Detekce DNS tunelování

pomocí neuronové sítě

Hynek Šabacký • 4. 10. 2025

CZ.NIC | SPRÁVCE DOMÉNY CZ

Cíle

- Modul Knot Resolver
- DNS Patrol
- Detekce v reálném čase
- Nastavitelnost citlivosti
- Minimum falešných poplachů

Cíle

- Modul Knot Resolver
- DNS Patrol
- Detekce v reálném čase
- Nastavitelnost citlivosti
- Minimum falešných poplachů

Jak na to?

Princip tunelování

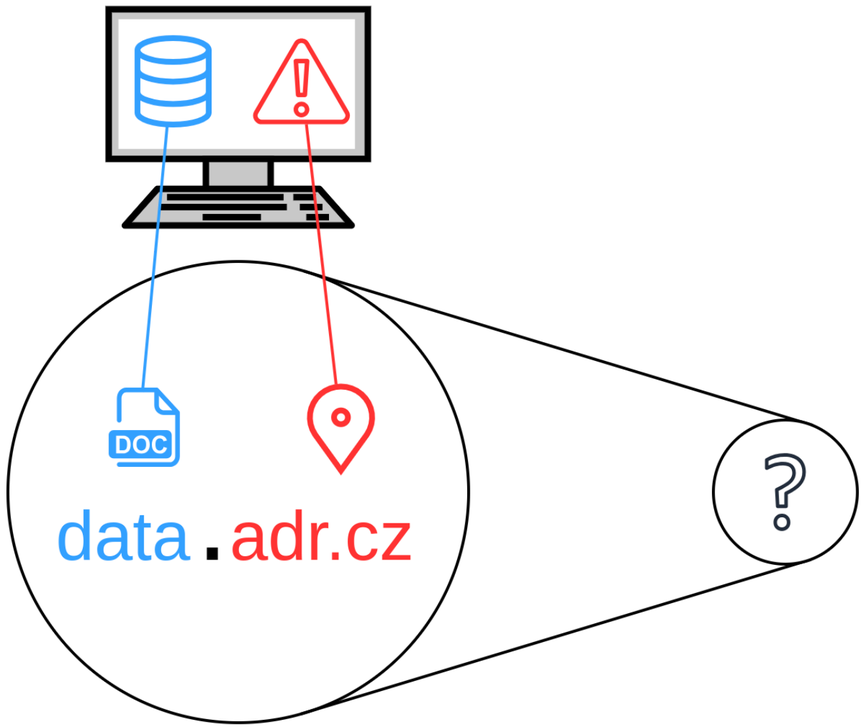
1. Klient

Princip tunelování

1. Klient
2. Malware

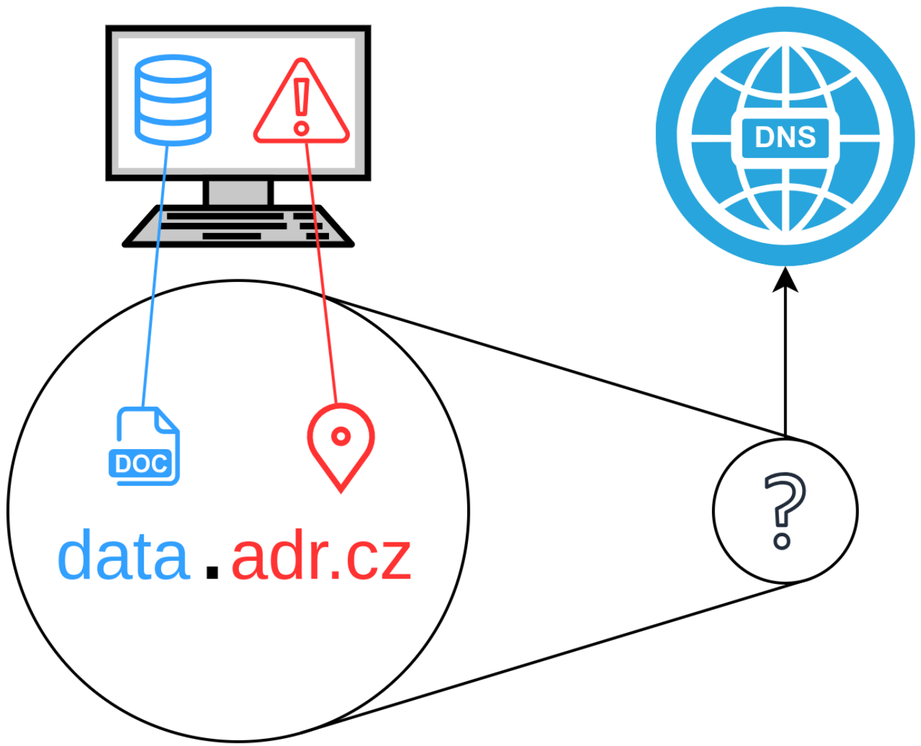
Princip tunelování

1. Klient
2. Malware
3. Tvorba dotazu



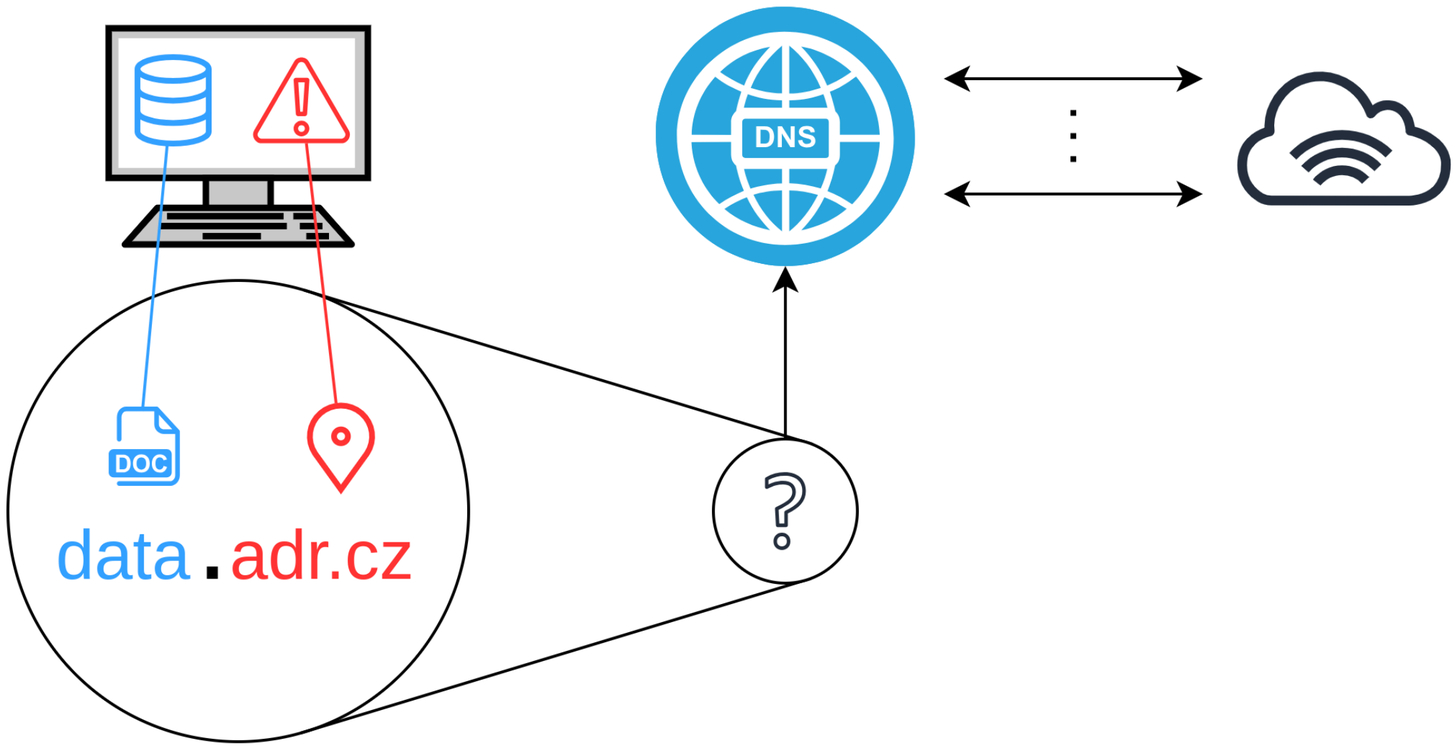
Princip tunelování

1. Klient
2. Malware
3. Tvorba dotazu
4. Zpracování dotazu



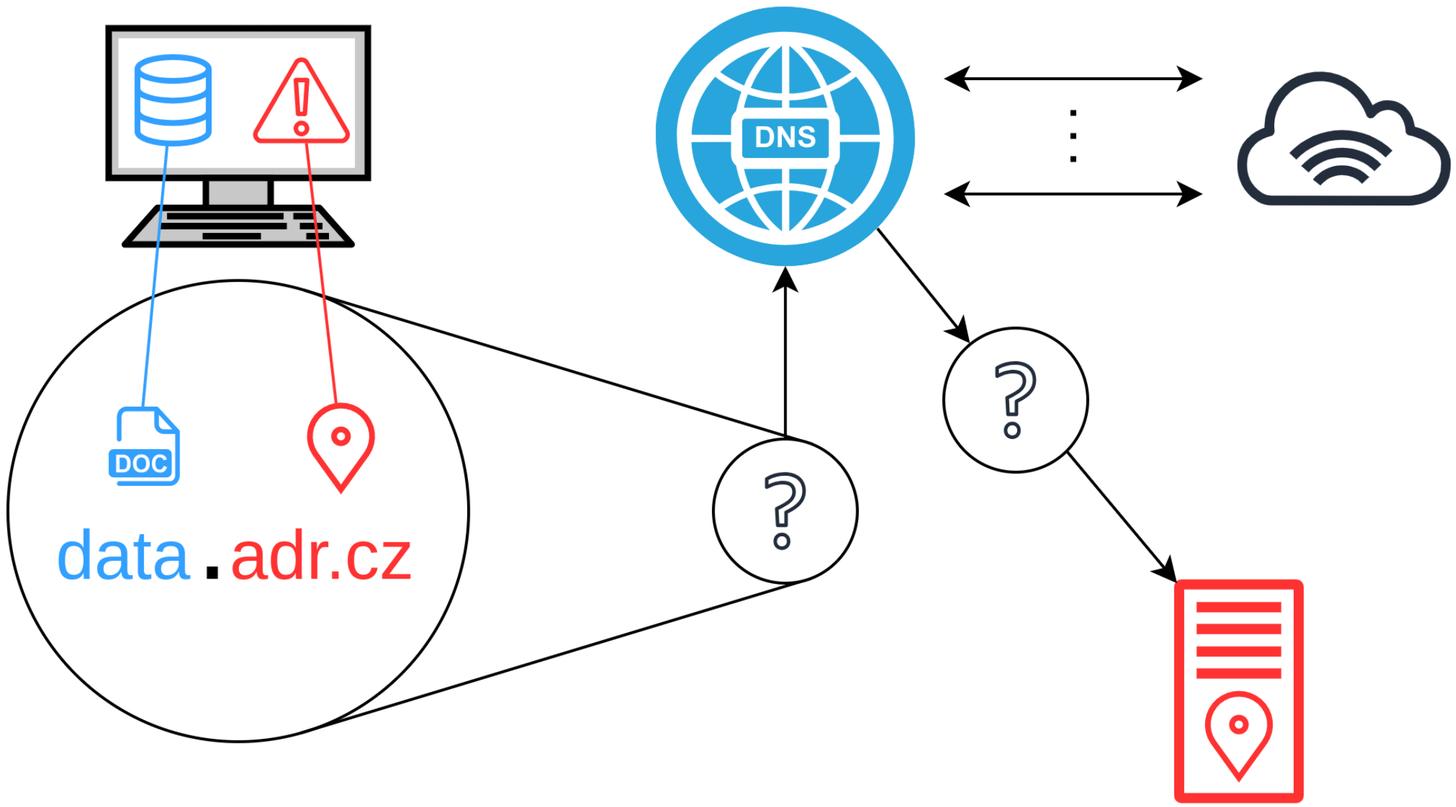
Princip tunelování

1. Klient
2. Malware
3. Tvorba dotazu
4. Zpracování dotazu



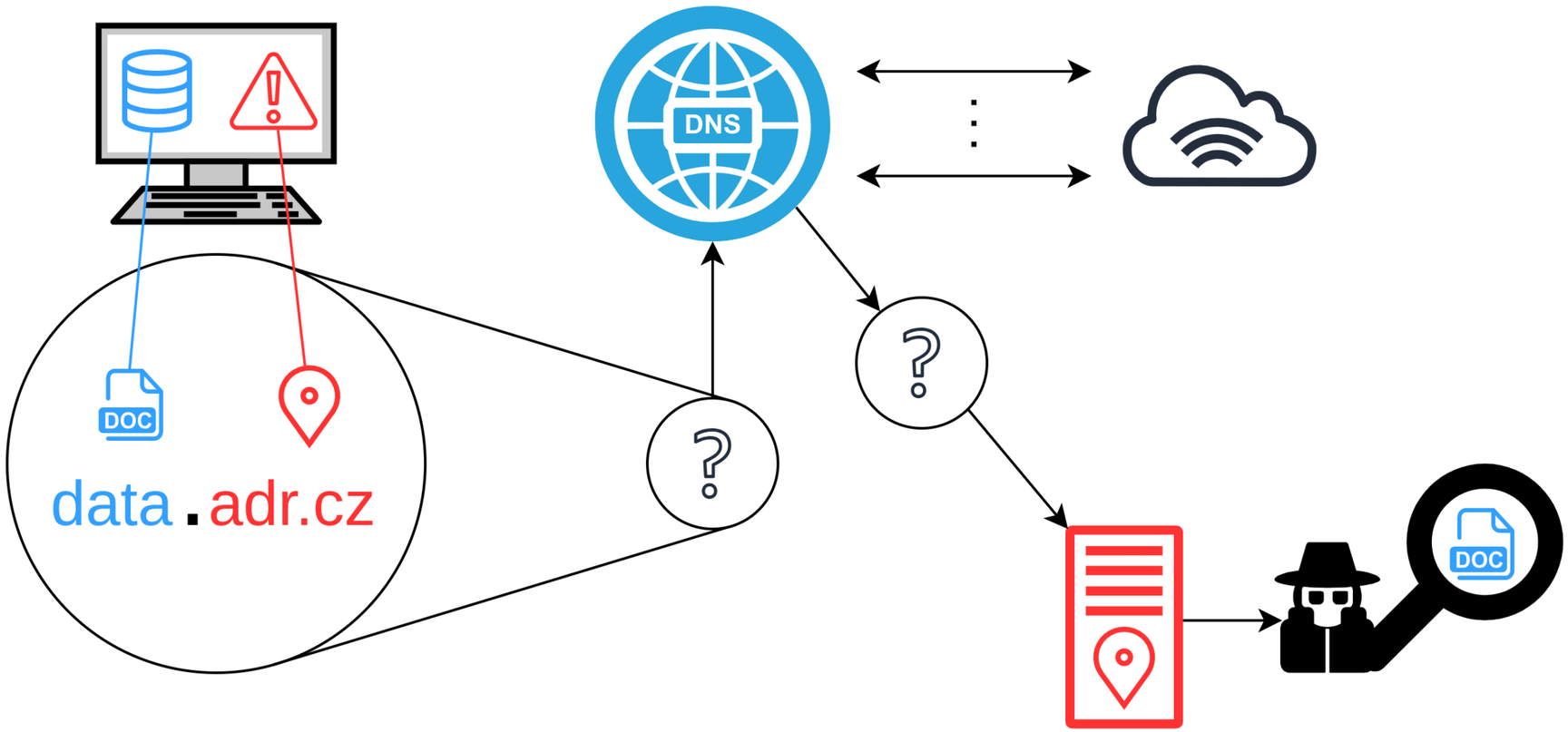
Princip tunelování

1. Klient
2. Malware
3. Tvorba dotazu
4. Zpracování dotazu



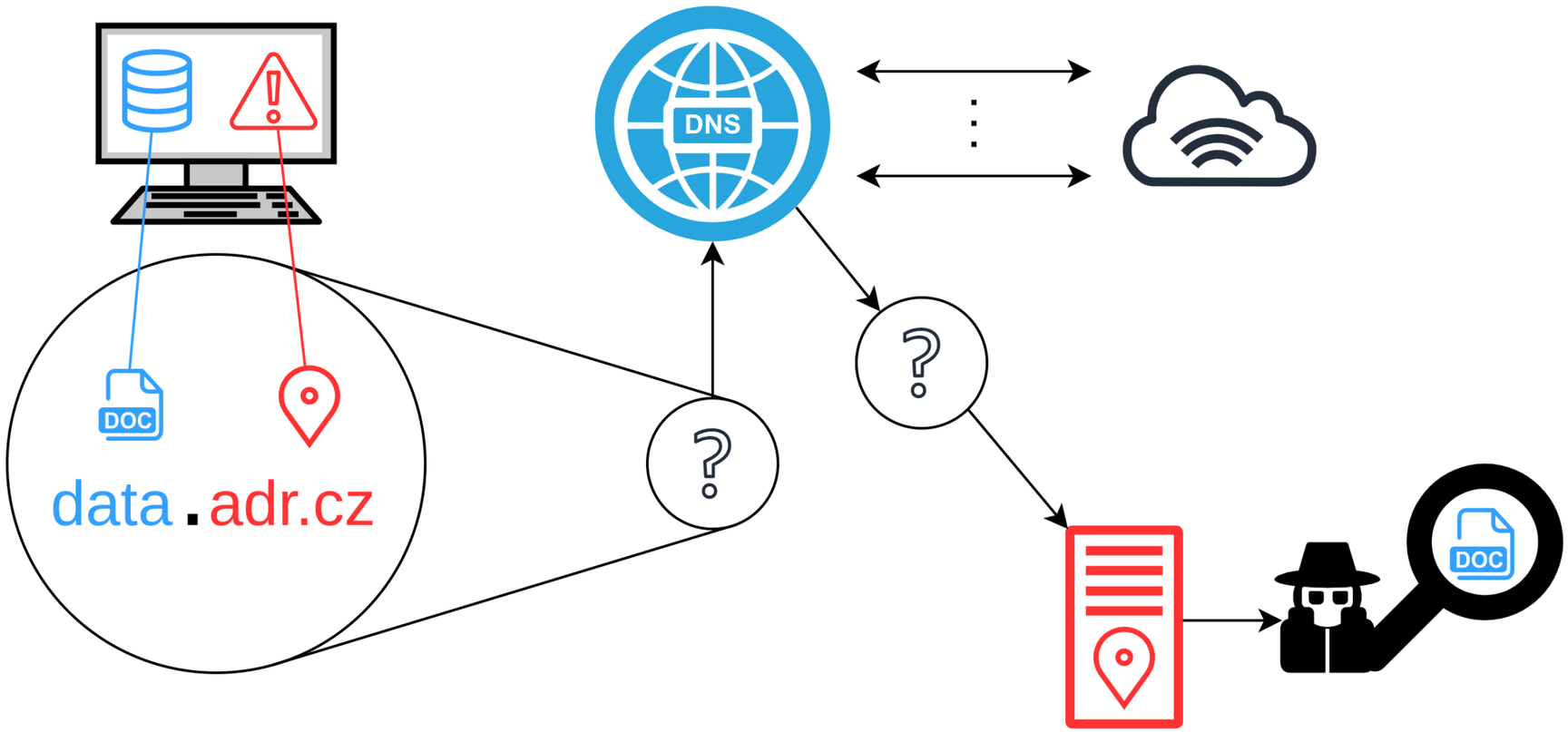
Princip tunelování

1. Klient
2. Malware
3. Tvorba dotazu
4. Zpracování dotazu
5. Únik dat



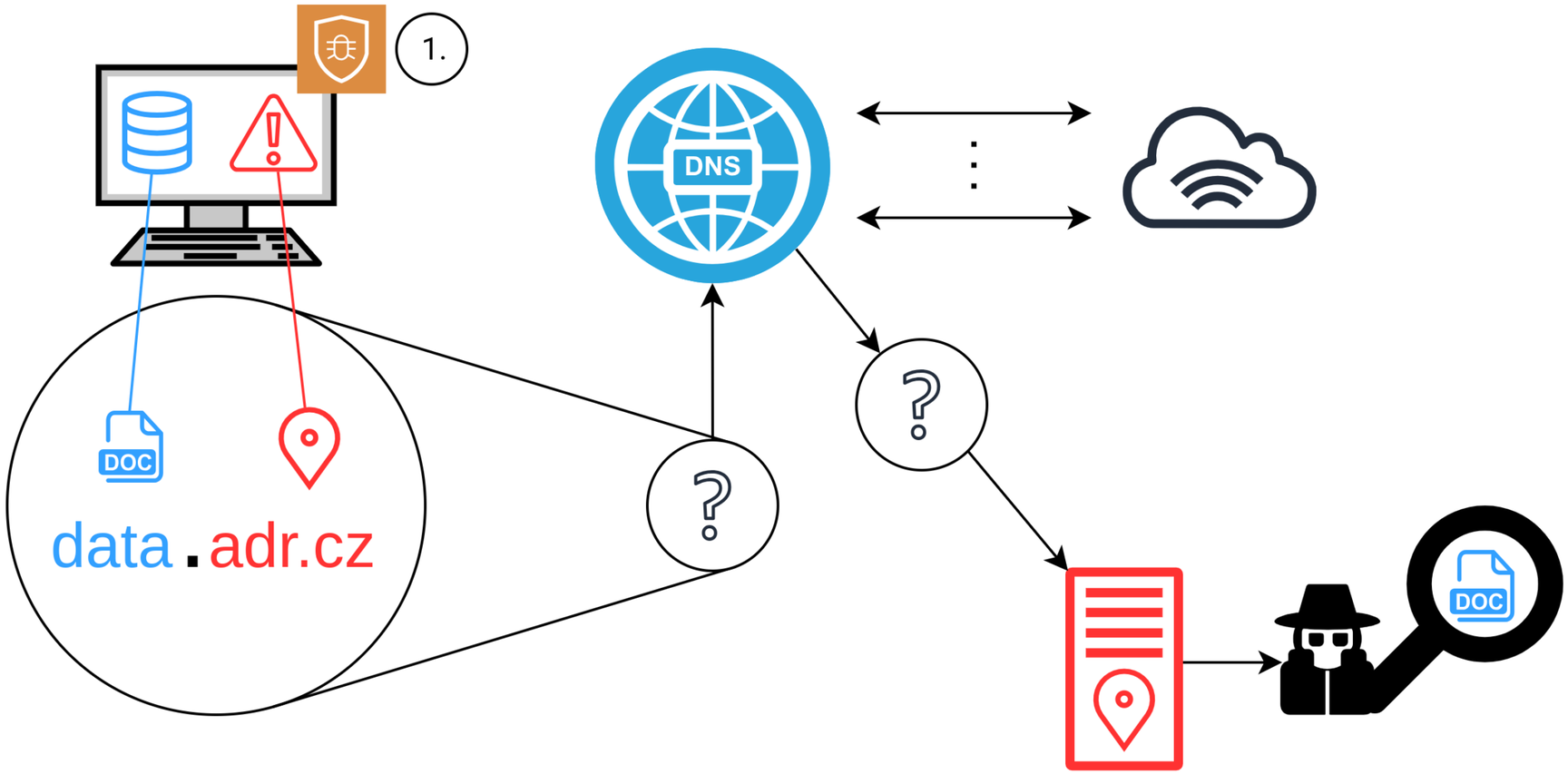
Ochrana

- Architektura



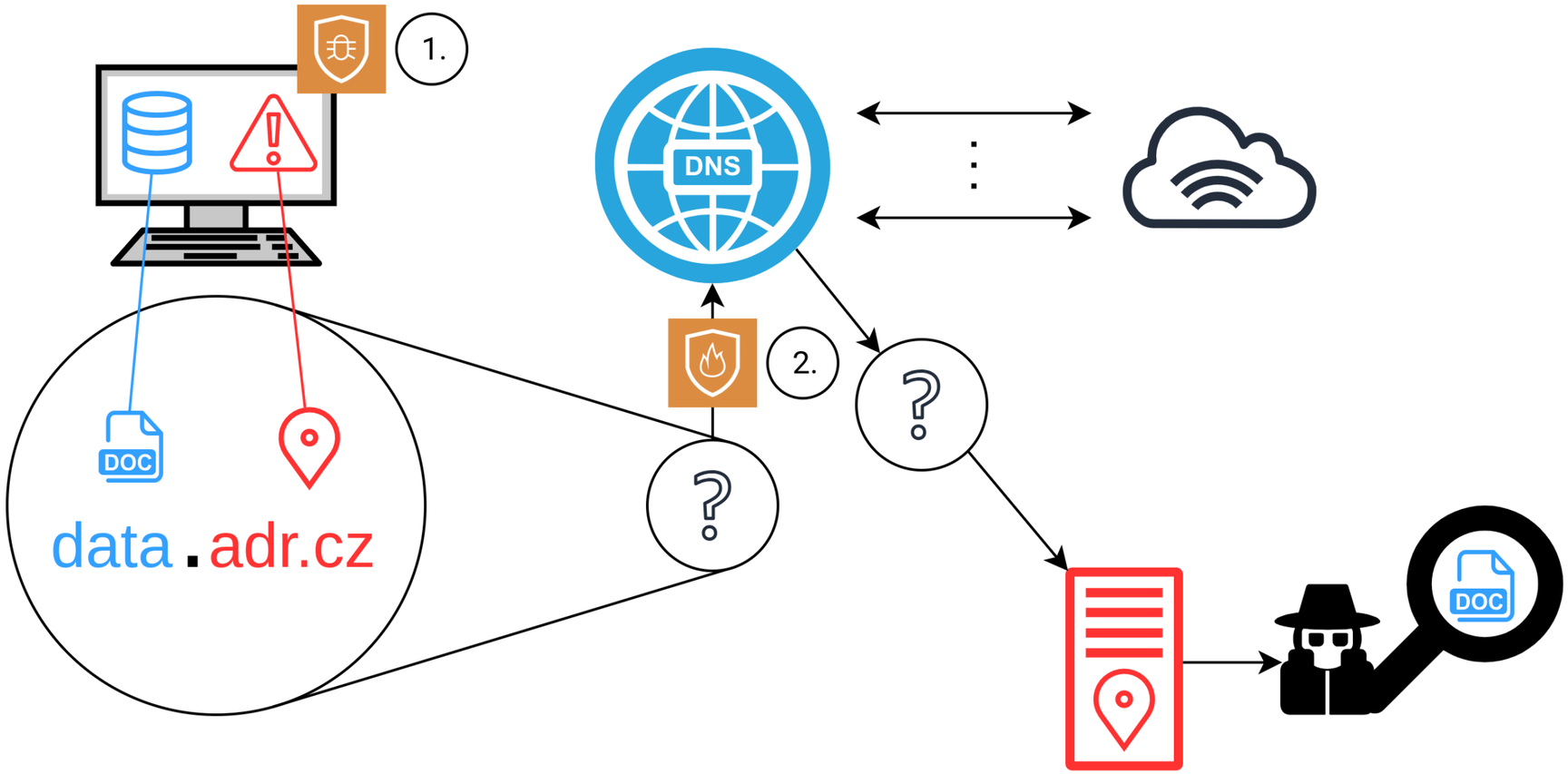
Ochrana

- Architektura
  1. + Antivirus



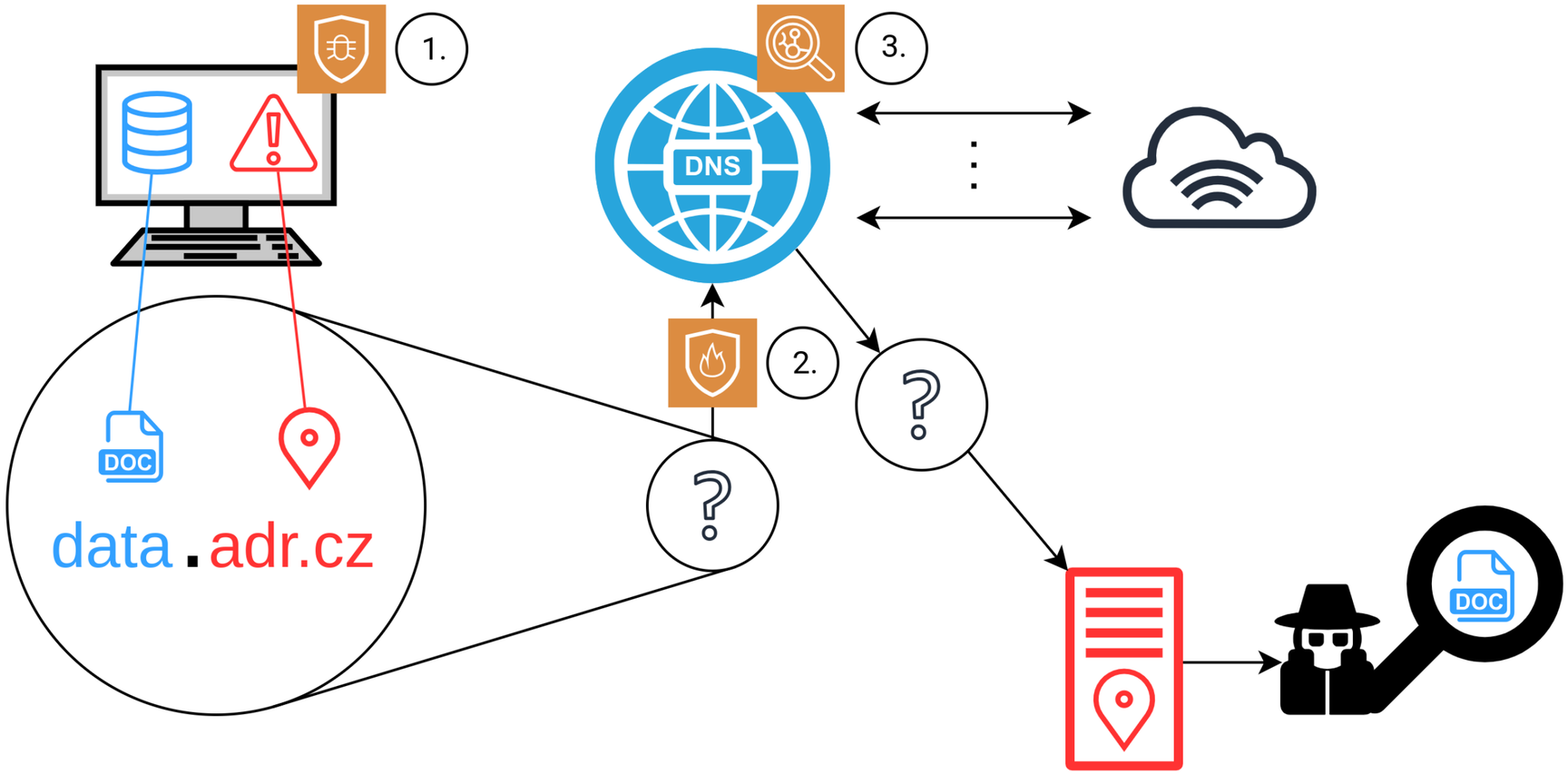
Ochrana

- Architektura
  1. + Antivirus
  2. + Firewall/IDS



Ochrana

- Architektura
  1. + Antivirus
  2. + Firewall/IDS
  3. **+ Analyzátor**



Způsoby detekce

- Tradiční metody

Způsoby detekce

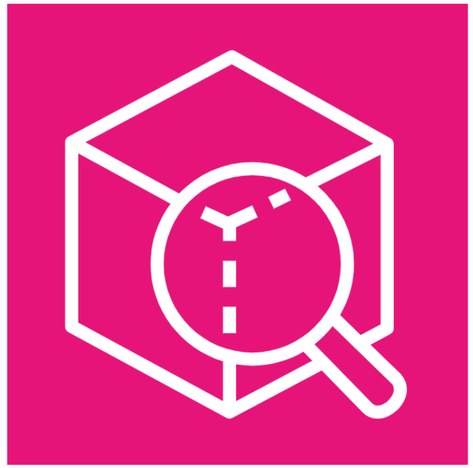
- Tradiční metody
  1. Analýza provozu

1.

Způsoby detekce

- Tradiční metody
  1. Analýza provozu
  2. Analýza paketu

1.

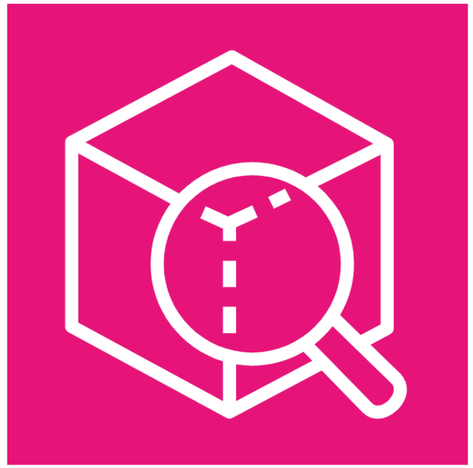


2.

Způsoby detekce

- Tradiční metody
  1. Analýza provozu
  2. Analýza paketu
- Moderní metody

1.

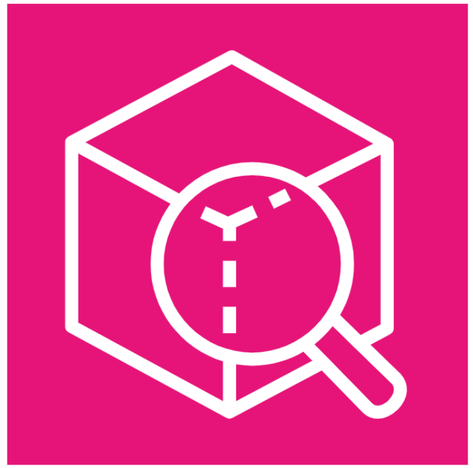


2.

Způsoby detekce

- Tradiční metody
  1. Analýza provozu
  2. Analýza paketu
- Moderní metody
  3. Strojové učení

1.



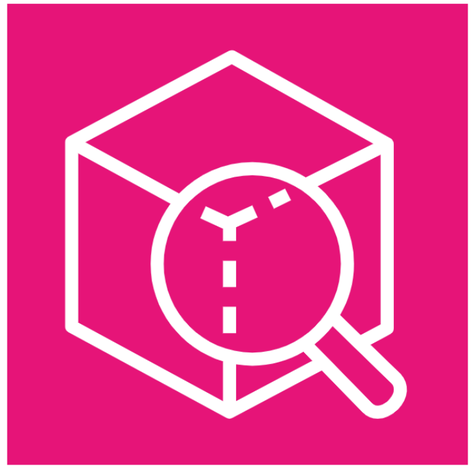
2.

3.

Způsoby detekce

- Tradiční metody
  1. Analýza provozu
  2. Analýza paketu
- Moderní metody
  3. Strojové učení
  4. Neuronové sítě

1.



2.

3.

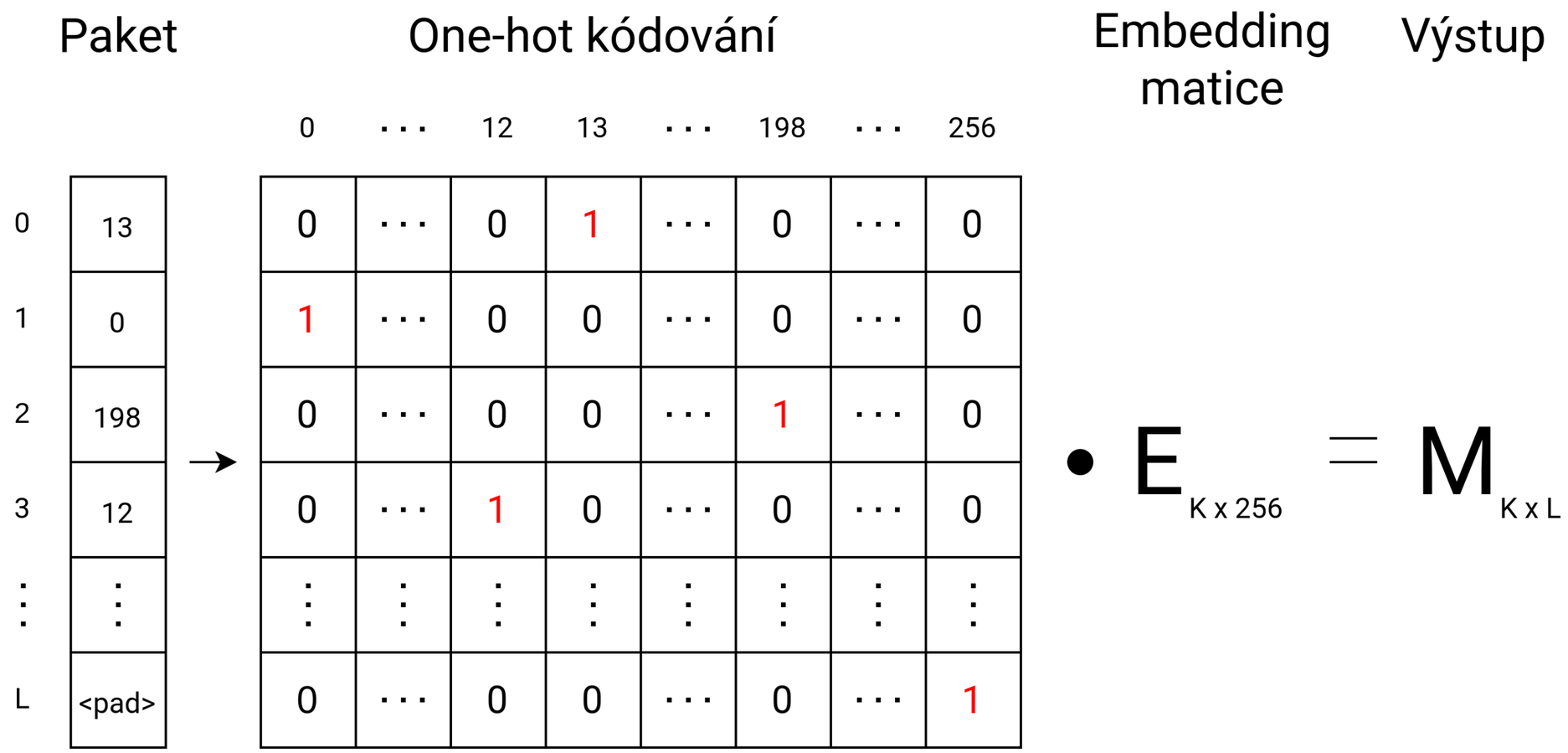
4.

Proč neuronová síť?

- **Výhody**
  - Jednoduchost extrakce rysů
  - Nízké výpočetní náklady (u CNN)
  - Nejlepší výsledky v současnosti
  - Lze specializovat dle nasazení
- **Nevýhody**
  - Potřeba velkého množství trénovacích dat
  - Těžko rozezná nové metody
  - Riziko přeučení

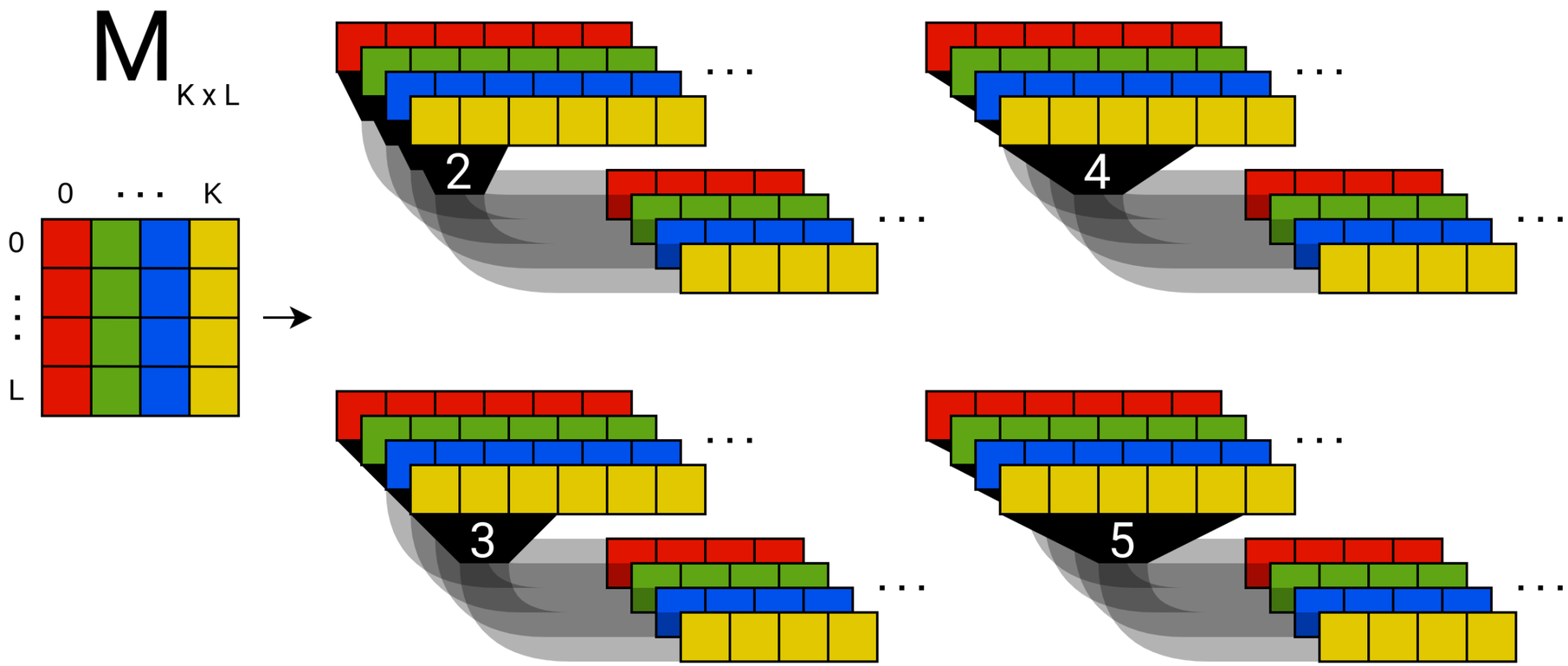
Architektura neuronové sítě

1. Předzpracování



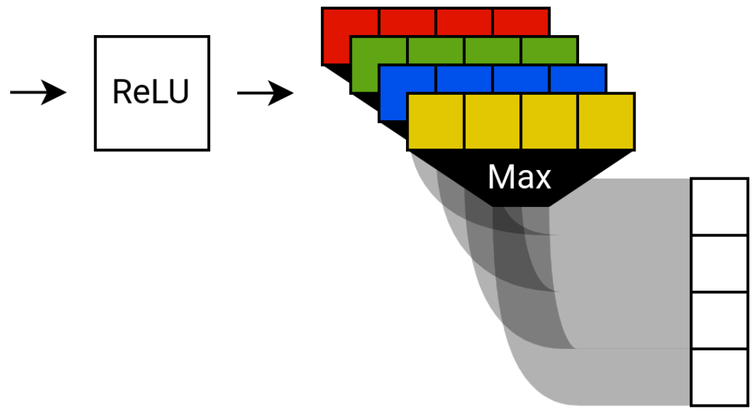
Architektura neuronové sítě

1. Předzpracování
2. Konvoluce



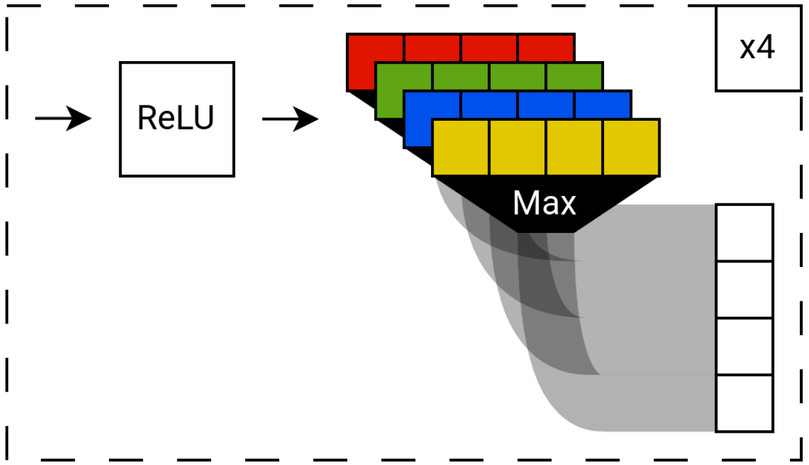
Architektura neuronové sítě

1. Předzpracování
2. Konvoluce
3. Aktivace a pooling



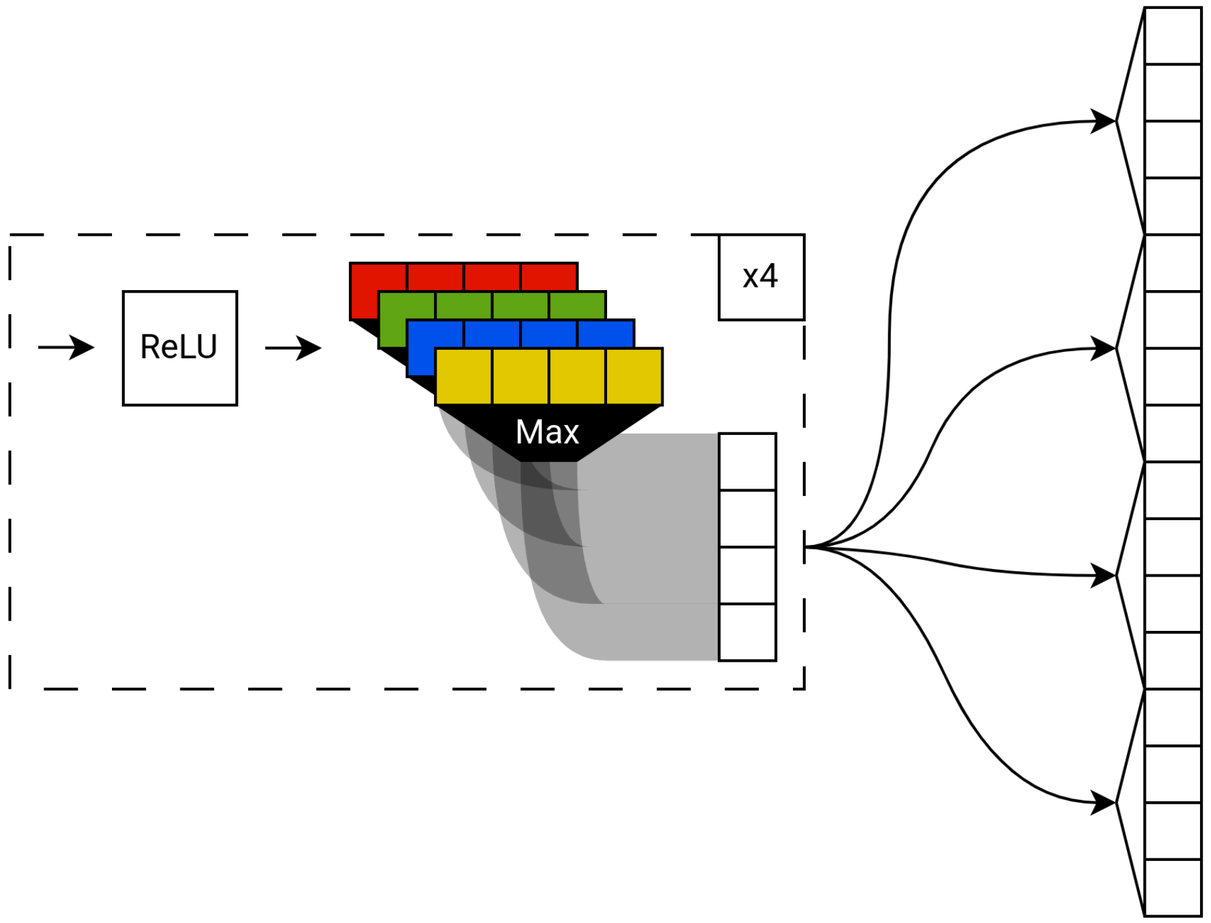
Architektura neuronové sítě

1. Předzpracování
2. Konvoluce
3. Aktivace a pooling



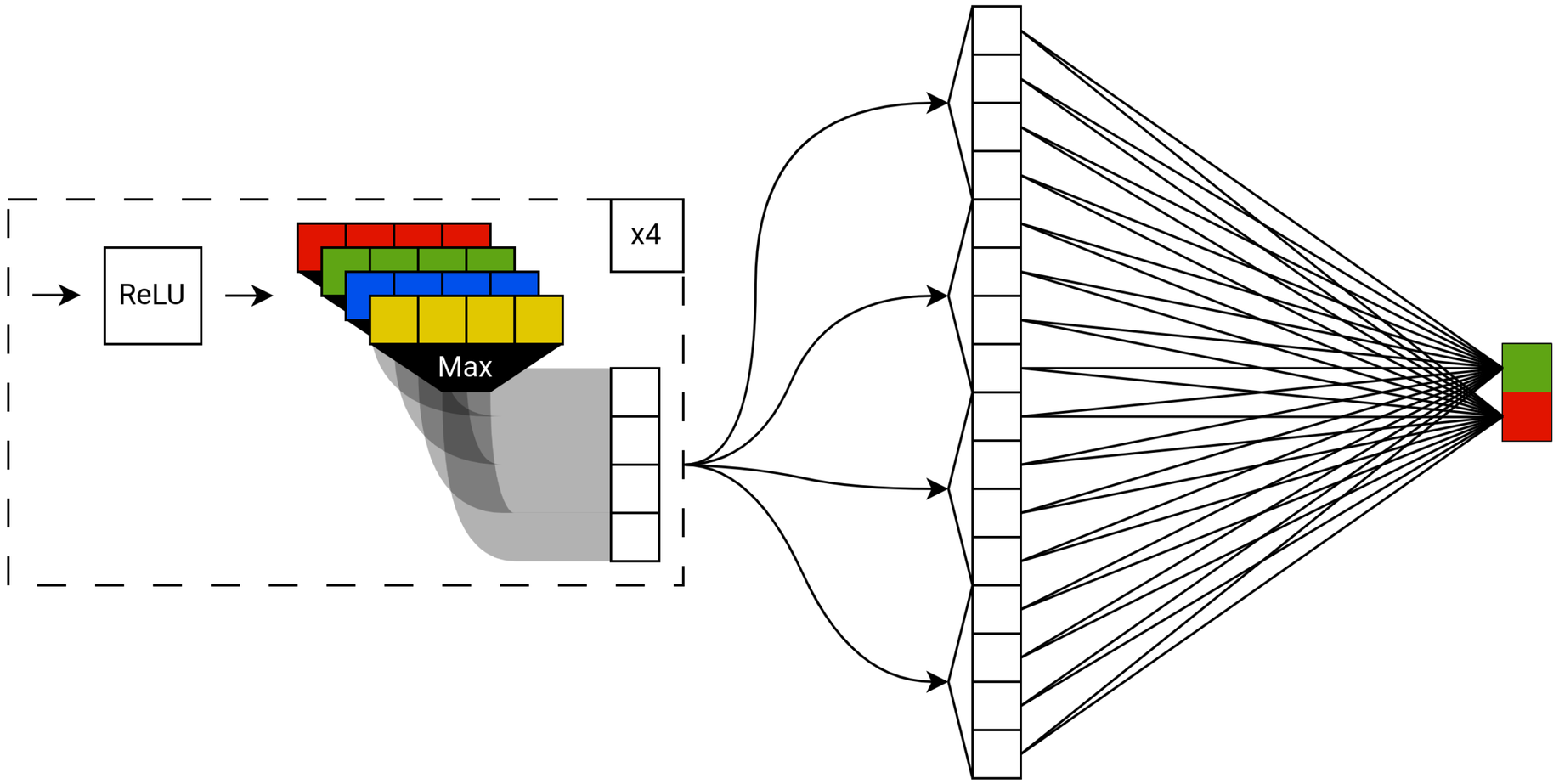
Architektura neuronové sítě

1. Předzpracování
2. Konvoluce
3. Aktivace a pooling

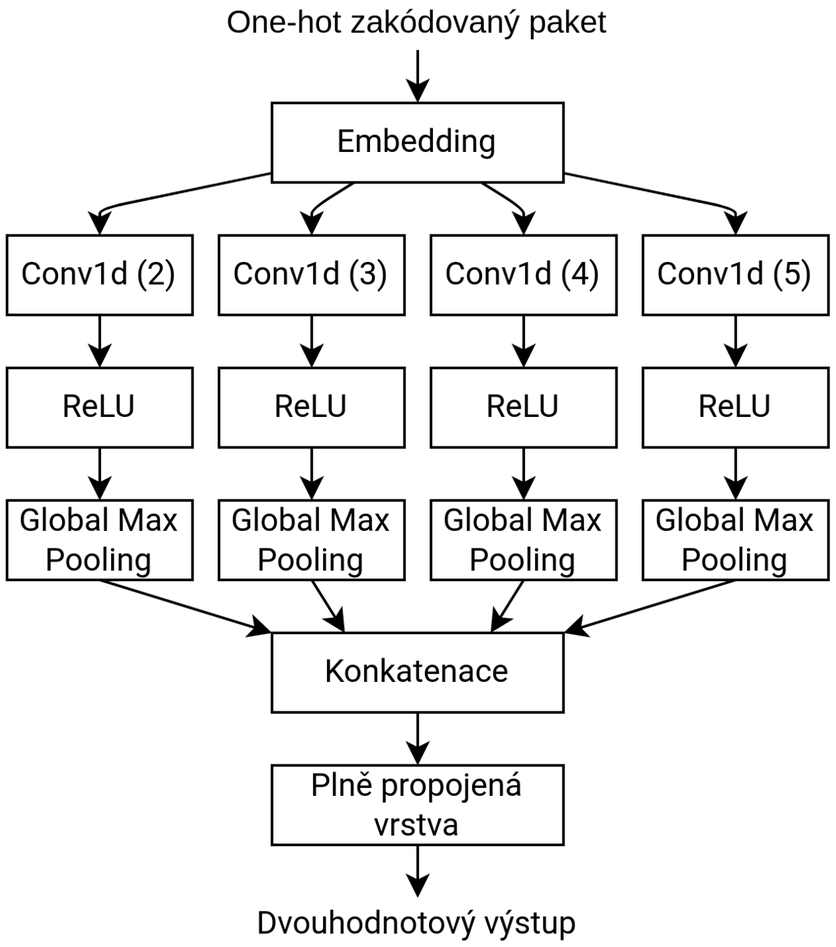


Architektura neuronové sítě

1. Předzpracování
2. Konvoluce
3. Aktivace a pooling
4. Plně propojená vrstva



Souhrnný diagram



Implementace

PyTorch logo © Facebook, Inc. (BSD license) https://github.com/pytorch/pytorch/blob/main/LICENSE

ONNX logo © Microsoft Corporation (MIT license) https://github.com/onnx/onnx/blob/main/LICENSE

Datové sady

- PCAP s DNS pakety pro:
  - Trénování sítě
  - Testování modelu

	Daumel [1]	**ADAM**
Původ	Volně dostupný na internetu	Testovací prostředí + sonda
Objem	3 M paketů	15 k paketů
Algoritmy	9 různých	Iodine
Primární účel	Trénování	Validace

[1] - https://github.com/Daumel/dns-exfiltration-dataset

Výsledky

Daumel

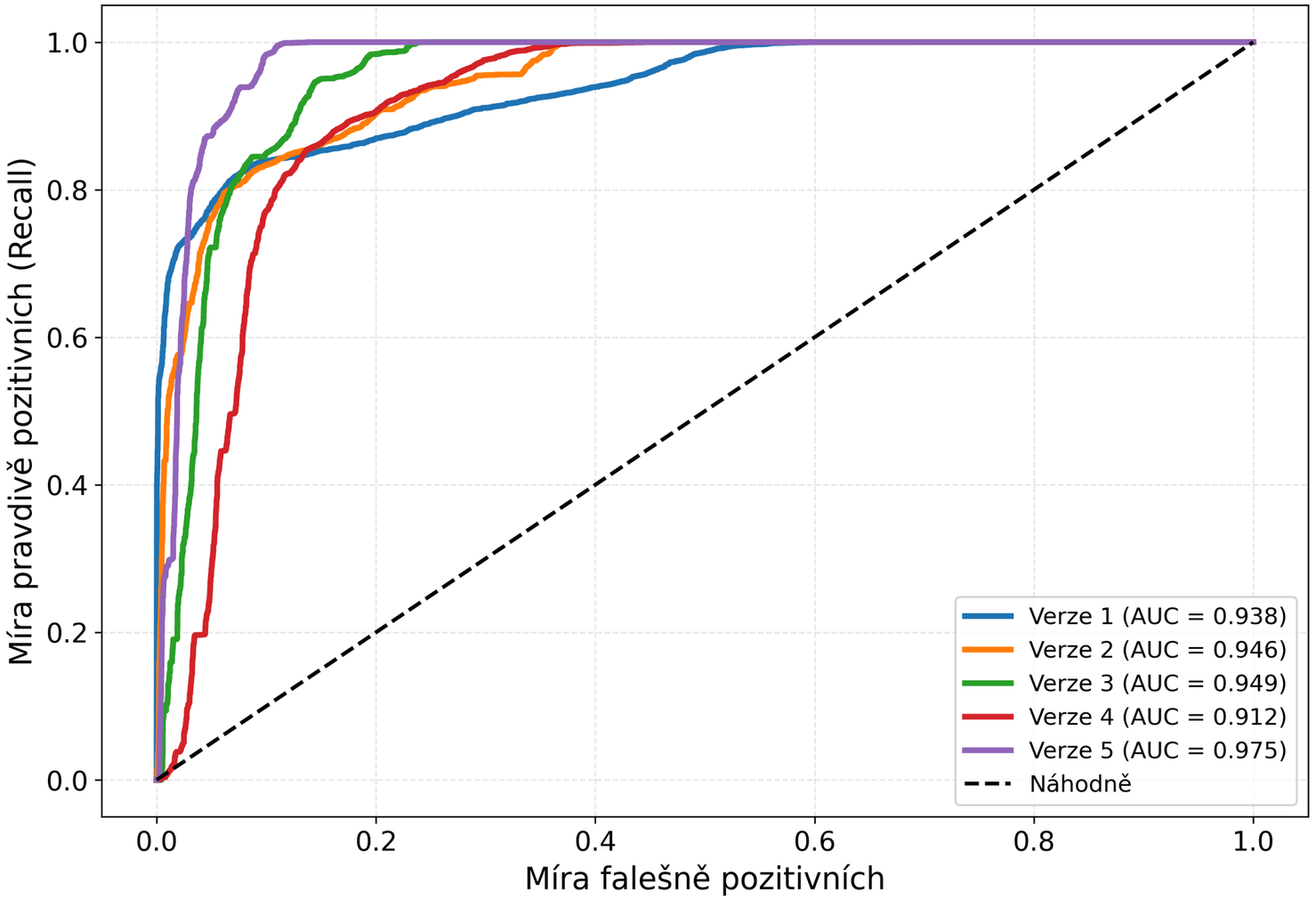
Model	F1	Precision	Recall
1	96,83	100	93,87
2	99,99	99,99	99,99
3	99,99	99,99	99,99
4	98,16	99,99	96,41
5	99,99	100	99,99

ADAM

Model	F1	Precision	Recall
1	70,13	99,63	54,11
2	86,44	92,10	81,43
3	92,03	89,18	95,08
4	83,45	71,60	100
5	93,85	95,10	92,63

- **Precision:** Podíl skutečně škodlivých z označených jako škodlivé. [TP / (TP + FP)]
- **Recall:** Podíl označených škodlivých ze všech škodlivých. [TP / (TP + FN)]

ADAM ROC křivka



Co dál?

Metoda	F1	Precision	Recall
Základní	93,85	95,10	92,63

- **Precision:** Podíl skutečně škodlivých z označených jako škodlivé. [TP / (TP + FP)]
- **Recall:** Podíl označených škodlivých ze všech škodlivých. [TP / (TP + FN)]

Co dál?

Metoda	F1	Precision	Recall
Základní	93,85	95,10	92,63
Whitelisty	95,84	99,27	92,63

- **Precision:** Podíl skutečně škodlivých z označených jako škodlivé. [TP / (TP + FP)]
- **Recall:** Podíl označených škodlivých ze všech škodlivých. [TP / (TP + FN)]

Co dál?

Metoda	F1	Precision	Recall
Základní	93,85	95,10	92,63
Whitelisty	95,84	99,27	92,63
Posun práhu detekce	96,23	92,99	99,70

- **Precision:** Podíl skutečně škodlivých z označených jako škodlivé. [TP / (TP + FP)]
- **Recall:** Podíl označených škodlivých ze všech škodlivých. [TP / (TP + FN)]

Co dál?

Metoda	F1	Precision	Recall
Základní	93,85	95,10	92,63
Whitelisty	95,84	99,27	92,63
Posun práhu detekce	96,23	92,99	99,70
Kombinace	98,88	98,07	99,70

- **Precision:** Podíl skutečně škodlivých z označených jako škodlivé. [TP / (TP + FP)]
- **Recall:** Podíl označených škodlivých ze všech škodlivých. [TP / (TP + FN)]