cesnet

BEZPEČNOST

TLP: AMBER

Andrea Kropáčová
CESNET

1. 2. 2023
Praha

Hlavní mise

1) Udržet e-infrastrukturu CESNET a služby v běhu, zabezpečenou a obrany schopnou
2) Poskytnout připojeným organizacím bohaté portfolio bezpečnostních služeb
3) Sdílet informace a know-how napříč komunitou, spolupracovat

Prostředky

- Bohaté a komplexní portfolio nástrojů a služeb pro monitoring, detekci anomálií, analýzu, mitigaci ...
- Data pro online i offline analýzu
- Soubor postupů, metod, procesů ... know-how ...
- Připravené a otestované mechanismy pro zásah
- Efektivní týmy a pracoviště – PSS, NOC, CESNET-CERTS, FLAB
- Gramotní správci

Bezpečnostní služby CESNET

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Bezpečnostní služby CESNET

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Bezpečnostní služby CESNET

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Strategie v oblasti zajištění provozu a obrany sítě

- Transparentní přístup
- Žádné zásahy/omezování legitimního provozu
- V případě problému se rozhodujeme na základě vyhodnocení konkrétní situace
- V případě ohrožení stability infrastruktury zasahujeme
- V případě žádosti uživatele můžeme nastavit regulaci v páteři pro koncovou síť (nepodstatná anomálie z perspektivy páteře může být likvidační pro chod koncové sítě)

Bezpečnostní monitoring

- **FTAS (Flow Trafic Analysis System)**
  - Detekce pro základní síťové útoky a anomálie (základní principy)
    - události mající původ uvnitř připojené sítě – notifikujeme
    - události směrem dovnitř připojené sítě – regulujeme, blokujeme, zahazujeme
      - automaticky ovládá exaFS
- **Služba FTAS** (3 varianty)
  1. zpřístupnění dat týkající se konkrétní instituce (z hraničních boxů), uvidíte provoz, který protekl infrastrukturou, tj. provoz mezi „námi a vámi“
  2. export vlastních dat do hlavní instance (exkluzivní přístup pouze v vlastním datům konkrétní připojené organizace)
  3. dedikovaná instance v síti organizace (typicky velké univerzity)

- **Služba exaFS** – rozhraní pro aplikaci BGPflowspec a RTBH
  - regulace provozu ***z*** nebo ***do*** prefixů připojených organizací
  - webový i-face, nebo API pro strojové ovládání
  - součástí je proškolení uživatele
  - sluzby@cesnet.cz

Bezpečnostní služby CESNET

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Spolupráce v CSIRT komunitě e-INFRA

- Propojuje týmy i jednotlivce,
- každý se může zapojit se svou expertízou, zkušeností, nalezenou zranitelností,
- každý může požádat o radu, konzultovat svou bezpečnostní situaci.

Forma moderovaného mailing listu

- Nejdůležitější informace v kompaktní formě,
- obvykle 1 příspěvek denně,
- **zápis mailem na adresu csirt-forum-subscribe@cesnet.cz**

Informace k aktuálním hrozbám (Situational Awareness)

- ověřené, důvěryhodné a ozdrojované
- strukturovaná data o zranitelnostech, typech útoků a rizicích,
- doporučení mitigací a řešení limitujících dopady hrozeb.

Spolupráce v CSIRT komunitě e-INFRA

- Propojuje týmy i jednotlivce,
- každý se může zapojit se svou expertízou, zkušeností, nalezenou zranitelností,
- každý může požádat o radu, konzultovat svou bezpečnostní situaci.

Forma moderovaného mailing listu

- Nejdůležitější informace v kompaktní formě,
- obvykle 1 příspěvek denně,
- **zápis mailem na adresu csirt-forum-subscribe@cesnet.cz**

Informace k aktuálním hrozbám (Situational Awareness)

- ověřené, důvěryhodné a ozdrojované
- strukturovaná data o zranitelnostech, typech útoků a rizicích,
- doporučení mitigací a řešení limitujících dopady hrozeb.

Příklad příspěvku:

Dobrý den,

v oblíbeném nástroji **Splunk**, konkrétně ve verzi Enterprise, byla objevena **kritická zranitelnost** (CVSS nespecifikováno) [1] v nástroji "Deployment server", která se stará o distribuci konfigurací a může obsahovat i binární soubory. Ty pak mohou být staženy a spuštěny Splunk Universal Forwardery či dalšími instancemi Splunk Enterprise. Pokud by došlo ke kompromitaci jediného SUF, útočník by mohl rozšířit modifikovanou konfiguraci se škodlivým obsahem na všechny ostatní SUF.

Doporučení:

Řešením je aktualizace na Splunk v.9 [2], který je však velmi mladá - světlo světa spatřila teprve před dvěma dny. Pro ostatní verze zatím nebyla oprava vydána.

Workaround:

Další možností je vypnout Deployment server a zapnout jej v momentě, kdy je třeba distribuovat novou konfiguraci. K tomu slouží příkaz:

$ /opt/splunk/bin/splunk disable deploy-server

Poté je ještě třeba Splunk restartovat, aby došlo k přerušení již navázaných spojení s Deployment serverem.

Identifikátor zranitelnosti:

CVE-2022-32158 (CVSSv3 skóre nebylo stanoveno) [1]

Tuto zranitelnost popsal Bojan Zdrnja na webu SANS [3].

Zdroje:

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32158
[2] https://www.splunk.com/en_us/product-security/announcements/svd-2022-0608.html
[3] https://isc.sans.edu/diary/rss/28760

cesnet Seminář o bezpečnosti – 7. 2. 2023

Program:

8:30 – 9:00 Registrace

9:00 – 9:10 **Přivítání a úvodní slovo**
Andrea Kropáčová

9:10 – 10:00 **(Ne)bezpečnost 2022**
Radoslav Bodó, Jakub Urbanec
Standardní příspěvek se bude již poněkolikáté věnovat stavu informační bezpečnosti. Dozvíte se, jaké průšvihy se v roce 2022 udály ve světě IT.

10:00 – 10:30 **FTAS as a service**
Tomáš Košňar
Varianty využití systému FTAS pro sítě uživatelů. Od služby základního zpracování, uložení a zpřístupnění informací o provozu vlastní sítě až po sestavení schématu automatické obrany proti síťovým útokům.

10:30 – 11:00 **Role SOC v organizaci**
Jan Kolouch, Andrea Kropáčová
Security Operation Centre (SOC), je řešením, které musíte mít a bez kterého v současné době není informační a kybernetickou bezpečnosti řešit. Je tomu skutečně tak? Vyřeší za vás SOC vaše problémy? Jaká je vlastě role SOC a organizace?

11:00 – 11:30 **Situational Awareness – zranitelnosti jak je neznáte**
Mirek Sochor
Proč je dobré mít přehled o aktuálních hrozbách nejen v online prostoru a jak jsme tento nelehký úkol uchopili v rámci služby CSIRT-FORUM@.

11:30 – 12:30 Oběd

12:30 – 13:20 **Asset (IT INVENTORY) management**
Dan Tovarňák (CSIRT-MU)
Dobře zvládnutý asset management je jeden ze základních atributů pro zvládnutí bezpečnosti. Probereme, jak by tato oblast mohla a měla vypadat v prostředí vysoké školy.

FA1/FA2 školení

- Hands-on školení v laboratoři pod vedením zkušených školitelů (by FLAB)
- Základy forenzní analýzy digitálních dat
- 2 dny, plus Forensic Night@CESNET

- FA1: *Zajišťování dat, vytváření časové osy ze souborového systému, následná analýza, identifikování jednotlivých stopy vedoucích k vytvoření komplexního obrazu analyzovaného incidentu. Prezentování výsledků jako součást tréninku.*
- FA2: *Analýza síťového provozu, teoretický úvod do problematiky, seznámení s postupy pro zajištění podkladů, analýzou toků v sítích (netflow) a analýzou částečného i plného záznamu provozu (packet capture). Součástí školení je také seznámení s jednotlivými nástroji používanými pro analýzu.*

- **6. - 10. března 2023**
- **5. - 9. června 2023**

The Catch

- Hra/soutěž/školení na bázi CTF (Capture The Flag)
- CESNET příspěvek k Měsíci Kybernetické Bezpečnosti (říjen)
- Sada úloh na bázi analýzy logů, kódu, šifrování ...
- The Catch 2023 bude!

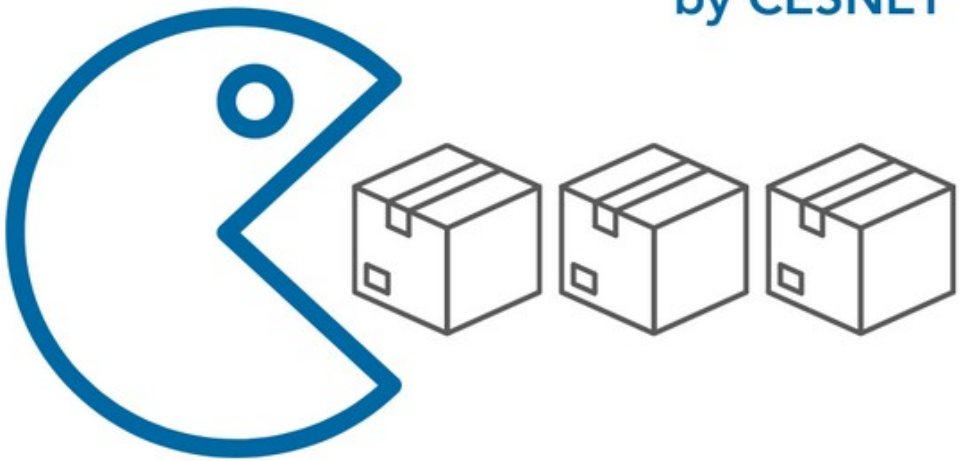
... Kdo si hraje, nezlobí :-)...

cesnet

The Catch, www.thecatch.cz

The Catch 2022 Write-ups Awards VPN Users Scoreboard Challenges Register Login

The Catch – Catch the packet
by CESNET



Main competition is over, however you can still join and play!

Through the organization of the annual Catch competition, we endorse the ideas of the **Cyber Security Month in 2022**, thus contributing to building a more secure Internet environment and cyberspace. The competition is organised by the CESNET Association.

We are hiring!

Announcements

- The write-up winners were published

cesnet

Phishingator

Služba Phishingator je webová aplikace, jejímž cílem je provádět praktické školení uživatelů v oblasti phishingu a sociálního inženýrství, a to odesíláním cvičných phishingových e-mailů.

Phishingator je navržen jako co nejvíce intuitivní a automatizovaný systém tak, aby jeho používání nevyžadovalo téměř žádné technické znalosti. Součástí systému je vedení jak globální, tak osobní statistiky u každého z uživatelů, a také vedení podrobné statistiky u každé phishingové kampaně.

Standardní služba Phishingator obsahuje:

- provoz a správa služby na prostředcích CESNET
- podpora služby – Helpdesk
- 3x registrace domény pro cvičnou podvodnou stránku
- 3x příprava podvodné stránky
- 3x příprava vzorového podvodného e-mailu
- neomezený počet phishingových kampaní

Bezpečnostní služby CESNET

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Služby Forenzní laboratoře

- Analýza událostí

https://flab.cesnet.cz

- Plošné testy e-infrastruktury na zranitelnosti
  - heartbleed, memcached, shellshock ...

- Penetrační testy
- Zátěžové testy
- Testy sociálního inženýrství („phishingové testy“)
  - na míru zákazníkovi

- Zadání --> Testy --> Zpracování --> Závěrečná zpráva & workshop
  - přehled provedených testů
  - zhodnocení výsledků (nálezů)
  - doporučení nápravných opatření
  - školení pro uživatele

Bezpečnostní služby CESNET

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

SNER Instance

Slow Network Recon Service (SNER)

SNER is proactive network monitoring service operated by CESNET for network security and research purposes in CESNET2 network.

Service continuously maps enrolled networks and performs service discovery and fingerprinting similarily to Shodan, Censys and Shadowserver services. Participating networks can leverage extended visibility of their address space and might benefit in early warnings of possible vulnerabilities.

- Github project: https://github.com/bodik/sner4
- Scanning sources: dynamic, identifiable via DNS as snerXX.flab.cesnet.cz.
- Scanning techniques:
  - IP enumeration
  - DNS enumeration
  - TCP SYN scan
  - UDP service discovery
  - service version fingerprinting
  - JA3/JARM scanning
  - TLS scanning

https://sner.flab.cesnet.cz/

Entrollment procedure

TBD

Data access

See service OpenAPI or Swagger documentation

Contact

Email: flab@cesnet.cz

SNER cesnet

Bezpečnostní služby CESNET

Služba	Oblast využití
FTAS – sledování provozu sítě	Máš k dispozici skupinu nástrojů pro monitoring síťového provozu a obranu. Budeš automaticky pod obrannými mechanismy, které má CESNET aplikovány na globálním perimetru a na páteří a na tvém perimetru ti tvou obranu ještě pomůžeme individualizovat.
exaFS – regulace provozu sítě	
FTAS a exaFS – monitoring a obrana	
csirt-forum@ - zapoj se do komunity	Máš k dispozici sadu prostředí, školení a cvičení, které ti pomohou s neustálým vzděláváním tvých zaměstnanců a uživatelů.
csirt-forum@ - situational awareness	
Seminář o bezpečnosti (každoročně)	
Školení FT1 a FT2	
The Catch	
Pracovní skupiny CESNET CSIRT	
Phishingator	
Penetrační testy	Máš k dispozici nástroje pro otestování stavu zabezpečení své infrastruktury, zdatnosti svých pracovníků, stavu svých procesů.
Zátěžové testy	
Analýza bezpečnostního incidentu	
Scan sítě na zranitelnosti (sner4)	Když nás necháš scanovat svoji síť, pomůžeme ti s vulnerability assesmentem a budeš lépe připraven na situaci, kdy se objeví nová zranitelnost, kterou je potřeba urychleně adresovat.
Individuální scan sítě nástrojem Nessus	
Mentat	Předáváme ti veškeré bezpečnostní události, které detekujeme, a které mají vztah ke Tvé síti. A pokud se zapojíš do komunitního sdílení dat (a dáš nám data ze svých bezp. nástrojů) pomůžeš sobě i ostatním.
HaaS	
NERD	A máš k dispozici řadu dalších nástrojů, které Ti mohou pomoci v zajišťování bezpečnosti, hledání informací, souvislostí při řešení bezpečnostních problémů a jejich předcházení
Passive DNS	

Warden & Mentat

warden

- https://warden.cesnet.cz
- Platforma pro automatizované sdílení informací o incidentech
- Zapisující konektory zasílají události do „fronty“
- Čtoucí konektory odebírají vše, co se objevilo
- Jednotný formát (https://idea.cesnet.cz)
- Kdo ostatním poskytuje data, dostane se k datům ostatních

mentat

- https://mentat.cesnet.cz
- Jednotné automatizované zpracování
- Zpřístupňuje informace lidským způsobem přes GUI
- Příklad: DDoS
  - Informace dorazí přes FTAS, sondy a LaBreu do Wardenu
  - Mentat zagreguje informace z různých zdrojů
  - … a roztřídí podle zdrojů útoku
  - Jednotlivé organizace dostanou specifický report o svých IP

warden-info@cesnet.cz
mentat-info@cesnet.cz

Sběr, analýza a sdílení dat ...

NERD
NETWORK ENTITY REPUTATION DATABASE

- https://nerd.cesnet.cz
- Databáze síťových entit (IP adresy, sítě, domény, ...)
- Seznam nám známých zdrojů škodlivých aktivit
  ... a všeho, co o nich víme
- Primární zdroj – Warden, MISP). Data jsou obohacena o další informace z externích zdrojů
- Shrnutí všech informací do reputačního skóre, predikce míry hrozby entity pro následující den (strojové učení z dostupných dat)

PassiveDNS

- DNS odráží okamžitý stav – Passive DNS udržuje historii
- Sleduje DNS transakce a staví databázi
- Příklady využití
  - Jaké všechny jmenné záznamy ukazují na IP a.b.c.d?
  - Jaké záznamy známe v doméně example.org?
  - Jak se měnilo doménové jméno v čase? Není to fast-flux?
  - Není příliš podobné existujícímu jménu? Nejde o phishing?

- Pracovní skupiny CESNET CSIRT
  - 8. června 2022: Bezpečnostní události
  - 6. září 2022: Návrh bezpečné sítě
  - 13. prosince 2022: školení FTAS
  - ... vulnerability assesment
  - ... asset management
  - ...

- Pracovní skupiny CESNET CSIRT
  - 8. června 2022: Bezpečnostní události
  - 6. září 2022: Návrh bezpečné sítě
  - 13. prosince 2022: školení FTAS
  - ... vulnerability assessment
  - ... asset management
  - ...

- Sdružování bezpečnostních služeb a aktivit pod značku SOC
  - služba SOC BASIC (SLA)
  - rozvoj bezpečnosti, služeb a nástrojů pro dohled a obranu e-infrastruktury

cesnet

SOC

- **NOC**

  - správci páteřní infrastruktury

  - řeší provozní a bezpečnostní problémy e-infrastruktury CESNET

  - 24/7, v nočních hodinách „on phone“

- **FLAB**

  - řešení závažných bezpečnostních incidentů

  - analýzy, scanování, ...

- **Správci sond umístěných na perimetru**
- **Správci služeb ...**

- **Monitoring a detekce**
  - **FTAS**
  - **ExaFS**

- **CESNET-CERTS**

  - řešení a koordinace řešení bezpečnostních incidentů (reponse)

  - bezpečnostní tým, constituency = AS2852, 9:00 – 17:00

  - csirt.cesnet.cz, abuse@cesnet.cz

- **PSS, Pracoviště stálé služby**

  - dohledové centrum, 24/7

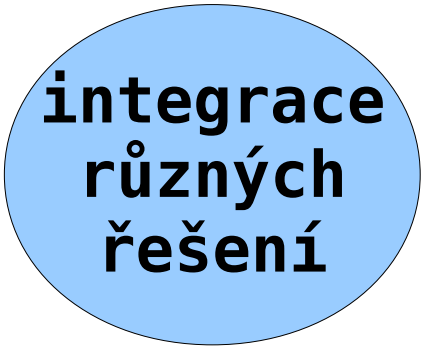
  - dohled nad e-infrastrukturou CESNET a službami

  - POC, koordinační role

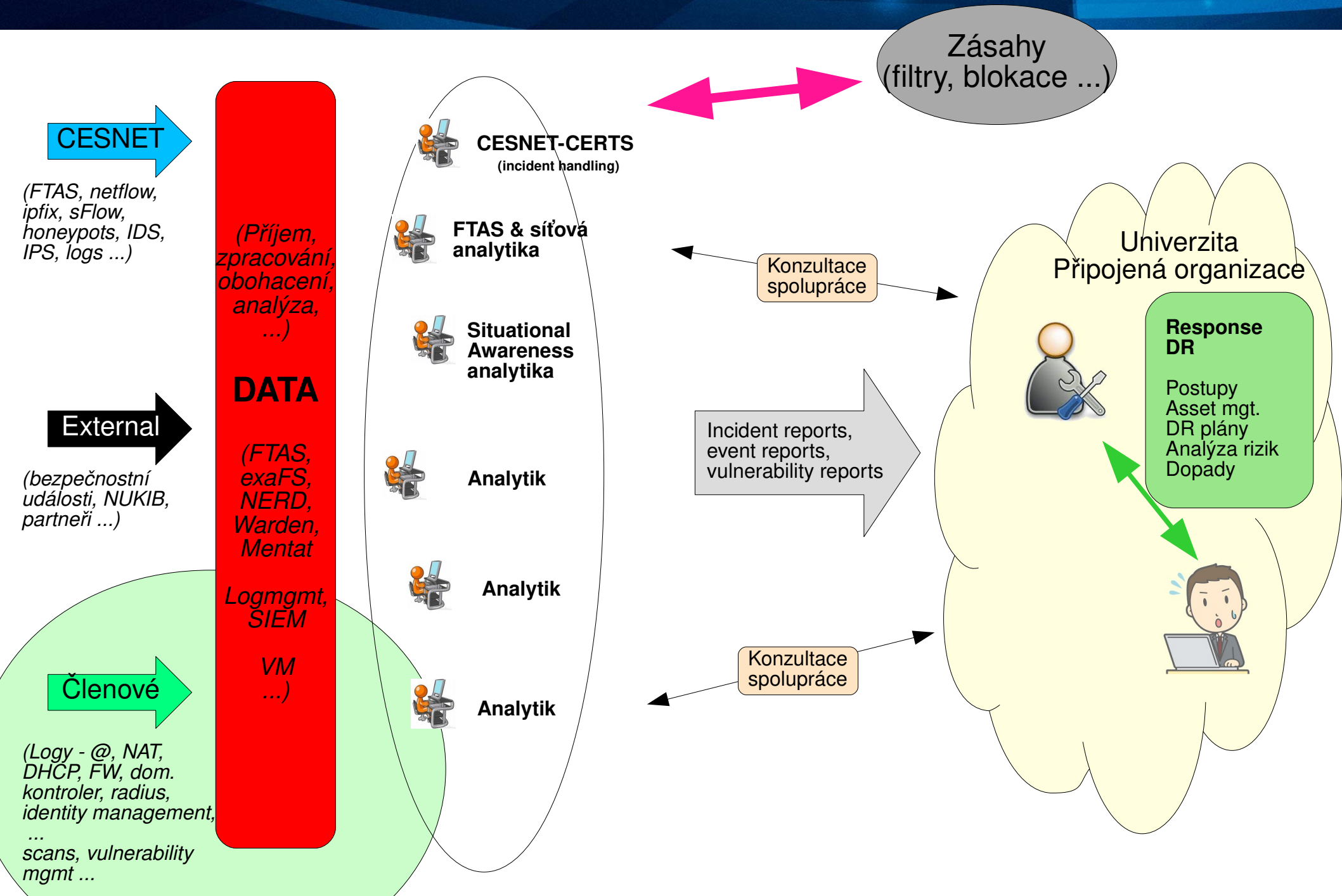
  - www.cesnet.cz --> kontakty

Nové služby

- **Logmanagement**
  - lokální (organizace) versus centrální (CESNET), oboje, kombinace ...
  - prvek nepopiratelnosti (archiv)
  - analytika
    - události, incidenty, zjištění ==> reporting, incident handling, warning
    - budování know-how pro oblasti, kde v koncové síti není expertnost
  - synergie „více dat“
  - vertikální a horizontální korelace dat
- **Scanování zranitelností**
  - plošné, systematické, podklad pro Vulnerability Management
  - CESNET rozsahy, TUL, MUNI a VUTBR v domluvě
  - „scan části sítě nebo jednoho zařízení na míry a automatizovaně“
- **Situational Awareness/Vulnerability Management**
  - reporting do csirt-forum@cesnet.cz (aktuálně běžící)
  - další rozvoj v kombinaci s předchozími službami
  - DB entit ==> využití pro rychlou identifikaci zranitelných zařízení



CESNET SOC model zítra ...



SOC: CESNET versus člen

[z prezentace na Klubu ředitelů VC dne 15. 11. 2022]

- Správa infrastruktury – koncová zřízení, servery, síťové prvky, provoz sítě a služeb ...
- Vnitřní pravidla, postupy, dokumentace
- **Incident response** – řešení bezpečnostních incidentů a událostí
  - use-case: DR ransomware pracovního počítače
- Asset management
- Ochrana sítě a běžících služeb v koncové síti
  - lokální FW, antivir, antispam, antimalware na zařízeních
  - DMZ
  - pokročilejší FW systémy na úrovni sítě, IDS, IPS
  - ochrana na perimetru (monitoring, detekce, obrana u upstreamu)
- **Logmanagement** – zpracování logů z běžících služeb (zařízení)
- **Scanování zranitelností**
- **Situational Awareness/Vulnerability management**
- Sběr, zpracování a distribuce bezpečnostních událostí

Zajišťuje CESNET

V gesci připojené organizace, ale CESNET může pomoci. Zde je možné využít komunitní share přístup a podělit se o zkušenosti.

Hints ...

- **7. 2. 2022**
  - Seminář o bezpečnosti
- **6. - 10. března 2023**
  - Forenzní trénink 1 & Forenzní trénink 2
- **5. - 9. června 2023**
  - Forenzní trénink 1 & Forenzní trénink 2

sluzby@cesnet.cz

- **17. 2. 2023** – podání projektů do Fondu rozvoje CESNET
- **Pracovní skupiny CESNET CSIRT**
  - incident response
  - zpracování výstupů nástrojů pro management zranitelností

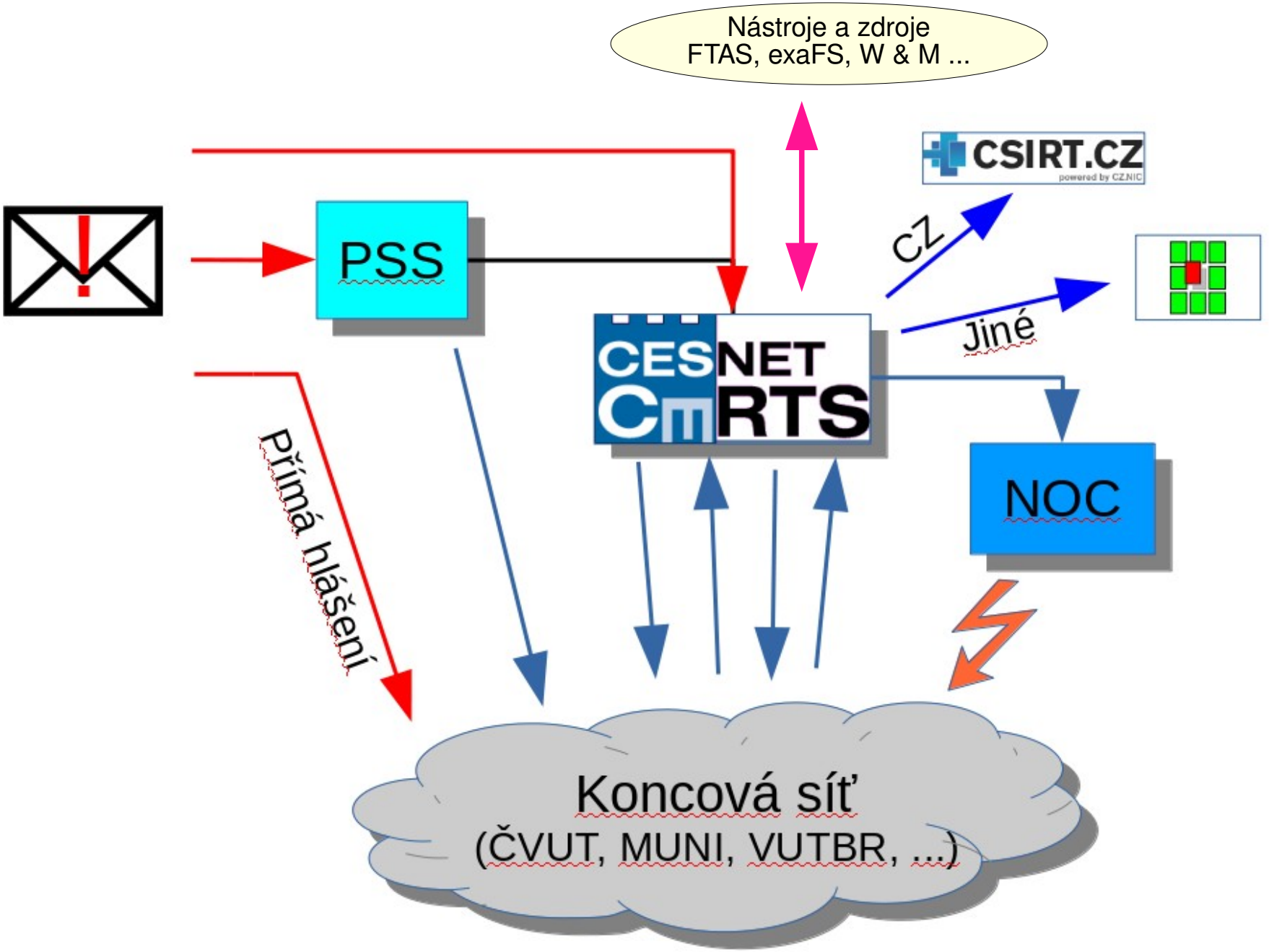
Kontakty

- www.cesnet.cz
- https://www.cesnet.cz/sluzby/
- www.cesnet.cz/enews - e-mail Newsletter
- **sluzby**@cesnet.cz
- **support**@cesnet.cz

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz

Incident handling by CESNET-CERTS



CESNET SOC model - rozvoj