozwiązań w obszarze cyberbezpieczeństwa OT/ICS,
    e) posiadacie pełną zdolność do czynności prawnych.
4. Polecamy zapoznanie się z Regulaminem Konkursu zamieszczonym na stronie https://www.gov.pl/web/cyber-nccpl/ot-cyber-challenge
5. Pola formularza należy wypełnić w języku polskim.
6. Wszystkie pola formularza muszą zostać wypełnione. Wymogiem udziału w Konkursie jest akceptacja wszystkich oświadczeń zawartych w formularzu.
7. Wskazane jest, by zgłoszenie wypełniał prezes, właściciel lub inna osoba uprawniona do reprezentowania podmiotu.
8. **UWAGA**: Konstrukcja formularza nie pozwala na zapisanie kolejnych wersji odpowiedzi. Zachęcamy do archiwizowania odpowiedzi w osobnym dokumencie.
9. Do formularza zgłoszeniowego należy dołączyć prezentację w formacie pdf lub pptx, zawierającą maksymalnie 15 slajdów. Maksymalna wielkość pliku to 10 MB. Prosimy o zwięzłe i jasne opisy pozwalające zrozumieć charakter zgłaszanego rozwiązania i jego atuty.
   Prezentacja musi zawierać następujące informacje:
   - Informacje o podmiocie:
     a) rodzaj podmiotu, jego wielkość, lokalizacja,
     b) struktura kapitałowa podmiotu (tj. wskazanie krajów, z których pochodzi kapitał organizacji z określeniem wielkości poszczególnych udziałów),
     c) krótki opis obszaru działalności podmiotu,
     d) data, od której podmiot oferuje bądź opracowuje rozwiązania w obszarze cyberbezpieczeństwa OT/ICS,
     e) informacje o rezydencji - gdzie przechowywane są dane użytkowników,
     f) praktyki bezpieczeństwa – informacje jak firma zapewnia bezpieczeństwo swojej infrastruktury i wdraża ocenę bezpieczeństwa, w tym bezpieczeństwo osobowe (pracownicy)?
     g) opcjonalnie – inne informacje dotyczące organizacji, które aplikujący chciałby przekazać, np. liczba klientów, lista głównych klientów, informacja czy wśród klientów firmy są operatorzy IK, podmiotów objętych dyrektywą NIS2, administracja publiczna, informacja jak długo podmiot działa na rynku, uzyskane certyfikaty branżowe, uzyskane akredytacje związane z bezpieczeństwem informacji itp.
   - Opis zgłaszanego rozwiązania:
     a) Istota rozwiązania – czym jest, jak działa, w jakim celu się je stosuje, dla kogo jest dedykowane/przez kogo może być stosowane (grupy odbiorców);
     a) Przykładowy sposób użycia rozwiązania (use cases),
     b) Wyjaśnienie dlaczego to rozwiązanie jest potrzebne i w jaki sposób odpowiada na aktualne potrzeby rynku;
     c) Czy to rozwiązanie różni się czymś od innych rozwiązań już dostępnych na rynku?

d) Łatwość wdrożenia – jak szybko można wdrożyć rozwiązanie i ile zasobów jest do tego potrzebnych, czy istnieją jakieś bariery w jego wdrażaniu?
e) Potencjał integracyjny – jak to rozwiązanie może zintegrować się z ramami IT i innymi produktami cyberbezpieczeństwa?
f) Możliwość utrzymania – jaki rodzaj zasobów i w jakiej liczbie jest potrzebny do monitorowania rozwiązania, jak przebiega utrzymanie rozwiązania i czy wymaga to zatrudnienia lub zaangażowania stron trzecich?
g) Bezpieczeństwo samego rozwiązania i jego odporność na zagrożenia w cyberprzestrzeni - jakie narzędzia, technologie, strategie w celu zapewnienia bezpieczeństwa informacji (czyli poufności, integralności, dostępności) lub ochrony przed cyberzagrożeniami zastosowano w rozwiązaniu, czy rozwiązanie było testowane?
h) Jeśli rozwiązanie przeszło pomyślnie proces certyfikacji – wskazanie uzyskanego certyfikatu;
i) Jaka jest najważniejsza korzyść z rozwiązania w każdym z aspektów – biznesowa, społeczna, edukacyjna, usprawniająca, innowacyjna?
j) Argumenty, dlaczego właśnie w to rozwiązanie warto jest zainwestować.