Co je nového v Sentinelu?

Miroslav Hanák • miroslav.hanak@nic.cz
Martin Prudek • martin.prudek@nic.cz
10.11.2021

CZ.NIC | SPRÁVCE DOMÉNY CZ

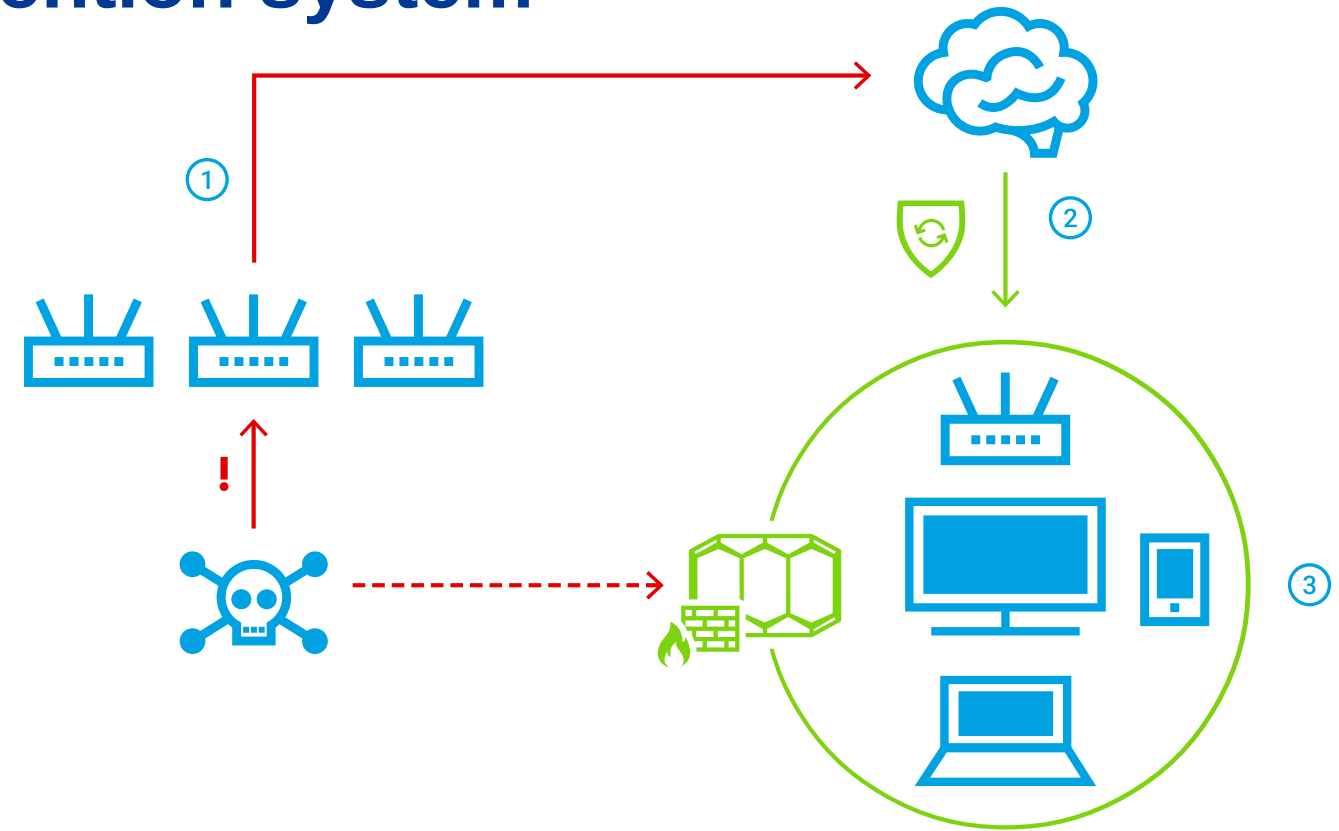
Co Vás čeká ?

- Pár slov o Turrisu
- Co to je a jak funguje Sentinel
- Novinky
- Plány do budoucna

Turris

- Výkonná síťová zařízení
  - (WIFI) router, NAS, VPN server, ...
- Spousta super vlastností:
  - Opensource SW (TOS založen na OpenWRT) i HW
  - Plná kontrola zařízení - root účet
  - Automatické aktualizace, opravy CVE
  - Sentinel
  - ...
- Více o Turrisu
  - https://www.turris.cz
  - přednášky Michala Hrušeckého

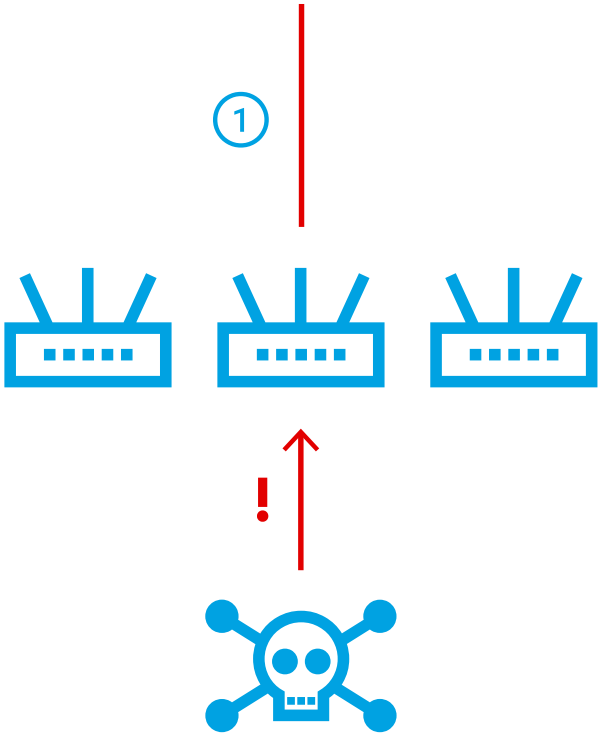
Sentinel – threat detection and cyberattack prevention system



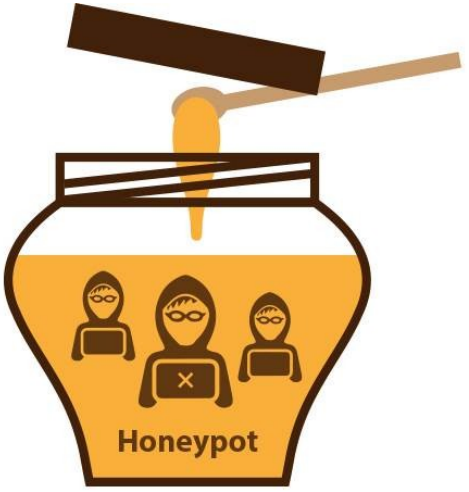
Sběr dat

- Na routeru:
  - Minipoty
  - Firewall logy
  - Dobrovolnost
- Externí zdroje:
  - HaaS – SSH Honeypot as a Service

    https://haas.nic.cz



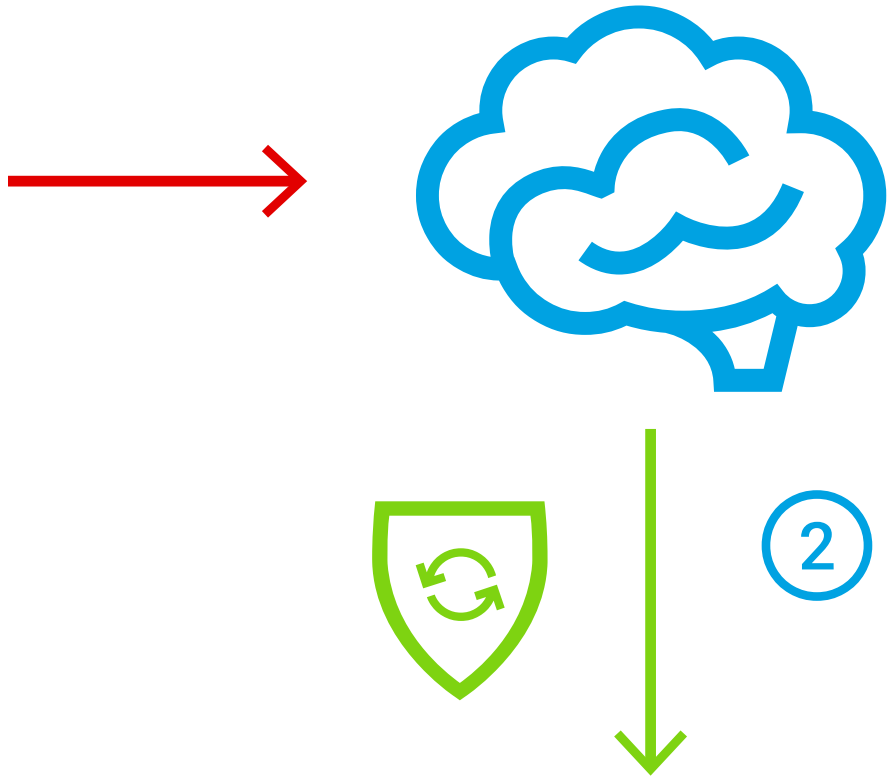
Minipot – minimální honeypot



- Honeypot – past
  - Kontrolované prostředí
  - Sledování útočníkovy aktivity
- Minimální
  - Emulace známých služeb na aplikační vrstvě – Telnet, HTTP, FTP, SMTP
  - Pokusy o připojení a přihlášení

Zpracování dat

- Proudově – data pipelines
  - Message queues
- Série propojených komponent
  - Obohacení dat
  - Analýza
  - Databáze
- Každá IP adresa má skóre
  - Práh



Výstupy

- Seznam škodlivých IP adres – Greylist
  - Veřejně dostupný
- Sentinel View
  - Statistiky dat
  - https://view.sentinel.turris.cz
- Spolupráce s národním CSIRT týmem

Sentinel novinky v TOS 5.3

- Turris Survey v0.2
- Minipoty v2.2 – sjednocení typů zpráv
- Nikola → FWLogs Collector
- Sentinel Proxy v1.4
- Sentinel Overview v reForisu
- Update serverové infrastruktury

Sentinel novinky v TOS 5.3 – Turris Survey

- Volitená část Sentinelu
- Informace o používaných funkcích
  - Nainstalované balíčky
  - Jazykové mutace
- Nově ve verzi 0.2

Sentinel novinky v TOS 5.3 – Minipoty

- Volitená část Sentinelu
- „Minimální honeypoty“ - Telnet, SMTP, FTP, HTTP
- Produkují eventy na základě chování útočníků
- Nově ve verzi 2.2 – sjednocení eventů
  - Connect
  - Login
  - Invalid
  - Message (pouze HTTP)

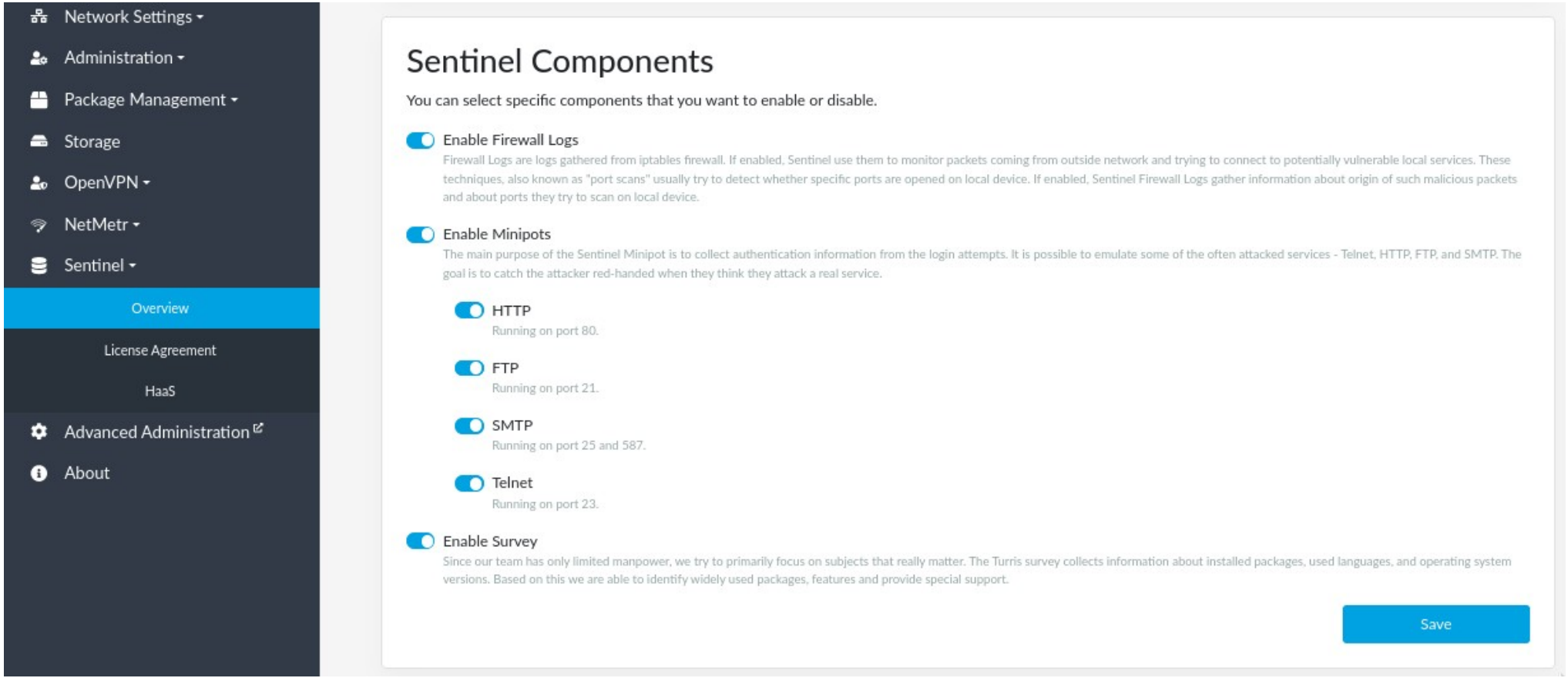
Sentinel novinky v TOS 5.3 – FWLogs collector

- Volitená část Sentinelu
- = Firewall monitoring
- Sběr FW logů o odmítnutých nebo zahozených spojeních
- Náhrada „one shot“ skriptu Nikola za FWLogs collector
  - C
  - Netlink, knihovna libnetfilter_log
  - Rychlejší odezva na události
  - Nižší režie

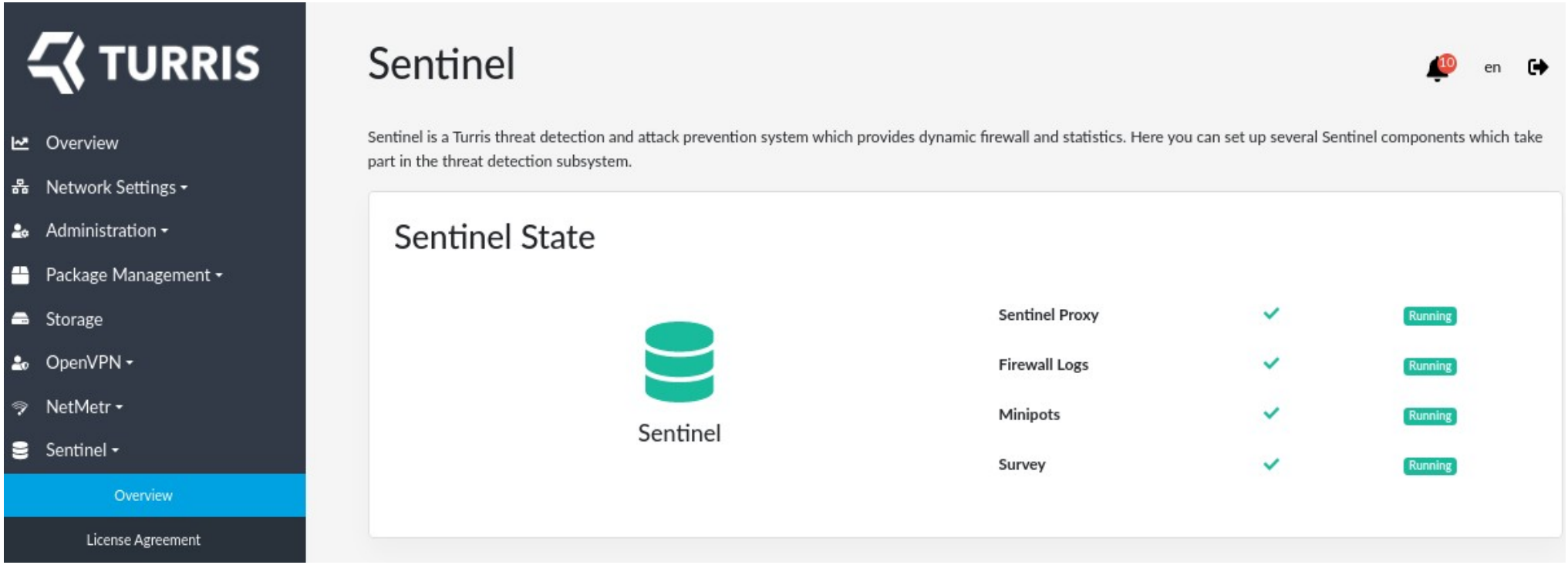
Sentinel novinky v TOS 5.3 – Sentinel Proxy

- Vychozí brána na routeru pro spojení na server
- Udržuje bezpečný komunikační kanál
- Nově ve verzi 1.4
  - Interní refactoring
  - Příprava pro zobrazení informací o aktivitě v reForisu

Sentinel novinky v TOS 5.3 – Sentinel Overview



Sentinel novinky v TOS 5.3 – Sentinel Overview



Nápady do budoucna

- Zobrazení poslední aktivity v reForisu
- Inspirace službou „Have I been pwned“
- Příprava na plnohodnotný běh Sentinelu mimo Turris
- Nasazení nového Sentinel View

Děkujeme za pozornost

Miroslav Hanák • miroslav.hanak@nic.cz
Martin Prudek • martin.prudek@nic.cz
10.11.2021

CZ.NIC | SPRÁVCE DOMÉNY CZ