

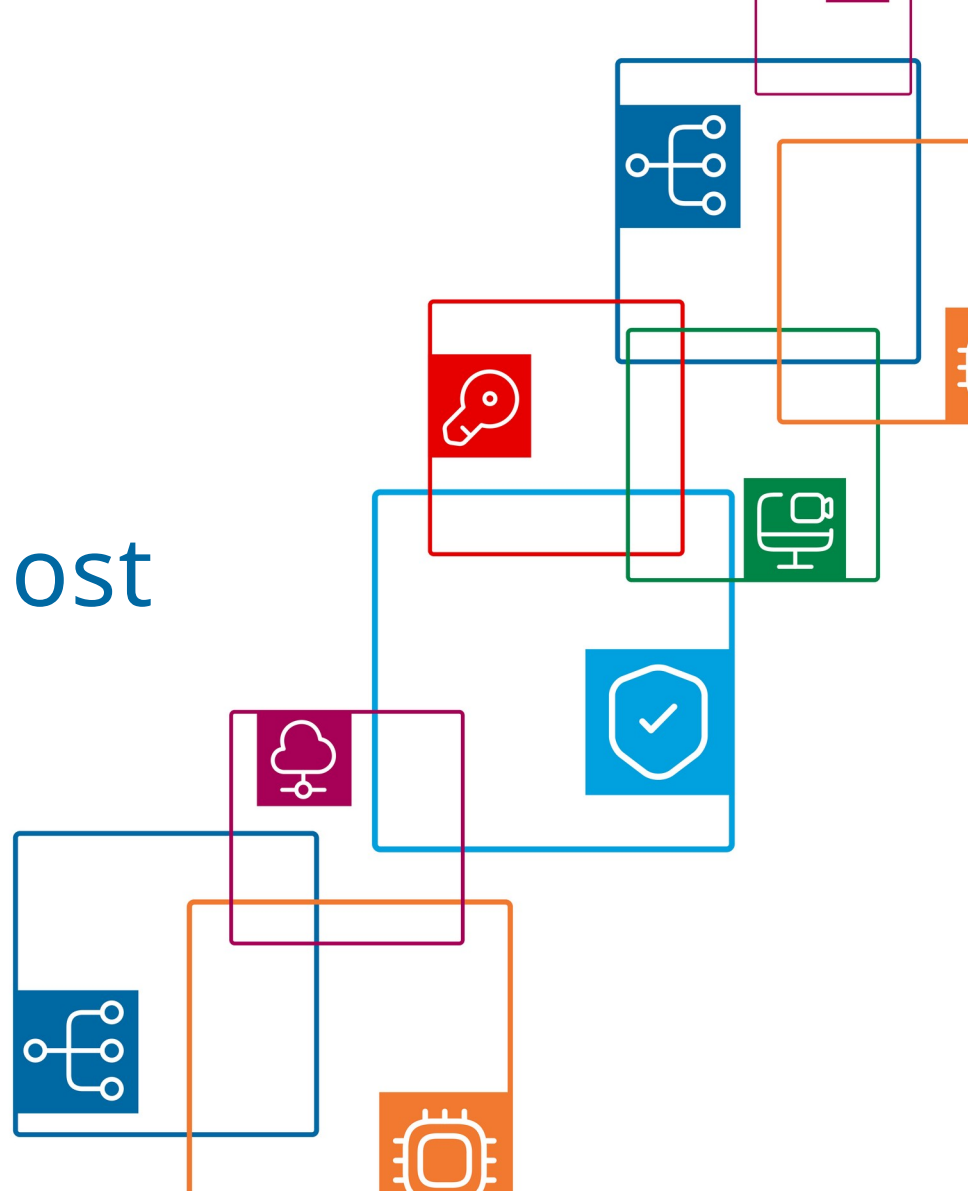


CESNET: (Ne)Bezpečnost

Andrea Kropáčová

30. 9. 2026, Praha

Konference e-infrastruktury CESNET

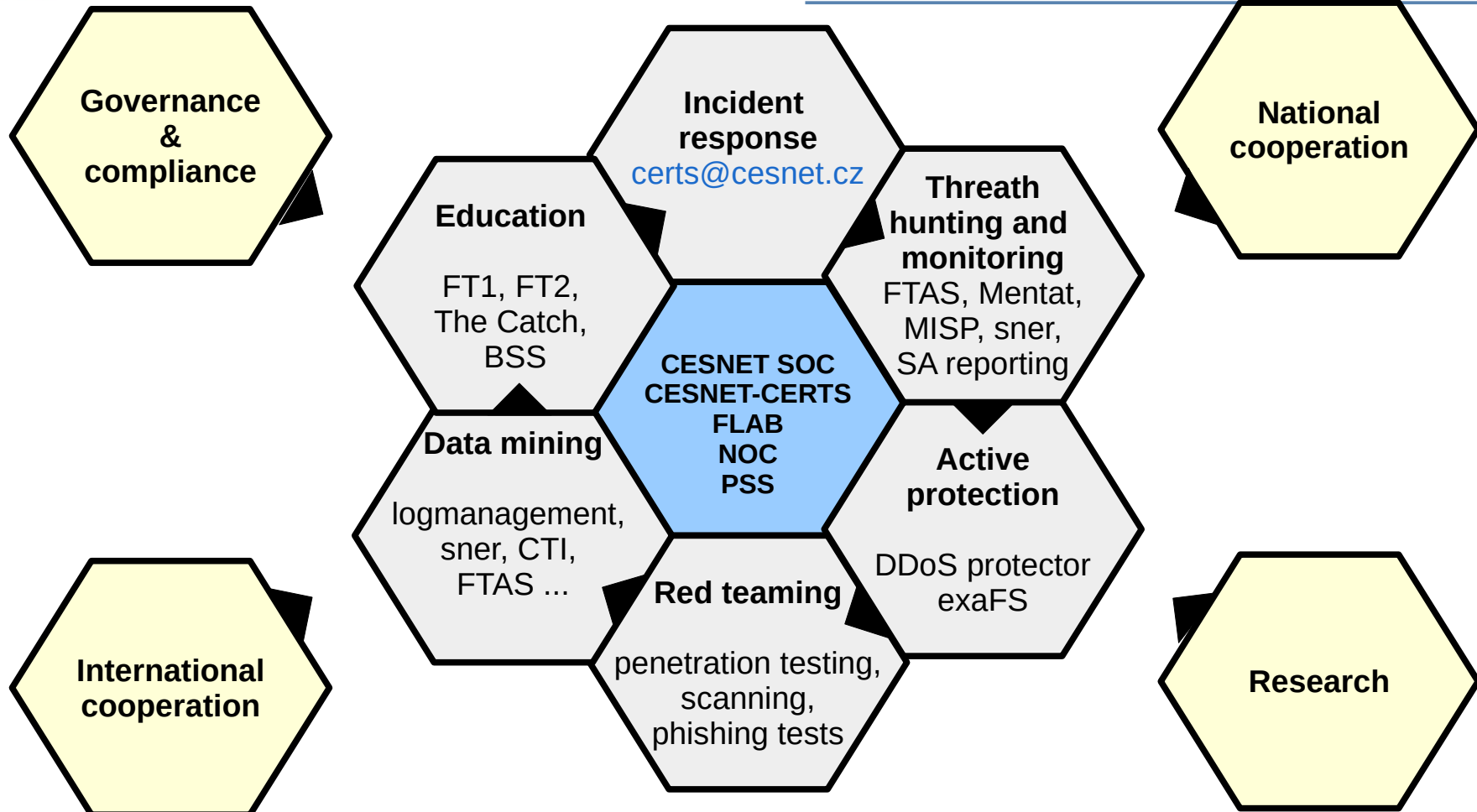


- Udržet e-infrastrukturu CESNET a služby v běhu, zabezpečenou a obrany schopnou
- Poskytnout správcům a připojeným organizacím ochranu na síťové úrovni a kvalitní portfolio bezpečnostních služeb
- Sdílet informace a know-how napříč komunitou, podporovat spolupráci, výměnu informací a vzdělávání



- Komplexní portfolio nástrojů a služeb pro monitoring sítě a služeb, detekci anomálií, regulaci provozu, analýzu a mitigaci
- Proaktivní i reaktivní přístup
- Data pro online i offline analýzu problémů
- Soubor postupů, metod, procesů, know-how
- ISMS jako formální rámec pro podporu bezpečnosti
- Efektivní týmy a pracoviště – PSS, NOC, CESNET-CERTS, FLAB, SOC
- Vysoce erudovaní správci
- Bohatá národní a mezinárodní spolupráce



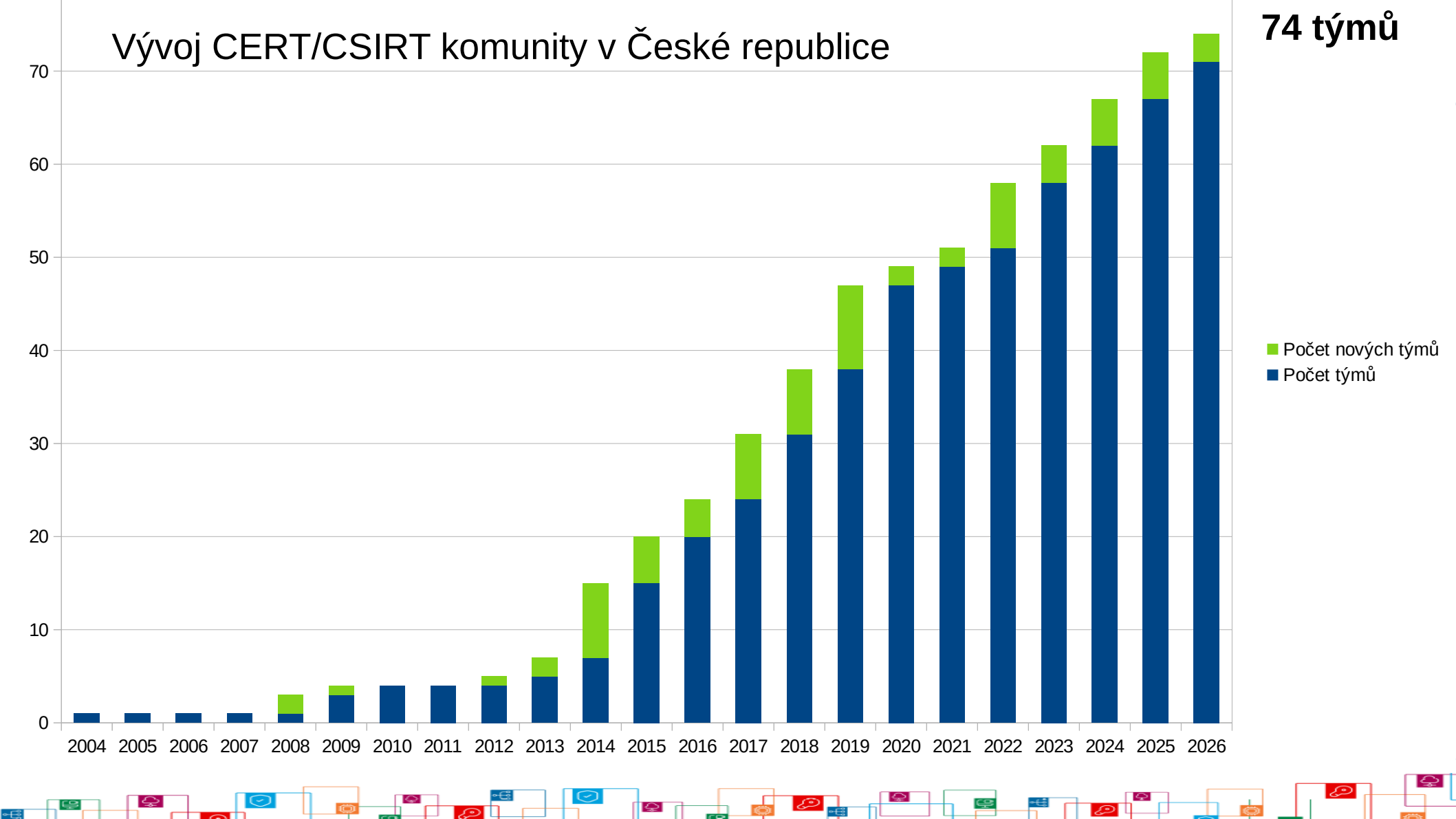




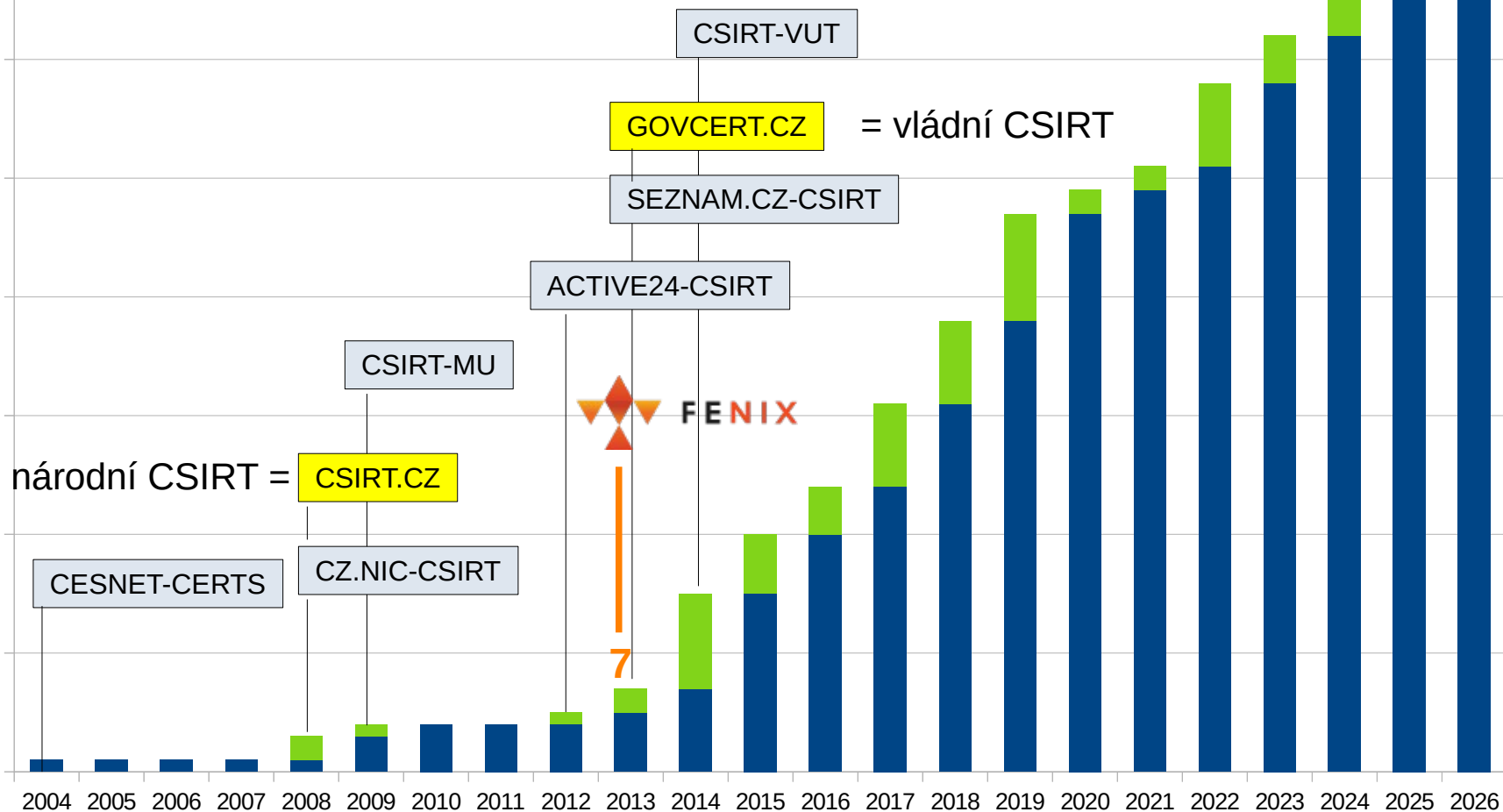
- Computer Security Incident Response Team
- 2004: status „listed“ od úřadu Trusted Introducer, člen TF-CSIRT
- 2008: status „accredited“ od úřadu Trusted Introducer
- 2026: v procesu certifikace
- Constituence (pole působnosti): AS2852 (e-infrastruktura CESNET)
- Kontaktní informace:
 - <https://csirt.cesnet.cz>
 - abuse@cesnet.cz, certs@cesnet.cz
- Typ: interní a koordinační
- Hlavní role/služba
 - řešení a koordinace řešení bezpečnostních incidentů
 - dostupnost: 9 – 17 v pracovních dnech

Vývoj CERT/CSIRT komunity v České republice

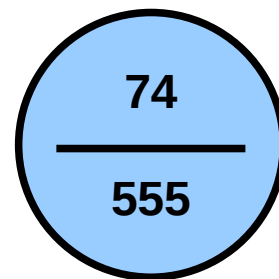
74 týmů



Vývoj CERT/CSIRT komunity v České republice



74 týmů



Počet nových týmů
Počet týmů

~ 5mil. KBU denně (z detekčních systémů CESNET)

- 40 000 je zpracováno...
- ... a zagregováno do cca 20 reportů pro 326 bezpečnostních týmů v e-infrastruktuře CESNET

Systematický scanning e-infrastruktury CESNET:

	CESNET	Customers	Global
Hosts	3266	24785	28051
Services	11928	43835	55763
Vulnerabilities	103857	99512	203339

Situational awareness – sledování zranitelností a informování o nich:

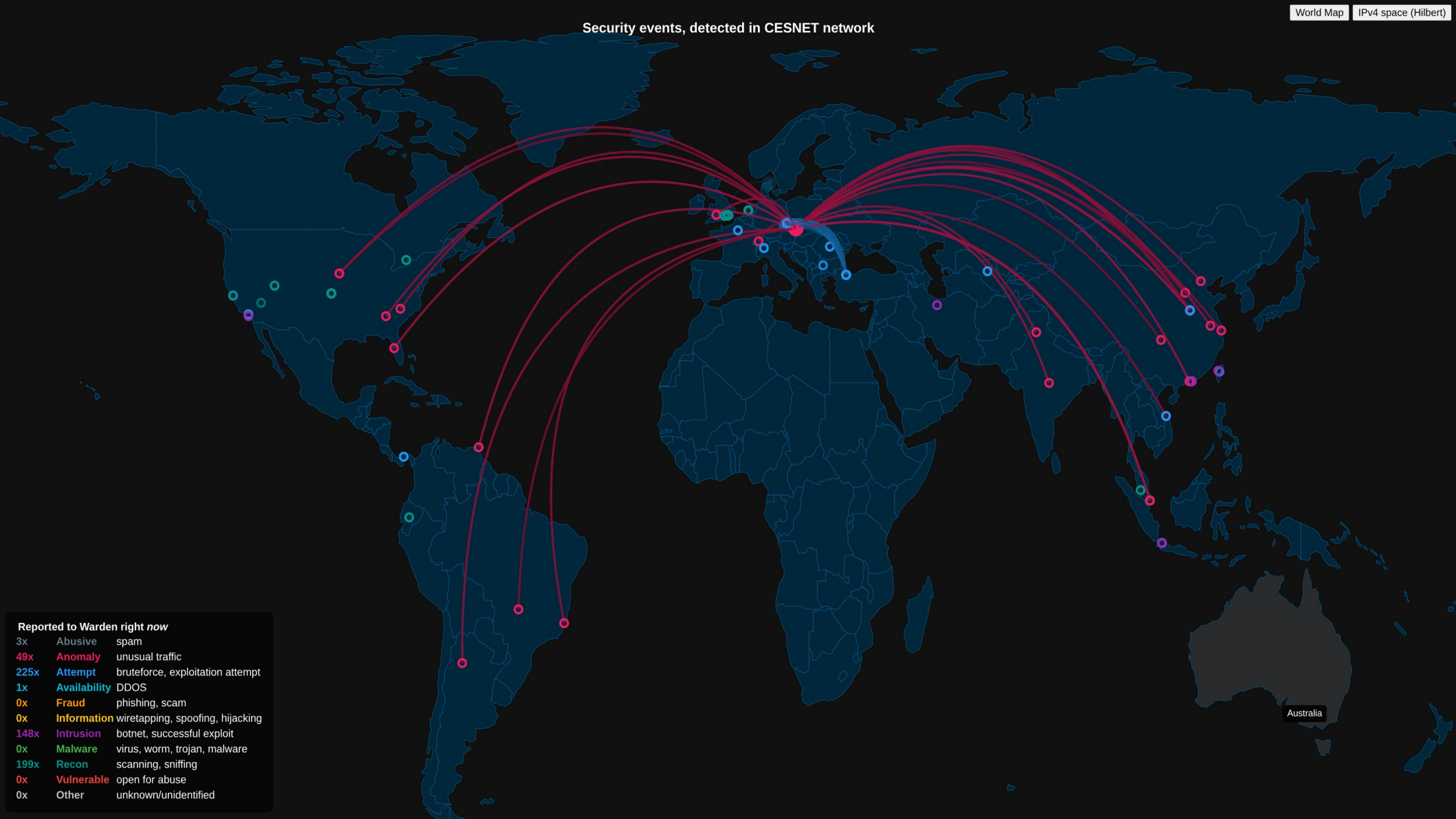
- 411 odběratelů (týmů a jednotlivců)
- csirt-forum@, hsoc@, csirt-cz@, cyberfeed.cesnet.cz
- ~ 1300 reportů (od února 2022)

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	sum	
Fraud.Copyright	3	28	94	619	929	565	314	388	680	639	4382	4812	2222	576	876	868	938	625	350	263	80	20251	
- Uncategorized -	34	194	101	393	341	511	2199	4555	2635	394	3630	961	124	235	73	341	37	25	38	15	12	16848	
Abusive.Spam	121	905	535	799	244	214	193	175	515	801	1324	205	167	162	67	55	255	127	87	201	60	7212	
Other	1	1	4	12	36	24	1611	13	91	1201	283	121	42	20	90	1649	409	17	33	36	8	5702	
Recon.Scanning	6	71	52	72	124	56	58	73	35	160	126	352	253	413	2088	162	229	90	105	55	16	4596	
Anomaly.Traffic										97	319	1		2029	1623	2	19	1	9	64	256	4420	
Availability.DoS			6	1	4	3	8	2	1	4093	152	3	3	3	6	2		1	1	1	3	2	4295
Vulnerable.Config										2066	855	275	18	33	101	8	3	61	30	84	120	46	3700
Intrusion.Botnet			12	5	34	2	13	2	2	356	61	21	60	79	26	12	20	34		7	3	749	
Availability.DDoS			15	8		1	18	7	82	21	96	14	1	12	17	19	50	56	52	22	14	4	509
Fraud.Phishing		2	11	24	10	25	39	13	46	12	7	9	10	13	11	5	9	13	15	7	11	5	297
Vulnerable.Open																							
Malware.Trojan			28	13	14	1								1	1	4	8	31	46	84	88	21	287
Attempt.Exploit																							
Attempt.Login																							
Intrusion.UserCompromise		6	32	5	13	2	2	1	6		1			2	4	7	1	2	61	2	13	11	121
Anomaly.Connection																							
Intrusion.AppCompromise							1			5													
Vulnerable																							
Fraud.UnauthorizedUsage																					1	4	5
Intrusion.AdminCompromise																					1		3
Anomaly.Behaviour														1								1	2
Anomaly.Protocol																						1	1
Fraud.Masquerade					1																	1	1
Information.UnauthorizedModification																							
sum	173	1303	848	1983	1727	1453	4402	5352	10526	4477	10414	6551	2958	3620	4887	3200	2117	1123	858	908	531	69411	

1000 KBU processed manually per year

Security events, detected in CESNET network

World Map IPv4 space (Hilbert)



Reported to Warden right now

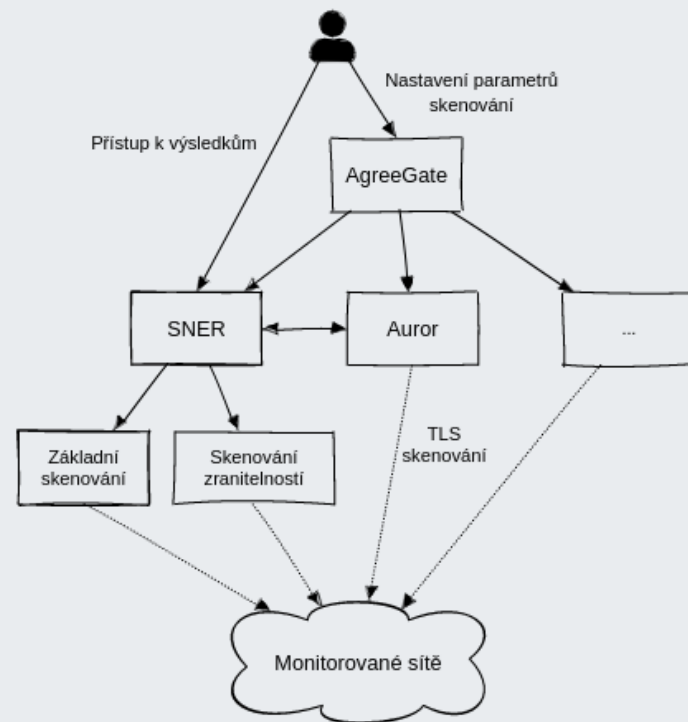
3x	Abusive	spam
49x	Anomaly	unusual traffic
225x	Attempt	bruteforce, exploitation attempt
1x	Availability	DDOS
0x	Fraud	phishing, scam
0x	Information	wiretapping, spoofing, hijacking
148x	Intrusion	botnet, successful exploit
0x	Malware	virus, worm, trojan, malware
199x	Recon	scanning, sniffing
0x	Vulnerable	open for abuse
0x	Other	unknown/unidentified

Služba Skenování sítě

Kdo slyší první varování, nemusí hasit poslední požár.

AgreeGate

SNER



Skenování sítě je sada proaktivních nástrojů pro monitorování sítí, kterou provozuje sdružení CESNET za účelem zajištění bezpečnosti v e-infrastruktuře CESNET2.

Cílem je získat informace o provozovaných síťových službách a následně jejich využití při identifikaci potenciálně zranitelných zařízení anebo služeb. Služba je jedním z nástrojů na podporu zajištění bezpečnosti infrastruktury připojené organizace. Zároveň napomáhá zvyšovat bezpečnost celé e-infrastruktury CESNET.

Provozované nástroje nepřetržitě mapují zapojené sítě, provádí detekci dostupných služeb a fingerprinting podobný tomu, jaký nabízejí služby jako Shodan, Censys nebo Shadowserver. Administrátoři skenovaných sítí mohou s využitím této služby získat lepší přehled o svém adresním prostoru a případně i včasné varování před možnými zranitelnostmi.

CESNET CyberFeed – reporty o zranitelnostech

Tato služba je blíže popsána na webu [CESNET-CERTS](#).



Bezpečnostní služby poskytované organizací CESNET jsou navrženy jako významná podpora při zajišťování kybernetické bezpečnosti připojených organizací. Přestože usilujeme o poskytování absolutní pokrýtky všech bezpečnostních zranitelností. Naše služby by měly být vnímány jako doplněk k vlastnímu bezpečnostnímu řízení organizací, nikoli jako jeho náhrada. Klientského prostředí.

Vyhledat



Citrix opravuje 8 zranitelností Max CVSS 9.5 (Critical)

Publikované dňa 29. 9. 2026.



Prehľad zaujímavých zranitelností

Publikované dňa 25. 9. 2026.



OpenStack opravuje 6 zranitelností vo svojich produktoch Max CVSS 9.4 (Critical)

Publikované dňa 25. 9. 2026.



WordPress opravuje aktívne zneužívanú zraniteľnosť Max CVSS 9.2 (Critical)

Publikované dňa 24. 9. 2026.



GitLab opravuje 11 zranitelností Max CVSS 9.9 (Critical)

Publikované dňa 24. 9. 2026.



SolarWinds opravuje 3 zranitelnosti Max CVSS 9.8 (Critical)

Publikované dňa 23. 9. 2026.



F5 BIG-IP opravuje aktívne zneužívanou zranitelnost Max CVSS 9.3 (Critical)

Publikováno dne 23. 9. 2026.



Arista opravuje aktívne zneužívanú zraniteľnosť Max CVSS 9.5 (Critical)

Publikované dňa 23. 9. 2026.

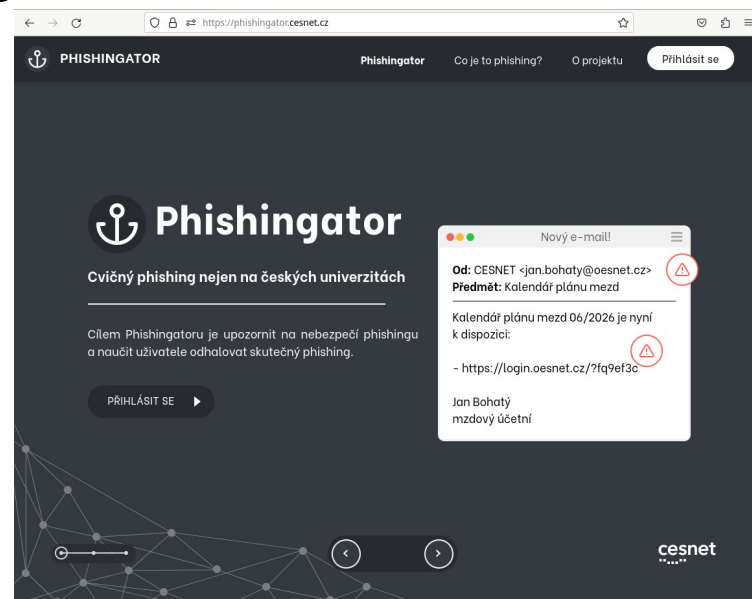
	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	sum
Fraud.Copyright	3	28	94	619	929	565	314	388	680	639	4382	4812	2222	576	876	868	938	625	350	263	142	20313
- Uncategorized -	34	194	101	393	341	511	2199	4555	2635	394	3630	961	124	235	73	341	37	25	38	15	16	16852
Abusive.Spam	121	905	535	799	244	214	193	175	515	801	1324	205	167	162	67	55	255	127	87	200	79	7230
Other	1	1	5	12	36	24	1611	13	91	1201	283	121	42	20	90	1649	409	17	33	36	20	5715
Recon.Scanning	6	71	52	72	124	56	58	73	35	160	126	352	253	413	2088	162	229	90	105	55	26	4606
Anomaly.Traffic										97	319	1		2029	1623	2	19	1	9	64	273	4437
Availability.DoS		6	1	4	3	8	2	1	4093	152	3	3	3	6	2		1	1	1	3	4	4297
Vulnerable.Config									2066	855	275	18	33	101	8	3	61	30	84	119	139	3792
Intrusion.Botnet		12	5	34	2	13	2	2	356	61	21	60	79	26	12	20	34		7	3	2	751
Availability.DDoS		15	8		1	18	7	82	21	96	14	1	12	17	19	50	56	52	22	14	5	510
Vulnerable.Open						1		1	2			1	1		4	8	31	46	84	88	61	328
Fraud.Phishing	2	11	24	10	25	39	13	46	12	7	9	10	13	11	5	9	13	15	7	11	15	307
Attempt.Exploit					1						1	4	4	16	11	28	28	25	22	13	3	156
Malware.Trojan		28	19	24	14		2	9	13	12	1	1	2	3	1	2	4	7	2	4	6	154
Attempt.Login				2	5	1		1	2	1	6		2	4	7	1	2	61	2	13	18	128
Intrusion.UserCompromise	6	32	5	13	2	2	1	6		1				1	1	1		1	2	2	2	78
Anomaly.Connection											20	1									1	22
Intrusion.AppCompromise						1			5												1	7
Vulnerable																				1	3	4
Fraud.UnauthorizedUsage																1			1	1	1	4
Intrusion.AdminCompromise													1								1	2
Malware																					2	2
Anomaly.Behaviour																				1		1
Abusive																				1		1
Anomaly.Protocol																			1			1
Fraud.Masquerade				1																		1
Information.UnauthorizedModification																			1			1
sum	174	1303	849	1983	1727	1453	4402	5352	10526	4477	10414	6551	2958	3620	4887	3200	2117	1123	858	907	820	69701

- Speciální jednotka pro CESNET-CERTS
- 2011: start
- 2014: spuštění prvních služeb
- Poskytované služby (nadstavbové)
 - Analýzy závažných bezpečnostních incidentů
 - Penetrační testy
 - Testy sociálního inženýrství („phishingové testy“)
 - Služba Phishingator
 - Služba netscan (systematické scanování sítě)

<https://flab.cesnet.cz>

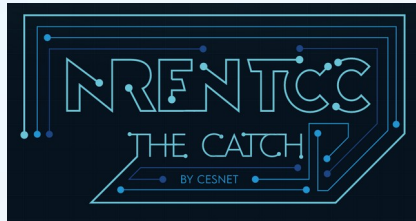


- Webová aplikace pro automatizované **rozesílání cvičných phishingových zpráv**
- Původně **bakalářská práce na ZČU** (2019), nyní OpenSource
- **CESNET poskytuje formou Software as a Service**
 - Technicky se nemusíte o nic starat
 - Phishingator napojíme na Vaši organizaci
 - Každá organizace = **vlastní instance Phishingatoru**
- Praktický doplněk ke školení „kdykoliv a kdekoliv“
 - Přímá **konfrontace** s phishingem
 - **Cílené školení** uživatelů
 - **Zpětná vazba pro uživatele** o absolvování cvičného phishingu



- Monitoring a obranu páteře
 - s možností přísnějších pravidel na přípojce (perimetru)
 - s možností samoregulace
 - hSOC VRF
- Monitoring zájmového provozu – kryptomining, DeepSeek, zajímavé „on-demand“
- Hlášení KBU, pomoc se zvládáním KBU (by CESNET-CERTS/SOC)
- Penetrační testování, sledování zranitelností
- Bezpečnostní data – Mentat, NERD, pDNS, netscan.cesnet.cz
- Zvyšování odolnosti uživatelů – phishingové testy, Phishingator
- Edukace a spolupráce
 - seminář o bezpečnosti sítí a služeb (aka BSS)
 - FT1 a FT2, pracovní skupiny





The Catch, start 5. října ve 14:00

Oblíbená tematická CTF soutěž startuje 5. října ve 14:00. V roce třicátého výročí sdružení CESNET vás The Catch zavede do světa národní výzkumné a vzdělávací sítě (NREN). Úlohy v soutěži The Catch vycházejí z principu Capture the Flag (CTF). Soutěžící hledají ukryté řetězce, tzv. flagy. Kromě otestování vlastních schopností můžete získat také zajímavé ceny. www.thecatch.cz

Forenzní trénink I a II

Termín: 25.–26. května 2027 FT I, 27.–28. května 2027 FT II

Místo: TELEHOUSE, CESNET, Modrá zasedací místnost

Jak postupovat při bezpečnostní události, abyste nepřišli o důležité stopy a dokázali přesně zjistit, co se stalo? Na praktických školeních Forenzní trénink I a II získáte důležité odpovědi, a především si sami vyzkoušíte, jak na to – od správného zajištění dat až po jejich analýzu v konkrétních scénářích. Čeká vás práce v počítačové laboratoři, reálné situace z praxe i kombinace metodického výkladu s hands-on cvičeními.



Seminář o bezpečnosti sítí a služeb 2027

Termín: 2.–3. února 2027

Místo: Hotel Pyramida, Praha 6

Na začátku února se uskuteční tradiční dvoudenní Seminář o bezpečnosti sítí a služeb. Zaměříme se na aktuální témata z kybernetické bezpečnosti, správy sítí a moderních technologií. Akce nabídne přednášky věnované monitoringu, řešení incidentů i vývoji a provozu služeb sdružení CESNET. Poznamenejte si tento termín do kalendáře.

Seminář o bezpečnosti sítí a služeb 2027

Termín: 2.–3. února 2027

Místo: Hotel Pyramida, Praha 6

Na začátku února se uskuteční tradiční dvoudenní Seminář o bezpečnosti sítí a služeb. Zaměříme se na aktuální témata z kybernetické bezpečnosti, správy sítí a moderních technologií. Akce nabídne přednášky věnované monitoringu, řešení incidentů i vývoji a provozu služeb sdružení CESNET. Poznamenejte si tento termín do kalendáře.

Call for papers!!!

Máte zajímavé téma a jste ochotni vystoupit? Kontaktujte nás!

- ISMS (Systém řízení bezpečnosti informací)
 - soubor pravidel zajišťující bezpečnost informací (dostupnost, důvěrnost a integritu)
- Dva formální rámce
 - ČSN EN ISO/IEC 27001:2023
 - 2015 – rozhodnutí o zavedení ISMS
 - 2018 – certifikace
 - zákon o kybernetické bezpečnosti (od 1. 11. 2025 zákon č. 264/2025 Sb.)
 - 2015 – povinný subjekt
 - 2022 – prvek KII
 - 2026 – provozovatel regulovaných služeb
 - 16.8 **Poskytování služby cloud computingu** (odvětví: Digitální infrastruktura a služby)
 - 19.1 **Výzkum a vývoj** (odvětví: Věda, výzkum a vzdělávání)

- Teorie a praxe nového zákona o kybernetické bezpečnosti (TaPnZKB)
 - 8. díl – 23. září 2026
 - říjen – listopad 2026
 - due dilligence, nástroje pro zpracování DB aktiv a rizik
 - zpracování KBU a KBI (ve spolupráci s NÚKIB)



Protivliv
Due diligence
Institucionální odolnost



Zákon č. 328/2025 Sb., o výzkumu, vývoji, inovacích a transferu znalostí

§ 7 - Institucionální odolnost

(1) Příjemce institucionální podpory je povinen zajistit institucionální odolnost proti vlivovému působení cizí moci, kybernetickou a informační bezpečnost a dodržování předpisů a pravidel týkajících se ochrany duševního vlastnictví, mezinárodních kontrolních režimů a mezinárodních sankcí, a to v souladu se zásadou tak otevřeného přístupu k výsledkům, jak je jen možné.



- **Období:** 10/2026 do 10/2027
- **Členský poplatek 60 000,-**
- **Počet requestů**
 - 25 fyzických osob
 - 5 právnických osob
 - Vyšší náročnost
 - **evoluce** – možnost modifikace requestů, budování znalostní báze a sdílení
- **Výstupní zpráva**
 - datový výstup – základní výpis zjištěných informací, uvedení zdrojů
 - analytická zpráva – vyhodnocení zjištění v kontextu v kontextu konkrétního účelu



- www.cesnet.cz - služby, akce, VaV
- sluzby@cesnet.cz - péče o uživatele
- csirt-forum@cesnet.cz - informace z oblasti bezpečnosti, informace o akcích
- **<https://www.cesnet.cz/bezpecnost> - kybernetická bezpečnost by CESNET**
- <https://csirt.cesnet.cz> – bezpečnostní tým CESNET-CERTS
- <https://flab.cesnet.cz> - forenzní laboratoř
- <https://phishingator.cesnet.cz> - služba cvičného phishingu
- <https://cyberfeed.cesnet.cz> – informace o zranitelnostech
- <https://netscan.cesnet.cz> - skenování sítí
- <https://mentat.cesnet.cz> - kybernetické bezpečnostní události
- <https://warden.cesnet.cz> - sběr kybernetických bezpečnostních událostí
- <https://www.thecatch.cz> - soutěž CTF
- <https://hugo.cesnet.cz> - honeypoty v e-infrastruktuře CESNET
- <https://nerd.cesnet.cz> - reputace síťových entit

csirt-forum-subscribe@cesnet.cz



Děkuji za pozornost.

Zítra na viděnou na bezpečnostním
tracku!

Andrea Kropáčová, andrea@cesnet.cz