BEZPIECZNE MIASTO

C & C solution partner

Nowa perspektywa dla systemu zarządzania bezpieczeństwem i informacją w przestrzeni publicznej, czyli jak efektywnie, organizacyjnie i finansowo monitorować JST

PRELEGENT: Martyna Kubiak, Rafał Krawczyk

Agenda

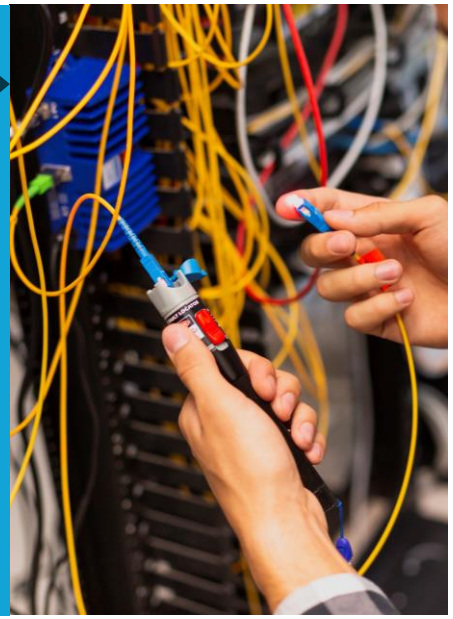
Program prezentacji:

1. Kilka słów o C&C
2. Projekty na jakie można dostać dofinansowania
3. Referencje
4. Cyberbezpieczeństwo – NIS 2
5. Nowoczesne systemy bezpieczeństwa:
    a. Platforma CCTV VDG Sense
    b. Komunikacja INFO/SOS
    c. Platforma integrująca PSIM:
    - Ćwiczenia - gdzie te oszczędności

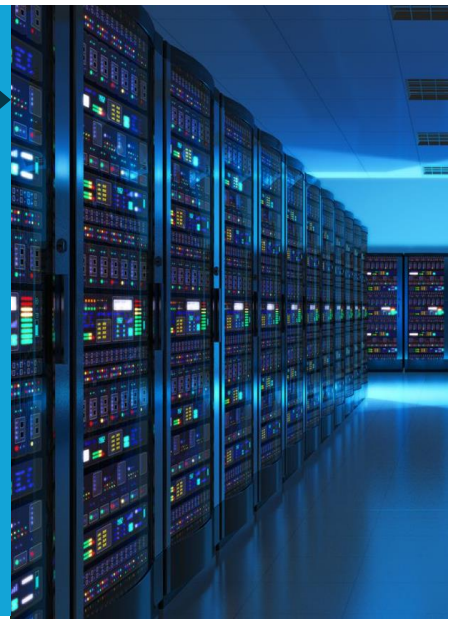
NOWOCZESNE ROZWIĄZANIA

sprawdzone przez tysiące użytkowników na świecie

TELEKOMUNIKACYJNE



TELEINFORMATYCZNE



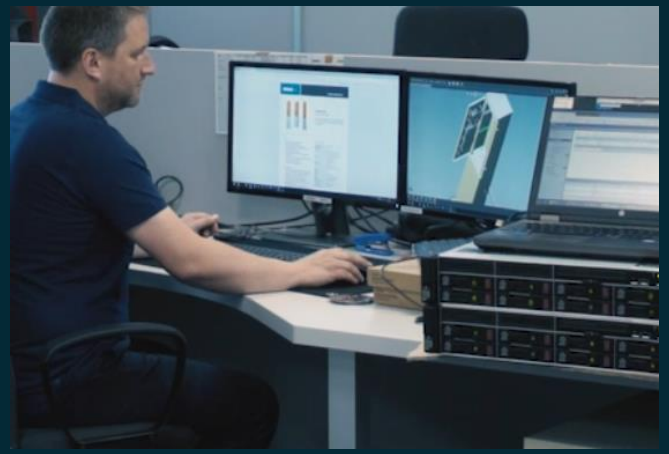
ZABEZPIECZEŃ

DOSTARCZAMY

KOMPLEMENTARNE ZINTEGROWANE

SYSTEMY

DOSTARCZAMY
KOMPLEMENTARNE ZINTEGROWANE
SYSTEMY



PROJEKTUJEMY

SZKOLIMY

WSPIERAMY WDROŻENIE

TKH na świecie

138 firm w 28 krajach

TKH GROUP

w LICZBACH

- zespół **6899** pracowników
- ponad **1,85** mld euro obrotu w 2023
- notowana na giełdzie w Amsterdamie
- **16,1**% - **30** mln euro obrotu z innowacji
- >**500** patentów z zakresu nowych technologii

TKH GROUP **w POLSCE**

5 FIRM - 579 PRACOWNIKÓW

JESTEŚMY BLISKO KLIENTA

POLSKA

ODDZIAŁY REGIONALNE

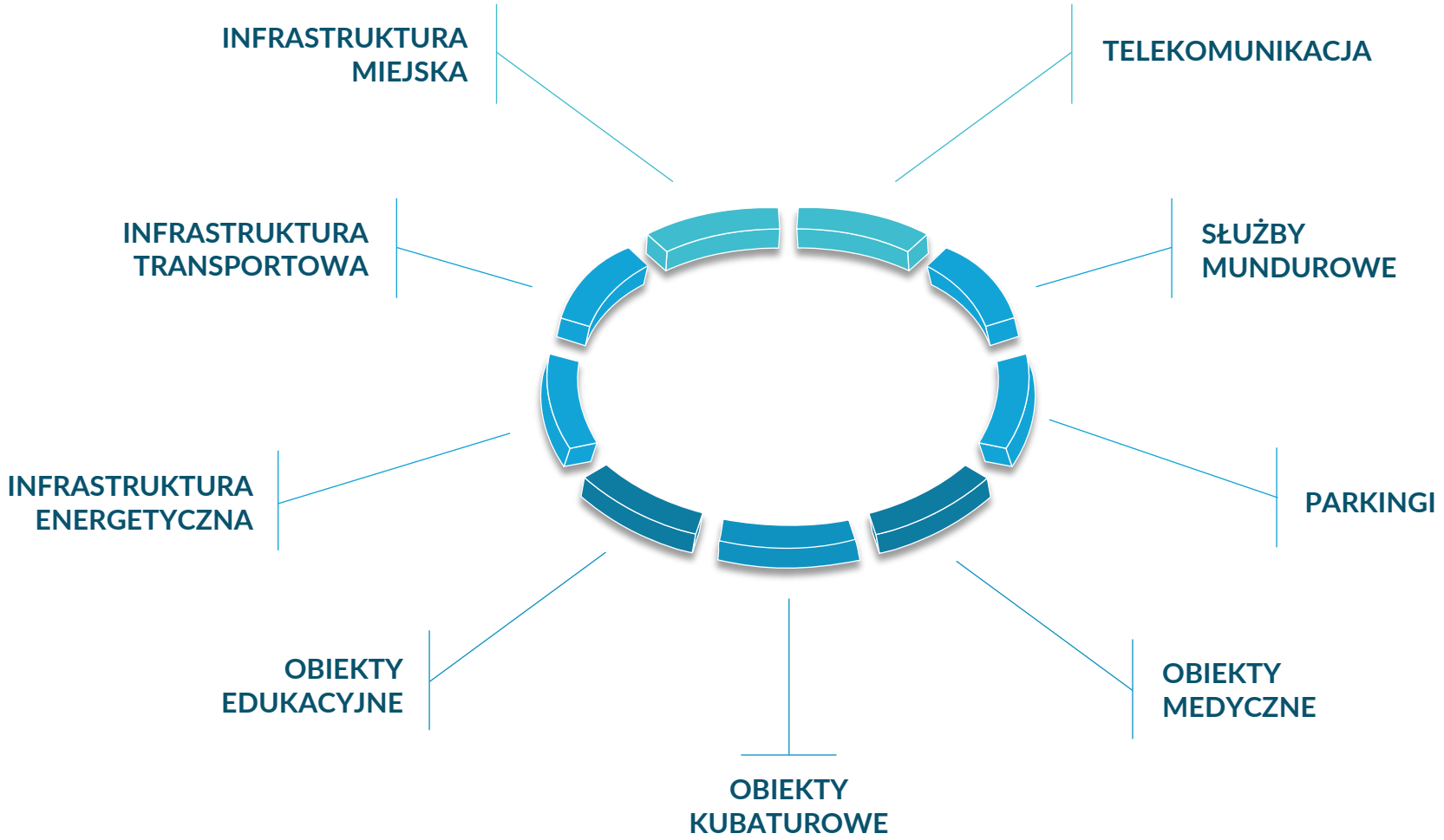
LESZNO

WARSZAWA

GDAŃSK

KATOWICE

KLUCZOWE OBSZARY DZIAŁAŃ



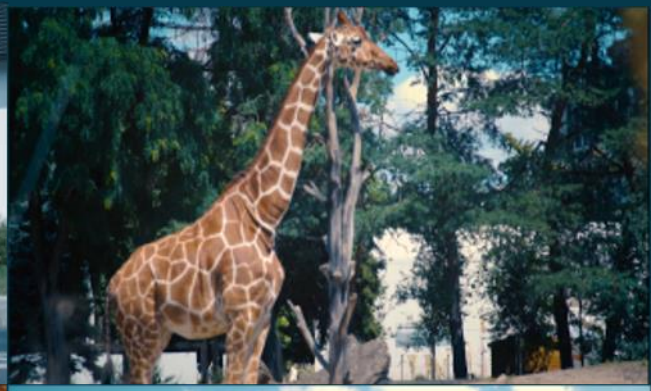
SYSTEMY C&C Partners

1. Integrujące i wizualizacyjne (PSIM)
2. Interkomowy
3. Kamery specjalistyczne
4. Kontroli dostępu
5. Monitoringu i analizy obrazu
6. Zarządzania parkingiem
7. Sygnalizacji włamania i napadu
8. Okablowania strukturalnego
9. Światłowodowy
10. Telekomunikacyjny miedziany



C&C Partners Referencje






Monitoring VDG Sense – referencje w wielkopolsce

Leszno

Rawicz

Gostyń

Lwówek

ZTP Poznań

Lipno

Czempiń

Cele na które można pozyskać dofinansowanie

Cele na które można pozyskać dofinansowanie

***EFRR.CP1.II Czerpanie korzyści z cyfryzacji** dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych.*

- ***„Inwestycje w obszarze cyberbezpieczeństwa, tj. wzmacniania odporności systemów, zdolności do skutecznego zapobiegania i reagowania na incydenty (w systemach informatycznych JST, podmiotów publicznych podlegających JST)** wyłącznie jako element projektu określonego w Typie 1."*
- *„**Wsparcie skalowalnych nowoczesnych rozwiązań informatycznych i technologicznych w ramach współpracy międzysektorowej obejmującej, w szczególności administrację publiczną, przedsiębiorców i organizacje badawcze**."*

Cel na które można pozyskać dofinansowanie

- *„Wsparcie w zakresie **rozwijania i wprowadzania systemów monitorowania i zarządzania energią** (energia elektryczna, ciepło, gaz) **w budynkach należących do JST”***

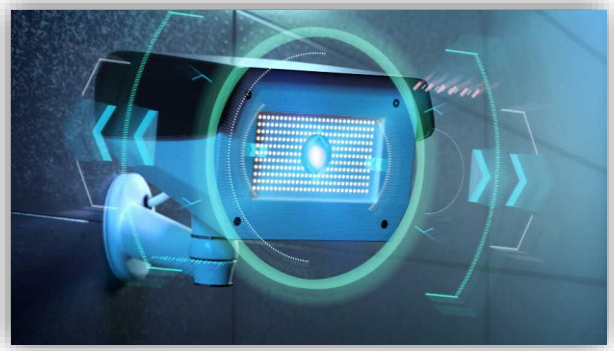
Technologie innowacyjne, na które można dostać dofinansowanie

System PSIM

Zarządzania wszystkimi systemami fizycznymi oraz bezpieczeństwa w JST

Monitoring CCTV z AI

Sztuczna inteligencja wykonująca zawansowane analityki na bazie monitoringu wizyjnego



Komunikacja INFO / SOS

Systemy komunikacji interkomowej wspierane przez sztuczną inteligencje AI

BEZPIECZNE MIASTO

Cyberbezpieczeństwo

BEZPIECZNE MIASTO

Cyberbezpieczeństwo – NIS 2 (Dyrektywa Unii Europejskiej

Podmioty
w NIS2

Kogo dotyczy NIS 2 ?

Nowe podmioty w NIS 2

Dyrektywa Unijna - NIS 2 obejmuje dwa typy podmiotów w zależności od czynników takich jak:

- **Wielkość**,
- **Sektor**,
- **Krytyczność**.

Typy Podmiotów :

- podmioty **niezbędne** (*essential entities*)
- podmioty **istotne/ważne** (*important entities*).

NIS2 podmioty niezbędne i istotne

Podmioty niezbędne (*essential entities*) to podmioty z następujących sektorów:

1. **Energetyka**
2. **Transport**
3. **Bankowość**
4. **Infrastruktura rynków finansowych**
5. **Zdrowie**
6. **Woda pitna**
7. **Ścieki**
8. **Infrastruktura cyfrowa**
9. **Zarządzanie usługami ICT**
10. **Administracja publiczna**
11. **Przestrzeń kosmiczna**

NIS 2 Podmioty istotne (important entities)

Podmioty istotne (*important entities*) to podmioty z następujących sektorów:

1. **Usługi pocztowe i kurierskie**,
2. **Gospodarowanie odpadami,**
3. **Produkcja** (wyroby medyczne i wyroby medyczne do diagnostyki in vitro, produkty komputerowe, elektroniczne i optyczne; sprzęt elektryczny; maszyny i wyposażenie; pojazdy samochodowe, przyczepy i naczepy; inny sprzęt transportowy)
4. **Produkcja i dystrybucja chemikaliów**,
5. **Produkcja, przetwarzanie i dystrybucja żywności,**
6. **Dostawcy cyfrowi**

UWAGA!

Poza **dostawcami cyfrowymi**, żaden z tych sektorów nie był, jak dotąd objęty Dyrektywą NIS.

NIS2 (network and information systems)

Kary

- NIS 2 przewiduje wysokie kary finansowe dla podmiotów nie realizujących zapisów we właściwy sposób.
- Kary te mają wynosić nawet **10 mln EUR** lub do **2% całkowitego rocznego światowego obrotu** przedsiębiorstwa, w zależności od tego, która kwota jest wyższa.
- Jest to duża zmiana w porównaniu do wcześniejszej Dyrektyw, której zapisy mówiły tylko o karach „poziomie psychologicznym” → RODO

Środki zarządzania ryzkiem w cyberbezpieczństwie

Artykuł 21

Środki zarządzania ryzykiem w cyberbezpieczeństwie

1. Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należycie uwzględnia się stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:

a) politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;

b) obsługę incydentu;

c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;

d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;

e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;

f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;

g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;

h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;

i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;

j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

Oświadczenie Polsko-Chińskiej Głównej Izby Gospodarczej SinoCham w sprawie „Projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa".

rtnerem publikacji jest Polsko-Chińska Główna Izba Gospodarcza noCham

opublikowano: 2024-05-24 09:41

kwietnia 2024 r. Ministerstwo Cyfryzacji przedstawiło projekt iany ustawy o krajowym systemie cyberbezpieczeństwa oraz których innych ustaw („KSC"). Wyznaczono jednocześnie termin nsultacji publicznych do 24 maja 2024 r. Polsko-Chińska Główna Izba ospodarcza SinoCham („SinoCham") przywiązuje dużą wagę do tej kwestii i z zaniepokojeniem patrzy na proponowane przez legislatora zapisy.

Posłuchaj

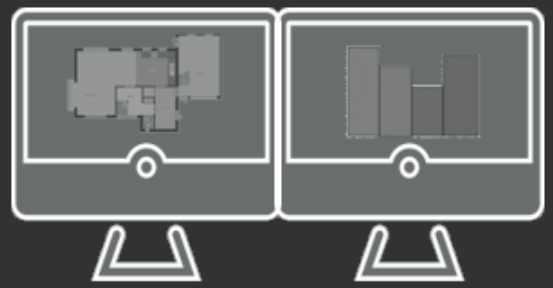
https://www.pb.pl/oswiadczenie-polsko-chinskiej-glownej-izby-gospodarczej-sinocham-w-sprawie-projektu-nowelizacji-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-1216617

C&C solution partner

VDG SENSE

VDG SENSE VMS

BEZPIECZNE MIASTO



TKH Security

Security & Park Management

TKH Security
iProtect
Access Control

TKH Security
VDG Sense
Video Management

TKH Security
Siqura
Integrated Camera Solutions

TKH Security
ParkEyes ParkAssist
Parking Guidance

TKH Group
Tattile
ANPR Cameras

TKH Group
Commend
Intercom

TKH Group
Alphatronics
Intrusion Detection

Cyberbezpieczeństwo

BEZPIECZNE MIASTO

VDG SENSE – certyfikaty, standardy

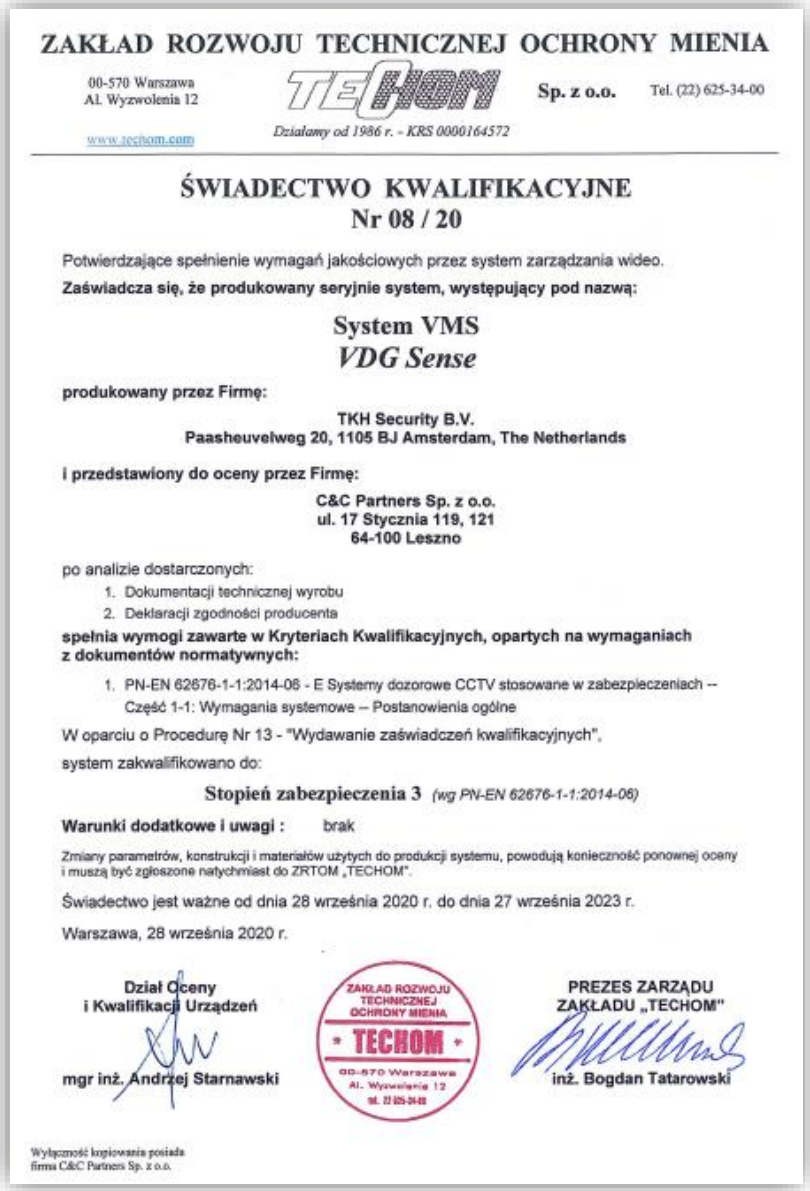
VDG SENSE Grade 3

Zgodność z normą CCTV:

- PN-EN-62676-1-1 2014-06
- Stopień zabezpieczenia 3

VDG SENSE Grade 4

W opracowaniu



ZAKŁAD ROZWOJU TECHNICZNEJ OCHRONY MIENIA

00-570 Warszawa
Al. Wyzwolenia 12

TECHOM Sp. z o.o. Tel. (22) 625-34-00

www.techom.com

Działamy od 1986 r. - KRS 0000164572

ŚWIADECTWO KWALIFIKACYJNE
Nr 08 / 20

Potwierdzające spełnienie wymagań jakościowych przez system zarządzania wideo.

Zaświadcza się, że produkowany seryjnie system, występujący pod nazwą:

System VMS
VDG Sense

produkowany przez Firmę:

TKH Security B.V.
Paasheuvelweg 20, 1105 BJ Amsterdam, The Netherlands

i przedstawiony do oceny przez Firmę:

C&C Partners Sp. z o.o.
ul. 17 Stycznia 119, 121
64-100 Leszno

po analizie dostarczonych:

1. Dokumentacji technicznej wyrobu
2. Deklaracji zgodności producenta

spełnia wymogi zawarte w Kryteriach Kwalifikacyjnych, opartych na wymaganiach z dokumentów normatywnych:

1. PN-EN 62676-1-1:2014-08 - E Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-1: Wymagania systemowe -- Postanowienia ogólne

W oparciu o Procedurę Nr 13 - "Wydawanie zaświadczeń kwalifikacyjnych",

system zakwalifikowano do:

Stopień zabezpieczenia 3 *(wg PN-EN 62676-1-1:2014-06)*

Warunki dodatkowe i uwagi : brak

Zmiany parametrów, konstrukcji i materiałów użytych do produkcji systemu, powodują konieczność ponownej oceny i muszą być zgłoszone natychmiast do ZRTOM „TECHOM".

Świadectwo jest ważne od dnia 28 września 2020 r. do dnia 27 września 2023 r.

Warszawa, 28 września 2020 r.

Dział Oceny i Kwalifikacji Urządzeń
mgr inż. Andrzej Starnawski

ZAKŁAD ROZWOJU TECHNICZNEJ OCHRONY MIENIA * TECHOM * 00-570 Warszawa Al. Wyzwolenia 12

PREZES ZARZĄDU ZAKŁADU „TECHOM"
inż. Bogdan Tatarowski

Wyłączność kopiowania posiada firma C&C Partners Sp. z o.o.

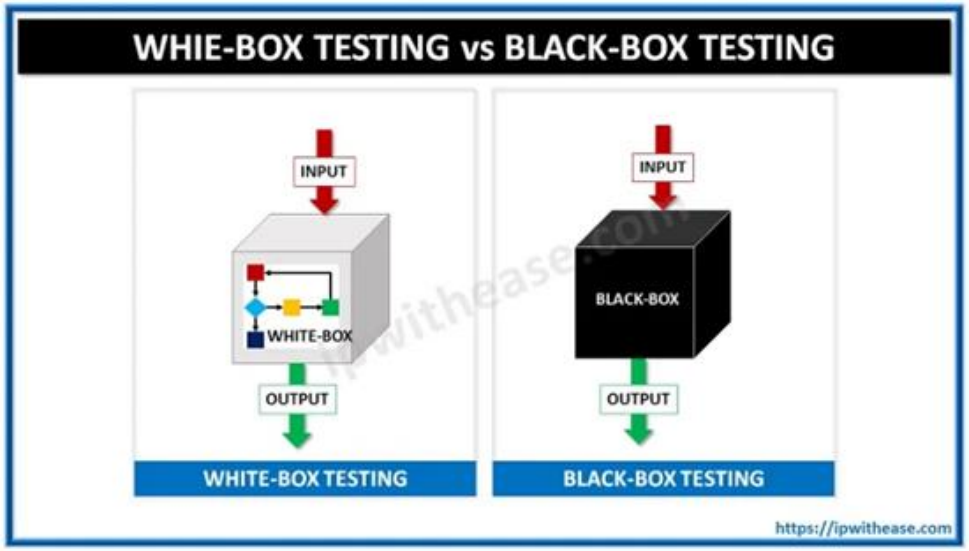
VDG SENSE Cyberbezpieczeństwo

TKH Security – cyberbezpieczeństwo

- Najwyższy priorytet w zakresie rozwoju, wdrażania, kontroli i utrzymania
- **Pełnoetatowy certyfikowany specjalista ds. ryzyka cybernetycznego Cyber Risk Officer**
- TKH Security realizuje projekty zgodne z normą IEC 62443 min dla instytucji rządowych na całym świecie
- Certyfikaty ISO9001, ISO14001, **ISO 27001** (finalizacja)
- Doświadczony partner w złożonych, dużych i cyberbezpiecznych instalacjach

VDG SENSE 2.7.1 – kwiecień 2023

- Ulepszenia bezpieczeństwa cybernetycznego w wersji 2.7
- Black Box Pen Testing
- White Box Pen Testing



VDG SENSE

- Cała komunikacja SenseServer SenseClient jest szyfrowana
- **Silniejsze szyfrowanie haseł (od AES 128 do AES 256)**
- Opcjonalna historia haseł (nie używaj ponownie starego hasła)
- Ulepszona funkcja przełączania awaryjnego (bardziej niezawodna w większych instalacjach)
- **Koniec z domyślnymi hasłami, wszystkie hasła muszą być skonfigurowane (koniec z backdoorami)**
- Wszystkie hasła muszą być ustawione z nowymi regułami złożoności haseł podczas aktualizacji z 2.5/2.6 -> 2.7
  - 12 znaków, 1 cyfra, 1 wielka litera, 1 symbol
  - Nie można użyć hasła, które jest zbyt podobne do nazwy użytkownika

VDG SENSE - bezpieczeństwo danych

- Szyfrowanie konfiguracji
- **Szyfrowanie transmisji danych AES256**
- **Integracja z Active Directory (LDAP)**
- HTTP OpenAPI SSL
- Dualne logowanie
- Szyfrowanie danych, konfiguracji
- Wielopoziomowe bezpieczeństwo danych - redundancje
- Audyt działań operatora

VDG SENSE – certyfikaty, standardy

NDAA 889

SIQURA

Siqura B.V.

Meridiaan 32
2801 DA Gou
The Netherla

+31 182 592
info@siqura.
siqura.com

August 14 2020

National Defense Authorization Act (NDAA) Statement

On August 13 2018, the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 was signed into U.S. Law*. NDAA Section 889 prohibits the U.S. government from procuring or using video surveillance and telecommunications equipment or services from certain Chinese companies and their subsidiaries. The NDAA ban includes the following companies:

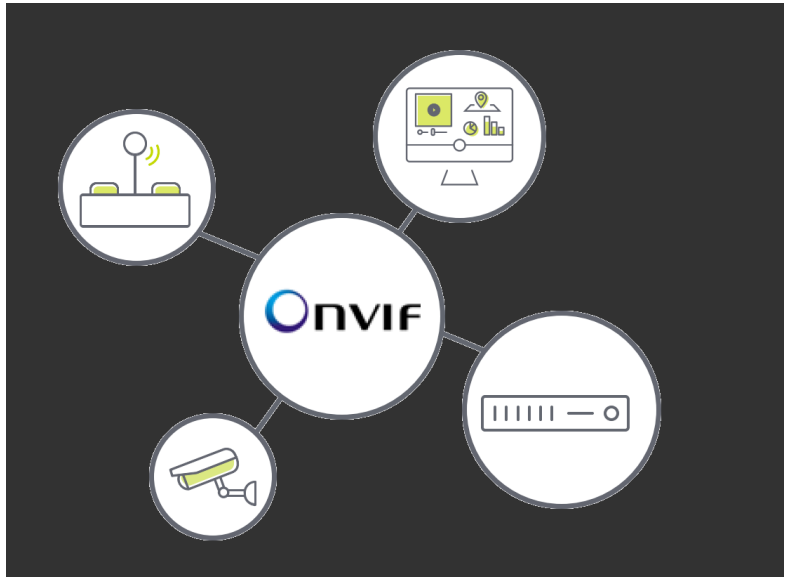
- Hytera Communications Corporation Limited
- Hangzhou Hikvision Digital Technology Company Limited
- Zhejiang Dahua Technology Company Limited
- Huawei Technologies Company
- ZTE Corporation.

With this statement, Siqura, Inc. declares that the following products within its product range are NDAA section 899, compliant**:

- Video Over Fiber
- EVE Encoders
- Industrial encoders and decoders
- Hardened encoders
- Power supplies
- Box cameras
- Bullit cameras
- Fixed Domes
- High speed PTZ domes
- Varifocal lenses DC-iris
- Safe area cameras
- Explosion proof cameras
- EX/SA Integrated cameras
- EX/SA Interface/cable tail
- Accessories for SA/EX cameras
- XCU Fusion
- XCU Compact
- Traffic PTZ
- Media Converters
- Ethernet switches
- SFP Plugs

Otwartość na urządzenia końcowe:

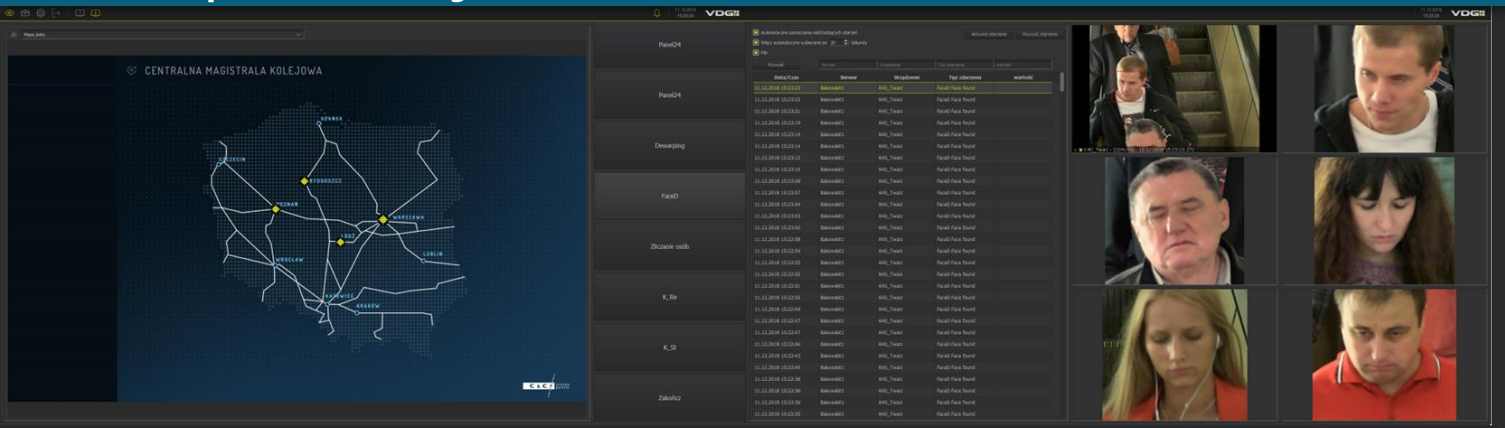
- ONVIF G, S, T, RTSP
- Ponad 30 producentów zintegrowanych w protokołach producenckich
- Tysiące modelu kamer

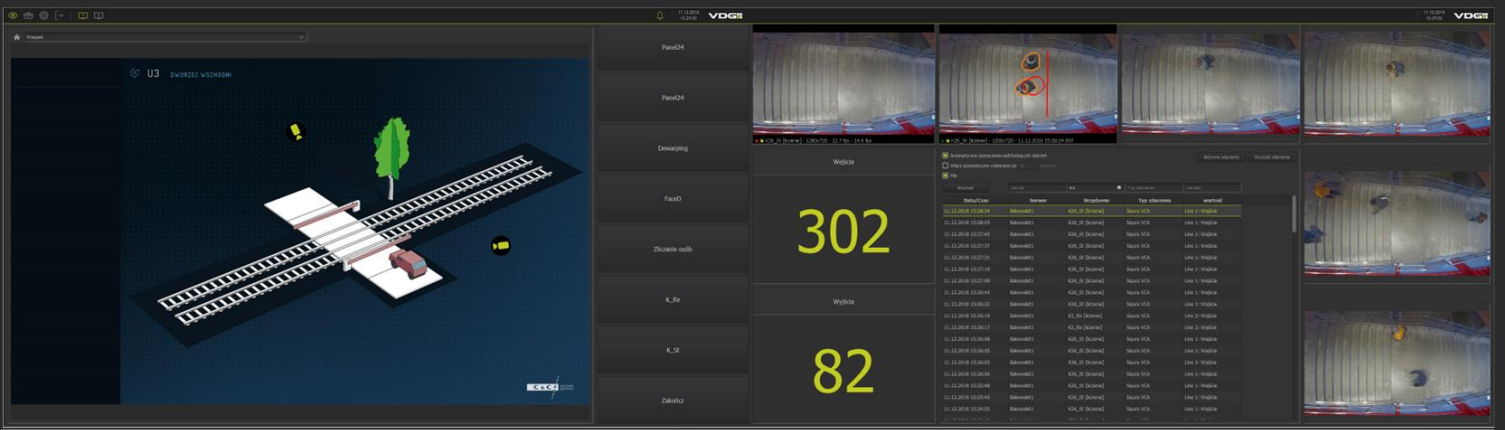


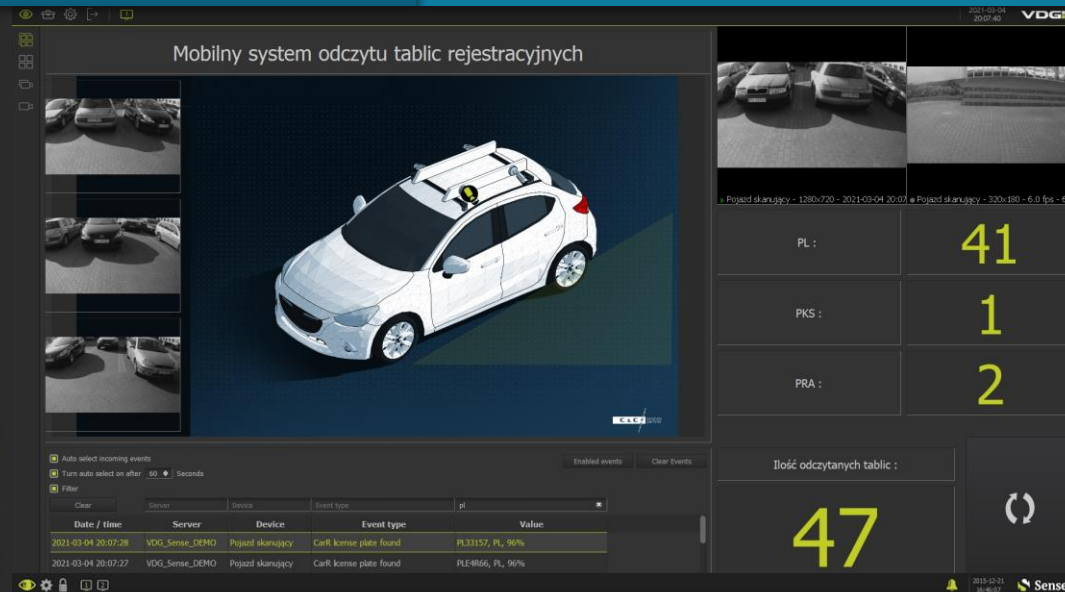
Otwartość na urządzenia serwerowe:

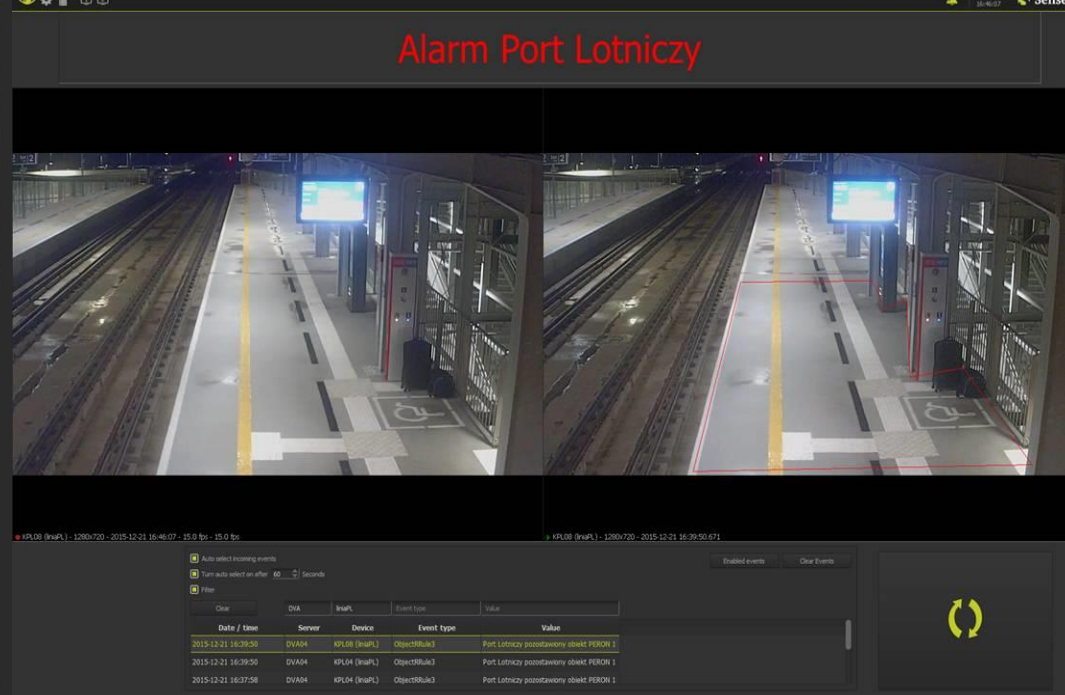
- Dedykowanie serwer VDG SENSE – prekonifgurowane, dopasowane komponentami
- Serwery Dell, HP itd.
- Wirtualizacja VMware, Hyper-V

Intuicyjna obsługa = szybkość wsparcie operatora = bezpieczniejsi ludzie i obiekt

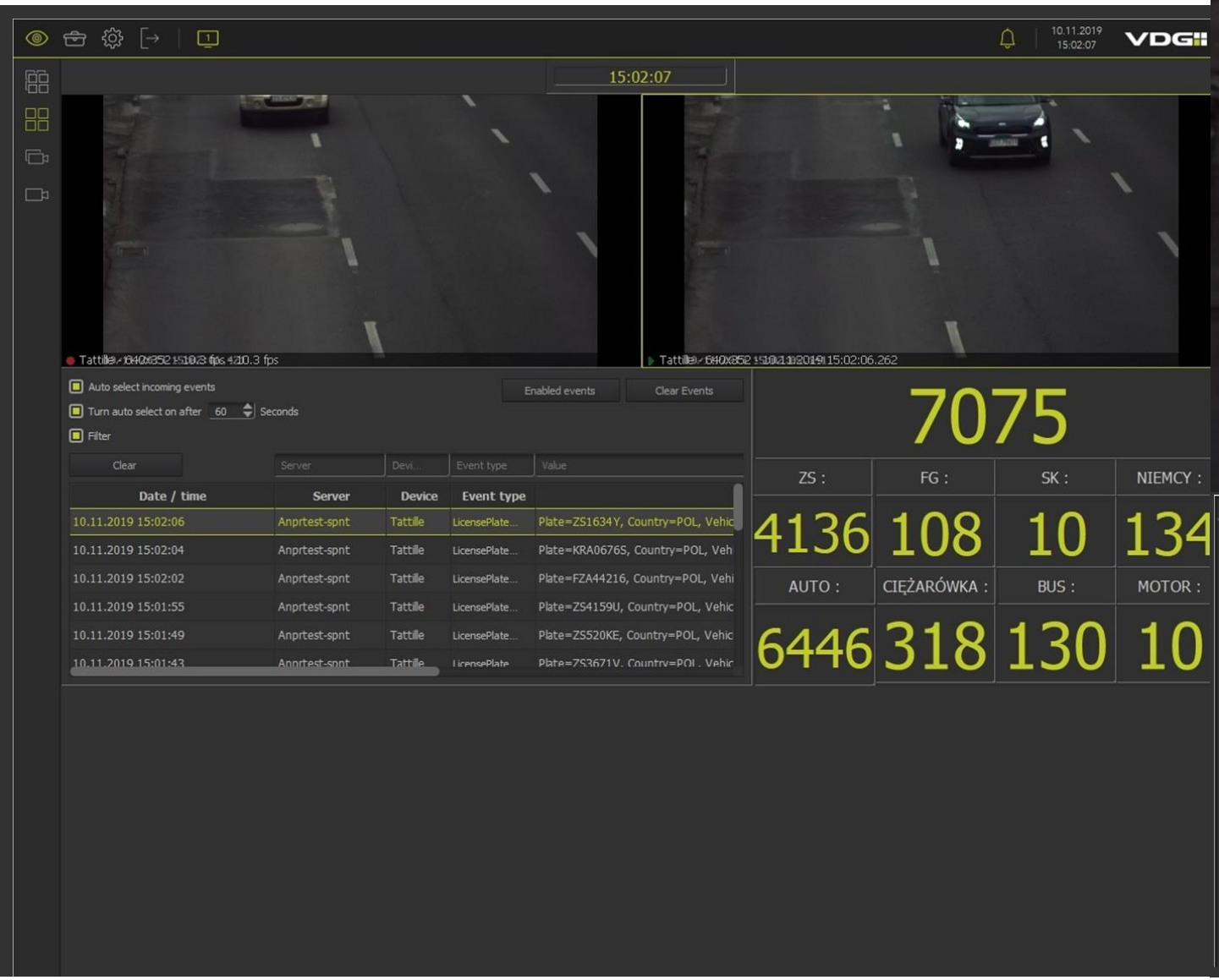


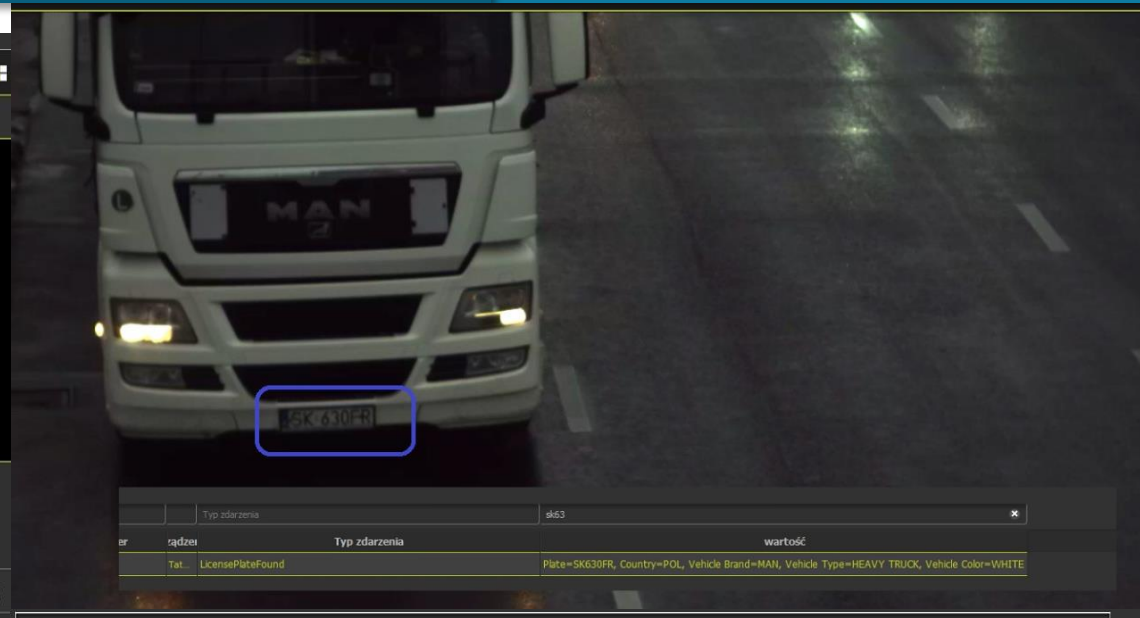


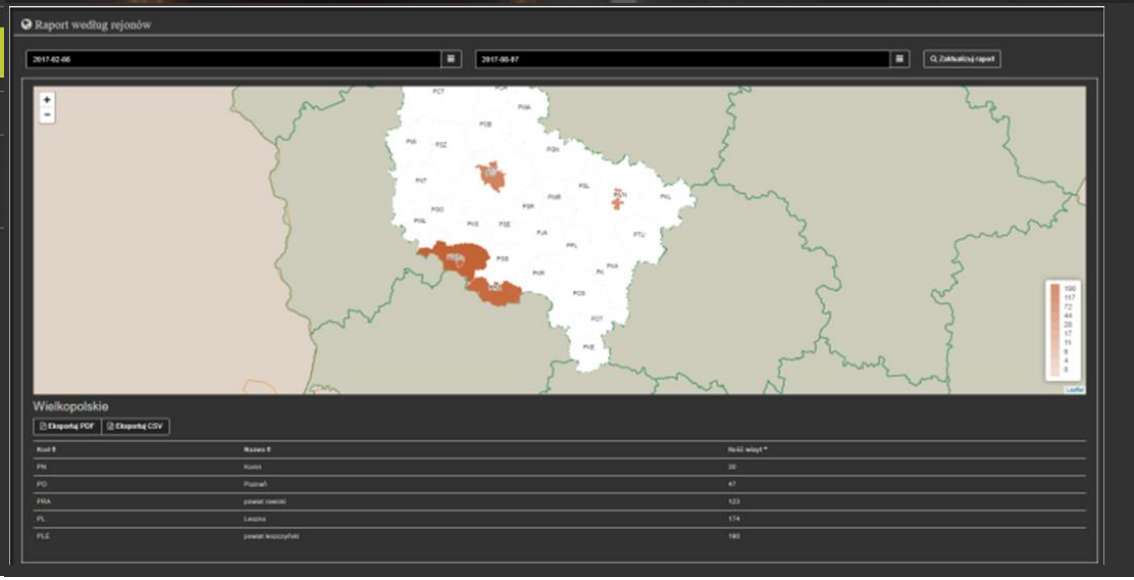




VDG SENSE - raporty



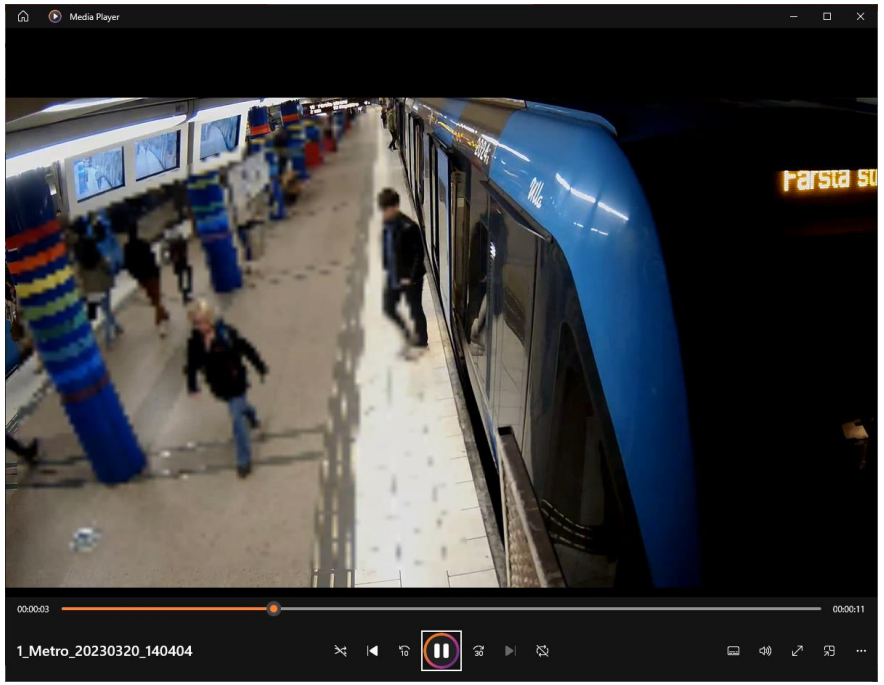


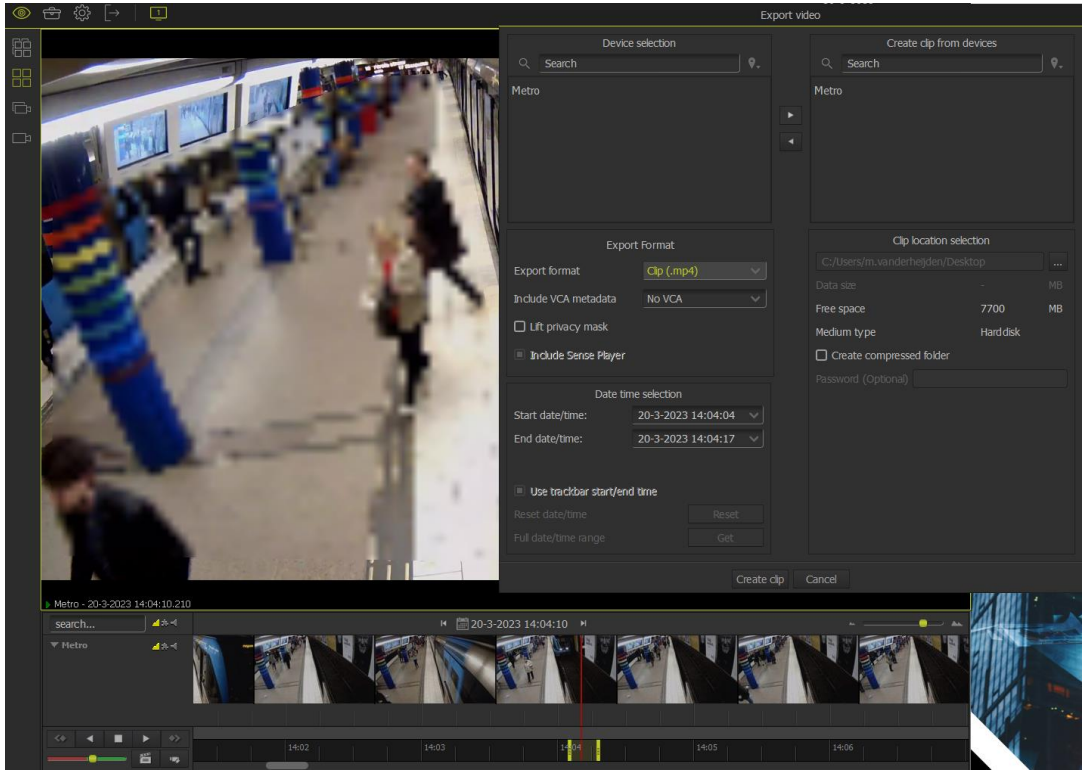


VDG SENSE 2.7 - Funkcja ANONIMIZACJA (zgodność z RODO)

Zdefiniowana przez użytkownika maska prywatności – eksport zdjęcia

- Użytkownik z uprawnieniem „ Usuń maskę prywatności” może eksportować eksport obrazu/pdf z maską prywatności lub bez niej





Kamery wieloobiektywowe

Wybór urządzeń dopasowany do planowanej metody eksploatacji systemu

- stosowanie kamer szybkoobrotowych w systemach z personelem operatorów
- unikanie nagromadzenia wielu kamer w jednej lokalizacji
- dopasowanie akcesoriów montażowych do architektury

Kamery wieloobiektywowe - estetyka

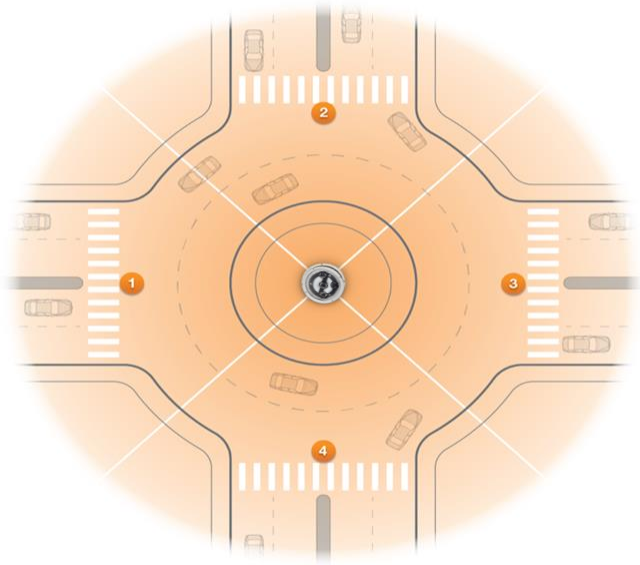
Klasyczne rozwiązania vs. rozwiązanie C&C

Kamery wieloobiektywowe

Zalety kamer wielobiektywowych:

- Większa rozdzielczość 12-40 Mpx
- Większa skuteczność przy zwiększonej estetyce
- Mniejsza liczba urządzeń = mniejsze koszty utrzymar
- Mniej okablowania, przełączników , licencji VMS
- Niski pobór mocy (GreenIT)

Kamery wieloobiektywowe – brak ślepych stref



BEZPIECZNE MIASTO

Kamery wieloobiektywowe – brak ślepych stref

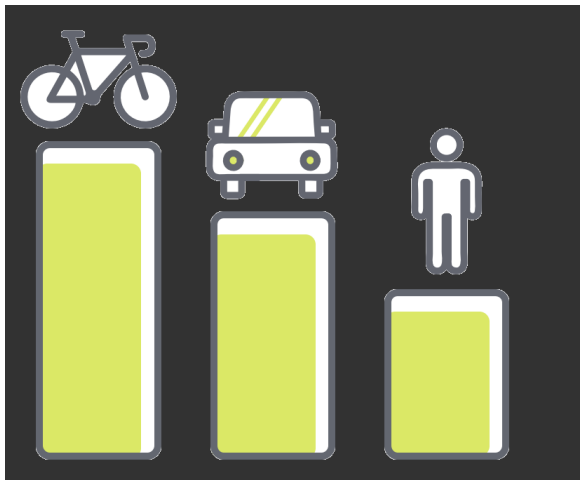
Analiza obrazu VCA

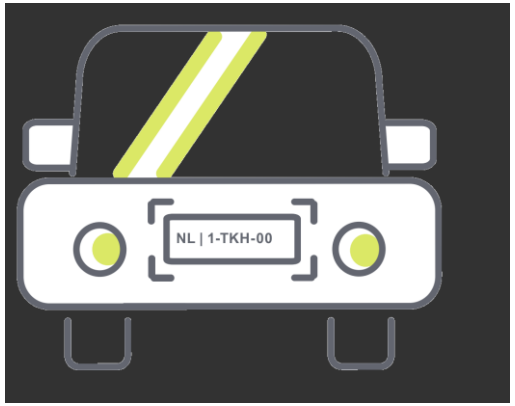
W standardzie:

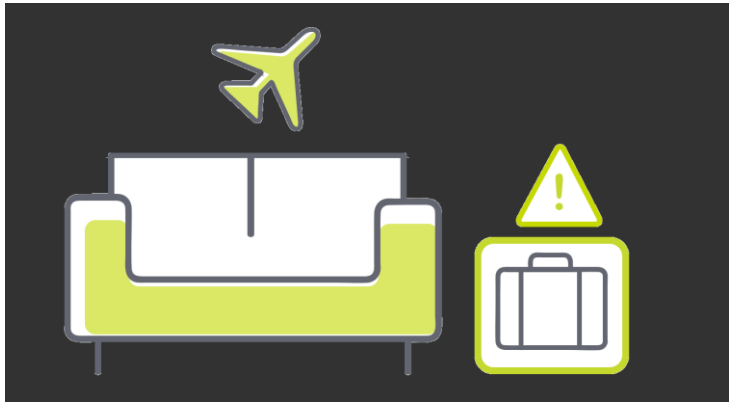
- MotionD – detekcja ruchu
- ColorD- wykrywanie koloru
- SceneR - wykrywanie zmiany sceny
- FaceD - wykrywanie twarzy

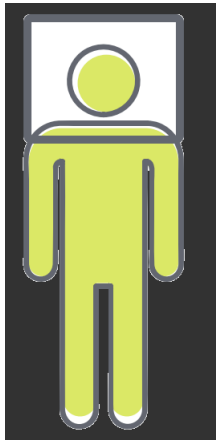
Licencjonowane:

- ObjectR - wykrywanie obiektów
- ObjectC - klasyfikacja obiektów
- CarR - rozpoznawanie tablic rejestracyjnych
- Moduły inspekcyjna VCA AI
- Analizy drogowe AID







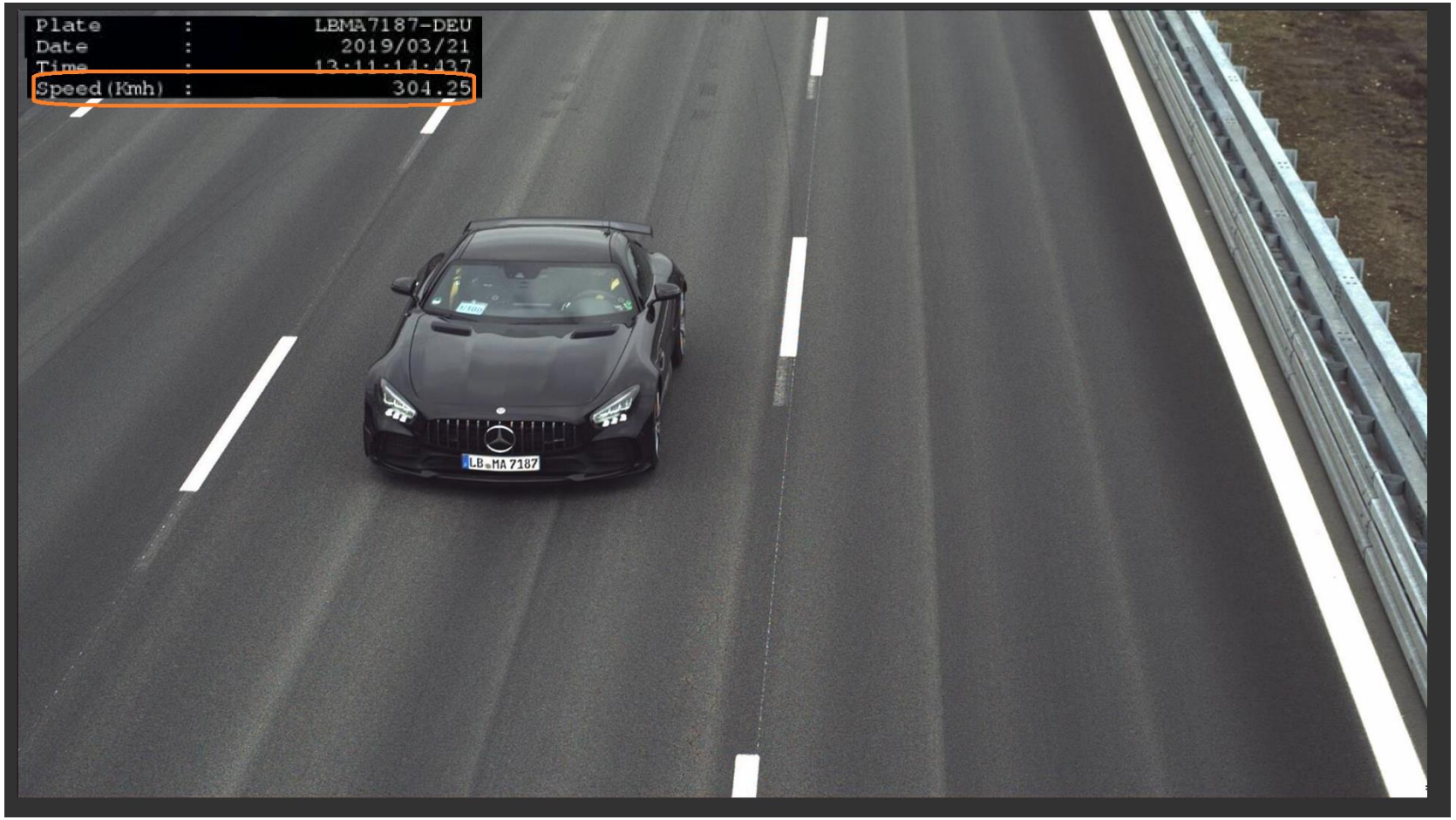


Moduł parkingowy – on street – zajętość miejsc

- Nowy modelu AI do wykrywania zajętości miejsc parkingowych za pomocą kamer CCTV
- Dana dla systemów ITS/Parkingowych o zajętości miejsc
- Model AI działający w oddzielnej usłudze, umożliwiający łatwe aktualizacje
- Implementacja jest podstawą przyszłych aktualizacji do ObjectC

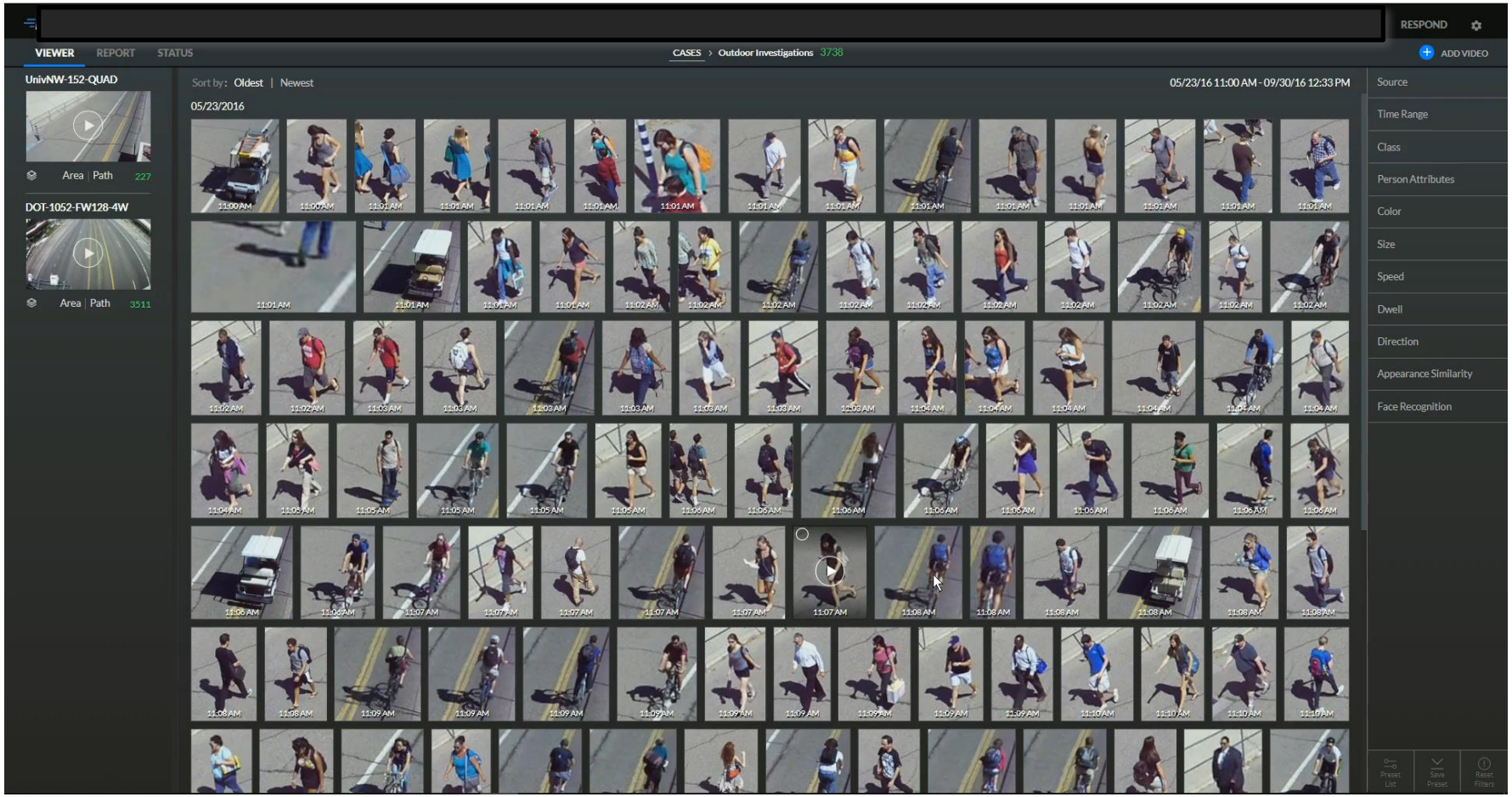
VDG SENSE – analiza tablic LPR Tattile AI

Wydajność 320 km/h +



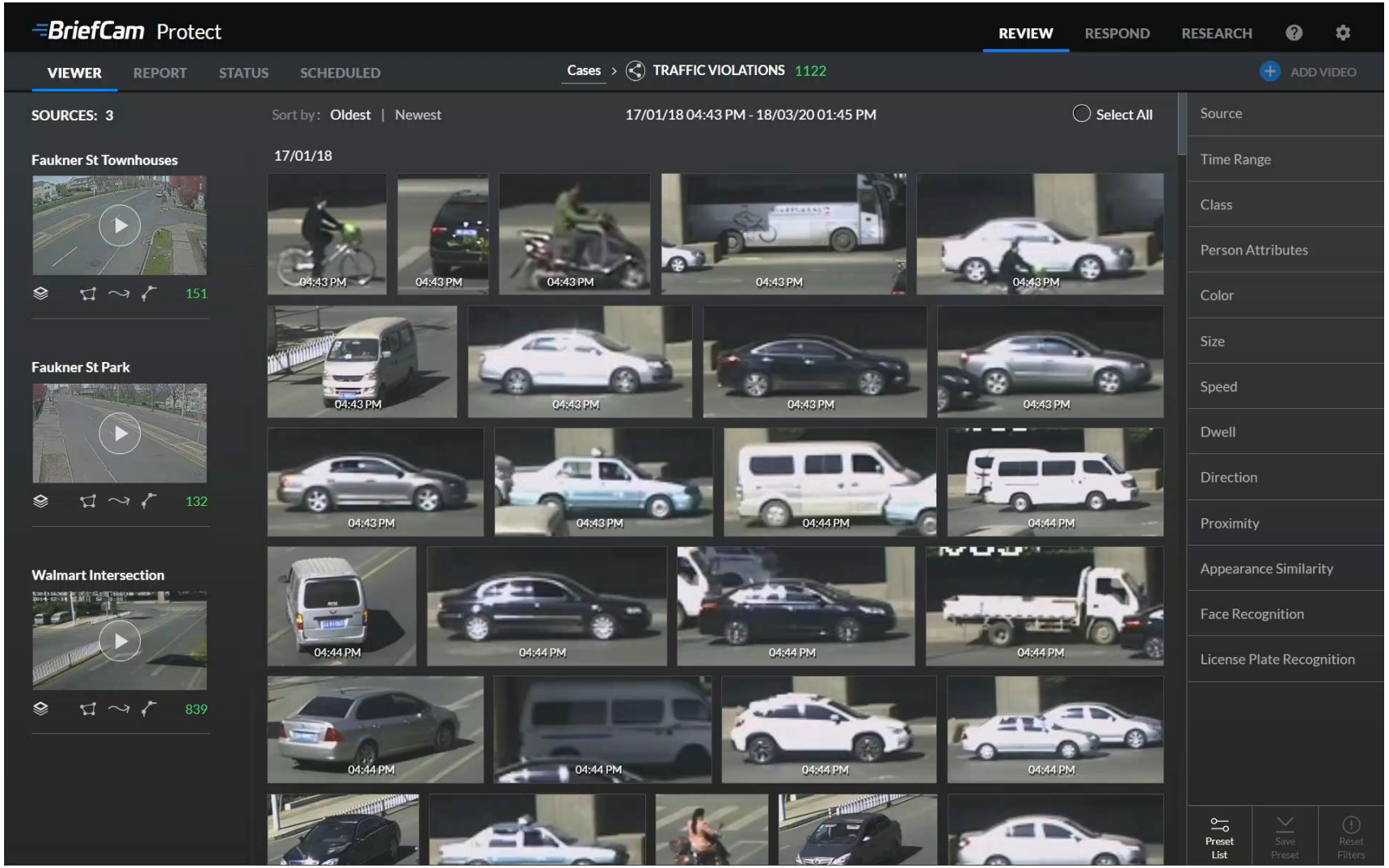
VDG SENSE – analiza obrazu AI

Moduł inspekcyjny



VDG SENSE – analiza obrazu

Moduł inspekcyjny – wykroczenia – jazda pod prąd



Centralny System monitoringu – platforma wizyjna VMS VDG Sense

Wzrost bezpieczeństwa i obniżenie kosztów poprzez zabezpieczenie infrastruktury krytycznej Centralnym Systemem Monitoringu (ujęcia wody, źródła ciepła, kolektory wody, itd.) np. Rzeszów - skażenie wody

BEZPIECZNE MIASTO

Prewencja – integracja monitoringu z systemem komunikacji INFO/SOS Commend

Ochrona obiektów przed dewastacją – dzięki integracji monitoringu z tubami rozgłoszeniowymi np.: Straż Miejska może zapobiegać dewastacji (graffiti, niszczenie koszy na śmieci itd.)

Zarządzanie efektywnością energetyczną

Wykorzystanie systemów monitoringu jako sensorów do wygaszania światła w obiektach, obszarach publicznych jeżeli nie wykrywamy ruchy (place zabaw, parki).

Konsolidacje systemów monitoringu zainstalowanych w obiektach zarządzanych przez miasto (szkoły, muzea, parki obiekty sportowe)
w jeden system z wykorzystaniem infrastruktury światłowodowej. Cel to:

- redukcja kosztów energii,
- redukcja ilość sprzętu lokalnego,
- obniżenie kosztów osobowych,
- wzrost nadzoru nad nieruchomościami miejskimi,
- obniżenie kosztów serwisu,
- poprawić jakość i sprawność systemu poprzez włączenie analityk obrazu jako aktywną ochronę obiektów.

BEZPIECZNE MIASTO

Inne usługi realizowane dzięki zaawansowanej analityce obrazu CCTV AI

1. Monitoring ruchu pojazdów z podziałem na typ np. ciężarówki - monitoring przejazdu ciężarówek przez miasto (noc, dni wolne od pracy itd., lato ograniczenia ze względu na temperaturę jezdni)
2. Lokalizacja ruchu służbowych pojazdów: np. autobusy komunikacji miejskiej, mapy GIS
3. Aplikacja lub Karta Mieszkańca np. Karta Leszczyniak:
    - karta dostępowa, dzięki której mieszkańcy miasta i gmin ościennych będą mieli mniejsze opłaty parkingowe lub wejścia na imprezy masowe (np. mecze koszykówki, żużel)
    - aplikacja poprzez, którą mieszkańcy będą mogli po identyfikacji komunikować się z urzędami (ograniczenie hejtu)
4. Monitoring Jakości Powietrza:
    - ekrany z informacją o jakości powietrza w mieście
    - dron, który monitoruje jakość powietrza pobiera próbki z aktywną mapą lokalizacji GIS

Parkingi

Parkingi – zarządzanie (ochrona klimatu, zmniejszenie smogu przez ograniczenie ruchu w poszukiwaniu wolnych miejsc parkingowych)

- Monitoring miejsc parkingowych i ilości samochodów na danych ulicach – pętle indukcyjne połączone z kamerami monitoringu w celu zliczania ilości samochodów na ulicach
- Wolne miejsca parkingowe – aplikacja internetowa
- Mapa ciepła ruchu samochodów – informacja o natężeniu ruchu dostępna na aplikacji mobilnej poprzez zliczanie ilości samochodów przez kamery z analityką obrazu

Systemy SOS – Komunikacja interkomowa informacyjno - ratunkowa

DOFINANSOWANIE

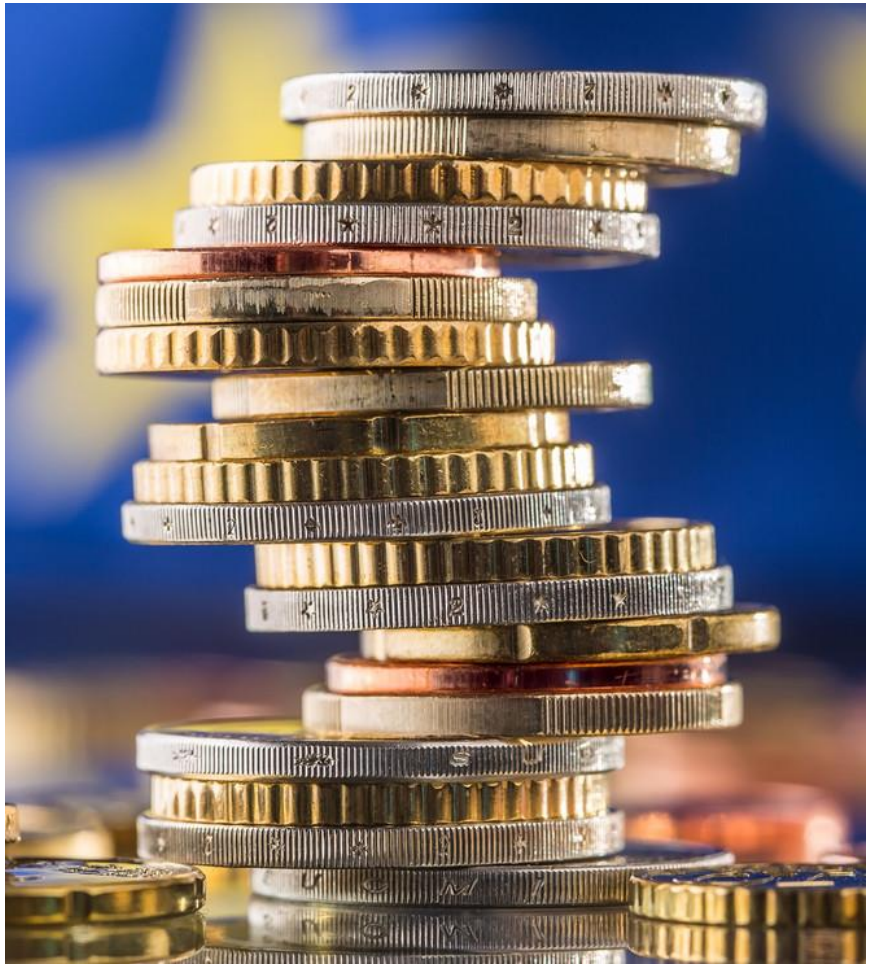
PPROGRAM

Dostępny Samorząd 2.0

Program na rzecz zwiększania dostępności usług publicznych w JST:

- Ograniczenie problemu wykluczenia społecznego poprzez lepszego udostępnienia usług publicznych oraz dostępu do obiektów i przestrzenie pozostające w dyspozycji JST

- **JST będą mogły otrzymać granty o średniej wartości 300 tys. zł (min. 200 tys. zł; max 400 tys. zł)**



DOFINANSOWANIE - Dostępny Samorząd 2.0

Propozycja na rozpisanie grantu zgodnie z rozporządzeniem

W ramach grantu należy sfinansować wydatki dotyczące zapewnienia dostępności usług świadczonych przez samorządy.

Mogą to być przedsięwzięcia takie jak np.:

- likwidacja barier komunikacyjnych w budynkach i przestrzeni publicznej,
- **instalacja urządzeń lub innych środków technicznych do obsługi osób słabosłyszących**
- zapewnienie na stronie internetowej JST informacji w postaci nagrań w polskim języku migowym.

DOFINANSOWANIE - Dostępny Samorząd 2.0

Przykładowe propozycje rozwiązań:

- Rozwiązania oparte na urządzeniach interkomowych np. **Punkty komunikacji informacyjno-ratunkowej** (INFO/SOS np. firmy Commend) wykonane w formie kolumn, słupków, w zabudowie naściennej lub aplikacji na smartfony **)**

- Monitoringu urządzeń do komunikacji dla osób niepełnosprawnych

- Ekologicznym oraz równomiernym oświetleniu tunelowym wraz z wbudowanymi głośnikami, z których w razie potrzeby rozgłaszane są komunikaty przez osoby sprawujące nadzór nad bezpieczeństwem w mieście.

Mieszkańcy – usługi

Punkt INFO SOS

Kolumny wykorzystujące sztuczna inteligencje – Asystent Commend IVY:

- Wzrost komunikacji poprzez szybki dostęp do informacji – ograniczenie kosztu – całą prace wykonuje Asystent IVY - sztuczna inteligencja
- Wzrost bezpieczeństwa poprzez bezpośrednią komunikacje z operatorem w momencie zagrożenia życia, utraty mienia itd.
- Np..: News Leszno – wyświetlanie na kolumnach (interkomach) informacji dla mieszkańców
- Turysta - Informacja – punkty Kolumny Info SOS przed ważnymi miejscami, zabytkami Leszna i okolic - odsłuchanie informacji o zabytkach, itd.
- **Zapobieganie wykluczeniu osób niepełnosprawnych** – kolumny INFO-SOS w miejscach kluczowych dla miasta: budynki użyteczności publicznej, szkoły, place zabaw, park 1000-lecia (ZOO), rynek.

BEZPIECZNE MIASTO

PROPOZYCJA REALIZACJI DOFINANSOWANIA Z PROGRAMU „DOSTĘPNY SAMORZĄD 2.0 ”

Przykłady dostępnych rozwiązań komunikacji interkomowej

Stacje z ekranem dotykowym

Stacje naścienne wideo

Stacje nabiurkowe

Stacje SOS

Stacje i oprogramowanie do zarządzania Control Desk

Stacje do pomieszczeń czystych

Kolumny SOS

Stacje przemysłowe

Urządzenia niestandardowe

JEDNA PLATFORMA

Apikacje

Moduły

Integracja z centralami telefonicznymi

Radiotelefony

Integracja systemów i urządzeń innych firm

Sieciowanie LAN/WAN

Wzmacniacze i głośniki IP

Referencja :Pomorska Kolej Metropolitalna (PKM)

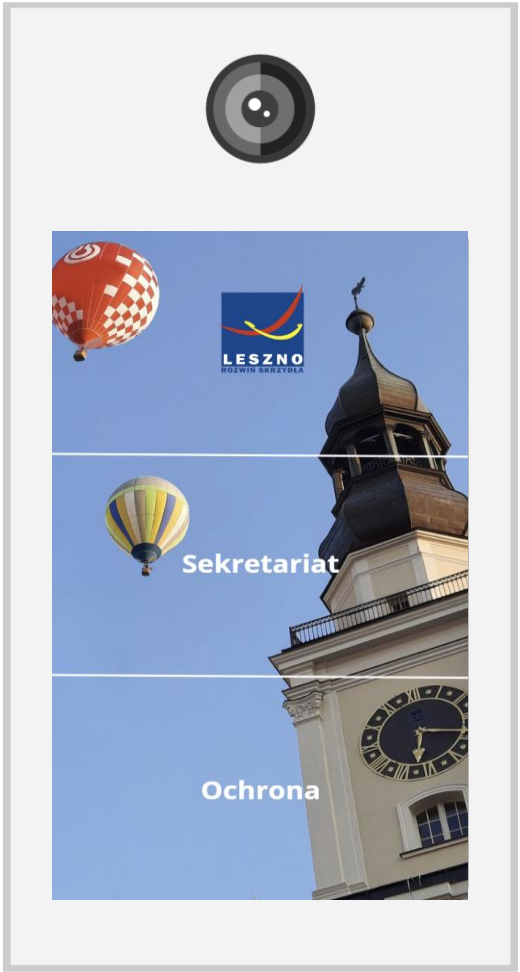
Interkomy – personalizacja widoków i treści

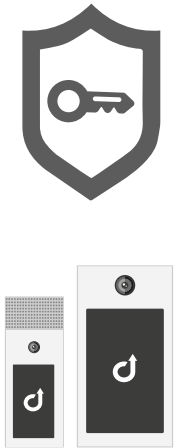
Informacje o promocjach, wydarzeniach

- Możliwość wyświetlenia spersonalizowanych informacji

Niestandardowy interfejs graficzny

- Interfejs użytkownika wykonany zgodnie ze specyfikacją klienta

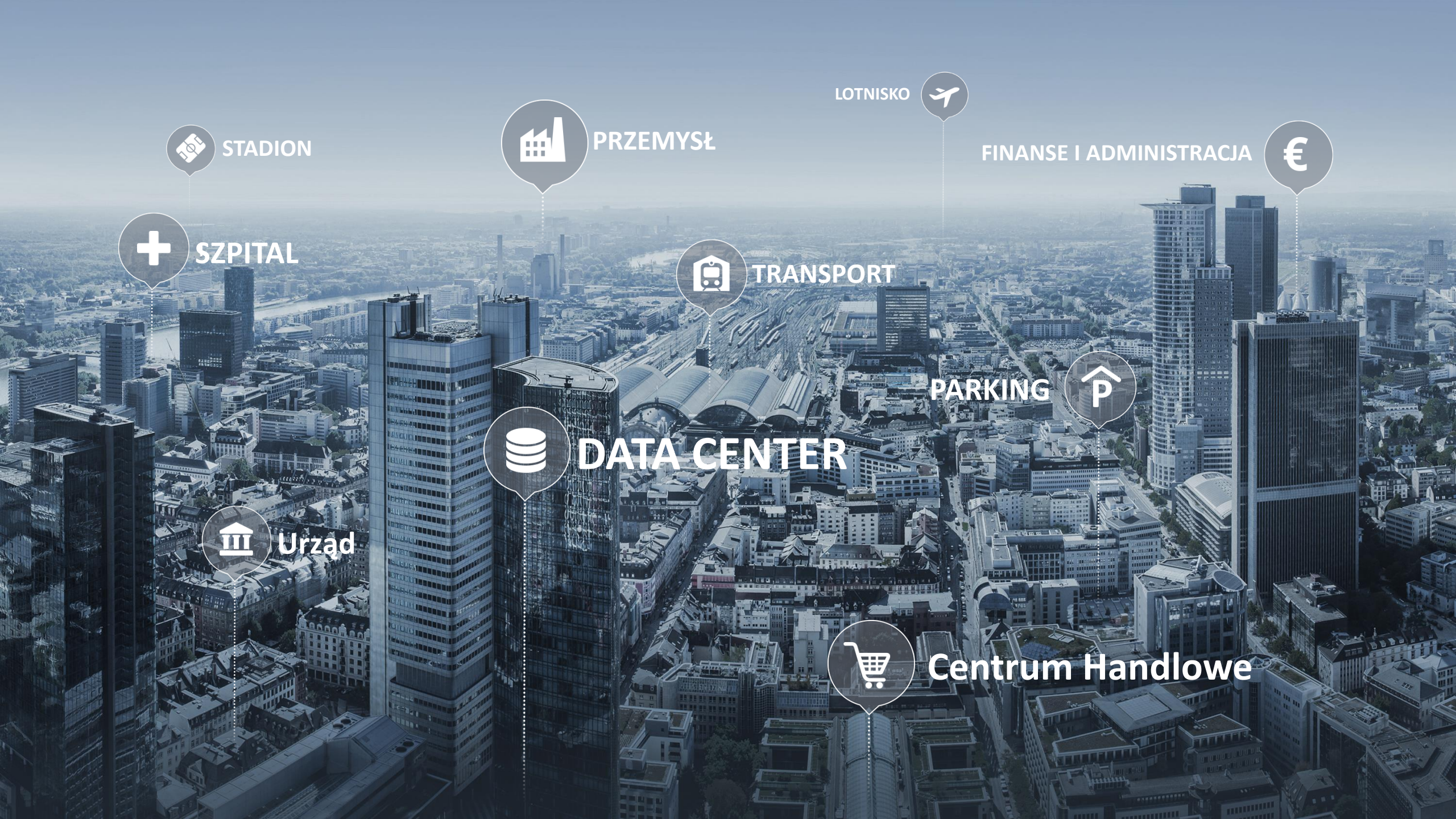




BEZPIECZNE MIASTO

Systemy integrujące

PSIM

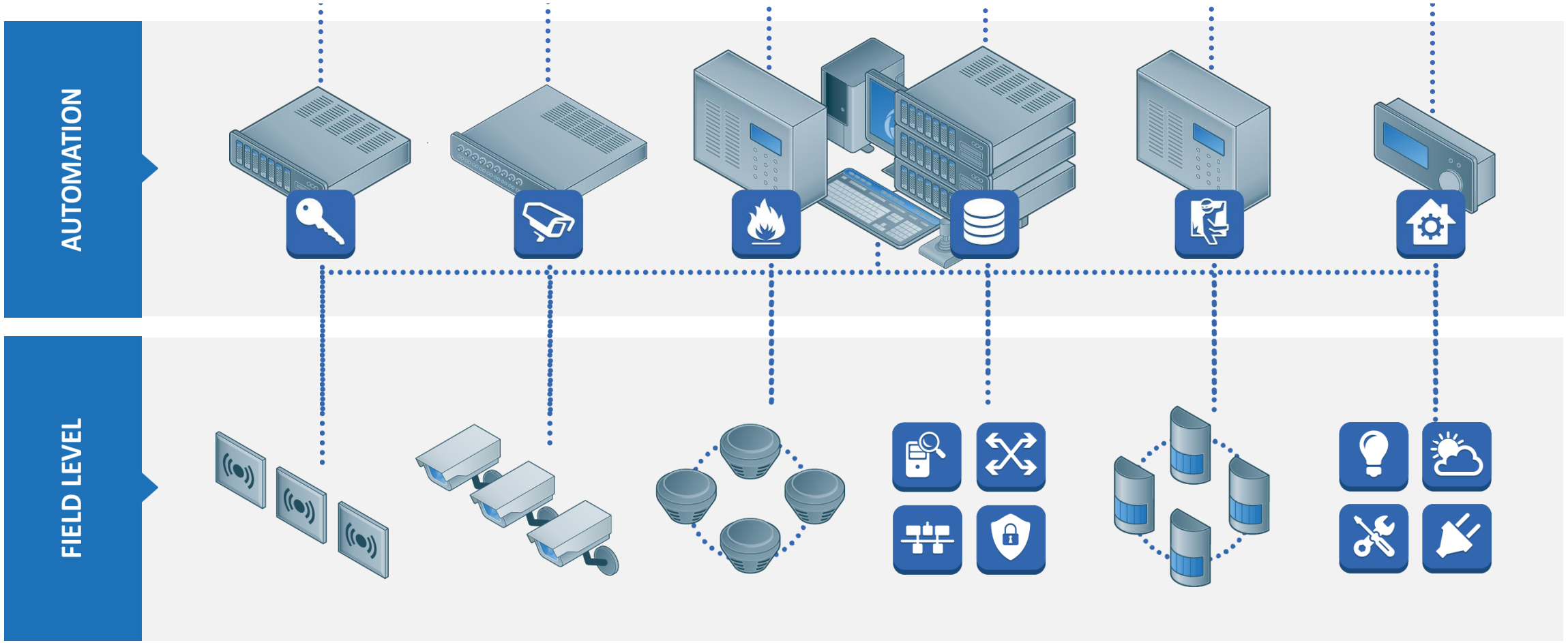

LOTNISKO
STADION
PRZEMYSŁ
FINANSE I ADMINISTRACJA
SZPITAL
TRANSPORT
PARKING
DATA CENTER
Urząd
Centrum Handlowe

Dlaczego PSIM?

PSIM to kompletny system oprogramowania, który posiada sześć kluczowych możliwości:

- **Zbieranie**: gromadzenie danych z dowolnej liczby różnych urządzeń lub systemów.
- **Analiza**: system analizuje i łączy dane, zdarzenia i alarmy w celu identyfikacji rzeczywistych sytuacji, określa ich priorytety.
- **Weryfikacja**: oprogramowanie PSIM przedstawia istotne informacje za pomocą GUI, aby umożliwić operatorowi weryfikację sytuacji.
- **Rozwiązanie**: „Scenariusze obsługi” (Standardowe procedury operacyjne (SOP)), instrukcje krok po kroku oparte na najlepszych praktykach i zasadach organizacji, a także narzędzia do rozwiązania sytuacji.
- **Raportowanie**: Wbudowane raporty z obsługi zdarzeń.
- **Ścieżka audytu**: Możliwość weryfikacja wprowadzanych zmian w systemie przez administratora, operatora.

PSIM

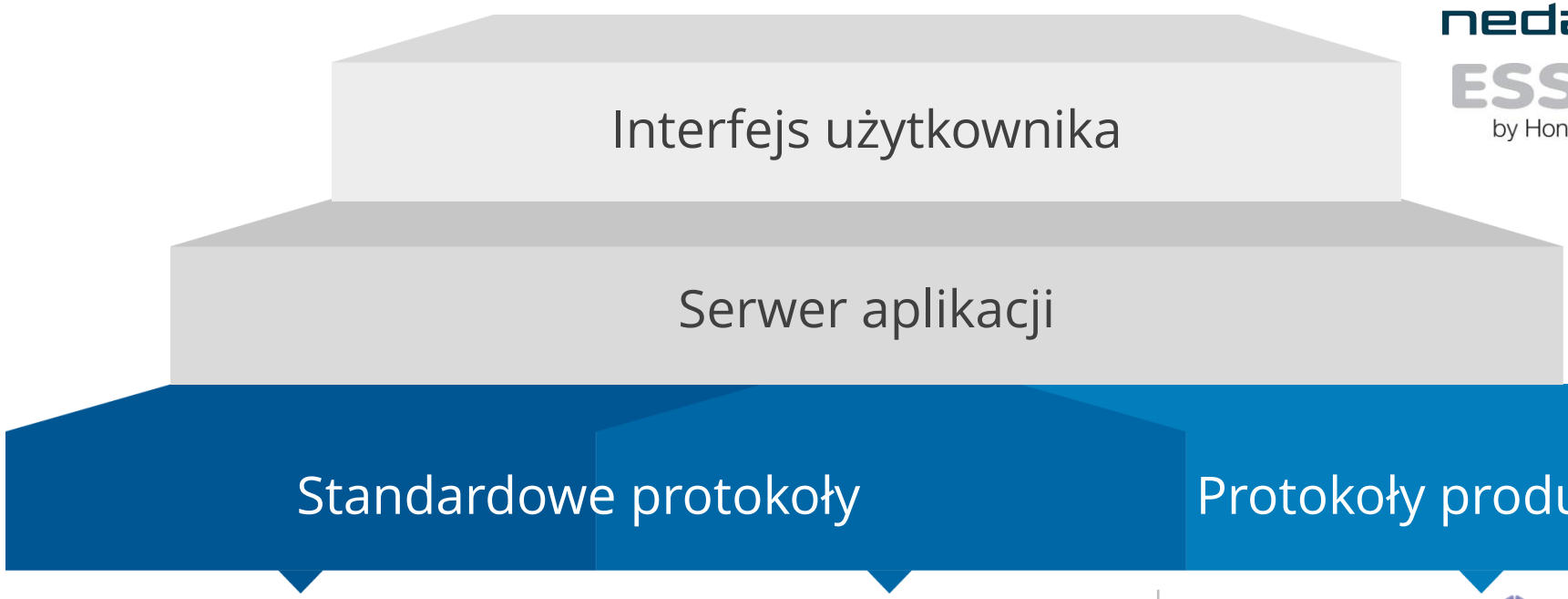


PSIM – najważniejsze cechy

- System niezależny od dostawców systemów integrowanych
- Ponad 500 interfejsów
- Jednolity interfejs użytkownika
- Plany sytuacyjne
- Raporty i oceny
- Bezpieczeństwo i niezawodność
- Ochrona inwestycji ze względu na skalowalność

BEZPIECZNE MIASTO

PSIM - interfejsy



PSIM – możliwości systemu WinGuard

Analiza danych
Statystki i wykresy KPI
Raporty

Bezpieczeństwo i ochrona przeciwpożarowa
Pożar, włamanie, wideo (alarmy analityczne), kontrola dostępu, ochrona obwodowa, drony itp.

Lokalizacja
Lokalizacja systemów (CAD)
Lokalizacja osób (GIS)

Wytyczne dla operatora
Plany sytuacyjne
Standardowe procedury operacyjne

3rd Party Integration
Zarządzanie incydentami
System Ticketowy

BMS i IoT
Ogrzewanie, chłodzenie, wentylacja, oświetlenie, jakość powietrza, temperatura itp.

Zdarzenia infrastruktury IT
Incydenty związane z bezpieczeństwem cybernetycznym
Integracja z centrum danych

Komunikacja
Połączenia głosowe z zespołem/stronami zewnętrznymi
Dystrybucja informacji poprzez sms, e-mail, wiadomość głosową,

WinGuard Aplikacja Moblina
Utrzymanie, Ochrona, itd.

BEZPIECZNE MIASTO

Dlaczego warto posiadać PSIM?

Rozwój systemów bezpieczeństwa

Systemy niezintegrowane lub o niskim stopniu integracji

- Znikoma wizualizacja
- Brak otwartości na inne systemy
- Brak możliwości implementacji procedur
- Brak zarządzania alarmami
- Brak wspólnego systemu raportowania

Systemy zintegrowane w ramach jednego producenta lub grupy producentów

- Wizualizacja Bmap
- Słaba otwartość na inne systemy
- Niska możliwość implementacji procedur
- Niska możliwość zarządzania alarmami
- Brak wspólnego systemu raportowania

Systemy zintegrowane na poziomie protokołów natywnych

- Wizualizacja wektorowa
- Pełna otwartość na inne systemy
- Wyjście poza systemy bezpieczeństwa
- Zarządzanie zdarzeniami poprzez procedury
- System zarządzania alarmami
- Pełen system raportowy

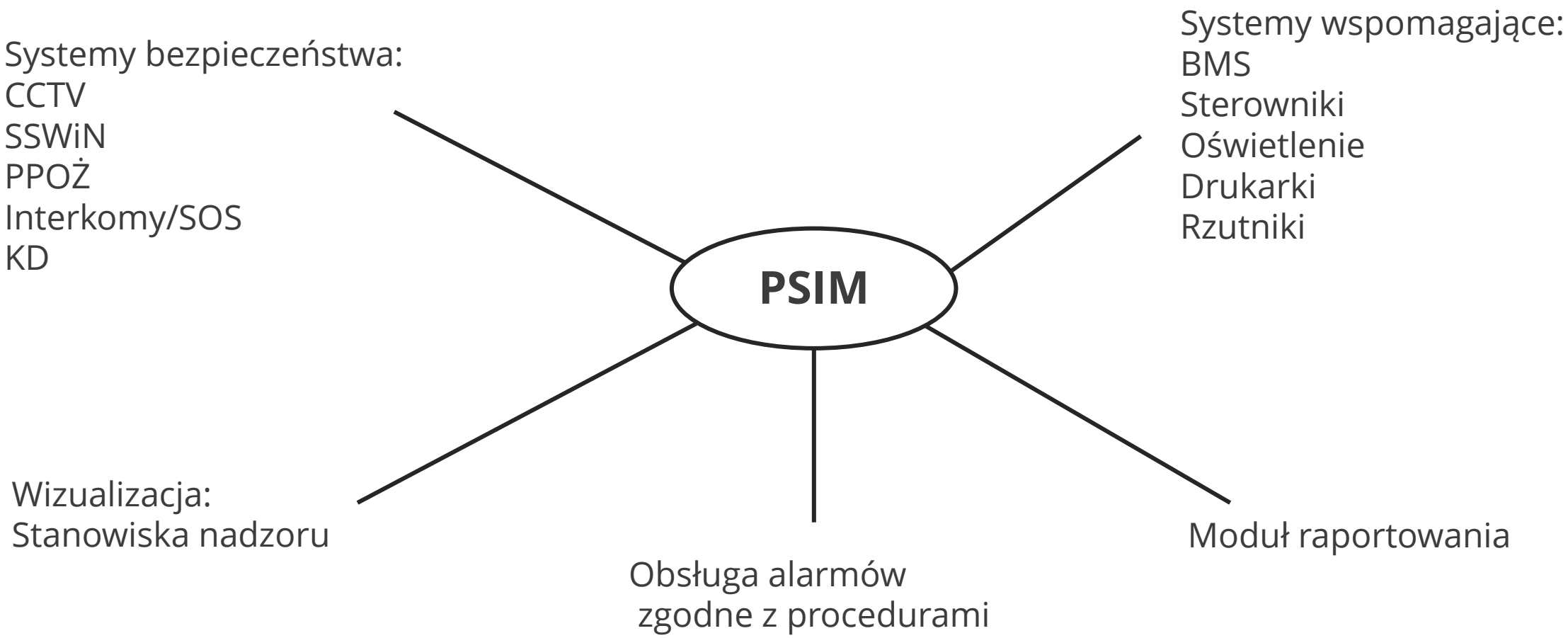
Systemy Wyspowe

Systemy SMS

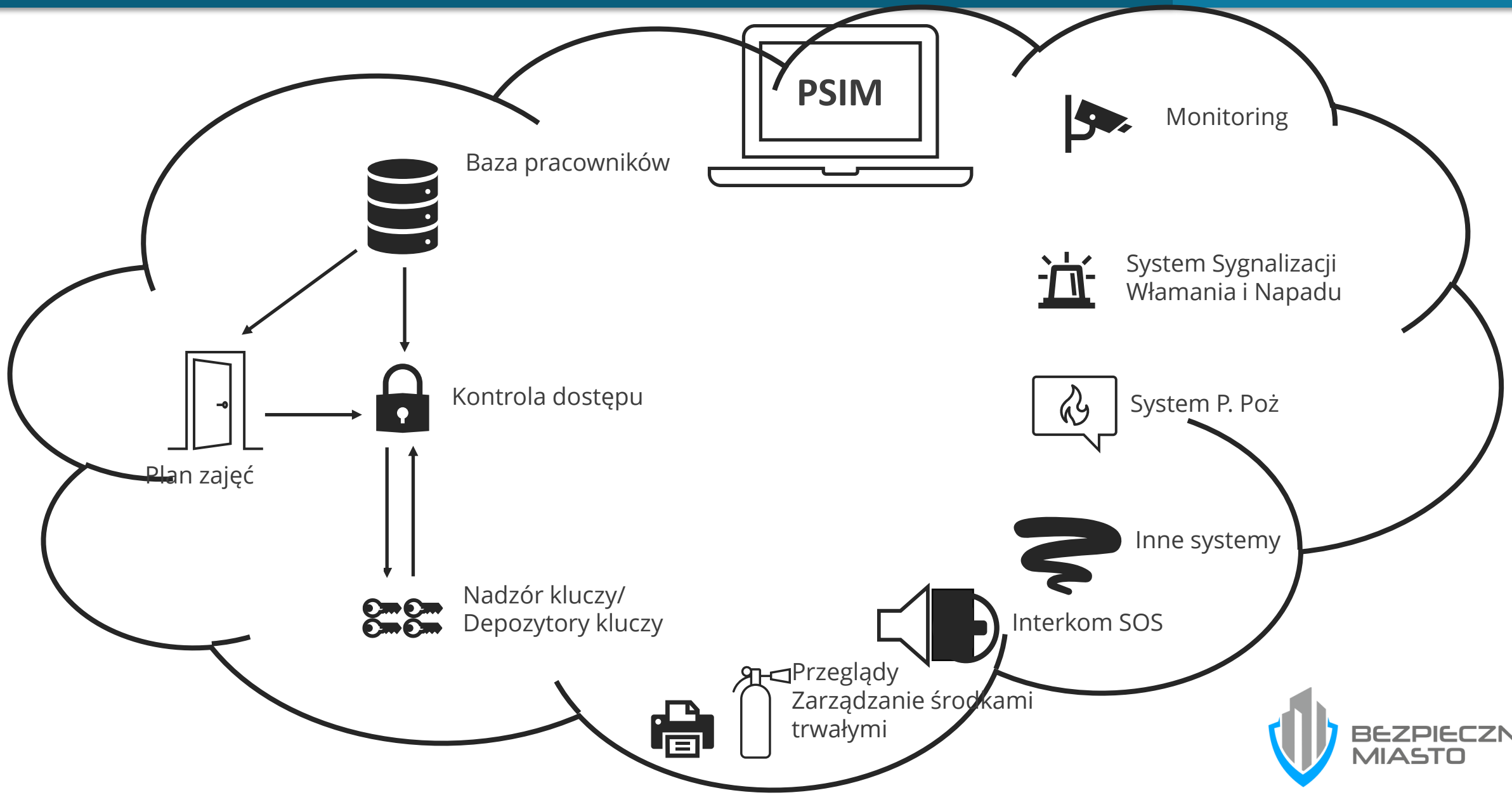
Systemy klasy PSIM

PSIM – System zarządzania bezpieczeństwem i informacją

PSIM –architektura systemu

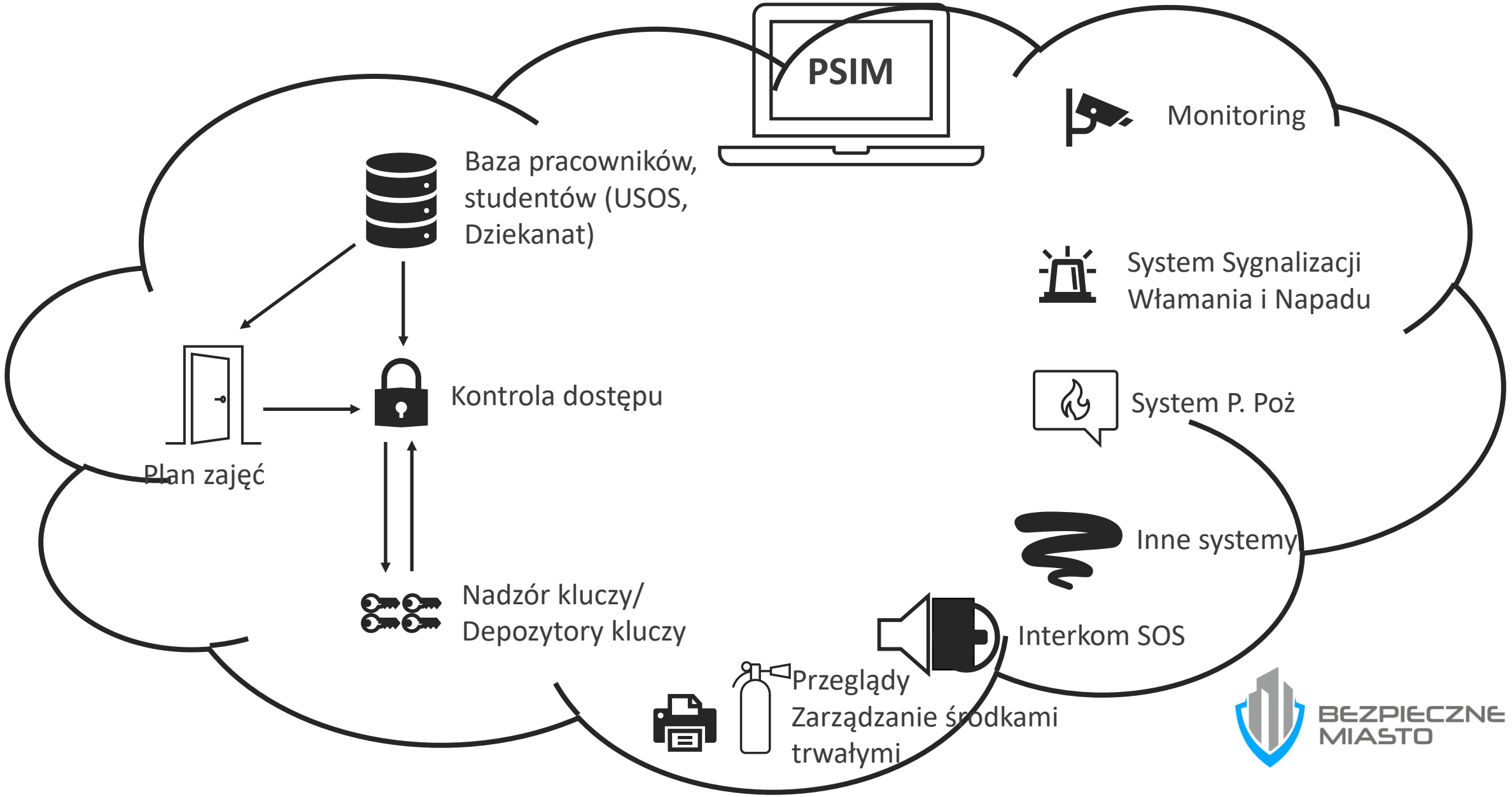


Wybrane systemy



PSIM – System zarządzania bezpieczeństwem i informacją – prezentacja aplikacji

Co może PSIM?


PSIM
Monitoring
Baza pracowników, studentów (USOS, Dziekanat)
System Sygnalizacji Włamania i Napadu
Kontrola dostępu
System P. Poż
Plan zajęć
Inne systemy
Nadzór kluczy/ Depozytory kluczy
Interkom SOS
Przeglądy
Zarządzanie środkami trwałymi

Jak to działa w praktyce ?
Stan obecny

BEZPIECZNE MIASTO

Koszty – ćwiczenie praktyczne

BEZPIECZNE MIASTO

Jak to może wyglądać?

BEZPIECZNE MIASTO

Gdzie oszczędność?
Jaki jest koszt?

BEZPIECZNE MIASTO

Gdzie oszczędność?
Jaki jest koszt?

Oszczędności:

- Personalne
- Energia
- Organizacyjne – efektywność

BEZPIECZNE MIASTO

Gdzie oszczędność?
Jaki jest koszt?

Nakłady:

- Zakup systemu - Wykorzystujemy istniejące systemy
- Budowa centrum nadzoru
- Nadzór informatyczny

BEZPIECZNE MIASTO

Gdzie oszczędność?
Jaki jest koszt?

Nakłady:

- Zakup systemu - Wykorzystujemy istniejące systemy
- Budowa centrum nadzoru
- Nadzór informatyczny

Oszczędności:

- Personalne
- Energia
- Organizacyjne – efektywność

BEZPIECZNE MIASTO

Podsumowanie

BEZPIECZNE MIASTO

Podsumowanie

- Personalne
- Energia
- Organizacyjne – efektywność

Jak zacząć - horyzont czasowy

Etap I

- Wizyty referencyjne
- Spotkania
- Określenie celu

Etap II

- PFU
- Zalążek systemu
- Inwestycja

Etap III

- Kontynuacja
- Współpraca

Dobre praktyki

Wymagania wobec wykonawców

Portfolio

Certyfikaty i kwalifikacje

Referencje

Potencjał firmy

Pakiet szkoleń

Wymagania wobec dostawców

Kraj pochodzenia

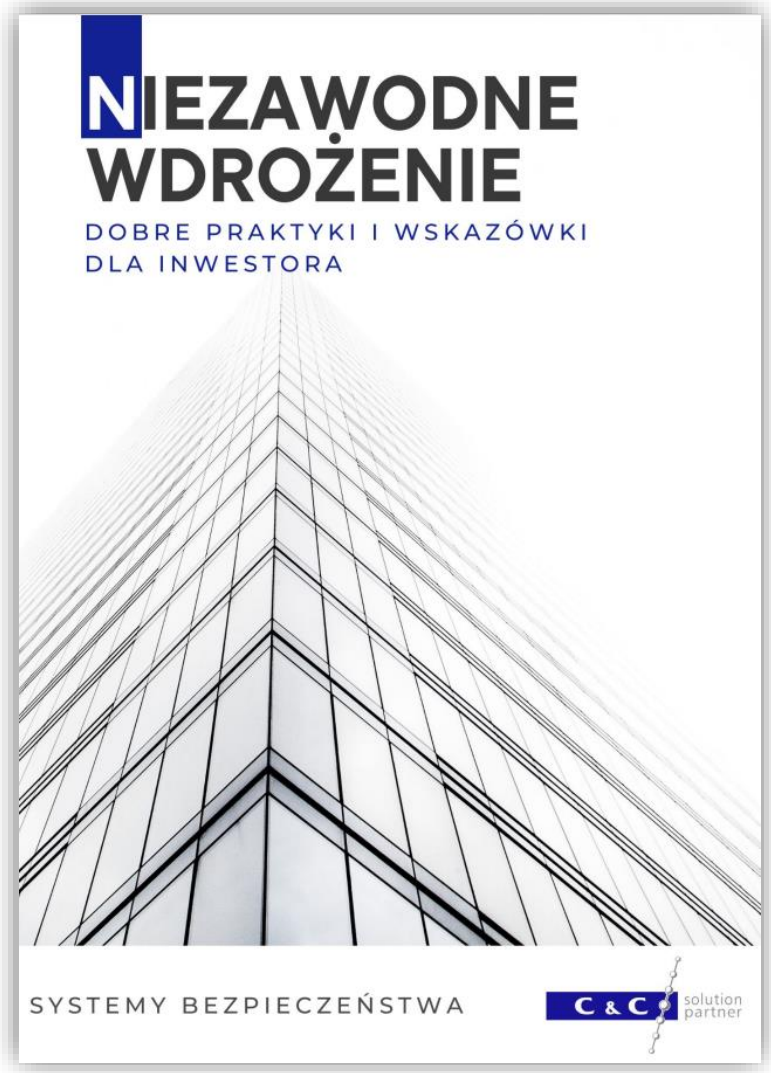
Certyfikaty i dopuszczenia

Referencje

Potencjał finansowy

Pakiet szkoleń

Jesteśmy do państwa dyspozycji

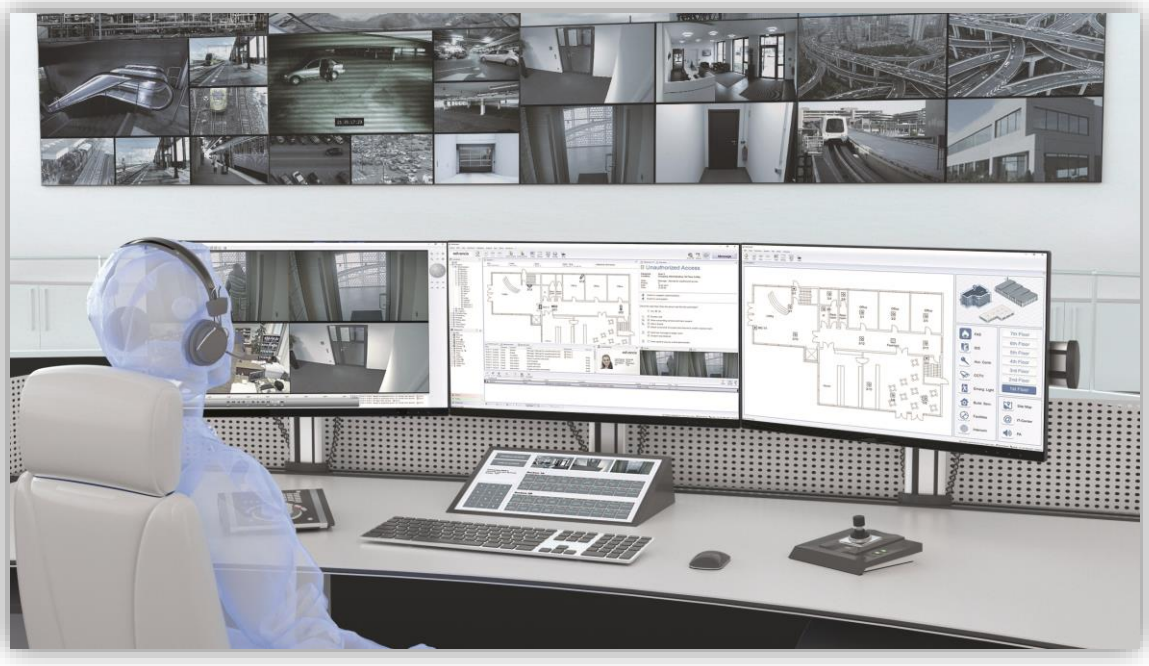


BEZPIECZNE MIASTO

Zintegrowany System Bezpieczeństwa klasy PSIM

Lokalizacja: **Centrum Zarządzania Kryzysowego / Centrum Monitoringu / Straż Miejska**

Realizacja: **Budowa nadrzędnego systemu do monitorowania i zarzadzania zdarzeniami dla JST**.



Korzyści:

- wzrost decyzyjności i odpowiedzialności gdyż wszystkie alarmy schodzą do jednego miejsca
- oszczędność kosztów
- szybka reakcja na zdarzenie - współpraca z mieszkańcami, którzy będą mieli możliwość wysyłania zgłoszeń o nadużyciach, awariach, niebezpiecznych sytuacjach, możliwościach skażeń środowiska, złe parkowanie, itd. – (możliwość wysyłania zdjęć itd.)

BEZPIECZNE MIASTO

Zintegrowany System Bezpieczeństwa klasy PSIM

Wdrożenie jednego systemu zarządzania bezpieczeństwem dla wszystkich jednostek samorządowych i gmin ościennych – dzisiaj te instytucje często mają swoje zasoby co powoduje, że system nie jest jednolity, nie współpracuje z innym.

Cel:

- niższe koszty wdrożenia i utrzymania systemu
- bezpieczne i sprawne udostępnianie nagrań stanowiących materiał dowodowy
- delegowanie obrazu do innych operatorów
- gwarancja ciągłości zapisu przez stosowanie redundancji
- skuteczna współpraca służb odpowiadających za bezpieczeństwo

PSIM Referencja

BEZPIECZNE MIASTO

Zachęcamy do wypełnienia ankiety

na stoisku C&C Partners

i wzięcia udziału w losowaniu nagród!

Dziękujemy za uwagę!

Martyna Kubiak
+ 48 665 551991
m.kubiak@ccpartners.pl