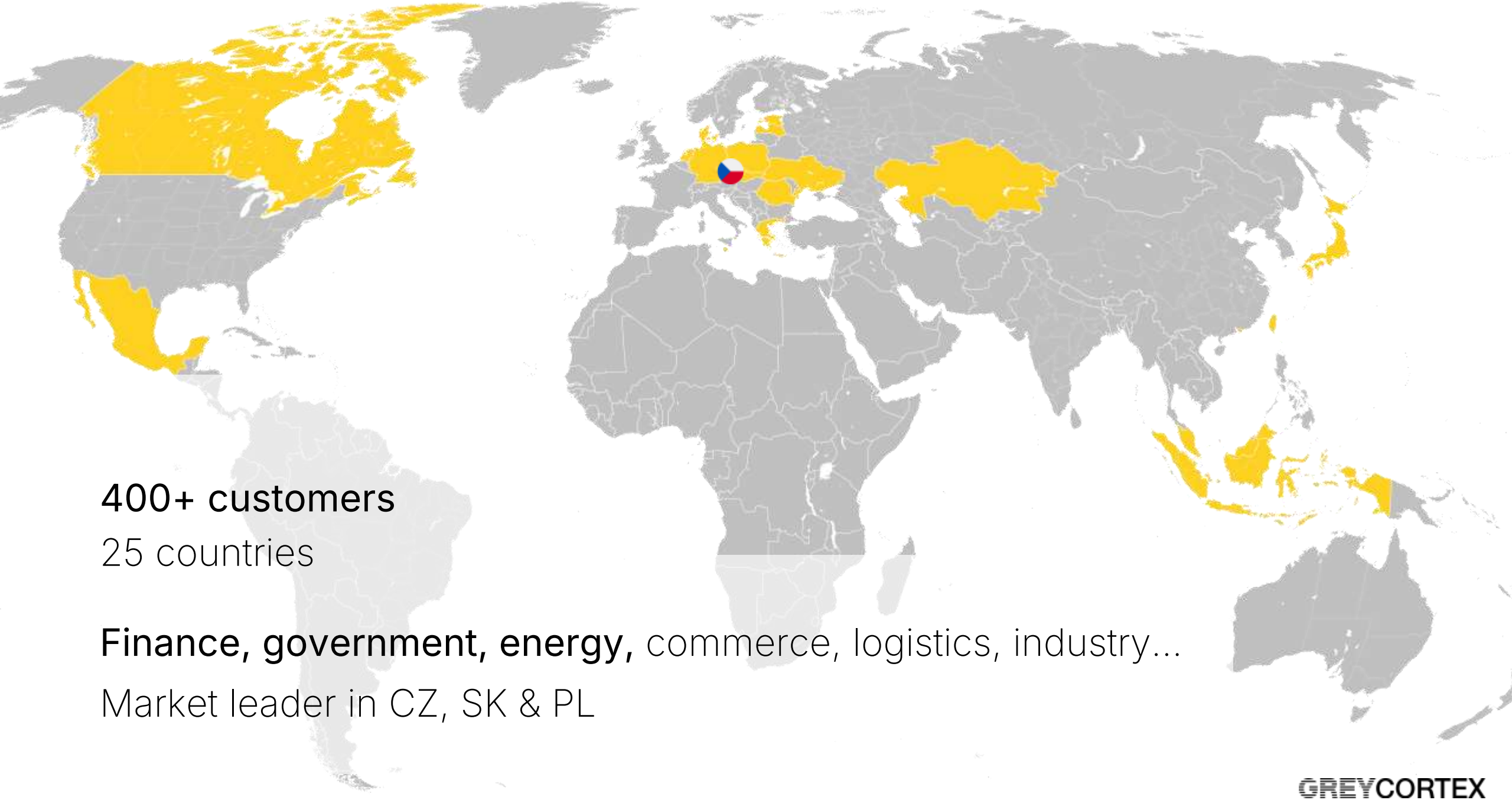
GREYCORTEX

Power of Network Traffic Analysis (NTA) for Enterprise & ICS Networks

Pavel M. Chmelar

Baku | 23th April 2026



400+ customers

25 countries

Finance, government, energy, commerce, logistics, industry...

Market leader in CZ, SK & PL

GREYCORTEX

Is my cyber security working?

Cyber crime, hackers, ransomware and other undetected malware

Firewalls, endpoint security working well

Security policies, compliance & best practices

Protection of IT, OT and IoT

NIS2, ISO27000, PCI DSS, DORA, IEC 62443

Network Security Monitoring

Network Detection and Response / Network Traffic Analysis
Industrial IDS / OT monitoring

GREYCORTEX

What is going on in the network?

Support of **SDN segmentation & microsegmentation**

Performance of applications, devices and network

Control over behavior of users and contractors

Misconfigurations and changes of network configuration

Forensics, Root-Cause Analysis & Troubleshooting

Real-time Network Analytics

On-premise & hybrid infrastructure
IT & OT networks

GREYCORTEX

How does it work?

Main input: Mirrored network traffic

= SPAN, RSPAN, ERSPAN, TAP, packet brokers

Optional: IPFIX, NetFlow, NSEL, NetStream, ...

Optional: Application logs

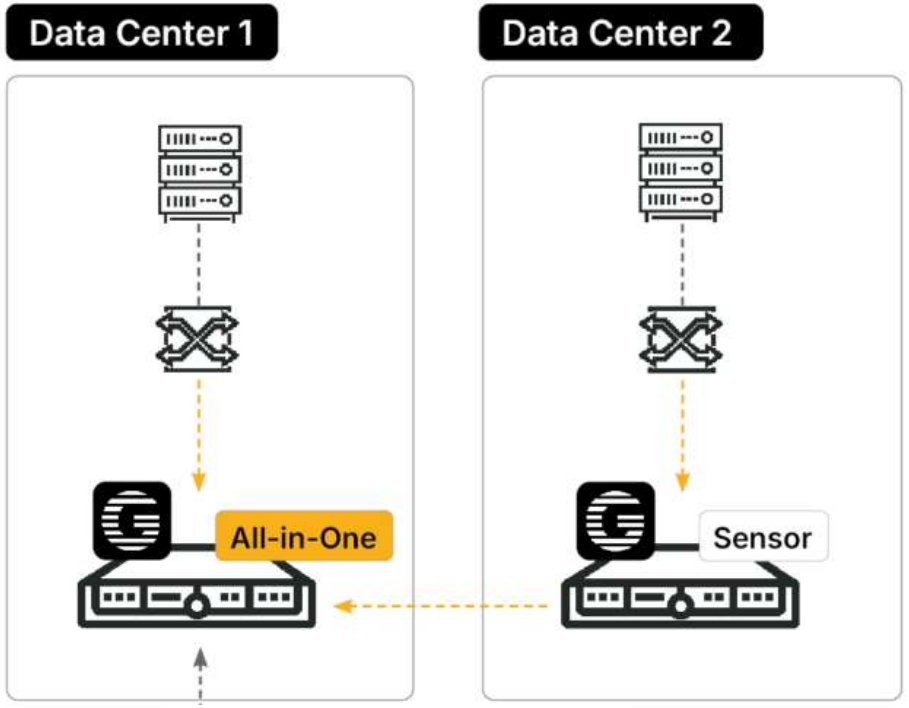
Why network traffic?

All devices communicate over network

Similar language for all the devices

Many security information

Many other info: misconfigs performance, ...



Advantages of Traffic Analysis by GREYCORTEX

Quick to deploy even in large & complex networks

Adapts as the network evolves over time using machine learning

Combinations of detection methods threat intel, advanced statistics & AI

Filter, search & sort anything communication and metadata of devices/users/applications

Intuitive & easy to use by skilled cyber security & networking people

Passive – cannot be seen by hackers

Synergies?

EDR/XDR

+ easy to manage

− not covering OT, IoT, network infra, ATMs, 3rd party devices ...

− easy to avoid: threats in browsers (avoiding OS), BYOD

With GREYCORTEX → full network coverage

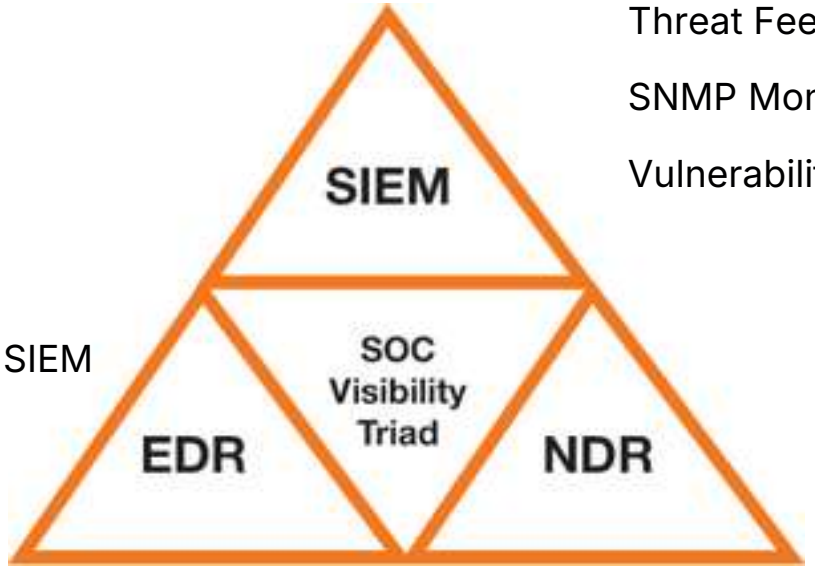
SIEM & SOAR

+ deep insight & great potential

− complex to implement

− hard to keep up to date

With GREYCORTEX → actionable & effective SIEM



Other Tools

Network Access Control

User Identity Services

Software Defined Networks

Firewalls

Proxy

Threat Feeds

SNMP Monitoring

Vulnerability Monitoring

GREYCORTEX in a bank?

Real-time network analytics of large infrastructures
Quick trouble shooting, decision making and timely reaction

Policy Enforcement
Eliminate risks and enforce policies

Building internal SOC / security monitoring
Integrations with SIEM & SOAR via ...
... filtered events, filtered IPFIX flows & API queries

Compliance requirements
ISO2700x, PCI DSS, DORA & NIS2 (EU), audits from central banks...

Case study

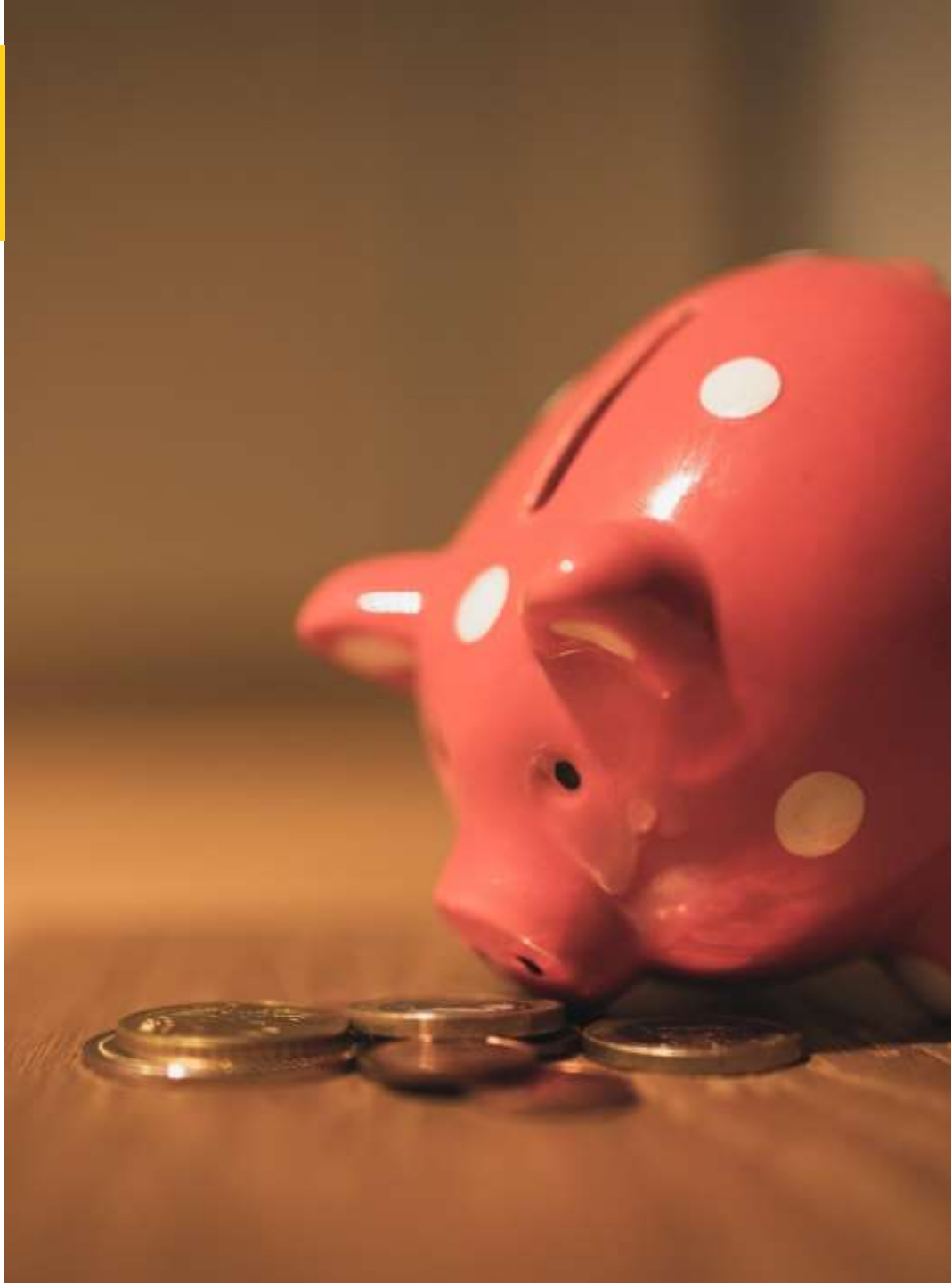
Societe General Czech Republic

1st phase (2018)

- 2 DCs covered with 2 HW appliances
- Analysis of mirrored network traffic via packet brokers
- Primary use cases: cyber sec monitoring, esp. policy enforcement
- Primary end users: cyber security team
- DORA, NIS2, PCI DSS

2nd phase (2022)

- 1 HW appliance added for Netflow monitoring of all 150+ locations / 800 sources of Netflow
- Cisco Secure Workload (Tetration) was the only "alternative"
- Primary end users: cyber security team and networking team
- Implementation of software defined networking (Cisco ACI/APIC) – as a critical use case



GREYCORTEX in a govt?

Used by multiple teams

Security, network, IT admins

Quick & easy deployment

Even in “less than perfect” networks

Example of customers

Offices of key government & state representatives

Ministries & other central institutions

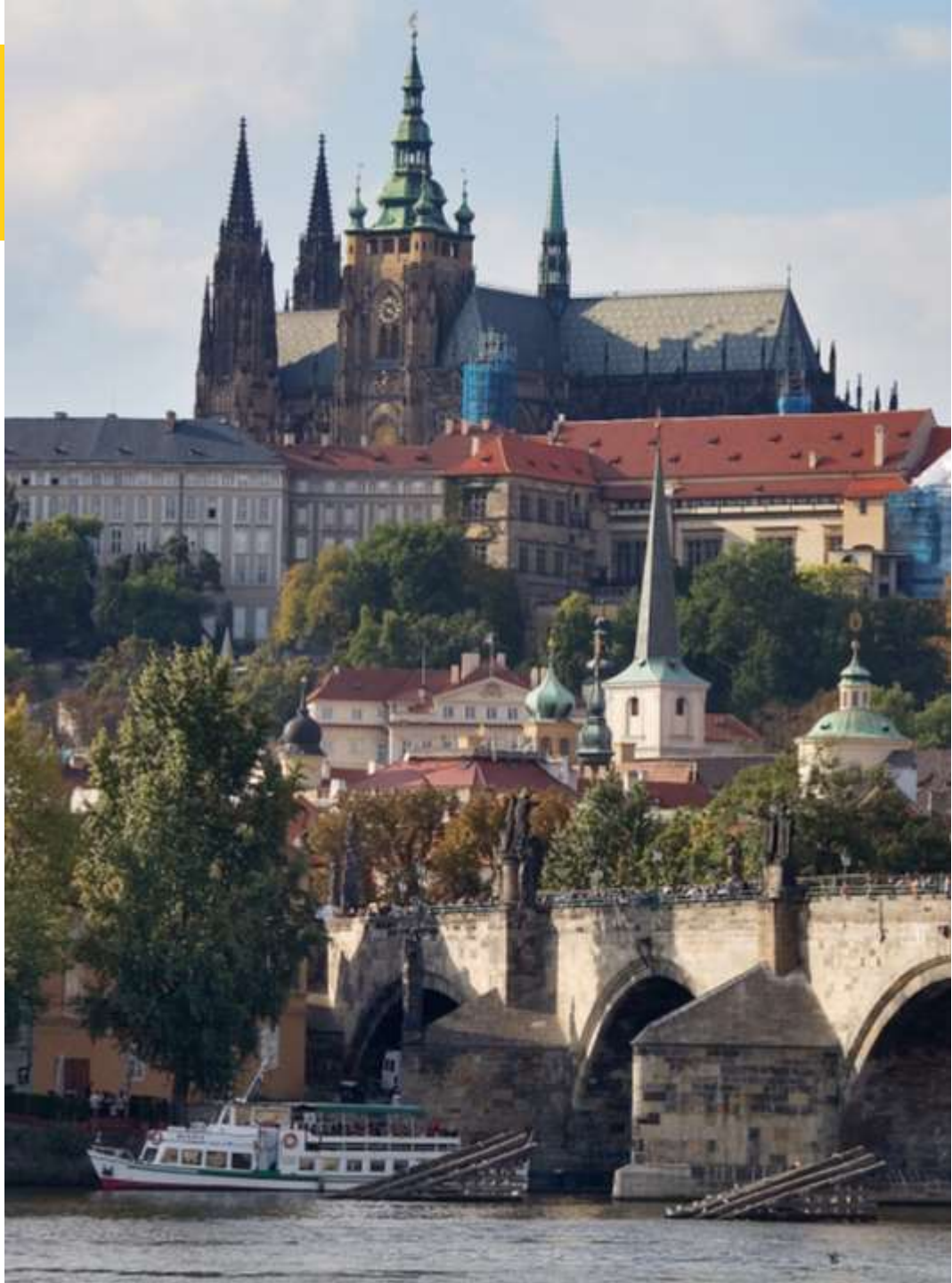
Polices & emergency units, courts, prisons …

Hospitals

Towns & Regions

Public companies – water management, heat generation, street lightning & other utilities, metropolitan networks, public transport, …

Army organizational sections / units (even one NATO missile base)



GREYCORTEX in a telco?

Monitoring of internal network
Analytics, detection, response

Monitoring of smart-meter networks
Up to 5 million devices monitored by a single appliance
Orange PL monitoring network of Tauron PL

Managed services provided telco operators
Smart-meter network monitoring
Monitoring of other private networks
Monitoring of managed infrastructure of customers

Customers incl. T-Mobile in PL

Case study

Eastern Slovek Distribution (E.ON)

3 Teams: IT, OT, Cybersecurity

Infrastructure using Siemens and ABB ++ (IEC104, GOOSE, MMS)

- Cyber security monitoring
- Resolution of operations issues
- Policy monitoring
- Deployment & configuration verification, ...
- After 2 yrs. SPLUNK implemented and integrated with MENDEL

Common platform for collaboration for all teams

What GREYCORTEX is NOT

Expensive and heavy system
with bad pre- and aftersales support
made in US or Israel.

What is GREYCORTEX?

Practical tool for cyber security & operations monitoring

Designed for use in less than perfect networks to be used every day

Doing things competitors cannot

Serving customers of **500 IPs to 200.000 IPs** in the network most customers 5k to 100k IPs

Search 10TB of network metadata **in 5 seconds** using clever aggregations in the dtb

Full **IT, OT & IoT** interoperability 15+ OT protocols parser & predefined detection profiles

Automated response on 500Gbps throughput analyzing IPFIX Aruba CX10000 and a plugin for integration

Support of SDN networks integrating with Cisco APIC/ACI

Great technical support in English or Russian

GREYCORTEX

www.greycortex.com