# CSIRT.CZ

## Ověřování architektury systému PROKI

**Robert Šefr • robert.sefr@nic.cz • 13. 11. 2015**

CZ.NIC | SPRÁVCE DOMÉNY CZ

# PROKI

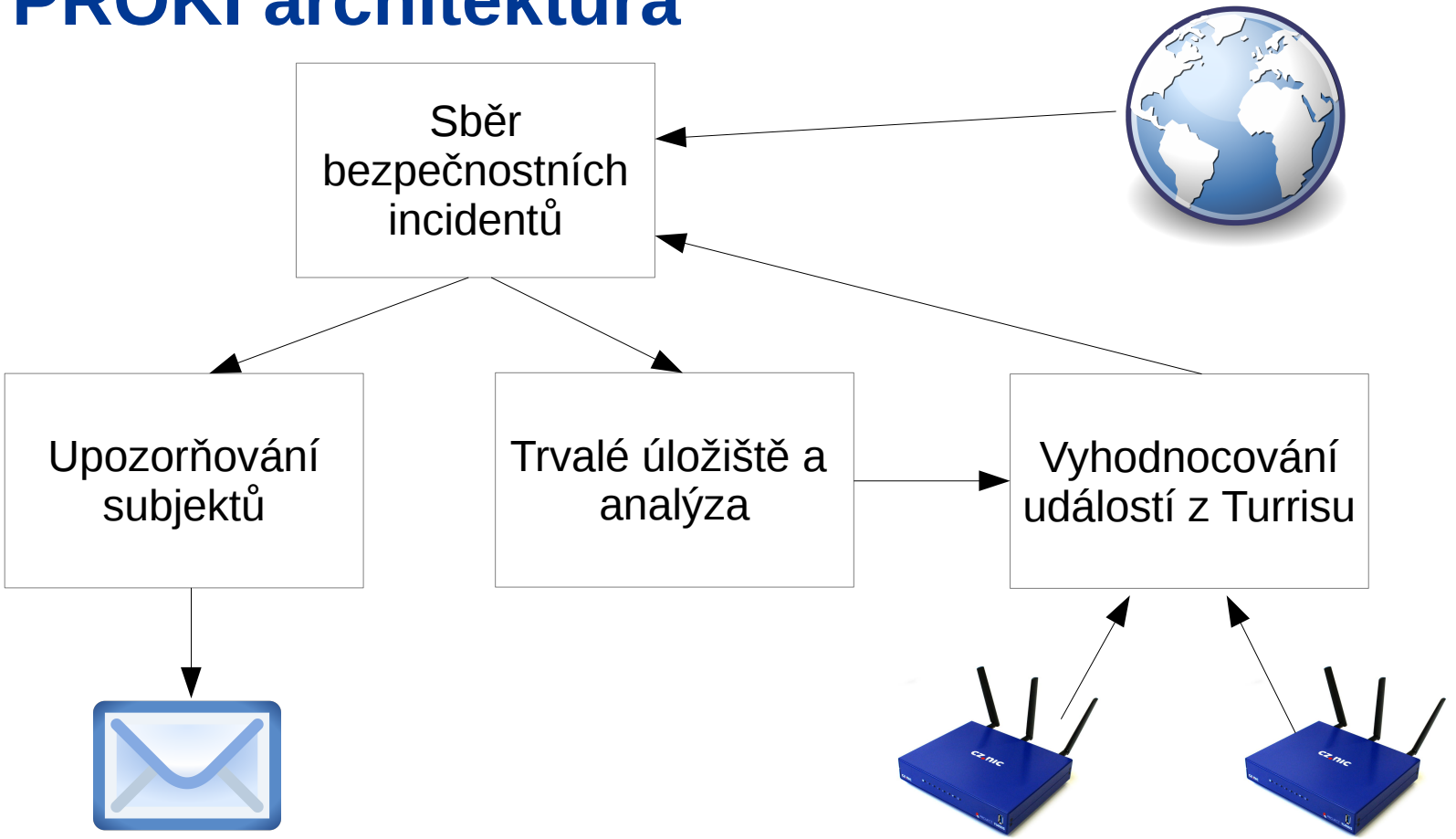
## PREDIKCE A OCHRANA PŘED KYBERNETICKÝMI INCIDENTY

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

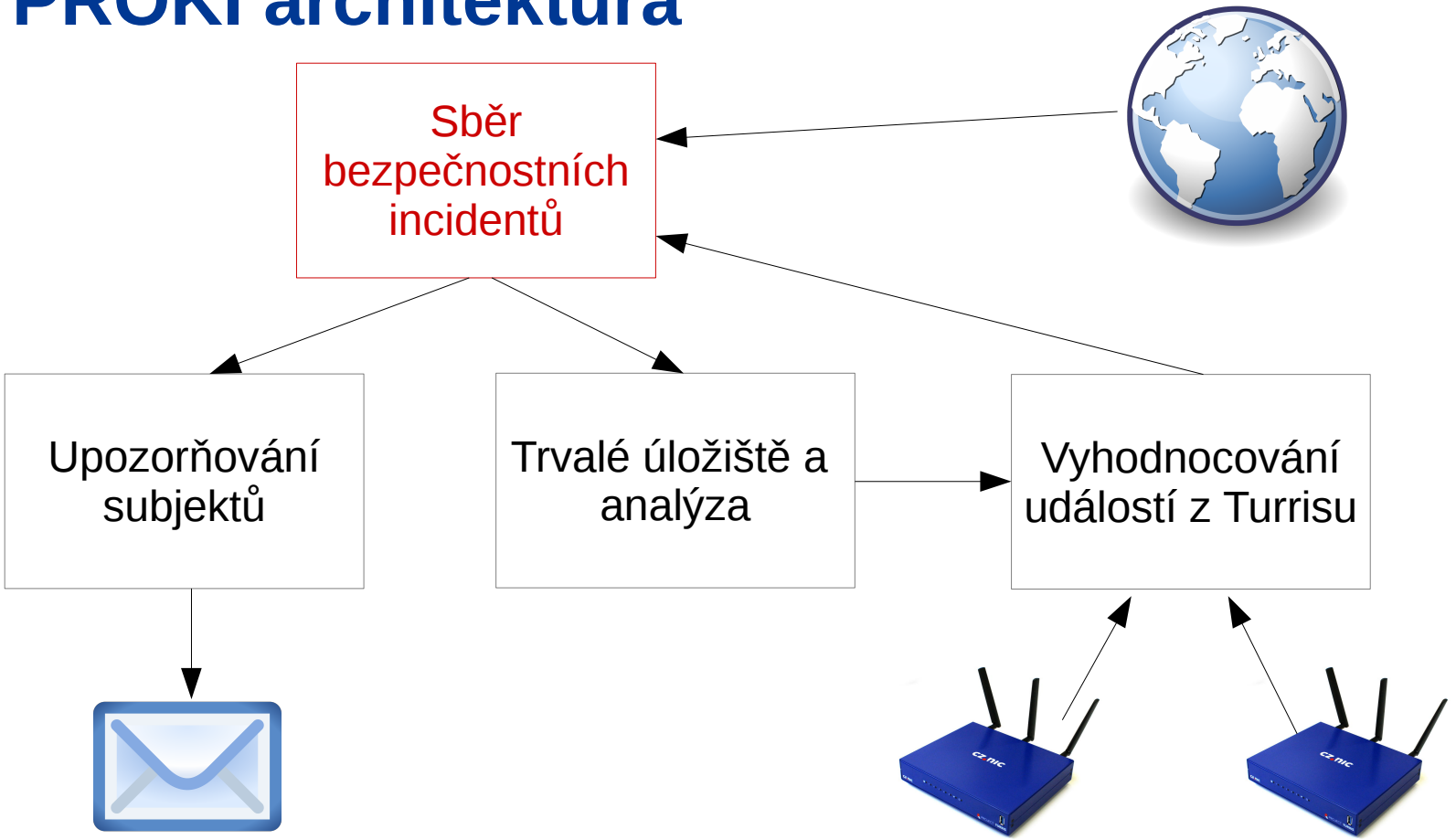
Projekt **„Predikce a ochrana před kybernetickými incidenty (PROKI)“** (*VI20152020026)* je realizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020.

CZ.NIC | SPRÁVCE DOMÉNY CZ

# PROKI architektura



# PROKI architektura



# Požadavky na systém na sběr bezpečnostních událostí

- Open source
- Jednoduché na konfiguraci
- Možnost jednoduchého psaní vlastních zdrojů dat
  - Preferovaným jazykem je Python
- Spolehlivost a stabilita
- Různé typy výstupů

# 1. Abusehelper

- CERT.FI, CERT.EE a ClarifiedNetworks
- Řešení preferované mnoha týmy
  - Doporučuje i ENISA
  - Dlouhá historie a stabilita
- Pro předávání zpráv používá XMPP
- Malý důraz na open source aspekt, částečně proprietární
- Zmatená a roztříštěná dokumentace

# 2. Megatron

- CERT-SE
- Použitým jazykem je Java
- Vlastní GUI
  - Může být výhodou ale i omezením
- Minimální dokumentace

# 3. Collective Intelligence Framework

- Primárním jazykem je Perl
- Předdefinovaný tok dat
- API nad databází pro přístup k datům
- Velké množství integrovaných funkcí pro PROKI nezajímavých

# 4. IntelMQ

- Dokumentace opravdu popisuje asktuální stav projektu
- Psáno v Pythonu
- Živý (někdy ale až hektický) vývoj
- Stále chybějí některé podstatné zdroje dat
- Spolehlivá fronta zpráv (Redis nebo ZeroMQ)
- Silný důraz na modularitu (inspirace Abusehelperem)

# Formát události

```
VX Vault last 100 Links
Fri, 13 Nov 2015 09:53:41 +0000
http://193.28.179.38
http://www.microads.me/files
http://212.129.31.67/usb.exe
http://www.microads.me/downloads
```


```
{
  "feed": {
    "url": "http://vxvault.siri-urz.net/URL_List.php",
    "name": "vxvault"
  },
  "source": {
    "url": "http://212.129.31.67/usb.exe",
    "geolocation": {
      "latitude": 48.86,
      "cc": "FR",
      "longitude": 2.35
    },
    "asn": 12876,
    "network": "212.129.0.0/18",
    "ip": "212.129.31.67",
    "abuse_contact": "abuse@proxad.net"
  },
  "raw": "aHR0cDovLzIxMi4xMjkuMzEuNjcvdXNiLmV4ZQ==",
  "classification": {
    "taxonomy": "Malicious Code",
    "type": "malware"
  },
  "time": {
    "observation": "2015-10-12T19:57:09+00:00"
  }
}
```

# Formát události

- Vlastní formát IntelMQ :(
- Standardy jako STIX a IODEF jsou příliš těžkopádné

| Type | Taxonomy | Description |
|---|---|---|
| spam | Abusive Content | This IOC refers to resources, which make up a SPAM infrastructure, be it a harvester, dictionary attacker, URL etc. |
| malware | Malicious Code | A URL is the most common resource with reference to malware binary distribution. |
| botnet drone | Malicious Code | This is a compromized machine, which has been observed to make a connection to a command and control server. |
| ransomware | Malicious Code | This IOC refers to a specific type of compromized machine, where the computer has been hijacked for ransom by the criminals. |
| malware configuration | Malicious Code | This is a resource which updates botnet drones with a new configuration. |
| c&c | Malicious Code | This is a command and control server in charge of a given number of botnet drones. |
| scanner | Information Gathering | This IOC refers to port scanning activity specifically. |
| exploit | Intrusion Attempts | An exploit is often executed through a malicious URL. |
| brute-force | Intrusion Attempts | This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol. Please see the IOC protocol below. |

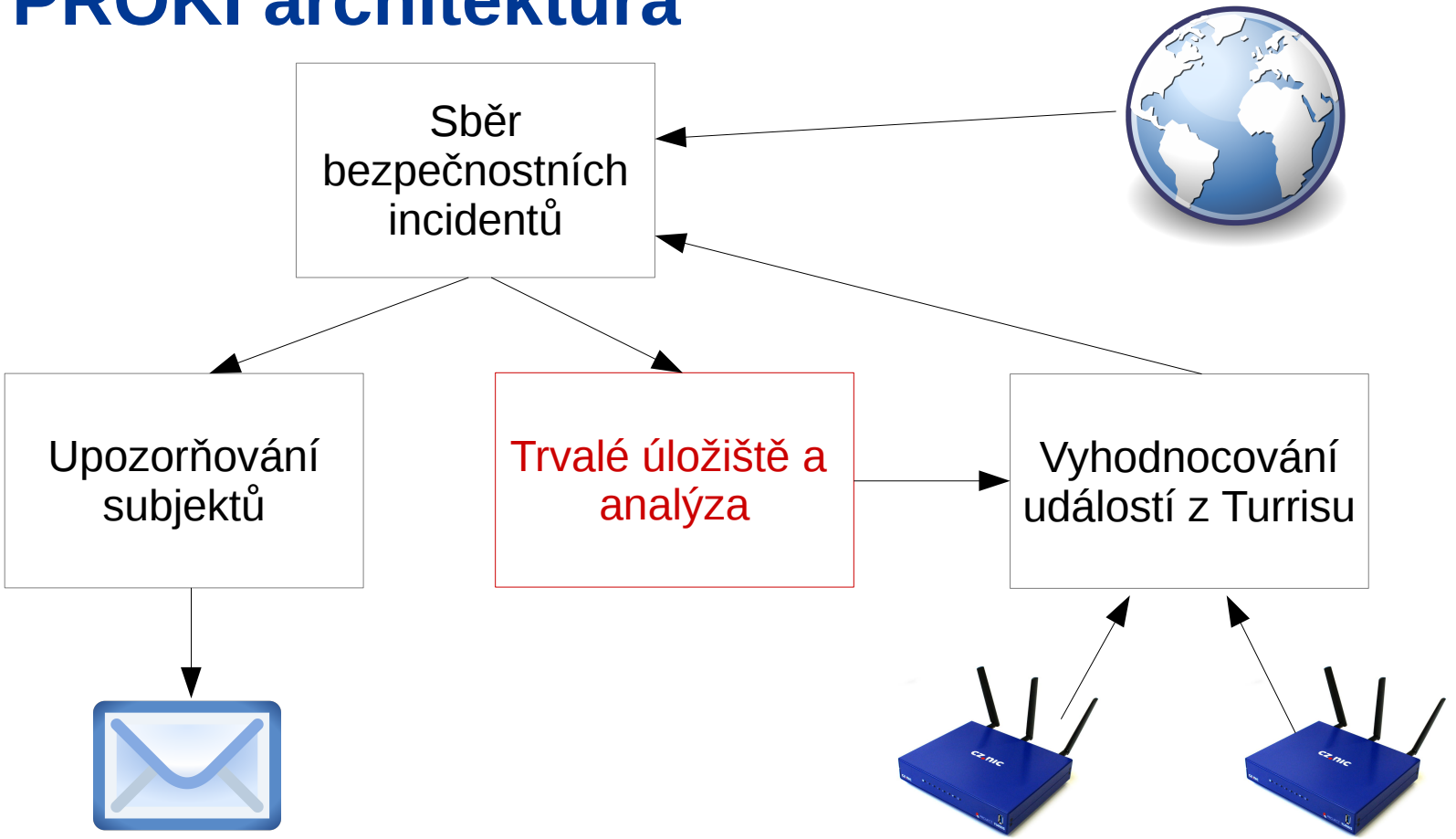
# Aktuálně podporované zdroje

- Abuse.ch Feodo Tracker Domains
- Abuse.ch Feodo Tracker IPs
- Abuse.ch Palevo Tracker Domains
- Abuse.ch Palevo Tracker IPs
- Abuse.ch ZeuS Tracker Domains
- Abuse.ch ZeuS Tracker IPs
- AlienVault
- AlienVault OTX
- Arbor
- Autoshun
- BlockList.DE Apache
- BlockList.DE Bots
- BlockList.DE Brute-force Login
- BlockList.DE FTP
- BlockList.DE IMAP
- BlockList.DE IRC Bot
- BlockList.DE Mail
- BlockList.DE SIP
- BlockList.DE SSH
- BlockList.DE Strong IPs
- CI Army
- CleanMX Phishing
- CleanMX Virus
- Cymru Full Bogons
- DShield AS
- DShield Block
- DShield Suspicious Domains
- Danger Rulez
- Dragon Research Group SSH
- Dragon Research Group VNC
- Dyn
- Fraunhofer DGA
- HpHosts
- Malc0de Domain Blacklist
- Malc0de IP Blacklist
- Malware Domain List
- Malware Domains
- Malware Group Domains
- Malware Group IPs
- Malware Group Proxies
- MalwarePatrol Dans Guardian
- OpenBL
- OpenPhish
- PhishTank
- Taichung
- **Turris Greylist**
- URLVir Hosts
- URLVir IPs
- Spamhaus CERT
- Spamhaus Drop
- VXVault

# Další plánované zdroje

- 1d4
- Abuse.ch (RSS)
- Abusix
- ADB Lock Plus
- Affairedhonneur
- Animus Project
- Arbor FastFlux
- Bad IPs
- Bambenek Consulting
- Berkeley
- Binary Defense
- Bit Cash
- Blade-Defender
- Blueliv
- BlutMagie
- Botscout
- Brawg
- Callback Domains
- Carbon Black
- CERT.org
- Chaos Reigns
- Critical Stack
- Cruzit
- Cyber Crime Tracker
- Cydef
- Dan.me
- Deny Hosts
- DNS DB
- Dyn DNS
- Emerging Threats
- Falconcrest
- Geo SPY
- Gofferje
- GPF Comics
- H3X
- Hosts File
- Inflitrated
- ISC SANS
- ISightPartners
- Jeek
- Joewein
- Joxeankoret
- Kids Clinic JP
- Kolatzek
- Malc0de
- Malekal
- Malware BlackList
- Malware.br
- Malware Config
- Malwared
- MalwareDomains
- MalwareInt
- Manity
- Martin Cyber
- MaxMind Proxies
- Minotaur Analysis
- mIRC
- Monzymerza
- Multiproxy
- MVPS
- Nothink
- Malwr
- Null Secure
- OpenBL
- OpenPhish
- PacketMail
- Payload Security
- PHP Black
- Project Honeypot
- Prometheus Group
- Proxylists
- ProxySpy
- Sacour
- Sender Base
- Sigma Projects
- Skygeo JP
- Snort
- Snort
- SPAMHaus
- Spys RU
- SRI
- SSH BL
- Steeman
- StopForumSPAM
- Surriel
- t-Arend
- TheCyberThreat
- The Haleys
- Threat Grid
- TOR Project
- TotalHash
- Trailswest
- TrustedSec
- URI BL
- URL Query
- Vir BL
- Voipbl
- VX Vault
- YourCMC
- Yoyo

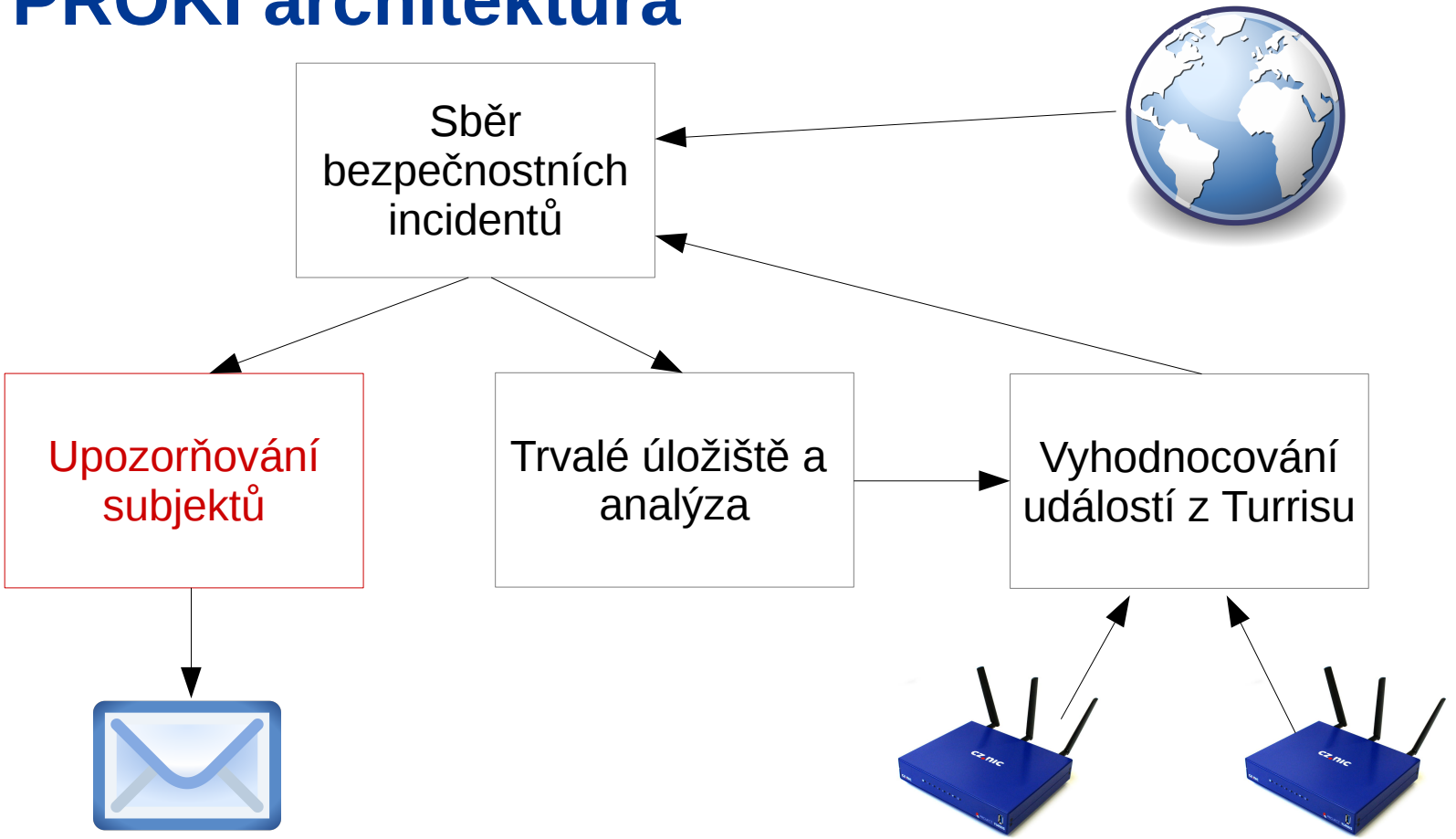
# PROKI architektura



# Trvalé úložiště a analýzu událostí

- Požadavky
  - Ukládání dat i v řádu několika let
  - Jednoduché analytické funkce
  - Zvládne změny dat v čase
- Vybrané řešení – Elasticsearch
  - Jednoduché na nasazení a integraci s dalšími moduly
  - Velmi jednoduché prototypování nových dotazů a analýz
  - NoSQL svět není tak růžový, jak se může zdát

# PROKI architektura



# Upozorňování subjektů

- Odfiltrujeme události relevantní pro ČR
- Agregujeme podle více stupňů
  - Typ události (malware, open resolver, bot, …)
  - Cílový adresát
- Semi-manuální odesílání výsledných notifikací (kontrola analytikem)

# Děkuji za pozornost

**Robert Šefr • robert.sefr@nic.cz**

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt **„Predikce a ochrana před kybernetickými incidenty (PROKI)“** (*VI20152020026)* je realizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020.

CZ.NIC | SPRÁVCE DOMÉNY CZ