

Zakres programu „Innowacje dla odporności”

Innowacja może mieć różne oblicza. Nie zawsze oznacza stworzenie rozwiązania od podstaw. Czasem polega na nowym zastosowaniu dostępnej technologii, połączeniu danych z różnych źródeł lub istotnej zmianie dotychczasowego sposobu działania.

Poniższe kryteria i przykłady pokazują, jakie projekty wpisują się w zakres programu „Innowacje dla odporności” i pomagają odróżnić innowacyjne rozwiązania od standardowych działań w zakresie bezpieczeństwa.

Definicja innowacyjnego rozwiązania

Na potrzeby programu „innowacyjne rozwiązanie” oznacza rozwiązanie, które w porównaniu ze standardowym sposobem zarządzania danym ryzykiem:

- wykorzystuje nowe technologie, dane, metody lub sposób organizacji działań;
- służy wcześniejszemu wykrywaniu zagrożeń, przewidywaniu szkód, ograniczaniu ich skutków albo szybszemu przywróceniu działalności;
- wprowadza zmianę istotną dla organizacji, jej procesów lub poziomu odporności;
- ma określony sposób pomiaru rezultatów;
- może być rozwijane lub zastosowane w innych lokalizacjach, procesach albo przedsiębiorstwach.

Innowacyjne rozwiązania w obszarze cyberbezpieczeństwa

Za innowacyjny projekt z zakresu cyberbezpieczeństwa uznaje się przedsięwzięcie wykorzystujące nowe lub istotnie ulepszone rozwiązania technologiczne, organizacyjne lub procesowe, które w sposób mierzalny zwiększają poziom bezpieczeństwa informacji lub odporności cybernetycznej przedsiębiorstwa, a jednocześnie wykraczają poza standardowe i powszechnie stosowane środki ochrony.

Innowacyjność może wynikać w szczególności z wykorzystania sztucznej inteligencji, automatyzacji działań związanych z bezpieczeństwem, zaawansowanej analityki danych, nowych metod wykrywania zagrożeń, integracji różnych źródeł danych lub nowatorskiego zastosowania istniejących technologii.

Na czym może polegać innowacyjność?

Innowacyjność może dotyczyć w szczególności:

- zastosowania sztucznej inteligencji do wykrywania anomalii lub przewidywania zagrożeń;
- połączenia danych z różnych systemów w celu bieżącej oceny poziomu ryzyka;
- wykorzystania urządzeń IoT do monitorowania krytycznych parametrów, takich jak temperatura, wilgotność, poziom wody, ciśnienie lub stan urządzeń;

- automatycznego uruchamiania działań ostrzegawczych lub ograniczających skutki zdarzenia;
- stworzenia cyfrowego modelu lub symulacji scenariuszy ryzyka;
- zastosowania nowej metody testowania ciągłości działania lub odtwarzania procesów;
- integracji istniejących technologii, danych i procesów w sposób, który daje nowy efekt prewencyjny;
- opracowania rozwiązania, które może zostać wykorzystane także u innych klientów lub w innych branżach.

Czego nie uznajemy za innowacyjne rozwiązanie?

Za innowacyjne rozwiązanie nie uznaje się samodzielnego zakupu lub wymiany standardowych urządzeń, instalacji albo infrastruktury, jeżeli projekt nie zawiera dodatkowego elementu, który zwiększa zdolność do przewidywania lub wykrywania zagrożeń, automatyzuje reakcję, umożliwia analizę danych, poprawia pomiar skuteczności zabezpieczeń lub prowadzi do istotnej zmiany sposobu zarządzania ryzykiem.

Samo użycie określeń „AI”, „IoT”, „analitika predykcyjna” lub „automatyzacja” nie jest wystarczające do uznania projektu za innowacyjny. Uczestnik powinien opisać:

- jaki problem rozwiązuje projekt;
- jak działa proponowane rozwiązanie;
- czym różni się ono od obecnego sposobu działania;
- jaki rezultat ma zostać osiągnięty;
- w jaki sposób rezultat będzie mierzony.

Przykłady projektów, które mogą zostać uznane za innowacyjne:

- system analizujący dane z czujników i ostrzegający o ryzyku przegrzania urządzeń przed wystąpieniem pożaru;
- połączenie czujników poziomu wody, prognoz pogody i procedur operacyjnych w celu automatycznego uruchomienia działań przeciwpowodziowych;
- model predykcyjny wykrywający ryzyko awarii kluczowych maszyn na podstawie parametrów ich pracy;
- system, który automatycznie przełącza proces na zapasową lokalizację po wykryciu zakłócenia;
- cyfrowa symulacja wpływu pożaru, powodzi lub awarii dostaw na ciągłość działania przedsiębiorstwa;
- inteligentny monitoring instalacji przeciwpożarowej, który wykrywa spadek jej sprawności i automatycznie przekazuje informację do osób odpowiedzialnych;
- integracja systemu zarządzania budynkiem, monitoringu, danych pogodowych i procedur BCM w jeden system ostrzegania i reakcji;

- wykorzystanie GenAI do analizy incydentów;
- wykorzystanie AI do wykrywania phishingu;
- wykorzystanie AI do wspierania SOC;
- wykorzystanie AI do automatycznej klasyfikacji podatności;
- automatyczne izolowanie urządzeń;
- automatyczna reakcja na incydenty;
- niezmiennalna kopia zapasowa z automatycznym testowaniem odtworzeń;
- cyfrowe bliźniaki środowisk IT wykorzystywane do symulacji ataków;
- automatyzacja Disaster Recovery;
- budowa własnych modeli predykcyjnych dla obszaru cyberbezpieczeństwa;
- analiza zachowań użytkowników pod kątem skłonności do naruszeń bezpieczeństwa;
- zautomatyzowane wykrywanie i analizowanie zagrożeń wewnętrznych, tzw. insider threat;
- integracja danych dotyczących cyberbezpieczeństwa z danymi operacyjnymi przedsiębiorstwa.

Przykłady projektów, które co do zasady nie będą uznawane za innowacyjne:

- sam zakup i montaż standardowej instalacji tryskaczowej;
- wymiana istniejącego systemu sygnalizacji pożaru na urządzenie o podobnych funkcjach;
- zakup gaśnic, hydrantów, drzwi przeciwpożarowych lub agregatu prądotwórczego;
- zwykły remont lub odtworzenie infrastruktury po uszkodzeniu;
- sam zakup licencji na oprogramowanie bez wdrożenia, wykorzystania danych i pomiaru efektów;
- szkolenie pracowników bez powiązania z nowym rozwiązaniem lub testem jego działania;
- ogólna deklaracja wykorzystania AI bez wskazania danych, procesu, rezultatu i sposobu pomiaru.