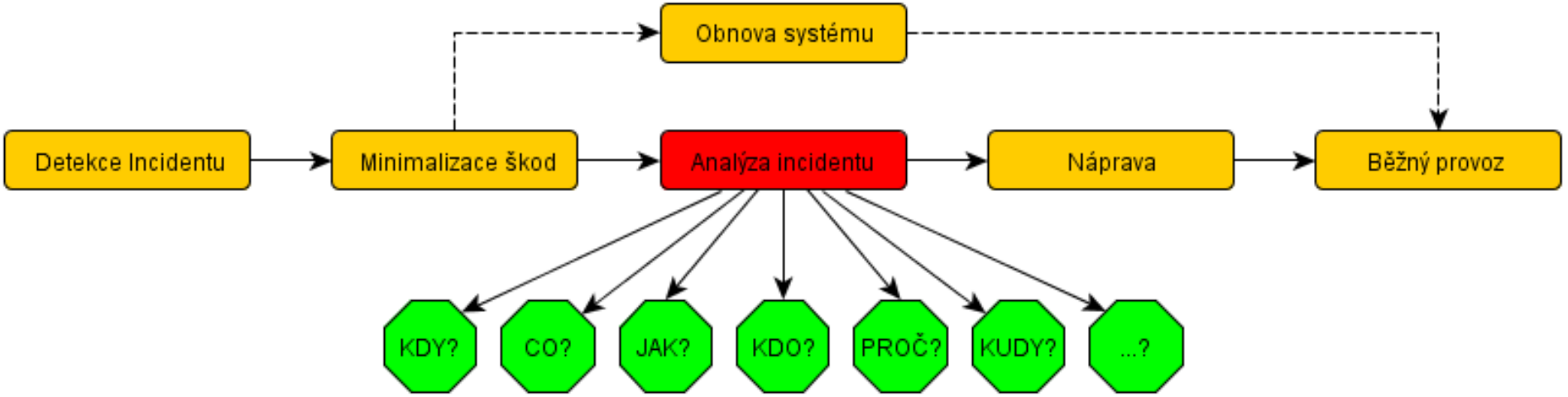
Forenzní laboratoř

Aleš Padrta, apadrta@cesnet.cz
CESNET, z. s. p. o.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

Forenzní laboratoř

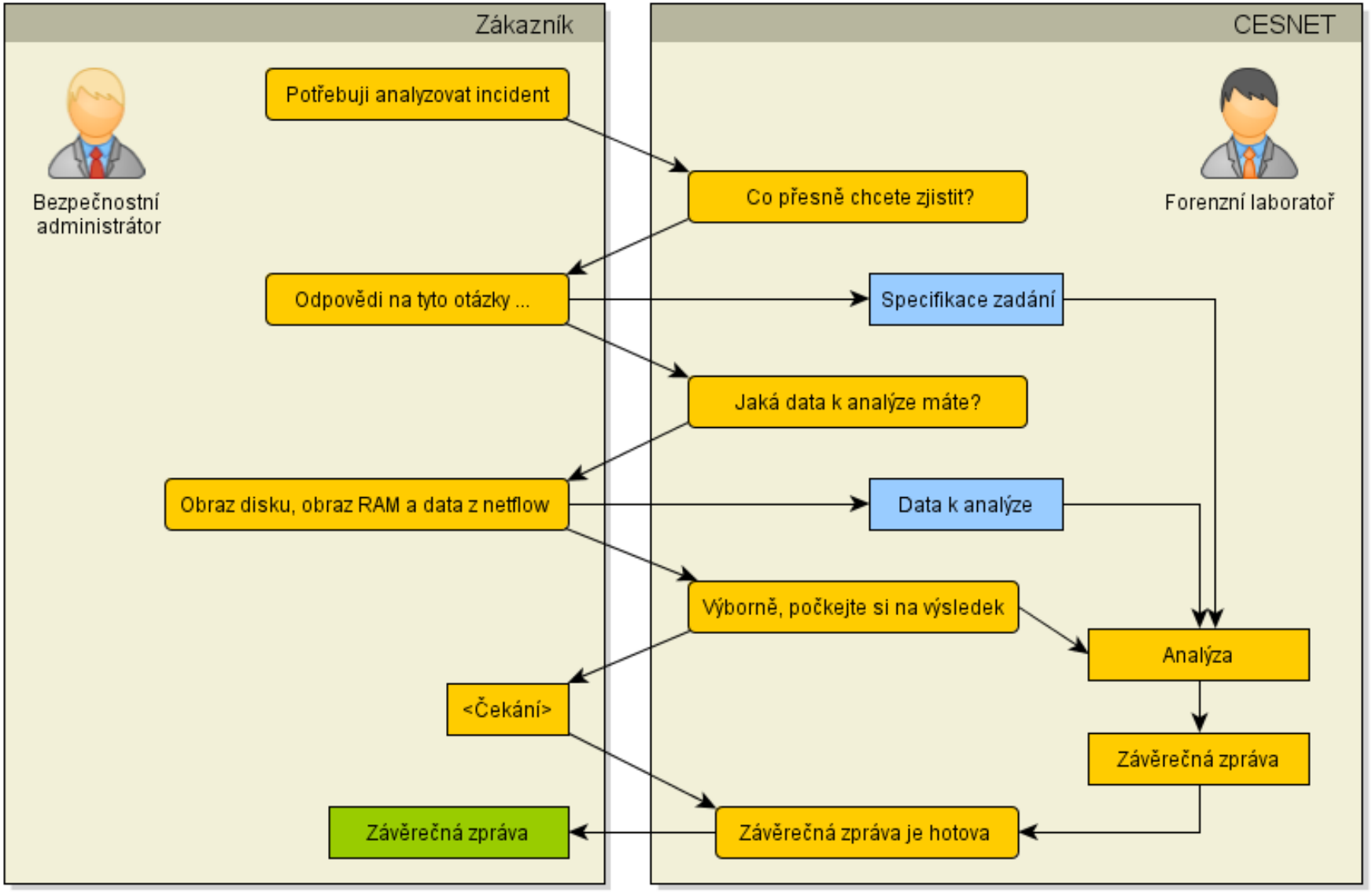
- Řešení bezpečnostní incidentů
  - Standardní postup



  - Vzniká mnoho otázek
- Analýza incidentu – poskytuje cenné informace
  - Náročné na čas + znalosti
  - Mimo možnosti některých organizací

Forenzní laboratoř

- Zadání analýzy CESNETu (forenzní laboratoři)



Závěrečná zpráva

- Zadání
  - Důkazy
  - Otázky
  - Doplňující informace
- Postup
  - Popsána posloupnost kroků
  - Technické detaily v přílohách
- Závěry
  - Shrnutí zjištěných faktů
  - Odpovědi na otázky
  - Manažerské shrnutí

Dva příklady z nedávné minulosti

- Analýza napadeného webového serveru
  - Jak získal útočník přístup
  - Jaká data byla stažena
  - Jaké změny provedl
  - Zda byla vytvořena zadní vrátka
- Reverzní analýza malware na koncové stanici
  - Jak se malware dostane na stanici
  - Jaké změny provede v systému
  - Jaká data sbírá a kam je posílá?
  - Jaké jsou IP adresy C&C

Využití výstupů

- Ochrana proti opětovnému napadení
  - Nalezení míst průniku
  - Možnost zamezení stejného scénáře
  - Více stejných zařízení (class-attack)
- Prokázání nevhodného chování uživatele
  - Porušování interních směrnic
  - Zacházení s dokumenty, závadné aplikace, …
- Možnost nalézt další členy botnetu v síti
  - Zjištění typického chování
  - Reverzní analýza malware, chování systému, soubory
- ...

Komunikace s forenzní laboratoří

- Webové stránky
  - https://csirt.cesnet.cz/FLAB/
  - https://flab.csirt.cesnet.cz
  - Kontakty
- Vše “bezkontaktně”
  - Komunikace
    - E-mail, telefon, VoIP, …
  - Přenos dat
    - Datové úložiště CESNET (https://filesender.cesnet.cz)
    - FTP/WWW/SSH server
    - ...
    - Eventuelně poštou

Jak postupovat?

- Kontaktovat pracovníky FLAB
  - Domluvení vhodného postupu
- Specifikovat zadání
  - S pomocí pracovníka FLAB
- Předat dat
  - Návody na zajištění na webu FLAB
- Trpělivě čekat
  - Typicky 1-N týdnů
- Převzít si závěrečnou zprávu

Shrnutí

- Analýza
  - Detailní náhled na incident
  - Potřebná k řádnému vyřešení
- Náročná
  - Čas i peníze
- Forenzní laboratoř CESNETu
  - “outsourcing” analýzy
- Postup
  - Najít kontakt na webu
  - Domluvit si další postup

Děkuji za pozornost.