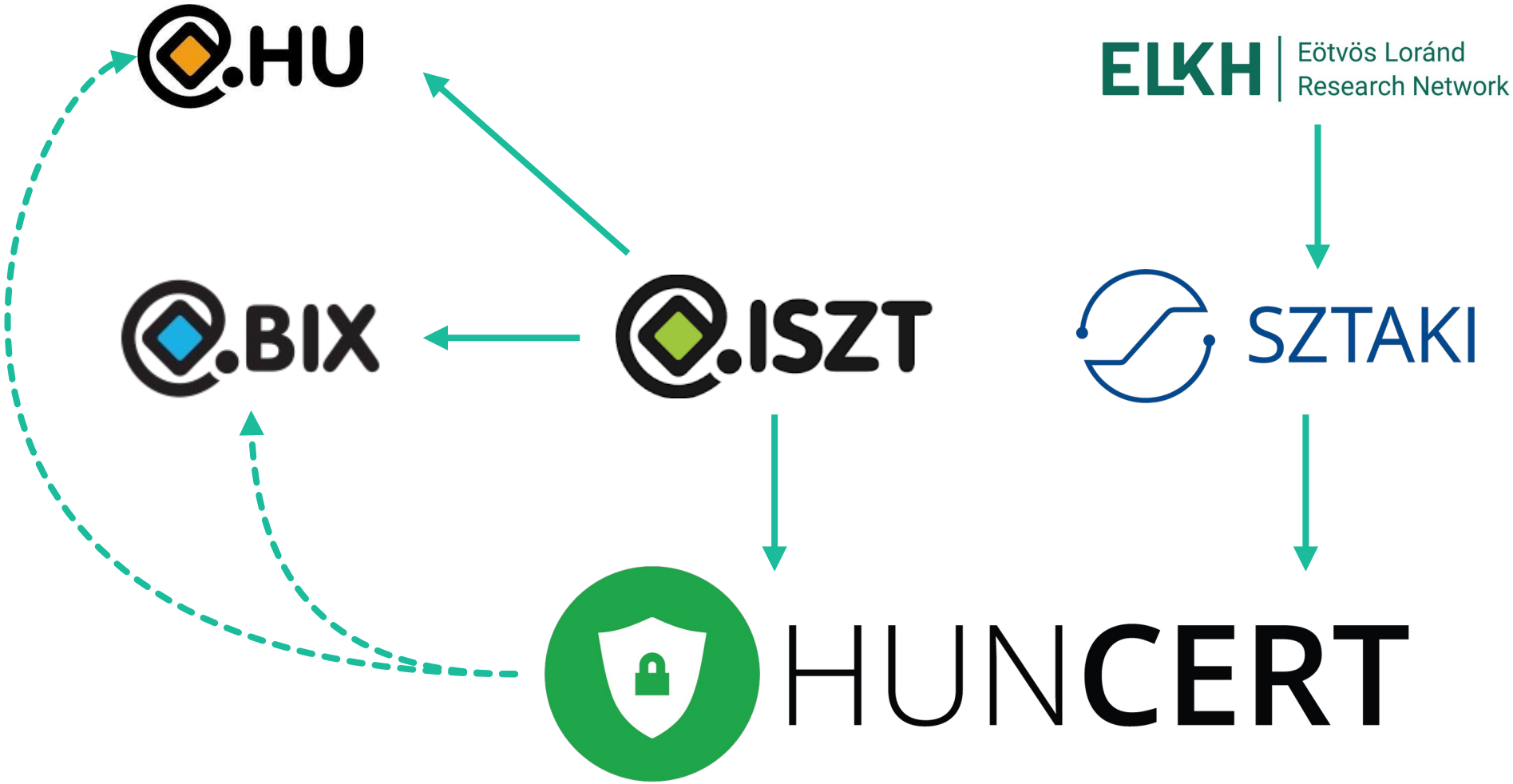
Distributed honeypot at BIX

Ernő Rigó, BIX / HunCERT
<rigo@cert.hu>

Who we are?


.HU
.BIX
.ISZT
ELKH
Eötvös Loránd
Research Network
SZTAKI
HUNCERT

What is a “honeypot”?

- **A tool for defensive deception**
- **Appears to be a real service**
- **Passive – waiting to be found**

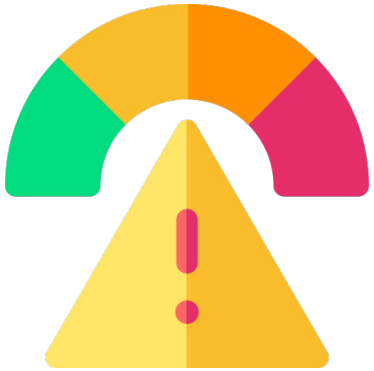
- **Also known as**
  - “trap” or “decoy”
- **Variations**
  - “tarpit” – service for wasting attacker resources
  - “honeynet” – appears to be a real network or set of services
  - distributed honeypot
- **Related to**
  - “canary” – tracking / triggering

Main differences from...

- **Firewalls, intrusion prevention systems (IPS), antivirus**
  - honeypots can not block attacks
  - BUT can be used to generate rules (think fail2ban)
- **Full traffic capture / netflow**
  - honeypots are only involved in malicious traffic
  - BUT low level capture (PCAP) of attacks is possible
- **UTM, SIEM and ISMS**
  - honeypots are not a complete solution
  - BUT can provide:
    - threat logs
    - alert triggers
    - IP reputation
    - insight to build a threat map
  - they are useful additions to any security system

Cost and risk factors

- **Main costs**
  - hardware / power
  - virtual resources
  - network traffic
  - maintenance



- **Main risks**
  - isolation breach
  - attack reflection
  - service collision
  - challenge / spite

Level of interaction

- **Low interaction / dumb**
  - Open TCP port
  - Optionally a simple (static) banner
  - Might fool simple network scanners
  - Operation risk and cost: low
- **High interaction / sandbox**
  - Real services
    - one container/VM per attack(er)
    - might emulate complex service networks
    - might deploy canaries
  - Can deceive human attackers
  - Risk and cost: high
- **Medium interaction**
  - Dynamic answers
    - partial protocol implementations
    - successful login or transaction
    - emulated resources and files
    - might deploy canaries
  - Aiming to deceive
    - service scanners
    - attack bots or scripts
    - casual attackers
  - Risk and cost: medium

Honeypot placement

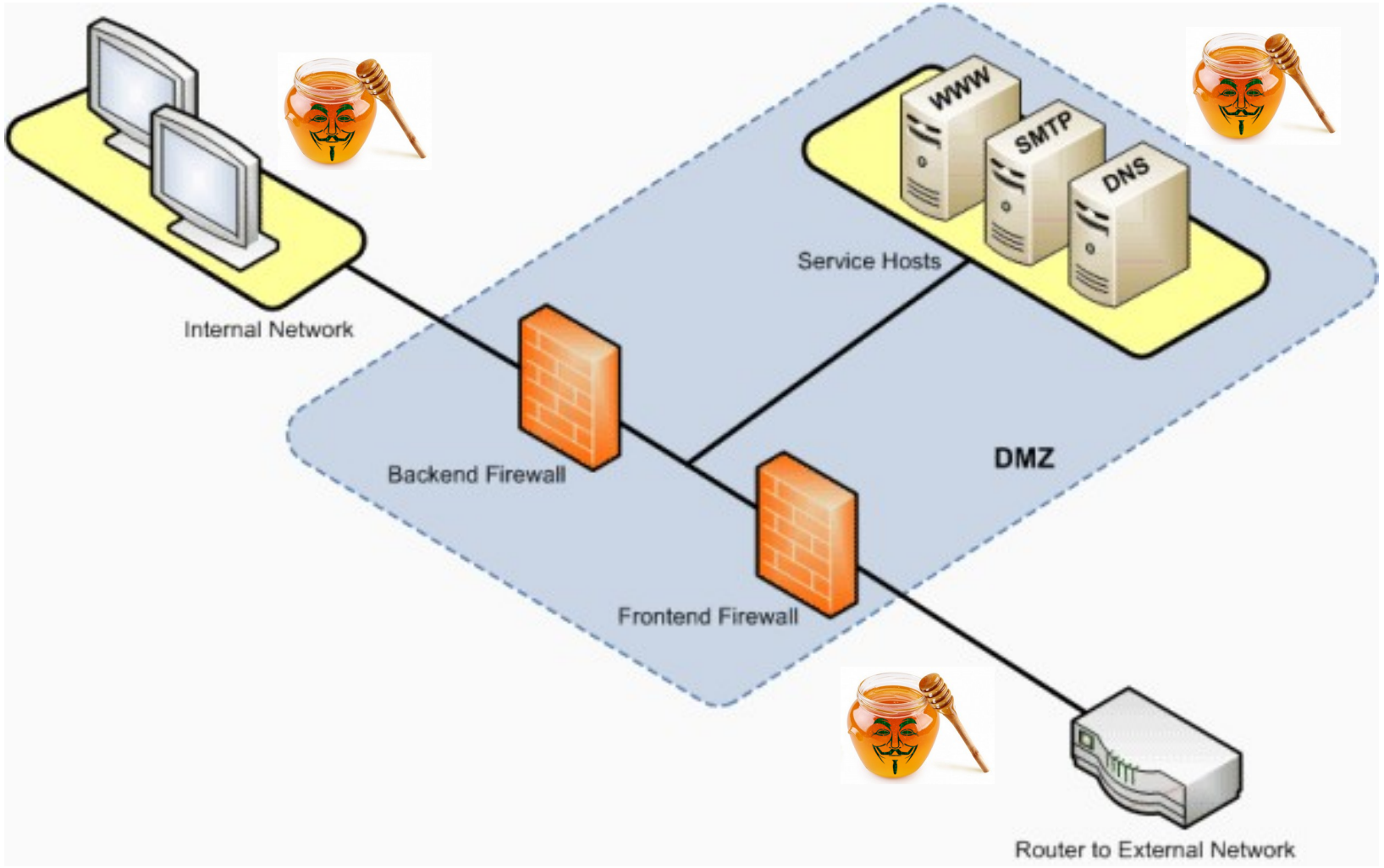


Image from: help.sap.com

Data extraction

- **Low+ interaction**
  - IP address / ASN
    - reputation based filtering
  - Target service (TCP/UDP port)
    - attack trends
- **Medium+ interaction**
  - Credentials
    - well known accounts / passwords
  - Requests
    - attack trends
  - Attack payloads
    - 0day attacks
- **High interaction**
  - Modified resources
    - system files
    - service configuration
  - Attacker strategy
    - pivoting attempts
      - horizontal movement
      - lateral movement
    - persistence attempts
      - backdoors
    - tooling
- **Most data can contain important signs of previous compromise, reused passwords, targetted attacks**

Distributed honeypot at BIX

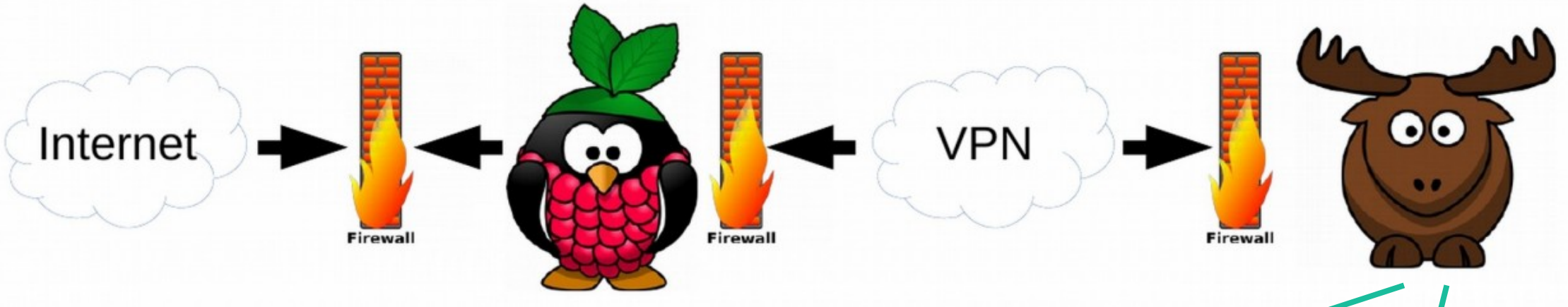
HUNCERT PROBE

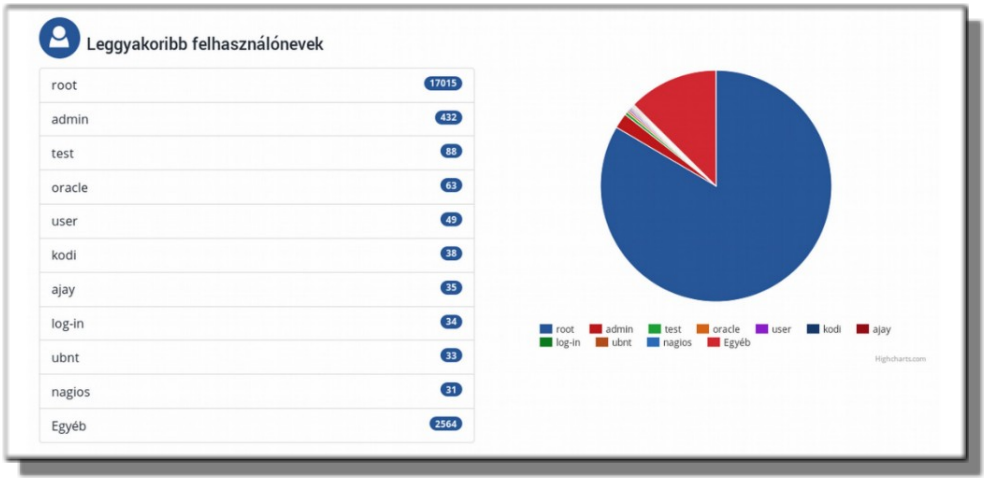
- **Since 2015**
- **Based on**
  - Raspberry Pi / Raspbian
  - Docker + Ansible
- **Target: public IPv4**
- **Traps:**
  - TCP SYN / UDP
  - SSH
  - SMTP
  - HTTP

Model of participation

- **Open participation**
  - Service and device is provided for free
  - Probe need to be kept in operation
  - Data is collected through VPN to central HunCERT servers
- **Data sharing tiers**
  - full log data for own probes
  - destination data is stripped from others
  - data aggregates are public
  - HunCERT / SZTAKI can use data for research purposes
- **All 50 probes are in service**

HunCERT PROBE system architecture





HUNCERT

PROBE development plans

- **Sharing of reputation data**
  - project DNS4EU
- **Virtual probes**
- **Additional traps**
  - Wordpress, Cisco SSH, Radius, LDAP, DNS, IMAP, POP, ...
- **UI improvements and facelift**


Thank you!