

Co je nového v Sentinelu?

Miroslav Hanák • miroslav.hanak@nic.cz

Martin Prudek • martin.prudek@nic.cz

10.11.2021

Co Vás čeká ?

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

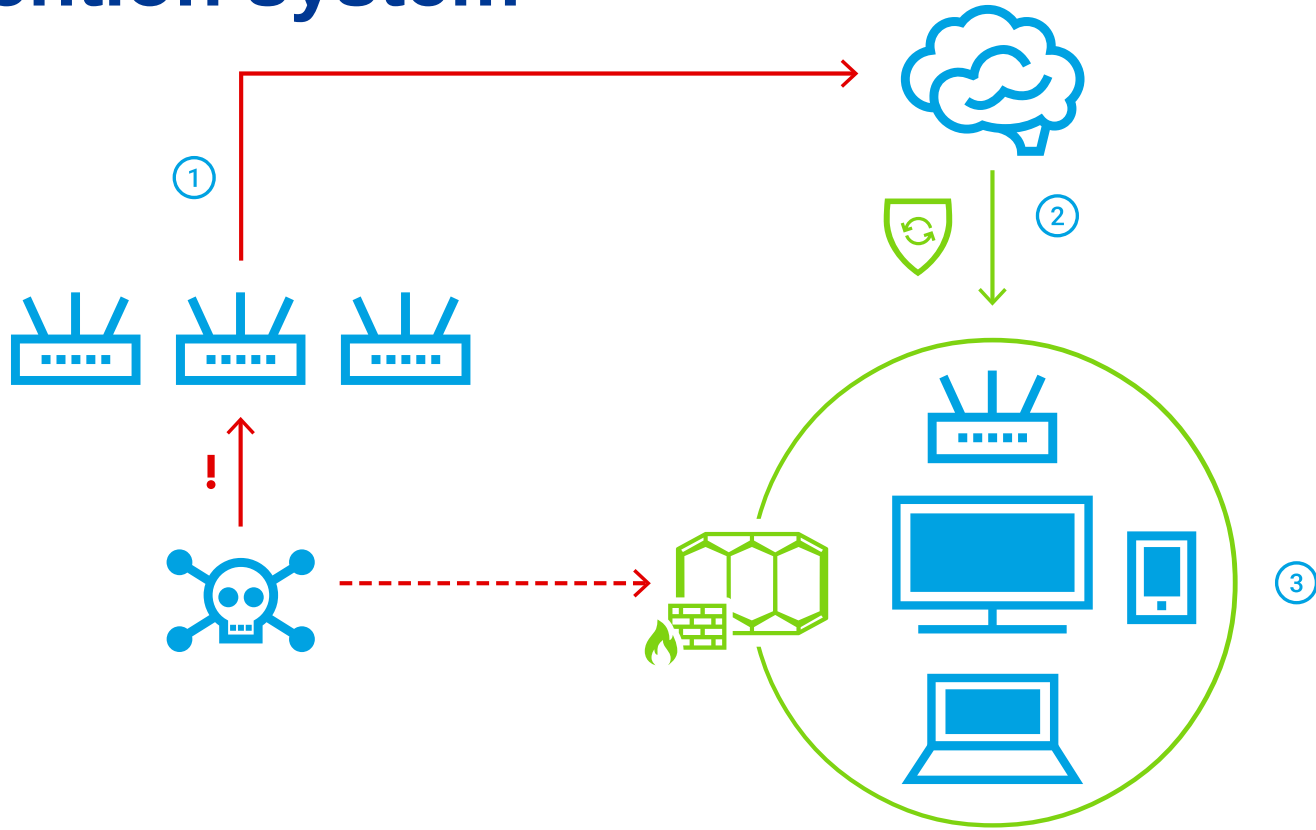


Turris

- 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

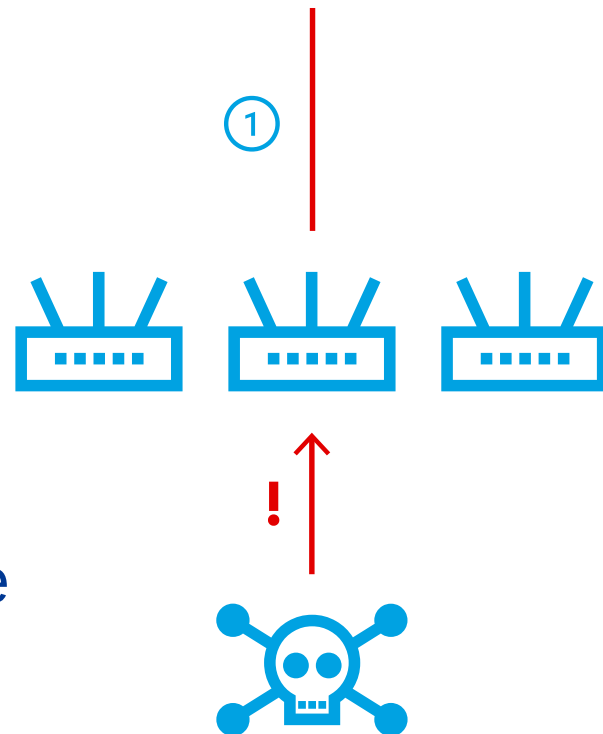


Sentinel – threat detection and cyberattack prevention system



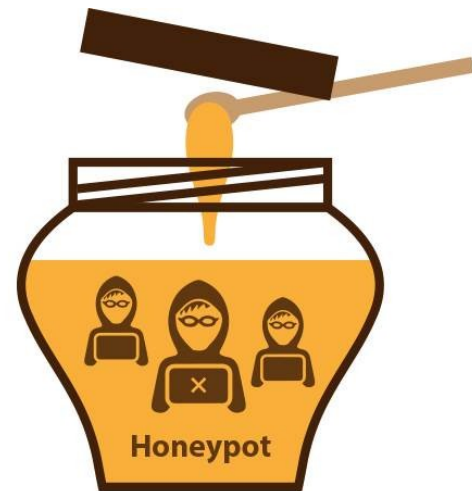
Sběr dat

- Na routeru:
 - Minipoty
 - Firewall logy
 - Dobrovolnost
- Externí zdroje:
 - HaaS – SSH Honeypot as a Service
<https://haas.nic.cz>



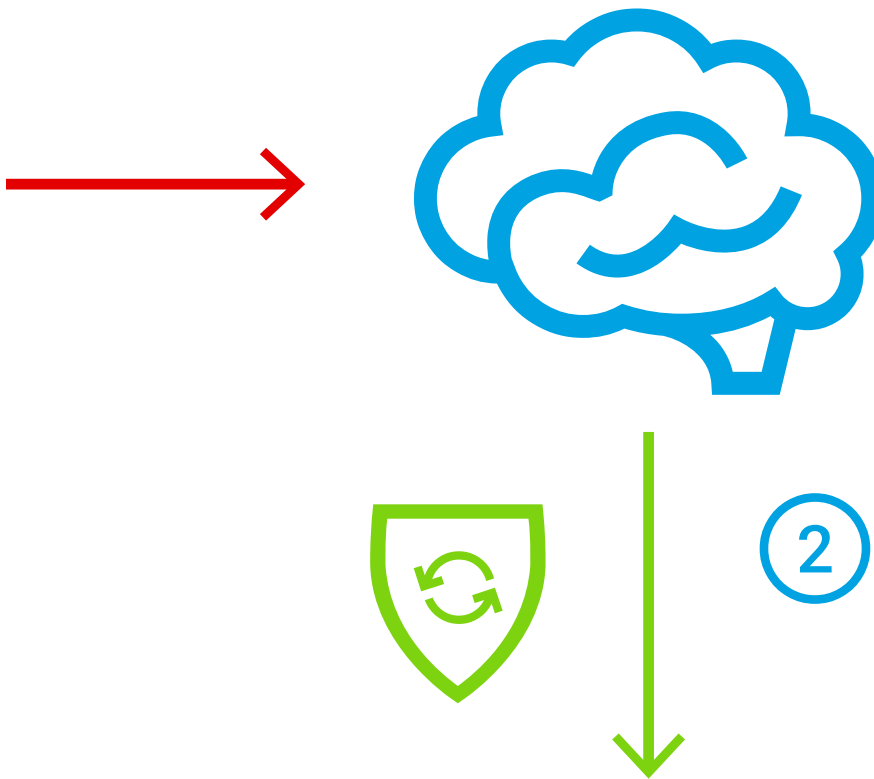
Minipot – minimální honeypot

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



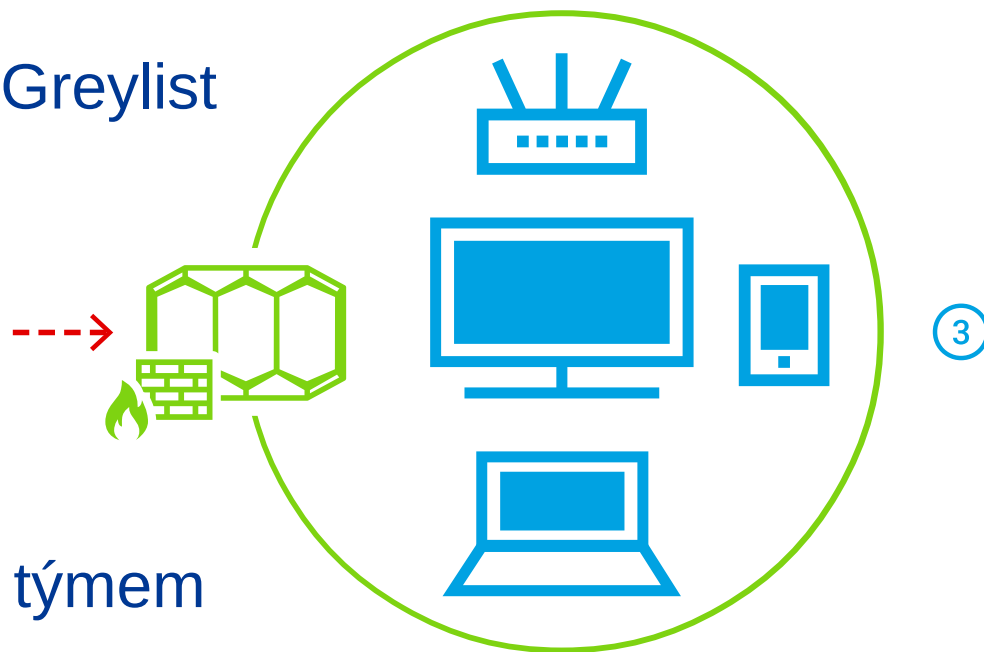
Zpracování dat

- 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

- Vychází 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

Network Settings ▾

Administration ▾

Package Management ▾

Storage

OpenVPN ▾

NetMetr ▾

Sentinel ▾

Overview

License Agreement

HaaS

Advanced Administration ↗

About

Sentinel Components

You can select specific components that you want to enable or disable.

☒

Enable Firewall Logs
Firewall Logs are logs gathered from iptables firewall. If enabled, Sentinel use them to monitor packets coming from outside network and trying to connect to potentially vulnerable local services. These techniques, also known as "port scans" usually try to detect whether specific ports are opened on local device. If enabled, Sentinel Firewall Logs gather information about origin of such malicious packets and about ports they try to scan on local device.

☒

Enable Minipots
The main purpose of the Sentinel Minipot is to collect authentication information from the login attempts. It is possible to emulate some of the often attacked services - Telnet, HTTP, FTP, and SMTP. The goal is to catch the attacker red-handed when they think they attack a real service.

☒

HTTP
Running on port 80.

☒

FTP
Running on port 21.

☒

SMTP
Running on port 25 and 587.

☒

Telnet
Running on port 23.

☐

Enable Survey
Since our team has only limited manpower, we try to primarily focus on subjects that really matter. The Turris survey collects information about installed packages, used languages, and operating system versions. Based on this we are able to identify widely used packages, features and provide special support.

Save



Sentinel novinky v TOS 5.3 – Sentinel Overview



- Overview
- Network Settings ▾
- Administration ▾
- Package Management ▾
- Storage
- OpenVPN ▾
- NetMetr ▾
- Sentinel ▾

Overview

License Agreement

Sentinel

 en 

Sentinel is a Turrus threat detection and attack prevention system which provides dynamic firewall and statistics. Here you can set up several Sentinel components which take part in the threat detection subsystem.

Sentinel State



Sentinel

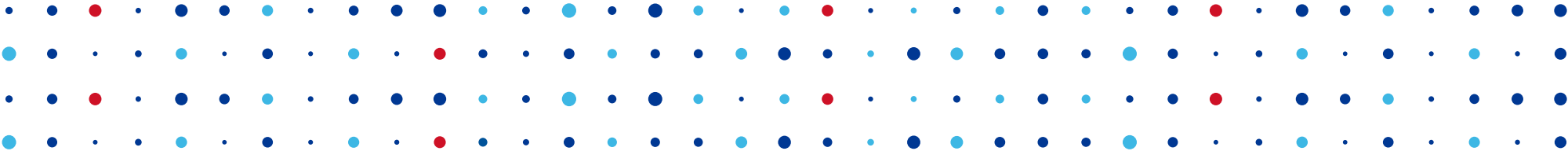
Sentinel Proxy	✓	Running
Firewall Logs	✓	Running
Minipots	✓	Running
Survey	✓	Running



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