



MyNetScope®

**Next Generation
Network Security Monitoring**

AdvaICT, a.s.

Company introduction

- Founded in 2006
- Masaryk University spin-off company
- Active in network monitoring and security
- Cooperation in research and development in network security

We are facing cyber threats on daily basis

- **Profit from cybercrime** exceeds profit from drugs worldwide since 2006. [FBI, 2006]
- CIA confirms cyber attack caused **multi-city power outage**. [New Orleans, 2008]
- Corporations and government spend **billions of dollars** a year to detect and combat malware. Still, the black hats seem to be gaining the upper hand. [NYT, 2010]
- New **botnet** spreading from routers, DSL modems and webcams discovered by Czech researchers. [MU, 2010]
- USA declared not to use **nuclear weapons** against non-nuclear states, even if they launched a crippling cyber attack against USA. [Barrack Obama, 2010]

Network Security Trends

www.enisa.europa.eu/act/it/library/deliverables/procent

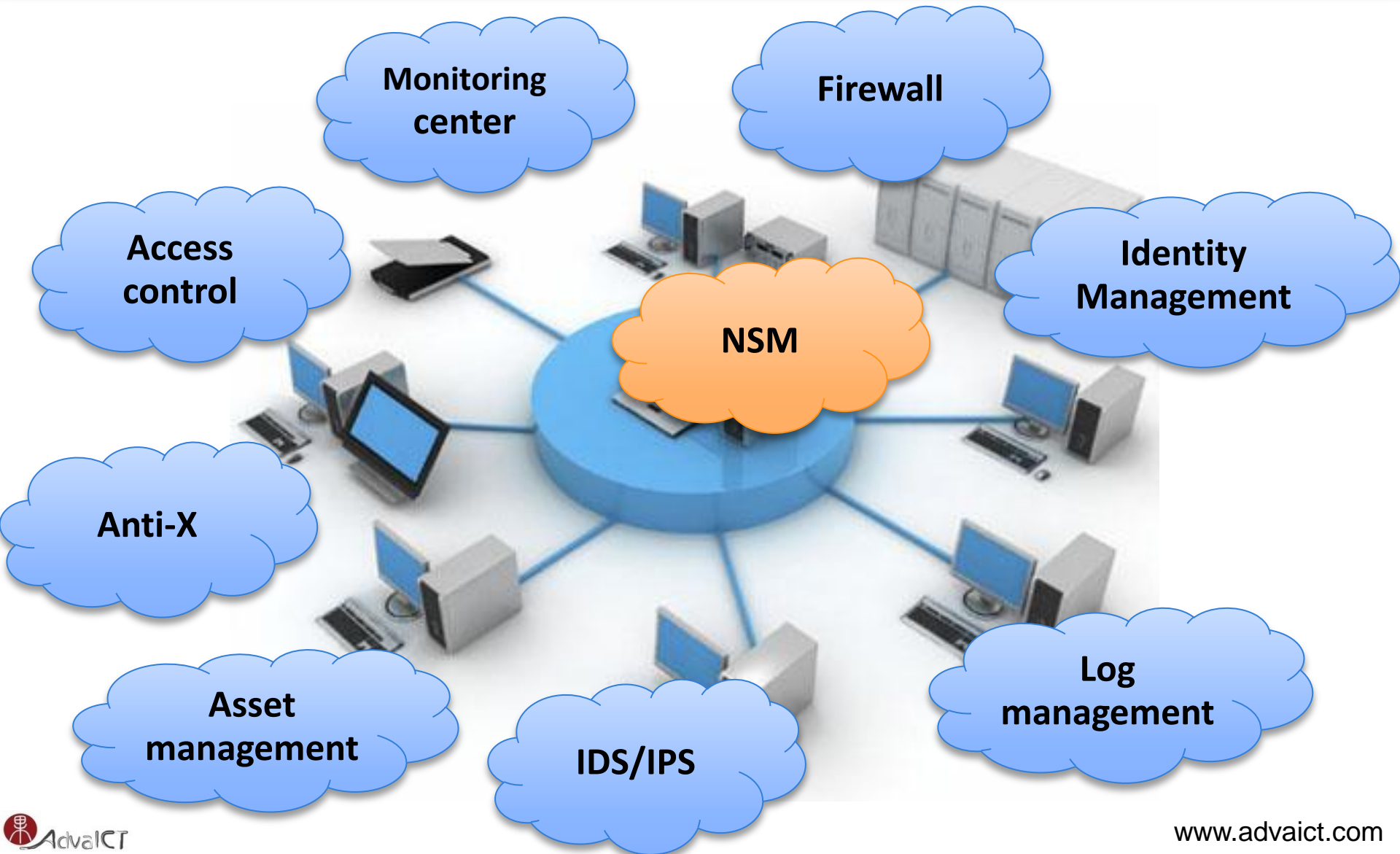
Network
Security
Monitoring

Computer Security
Incident Response
Team

Antiviruses
Firewalls

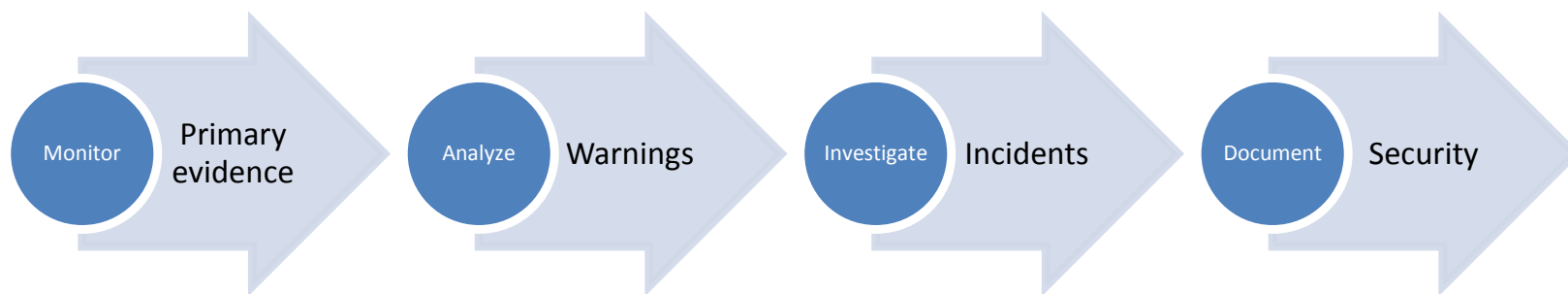


Network Security Tools in Use

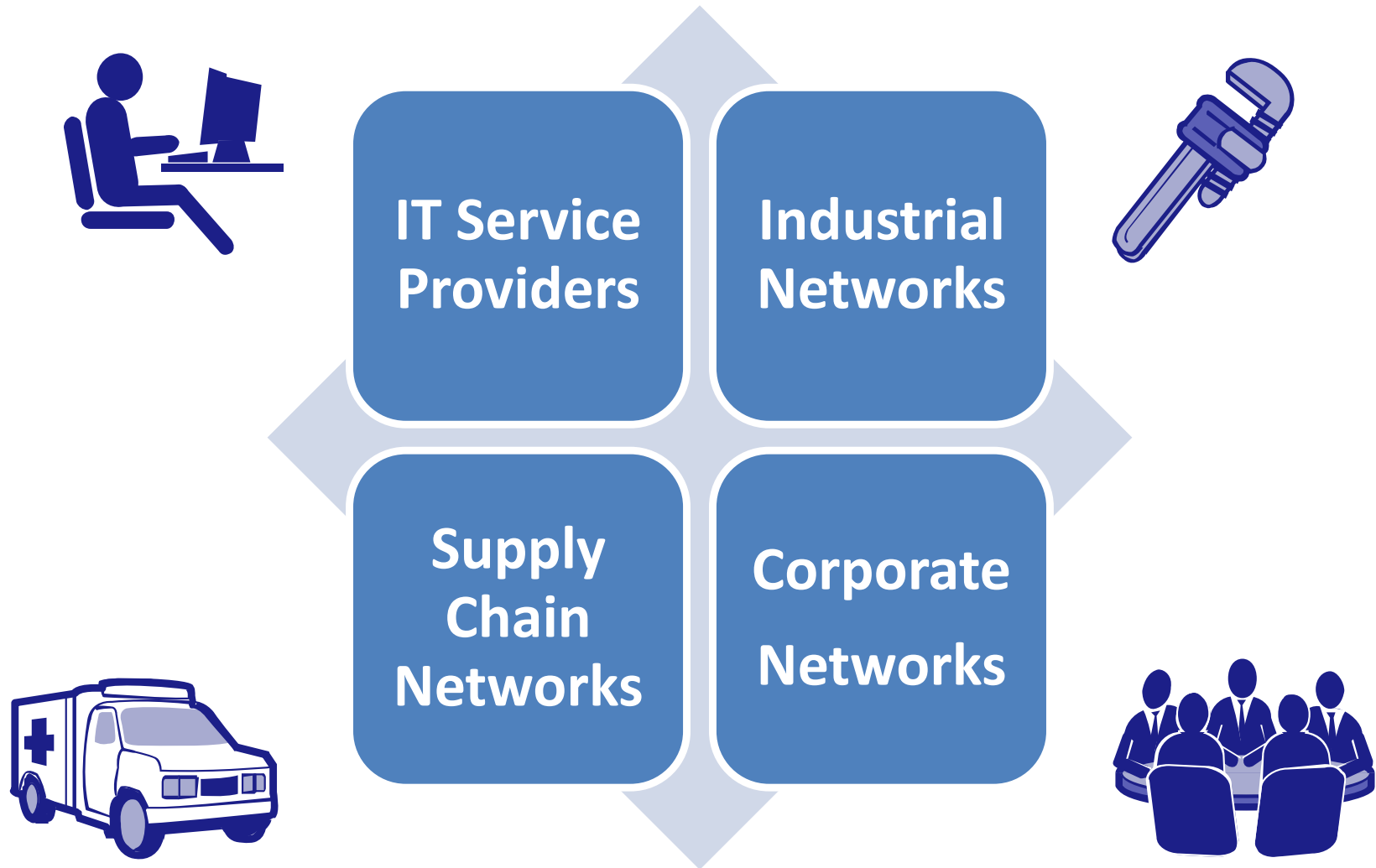


What is Network Security Monitoring?

- **NSM** is sustainable process of indicators **collection, analysis, investigation** and **escalation**
- Indicators are observable or discernible actions that confirm or deny enemy capabilities and intentions



Who should perform NSM?



What problems NSM solves?

Unknown structure of network traffic

Expensive operations and support

Network latency, failures and outages

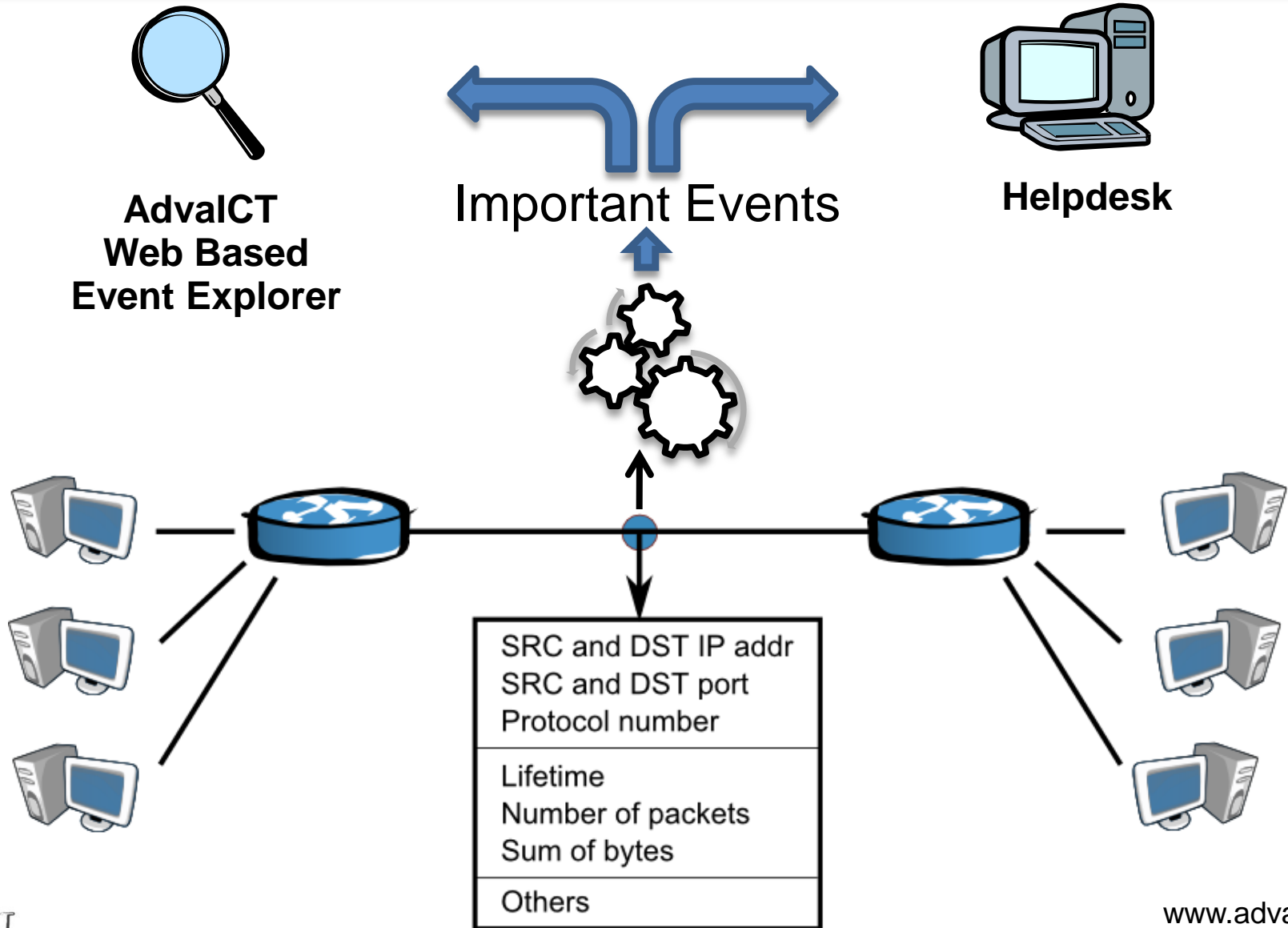
Activities under stolen identity, insider attacks and misuse

Network misconfiguration

Infected computers and incontrollable outgoing traffic

Masked network traffic, undesired applications

MyNetScope[®] Network Security Monitoring Platform



MyNetScope[®] Platform – Principles



**Behavior
Detection**



**Signature
Based**



**Network
Based**



**Host
Based**



MyNetScope[®] Platform – Features

Undesirable Behavior Detection

- Attacks
- Undesirable services
- Operational problems

Behavioral Profiles Computing

- Traffic volume
- Traffic structure split up by network services
- Communication partners

Anomaly Detection

- Change in behavior profile
- New network devices/services

Supplemental Events Processing

- System and application logs
- Databases...

Control IT infrastructure with us

More
efficient

- Problems are detected and isolated in time – before they cause night shifts, outages and unsatisfied customers
- Administrators can deal with infrastructure development and service improvements

More
secure

- Infrastructure is better protected to new threats (malware, attacks, social engineering, ...)
- Security incidents are detected and investigated in time
- Undesired services usage can be eliminated

Solution Options

Products

- FlowMon ADS
- MyNetScope – Live

Outsourcing

- Permanent network supervision
- On-line service

Traffic analysis

- Comprehensive network analysis

Getting started?

- Real traffic demo
- Short-term trial
- Comprehensive network analysis
- **On-line demo right now**





MyNetScope[®]

Next Generation Network Security Monitoring

AdvaICT, a.s.

Questions?

Jundrovská 31
624 00 Brno

info@advaict.com
www.advaict.com