

KONFERENCE E-INFRASTRUKTURY CESNET | 1. ŘÍJNA 2026

Spolupráce a podpora řešení IT bezpečnosti



Martin Pustka (a kolektiv řešitelů)

Martin.Pustka@vsb.cz

Fond rozvoje CESNETu



Podpora rozvoje IT bezpečnosti

Aktivita je realizována i díky finanční podpoře Fondu rozvoje CESNETu
pro akademické a výzkumné instituce.



Spolupracující organizace



**Vysoká škola báňská – Technická
univerzita Ostrava**



Ostravská univerzita



**SLEZSKÁ
UNIVERZITA**

Slezská univerzita



Fakultní nemocnice v Ostravě



**Středisko společných činností
Akademie věd ČR**

**Středisko společných činností
AVČR**

fond rozvoje cesnet
■■■■■

Motivace pro společný postup

Vycházeli jsme z myšlenky, že v oblasti bezpečnosti řešíme podobné problémy a máme na to (podobně) málo prostředků - vývojářů, obsluhy i techniky.



Sdílené problémy

Stejné bezpečnostní hrozby.

Omezené kapacity vývojářů a techniků.

Omezené kapacity dohledu.



Strategická autonomie

Klíčové kompetence musí být uvnitř organizací.



Otevřený a modulární systém

Společný pracovní tým a postupy.

Modularizované a škálovatelné řešení.

SW uvolněn jako open-source.

Fáze I: Rychlá reakce na hrozby (hasíme to, co nás nejvíc pálí)

Koho do řešení zapojit?

Nutná angažovanost a koordinace mnoha technicky kvalifikovaných osob. Roztříštěnost, pomalé reakce.



Rychlý a jednoduchý zásah

Kompetence nemusí mít seniorní technik, mohou vyhodnotit i operátoři HD.

Kde všude blokovat?

Další rozhodovací proces, kde všude se budou pravidla aplikovat?

Další zdržení, zdroj chyb.



Blokace v různých systémech

Automatická aplikace na firewallech, VPN, IPAM, mailových a antispam systémech, DNS/RPZ, RADIUS, AV/EDR, ...

Co teď a co potom

Složité životní cyklus pravidel.

Kdy, jak a kdo má pravidla rušit? Jak řešit opomenutí?



Životní cyklus pravidla

Řízená expirace, auditní historie (kdy, kdo, proč a do kdy).

Omezené reakce

Velmi omezené reakce mimo běžnou pracovní dobu.



Režim 24/7

Získali jsme schopnost reakce v režimu 24x7.

Systémy BANANA a CENBAN

Vyvinuli jsme relativně jednoduché a modulární aplikace BANANA a CENBAN.

Case ID ↑↓	Value ↑↓	Module ↑↓	Note ↑↓	Created ↑↓	Created by ↑↓	Mail to ↑↓	Notify ↑↓	Activate ban ↑↓	Delete ban ↑↓	External ID ↑↓	Delete ↑↓
mZ3MtleGBQLqOpj	142.252.236.231	bhr	fail2ban - radiator1	2026-09-30 12:26:22+02	vpn				2026-10-01 12:26:00+02		Delete
B0rYkwt9ZNqDgHm	172.120.12.213	bhr	fail2ban - radiator1	2026-09-30 12:18:01+02	vpn				2026-10-01 12:18:00+02		Delete
GFKVtX8RluhkiP6	155.212.77.151	bhr	fail2ban - radiator1	2026-09-30 12:15:16+02	vpn				2026-10-01 12:15:00+02		Delete
deWZ3cArztjmCIs	Opportunity to Publish Your Research	fortimail-subject-body		2026-09-30 12:12:33+02	wer022				2026-12-29 12:00:00+01		Delete
m3DZ9kyaMEFSGCI	editor049@scopusjournal.top	fortimail-from		2026-09-30 12:11:41+02	wer022				2026-12-29 12:00:00+01		Delete

BANANA

LOKÁLNÍ BLOKACE V ORGANIZACI

Správa blokad uvnitř organizace.

Delegace práv pro bezpečnostní tým a Helpdesk.

CENBAN

CENTRÁLNÍ SDÍLENÍ BLOKACÍ

Zadávat dat pro centrální dohled (IP, FQDN, URL).

Řízená distribuce do dalších lokálních instancí BANANA.

AUTOMATIZACE

Propojení na firewally, EDR, black-hole routing, DNS/RPZ, mailové služby, RADIUS atd.

Automatizovaná aplikace i revokace pravidel.

System BANANA – Uživatelské rozhraní



Give banana

Case ID* (leave empty for auto)

<Generate>

Value*

IP, domain name etc.

Module(s)*

Select modules

Note

Was sending out phishing

Delete ban (leave empty for permaban)

2026-12-29 12:00

Default

Submit

Rychlé zadání blokace

Jednoduchý formulář pro vložení závadné IP, URL nebo domény.

Přehledná auditní stopa

Okamžitý přehled: kdo, kdy a proč blokoval, expirace.

Fáze II: od reakce zpět k detekci (aneb cesta tam a zase zpátky)

„Už umíme i celkem rychle reagovat, ale chceme umět lépe detekovat.“

Centralizace logů

Rozšiřování SIEM platformy pro sběr dat.

Centrální systém pro organizaci i ostatní organizace (sdílení přináší úspory).

Širší záběr logování

Shadow IT, systémy řízení budov, fyzické bezpečnosti...

Ne-IT provozovatelé IT systémů

“My nejsme ajťáci, co po nás chcete?”

Logy? Reakce? My tu nejsme od toho!

Je toho hodně...

Logů je hodně, kdo se v tom má vyznat?

Fáze III: a chceme více informací (s jídlem roste chuť)



Potřebujeme asset management

Aktuální informace o zařízeních na jednom místě.

Vyvinut systém MUDRC s otevřeným REST API.

Specifika BYOD systémů.



Kde všude máme informace?

Moduly pro INTUNE, EDR, VMware, Nessus, Zabbix, vlastní skeny, ...

Automatizovaná aktualizace – žádné zbytečné zapojování dalších techniků.



Komu to bude k užitku?

CESNET – jeho bezpečnostní hlášení by mohla být doplněna o některé naše interní informace. Realizovaný PoC, který se používá v provozu.

Kdo má starý prohlížeč, office, Acrobat, ... ?

MUDRC má API a vrací informace

MUDRC vrací selektivně informace - podrobnější interním řešitelům, obecné třeba CESNETímu dohledu.

```
@timestamp: "2026-09-30T03:55:16.884525+00:00"
```

```
target: {  
  ipv4: [ "1.2.3.4" ],  
  ipv6: [ "2001:718:aaaa:bbbb::30", "fe80::250:56ff:fead:d9f9" ],  
  mac: [ "00:50:56:ad:d9:f9" ],  
  hostname: [ "aaa.domena.cz", "vm-82707" ],  
  last_seen: [ "2026-09-30 05:30:12 UTC+2:00" ],  
  subnet: [ "Provozni servery" ] },  
service: [  
  { protocol: "tcp", port: 22, version: "OpenSSH 9.2p1" }  
],  
person: { username: "mravenec", fullname: "Ing. Ferda Mravenec", role: [ "owner" ]  
}
```

MUDRC má API a vrací informace

MUDRC vrací selektivně informace - podrobnější interním řešitelům, obecné třeba CESNETímu dohledu.

. . .

```
software: {
```

1. [**"7-Zip 26.02 (x64 edition)"**, "26.02.00.0", "Igor Pavlov"],
2. [**"Adobe Acrobat (64-bit)"**, "26.002.21931", "Adobe"],
3. [**"Adobe Audition 2026"**, "26.5", "Adobe Inc."],
4. [**"Adobe Creative Cloud"**, "6.10.0.252.41", "Adobe Inc."],
5. [**"Adobe Illustrator 2026"**, "30.8.1", "Adobe Inc."],
6. [**"WinRAR 7.13 (64-bit)"**, "7.13.0", "win.rar GmbH"],

. . .

7. [**"YSoft SafeQ client components"**, "6.0.105.1", "Y Soft Corporation, a.s."],
 8. [**"Yubico Authenticator"**, "7.1.1", "Yubico AB"]
- ```
}
```

## Fáze IV: logů není nikdy dost (a kdo hledá, ten najde)



### Centrální SIEM

Spousty dat na jednom místě.

Co teď s nimi?

Blacklisty / whitelisty?

Korelace?

Kolik potřebujeme kapacit?

Jaký výkon?

Jaká je retence dat?



### Dedikovaná infrastruktura

Dedikované servery i diskové pole (\*).

Od provozu oddělené technologie.

(\*) Štěstí přeje připraveným, pole jsme koupili včas!



### Poskytování dat

Vlastníci a provozovatelé aktiv.

Bezpečnostní tým

IT Helpdesk.

Reporty.

Reakční utility (např. fail2ban).

Korelace.

(\*) "Lidé umí hledat, ale nevydrží..."

# Máte pocit, že řešíte podobné problémy?

Využijte vyvinuté nástroje BANANA, CENBAN, MUDRC, SIEM.

Nebo se s námi spojte.

---

Děkuji za pozornost.