anzena.

BEZPIECZEŃSTWO IT/OT

Budujemy cyberbezpieczeństwo polskiego przemysłu

Anzena to zespół inżynierów, mających wieloletnie doświadczenie w pracy z zaawansowanymi technologiami u Klientów z branży przemysłowej.
Dzięki zdobytej wiedzy produktowej, gwarantujemy jakość usług na każdym etapie współpracy - od koncepcji i projektowania, aż po pełne wdrożenie rozwiązania, utrzymanie oraz wsparcie. Nasze portfolio zawiera najważniejsze linie produktowe uznanych liderów rynku.

Aktywnie budujemy świadomość w zakresie cyberbezpieczeństwa należąc do:

FAIRP Forum Automatyki i Robotyki Polskiej

silesia automotive & advanced manufacturing

PI PROFIBUS • PROFINET

AHK Deutsch-Polnische Industrie- und Handelskammer Polsko-Niemiecka Izba Przemysłowo-Handlowa

anzena.
BEZPIECZEŃSTWO IT/OT

Proces budowy bezpieczeństwa infrastruktury IT/OT

anzena.
BEZPIECZEŃSTWO IT/OT

Portfolio przemysłowe

Doradztwo i consulting

- W zakresie: NIS2, uKSC, IEC 62443, ISO 27001 i NIST 800-82.
- W zakresie projektowania, hardeningu i wdrażania software oraz hardware.
- Ocena i wsparcie w zakresie bieżącego monitorowania poziomu bezpieczeństwa infrastruktury.
- Plany DRP.
- Opracowanie i wdrażanie procedur i polityk bezpieczeństwa.

Audyty IT/OT

- Audyty zerowe oraz audyty całościowe.
- Ocena poziomu i polityk bezpieczeństwa (uKSC, NIS2, ISO 27001, IEC 62443).
- Identyfikacja obszarów o podwyższonym poziomie zagrożeń i analiza podatności CVE.
- Analiza topologii i ruchu sieciowego.
- Ocena dostępu do systemów.
- Bezpieczeństwo protokołów przemysłowych.
- Weryfikacja konfiguracji urządzeń.
- Testy penetracyjne.
- Assessment infrastruktury.
- Wykorzystanie pasywnego i aktywnego skanera sieci oraz podatności.
- Raporty i zalecenia poaudytowe.

anzena.
BEZPIECZEŃSTWO IT/OT

Portfolio przemysłowe

Ochrona danych

- DLP - ochrona przed wyciekiem danych.
- PAM – kontrola dostępu uprzywilejowanego.
- Backup Disaster Recovery.
- Antivirus/Antimalware.
- NAC – ochrona dostępu do sieci.

Bezpieczeństwo sieci

- Segmentacja sieci przemysłowych – skalowalnych i łatwo zarządzalnych, zgodnie z IEC 62443.
- Modernizacja infrastruktury IT/OT w oparciu o standardy i normy dot. cyberbezpieczeństwa.
- Hardening urządzeń sieciowych.
- Zwiększanie poziomu bezpieczeństwa krytycznej infrastruktury produkcyjnej (IEC 62443, ISO 27001, NIS2, uKSC).

anzena.
BEZPIECZEŃSTWO IT/OT

Portfolio przemysłowe

SOC, SIEM, SOAR

- SOC 24/7
- Consulting w zakresie funkcjonowania komórki SOC.
- Analiza potrzeb klienta i przełożenie zapotrzebowania na projekt wdrożeniowy.
- Dobór i wdrożenia rozwiązań software'owych.
- Parsowanie danych i logów.

Architektura bezpieczeństwa IT/OT

- Koncepcje budowy lub modernizacji cyberbezpiecznej infrastruktury.
- Proof of concept.
- Kompleksowe rozwiązania Data Center.
- Implementowanie software'u ukierunkowanego na zwiększenie bezpieczeństwa infrastruktury.

anzena.
BEZPIECZEŃSTWO IT/OT

Portfolio przemysłowe

Wirtualizacja

- Zastąpienie przestarzałych stacji operatorskich, paneli HMI technologią wirtualizacji.
- Uniezależnienie systemów i aplikacji od sprzętu fizycznego.
- Zapewnienie ciągłości działania krytycznych systemów, nawet w przypadku awarii wirtualizatora.
- Minimalizacja ryzyka przestojów produkcyjnych spowodowanych awariami sprzętu.

Systemy akwizycji danych

- Wdrożenia systemów do monitorowania infrastruktury sieciowo-serwerowej oraz systemów produkcyjnych.
- Przygotowanie funkcjonalnych dashboard'ów do monitorowania alertów, zdarzeń, przepływu danych.

anzena.
BEZPIECZEŃSTWO IT/OT

Portfolio przemysłowe

Infrastruktura IT/OT

- Modernizacja i hardening urządzeń serwerowni
  - identyfikacja i zabezpieczenie krytycznych segmentów sieci.
- Hosty serwerowe i stacje robocze, serwery NAS, macierze SAN
  - klasy Enterprise.
- UTM dedykowane dla przemysłu.
- IPS/IDS.
- Diody danych.
- Switche L2/L3, firewalle, cienkie klienty, routery.
- Sieci bezprzewodowe oparte o kontroler.
- Zasilacze UPS.
- Klimatyzacja precyzyjna.

Przemysłowe sieci bezprzewodowe

- Projektowanie sieci bezprzewodowych WIFI oraz GSM z wykorzystaniem technologii: WIFI6, LTE/5G, iWLAN.
- Konsultacje, testy.
- Audyty przedwdrożeniowe.
- Dobór rozwiązań sprzętowych uwzględniających potrzeby Klienta.
- Wdrożenie i konfiguracja sieci bezprzewodowych.

anzena.
BEZPIECZEŃSTWO IT/OT

Portfolio przemysłowe

Szkolenia

- Stacjonarne/on-line.
- Zakres dobierany pod potrzeby Klienta.
- Webinary techniczne budujące kompetencje w zakresie cyberbezpieczeństwa IT/OT.
- **Szkolenia dla administratorów:** obsługa oferowanych i wdrożonych przez Anzenę rozwiązań, procedury postępowania w przypadku incydentów cyberbezpieczeństwa, dobre praktyki projektowania i rozwijania infrastruktur sieciowych.
- **Szkolenia pracowników biurowych:** dobre praktyki pracy w zakresie ISO 27001 oraz RODO, realne zagrożenia (phishing + socjotechniki), obsługa rozwiązań zapewniających bezpieczeństwo pracy (Manager haseł, VPN).

Wdrożenia i usługi inżynierskie

- Projektowanie, hardening i wdrażanie software i hardware, w tym wizje lokalne i nadzór nad inwestycjami.
- Wdrożenia infrastruktury, hardware i software, konfiguracja switchy, routerów, macierzy, dysków, klastrów.
- Wsparcie powdrożeniowe.

anzena.
BEZPIECZEŃSTWO IT/OT

Nasze realizacje: Przedsiębiorstwo z branży energetycznej

PROJEKT:

Kompleksowa modernizacja i hardening infrastruktury IT/OT w przedsiębiorstwie świadczącym usługi na infrastrukturze krytycznej.

CEL:

Dostosowanie infrastruktury przemysłowej przedsiębiorstwa do wymogów ustawy o KSC, a w szczególności zaprojektowanie nowej sieci szkieletowej do wymiany danych pomiędzy segmentami poszczególnych obszarów, segmentacja sieci, migracja systemów SCADA oraz zapewnienie bezpiecznej transmisji danych pomiędzy sterownikami PLC, serwerami oraz stacjami operatorskimi.

WYZWANIA PROJEKTOWE: Zachowanie ciągłości pracy systemów SCADA oraz sterowania, w przedsiębiorstwie świadczącym usługi kluczowe na infrastrukturze krytycznej.

Zbudowanie nowej infrastruktury sieciowej w obrębie starej, a następnie przekazanie funkcji starej w obręb nowej infrastruktury – bez możliwości przeprowadzenia przestoju produkcyjnego.

Braki dokumentacyjne.

anzena.
BEZPIECZEŃSTWO IT/OT

Nasze realizacje: Przedsiębiorstwo z branży energetycznej

TECHNICZNY OPIS DZIAŁAŃ:

Zbudowanie środowiska wirtualizacyjnego w oparciu o klaster HA, z wykorzystaniem technologii VMware.

Zbudowanie klastra macierzy produkcyjnej dla środowiska wirtualizacyjnego.

Zbudowanie sieci core'owej w oparciu o STACK switchy Netgear oraz klaster UTMów FortiGate.

Hardening urządzeń sieciowych i serwerowych.

Projekt i modernizacja infrastruktury przemysłowej w oparciu o switche Scalance, Moxa z wykorzystaniem technologii turbo coupling.

Projekt i konfiguracja systemu do backupu.

Projekt i konfiguracja rozwiązania klasy PAM do autentykacji i weryfikacji działań użytkowników w obszarze systemów OT.

Projekt i implementacja rozwiązania klasy IDS.

Wdrożenie środowiska FortiAnalyzer i FortiEMS do sprawnego audytowania ruchu sieciowego oraz zabezpieczenia endpointów.

KORZYŚCI DLA KLIENTA:

Sprostanie wymaganiom narzuconym przez ustawę o KSC.

Eliminacja wcześniejszych błędów koncepcyjnych dot. infrastuktury. Aktualizacja dokumentacji technicznej i proceduralnej.

Zwiększenie poziomu cyberbezpieczeństwa przedsiębiorstwa, implementacja polityk, oprogramowania i sprzętu dedykowanego wykrywaniu podatności i anomalii, co wymiernie przekłada się na wykrywanie zagrożeń we wczesnym stadium.

Zapewnienie klientowi magazynu kopii bezpieczeństwa systemów infrastruktury krytycznej i możliwości szybkiego powrotu do pracy w przypadku awarii krytycznej.

Większe poczucie bezpieczeństwa i wzrost świadomości.

anzena.
BEZPIECZEŃSTWO IT/OT

Nasze realizacje: Przedsiębiorstwo z branży spożywczej

PROJEKT: Wirtualizacja stacji operatorskich analizatora spożywczego.

WYZWANIA PROJEKTOWE: Wąskie okno czasowe na realizację zadania, z uwagi na konieczność zachowania ciągłości produkcji.

CEL PROJEKTU: Utworzenie środowiska wirtualizacyjnego pozwalającego na zastąpienie fizycznych stacji operatorskich, wykorzystujących system Windows XP SP2 i SP3. Wytunelowanie do wirtualnego środowiska fizycznego interfejsu USB, do którego podłączony jest analizator spożywczy.

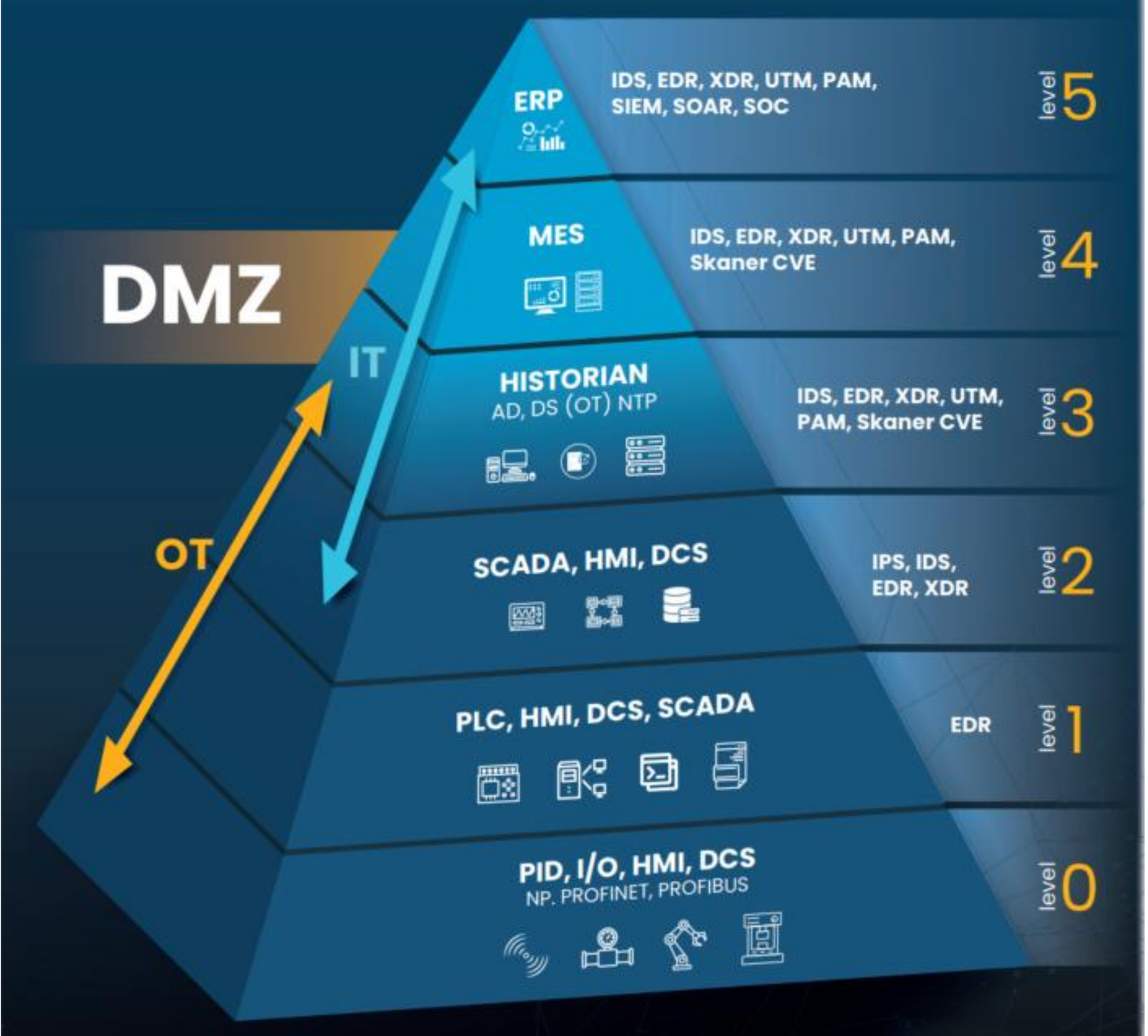
TECHNICZNY OPIS DZIAŁAŃ: Utworzenie środowiska wirtualnego w oparciu o dwa serwery fizyczne z wirtualizatorem Hyper-V, z przestrzenią dyskową serwera NAS jako storage dla maszyn wirtualnych. Wirtualizacja stacji operatorskich. Dostosowanie systemów Windows XP do pracy w środowisku wirtualnym. Konfiguracja cienkich klientów jako terminali RDP do wirtualnych systemów. Wykorzystanie technologii passthru do tunelowania interfejsu fizycznego USB, cienkiego klienta do wirtualizatora Hyper-V.

KORZYŚCI DLA KLIENTA:

Elastyczne środowisko dzięki zastosowaniu maszyn wirtualnych.

Ta sama funkcjonalność maszyn przy jednoczesnym **zabezpieczeniu się przed starzeniem sprzętu.** Rezygnacja z zakupu nowych, drogich maszyn fizycznych, **oszczędność** dla przedsiębiorstwa.

anzena.
BEZPIECZEŃSTWO IT/OT



Portfolio produktów

Rozwiązania klasy SIEM

LogRhythm

FortiSIEM

PAM

senhasegura

WALLIX CYBERSECURITY SIMPLIFIED

DLP

Acronis

safetica

AV, EDR, XDR

ESET

Trellix

txOne networks

Skanery podatności

NOZOMI NETWORKS

nessus

IDS

tenable

NOZOMI NETWORKS

IPS

Trellix

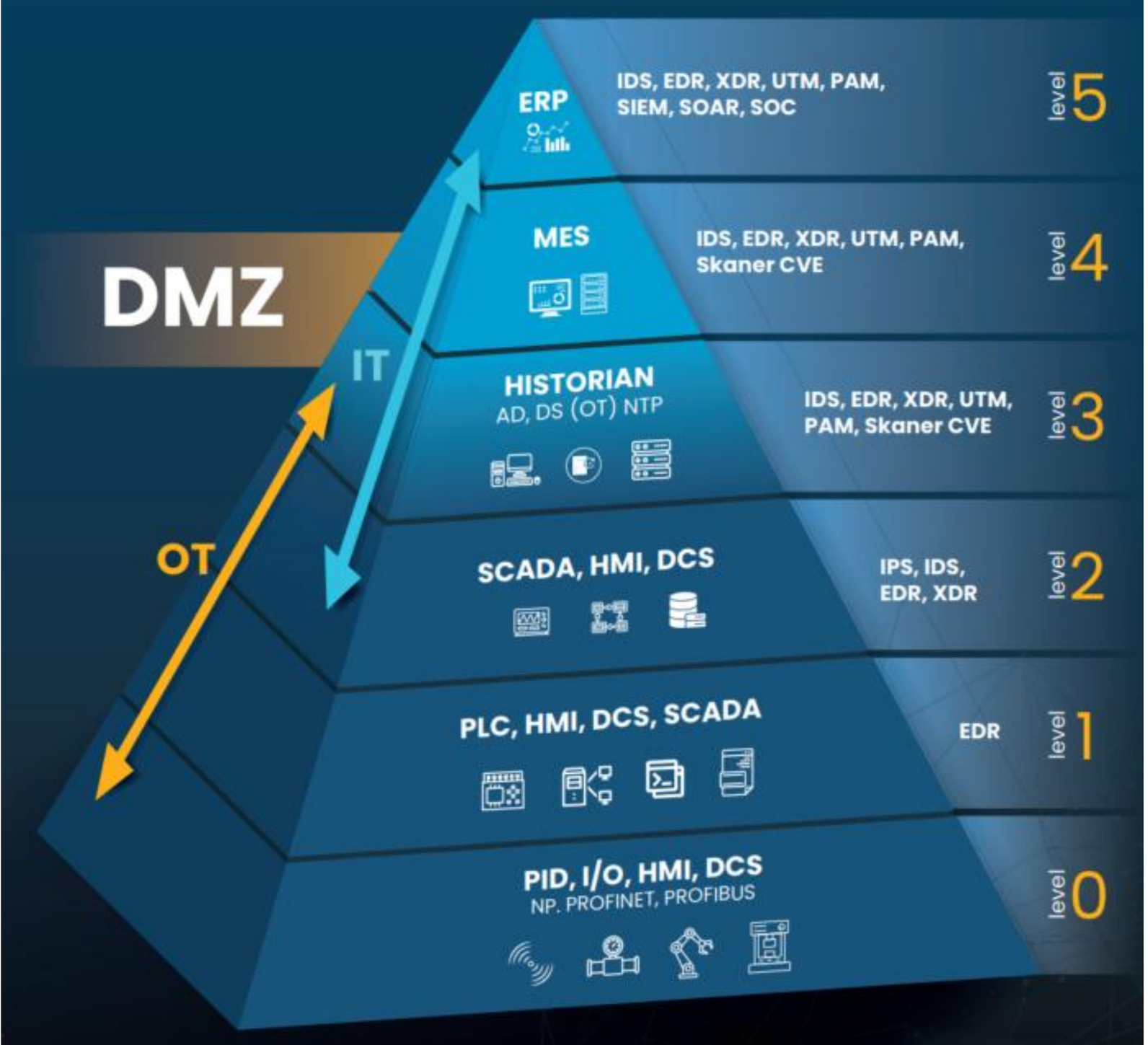
txOne networks

NAC

NACVIEW

OPSWAT.

FortiNAC



Portfolio produktów

Backup

Acronis · arcserve ShadowProtect · SPX · VEEAM

Wirtualizacja

PROXMOX · vmware

Network L3/UTM

FORTINET · STORMSHIELD · MOXA

Network L2

NETGEAR · JUNIPER NETWORKS · aruba · CISCO · MOXA

Sieci bezprzewodowe

TELTONIKA · NETGEAR INSIGHT · CISCO Meraki

Serwery i stacje robocze

DELL · elmatic · Hewlett Packard Enterprise

Storage

DELL · IBM · Hewlett Packard Enterprise

anzena.

BEZPIECZEŃSTWO IT/OT

Dziękujemy za uwagę i zapraszamy do kontaktu

www.anzena.pl

e-mail: kontakt@anzena.pl, tel. +48 32 420 90 00

Katowice, ul. Pszczyńska 15, woj. śląskie