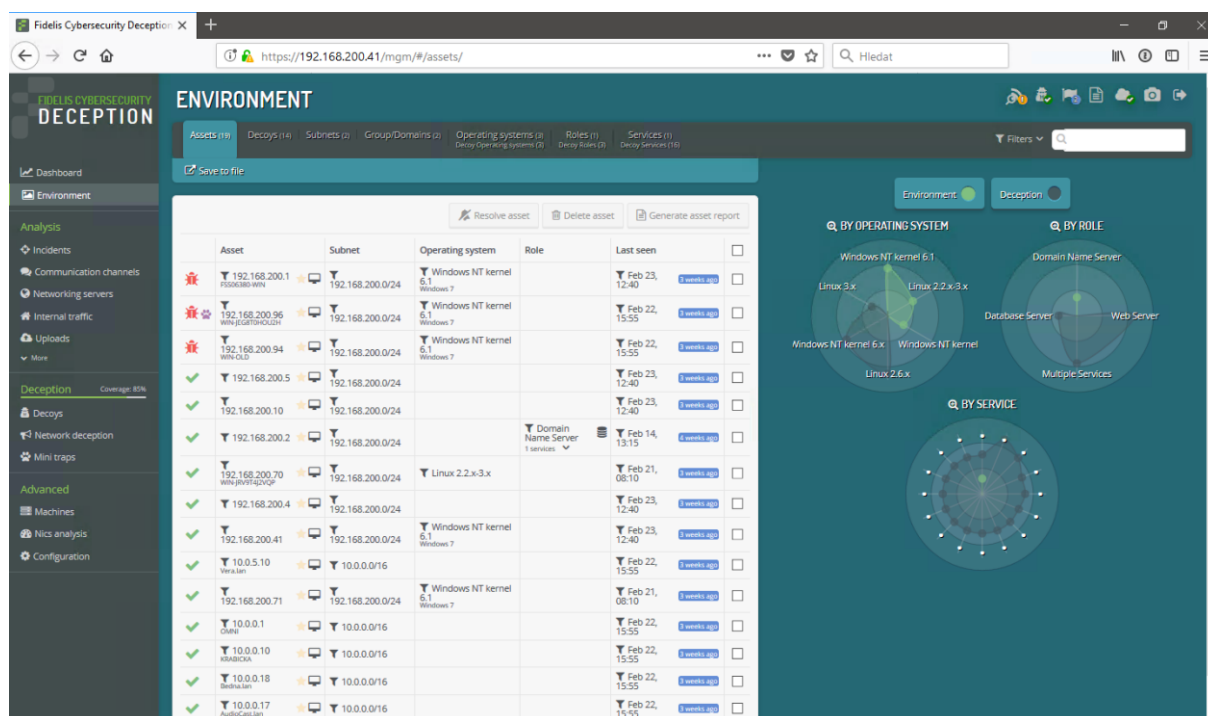


Obr. 1 - Snímek se zobrazením "Subnets"



Obr. 2 – Snímek se zobrazením "Assets"

MINI TRAPS

Add mini traps Create new generator

Minitrapped program	Leads to decoy	Leads to decoy service	Subnet
Putty SSH Client	10.0.9.9	SSH server	10.0.0.0/16
WinSCP Client	10.0.9.9	SSH server	10.0.0.0/16
Internet Explorer	10.0.9.3	Web Server	10.0.0.0/16
Putty SSH Client	10.0.9.4	SSH server	10.0.0.0/16
Internet Explorer	10.0.9.4	Web Server	10.0.0.0/16
WinSCP Client	10.0.9.4	SSH server	10.0.0.0/16
Internet Explorer	10.0.9.9	Web Server	10.0.0.0/16
Putty SSH Client	10.0.9.3	SSH server	10.0.0.0/16
WinSCP Client	10.0.9.3	SSH server	10.0.0.0/16

Instructions: To apply mini traps on entire network, please run the downloaded script using power shell and follow instructions. Note that the power-shell script is unsigned; you can either sign it manually or allow the unsigned execution using the following power-shell command: "Set-ExecutionPolicy Unrestricted".

Obr. 3 – Snímek se zobrazením "Minitraps"

INCIDENTS

3 Infected assets 15 Decoy activity

Incident (19) Decoy activity (19) Network incident activity (0)

Feb 22

Severity	Incident	Incident group	Asset	Subnet	Time
High	SSH Session Manipulation (5 events)	Decoy Interaction	192.168.200.1	192.168.200.0	Feb 22, 10:40
High	Web Server Manipulation (4 events)	Decoy Interaction	192.168.200.94	192.168.200.0	Feb 22, 06:20

A Node is accessing the Web Server on the DECOY System. This is a severe indication as no Node in the organization should be accessing this resource.

IP	Port	Host	Protocol	Time
192.168.200.4 (Decoy)	80	MULTIPLESERVD	HTTP	Feb 22, 06:19

Obr. 4 - Snímek se zobrazením "Incidents"