GREYCORTEX

Ako na detekciu a vyhodnotenie kybernetických bezpečnostných udalostí

| Jesenná ITAPA 2024 |

Ondřej Hubálek

Company Highlights

Established in Czech Republic

- **2013:** Commenced as AI research university project
- **2016:** Transformed through seed investment and spin off

Mentioned by Gartner, Forrester, Kuppinger-Cole...

- NTA, NDR, NAV, IT & OT

300+ customers / 500+ deployments worldwide

- Government & Public, healthcare, energy, e-commerce, critical infrastructure, banks and finance...

Research and Development

- AI/ML applications
- Detection methods & Wireless Analysis
- New OT applications

CD PROJEKT · SOCIETE GENERALE · empik

Sąd Apelacyjny w Warszawie · albert · NBU

NEC NECネッツエスアイ · YSOFT · SeaChange

Ministry of Foreign Affairs of the Czech Republic · PRE

hilase · Česká pošta · RIKEN

GREYCORTEX

GREYCORTEX MENDEL

Visibility

All the network communication, devices with inventory details, and user behavior

Detection

From misconfigurations, performance problems, or policy violations to undetected malware, ransomware, and hacker activities which are able to bypass existing security tools

Response

Rapid attack response, and incident investigation and management

+

SCADA/ICS Monitoring

Application Performance Monitoring

Asset Inventory (2021)

Network Detection and Response

GREYCORTEX

Endpoint | EDR | Server | Workload protection | Cloud | Email | Mobile | Firewall | Switch | Wireless | ZTNA

Network Detection and Response

Open APIs

- Industry/Developer
- Service Provider
- Administrator
- Security Operations

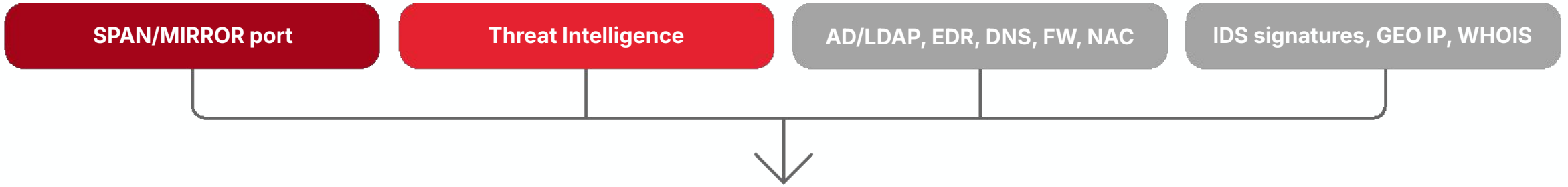
Threat Intelligence

Artificial Intelligence

Data Lake

Adversaries Exploit Legitimate It Tools

Architecture



Signatures & DPI
Signatures & Deep Packet Inspection

Signature-based detection

- Known malware
- Known attacks
- Known exploitations
- Policy violations
- High performance packet capture

NBA
Network Behavior Analysis

Behavior-based detection

- Malware activity propagation, downloading, spamming
- Attacker activity - scanning, brute-forcing, exploitation
- C&C activity - RAT, APT, AVT, bots, worms, rootkits
- Data exfiltration

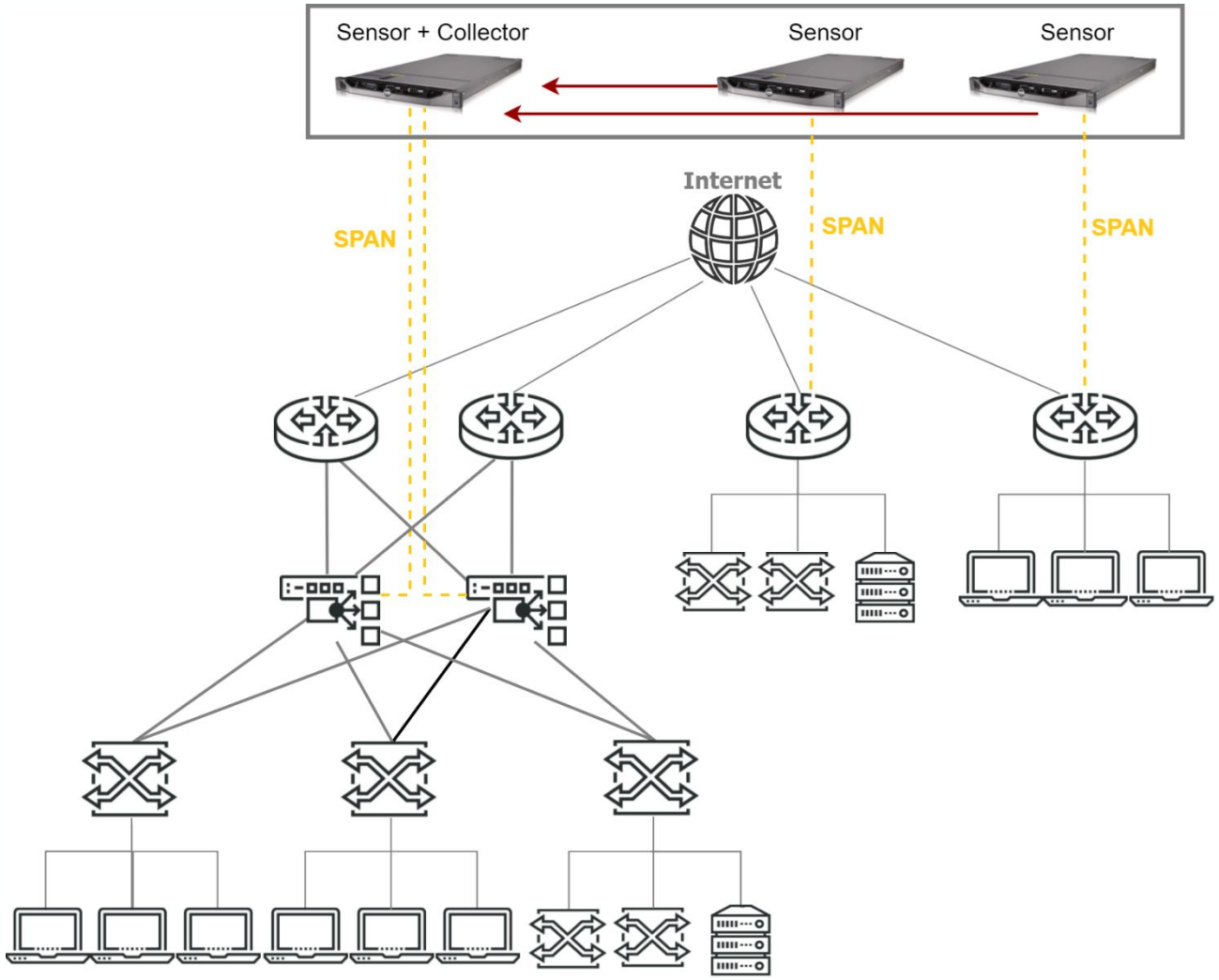
Stats
Network Statistics

Visibility & Performance

- Complete network visibility
- Application performance
- Network performance
- Application & user awareness

User interface, Reporting, Notification & Integration (SIEM, Firewall, ...), Response

Deployment



Sensors

- Port Mirroring (SPAN, RSPAN, ERSPAN)/TAP
- ASNM output (= 0,5% - 2% of traffic)
- Up to 100Gbps/sensor

Collectors

- 1 collector = 50+ sensors
- Aggregated input up to 100Gbps+
- Central collector for Events visualization

Devices

- Hardware
- Virtual (VMware ESXi, Hyper-V, KVM, ...)
- Cloud (AWS, Azure, GCP)

WORKSHOP

www.greycortex.com

Malware, Exploits and Hacker's activities

- Known Threats Link
- Projevy nebezpečného chování
  - C&C odchozí komunikace Link
  - Útoky hrubou silou Link
  - Skeny Link
- Co neodpovídá best practices interní sítě
- Plain-text authentizace Link

GREYCORTEX

GREYCORTEX

www.greycortex.com