#CyberMadeInPoland
Academy

www.cybermadeinpoland.pl

Droga do NIS2

Poznaj najważniesze zagadnienia związane z wdrażaniem dyrektywy **NIS2** oraz **polskie** produkty i usługi, które mogą pomóc Twojej organizacji

CZYM JEST DYREKTYWA NIS2?

1

16 stycznia 2023 r. na terenie Unii Europejskiej przyjęta została dyrektywa **NIS2 tj. Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE.** Są to ogólnounijne przepisy, dotyczące cyberbezpieczeństwa. Aby nadążyć za rosnącą cyfryzacją i zmieniającym się krajobrazem zagrożeń dla cyberbezpieczeństwa zmodernizowano w niej istniejące ramy prawne, tak aby odpowiadały na najbardziej aktualne wyzwania.

NIS2 (NETWORK AND INFORMATION)

DATA WEJŚCIA W ŻYCIE: 16 STYCZNIA 2023

DATA IMPLEMENTACJI W PAŃSTWACH CZŁONKOWSKICH: DO 17 PAŹDZIERNIKA 2024

DOKUMENT

OPRACOWANIA

KOGO OBEJMIE?

SEKTORY KLUCZOWE

- INFRASTRUKTURA RYNKÓW FINANSOWYCH
- INFRASTRUKTURA CYFROWA
- PRZESTRZEŃ KOSMICZNA
- BANKOWOŚĆ
- ENERGETYKA
- TRANSPORT
- OPIEKA ZDROWOTNA
- SEKTOR WODY PITNEJ
- ZARZĄDZANIE USŁUGAMI ICT
- ŚCIEKI
- PODMIOTY ADMINISTRACJI PUBLICZNEJ

SEKTORY WAŻNE

- USŁUGI POCZTOWE I KURIERSKIE
- PRZETWARZANIE I DYSTRYBUCJA ŻYWNOŚCI
- GOSPODAROWANIE ODPADAMI
- USŁUGI CYFROWE
- PRODUKCJA
- PRZETWARZANIE I DYSTRYBUCJA CHEMIKALIÓW
- BADANIA NAUKOWE

Dyrektywa NIS2 obejmie zarówno podmioty publiczne, jak i prywatne, które świadczą usługi lub prowadzą działalność w UE i jednocześnie spełniają kryteria klasyfikujące je jako średnie przedsiębiorstwa.

CO WARTO WIEDZIEĆ?

- Dyrektywa NIS2 to kontynuacja wcześniejszych dyrektyw NIS, uwzględniająca bardziej szczegółowe zapisy odnośnie regulacji rynków wpływających na cyberbezpieczeństwo w państwach członkowskich UE.
- Dyrektywa przewiduje **konsekwencje finansowe**, które będą groziły za nieprzestrzeganie wymogów dyrektywy.
- Dyrektywa wprowadza również szereg środków nadzoru oraz egzekwowania przepisów. **Nadaje uprawnienie organom właściwym m.in. do przeprowadzenia kontroli, audytu i skanu bezpieczeństwa (skany podatności sieci i systemów)**, ale też wystąpienia z wnioskiem o przedstawienia dowodów realizacji wymogów cyberbezpieczeństwa przez dany podmiot.
- W celu zapewnienia realnej odpowiedzialności za środki cyberbezpieczeństwa na poziomie organizacyjnym, **NIS2 wprowadza przepisy dotyczące odpowiedzialności osób fizycznych zajmujących stanowiska kierownicze wyższego szczebla** w podmiotach objętych zakresem nowej Dyrektywy NIS.

CEL

osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego.

NAJWAŻNIEJSZE POSTANOWIENIA:

Od podmiotów objętych dyrektywą oczekuje się wdrożenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu:

- zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do prowadzenia działalności,
- świadczenia usług,
- zapobiegania wpływowi incydentów na odbiorców usług lub na inne usługi bądź minimalizowania takiego wpływu.

Wdrożenie środków, o których mowa powyżej powinno być adekwatne w stosunku do:

- **najnowszego stanu wiedzy,**
- **odpowiednich norm europejskich i międzynarodowych,**
- **kosztów wdrożenia,**
- **istniejącego ryzyka.**

Ocena proporcjonalności tych środków uwzględnia stopień narażenia podmiotu na ryzyko, wielkości podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

Zgodnie z tym zapisem wszystkie podmioty będą musiały wdrożyć odpowiednie środki związane z:

- **polityką analizy ryzyka i bezpieczeństwa systemów informatycznych;**
- **obsługą incydentu;**
- **ciągłością działania, np. zarządzania kopiami zapasowymi i przywracaniem normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;**
- **bezpieczeństwem łańcucha dostaw, w tym aspektach związanych z bezpieczeństwem dotyczących stosunków między każdym podmiotem, a jego bezpośrednimi dostawcami lub usługodawcami;**

- bezpieczeństwem w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowaniem w przypadku podatności i ich ujawnienia;
- politykami i procedurami służącymi ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
- podstawowymi praktykami cyberhigieny i szkoleń w zakresie cyberbezpieczeństwa;
- politykami i procedurami służącymi stosowania kryptografii i, w stosownych przypadkach, szyfrowania;
- w niektórych przypadkach będzie to również stosowanie uwierzytelnienia wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.
- bezpieczeństwem zasobów ludzkich, polityką kontroli dostępu i zarządzaniem atywami;

PONADTO:

Incydenty mające istotny wpływ na świadczenie usług przez podmioty kluczowe i ważne, a także tzw. incydenty poważne, zgodnie z dyrektywą NIS2, muszą być zgłaszane bez zbędnej zwłoki właściwemu **CSIRT** lub **innemu właściwemu organowi. W zależności od przypadku jest to 24 h lub 72 h.**

CO WIĘCEJ?

Incydent uznaje się za poważny, gdy:

- **spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu,**
- **wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.**

Wszystkie objęte dyrektywą organizacje powinny ustanowić 24-godzinny mechanizm raportowania incydentu do CSIRT lub organu właściwego incydentu poważnego.

Mikroprzedsiębiorstwa i małe przedsiębiorstwa również zostaną objęte dyrektywą o ile spełnią kryteria wskazujące na ich kluczową rolę dla społeczeństwa, gospodarki lub określonych sektorów, bądź typów usług.

Szkolenia z zakresu cyberbezpieczeństwa będą obowiązkowe dla wszystkich pracowników organizacji w tym dla zarządzających podmiotami kluczowymi i ważnymi.

JAK PRZYGOTWAĆ SIĘ DO WDROŻENIA DYREKTYWY?

1. Sprawdź, czy Twoja organziacja podlega dyrektywie (tj. znajduje się wśród podmiotów Sektorów Kluczowych lub Ważnych).

   PEŁEN WYKAZ PODMIOTÓW WEDŁUG USTAWY WRAZ Z DEFINICJAMI -> LINK

2. Zapoznaj się w najważniejszymi zagadnieniami, dotyczącymi wprowadzenia nowych regulacji oraz rozwiązań w podmiotach uwzględnionych w dyrektywie.

3. Aby jak najlepiej zidentyfikować potrzeby Twojej organizacji w kontekście regulacji dyrektywy NIS2 przeprowadź **AUDYT LUK**.

4. Po dokładniej analizie dowiesz się, jakie luki posiada Twoja organizacja i będziesz w stanie określić, jakich rozwiązań potrzebujesz - przykładowe możesz znaleźć w naszym katalogu.

5. Na bieżąco **monitoruj** stan cyberbezpieczeństwa w Twojej organizacji - identyfikuj słabe punkty infrastruktury pod kątem podatności na cyberataki. **Edukuj i przygotuj szkolenia dla** pracowników, tak aby wszyscy byli świadomi ryzyka związanego z nieprzestrzeganiem podstawowych zasad cyberbezpieczeństwa.

JEŻELI NIE JESTEŚ PEWNY, CZY TWOJĄ ORGANIZACJĘ OBEJMIE DYREKTYWA NIS2 LUB NIE WIESZ NA CZYM PRZY JEJ WDRAŻANIU POWINIENEŚ SIĘ SKUPIĆ - **SKONTAKTUJ SIĘ Z NAMI!**

KONTAKT

OFFICE@CYBERMADEINPOLAND.PL

KATALOG ROZWIĄZAŃ

#CyberMadeInPoland

POZNAJ POLSKIE ROZWIĄZANIA I PRODUKTY, KTÓRE POMOGĄ SPEŁNIĆ WYMAGANIA NIS 2 I ZABEZPIECZYĆ PRZED CYBERZAGROŻENIAMI

Axence

KONTAKT

ROBERT POSŁAJKO
DYREKTOR MARKETINGU I ROZWOJU

ROBERT.POSLAJKO@AXENCE.NET

KLASA PRODUKTU/USŁUGI

- **Zarządzanie zasobami IT**
- **Bezpieczeństwo stacji roboczych**
- **Budowanie świadomości**
- **Zdalne wsparcie IT**

ZAKRES DZIAŁALNOŚCI

Bezpieczna praca i wsparcie użytkowników z Axence nVision® oraz Axence SecureTeam®

Axence od ponad 19 lat dostarcza ponad 3500 organizacjom na całym świecie profesjonalne rozwiązania do kompleksowego zarządzania IT, od niedawna tworzy również platformę security awareness do edukowania użytkowników w zakresie bezpiecznej pracy w cyfrowym świecie.

Axence nVision®:

- pozwala zarządzać wszystkimi procesami w dziale IT, łączy w jednej konsoli monitorowanie IT, zarządzanie zasobami (ITAM), licencjami (SAM), system zgłoszeń i zdalne wsparcie użytkowników (service desk) oraz zarządzanie usługami IT (ITSM) wraz z najważniejszymi elementami zarządzania stacjami roboczymi (end-point management);
- oferuje łatwość użytkowania, utrzymania i instalacji oraz bezpieczeństwo danych.

Znani klienci: e-obuwie.pl, morele.net, Phoenix Contact, ArcelorMittal, Bulgarian Stock Exchange, liczne szpitale, urzędy i instytucje publiczne na całym świecie.

Axence SecureTeam®:

Platforma edukacyjna dostarczającą praktyczną wiedzę i dobre praktyki w zakresie cyberbezpieczeństwa, możliwość testowania wiedzy użytkowników. W materiałach trenerzy omawiają codzienne, praktyczne przypadki ataków i niebezpiecznych zachowań oraz doradzają jak bezpiecznie korzystać z sieci, komputera i smartfona.

Szkolenie na platformie pozwala na utrwalanie wiedzy, eliminuje problem zapominania i nieobecności na szkoleniach stacjonarnych. Wyniki są dostępnie w formie statystyk i raportów. Każdy przeszkolony otrzymuje certyfikat!

Korzystając z produktów **Axence** możemy realizować szereg norm i wytycznych **NIS2** w tym m.in.: art. 54, art. 77, art. 78, art. 79 i art. 89.

BW Advisory

KONTAKT

SEBASTIAN BURGEMEJSTER
PREZES ZARZĄDU
PIOTR WELENC
PARTNER SPÓŁKI

KONTAKT@ITGRC.PL

KLASA PRODUKTU/USŁUGI

- **Wdrażenie frameworków i standardów w obszarze cyberbezpieczeństwa**
- **Edukacja/szkolenie w zakresie bezpieczeństwa**
- **Audyty bezpieczeństwa**
- **Budowanie systemu zarządzania bezpieczeństwem informacji**

ZAKRES DZIAŁALNOŚCI

Bezpieczeństwo i odporność organizacyjna: wdrażanie i doskonalenie systemów zarządzania bezpieczeństwem informacji i ciągłości działania. Budowa systemu zarządzania bezpieczeństwem informacji. Wdrażanie dokumentacji i rozwiązań w obszarze zarządzania ciągłością usług.

Audyt: analiza luki pomiędzy obecnym stanem cybersecurity & continuity a stanem docelowo wynikającym z NIS2, audyt bezpieczeństwa zgodnie z NIS2, audyt łańcucha dostaw, w tym dostawców i usług zgodnie z m.in. ISAE 3402, SSAE18, SOC 1, 2, 3.

Systemy IT GRC: wsparcie przy wyborze i wdrożeniu narzędzi GRC oraz systemowych narzędzi wspierających zgodność z NIS2.

Akademia IT GRC: szkolenia, edukacja z IT GRC & Audit i cyberbezpieczeństwa. Szkolenia z NIS2 i DORA (projektowanie, utrzymanie, przeglądy, ewaluacja).

Problem, który rozwiązujemy: dostarczamy wiedzę, profesjonalne wsparcie, szyte na miarę rozwiązania w zakresie NIS2 i DORA. Przygotowujemy współistnienie NIS2, DORA z istniejącymi w organizacji systemami Governance, Risk, Compliance & Audit. Prowadzimy pogłębione audyty bezpieczeństwa.

akademia // ITGRC

ZOBACZ OFERTĘ SZKOLEŃ

ChangePro

ChangePro
CYBERSECURITY AWARENESS COMPANY

KONTAKT

RADOSŁAW CHINALSKI
SECURITY AWARENESS EXPERT

+48 604 495 821

RADOSLAW.CHINALSKI@CHANGEPRO.PL

KLASA PRODUKTU/USŁUGI

- **Security Awareness Training**
- **czytniki eDowodów**
- **Mobile Device Management**
- **badanie bezpieczeństwa systemów IT**

ZAKRES DZIAŁALNOŚCI

Security Awareness Training polega na ciągłym, ukierunkowanym i opartym na zachowaniu szkoleniu w rozpoznawaniu zagrożeń płynących z cyberprzestrzeni. Treningiem objęte są zagrożenia, takie jak: phishing, spear phishing, ransomware czy ataki przeprowadzane z wykorzystaniem socjotechniki. Oferowane narzędzia umożliwiają prowadzenie dedykowanych kampanii e-mail symulujących ataki typu phishing oraz naukę z wykorzystaniem biblioteki treści szkoleniowych. Narzędzia umożliwiają zautomatyzowanie kampanii i połączenie z przekazywaniem treści szkoleniowych, generowanie raportów analitycznych oraz adaptacyjne planowanie kolejnych etapów szkoleń.

eDowód to dowód osobisty z warstwą elektroniczną w formie konwencjonalnej karty wyposażony w bezstykowy mikroprocesor, który praktycznie uniemożliwia kradzież tożsamości oraz wytwarzanie fałszywych dokumentów. Czytnik eDowodów musi być zgodny ze specyfikacją wymagań technicznych dla czytnika kart z pinpadem opublikowanym przez MSWiA. Aktualnie w ofercie znajdują się 2 modele czytników z obsługą w języku polskim, przygotowane do działania na rynku polskim.

Systemy Mobile Device Management (MDM), umożliwiają zabezpieczanie urządzeń, danych i aplikacji mobilnych (smartfony, tablety). Pozwalają zarządzanie konfiguracjami bezpieczeństwa na wszystkich urządzeniach, monitorowanie i wymuszanie zgodności z politykami IT, tworzenie reguł postępowania w przypadku naruszenia polityki (np. instalacji aplikacji z czarnej listy, roota urządzenia, usunięcia karty SIM).

Badanie bezpieczeństwa systemów IT jest realizowane poprzez przeprowadzenie testów penetracyjnych, które pozwalają na weryfikację zabezpieczeń systemu oraz identyfikację jego słabych punktów. Zakres testów penetracyjnych obejmuje weryfikację architektury, uwierzytelniania, zarządzania sesją, kontroli dostępu, obsługi złośliwych danych wejściowych, nieaktywnych mechanizmów kryptograficznych, mechanizmów ochrony danych, zabezpieczenia komunikacji, konfigurowania bezpieczeństwa http, zabezpieczeń przed złośliwym kodem, web serwisów oraz procesu konfiguracji. Realizujemy testy penetracyjne typu black-box, gray-box oraz white-box.

CyCommSec

KONTAKT

PRZEMYSŁAW KUCHARZEWSKI
SALES CHANNEL DIRECTOR

PRZEMYSLAW.KUCHARZEWSKI@CYCOMMSEC.COM

KLASA PRODUKTU/USŁUGI

- **Ofensywne cyberbezpieczeństwo jako usługa**
- **Audyt bezpieczeństwa**
- **Testy penetracyjne**
- **Skany podatności**

ZAKRES DZIAŁALNOŚCI

CyCommSec to firma specjalizująca się w inżynierii rozwiązań, której kluczowym aspektem działalności, jest nie tylko sukces w realizacji projektów i ich pełna integracja z oczekiwaniami klienta, ale również zdolność do przewidywania potencjalnych problemów, które mogą pojawić się w przyszłości, i adresowanie ich z wyprzedzeniem.

FuseAI, kluczowe rozwiązanie firmy **CyCommSec**, to zaawansowana platforma wykorzystująca sztuczną inteligencję do usprawnienia bezpieczeństwa informatycznego firm. Technologia ta wyróżnia się poprzez połączenie automatycznych i manualnych testów penetracyjnych, umożliwiając ciągłe monitorowanie i zarządzanie podatnościami w aplikacjach, chmurze i na stronach internetowych. **FuseAI** oferuje kompleksowe rozwiązania z zakresu bezpieczeństwa ofensywnego, w tym Pentest-as-a-Service, audyty podatności oraz narzędzia do ciągłego testowania, zapewniając firmom spójny obraz bezpieczeństwa. Platforma ta wspiera również zgodność z kluczowymi ustawami, takimi jak **PCI**, **ISO**, **SOC2**, **GDPR**, **HIPAA**, **DORA** czy **NIS2** pomagając budować zaufanie klientów poprzez solidną ochronę przed atakami.

ComCERT

KONTAKT

+48 22 112 06 83

KONTAKT@COMCERT.PL

KLASA PRODUKTU/USŁUGI

- **Systemy cyberbezpieczeństwa**
- **Zarządzanie incydentami**
- **Polityki i procesy cyberbezpieczeństwa**
- **Outsourcing SOC**

ZAKRES DZIAŁALNOŚCI

ComCERT od 2011 roku świadczy usługi cyberbezpieczeństwa dla swoich Klientów. Obszar specjalizacji naszych pracowników obejmuje szerokie spektrum wiedzy i praktycznych kompetencji. Wspieramy naszych Klientów zarówno w wymiarze zapobiegania, rozpoznawania, jak i przeciwdziałania zagrożeniom w cyberprzestrzeni. Poza działalnością usługową, skupioną wokół cyberbezpieczeństwa, prowadzimy również działalność edukacyjną i szkoleniową, wraz z praktycznymi warsztatami i symulacjami.

- Audyty bezpieczeństwa
- Cyber Threat Intelligence (C3TI)
- Outsourcing SOC (1L, 2L, 3L)
- Budowa zespołów SOC, CSIRT
- Scentralizowany SOC dla JST
- Usługi szkoleniowe
- Analizy powłamaniowe
- Zgodność z regulacjami (min. NIS2)
- ISO 27001 | ISO 22301
- CISOaaS (CISO as a service)

Usługi wdrożeniowe systemów cyberbezpieczeństwa:

- Integracja systemów
- Utrzymanie i serwis
- Modernizacja i rozwój
- Doradztwo technologiczne
- Wsparcie w administracji
- Zarządzanie uprawnieniami

Zakres usług wdrożeniowych obejmuje kluczowe usługi związane z systemami klasy: **Firewall, VPN, WAF, DAM, EDR, DLP, SIEM i SOAR**.

WIĘCEJ NA STRONIE:

DC9 Group

KONTAKT

MACIEJ BRONIARZ
PREZES, SPECJALISTA CYBERSEC

MACIEJ.BRONIARZ@DECODE9.PL

KLASA USŁUGI

- **Reagowanie kryzysowe na cyberataki**
- **Cyber kryminalistyka**
- **Cyber prewencje w tym testy i audytyt**
- **Hardening po incydentach**

ZAKRES DZIAŁALNOŚCI

Ryzyko najlepiej zmniejsza się regularną prewencją i posiadaniem procesu na wypadek kryzysu. **DC9 Group** to sprawdzone zespoły specjalizujące się w:

- **Emergency response** — Wyciek lub zaszyfrowanie danych firmowych może przydarzyć się każdemu DC9 pomaga opanować sytuację. Od analizy sytuacji, zabezpieczenia dowodów po plan działania dla lokalnego działu IT lub czasowego przejęcie jego obowiązków. Wraz z partnerami możemy zapewnić także wsparcie prawne i PR-owe.

- **Cyber forensics** — Były pracownik skasował dane? Konkurencja przejmuje kontrakty i klientów? Ktoś uruchomił nieznane skrypty na firmowych serwerach? Cyber kryminalistyka może dotyczyć dowolnej organizacji. DC9 przeprowadza dochodzenie, zabezpiecza dowody i przygotowuje dokumentację do sądu.

- **Penetration testing** — Dbanie o bezpieczeństwo systemów informatycznych należy wspierać regularnym badaniem podatności. Testowanie przed startem jest już standardem. Warto pamiętać, że wraz z każdą aktualizacją firmowego serwera, oprogramowania lub samego kodu mogą pojawić się nowe podatności, które DC9 pomoże znaleźć.

- **Organization monitoring** — Śledzenie aktualizacji oprogramowania i sprzętu czy śledzenie wycieków danych powiązanych z organizacją i pracownikami. To działania, które zaniedbane potrafią być przyczyną ataku na organizację. Niezałatana aktualizacja, firmowe dane dostępowe w wycieku z komputera domowego pracownika. DC9 zadba o Twój monitoring.

DC9 Group rozwiązuje cyber problemy i zmniejsza ryzyko ich wystąpienia. Prewencja i posiadanie planu awaryjnego to ważne punkty przy wdrażaniu dyrektywy NIS2.

DEKRA Certification sp. z o.o.

KONTAKT

TOMASZ SZCZYGIEŁ
EKSPERT DS. OCHRONY DANYCH I AUDYTOR

TOMASZ.SZCZYGIEL@DEKRA.COM

KLASA PRODUKTU/USŁUGI

- **Audyty eksperckie**
- **Certyfikacja systemów**
- **Badania i certyfikacja wyrobów**
- **Certyfikacja osób**

ZAKRES DZIAŁALNOŚCI

DEKRA Certification sp. z o.o. to część międzynarodowego koncernu DEKRA SE z siedzibą w Stuttgarcie, globalnego lidera na rynku **certyfikacji systemów zarządzania** i pioniera w dziedzinie w **dziedzinie bezpieczeństwa informacji**, zrównoważonego biznesu, specjalistycznych audytów, certyfikacji oraz rozwoju kompetencji.

Działająca od niemal 100 lat na świecie - oraz od ponad 20 lat w Polsce - DEKRA wychodzi naprzeciw wyzwaniom współczesnego świata i stawia na dynamiczny rozwój usług z zakresu **cyberbezpieczeństwa, bezpieczeństwa informacji** i **zarządzania ciągłością działania**, oraz na usługi wspierające zrównoważony rozwój organizacji i **elektromobilność**.

Z jasną i ambitną wizją bycia **partnerem dla bezpiecznego** i **zrównoważonego świata** DEKRA oferuje swoim klientom rzetelną wiedzę i praktyczne narzędzia, takie jak m.in. **certyfikacja ISO 27001 i ISO 22301**, innowacyjne **badania i usługi certyfikacji wyrobów** (w tym badania zgodności z nową dyrektywą RED-DA 2022/30 w aspektach cyberbezpieczeństwa - **dyrektywa NIS2**), czy **specjalistyczne audyty** (np. audyt bezpieczeństwa systemu informacyjnego dla operatorów usług kluczowych).

Dzięki połączeniu wiedzy i doświadczenia polskich i światowych ekspertów, klienci DEKRA mają dostęp do najnowszych technologii i rozwiązań dopasowanych do ich indywidualnych potrzeb.

Dynacon Sp. z o.o.

KONTAKT

ZUZANNA GRAJEK
BIURO ZARZĄDU

+48 71 307 51 73

BIURO@DYNACON.PL

KLASA PRODUKTU/USŁUGI

- **Oprogramowanie dla cyberbezpieczeństwa**
- **SOC OT**
- **Urządzenia sieciowe i platformy USS**
- **Szkolenia, audyty, oceny bezpieczeństwa**

ZAKRES DZIAŁALNOŚCI

DYNACON Sp. z o.o. to polski producent rozwiązań komunikacji sieciowej, a także cyberbezpieczeństwa w środowisku przemysłowym. **Specjalizujemy się w optymalizacji jakości połączeń w technologii operacyjnej (OT) oraz IT.**

Reprezentujemy polską myśl technologiczną na rynku polskim i europejskim, rozwijając komunikację i bezpieczeństwo najważniejszych obszarów Infrastruktury Krytycznej Kraju i usług kluczowych. Projektujemy i wdrażamy systemy: **cyberbezpieczeństwa, sieci komunikacyjnych, OT/IT** oraz **automatyki przemysłowej** dla kluczowych sektorów przemysłu takich jak: energetyka, gospodarka wodna, branża chemiczna, farmaceutyczna, sektor paliwowy i automotive.

DYNACON jako pierwsza firma z obszaru komunikacji i bezpieczeństwa przemysłowych systemów sterowania OT, dołączyła do Rządowego Programu Współpracy w Cyberbezpieczeństwie w celu intensyfikacji działań nad schematami certyfikacji, dla zapewnienia adekwatnego poziomu cyberbezpieczeństwa procesów technologicznych.

W programie Droga do NIS2 fachowo wyjaśniamy czym są incydenty w przemyśle. Jak zgodnie z nowelizowanym prawem należy je obsługiwać oraz jak przetwarzać i pracować z danymi o incydentach, dla zapewnienia optymalnych działań, zwiększających bezpieczeństwo przedsiębiorstwa we wszystkich obszarach. Zapewniamy specjalistyczne oprogramowanie i urządzenia sieciowe optymalizujące zarządzanie zagrożeniami. Oferujemy SOC dla OT.

ZOBACZ TEŻ:

EKOSYSTEM CYBERMADEINPOLAND
IGEOS - CZŁONKOWIE IZBY
PROFIBUS - FIRMY CZŁONKOWSKIE

Energy Logserver

KONTAKT

ŁUKASZ NIEBOREK
BUSINESS DEVELOPMENT MANAGER

+48 601 199 639

SALES@ENERGYLOGSERVER.COM

KLASA PRODUKTU/USŁUGI

- SIEM
- SOAR
- XDR

ZAKRES DZIAŁALNOŚCI

Dzięki **Energy Logserver** zyskujesz szybki dostęp do logów, ich analizę i raportowanie - bez względu na skalę. Nasze narzędzie zapewnia kompleksowe zarządzanie logami ze wszystkich elementów infrastruktury teleinformatycznej. Wyposażone w funkcje automatycznego alarmowania o naruszeniach bezpieczeństwa, pozwala działom operacyjnym i centrom bezpieczeństwa SOC zwiększyć efektywność i skuteczność pracy, eliminując czasochłonne i skomplikowane ręczne korelacje, w zamian oferując w pełni zautomatyzowany proces. Dostęp do różnorodnych modułów analizy zdarzeń, wizualizacji danych i interaktywnych dashboardów umożliwia dostosowanie prezentowanych informacji do indywidualnych potrzeb użytkowników.

ZOBACZ TEŻ:

SIEM FOR BEGINNERS

SOAR FOR BEGINNERS

Fudo Security

KONTAKT

KAMIL CHRAPEK
SALES SPECIALIST

K.CHRAPEK@FUDOSECURITY.COM

KLASA PRODUKTU/USŁUGI

- **Zarządzanie dostępem uprzywilejowanym (PAM)**
- **Inteligentny System PAM wspierany AI**
- **Bezpieczeństwo infrastruktury IT**
- **Zgodność z NIS2 i RODO**

ZAKRES DZIAŁALNOŚCI

Fudo Enterprise to innowacyjne, wspierane przez AI rozwiązanie PAM, które nie wymaga instalacji dodatkowych narzędzi. Dzięki temu zaimplementujesz je nawet w 24 godziny, zyskując natychmiastowy efekt. Fudo zapewnia przyjazne środowisko pracy dla użytkownika i nie wymaga zmiany codziennych nawyków Twojego zespołu. System PAM od Fudo gwarantuje bezpieczne zarządzanie zdalnym dostępem, zapewniając zgodność z NIS 2.

Dlaczego warto wybrać Fudo Enterprise?

- Efektywność operacyjna: Zapewnia łatwe zarządzanie dostępem uprzywilejowanym, wykluczając potrzebę złożonych procesów instalacyjnych.
- Monitoring sesji: Każda sesja jest rejestrowana i analizowana, co pozwala na natychmiastowe wykrywanie i reagowanie na anomalie.
- Analiza produktywności: Umożliwia ocenę wydajności pracy i zapewnia wysoki ROI.
- AI i biometria: Innowacyjne technologie dla szybkiej reakcji na zagrożenia i zwiększonej ochrony.

Korzyści dla Twojej firmy w świetle NIS2:

- Wsparcie dla zgodności z NIS2: Fudo Enterprise dostarcza narzędzia niezbędne do zarządzania ryzykiem i ochrony infrastruktury IT.
- Szybkość działania: Nasze rozwiązania gwarantują błyskawiczne wykrywanie i reagowanie na incydenty, co jest kluczowe dla zgodności z wymogami raportowania w ramach NIS2.
- Bezpieczeństwo infrastruktury: Zaawansowane mechanizmy uwierzytelniania chronią dostęp do kluczowych systemów, wspierając cele NIS2.

Wybierając Fudo Enterprise, zyskujesz nie tylko technologię, ale strategicznego partnera, gotowego pomóc wzmocnić Twoje cyberbezpieczeństwo w myśl NIS2.

ZOBACZ TEŻ:

EBOOK NIS2/RODO
CISO 2024 - CHECKLIST

ICsec

KONTAKT

KATARZYNA BERBEĆ
DYREKTOR DS. STRATEGII I ROZWOJU

KATARZYNA.BERBEC@ICSEC.PL

KLASA PRODUKTU/USŁUGI

- **System monitorowania sieci przemysłowych i detekcji podatności, cyberzagrożeń oraz incydentów**
- **Nowej generacji IDS (Intrusion detection system) dla sieci OT**

ZAKRES DZIAŁALNOŚCI

Opracowane przez **ICsec** rozwiązanie SCADvance XP® to innowacyjny system monitorowania sieci przemysłowych. W kontekście Dyrektywy NIS2 rozwiązanie SCADvance XP® wspiera zespoły odpowiedzialne za bezpieczeństwo sieci przemysłowych w obszarach takich jak:

- **Audyt i inwentaryzacja sieci OT** - SCADvance XP® dostarcza wiedzę na temat bieżącej architektury sieci: identyfikuje urządzenia, tworzy mapy urządzeń oraz połączeń między nimi.
- **Monitoring sieci pod kątem zagrożeń i anomalii** - System umożliwia ciągły, pasywny monitoring sieci pod kątem podatności, cyberzagrożeń oraz incydentów.
- **Klasyfikacja zdarzeń oraz incydentów** - Scadvance XP® gromadzi informacje o zagrożeniach i podatnościach oraz umożliwia kwalifikację zdarzenia w incydent zapisując jednocześnie historię procesu, podjęte działania, osoby odpowiedzialne oraz kopię ruchu, która dokumentuje przebieg incydentu.
- **Raportowanie incydentów** - funkcje raportowania systemu pomagają w zautomatyzowaniu zgłaszania incydentów w ramach własnego systemu bezpieczeństwa (np. Security Operation Center) lub w ramach wypełniania obowiązków wynikających z aktów prawnych np. Ustawy o KSC.
- **Wsparcie SOC i integracja z systemami typu SIEM -** Scadvance XP® integruje się z systemami typu SIEM funkcjonujących w ramach SOC lub zespołów reagowania dostarczając wartościowych danych do dalszej analizy.

LOG Plus

KONTAKT

ANNA CHODUN
DYREKTOR SPRZEDAŻY

DWS@LOG-SYSTEMS.COM

KLASA PRODUKTU/USŁUGI

- **Zarządzanie aktywami**
- **Zarządzanie i obsługa incydentów**
- **Kontrola dostępu do danych**
- **Zarządzanie usługami**

ZAKRES DZIAŁALNOŚCI

Spółka LOG Plus jest wiodącym na polskim rynku producentem oprogramowania, specjalizującym się w nowoczesnych rozwiązaniach, wspomagających zarządzanie zasobami informatycznymi (IT Asset Management), procesy biznesowe zgodnie ze standardami ITIL oraz bezpieczeństwo organizacji.

Flagowy produkt LOG Plus to fundament każdej organizacji, chcącej kompleksowo zarządzać aktywami i usługami IT. Oprogramowanie gromadzi w jednym miejscu wszystkie niezbędne dane oraz narzędzia umożliwiające kontrolę nad infrastrukturą informatyczną, zapewniając ciągłość działania usług. System jest nie tylko wsparciem w zarządzaniu i organizacji pracy dla zespołu IT, ale również dla całego biznesu.

Najważniejsze obszary LOG Plus z zakresu cyberbezpieczeństwa:

- Zarządzanie i obsługa incydentów;
- Bezpieczeństwo informacji, kontrola uprawnień i dostępu do danych i SI;
- Zarządzanie usługami, kontrola dostępności i przewidywanie ryzyk;
- Zarządzanie aktywami organizacji, ewidencja i monitoring całego majątku informatycznego firmy oraz kontrola zainstalowanego oprogramowania;
- Monitoring pracowników, blokowanie dostępu do niebezpiecznych stron www i oprogramowania, blokowanie nośników danych oraz kontrola stanu komputerów i serwerów.

YOUTUBE PLATFORMA

Misja: Cyberbezpieczeństwo

KONTAKT

ALEKSANDER LUDYNIA, PARTNER
TOMASZ WILCZYŃSKI, PARTNER

KONTAKT@MISJACYBER.PL

KLASA PRODUKTU/USŁUGI

- **Program budowania świadomości**
- **Szkolenia z cyberbezpieczeństwa**
- **Symulowane ataki phishingowe**
- **Doradztwo z cyberbezpieczeństwa**

ZAKRES DZIAŁALNOŚCI

Misja: Cyberbezpieczeństwo to pierwszy tak rozbudowany program budowania świadomości wykorzystujący szkolenia w postaci scenariuszowych gier komputerowych, które w zabawnej, lekkiej i wciągającej formule skutecznie uczą cyberbezpieczeństwa. To innowacyjny sposób pozwalający trwale zmienić zachowania pracowników i podnieść poziom odporności organizacji na zagrożenia cyfrowego świata!

Zakres tematyczny programu szkoleniowego obejmuje między innymi: bezpieczeństwo informacji, ochronę stacji roboczej, bezpieczeństwo haseł i uwierzytelniania, obronę przed atakami typu phishing, złośliwe oprogramowania, ataki z wykorzystaniem technik inżynierii społecznej, bezpieczeństwo urządzeń mobilnych, zasady bezpieczeństwa podczas pracy zdalnej oraz rozpoznawanie i reagowanie na incydenty bezpieczeństwa.

Dzięki naszemu programowi budowania świadomości:

- **Zwiększasz odporność** organizacji na cyberataki poprzez skuteczne budowanie wiedzy pracowników o współczesnych zagrożeniach i poprzez praktyczne ćwiczenia obrony przed nimi.
- **Odciążasz kadry** organizacji poprzez przekazanie nam większości obowiązków związanych z edukacją pracowników w obszarze bezpieczeństwa.
- **Angażujesz pracowników** dzięki grywalizacji oraz pozytywnej promocji dbania o kulturę cyberbezpieczeństwa w organizacji.
- **Efektywnie wykorzystujesz czas** ponieważ gracze sami wybierają czas na grę, która dostępna jest przez platformę on-line.
- **Uzyskujesz zgodność z regulacjami**, wytycznymi oraz standardami bezpieczeństwa.
- **Oszczędzasz środki** poprzez wykorzystanie najbardziej efektywnego kosztowo sposobu edukacji.

Zainwestuj w świadomość pracowników swojej organizacji.

Bo wiedza chroni najlepiej.

Nacview

KONTAKT

ANNA KOLENDA-PARAKIEL
PRODUCT MANAGER

ANNA.KOLENDA@NACVIEW.COM

KLASA PRODUKTU/USŁUGI

- **NAC (802.1X)**
- **Zarządzanie dostępem**
- **Segmentacja sieci**
- **Monitorowanie i raportowanie**

ZAKRES DZIAŁALNOŚCI

NACVIEW jest systemem NAC (Network Access Control) opartym o protokół 802.1x. Rozwiązania tej klasy mogą być elementem strategii cyberbezpieczeństwa organizacji, mającymi na celu egzekwowanie zasad bezpieczeństwa i kontrolę dostępu do zasobów sieciowych zgodnie z wymogami dyrektywy NIS 2, w tym między innymi:

Zarządzanie dostępem: Organizacje muszą zapewnić skuteczne zarządzanie dostępem do sieci i zasobów informatycznych. System NAC oparty na standardzie 802.1x umożliwia kontrolę dostępu do sieci na poziomie użytkownika i urządzenia, zgodnie z zasadą Zero Trust.

Identyfikacja i autentykacja: System NAC umożliwia autentykację użytkowników i urządzeń, zanim uzyskają dostęp do zasobów sieciowych organizacji, co pozwala uzyskać pewność co do tożsamości korzystających z sieci.

Monitorowanie i raportowanie: Organizacje muszą monitorować aktywność sieciową oraz zgłaszać incydenty bezpieczeństwa. System NAC pozwala na prowadzenie audytów dostępu do sieci oraz generowanie raportów dotyczących aktywności użytkowników i urządzeń.

Zgodność z regulacjami: Implementacja systemu NAC opartego na standardzie 802.1x pozwala organizacjom spełnić wymagania związane z ochroną danych poprzez skuteczne zarządzanie dostępem do sieci oraz kontrolę użytkowników i urządzeń.

Reagowanie na incydenty bezpieczeństwa: W przypadku wykrycia incydentu bezpieczeństwa, organizacje muszą być w stanie szybko reagować i podejmować odpowiednie działania naprawcze. System NAC umożliwia szybką identyfikację i izolację potencjalnych zagrożeń, co pozwala na skuteczne reagowanie na incydenty bezpieczeństwa.

Omnilogy

KONTAKT

MAREK WALCZAK
SALES DIRECTOR

KONTAKT@OMNILOGY.PL

KLASA PRODUKTU/USŁUGI

- **Observability**
- **Cybersecurity**
- **Monitoring**

ZAKRES DZIAŁALNOŚCI

Omnilogy zapewnia bezpieczeństwo, wydajność oraz niezawodność systemów IT.

Pomagamy klientom w budowaniu, testowaniu i ciągłym doskonaleniu integralności technologicznej i operacyjnej ich organizacji.

Działamy w obszarze **cybersecurity, monitoringu, obserwowalności, testowania, automatyzacji procesów IT oraz audytów** - tworząc i wdrażając strategie, dostarczając i implementując najlepsze na rynku rozwiązania w obszarze DevSecOps oraz SRE (Site Reliability Engineering).

Specjalizujemy się w budowaniu obserwowalności dla hybrydowych środowisk łącząc świat legacy ze światem chmury prywatnej i publicznej. Wykrywamy anomalie w oparciu o logi, trace-y, metryki oraz zdarzenia Kubernetes. Analizujemy je za pomocą sztucznej inteligencji, aby w sposób automatyczny podnosić efektywność i dostępność aplikacji i infrastruktury.

Wspieramy podmioty podlegające regulacjom **NIS2** i **DORA** poprzez dostarczanie oprogramowania i usług bezpieczeństwa oraz promowanie kultury bezpieczeństwa.

Rublon

KONTAKT

AGNIESZKA KRAL
PRZEDSTAWICIEL DS. SPRZEDAŻY

SPRZEDAZ@RUBLON.PL

KLASA PRODUKTU/USŁUGI

- **Uwierzytelnianie wieloskładnikowe MFA**

ZAKRES DZIAŁALNOŚCI

Rublon to rozwiązanie z zakresu cyberbezpieczeństwa, które zapewnia pracownikom bezpieczny dostęp do zasobów IT ich organizacji za pomocą **nowoczesnego uwierzytelniania wieloskładnikowego.**
Po wprowadzeniu poprawnego hasła, użytkownik jest proszony o uwierzytelnienie za pomocą drugiego składnika, na przykład powiadomienia push, kodu TOTP, lub odpornego na phishing klucza FIDO.

Używając konektorów oraz API, Rublon umożliwia **integrację z technologiami biznesowymi** takimi jak:

- Windows, Active Directory, Remote Desktop, AD FS
- rozwiązania VPN oraz SSH
- protokoły LDAP, RADIUS i SAML
- aplikacje cloud i web

Zabezpieczając dostęp pracowników, Rublon pomaga Twojej firmie spełniać wymogi regulacji o ochronie danych, wymogi ubezpieczeń cybernetycznych i standardy bezpieczeństwa informacji, takie jak dyrektywa NIS2. Rublon chroni dostęp do sieci, serwerów, punktów końcowych i aplikacji przed zagrożeniami cybernetycznymi, takimi jak ransomware i ataki na uwierzytelnianie.

Dlaczego Rublon?

- Centralnie zarządzane MFA dla całej infrastruktury IT
- Szeroki wybór metod uwierzytelniania
- Dane osobowe przetwarzane na terenie UE
- Polskojęzyczne wsparcie techniczne

Rozpocznij trial Rublon MFA
www.rublon.pl/trial

Secfense

KONTAKT

ANTONI SIKORA

HEAD OF GROWTH

ANTONI@SECFENSE.COM

KLASA PRODUKTU/USŁUGI

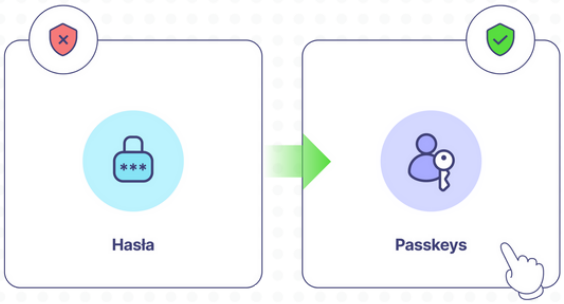
- Odporne na phishing MFA
- Ochrona przed podatnościami zero-day
- Odzyskanie kontroli nad IAM
- FIDO i passkeys dla organizacji
- Bezpieczeństwo dostępu zdalnego
- Zgodność z regulacjami (DORA, NIS2, itp.)

ZAKRES DZIAŁALNOŚCI

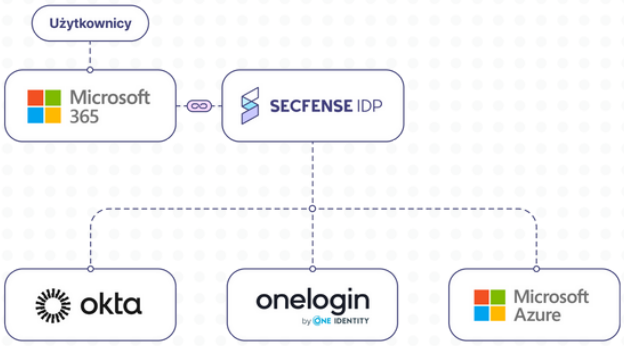
Poznaj kompleksowe rozwiązanie z obszaru IAM i silnego uwierzytelniania, odzyskaj pełną kontrolę nad tożsamościami w organizacji i uwolnij się od phishingu raz na zawsze.

Wybrane Korzyści:

Phishing-proof MFA w całej firmie.

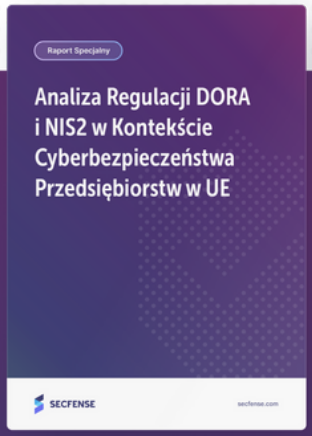


Zastąpienie haseł dzięki **FIDO passkeys.**



Zarządzaj tożsamościami **z jednego miejsca.**

Zabezpiecz wszystkie **aplikacje webowe.**



Kliknij i Pobierz Raport albo zeskanuj QR kod:

Wprowadzenie do FIDO i Passwordless:

Rozmowa z przedstawicielami FIDO Alliance rozwijającymi bezhasłowy standard uwierzytelniania w sieci.

WEBINARY SECFENSE

Kliknij i zapisz się na webinar albo zeskanuj QR kod:

Securivy

KONTAKT

Paweł Chudziński
CEO, Securivy

pawel.chudzinski@securivy.com

KLASA PRODUKTU/USŁUGI

- **Monitoring aktywności użytkowników**
- **Zarządzanie dostępem (PAM)**
- **Nagrywanie sesji zdalnych i lokalnych**
- **Wykrywanie zagrożeń wewnętrznych**

ZAKRES DZIAŁALNOŚCI

Jako **Securivy** jesteśmy dystrybutorem rozwiązań bezpieczeństwa IT, które cechują się łatwością we wdrożeniu i użytkowniku oraz intuicyjnym i przejrzystym modelem licencjonowania. W naszym portfolio znajduje się szereg produktów, które pomogą zadbać nie tylko o wysoki poziom cyberbezpieczeństwa, ale także uzyskać zgodność z dyrektywą NIS2. Jednym z narzędzi, jakie oferujemy, jest Ekran System – platforma zaprojektowana tak, by powstrzymywać, wykrywać i zapobiegać zagrożeniom wewnętrznym. **To właśnie dzięki Ekran System, wdrożysz większość wymagań NIS2 za pomocą jednego narzędzia.**

NIS2 Wymagane środki bezpieczeństwa	Ekran Odpowiadająca funkcjonalność
Analiza ryzyka i bezpieczeństwo systemów informacyjnych	• Zarządzaj zagrożeniami wewnętrznymi. • Monitoruj aktywność użytkowników i przeglądaj nagrania po wybranych filtrach. • Zarządzaj aktywnością użytkowników uprzywilejowanych.
Obsługa incydentów i raportowanie	• Dostarczaj władzom kompleksowy dziennik audytu. • Eksportuj dowody cyberbezpieczeństwa do celów sądowych.
Ciągłość działania	• Wykorzystaj alerty w czasie rzeczywistym i blokuj ryzykowne działania. • Wykorzystaj tryb Wysokiej Dostępności i Disaster Recovery Ekran System.
Ocena skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie	• Wykorzystaj dziennik audytu generowany przez Ekran System do oceny, jak działają środki cyberbezpieczeństwa w Twojej organizacji. • Monitoruj, jak Twoi pracownicy przestrzegają zasady bezpieczeństwa IT.
Bezpieczeństwo łańcucha dostaw	• Monitoruj aktywność dostawców zewnętrznych, partnerów i innych podmiotów łańcucha dostaw, którzy mają dostęp do Twojej infrastruktury. • Zabezpiecz połączenia RDP do swojego środowiska i kontroluj dostęp do danych.
Stosowanie uwierzytelniania wieloskładnikowego lub ciągłego	• Wykorzystaj możliwości zarządzania hasłami i tożsamością do ustanowienia bezpiecznego procesu żądania i zatwierdzania dostępu. • Zintegruj Ekran System z Active Directory i systemami Help-Desk.

Zapoznaj się z naszym **Kompletnym przewodnikiem po zgodności z NIS2**, aby dowiedzieć się więcej.

Skontaktuj się z nami i sprawdź Ekran System w praktyce. **Pobierz darmową 30-dniową wersję TRIAL** oraz **otrzymaj poglądową wycenę**.

Xopero Software S.A

KONTAKT

Łukasz Nowatkowski
Cybersecurity Advocate

l.nowatkowski@xopero.com

KLASA PRODUKTU/USŁUGI

- **Bezpieczeństwo danych**
- **Backup i odzyskiwanie danych**
- **Backup i Disaster Recovery**
- **Cyberbezpieczeństwo**

ZAKRES DZIAŁALNOŚCI

Wiodący producent rozwiązań do backupu i przywracania danych w Polsce i na świecie. Firma działa na rynku od 2009 roku oferując klientom biznesowym oprogramowanie do backupu klasy enterprise, wysoce wydajne i skalowalne rozwiązanie sprzętowe oraz platformę MSP dla dostawców usług zarządzanych. Jest również właścicielem marki **GitProtect.io** – najbardziej profesjonalnego oprogramowania do backupu środowisk DevOps. Z rozwiązań Xopero korzystają firmy z Fortune 500, Orange, T-Mobile, AVIS, RED, NHS, Gladstone Institutes, Zoop, Diebold Nixford i nie tylko. Firma jest również jedynym oprogramowaniem do backupu polecanym w ramach ESET Technology Alliance przez większość zagranicznych dystrybucji firmy ESET.

Xopero ONE Backup&Recovery

Rozwiązanie do backupu danych All-in-ONE, czyli niezawodny backup i odzyskiwanie danych, najbardziej przyjazna na rynku konsola centralnego zarządzania oraz kompatybilność z każdym najpopularniejszym magazynem na dane.

Łatwość wdrożenia i zarządzania sprawia, że zabezpieczenie nawet najbardziej złożonej infrastruktury IT jest tak proste, jak ochrona zaledwie kilku komputerów.

Z Xopero ONE zabezpieczysz:

- Microsoft 365
- Endpointy (Windows, Linux, MacOS)
- Serwery (Windows ,Linux)
- Maszyny wirtualne (Vmware i Hyper-V)
- Bazy danych (MySQL, MS SQL, Oracle,
- Firebird, PostgreSQL i inne)
- DevOps (Github, Gitlub, Jira, Bitbucket).

ZOBACZ TEŻ:

GITPROTECT.IO

MASZ JAKIEŚ PYTANIA?
SKONTAKTUJ SIĘ Z NAMI!

OFFICE@CYBERMADEINPOLAND.PL

#CyberMadeInPoland