Český router Turris

OpenSource a bezpečnost

Michal Hrušecký

michal.hrusecky@turris.com

Kdo jsme?

Projekt Turris by CZ.NIC

CZ.NIC

- správce české domény
- vývoj opensource SW knot, bird a další

Turris

- vyrábíme WiFi routery
- opensource software
- částečně open hardware
- důraz na bezpečnost

Co chtít od bezpečného zařízení

- bezpečnostní aktualizace
- důvěryhodnost - nedělá co nechci
- záruky/track record
  - opravdu nedělá co nechci ne že to jen tvrdí
  - aktualizace budou vycházet ještě nějakou rozumnou dobu

Ne všechna zařízení jsou dokonalá.

⇒ Je třeba je hlídat a chránit

Opensource - otevřenost

Výhoda

- je vidět co SW dělá

Nevýhoda

- je vidět jak to dělá
  - každý může hledat bezpečnostní chyby

Výhoda

- velká čast chyb byla nalezena už kdysi dávno

Opensource - otevřenost podruhé

Nevýhoda

- bezpečnostní problémy jsou oznamovány veřejně do světa
- je třeba na ně promptně reagovat

Výhoda

- většinou oznamováný až když jsou opraveny
- patche typicky k dispozici
  - nebývá to až tolik práce

Tak jako tak chcete bezpečnostní chyby opravit co nejdřív.

Opensource - podpora

Nevýhoda

- často bez záruky

Výhoda

- občas existují společnosti nabízející support
  - MariaDB
- některé společnosti nabízejí support na ledascos
  - SUSE, RedHat, …
- můžete si najít firmu která vám support udělá
  - nejste vázáni na jednoho dodavatele

Opensource obecně

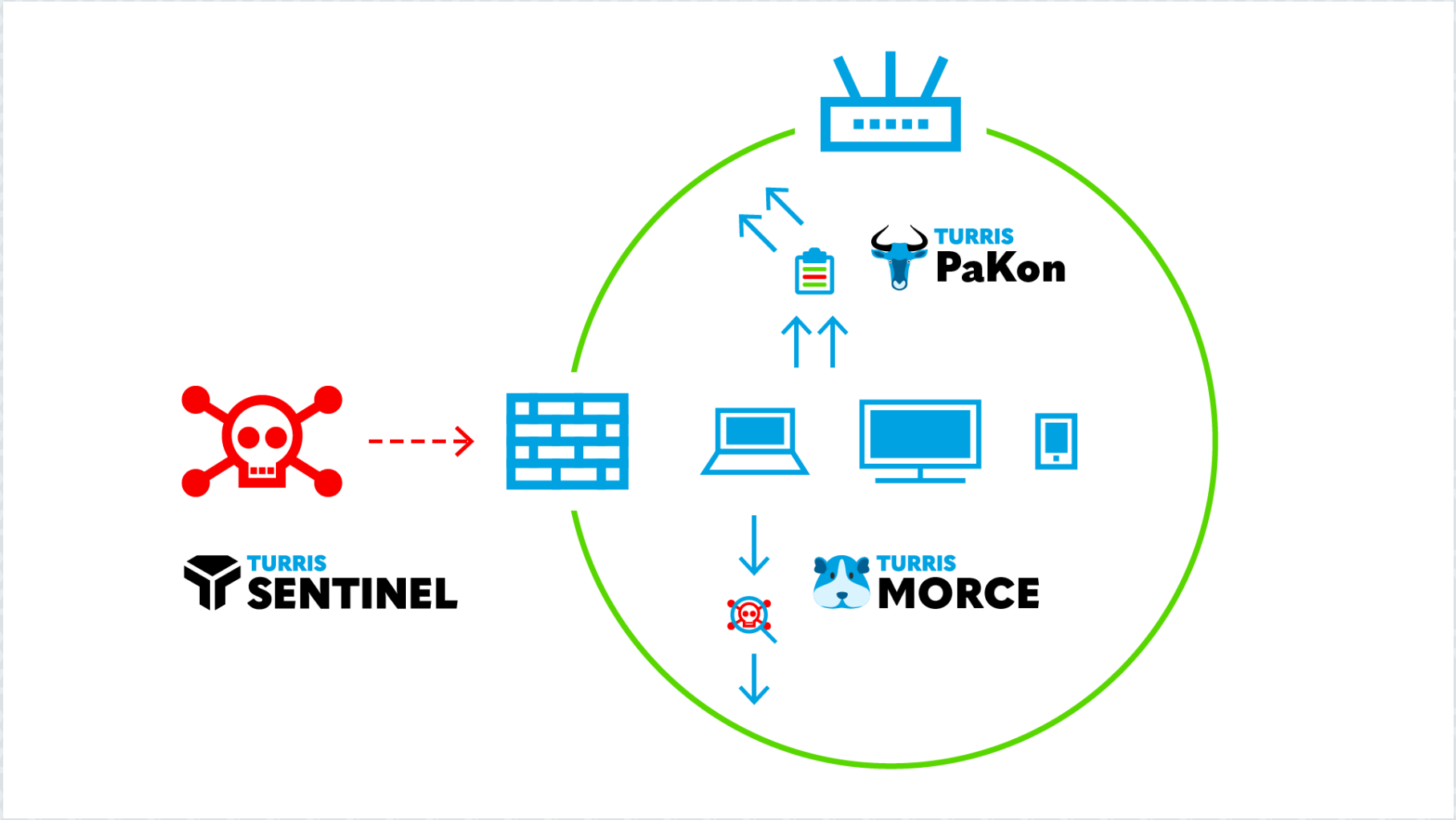
Výhoda

- snadno se nasazuje a integruje
- existuje množství dostupného software
- spolu toho uděláme víc než každý zvlášť

Nevýhoda

- špatně se prodávají licence
  - dají se ale prodávat konzultace, hosting, služby, …

Co děláme pro bezpečnost



Pakoň

- sbírá netflow z lokální sítě
  - stejná zdrojová a cíílová IP a port
  - kdo s kým
  - jak dlouho a kolik

Co sledovat

- přenáší zařízení odpovídající množství dat?
- ve správnou dobu?
- s kým komunikují?

Pakoň - under the hood

Suricata

- IDS/IPS
- dokáže sbírat data o DNS a TLS
- dokáže dodávat i statistiky o flow
- dokáže vše posílat jako json do souboru i socketu

SQLite

- ukládá data
  - jedna v RAM jedna v storage
  - agregace a přelaví dat mezi "buckety"

Problémy

- Suricata je trochu overkill
  - rychlá, ale vezme si nějakou RAM
  - spousta závislostí
  - speciální konfigurák pro Pakoně
  - nové verze závisí na Rustu
    - Rust není v OpenWrt

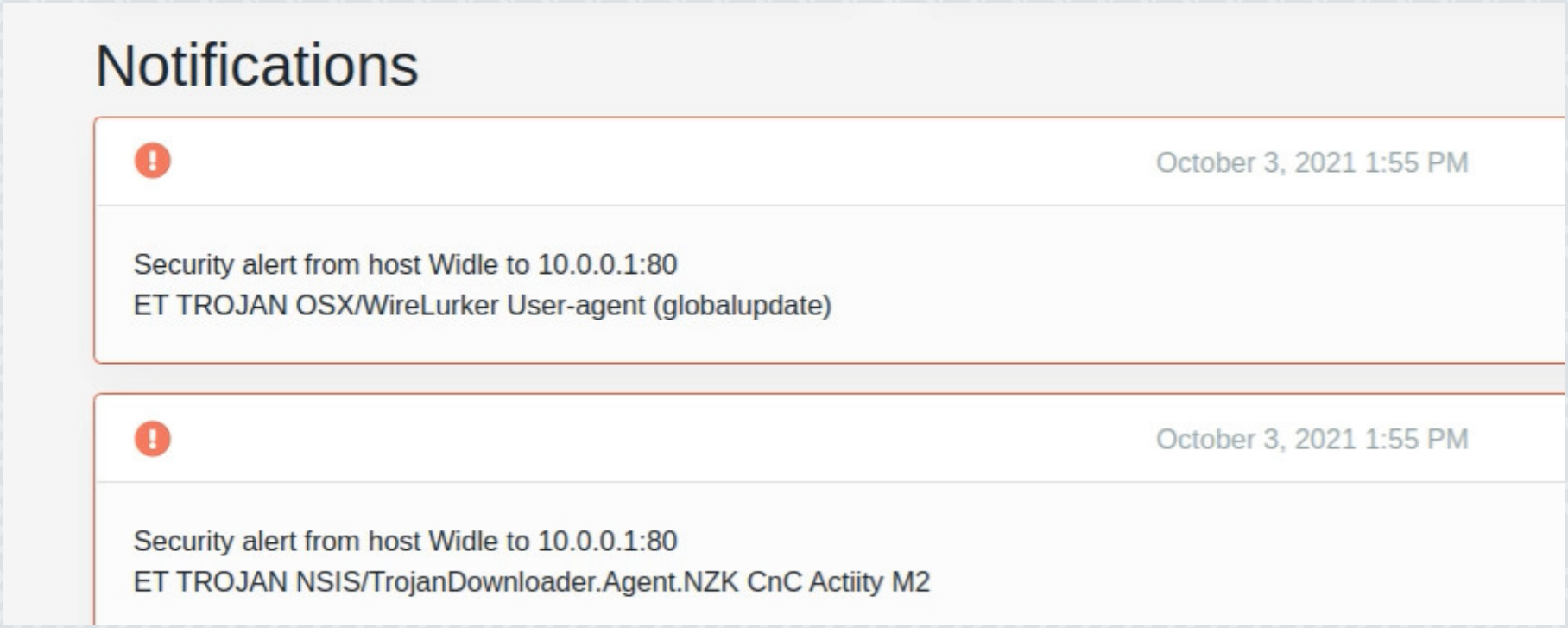
Budoucnost

- vlastní UI
  - aktuálně podobné tomu ve Forisu
  - CSV export navíc
  - bude časem hezčí
- nahrazení Suricaty
  - už teď používáme conntrack
  - nahradíme získávání dat jednoúčelovými programy

https://gitlab.nic.cz/turris/pakon-tools/

Morče - integrace IDS

- zapne IDS nad provozem
- aktualizuje sady pravidel
- generuje notifikace pokud narazí na problém



Morče - under the hood

Snort 3

- C++ only
- Má LUA API

Morče

- spouštěcí script pro Snort se správou pravidel
  - používá Emerging Threads ruleset
- Lua plugin pro Snort
- volání Turris API na generování upozornění
- SQLite na ukládání dat

Děkuji za pozornost

Otázky?

Důležité linky:

- https://view.sentinel.turris.cz
- https://gitlab.nic.cz/turris
- https://doc.emergingthreats.net