exeon

Use Case: Public

Cyber Resilience in Municipal Infrastructure

Insights for **Public Sector Security**

Modern municipalities are increasingly dependent on secure digital operations to maintain citizen services. From energy utilities to transportation and leisure facilities, the convergence of IT and OT has created new vulnerabilities. With limited IT resources and growing compliance demands from regulations like NIS2 and GDPR, city administrations must adopt a passive, scalable, and AI-driven approach to threat detection and response.

Case Overview

A mid-sized German city with 250,000 residents and 1,300 public employees manages 25+ municipal facilities across 15 districts. Their hybrid infrastructure spans over 12,000 IT and OT devices—supporting services including water, heating, waste, public transit, and administrative systems. The city faced an increasing risk of ransomware, APTs, shadow IT, and command-and-control (C2) communication, all within a fragmented network structure.

Want a closer look? Discover how it works in our **on-demand demos**.

Core Challenges

Challenge	Strategic Impact
Hybrid IT/OT Infrastructure	Requires passive monitoring that won't disrupt critical services.
Legacy Systems & Proprietary Apps	Demands agentless visibility and adaptive analytics.
Regulatory Compliance (NIS2, KRITIS, GDPR)	Needs structured incident response and reporting.
Shadow IT & Remote Access	Calls for anomaly detection and C2 identification.
Limited IT Security Staffing	Necessitates automation and high signal-to-noise ratio.

Adaptive Monitoring Framework

The municipality deployed Exeon's metadata-driven NDR platform to unify visibility across IT, OT, and cloud environments. Without requiring packet capture or agents, Exeon sensors provided full traffic telemetry—NetFlow, DNS, and encrypted stream metadata—across all segments. Integration with firewalls, SIEM, EDR, and ZTNA enabled real-time threat correlation and compliance automation.

Key elements

- Passive, agentless deployment across all segments
- Machine learning baselines for devices, users, and OT systems
- Detection of lateral movement, C2 channels, and unauthorized data access
- Forensic logging and reporting tailored to NIS2 and KRITIS

Outcomes & Metrics

Within six months, the city achieved:

60%
faster detection time across critical services

Full compliance with NIS2 and KRITIS mandates

70%
fewer false positives through behavioral tuning

No disruption to live operations during rollout

Recommendations for Public Sector Leaders

Deploy agentless NDR for unified visibility across IT, OT, and cloud.

Use **machine learning** to model normal behavior and surface hidden threats.

Integrate **automated compliance workflows** into your SOC stack.

Conclusion

Gartner Peer Insights™

Learn more

Public sector organizations can no longer afford to rely on reactive security. By adopting Exeon's AI-powered, passive monitoring approach, cities gain real-time detection, historical forensics, and regulatory readiness—all while protecting essential services and citizen trust.