



FORTINET Security Day

Digitální transformace jednoho města aneb Smart City a kybernetická bezpečnost

Mgr. Jan Hofman, Metropolnet a.s., člen představenstva
Petr Katzer, Fortinet

5. října 2026
O2 Universum, Praha

Metropolnet a.s. – krátké představení

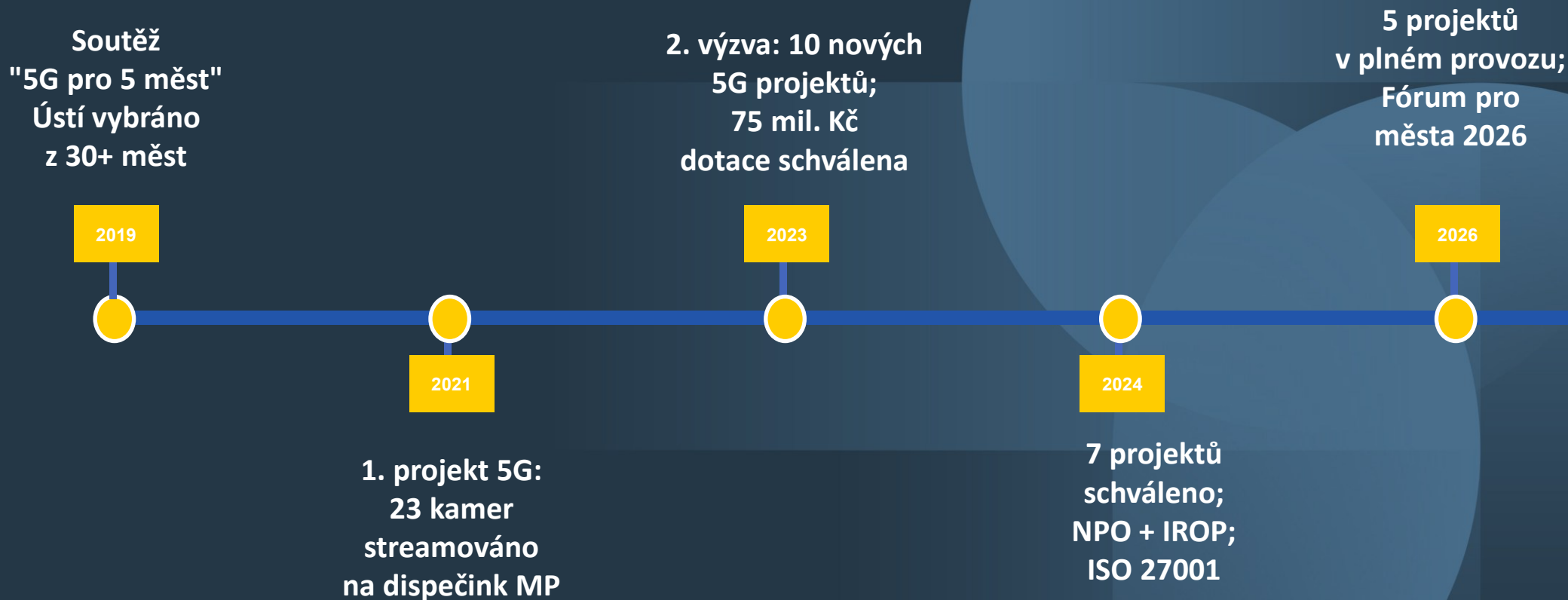


- 90 000 obyvatel, Ústecký kraj, strategická poloha: soutok Labe a Bíliny
- Vybrán v soutěži "5G pro 5 měst" v roce 2019
- Příjemce dotací EU: NPO, IROP, URBACT
- Pořadatel Fóra pro města 2026 – sdílení dobré praxe
- 100% vlastněná ICT společnost města
- Provozovatel městské privátní optické sítě
- Systémový integrátor 5G smart city projektů
- Certifikace ISO 27001:2022 (kyberbezpečnost)
- Technický dozor, projektový manažer a správce dotace

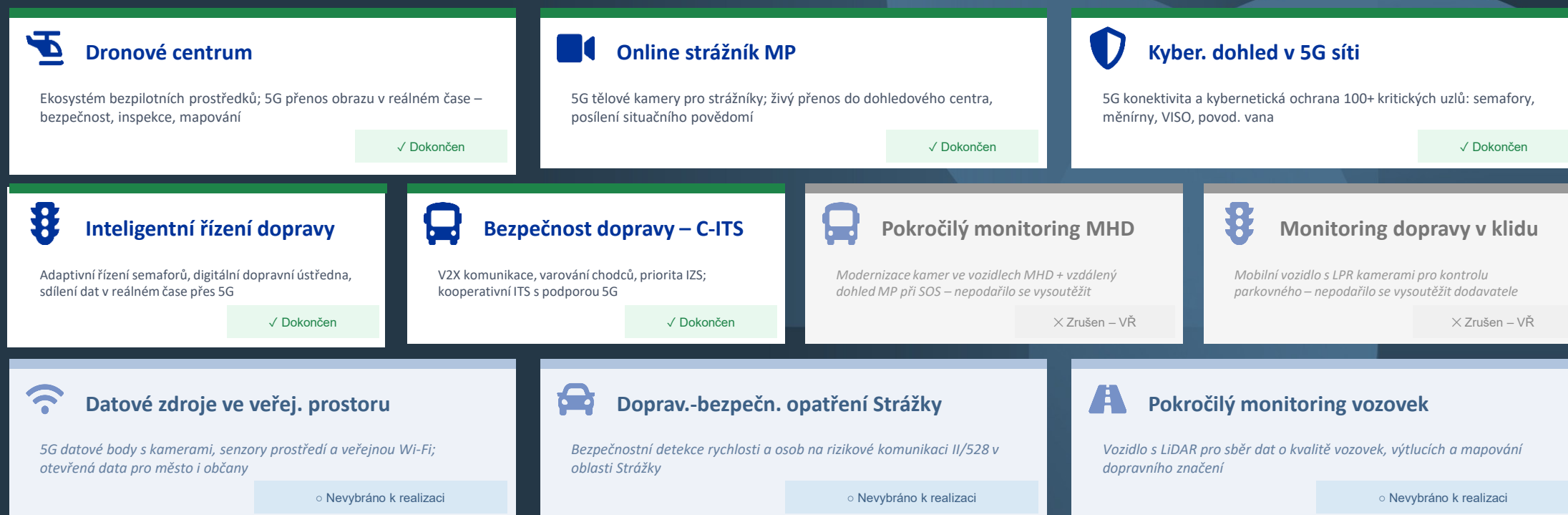


Naše cesta k 5G a kybernetickému dohledu

od pilotního města k vzoru dobré praxe v 5G



Portfolio 5G projektů



Dokončen (5×) Zrušen – VŘ (2×) Nevybráno k realizaci (3×)



Projekt kybernetického dohledu a zabezpečení datových bodů v 5G síti

Parametry projektu

Žadatel: Statutární město Ústí nad Labem

Program: Národní plán obnovy – 2. výzva 5G

Příprava a realizace: říjen 2023 – prosinec 2025

Rozpočet: 7 537 000 Kč bez DPH

Registrační číslo projektu: CZ.31.6.0/0.0/0.0/23_087/0008729

Partneři realizace: Metropolnet, a.s., Dopravní podnik města Ústí nad Labem (DPMÚL)

5G Ústí nad Labem

Veřejná 5G síť operátora, napojená privátním APN do interní sítě města, prodlužuje, nebo spíše **“virtualizuje”** městskou optiku vzduchem – umožňuje připojit prakticky jakýkoliv bod on-demand, bez pokládky nové optiky i bez vlastní 5G infrastruktury.

Inovace: metropolitní síť „virtualizovaná vzduchem“ nad operátorskou 5G – flexibilní připojení on-demand, nákladově efektivní a přitom zabezpečené na úrovni odpovídající optické páteři.

Ucelené řešení

Růst objemu dat v metropolitní síti zvýšil i její zranitelnost. Ovládání měření běželo na zastaralém rádiu, chyběl monitoring a vzdálená místa se nesledovala vůbec.

Inovace: jasně pojmenované slabiny se staly základem pro ucelené řešení, ne jen pro dílčí záplaty.

Co je kyber pro občany ?

Kybernetická bezpečnost se promítá do každodenního života – spolehlivější MHD, ochrana osobních údajů obyvatel a pružnější úřad.

Inovace: abstraktní téma převedené do konkrétních a viditelných přínosů pro občany.

Projekt zvýšení kybernetické bezpečnosti statutárního města Ústí nad Labem

Parametry projektu

Žadatel: Statutární město Ústí nad Labem

Program: Národní plán obnovy – Výzva č. 41, Kyber. bezpečnost – obce

Dotace: 49 700 000 Kč bez DPH

Registrační číslo projektu: CZ.31.2.0/0.0/0.0/23_093/000

Výstup

Výstup: Nezávislý audit kyberbezpečnosti · Certifikovaný soulad se ZoKB / NIS2 · Sdílené služby pro PO města

Pokročilá síťová segmentace

Zero-trust architektura; oddělení kritických systémů od obecné IT sítě

Monitoring bezpečnostních událostí

Sběr logů a detekce anomálií 24/7 v celé IT infrastruktuře města

Ochrana koncových bodů

Nasazení na všech zařízeních

Sekundární datové centrum

Redundantní cluster pro kontinuitu provozu a obnovu po havárii

Procesní rámec NIS2

Bezpečnostní politiky, řízení přístupů, zvládání incidentů – soulad s NIS2

Souvislost a návaznost s 5G projekty

Kyberbezpečnost přenosové sítě (5G), centrální monitoring

Kybernetická bezpečnost - struktura

★ Veškerá opatření jsou realizována v souladu s EU směrnicí NIS2 (2022/2555) · Zákon č. 264/2025 Sb. ★



Bezpečnostní politika

Cíle, zásady a odpovědnosti v kybernetické bezpečnosti



Řízení aktiv

Inventarizace a klasifikace HW, SW a datových aktiv



Řízení přístupů

MFA, správa privilegovaných účtů, princip min. oprávnění



Bezpečnost lid. zdrojů

Školení, проверки, smluvní odpovědnosti



Provozní bezpečnost

Monitoring, antivirus, zálohy, správa zranitelností



Fyzická bezpečnost

Serverovny, řízený přístup, kamerové systémy



Bezpečnost komunikací

Síťová segmentace, NGFW, šifrování, ochrana perimetru



Bezpečnost dodavatelů

Hodnocení supply chain, smluvní záruky bezpečnosti



Zvládání incidentů

Detekce, klasifikace, hlášení NÚKIB do 24 h



Kontinuita činností

DRP, BCP, testování zálohovacích scénářů



Audit kybernetické bezpečnosti

Nezávislý audit · plný soulad ZoKB · realizuje Metropolnet · 06/2026



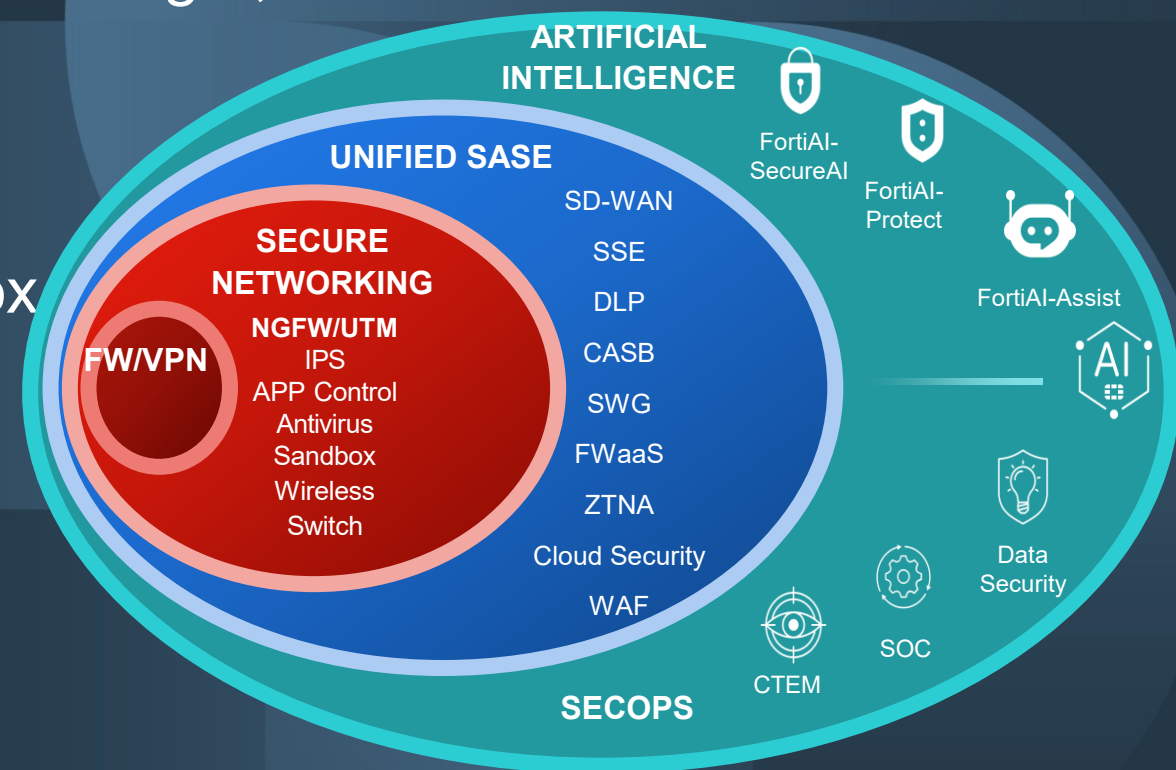
Technologie v projektech

5G sítě

- FortiGate, FortiNDR, FortiAnalyzer a FortiManager,

Kybernetické zabezpečení města

- NGFW - FortiGate (v režimu HA), Sandbox
- FortiAnalyzer a FortiManager,
- FortiEDR,
- FortiDeceptor,
- FortiZTNA - VPN + FortiAuthenticator,
- FortiPAM



Technologický ekosystém města – vše naráz

Chytré a propojené město

- › Řídicí platforma a dohledové centrum
- › Dopravní ústředna a řízení křižovatek
- › C-ITS — kooperativní doprava
- › Metropolitní optická síť (MOS)
- › Data, analytika a reporting

Bezpečnost občanů

- ★ **Dronové centrum**
- › Městský kamerový systém (MKDS)
- › Online strážník MP (5G)
- › Operační středisko Na Nivách
- › Integrace HZS, IZS, MP · varování

Jednotné městské ICT

- › Kybernetická bezpečnost (ZoKB)
- › Neveřejná síť veřejné správy (CMS2)
- › Centrální ICT a datové centrum
- › Rozvoj informačních systémů
- › Regulace: NIS2, ISO 27001, GDPR

Technologické kompetenční centrum – Metropolnet, a.s.

2022 – 2026: 9+ investičních 5G projektů z NPO

2026 – 2030: 3 rozvojové cíle města



Q&A



The image features the Fortinet logo centered on a light gray background. The logo consists of the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is replaced by a red square icon with a white grid pattern. Surrounding the logo are several decorative geometric elements: a solid red horizontal bar in the top left; a red horizontal bar to the right of the logo; a red horizontal bar in the bottom left; a gray square with a white grid pattern in the bottom right; and various gray squares and semi-circles of different sizes scattered across the background.

FORTINET